KriPoZ Kriminalpolitische Zeitschrift JuP

„Junges Publizieren“

Seminararbeit von

Annika Schulte

Das Eckpunktepapier zum Gesetz gegen digitale Gewalt

Universität zu Köln
Institut für Strafrecht und Strafprozessrecht
Prof. Dr. Anja Schiemann
Abgabedatum: 27.10.2023

Inhaltsverzeichnis

I. Einleitung

Hate Speech, Cyber-Grooming, Cyber-Stalking, Cyber-Mobbing, Diskriminierung, Beleidigung, Belästigung, Doxing, Revenge Porn, Deepfakes, etc. Den Möglichkeiten von Rechtsverletzungen oder sogar Straftaten im digitalen Raum scheinen keine Grenzen gesetzt zu sein. Deshalb überrascht es nicht, dass bei einem Blick in soziale Medien, Kommentarfelder, Webseiten, Blogs, Instant Messenger oder Chatforen rechtsverletzendes Verhalten in den verschiedenen Formen immer wieder zu finden ist. Die Vielzahl der Fälle legt die Vermutung nahe, dass Nutzer den Eindruck haben, dass beim sozialen Umgang im Internet im Vergleich zum analogen Raum wohl andere (oder sogar weniger) Regeln herrschen könnten, so oft wie es dort zu sichtbarem, rechtsverletzendem oder strafbarem Verhalten kommt. Ein immer wieder gern zitierter Satz dazu ist jedoch: „Das Internet ist kein rechtsfreier Raum". Und das nicht zu Unrecht, denn im Internet finden die gleichen Normen Anwendung, wie auch im analogen Raum. Obwohl einige bestimmte delinquente Verhaltensweisen (wie beispielsweise Cybermobbing), die ausschließlich den digitalen Raum betreffen, (bisher) keine eigenständigen Straftatbestände sind, so können dennoch, je nach Fallgestaltung, andere Strafnormen wie beispielsweise Beleidigung (§ 185 StGB), Üble Nachrede (§ 186 StGB), Verleumdung (§ 187 StGB) oder Bedrohung (§ 241 StGB) verwirklicht sein. Dennoch kommt es häufig zu offensichtlichen und nicht verfolgten oder nicht verfolgbaren Rechtsverletzungen und Straftaten im Internet. Damit muss zwangsläufig die Frage gestellt werden: ist das Internet kein rechtsfreier, sondern vielmehr ein rechtsdurchsetzungsfreier Raum? Mit dieser Frage hat sich auch die Ampelregierung beschäftigt, die bereits in ihrem Koalitionsvertrag festhielt, ein „Gesetz gegen digitale Gewalt" schaffen zu wollen.[1] Damit soll eine leichtere und effektivere Rechtsdurchsetzung für Privatpersonen im digitalen Raum geschaffen werden.

Die Aktualität und Relevanz dieses Vorhabens und dessen Umsetzung wird vor allem auch im Bereich der Verbreitung von Falschinformationen und Gewaltaufrufen deutlich. Während soziale Medienplattformen durch die Digitalisierung ein wichtiges Medium zur Verbreitung von Informationen und Nachrichten sowie des Meinungsaustauschs geworden sind, ist die Gefahr für eine ungehinderte Verbreitung von Fehlinformationen und die Auslösung digitaler Hasswellen (sog. Hate-Speech), die auf bestimmte Bevölkerungsgruppen gerichtet sind, groß. Besonders deutlich wird die Tragweite bei Konflikten und Kriegen wie der aktuellen Eskalation des Nahostkonflikts. Die Vermutung einer sich bedingenden Relation zwischen ansteigender digitaler sowie analoger Gewalt demonstriert die Signifikanz und Notwendigkeit digitaler durchsetzbarer Regelungen. Im April 2023 wurde vom Bundesministerium für Justiz das Eckpunktepapier zum Gesetz gegen digitale Gewalt veröffentlicht, um die Herausforderungen im digitalen Raum zu adressieren.

Gegenstand dieser Arbeit ist es, zu erörtern, ob und inwiefern die im Eckpunktepapier aufgeführten Vorhaben dem Ziel des Gesetzes gerecht werden und inwiefern dabei europäische Vorgaben sowie die (Grund-)Rechte der Beteiligten hinreichend gewürdigt werden.

Im Zuge dessen wird zunächst ein Überblick über das Phänomen digitaler Gewalt, sowie die historische und rechtliche Ausgangslage gegeben. Daraufhin folgt eine Erläuterung des Ziels des geplanten Gesetzes, sowie die Darlegung der einzelnen im Eckpunktepapier beschriebenen Vorhaben. Diese werden anschließend kritisch eingeordnet.

[1] Koalitionsvertrag 2021, S. 17 f., abrufbar unter: https://www.bundesregierung.de/resource/blob/974430/1990812/1f422c60505b6a88f8f3b3b5b8720bd4/2021-12-10-koav2021-data.pdf?download=1 (zuletzt abgerufen am 27.10.2023).

II. Digitale Gewalt

Aufgrund der Komplexität von „digitaler Gewalt" gibt es (bisher) keine einheitliche Definition des Phänomens und nur wenige konkrete empirische Daten zum Erscheinungsbild. 2021 verzeichnete das Bundeskriminalamt (BKA) mit 146.363 Delikten einen neuen Höchstwert bei Cyber-Straftaten.[2] Doch spezifische Zahlen zum Bereich digitaler Gewalt werden nicht ermittelt. Allerdings ist ersichtlich, dass sich Kriminalität zunehmend in den digitalen Raum verlagert – während die in der PKS erfassten Straftaten 2015-2022 rückläufig sind, sind Straftaten im digitalen Raum deutlich angestiegen.[3] Hasspostings im Bereich „ausländischer Ideologie" verzeichneten beispielsweise zwischen 2021 und 2021 einen Anstieg von ca. +128 %.[4]

Digitale Gewalt lässt sich schemenhaft beschreiben als verschiedene Formen der Herabsetzung, Belästigung, Diskriminierung und Nötigung anderer Menschen mit Hilfe elektronischer Kommunikationsmittel über soziale Netzwerke, in Chaträumen, beim Instant Messaging und/oder mittels mobiler Telefone. Dabei kann digitale Gewalt verschiedene Delikte wie Beleidigung (§ 185 StGB) oder Verleumdung (§ StGB) umfassen, aber auch Handlungen, welche die Strafbarkeitsschwelle gar nicht übertreten oder die (bisher) keine eigenen Straftatbestände sind. Dazu bespielhaft zu nennen ist Cybermobbing, welches ein „vorsätzliches, aus negativen Einzelhandlungen bestehendes Verhalten, das sich gegen eine – zumindest in Folge dieser Handlung – schwächere Person richtet und mit Hilfe von Informations- und Kommunikationsmedien erfolgt" beschreibt.[5] Ebenfalls beispielhaft zu nennen ist sog. Hate Speech, welche als „öffentlich, gegen bestimmte Personengruppen gerichtete Aussage mit dem Ziel, diese Gruppen abzuwerten, auszugrenzen oder zu demütigen" beschrieben werden kann.[6]

Digitale Gewalt zeichnet sich zusätzlich dadurch aus, dass sie im Internet, also beispielsweise in sozialen Medien oder Chatforen, ausgeübt wird. Für den digitalen Raum ist kennzeichnend, dass darin sehr günstige Tatbegehungsstrukturen für Rechtsverletzungen (bis hin zu digitaler Gewalt) bestehen.[7] Im Internet bietet sich ein unendlicher sozialer Raum, um potenzielle Opfer kontaktieren zu können.[8] Die dabei leicht umsetzbare Anonymität im Internet unterstützt zudem den hohen Nutzen für Täter im Gegensatz zum niedrigen Entdeckungs- und Sanktionsrisiko (welches maßgeblicher Faktor bei der Begehung von Straftaten ist).

Der grundsätzlich geringe zeitliche und finanzielle Aufwand (beispielsweise eine Nachricht ist schnell geschrieben und veröffentlicht) steht im außerordentlich unausgeglichenen Verhältnis zu den Auswirkungen, die (sogar nur einmal) veröffentlichte Bilder, Videos oder Nachrichten erwirken können. Denn die Speicherung digitaler Inhalte ist umfassend, ungefiltert und grundsätzlich dauerhaft,[9] sodass vor allem von digitaler Gewalt regelmäßig erhebliche Belastungen für Betroffene ausgehen. Dabei verdeutlicht die sog. „Mediatisierung" des Alltags, also der gesellschaftliche Wandel hin zu einer Verschmelzung von Alltag, Kultur, Gesellschaft und digitalen Medien,[10] dass sich die Auswirkungen von digitaler Gewalt, obwohl diese im digitalen Raum begangen wird, keinesfalls nur auf diesen beschränken, sondern sich auf alle (auch analoge) Lebensbereiche ausbreiten. Meist ist digitale Gewalt

---

2 BKA, Bundeslagebild Cybercrime, S. 3, abrufbar unter: https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2022/Presse2022/220509_PM_CybercrimeBLB.html (zuletzt abgerufen am 27.10.2023).
3 BKA, Cybercrime 2021, S. 4.
4 BKA, Politisch motivierte Kriminalität: Bundesweite Fallzahlen, S. 12, abrufbar unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2021.pdf?__blob=publicationFile&v=6 (zuletzt abgerufen am 27.10.2023).
5 *Doerbeck*, Cybermobbing: Phänomenologische Betrachtung und strafrechtliche Analyse, 2019, S. 114.
6 *Wachs/Schubarth/Blitz*, Hate Speech als Schulproblem? Erziehungswissenschaftliche Perspektiven auf ein aktuelles Phänomen, 2020, S. 224.
7 *Neubacher,* Kriminologie, 5. Aufl. (2023), S. 236.
8 Ebd.
9 *Nolte,* ZRP 2011, 236 (236).
10 *Hartmann/Krotz*, in: Schweiger/Beck, Handbuch Online-Kommunikation, 2. Aufl. (2019), S. 275.

darüber hinaus Ergänzung oder Verstärkung von „analoger Gewalt“.[11] Die Folgen für Betroffene sind unterschiedlich und komplex, sie reichen von Wut, Angst sozialem Rückzug und psychosomatischen Beschwerden über Traumatisierung und Depression bis hin zu Suizidgedanken, -versuchen oder sogar -vollendungen.[12] Die Komplexität des Themas der digitalen Gewalt und günstige Tatbegehungsstrukturen für Täter betonen, dass effiziente und durchsetzbare Regelungen auch im digitalen Raum von erheblicher Bedeutung sind.

III. Ausgangslage

Bemühungen des Gesetzgebers, die Verfolgung von Straftaten und Rechtsverletzungen im Internet effizienter zu gestalten sind daher keinesfalls eine neue Initiative. Nachdem bereits 2015 strafbare Hassbotschaften, die über soziale Netzwerke verbreitet wurden, besondere Aufmerksamkeit von Öffentlichkeit und Politik erhielten, trat schließlich am 1.10.2017 das Netzwerkdurchsetzungsgesetz (NetzDG) in Kraft.[13] Ziel war es, die Rechtsdurchsetzung in sozialen Netzwerken zu verbessern und gegen Hass und Hetze sowie gezielte Fake-News im Internet vorzugehen.[14] Maßnahmen waren dabei zum Beispiel die Verpflichtung sozialer Netzwerke, offensichtlich rechtswidrige Inhalte innerhalb enger Fristen zu löschen oder zu sperren (§ 3 Abs. 2 Nr. 2 NetzDG).[15] Dabei adressiert das NetzDG lediglich Telemedienanbieter unter bestimmten Voraussetzungen wie einer mindest-Nutzeranzahl[16] und unterlag im Laufe der Zeit mehreren Novellierungen.[17]

Der Mord an Walter Lübcke im Juni 2019 und die vorausgegangenen, jahrelangen Anfeindungen und Morddrohungen im Netz, haben die Debatte um Hasskriminalität im Internet erneut in den Fokus der Öffentlichkeit und Politik gerückt und maßgeblich geprägt. Zudem wird digitale Gewalt im Zusammenhang mit Desinformationen häufig als Faktor für Radikalisierung angesehen.[18] Das daraufhin 2021 beschlossene Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität[19] sollte daher insbesondere Tatbegehungen im Internet effektiver bekämpfen. Dabei wurde unter anderem für Anbieter sozialer Netzwerke eine Meldepflicht an das Bundeskriminalamt (BKA) für bestimmte strafbare Inhalte geschaffen (§ 3a NetzDG).[20] Außerdem wurden 2021 einige Änderungen eingeführt, die auch Straftaten im oder durch den digitalen Raum betreffen. [21] Dazu gehört bspw. die Einführung des § 192a StGB, welcher eine Schutzlücke zwischen Beleidigung (§ 185 StGB) und Volksverhetzung (§ 130) schließen sollte.[22] Dies betrifft vor allem auch online verbreitete verhetzende Beleidigungen und sog. Hatespeech. Neu eingeführt wurde darüber hinaus der § 126a StGB, mit dem vor allem der strafrechtliche Schutz vor sogenannten „Feindeslisten“ verbessert werden sollte, bei denen unter anderem persönliche Daten insbesondere im Internet verbreitet werden. [23] Novelliert wurde zudem ebenfalls 2021 der Cyberstalking-Tatbestand des § 238 StGB.[24]

---

11 *Clemm,* in: Prasad, Geschlechtsspezifische Gewalt in Zeiten der Digitalisierung, 2021, S. 129.
12 *Bocian/Lütgens/Wagner,* in: Prasad, S. 200.
13 BGBl. 2017 I, S. 3352, 3355.
14 *Apostel*, KriPoZ 2019, 287 (289).
15 *Liesching*, MMR 2023, 56 (56).
16 *Hoven/Gersdorf*, in: BeckOK-InfoMedienR, NetzDG, 41. Ed. (Stand 1.8.2023), § 1 Rn. 12 ff.; *Redeker*, IT-Recht, 8. Aufl. (2023), Rn. 1128.
17 *Gerhold/Handel*, in: NK-MedienStrafrecht, NetzDG, 2023, § 1 Rn. 3-5.
18 *Paal/Hennemann,* ZRP 2017, 215 (216).
19 BGBl. 2021 I, S. 441 ff.
20 *Liesching*, MMR 2023, 56 (57).
21 BGBl. 2021 I, S. 4250.
22 *Kargl,* in: NK-StGB, Bd. 3, 6. Aufl. (2023), § 192a Rn. 3.
23 BT-Drs. 19/28678, S. 1.
24 BGBl. 2021 I, S. 3513 f.

Auch die Europäische Union beschäftigt sich kontinuierlich mit der Nutzung und Bereitstellung digitaler Dienste, wobei auch immer wieder digitale Gewalt eine entscheidende Rolle spielt. Besonders hervorzuheben ist dabei der Digital Services Act des Europäischen Parlaments, der am 19.10.2022 erlassen wurde.[25] Während einige Normen dessen bereits in Kraft sind, erlangt der DSA vollständige Geltung im Februar 2024. Gegelt wird damit primär die Haftung sowie besondere Sorgfaltspflichten digitaler Vermittlungsdienste, wie Regeln zur Moderation und Ansprechstellen für Betroffene großer Online-Plattformen wie Facebook, X (ehemals Twitter) und Co.[26] Ziel des DSA ist durch die Harmonisierung der Vorschriften digitaler Vermittlungsdienste die Stärkung der Funktionsfähigkeit des Binnenmarkts sowie die Schaffung eines „sicheren, vorhersehbaren und vertrauenswürdigen Online-Umfelds" (Art. 1 Abs. 1 DSA).[27] Inwieweit EU-Mitgliedstaaten über den DSA hinausgehende Handlungsspielräume für nationale Regelungen haben ist fraglich und einzelfallabhängig. Für die Möglichkeit für zusätzliche nationale Regelungen ist notwendig, dass diese außerhalb des Anwendungsbereichs des DSA liegen oder der DSA dies ausdrücklich vorsieht bzw. andere Unionsrechtsakte noch Spielraum für eigene Maßgaben einräumen.[28] Während durch die Einführung des DSA große Teile des NetzDG ohnehin obsolet werden, da sich die Regelungsbereiche stark überschneiden,[29] soll das NetzDG laut Eckpunktepapier damit sogar gänzlich aufgehoben werden.[30]

IV. Ziel des Gesetzes

Während der Fokus der Bundesregierung der vorherigen Wahlperiode 2017-2021 auf der strafrechtlichen Verfolgung von „Hasskriminalität" und „Plattformregulierung" lag, soll nun im Sinne des Koalitionsvertrags 2021 die Durchsetzbarkeit der gesetzlichen Ansprüche durch die Betroffenen den Schwerpunkt des geplanten Gesetzes des Bundesjustizministeriums (BMJ) bilden. Konkretes Ziel ist der „Effektive Rechtsschutz im digitalen Raum".[31] Im Eckpunktepapier wird hervorgehoben, dass das gegenwärtige Recht keine hinreichenden Möglichkeiten zur Rechtsdurchsetzung für Betroffene von Rechtsverletzungen im digitalen Raum bietet.[32]
Daher soll für Betroffene erleichtert werden, gegen Rechtverletzungen effektiv vorgehen zu können, indem zügig und mit vertretbarem Aufwand Auskunft über die Identität der Verfasser rechtswidriger Inhalte erlangt werden kann.[33] Daraus sollen keine Änderungen des Strafrechts ergehen und die grundsätzliche Freiheit zur anonymen Meinungsäußerung soll gewahrt bleiben.[34]

V. Inhalt

Eine im Eckpunktepapier genannte zentrale Maßnahme des Gesetzes gegen digitale Gewalt soll ein ausgeweitetes Auskunftsverfahren (1.) für eine effizientere Möglichkeit der Identifizierung von Verfassern rechtsverletzender

[25] Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste, Digital Services Act), ABl. 2022 L 277, S. 1.
[26] *Raue/Heesen*, NJW 2022, 3537.
[27] *Hofmann,* in: NK-DSA, 2023, Rn. 1.
[28] *Kuhlmann,* ZUM 2023, 170 (172).
[29] *Gerdemann/Spindler,* GRUR 2023, 3 (3); *Hoven/Gersdorf,* in: BeckOK-InfoMedienR, § 1 Rn. 11c.
[30] BMJ, Eckpunkte für ein Gesetz gegen digitale Gewalt v. 10.4.2023, S. 6, abrufbar unter: https://www.bmj.de/SharedDocs/Downloads/DE/Gesetzgebung/Eckpunkte/Digitale_Gewalt_Eckpunkte.pdf?__blob=publicationFile&v=2 (zuletzt abgerufen am 27.10.2023).
[31] BMJ, Kurzpapier zum Erläuterungspapier für ein Gesetz gegen digitale Gewalt v. 10.04.2023, S. 1, abrufbar unter: https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/DE/2023_Digitale_Gewalt.html Gesetzgebung - Eckpunkte für ein Gesetz gegen digitale Gewalt (zuletzt abgerufen am 27.10.2023).
[32] BMJ, Eckpunktepapier, S. 1.
[33] BMJ, Eckpunktepapier, S. 1 f.
[34] BMJ, Eckpunktepapier, S. 2.

Äußerungen sein. Weitere Maßnahmen sind ein geplanter Anspruch auf richterlich angeordnete Accountsperren (2.) sowie die Erleichterung der Zustellung gerichtlicher sowie außergerichtlicher Schreiben an inländische Zustellungsbevollmächtigte (3.).

1. Stärkung privater Auskunftsverfahren

a) Erweiterung des Anwendungsbereichs des Auskunftsverfahren

Zunächst sollen Privatpersonen gestärkt werden, indem der Anwendungsbereich des Auskunftsverfahrens erweitert wird. Da die Herausgabe von Nutzungsdaten bisher auf Bestandsdaten wie Name und E-Mail-Adresse beschränkt waren, sollen zukünftig, insofern dies verhältnismäßig und für die Rechtsverfolgung notwendig ist, auch Nutzungsdaten wie z.B. die IP-Adresse von Nutzenden herausgegeben werden müssen.[35] Darüber hinaus soll die Herausgabe nicht wie bisher lediglich bei Fällen bestimmter strafbarer Inhalte möglich sein, sondern zusätzlich bei der Verletzung absoluter Rechte.[36] Zur Herausgabe der Daten sollen unter bestimmten Voraussetzungen auch Messenger- und Internetzugangsanbieter verpflichtet werden können, während bisher lediglich Anbieter von Telemedien umfasst waren.

b) Effektivere Ausgestaltung des Auskunftsverfahrens

Durch eine Beweissicherungsanordnung soll sichergestellt werden, dass verfahrensrelevante Daten nicht vor Ablauf des Verfahrens gelöscht (und ein Auskunftsanspruch damit verhindert) werden.[37] Um dies zu gewährleisten, sollen Dienstanbieter verpflichtet werden können, Bestands- und Nutzungsdaten des Verfassers, sowie die Äußerung selbst, bis zum Abschluss des Auskunftsverfahrens gezielt zu sichern. Dabei sollen Diensteanbieter bereits in einem frühen Verfahrensstadium zur Offenlegung der IP-Adresse eines Verfassers gegenüber dem Gericht (welches daraufhin ein Verbot der Datenlöschung ggü. Internetzugangsanbietern aussprechen kann) verpflichtet werden können.[38]
Darüber hinaus sollen Diensteanbieter bei offensichtlichen Rechtsverstößen bereits durch einstweilige Anordnung von Gerichten zur Ausgabe von Bestands- und Nutzungsdaten eines Verfassers verpflichtet werden können.[39]
Des Weiteren soll der gerichtliche Erörterungstermin auf Antrag der Parteien digital (durch Video-Verhandlung) stattfinden können und für das Auskunftsverfahren sollen keine Gerichtskosten erhoben werden.[40] Zudem soll die gerichtliche Zuständigkeit beim Landgericht liegen und das Verfahren nach den Grundsätzen der freiwilligen Gerichtsbarkeit (FamFG) geführt werden.[41] Dies führt unter anderem dazu, dass gem. § 10 FamFG kein Anwaltszwang besteht, sowie zu der Verpflichtung zur Amtsermittlung der Gerichte, § 26 FamFG.

2. Anspruch auf eine richterlich angeordnete Accountsperre

Unter bestimmten Voraussetzungen sollen Betroffene schwerwiegender Persönlichkeitsverletzungen zudem einen

35 Ebd.
36 BMJ, Eckpunktepapier, S. 3.
37 Ebd.
38 BMJ, Eckpunktepapier, S. 4.
39 Ebd.
40 Ebd.
41 Ebd.

Anspruch auf richterliche angeordnete Accountsperren haben. Dabei soll das Gericht gegenüber dem Diensteanbieter (nicht gegenüber dem Accountinhaber) die Sperrung des Accounts anordnen können, über den die Persönlichkeitsverletzungen verbreitet wurden.[42]
Damit die grundrechtlichen Positionen der Beteiligten hinreichend geschützt werden, soll die Accountsperre an folgende Bedingungen geknüpft sein: zum einen muss die Sperre verhältnismäßig sein, sodass lediglich eine Verletzung von Community-Standards nicht ausreicht. Zum anderen ist Voraussetzung, dass die Inhaltemoderation als milderes Mittel nicht ausreicht und die Gefahr besteht, dass sich schwerwiegende Beeinträchtigungen des allgemeinen Persönlichkeitsrechts durch von einem spezifischen Account veröffentlichte Inhalte wiederholen. Darüber hinaus soll die Sperre nur für einen angemessenen Zeitraum angeordnet werden können, der Accountinhaber zuvor über ein anhängiges Sperrersuchen informiert werden sowie die Möglichkeit zur Stellungnahme bekommen haben.

3. Erleichterung der Zustellung

Aufgrund der Aufhebung des NetzDG durch Inkrafttreten des Digital Service Act (DSA), soll für die bisher in § 5 NetzDG statuierte Pflicht zur Benennung eines Zustellungsbevollmächtigten im Inland eine neue Rechtsgrundlage im Gesetz gegen digitale Gewalt geschaffen werden.[43] Zusätzlich soll diese insofern ausgeweitet werden, als dass die neue Regelung auch die Zustellung außergerichtlicher Schreiben, wie beispielsweise die Aufforderung zur Löschung rechtswidriger Inhalte, erfassen soll.

VI. Bewertung

1. Begriff digitale Gewalt

Fraglich ist bereits der Titel des Eckpunktepapiers und damit des geplanten Gesetzes. Während nicht nur im Titel, sondern auch im Eckpunktepapier selbst mehrfach von „digitaler Gewalt“ die Rede ist, so bleibt die Suche nach einer Definition oder zumindest einer genauen Konkretisierung derselben vergebens. Tatsächlich werden im Eckpunktepapier „Persönlichkeitsrechtsverletzungen im digitalen Raum“ unpräzise als digitale Gewalt genannt.[44] Im dazugehörigen Kurzpapier werden hierfür beispielhaft Beleidigungen, Bedrohungen und Verleumdungen aufgezählt.[45] Diffus erscheint dahingehend, dass eine Ausweitung auf alle Fälle rechtswidriger Verletzungen absoluter Rechte unter diesem Titel geplant ist, wobei beispielhaft auf wahrheitswidrige Restaurantkritiken verwiesen wird.[46] Wenngleich der (wirtschaftliche) Schaden, welcher beispielsweise durch solche rechtswidrigen Restaurantkritiken oder Ähnliches entstehen kann, nicht trivialisiert werden sollte, so ist dennoch eine Subsumtion dessen unter den Begriff der „digitalen Gewalt“ mindestens fragwürdig. Bedenkt man beispielsweise die Ausweitung sexualisierter Gewalt in den digitalen Raum in Form widerrechtlich (aufgenommener und) veröffentlichter sexualisierter Foto- oder Videoaufnahmen, bis hin zu Missbrauchsdarstellungen, wird die Diskrepanz zwischen den Rechtsverletzungen schnell deutlich. Durch die besondere Sensibilität der davon betroffenen Lebensbereiche sind

[42] Ebd.
[43] BMJ, Eckpunktepapier, S. 6.
[44] BMJ, Eckpunktepapier, S. 1.
[45] BMJ, Kurzpapier, S. 1.
[46] BMJ, Eckpunktepapier, S. 3.

weitreichende und belastende Auswirkungen auf Betroffene die Folge.[47] Auch die Tragweite sog. Hasskriminalität und Hate-Speech, die vor allem marginalisierte Gruppen betrifft[48] und gesamtgesellschaftliche Auswirkungen haben kann, wird einer scheinbaren Gleichstellung mit wahrheitswidrigen Restaurantkritiken nicht gerecht.

Die dennoch im Eckpunktepapier vorgenommene gemeinsame Einordung unter dem gleichen Oberbegriff erweckt den Anschein von Verharmlosung digitaler Gewalttaten.[49] Die Begründung im Erläuterungspapier, dass das Gesetz jenseits des Kernanwendungsbereichs von Rechtverletzungen, die unter „digitale Gewalt" fallen, auch andere Rechtsverletzungen aufgrund vergleichbarer Interessenlagen miteinschließen soll[50], vermag für eine Einordnung unter dem Begriff der digitalen Gewalt nicht zu überzeugen. Obwohl eine konsequente Verbesserung der Durchsetzung auch anderer Rechte von Betroffenen digitaler Rechtsverletzungen begrüßenswert ist, so erfordert doch insbesondere die Thematik um digitale Gewalt und der Umstand, dass diese oft in Form schriftlicher Äußerungen auftritt, ganz besondere sprachliche Sensibilität. Diese kann allerdings eine undifferenzierte Subsumierung von Rechtsverletzungen wie solche am eingerichteten und ausgeübten Gewerbebetrieb unter den (unbestimmten) Oberbegriff „digitale Gewalt" nicht erfüllen.

Eine fehlende sprachliche Sensibilität wird darüber hinaus auch im Kurzpapier zum Eckpunktepapier deutlich, in dem beschrieben wird, dass der geplante Rechtsschutz genauso effektiv sein müsse, „wie wenn die Rechtsverletzung in der realen Welt geschehen wäre".[51] Wenngleich mit der Verwendung des Begriffs „real" in diesem Zusammenhang wohl der analoge Raum im Gegensatz zum digitalen Raum gemeint ist, erweist sich die gewählte Formulierung jedoch als äußerst inadäquat. Rechtsverletzungen im digitalen Raum bis hin zu digitaler Gewalt sind genauso „real" wie solche im analogen Raum – insbesondere, weil diese sich nicht auf den digitalen Raum beschränken, sondern immer auch Auswirkungen auf „analoge" Lebensbereiche haben.

Insofern ist es notwendig, dass im Gesetz gegen digitale Gewalt gravierende Rechtsverletzungen auch sprachlich differenziert gewürdigt werden und dabei keine inflationäre Verwendung des Begriffs der „digitalen Gewalt" vorgenommen wird.[52] Da keine einheitliche Definition dieser existiert, wäre bestenfalls eine konkrete Definition digitaler Gewalt im geplanten Gesetz begrüßenswert. Beispielsweise könnte digitale Gewalt als „Ehrverletzungen im digitalen Raum, die erheblich genug sind, um psychische Gewalt darzustellen, etwa auf Grund gruppenbezogener Menschenfeindlichkeit oder Cybermobbings"[53] konkretisiert werden. Rechtsverletzungen, die dabei nicht dieser Definition entsprechen, gleichwohl aber auch Durchsetzungsansprüche im Sinne des geplanten Gesetzes begründen sollen, könnten dabei unter dem weiteren Begriff der „Persönlichkeitsrechtsverletzungen (im digitalen Raum)" aufgegriffen werden. Eine genaue Definition digitaler Gewalt und eine auch sprachlich eindeutige Differenzierung der Rechtsverletzungen ist letztlich im Interesse aller Beteiligten. Dadurch würde Rechtssicherheit und -klarheit nicht nur für Diensteanbieter und Betroffene, sondern auch für Ermittlungsbehörden und alle (potenziell) an einem Verfahren Beteiligte geschaffen. Zudem würden Betroffene und die teilweise gravierenden Auswirkungen von digitaler Gewalt angemessen gewürdigt und einer möglichen Relativierung dessen entgegengewirkt werden.

47 Überblick bei: *Vobbe/Kärgel,* Sexualisierte Gewalt und digitale Medien: Reflexive Handlungsempfehlungen für die Fachpraxis, 2022, S. 143 f.
48 *Bredler/Markard*, JZ 2021, 864 (865).
49 *Panahi,* MMR 2023, 556 (557); *Valerius,* ZRP 2023, 142 (142 f.).
50 BMJ, Kurzpapier, S. 1.
51 Ebd.
52 *Valerius,* ZRP 2023, 142 (143).
53 *Panahi,* MMR 2023, 556 (557).

2. Stärkung privater Auskunftsverfahren

Fraglich ist, inwieweit eine effektive Stärkung privater Auskunftsverfahren, unter gleichzeitiger Würdigung grundrechtlicher und europarechtlicher Vorgaben, durch die im Eckpunktepapier aufgeführten Maßnahmen erreicht werden kann.

a) Erweiterung des Anwendungsbereichs des Auskunftsverfahrens

aa) Herausgabe von Nutzungsdaten

De lege lata richten sich Auskunftsverfahren nach § 21 Abs. 2 TTDSG. Danach können Betroffene bestimmter Rechtsverletzungen im Internet Auskunft über die Bestandsdaten von Anbietern von Telemedien verlangen.[54] Bestandsdaten sind personenbezogene Daten (wie Name oder E-Mail-Adresse), welche zur Vertragsbegründung, -gestaltung oder -änderung zwischen dem Telemedienanbieter und dem Nutzer notwendig sind, § 2 Abs. 2 Nr. 2 TTDSG.
Im Gesetz gegen digitale Gewalt soll die Herausgabe zukünftig unter bestimmten Voraussetzungen auf Nutzungsdaten erweitert werden.[55] Gem. § 2 Abs. 2 Nr. 3 TTDSG sind Nutzungsdaten personenbezogene Daten, welche für die Nutzung und Abrechnung von Telemedien erforderlich sind. Dazu gehören insbesondere Merkmale zur Identifikation des Nutzers, Zeiten der Nutzung sowie in Anspruch genommene Telemedien. Bisher sind Auskunftsersuche bezüglich solcher Nutzungsdaten gem. § 24 Abs. 3 TTDSG nur von wenigen Behörden als zulässige Stellen bei bestimmten Abrufzwecken zulässig.[56]
Die zukünftige Erweiterung auf Nutzungsdaten (wie z.B. die IP-Adresse) ist geplant, weil Anbietern häufig keine oder falsche Bestandsdaten vorliegen.[57] Dadurch kann das bisherige Verfahren nicht den Ansprüchen an eine effektive Möglichkeit zur privaten Rechtsdurchsetzung genügen und hat in der Praxis eine sehr geringe Relevanz.[58] Der aktuell hohe Aufwand für die betroffene Person gegenüber der dadurch erwirkbaren Auskunft über Daten, die in vielen Fällen nicht zu einer Identifizierung des Rechtsverletzers führen, ist unverhältnismäßig groß.[59]
Somit ist eine Änderung des Auskunftsverfahrens für eine effektive Durchsetzbarkeit von Ansprüchen bei rechtswidrigen digitalen Inhalten obligatorisch und wichtige Grundlage des gesamten Gesetzes gegen digitale Gewalt.

bb) Erstreckung auf Anbieter von Messenger- & Internetzugangsdiensten

Bisherige Auskunftsverfahren haben sich allerdings auf die Anbieter von Telemedien beschränkt, § 21 Abs. 2 TTDSG. Telemedienanbieter ist gem. § 2 Abs. 2 Nr. 1 TTDSG jede natürliche oder juristische Person, die eigene oder fremde Telemedien erbringt, an der Erbringung mitwirkt oder Zugang zur Nutzung eigener oder fremder Telemedien vermittelt (z.B. soziale Medien).

54 *Geppert/Schütz/Schreiber,* in: Beck-TGK, TTDSG, 5. Aufl. (2023), § 21 Rn. 36.
55 BMJ, Eckpunktepapier, S. 2.
56 *Geppert/Schütz/Schreiber,* in: Beck-TGK, § 24 Rn. 1.
57 BMJ, Eckpunktepapier, S. 3.
58 BMJ, Eckpunktepapier, S. 2.
59 DJB, Stellungnahme zu den Eckpunkten des Bundesjustizministeriums zum Gesetz gegen digitale Gewalt v. 26.5.2023, S. 5, abrufbar unter: https://www.bmj.de/SharedDocs/Downloads/DE/Gesetzgebung/Stellungnahmen/2023/0526_Stellungnahme_djb_Eckpunkte_Gesetz_digitale_Gewalt.pdf?__blob=publicationFile&v=2 (zuletzt abgerufen am 27.10.2023).

(1) Messengerdienste

Bisher waren Messengerdienste nicht vom Anwendungsbereich des Auskunftsanspruchs erfasst. Dazu gehören auch Dienste wie WhatsApp oder Messengerfunktionen von Telemediendiensten wie Facebook.[60]
Durch die nun geplante Ausweitung sollen auch solche Dienste unter bestimmten Voraussetzungen zur Herausgabe von Daten durch ein Gericht verpflichtet werden können.[61]
Bereits im Rahmen des Anwendungsbereichs im Sinne des § 1 Abs. 1 S. 3 NetzDG wurde diskutiert, ob oder inwiefern auch Messengerdienste davon erfasst sein könnten. Während der Wortlaut „Plattformen, die zur Individualkommunikation oder zur Verbreitung spezifischer Inhalte bestimmt sind" dies ausschließt[62], wird teilweise kritisiert, dass viele Telemedien von Individual- in Massenkommunikation umschlagen können und große WhatsApp-Gruppen kaum als „nicht-öffentlich" bezeichnet werden könnten, während kleinste X-Gruppen (ehemals Twitter) den sozialen Netzwerken zuzuordnen seien.[63] Dieses Problem kann mit der für das digitale Gewaltschutzgesetz geplanten Erweiterung auf Messengerdienste zukünftig gelöst werden. Indem Messengerdienste über Telemedienanbieter hinaus zum Anwendungsbereich möglicher Herausgabepflichten zählen, würden zudem auch Dienste wie Telegram erfasst, welche aufgrund der Möglichkeiten sowohl zur privaten Kommunikation als auch zu einseitiger Kommunikation mit/in großen Gruppen, meist nicht klar einer bestimmten Kategorie zuzuordnen sind.[64] Dementsprechend wäre begrüßenswert, wenn darüber hinaus im Gesetz ein technisch neutraler Begriff wie „Dienst mit Messenger-Funktion" verwendet werden würde, um sprachlichen Abgrenzungsproblemen von Anfang an vorzubeugen.[65]
Die besondere Gebotenheit der Integration von Messengerdiensten im Auskunftsverfahren wird darüber hinaus vor allem beim aktuellen medien- und öffentlichkeitspräsenten Thema extremistischer Chatgruppen (im öffentlichen Dienst) deutlich. Diesbezüglich wurde am 20.10.2023 ein Gesetzesentwurf des Bundesrates zur Änderung des StGB vorgestellt.[66] Dies unterstreicht, dass (gravierende) Rechtsverletzungen vermehrt nicht nur in sozialen Medien, sondern auch in Messengerdiensten stattfinden.
Zudem kann die Ausweitung auf Messengerdienste im Auskunftsanspruch dazu beitragen, dass rechtsverletzende Personen nicht einfach von bspw. sozialen Netzwerken auf Messengerdienste ausweichen, sodass Rechtsverletzungen nicht verhindert, sondern lediglich in einen anderen digitalen Raum verlagert würden.

(2) Internetzugangsdienste

Die nun geplante Ausweitung der Auskunftspflicht auch auf Internetzugangsdienste (Telekommunikations-/TK Unternehmen) ist für die Identifizierung rechtsverletzender Personen notwendig und somit grundsätzlich ebenfalls wünschenswert, da die Nutzungsdaten sowie IP-Adresse allein dafür häufig nicht ausreichend sind.
Doch wenngleich die IP-Adresse unter Zuhilfenahme der Auskunft von Internetzugangsanbietern zwar grundsätzlich die Identifizierung der rechtsverletzenden Person erwirken kann, ist fraglich, ob und wie lange Telekommunikationsunternehmen die Zuordnung der IP-Adresse überhaupt speichern und die Identifizierung praktisch also umsetzbar ist.

60 *OLG Frankfurt a.M.*, ZUM-RD 2019, 145.
61 BMJ, Eckpunktepapier, S. 3.
62 BT-Drs. 18/12012, S. 20; *OLG Frankfurt a.M.*, ZUM-RD 2019, 145.
63 *Spindler,* GRUR 2018, 365 (367).
64 *Gerhold/Handel*, in: NK-MedienStrafR, § 1 Rn. 41.
65 *Panahi,* MMR 2023, 556 (558).
66 BT-Drs. 449/23.

Denn TK-Anbieter speichern derzeit Daten bzgl. IP-Adressen nur zu eigenen Geschäftszwecken sowie zeitlich begrenzt. Nach Auskunft fünf großer TK-Anbieter in Deutschland speichern diese Daten nur bis maximal 7 Tage.[67] Es ist somit durchaus fraglich, ob die Beweissicherungsanordnung ggü. den Internetzugangsanbietern überhaupt so schnell ergehen kann.[68] Dadurch entsteht die Gefahr, dass ein sog. „Quick-Freeze" der Daten nicht durchgeführt werden kann, weil relevante Daten zum Zeitpunkt des Auskunftsersuchens bzw. der Beweissicherungsanordnung nicht mehr oder unvollständig gespeichert sind und Auskunftsersuchen deshalb ins Leere laufen.[69]

Aufgrund dessen wird teilweise die Einführung einer zusätzlichen Speicherfrist für relevante (Nutzungs-)Daten bei Internetzugangsanbietern im digitalen Gewaltschutzgesetz gefordert.[70] Allerdings wird im Erläuterungspapier klargestellt, dass keine anlasslose Speicherung von Nutzungsdaten vorgesehen ist und von Anbietern nur Daten herausgegeben werden müssen, die diese selbst erhoben haben.[71]

Zudem stellte der *EuGH* bereits 2022 fest, dass eine anlasslose und nicht begrenzte Vorratsdatenspeicherung von Verkehrsdaten unionrechtswidrig sei,[72] und ausschließlich bei erheblicher Gefahrenlage zulässig ist.[73] Die Einführung einer allgemeinen Speicherfrist für TK-Unternehmen wäre somit nicht angemessen.

Darüber hinaus wird teilweise bereits mit der geplanten Einführung des digitalen Gewaltschutzgesetzes eine „Vorratsdatenspeicherung durch die Hintertür" befürchtet.[74] Dies erscheint jedoch nicht nachvollziehbar, da die anlasslose Speicherung wie bereits festgestellt ausdrücklich ausgeschlossen wird.[75] Allenfalls besteht eine Gefahr von massenhafter Datenspeicherung, wenn Diensteanbieter, die ohnehin ein wirtschaftliches Interesse an der Verarbeitung von Nutzerdaten haben, das Gesetz gegen digitale Gewalt als Rechtfertigung hierfür heranziehen könnten.[76] Dem könnte jedoch beispielsweise durch eine zeitliche Beschränkung der Datensicherung entgegengewirkt werden.[77]

Nichtsdestotrotz besteht bei einer ausbleibenden zusätzlichen Speicherfrist das Problem, dass viele Auskunftsersuche deswegen erfolglos bleiben könnten. Um somit die Wahrscheinlichkeit des Auskunftserfolgs zu erhöhen, könnte zudem die regelmäßig diskutierte Möglichkeit einer Klarnamen- oder Identifikationspflicht bei der Telemediennutzung in Betracht kommen. Danach wäre die Nutzung von Telemedien ausschließlich unter Verwendung des Klarnamens (auch gegenüber anderen Nutzern) möglich. Die Einführung einer solchen Pflicht ist insbesondere bei Straftaten und Rechtsverletzungen im digitalen Raum ein wiederkehrendes Thema kontroverser öffentlicher Debatten.[78] Allerdings ist in Deutschland bereits in § 19 Abs. 2 S. 1 TTDSG festgelegt, dass von Telemedienanbietern die anonyme Nutzung oder die Nutzung unter Pseudonym zu ermöglichen sei, soweit dies technisch möglich und zumutbar ist. Diese Zumutbarkeit kann nur ggf. nach einer konkreten Verhältnismäßigkeitsprüfung des

67 BKA, Positionspapier zu erforderlichen Speicherfristen von IP-Adressen, v.21.6.2023, online abrufbar unter: https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/230623_Mindestspeicherfristen_IP-Adressen.html (zuletzt abgerufen am 27.10.2023).

68 DRB, Stellungnahme zu den Eckpunkten des Bundesjustizministeriums zum Gesetz gegen digitale Gewalt, Mai 2023, S. 6, online abrufbar unter: https://www.bmj.de/SharedDocs/Downloads/DE/Gesetzgebung/Stellungnahmen/2023/0523_Stellungnahme_DRB_Eckpunkte_Gesetz_digitale_Gewalt.pdf?__blob=publicationFile&v=2 (zuletzt abgerufen am 27.10.2023).

69 DJB, Stellungnahme, S. 8.

70 HateFree, Stellungnahme zu den Eckpunkten des Bundesjustizministeriums zum Gesetz gegen digitale Gewalt v. 26.5.2023, online abrufbar unter: https://www.bmj.de/SharedDocs/Downloads/ DE/Gesetzgebung/Stellungnahmen/2023/0526_Stellungnahme_hatefree_Eckpunkte_Gesetz_digitale_Gewalt.pdf?__blob=publicationFile&v=2 (zuletzt abgerufen am 27.10.2023).

71 BMJ, Erläuterungspapier, S. 3.

72 HateFree, Stellungnahme, S. 2.

73 *EuGH*, NJW 2021, 531 (531).

74 Chaos Computer Club, Stellungnahme zu den Eckpunkten des Bundesjustizministeriums zum Gesetz gegen digitale Gewalt, S. 4, online abrufbar unter: https://www.bmj.de/SharedDocs/Downloads/DE/Gesetzgebung/Stellungnahmen/2023/0526_Stellungnahme_CCC_Eckpunkte_Gesetz_digitale_Gewalt.pdf?__blob=publicationFile&v=2 (zuletzt abgerufen am 27.10.2023).

75 BMJ, Erläuterungspapier, S. 3.

76 *Panahi,* MMR 2023, 556 (558).

77 *Panahi,* MMR 2023, 556 (558).

78 *Oswald*, Nach Facebook-Urteil: Was würde eine Klarnamenpflicht bringen?, BR24 v. 27.1.2022, online abrufbar unter: https://www.br.de/nachrichten/netzwelt/facebook-was-wuerde-eine-klarnamenpflicht-bringen,SviKT1a (zuletzt abgerufen am 27.10.2023).

Einzelfalls nicht vorliegen.[79]

Denn gemäß *BGH*-Rechtsprechung ist die anonyme Nutzung des Internets diesem immanent und dient darüber hinaus dem Schutz der Meinungsäußerungsfreiheit.[80] Wenn die Nutzung von Telemedien nur unter Klarnamen möglich wäre, ist darüber hinaus zu befürchten, dass viele Nutzer beispielsweise bereits von der Veröffentlichung (berechtigter) Kritik aus Angst vor (auch nicht staatlicher Konsequenzen) absehen würden. Dies wäre eine erhebliche Einschränkung der Meinungsfreiheit (Art. 5 Abs. 1 GG, Art. 11 GRCh) mit einem darüberhinausgehenden erheblichen Rückverfolgungs-, Überwachungs- und Missbrauchspotenzial. Dadurch würde die Strafverfolgung und Rechtsdurchsetzung zwar selbstverständlich substanziell vereinfacht, dies würde aber außer Verhältnis zu den freiheits- und grundrechtlichen Einschränkungen stehen.

Somit stellt eine gesetzliche Klarnamenpflicht, die eine anonyme Internetnutzung vollkommen ausschließen und mithin auch das sog. Recht auf Vergessenwerden (Art. 17 DSGVO) sowie das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 GG) enorm verletzen würde, keine mögliche Lösung dar. Die alternative Möglichkeit einer Identifikationspflicht (bei der Nutzer bei der Registrierung ihren richtigen Namen, Anschrift und Geburtsdatum bei der Nutzung digitaler Dienste angeben müssen) ist dabei zwar weniger eingriffsintensiv als die Klarnamenpflicht, allerdings aus den gleichen Beweggründen abzulehnen. Die Pflicht zur Offenbarung sensibler persönlicher Daten ggü. Betreibern elektronischer Kommunikationsdienste schafft erhebliche Gefahren des Missbrauchs und des rechtswidrigen Zugangs.[81]

Somit ist festzuhalten, dass die Herausgabe der IP-Adresse zusammen mit der Auskunft von Internetzugangsanbietern, wem die IP-Adresse zum entsprechenden Zeitpunkt zugeteilt war, die eingriffsärmste und damit begrüßenswerteste Option darstellt, wenngleich die praktische und effiziente Umsetzbarkeit teilweise in Frage steht. Bei der Gefahr einer nicht möglichen Identifizierung ist jedoch zu beachten, dass das Gesetz gegen digitale Gewalt auch insbesondere für Fälle, bei denen die Identifizierung nicht erfolgreich war, die Option einer richterlich angeordneten Accountsperre gegen notorische Rechtsverletzer vorsieht und Betroffene somit auch bei erfolglosem Auskunftsersuchen nicht schutzlos sind.[82]

Darüber hinaus lässt sich auch im DSA keine Regelung zu einer Identifikations- oder Klarnamenpflicht finden, sodass die Einführung einer solchen Pflicht ohnehin in grundlegendem Widerspruch zu den harmonisierten Regelungen auf europäischer Ebene stehen würde.

(3) Grundrechtskonformität

Fraglich ist allerdings, ob das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GRCh bzw. Art. 8 GRCh) sowie die Meinungsfreiheit (Art. 5 Abs. 1 GG bzw. Art. 11 GRCh) auch bei der vorgesehenen Stärkung des Auskunftsverfahrens angemessen gewürdigt werden (können).

Durch die Herausgabe von Nutzungsdaten in Verbindung mit der Auskunft des Inhabernamens des Telekommunikationsanspruches (s. II. c)) wird in das Recht auf informationelle Selbstbestimmung des mutmaßlichen Rechtsverletzers gem. Art. 2 Abs. 1 GG, Art. 8 GRCh in erheblicher Weise eingegriffen. Die grundsätzliche Befugnis, selbst über Preisgabe und Verwendung persönlicher Daten zu bestimmen[83] wird hierdurch verletzt. Insbesondere bei der Ausweitung auf Messengerdienste ist kritisch zu betrachten, inwiefern der Grundrechtseingriff besonders

79 *OLG München*, MMR 2021, 245 (247); *OVG Hamburg*, NJW 2016, 3386 (3388).
80 *BGH*, NJW 2009, 2888 (2892); *BGH*, NJW 2022, 1314 (1320 f.).
81 *EuGH*, NJW 2021, 531 (536).
82 BMJ, Eckpunktepapier, S. 4 f.
83 *Fabio*, in: Dürig/Herzog/Scholz, GG, Bd. 1, 101. EL (2023), Art. 2 Abs. 1 Rn. 176.

bei privaten Chatverläufen oder kleinen Gruppen, der Eingriff in das Grundrecht auf Fernmeldegeheimnis bzw. auf private Kommunikation (Art. 10 Abs. 1 GG, Art. 7 GRCh)[84] angemessen ist. Denn die Kommunikation in beispielsweise privaten WhatsApp-Chats ist grundsätzlich Bestandteil einer vertraulichen Kommunikation zwischen den Teilnehmern und genießen als solche verfassungsrechtlichen Schutz.[85] Dahingehend stellte das *BVerfG* bereits 2020 fest, dass der Gesetzgeber bei der Einrichtung eines Auskunftsverfahrens auf Grundlage jeweils eigener Kompetenzen sowohl für die Übermittlung als auch für den Abruf der Daten verhältnismäßige Grundlagen schaffen muss.[86] Aufgrund dessen wird die hinreichende Rechtfertigung maßgeblich von der konkreten Ausgestaltung der Voraussetzungen im digitalen Gewaltschutzgesetz, die für das Auskunftsverfahren erfüllt sein müssen, abhängen.

Darüber hinaus bestehen insofern Bedenken gegenüber dem Grundrecht der Meinungsfreiheit, Art. 5 Abs. 1 GG, Art. 11 GRCh, als dass das geplante Gesetz bereits durch die neue bzw. ausgeweitete Möglichkeit und somit potenzielle Gefahr der Identifizierung eine abschreckende Wirkung auf Nutzer haben kann. Dies könnte dazu führen, dass sich Nutzer aus Angst auch aus dem rechtskonformen und grundrechtlich geschützten digitalen offenen Meinungsaustausch und Diskurs zurückziehen könnten.[87] Das Phänomen der Nicht-Ausübung von Grund- und Freiheitsrechten aus Furcht vor staatlicher Sanktion oder bspw. der Aufhebung der Anonymität wird auch als „Chilling-Effect“ (Abschreckungseffekt) bezeichnet.[88]

Im Rahmen der Meinungsfreiheitsdogmatik ist jedoch zu beachten, dass sich dabei nicht nur die beiden Individualfreiheiten, Meinungsfreiheit auf der Seite der von einem potenziellen Auskunftsverfahren betroffenen oder abgeschreckten Person, sowie beispielsweise der Ehrschutz bei Betroffenen digitaler Beleidigungen o.Ä. auf der anderen Seite, gegenüberstehen. Vielmehr ist auch zu beachten, dass durch beispielsweise Hate Speech auch ein sog. „Silencing-Effect“ (Verstummungseffekt) eintreten kann, bei dem sich Menschen wegen rechtsverletzender/strafbarer Inhalte anderer Nutzer weniger stark an politischen Diskursen beteiligen oder sich sogar ganz zurückziehen.[89] Das bestärkt die gesetzliche Handlungsgebotenheit bei rechtsverletzendem digitalem Verhalten, während die (Ausübung der) Meinungsfreiheit (auch in Anbetracht potenzieller „Chilling-Effects“) aller Beteiligten bestmöglich zu schützen ist.

Darüber hinaus ist bei dem Vorhaben der Stärkung der Rechte Betroffener bei Rechtsverletzungen wichtig, dass es einem Rechtsstaat inhärent ist, dass sich Betroffene von Rechtsverletzungen effektiv vor Gericht gegen diese wehren können - dieser Grundsatz besteht zweifelsfrei auch bei Rechtsverletzungen, die sich im digitalen Raum ereignen.[90]

cc) Erstreckung auf alle Fälle der Verletzung absoluter Rechte

Wie bereits aufgeführt, vermag die sprachliche Einordnung von Verletzungen aller absoluten Rechte unter der Terminologie „digitale Gewalt“ nicht zu überzeugen. Fraglich ist allerdings zudem, inwiefern das grundsätzliche Vorhaben der Ausweitung des Anwendungsbereichs überzeugt.

84 *Panahi,* MMR 2023 556 (558).
85 *LAG Niedersachsen*, NZA-RR 2023, 246 (248).
86 *BVerfG*, NJW 2020, 2699.
87 Amnesty International, Stellungnahme zu den Eckpunkten des Bundesjustizministeriums zum Gesetz gegen digitale Gewalt v. 26.6.2023, S. 1, online abrufbar unter: https://www.hilfe-info.de/SharedDocs/Gesetzgebungsverfahren/Stellungnahmen/2023/Downloads/0526_Stellungnahme_Amnesty_International_Eckpukte_Gesetz_digitale_Gewalt.pdf?__blob=publicationFile&v=2 (zuletzt aufgerufen am 20.2.2024).
88 *EuGH*, NJW 2021, 531 (548); *Bredler/Markard,* JZ 2021, 864 (870); *Schöbener/Knauff,* Allgemeine Staatslehre, 5. Aufl. (2023), § 8 Rn. 18; *Hallweger/Thümmler,* NStZ 2023 76 (80).
89 *Hallweger/Thümmler,* NStZ 2023 76 (80); *Apostel,* KriPoZ 2019, 287 (291).
90 BMJV, Erläuterungspapier, S. 1.

Aktuell besteht der Auskunftsanspruch gem. § 21 Abs. 2 S. 1 TTDSG zur Durchsetzung zivilrechtlicher Ansprüche wegen der Verletzung absolut geschützter Rechte aufgrund rechtswidriger Inhalte, die von § 10a Abs. 1 TMG oder § 1 Abs. 3 NetzDG erfasst werden. Darin genannte Tatbestände erstrecken sich über verschiedene Deliktsbereiche des Strafrechts, beispielsweise zu nennen sind Volksverhetzung (§ 130 StGB), Beleidigung (§ 185 StGB), Verleumdung (§ 187 StGB) oder Bedrohung (§ 241 StGB). Die Auflistung in § 1 Abs. 3 NetzDG ist dabei abschließend und eine Erweiterung auf andere Delikte im Wege einer Analogie unzulässig.[91] Diese Begrenzung auf die im NetzDG genannten Straftatbestände sollte (bei deren Einführung) verdeutlichen, dass explizit die Rechtsdurchsetzung bei der Bekämpfung von Hasskriminalität und strafbaren Falschnachrichten in sozialen Netzwerken geregelt werden solle und es nicht um „beliebige [geringfügige] Verletzungen des geltenden Rechts“ geht.[92]

Laut Eckpunktepapier soll sich dies allerdings zukünftig ändern und das Auskunftsverfahren bei allen absoluten Rechten, beispielsweise auch Verletzungen des allgemeinen Persönlichkeitsrechts oder des sog. Rechts am eingerichteten und ausgeübten Gewerbebetrieb (z.B. wahrheitswidrige Restaurantkritik), eröffnet sein.[93] Begründet wird dies damit, dass verletzende Äußerungen Menschen in ihrer privaten und beruflichen Existenz treffen können.[94]

Hervorzuheben ist diesbezüglich jedoch, dass auch bisherige Auskunftsverfahren bei Rechtsverletzungen wie dem eingerichteten und ausgeübtem Gewerbebetrieb zur Anwendung kommen können, wenn die Rechtsverletzung aufgrund einer der in § 1 Abs. 3 NetzDG aufgeführten Tatbestände, wie beispielsweise einer Beleidigung (§ 185 StGB) oder Verleumdung (§ 187 StGB), erfolgte. So ist beispielsweise auch eine (wegen eines in § 1 Abs. 3 NetzDG aufgeführten Tatbestands) rechtswidrige Arbeitgeberbewertung vom aktuellen Auskunftsanspruch erfasst.[95] Demnach wären auch bei Fortführung des aktuellen begrenzteren Anwendungsbereichs des Auskunftsrechts bereits viele rechtswidrige Restaurantkritiken erfasst.[96] Dies lässt das im Eckpunktepapier aufgeführte Beispiel (der wahrheitswidrigen Restaurantkritik)[97] irritierend wirken und könnte darüber hinaus den Anschein erwecken, dass eine Ausweitung des Anwendungsbereichs möglicherweise gar nicht notwendig ist.

Allerdings erscheint die Ausweitung dennoch sinnvoll. Denn die Ungleichbehandlung von grundrechtlich gleichermaßen geschützten Rechten, wie bei Inhabern immaterieller Schutzrechte, insbesondere Urheberrechte (§ 101 UrhG), im Vergleich zu Persönlichkeitsrechtsverletzungen von vergleichbarem Ausmaß, ist nicht gerechtfertigt.[98]

Darüber hinaus gab es bereits 2017 einen Vorschlag der Bundesregierung, den Katalog des § 1 Abs. 3 NetzDG um weitere Delikte zu erweitern.[99] Dabei wären zum Schutz der digitalen Kommunikationsstruktur und -kultur insbesondere die Aufnahme von Delikten wie § 80a StGB (Aufstacheln zum Verbrechen der Aggression) oder zum Schutz gegen „Fake-News“ die Aufnahme von § 145d StGB (Vortäuschen von Straftaten) und § 269 StGB (Fälschung beweiserheblicher Daten) sinnvoll gewesen.[100]

Denkbar wäre somit auch lediglich eine Ergänzung der in § 1 Abs. 3 NetzDG aufgelisteten Delikte. Allerdings würden dadurch Rechtsverletzungen aus dem Anwendungsbereich des Auskunftsrechts hinausfallen, welche zwar

91 *Liesching*, ZUM 2017, 809 (811).
92 BT-Drs. 18/12356, S. 19 f.
93 BMJ, Eckpunktepapier, S. 3.
94 BMJ, Erläuterungspapier, S. 1.
95 *OLG Celle*, MMR 2022, 690.
96 DJB, Stellungnahme, S. 6.
97 BMJ, Eckpunktepapier, S. 3.
98 DAV, Stellungnahme zu den Eckpunkten des Bundesjustizministeriums zum Gesetz gegen digitale Gewalt, Mai 2023, S. 6, online abrufbar unter: https://www.bmj.de/SharedDocs/Downloads/DE/Gesetzgebung/Stellungnahmen/2023/0526_Stellungnahme_DAV_Eckpunkte_Gesetz_digitale_Gewalt.pdf?__blob=publicationFile&v=2 (zuletzt abgerufen am 27.10.2023).
99 BT-Drs. 18/12727, S. 18 ff.
100 *Hoven/Gersdorf*, in: BeckOK-InfoMedienR, § 1 Rn. 38.

persönlichkeitsrechtsverletzend sind, jedoch nicht die Schwelle zur Strafbarkeit übertreffen.[101] Diese Strafbarkeitslücke kann die Erweiterung auf alle absoluten Rechte schließen.
Darüber hinaus erscheint eine abschließende Aufzählung betreffender Delikte ohnehin gerade in Anbetracht des schnell fortschreitenden Wandels digitaler Kommunikation nicht angemessen. Es kann nicht gewährleistet werden, dass mit der in § 1 Abs. 3 NetzDG vorgenommenen Auflistung alle (auch für die Zukunft) relevanten Delikte aufgefasst sein werden. Zudem muss beachtet werden, dass auch bei der Ausweitung auf alle absoluten Rechte, der Auskunftsanspruch ausschließlich unter den im Eckpunktepapier geplanten Voraussetzungen bestehen würde. Insbesondere erfolgt bei jedem Auskunftsersuchen eine Verhältnismäßigkeitsprüfung im konkreten Einzelfall.
Die Kritik, dass das zukünftige Auskunftsverfahren die Gefahr des Missbrauchs durch Unternehmen o.Ä. (bei beispielsweise berechtigter, aber ungewollter Kritik) vergrößere[102], ist darüber hinaus wenig überzeugend. Denn auch dabei gilt der Maßstab der hinreichenden Berücksichtigung und Abwägung der (Grund-)Rechte aller Beteiligten und die Einhaltung der Voraussetzungen des geplanten Gesetzes. Daran, was im Rahmen der Meinungsfreiheit (Art. 5 Abs. 1 GG) kommuniziert und veröffentlicht werden darf, ändert das geplante Gewaltschutzgesetz nichts.[103] Ein mögliches Missbrauchsrisiko eines Gesetzes sollte zwar entsprechend (vor allem bei dessen Anwendung) berücksichtigt werden, allerdings keinesfalls der Einführung eines sinnvollen Gesetzes im Wege stehen. Aufgrund dessen ist die Ausweitung des Anwendungsbereichs des Auskunftsanspruchs auf alle absoluten Rechte begrüßenswert.

b) Effektivere Ausgestaltung des Auskunftsverfahrens

Die Geltung des FamFG sowie die Konzentration der gerichtlichen Zuständigkeit an Landgerichte (§ 21 Abs. 3 S. 3 TTDSG) ist zu begrüßen, da dies die Effizienz des Verfahrens fördert und gewährleistet wird, dass in dem Bereich erfahrene Personen am Verfahren beteiligt sind.
Ebenso überzeugt die Möglichkeit zu Video-Verhandlungen sowie der Grundsatz, keine Gerichtskosten für das Auskunftsverfahren zu erheben. Betroffene digitaler Rechtsverletzungen sollten unabhängig von ihren finanziellen Voraussetzungen die Möglichkeit haben, sich gegen solche Rechtsverletzungen schützen zu können.
Dass Diensteanbieter dazu verpflichtet werden können, Bestands- und Nutzungsdaten der Nutzer sowie die mutmaßliche Rechtsverletzung gezielt zu sichern, ist unverzichtbar für die Durchführbarkeit des Auskunftsverfahrens. Dass die Offenlegung zudem nur ggü. dem Gericht erfolgt und die Zusammenführung von IP-Adresse und Bestandsdaten sowie die Offenlegung ggü. dem Geschädigten ausschließlich nach Abschluss des Verfahrens erfolgt[104] ist im Sinne des Schutzes der mutmaßlichen rechtsverletzenden Person von essenzieller Bedeutung und sehr positiv zu beurteilen.

3. Anspruch auf richterlich angeordnete Accountsperren

Eine weitere Maßnahme des Gesetzes gegen digitale Gewalt soll die Möglichkeit von richterlich angeordneten Accountsperren sein.[105]

---

101 HateAid, Stellungnahme zu den Eckpunkten des Bundesjustizministeriums zum Gesetz gegen digitale Gewalt, Mai 2023, S. 4 f., abrufbar unter: https://www.bmj.de/SharedDocs/Downloads/DE/Gesetzgebung/Stellungnahmen/2023/0526_Stellungnahme_HateAid_Eckpunkte_Gesetz_digitale_Gewalt.pdf?__blob=publicationFile&v=2 (zuletzt abgerufen am 27.10.2023).
102 Amnesty International, Stellungnahme, S. 2.
103 BMJ, Erläuterungspapier, S. 2.
104 BMJ, Eckpunktepapier, S. 4.
105 Ebd.

Dadurch sollen Betroffene unter bestimmten Voraussetzungen die Möglichkeit erhalten, sich gegen wiederholte Rechtsverletzungen effektiv wehren zu können, die über den gleichen Account verbreitet werden. Die Anordnung zur Accountsperre soll gegenüber dem Diensteanbieter erfolgen, was einen besonderen Mehrwert darstellt, falls die Identität des Accountinhabers nicht bekannt ist.[106] Dies ist insbesondere wichtig und somit erfreulich, da die Möglichkeit zur anonymen Nutzung digitaler Dienste (ohne Klarnamenpflicht o.Ä.) weiterhin bestehen bleiben wird.

Wenngleich ein Vorteil von Accountsperren somit darin liegt, dass sie gravierende Rechtsverletzungen im ersten Schritt unterbinden können, während sie gleichzeitig nicht die anonyme Nutzung des Internets angreifen, so ist jedoch die tatsächliche Praktikabilität solcher Accountsperren fraglich.

Problematisch ist insbesondere die Wirksamkeit solcher Sperren gegen erneute Rechtsverletzungen, wenn die Identität der rechtsverletzenden Person nicht bekannt ist und diese somit nach einer Accountsperre leicht und schnell (unter Angabe falscher Daten) einen neuen Account erstellen kann, mit dem daraufhin weitere Rechtsverletzungen begangen werden können.[107]

Dagegen wird allerdings teilweise argumentiert, dass große Accounts existieren, die gerade durch oder aufgrund des Verbreitens von rechtsverletzenden Inhalten eine hohe Reichweite (also viele Follower) generiert haben[108] und somit durch eine (temporäre) Accountsperre zumindest diese Reichweite temporär reduziert bzw. aufgehoben werden würde. Wenngleich solche Accounts durch eine Sperre in größerem Maße getroffen werden würden ist allerdings fraglich, wie viele der Accounts, über die rechtsverletzende Inhalte verbreitet werden, eine so große Reichweite haben, sodass es für sie aufgrund der daraufhin (temporär) fehlenden Reichweite nicht sinnvoll erscheint, einen neuen Account zu erstellen. Darüber hinaus haben vor allem viele Accounts mit einer gewissen Reichweite sog. Backup-Accounts, auf die sie zurückgreifen können, falls ihr Erstaccount beispielsweise gesperrt wurde. Dieser könnte ggf. auch erst erstellt werden, sobald der Accountinhaber mit einem Hinweis über ein anhängiges Sperrersuchen informiert wird. Wenn der Zweitaccount dann über einen anderen Account erstellt wurde/wird, könnte die Person trotz Accountsperre weiteren Rechtsverletzungen begehen. Dafür bietet das Eckpunktepapier keinen Lösungsansatz. Wünschenswert wäre beispielsweise eine Regelung, dass von Accountsperren auch Ersatzaccounts miteingeschlossen sind, die zur Umgehung von Accountsperren verwendet werden.[109]

Darüber hinaus ist kritisch zu betrachten, dass vor allem große Accounts, wie solche von Personen, die beruflich Inhalte auf sozialen Plattformen teilen (sog. Content Creator) sehr stark von möglichen Accountsperren getroffen werden würden. Das kann zu sog. Deplatforming, also der Wegnahme der Reichweite und damit der Finanzierungsquelle der betroffenen Person, führen, was einen erheblichen Grundrechtseingriff darstellen würde.[110]

Dagegen ist jedoch zu beachten, dass laut Eckpunktepapier jede Accountsperre an bestimmte Voraussetzungen geknüpft sein wird. Insbesondere unterliegen die Sperren einem Richtervorbehalt und müssen in jedem Einzelfall einer Verhältnismäßigkeitsprüfung standhalten.[111] Darüber hinaus darf eine Inhaltemoderation als milderes Mittel nicht ausreichen und es muss die Gefahr der Wiederholung schwerwiegender Rechtsverletzungen des allgemeinen Persönlichkeitsrechts bestehen. Zudem ist die Accountsperre nur für einen angemessenen Zeitraum anzuordnen und der Accountinhaber über ein Sperrersuchen zu informieren und muss die Möglichkeit zur Stellungnahme erhalten.[112] Durch diese Voraussetzungen ist es grundsätzlich möglich, die Rechtfertigung des Eingriffs in die

106 BMJ, Eckpunktepapier, S. 5.
107 *Holznagel*, MMR 2023, 634 (634).
108 DJB, Stellungnahme, S. 13 f.
109 *Panahi*, MMR 2023, 556 (560).
110 *Augsberg/Petras,* JuS 2022, 97 (105).
111 BMJV, Eckpunktepapier, S. 5.
112 Ebd.

Meinungsfreiheit (Art. 5 Abs. 1 GG, Art. 11 GRCh), die durch Accountsperren vorgenommen wird, zu gewährleisten. Zudem wird dadurch die Gefahr von Over-Blocking (das teilweise durch Onlineplattformen betreiben wird)[113] ebenfalls minimiert bzw. ausgeschlossen.

Nicht nachvollziehbar erscheint hingegen, warum sich die Möglichkeit richterlich angeordneter Accountsperren lediglich auf „schwerwiegende Beeinträchtigungen des allgemeinen Persönlichkeitsrechts“[114] beschränken soll. Ungeachtet dessen, dass nicht näher definiert ist, was konkret unter dem Begriff „schwerwiegend“ zu verstehen ist, ist vor allem in Anbetracht von beispielsweise Hate Speech, die sich regelmäßig nicht gegen Einzelpersonen, sondern gegen (Bevölkerungs-)Gruppen richtet, eine Erweiterung des Anwendungsbereichs für Accountsperren wünschenswert.[115] Accounts, die zum Beispiel volksverletzende Inhalte (§ 130 StGB) oder die Verwendung verfassungsfeindlicher Symbole (§ 86a StGB) verbreiten, sollten bei Erfüllung der vorgesehenen Voraussetzungen ebenfalls gesperrt werden können. Denn diese, sowie die Belohnung und Billigung von Straftaten (§ 140 StGB) und gegen Personen des politischen Lebens gerichtete Beleidigung, üble Nachrede und Verleumdung (§ 188 StGB) machen den größten Anteil der beim BKA gemeldeten Straftatbestände bei Hasspostings aus[116] und sind zweifelsfrei auch eine Form digitaler Gewalt.

Um die Gefahr von wiederholten, missbräuchlich angeforderten, ungerechtfertigten Accountsperren zu umgehen, wäre darüber hinaus die Möglichkeit zur Sperrung von Accounts, die wiederholt missbräuchlich Inhalte melden, wünschenswert.

a) Gelegenheit zur Stellungnahme

Gem. Art. 103 Abs. 1 GG besteht die Verpflichtung des Staates, jedem, der an einem gerichtlichen Verfahren förmlich beteiligt oder von einer gerichtlichen Entscheidung unmittelbar rechtlich betroffen ist, rechtliches Gehör zu verschaffen.[117] Dies soll durch die im Eckpunktepapier geplante Informierung und Möglichkeit zur Stellungnahme über die Kommunikationsplattform gewährleistet werden.[118] Dabei wird teilweise kritisiert, dass die Möglichkeit, zum anhängigen Sperrersuchen Stellung zu nehmen, dem Gericht obliege und somit abzulehnen sei, dafür Kommunikationskanäle der Plattform zu verwenden.[119] Zumal Nutzer nicht damit rechnen würden und die Seriosität der Nachricht über ein anhängiges Gerichtsverfahren in Frage stellen würden oder von Spam ausgehen würden.[120] Dagegen ist jedoch einzuwenden, dass vor allem anonyme Nutzer mit der Kommunikation über die Plattform erreicht werden sollen, die auf anderem Wege gar nicht erreicht werden könnten. Darüber hinaus ist am geplanten Vorhaben besonders vorteilhaft, dass die Nutzer durch den Hinweis über die Plattform innerhalb kürzester Zeit informiert werden können (was auch im Interesse der Nutzer selbst ist) und gerade auch die Unmittelbarkeit des Hinweises (direkt verknüpft mit der entsprechenden Plattform des betroffenen Accounts) besonders nutzerfreundlich ist. Problematisch könnte allenfalls sein, wenn Diensteanbieter bzgl. des Hinweises und der Möglichkeit zur Stellungnahme für den Nutzer nicht kooperativ mit staatlichen Behörden zusammenarbeiten. Um dies

113 *Denga*, in: Europäische Plattformregulierung, 2023, § 6 Rn. 12.
114 BMJ, Eckpunktepapier, S. 5.
115 GFF, Stellungnahme zu den Eckpunkten des Bundesjustizministeriums zum Gesetz gegen digitale Gewalt v.26.5.2023, S. 5, online abrufbar unter: https://www.bmj.de/SharedDocs/Downloads/DE/Gesetzgebung/Stellungnahmen/2023/0526_Stellungnahme_GFF_Eckpunkte_Gesetz_digitale_Gewalt.pdf?__blob=publicationFile&v=2 (zuletzt abgerufen am 27.10.2023).
116 BKA, Daten & Zahlen Meldestelle Hassposting, online abrufbar unter: https://www.bka.de/DE/KontaktAufnehmen/HinweisGeben/MeldestelleHetzeImInternet/DatenZahlen/datenzahlen_node.html (zuletzt abgerufen am 27.10.2023).
117 *Remmert*, in: Dürig/Herzog/Scholz, GG, Art. 103 Abs. 1 Rn. 1.
118 BMJ, Eckpunktepapier, S. 5.
119 Facebook, Positionspapier zu den Eckpunkten des Bundesjustizministeriums zum Gesetz gegen digitale Gewalt, S. 3, online abrufbar unter: https://www.bmj.de/SharedDocs/Downloads/DE/Gesetzgebung/Stellungnahmen/2023/0614_Stellungnahme_Meta_Eckpunkte_Gesetz_digitale_Gewalt.pdf?__blob=publicationFile&v=2 (zuletzt abgerufen am 27.10.2023).
120 Ebd.

zu verhindern wären Regelungen zu Sanktionsmöglichkeiten bei fehlender Kooperation von Diensteanbietern möglich[121], wobei diese dann ebenfalls neben den Regelungen des DSA anwendbar sein müssten.

b) Konflikt mit DSA

Gem. Art. 23 Abs. 1 DSA müssen Online-Plattformen die Accounts von Nutzern, die häufig rechtswidrige Inhalte verbreiten, vorübergehend aussetzen.[122] Fraglich ist somit, inwiefern zusätzliche nationale gesetzliche Regelungen zu Accountsperren neben den bereits im DSA vorgesehen Pflichten überhaupt möglich sind. Einer Ansicht nach besteht keine zusätzliche Regelungsmöglichkeit für nationale Accountsperren, da im Art. 23 des DSA genau diese geregelt werden und eine zusätzliche nationale Regelung der mit dem DSA bezweckten Harmonisierung der europäischen Regelungen entgegenstehen würde.[123] Zudem fehle es für eine ergänzende nationale Norm schon an einem „anderen berechtigten öffentlichen Interesse" (Erwägungsgrund 9 DSA).[124] Bei genauerer Betrachtung des Art. 23 DSA im Vergleich zu den im Gewaltschutzgesetz geplanten Accountsperren vermag dies allerdings nicht zu überzeugen. Denn Art. 23 DSA sieht lediglich Vorgaben zu Accountsperren durch Diensteanbieter vor.[125] Im Gegensatz dazu plant das Gewaltschutzgesetz jedoch richterlich angeordnete Accountsperren, die somit eine staatliche Anordnung zur Verpflichtung von Diensteanbietern darstellen. Damit ist eine Regelungsüberschneidung der Anwendungsbereiche des Art. 23 DSA sowie des geplanten Gesetzes gegen digitale Gewalt nicht ersichtlich und sollte nationalen Regelungen zur richterlich angeordneten Accountsperren nicht im Wege stehen.[126]

4. Erleichterung der Zustellung

a) Inländischer Zustellungsbevollmächtigte

Die geplante Fortschreibung und Ausweitung der Pflicht zur Bereitstellung eines inländischen Zustellungsbevollmächtigten soll Betroffenen die Rechtsdurchsetzung ebenfalls erleichtern, indem die Zustellung für sie erleichtert wird, weil sie dadurch wissen, an wen sie sich bei Rechtsverletzungen in Deutschland wenden können.[127] Bisher ist die Pflicht zur Ernennung eines inländischen Zustellungsbevollmächtigten in § 5 NetzDG geregelt. Aufgrund der Aufhebung des NetzDG durch Inkrafttreten des DSA soll diese Pflicht im Gesetz gegen digitale Gewalt weitergeführt werden.[128] Das ist insofern begrüßenswert, als dass damit eine erhebliche Erleichterung für Betroffene einhergeht, indem eine einfache und praktikable Zustellung von Schriftstücken etc. möglich sein wird. Besonders in Anbetracht der strengen Zustellungsregelungen beispielsweise im einstweiligen Rechtsschutz ist die Möglichkeit der einfachen Zustellung für Betroffene essenziell.[129] Allerdings gilt die in § 5 NetzDG statuierte Pflicht ausschließlich für Anbieter sozialer Netzwerke.[130] Dies scheint im digitalen Gewaltschutzgesetz so fortgeführt zu werden, denn im Eckpunktepapier wird sich ebenfalls nur auf sog. soziale Netzwerke bezogen.[131] Während private

121 *Panahi,* MMR 2023, 556 (560).
122 *Raue,* in: NK-DSA, Art. 23 Rn. 18.
123 *Härting/Adamek,* CR 2023, 316 (320); *Holznagel*, MMR 2023, 643 (644).
124 *Holznagel*, MMR 2023, 643 (644).
125 *Maamar*, in: Das neue Recht der digitalen Dienste, 2023, § 4 Rn. 139.
126 *Cole/Ukrow,* Der EU Digital Services Act und verbleibende nationale (Gesetzgebungs-)Spielräume, 2023, S. 36 ff., online abrufbar unter: https://freiheitsrechte.org/uploads/documents/Demokratie/Marie-Munk-Initiative/DSA_Gutachten_Cole_Ukrow.pdf. (zuletzt aufgerufen am 12.2.2024); *Panahi*, MMR 2023, 556 (559).
127 BMJ, Eckpunktepapier, S. 6.
128 Ebd.
129 DJB, Stellungnahme, S. 18.
130 *Gerhold/Handel*, in: NK-MedienStrafR, § 5 Rn. 5.
131 BMJ, Eckpunktepapier, S. 6.

Auskunftsverfahren unter anderem dadurch gestärkt werden sollen, indem diese auch auf Messenger- und Internetzugangsdienste ausgeweitet werden sollen, erschließt sich aus dem Eckpunktepapier nicht, wieso die Pflicht zu inländischen Zustellungsbevollmächtigten nur auf soziale Medien beschränkt bleiben soll, zumal es dabei zu Abgrenzungsschwierigkeiten bei hybriden Diensten wie Telegram kommen kann.[132] Begrüßenswert wäre darüber hinaus, die Pflicht zu inländischen Zustellungsbevollmächtigten auch für den Schutz vor ungerechtfertigten Accountsperren auszuweiten.[133]

b) Vereinbarkeit mit DSA

Allerdings ist fraglich, inwiefern die geplante Regelung zur Pflicht eines inländischen Zustellungsbevollmächtigten als zusätzliche nationale Regelung insbesondere mit dem Harmonierungsgrundsatz des DSA vereinbar ist. Denn gem. Art. 12 Abs. 1 DSA müssen Anbieter von Vermittlungsdiensten eine zentrale Kontaktstelle für die Behördenkommunikation einrichten und gem. Art. 13 Abs. 1 DSA einen gesetzlichen Vertreter innerhalb der EU ernennen, wenn sie dort keine Niederlassung haben. Somit unterscheiden sich die Regelungen enorm, weil nach dem DSA Anbieter lediglich eine Kontaktstelle (gem. Art. 13 DSA einen Vermittler) in einem EU-Mitgliedstaat einrichten müssen, nicht also (wie im digitalen Gewaltschutzgesetz geplant) eine Zustellungsvertretung in Deutschland. Teilweise wird argumentiert, dass die im digitalen Gewaltschutzgesetz geplante Pflicht der Harmonisierung europäischer Regelungen und der Rechtssicherheit durch den DSA widerspräche. [134] Andere sehen keine unionsrechtlichen Konflikte, weil die nationale Regelung über die des DSA hinausgeht und durch eine fehlende nationale Regelung eine erhebliche Schutzlücke entstehen würde.[135] Allerdings ist im Vergleich der Regelungen auch hier irritierend, wieso die Pflicht im Gesetz gegen digitale Gewalt nur für soziale Netzwerke gelten soll, während im DSA alle „Anbieter von Vermittlungsdiensten“ (Art. 12, 13 DSA) erfasst werden.[136] Es lässt sich kein sachlicher Grund erkennen, warum bestimmte Vermittlungsdienste durch nationale Gesetzgebung erheblicher in die Pflicht genommen werden sollen als andere.

Im Wesentlichen ist allerdings sehr zweifelhaft, ob zusätzliche nationale Pflichten bzgl. eines inländischen Zustellungsbevollmächtigten tatsächlich neben den Regelungen des DSA möglich sein werden. Denn in Erwägungsgrund 9 des DSA wurde festgestellt, dass Mitgliedstaaten keine zusätzlichen nationalen Anforderungen, die in den Anwendungsbereich des DSA fallen, erlassen oder beibehalten sollten.[137] Wenngleich die geplanten Regelungen weit über Art. 12, 13 DSA hinausgehen, so betreffen sie dennoch grundsätzlich den gleichen Anwendungsbereich einer Kontaktstelle für Betroffene.[138]

Zusammenfassend wären die geplanten Regelungen zu inländischen Zustellungsbevollmächtigten im Sinne der Betroffenen digitaler Rechtsverletzungen oder Gewalt zwar (sogar mit Erweiterung auf eine Beschwerdestelle für Accountsperren) durchaus sinnvoll, jedoch bestehen erhebliche Zweifel für eine zusätzliche nationale Regelungsmöglichkeit neben dem DSA. Dabei ist entscheidend, dass das maßgebliche Ziel des DSA die Harmonisierung der Regelungen in den EU-Mitgliedstaaten ist.

132 *Panahi*, MMR 2023, 556 (560).
133 Amnesty International, Stellungnahme, S. 3.
134 *Härting/Adamek*, CR 2023, 316 (319); DAV, Stellungnahme, S. 8; Facebook, Stellungnahme, S. 3.
135 *Cole/Ukrow* (Fn. 126), S. 26 f.
136 *Härting/Adamek*, CR 2023, 316 (319).
137 VO (EU) 2022/2065 (Digital Services Act).
138 *Panahi,* MMR 2023, 556 (561); *Härting/Adamek,* CR 2023, 316 (319).

5. Fehlende Aspekte

Für eine tatsächliche Verbesserung für Betroffene digitaler Gewalt sind jedoch nicht lediglich die gesetzlichen Grundlagen essenziell, sondern vor allem, dass diese auch tatsächlich umgesetzt werden können. Daran bestehen durch den Mehraufwand, den ein ausgeweitetes Auskunftsverfahren sowie der Anspruch auf richterlich angeordnete Accountsperren mit sich bringen würden, in Anbetracht der personellen Aufstellung der Justiz erhebliche Zweifel.[139] Ansonsten besteht die Gefahr, dass die Verbesserungen aufgrund personeller Defizite nicht umgesetzt werden können. Des Weiteren belegt das Eckpunktepapier (sowie das Erläuterungspapier) selbst mit der verwendeten Terminologie und der zu vermissenden sprachlichen Sensibilität, dass die konsequente und nachhaltige Bekämpfung digitaler Gewalt bereits viel früher ansetzen muss. Denn auch dabei zeigt sich ein Grundsatzproblem dieses Phänomens: dass häufig die Realität digitaler Gewalt und ihrer Folgen nicht vollständig realisiert oder anerkannt werden. Dies sowie die Qualifikation aller am Verfahren Beteiligten ist allerdings grundlegende Prämisse für die effektive (rechtliche) Unterstützung Betroffener. Deswegen sind darüber hinaus Maßnahmen wie Bildung und Sensibilisierung über die Erscheinungsformen, Gefahren und Auswirkungen digitaler Gewalt bereits im frühen Alter sowie Fortbildungen für am formellen Verfahren Beteiligte wie Mitarbeiter bei Polizei und Justiz notwendig.

Darüber hinaus ist kritisch zu betrachten, dass mit dem Eckpunktepapier der Anschein erweckt wird, dass die Verfolgung von Rechtsverletzungen (zunehmend) auf Betroffene umgelagert werden könnte. Dabei ist insbesondere die Formulierung, dass „die Durchsetzung von Recht nie allein Sache von Staatsanwaltschaften […]"[140] sein sollte, durchaus fragwürdig. Eine Verdeutlichung, dass trotz verbesserter Rechtsdurchsetzungsrechte für Betroffene weiterhin die Verpflichtung der Staatsanwaltschaften besteht, Straftaten grundsätzlich von Amts wegen nachgehen zu müssen, wäre erfreulich.[141]

VII. Fazit

In der Theorie lässt das Eckpunktepapier grundsätzlich gute Ansätze für die bessere Rechtsdurchsetzung und den besseren Schutz Betroffener digitaler Rechtsverletzungen erkennen. Dazu gehört insbesondere die Möglichkeit von Accountsperren, wenngleich auch diese in ihrer konkreten Ausgestaltung (wie ihrem Anwendungsbereich) teilweise noch verbesserungswürdig sind. Auch die Ausweitung des Auskunftsverfahrens auf Messenger- und Internetzugangsdienste sowie die effektivere Ausgestaltung dessen ist begrüßenswert. Jedoch bestehen teilweise erhebliche Zweifel an der tatsächlichen Umsetzbarkeit aufgrund des erheblichen personellen Mehraufwands und der (zeitlich) begrenzten Möglichkeiten der Identifizierung von rechtverletzenden Personen. Darüber hinaus ist die geplante Regelung (und Ausweitung) der Pflicht zur Bereitstellung eines inländischen Zustellungsbevollmächtigten im Sinne der Betroffenen zwar nachvollziehbar und wünschenswert, doch ist dessen Realisierbarkeit in Anbetracht des Harmonierungsgrundsatzes des DSA äußerst fragwürdig. Inwiefern die geplanten Maßnahmen grundsätzlich mit dem DSA vereinbar sein werden, bleibt abzuwarten.

Eine tatsächliche Verbesserung der Position Betroffener von digitalen Rechtsverletzungen und insbesondere digitaler Gewalt setzt Veränderung voraus, die weit über die im Eckpunktepapier geplanten Maßnahmen hinausgehen. Dazu gehören insbesondere der Ausbau des Opferschutzes und -beratungen, sowie Aus- und Fortbildungen für am

139 DRB, Stellungnahme, S. 4.
140 BMJ, Eckpunktepapier, S. 1 f.
141 *Valerius*, ZRP 2023, 142 (143).

Verfahren Beteiligte. Denn letztlich sind verbesserte Rechtsgrundlagen für Betroffene wenig hilfreich, wenn diese aufgrund fehlender Sensibilisierung nicht hinreichend angewendet werden. Die Notwendigkeit einer erhöhten Sensibilität für die mögliche Intensität und Auswirkungen digitaler Gewalt werden schließlich bereits mit der verwendeten Sprache im Eckpunkte- und Erläuterungspapier deutlich.

Darüber hinaus bleibt zu hoffen, dass durch die Einführung des digitalen Gewaltschutzgesetzes, dessen Fokus auf der Rechtsdurchsetzung für Betroffene liegt, die gesetzgeberischen Möglichkeiten für Strafänderungen oder -schärfungen nicht als ausgeschöpft betrachtet werden.

Der digitale Raum bietet unbegrenzte Möglichkeiten für die Vernetzung und den Meinungsaustausch unzähliger Menschen in kurzer Zeit und auf unkomplizierte Art und Weise. Diesen Raum zu schützen, wird Aufgabe des Gesetzgebers bleiben, indem die (Grund-)Rechte, insbesondere die Meinungsfreiheit und die Möglichkeit zur Anonymität, aller Beteiligten bestmöglich gewahrt werden.