

Der BMJ-Entwurf „Digitale Gewalt“ – Schnittstellen zu § 201a StGB und Plattformregulierung

Rechtsanwalt/Notar Dr. iur. Dr. rer. pol. Fabian M. Teichmann, LL.M. (London), MBA (Oxford), St. Gallen*

Dieser Artikel untersucht den Diskussionsentwurf des Bundesministeriums der Justiz für ein „Gesetz gegen digitale Gewalt“ und dessen Auswirkungen auf den strafrechtlichen Schutz der Persönlichkeitsrechte im Internet. Dabei liegt ein besonderer Fokus auf den Schnittstellen zu § 201a StGB (Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen) und zu bestehenden Plattformregulierungen. Der Entwurf zielt auf eine Stärkung der individuellen Rechtsdurchsetzung bei „digitaler Gewalt“ ab, insbesondere durch erweiterte Auskunftsansprüche gegen Diensteanbieter und richterlich angeordnete Accountsperrn. Gleichzeitig wirft er verfassungsrechtliche Fragen auf. Es ist zu prüfen, ob die neuen Maßnahmen den Bestimmtheitsgrundsatz wahren und mit den Kommunikationsgrundrechten (Meinungsfreiheit, Recht auf Anonymität) vereinbar sind. Die Analyse kommt zu dem Ergebnis, dass das geplante Gesetz wichtige Schutzlücken schließt und die Rechtsstellung von Opfern digitaler Übergriffe verbessert, jedoch bestimmte Begriffsbestimmungen und Verfahrensgarantien präzisiert werden müssen, um verfassungsrechtlichen Anforderungen, etwa an die Normenklarheit und die Verhältnismäßigkeit von Grundrechtseingriffen, gerecht zu werden.

I. Einleitung	826
II. Normative Grundlagen	827
1. Strafrechtlicher Persönlichkeitsschutz online und § 201a StGB	827
2. Zivilrechtliche Ansprüche und Lücken im Online-Kontext	828
3. Plattformregulierung und europäische Entwicklungen	829
III. Dogmatische Analyse des BMJ-Entwurfs „Digitale Gewalt“	829
1. Überblick über die Neuerungen des Gesetzentwurfs	829
a) Erweiterter Auskunftsanspruch gegenüber Diensteanbietern und Access-Providern	830
b) Gerichtliche Accountsperrre	830
c) Zustellungsbevollmächtigter für Auslandsplattformen	831
2. Verfassungsrechtliche Einordnung der Auskunftsansprüche	831
3. Verfassungsrechtliche Einordnung der Accountsperrre	832
IV. Rechtsprechung	833
1. Auskunftsansprüche und Anonymität	833
2. Maßnahmen gegen Online-Hass und -Hetze	834
V. Schluss	835

* Fabian Teichmann ist Lehrbeauftragter an der Universität zu Köln, der Universität Kassel und der Universität Trier sowie Managing Partner einer Anwaltskanzlei.

I. Einleitung

Das Internet hat sich zum zentralen Kommunikationsraum entwickelt, birgt jedoch auch neue Gefahren für die Persönlichkeitsrechte. Phänomene wie Cybermobbing, Hassrede („hate speech“), Doxing (Veröffentlichen personenbezogener Daten) oder das Verbreiten intimer Aufnahmen ohne Einwilligung („revenge porn“) werden unter dem Schlagwort digitale Gewalt zusammengefasst. Zwar sind viele dieser Verhaltensweisen bereits heute strafbewehrt – etwa als Beleidigung (§ 185 StGB), Bedrohung (§ 241 StGB), Verleumdung (§ 187 StGB) oder Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen (§ 201a StGB).¹ Dennoch zeigt sich in der Praxis, dass Betroffene digitaler Angriffe oft nur schwer effektiven Rechtsschutz erlangen. Hauptgründe sind die Anonymität im Netz und die rasante Verbreitungsmöglichkeit rechtswidriger Inhalte.²

Die Bundesrepublik Deutschland reagiert auf diese Problemlage mit dem geplanten „Gesetz gegen digitale Gewalt“ (GgdG). Ein im Dezember 2024 veröffentlichter Diskussionsentwurf des Bundesministeriums der Justiz (BMJ) sieht neuartige Instrumente vor, um Opfern digitaler Persönlichkeitsrechtsverletzungen schnellere und effektivere Gegenmaßnahmen an die Hand zu geben. Kernstücke des Entwurfs sind erweiterte Auskunftsansprüche gegen Diensteanbieter zur Identifizierung anonymer Täter sowie richterlich angeordnete Accountsperrern zur präventiven Unterbindung weiterer Rechtsverletzungen. Diese Maßnahmen sollen bestehende Schutzlücken schließen, indem sie die private Rechtsverfolgung im Internet erleichtern und beschleunigen.³ Dabei betont das BMJ, dass die neuen Eingriffsbefugnisse mit Richtervorbehalt versehen sind, um einen schonenden Ausgleich zwischen der Meinungsfreiheit der Äußernden, dem Persönlichkeitsschutz der Betroffenen und der unternehmerischen Freiheit der Plattformbetreiber zu gewährleisten.

Die Einführung solcher weitreichenden Instrumente wirft zugleich verfassungsrechtliche Fragen auf. Zum einen stellt sich die Frage nach der Bestimmtheit der gesetzlichen Grundlagen. Unklare Begriffe wie „digitale Gewalt“ oder nicht hinreichend konturierte Voraussetzungen für eine Account-Sperrung könnten gegen das Bestimmtheitsgebot nach Art. 103 Abs. 2 GG⁴ bzw. den allgemeinen Rechtsstaatsgrundsatz verstoßen. Zum anderen berühren Auskunftsanordnungen und Accountsperrern die Kommunikationsgrundrechte – insbesondere die Meinungsfreiheit gem. Art. 5 Abs. 1 S. 1 Var. 1 GG⁵ und das Recht auf informationelle Selbstbestimmung bzw. Anonymität im Netz gem. Art. 2 Abs. 1 GG.⁶ Kritiker warnen vor einem „chilling effect“ – einer abschreckenden Wirkung auf rechtmäßige Online-Kommunikation, wenn Nutzer verstärkt eine Enttarnung befürchten. Umgekehrt kann ungehinderte digitale Gewalt einen „silencing effect“ haben, indem sich Betroffene aus Furcht vor weiteren Angriffen aus dem öffentlichen Diskurs zurückziehen.⁷ Seitens des Gesetzgebers gilt es, beide Aspekte in ein verfassungskonformes Gleichgewicht zu bringen.

Die vorliegende Untersuchung beleuchtet zunächst die bestehenden normativen Grundlagen (II.), insbesondere § 201a StGB als zentrale Strafnorm zum Schutz vor bildbezogener digitaler Gewalt, sowie die einschlägigen Regelungen der Plattformregulierung (NetzDG, EU-DSA). Anschließend werden die wesentlichen Inhalte des BMJ-Entwurfs dogmatisch eingeordnet (III.), gefolgt von einem Blick auf die Rechtsprechung zu ähnlichen Fragestellungen (IV.). In Teil V. werden Stimmen aus der

¹ Diskussionsentwurf des Bundesministeriums der Justiz (13.6.2025), S. 24.

² Diskussionsentwurf des Bundesministeriums der Justiz (13.6.2025), S. 1.

³ Diskussionsentwurf des Bundesministeriums der Justiz (13.6.2025), S. 2.

⁴ Remmert, in: Dürig/Herzog/Scholz, Grundgesetz, Kommentar, 106. Lfg., Stand: Oktober 2024, Art. 103 Abs. 2.

⁵ Jarass, in: Jarass/Pieroth, Grundgesetz, Kommentar, 18. Aufl. 2024, Art. 5.

⁶ Eichberger, in: Huber/Voßkuhle, Grundgesetz, Kommentar, Bd. 1, 8. Aufl. 2024, Art. 2; Schulte, KriPoZ (JuP) 2024, 3 (13).

⁷ Schulte, KriPoZ (JuP) 2024, 3 (14).

Literatur und Kritik am Entwurf dargestellt. Der Schluss (VI.) fasst die Ergebnisse zusammen und wagt einen Ausblick auf etwaigen Nachbesserungsbedarf.

II. Normative Grundlagen

1. Strafrechtlicher Persönlichkeitsschutz online und § 201a StGB

Der deutsche Gesetzgeber hat in den letzten Jahren mehrfach auf neue Phänomene digitaler Gewalt reagiert und den strafrechtlichen Persönlichkeitsschutz ausgebaut. Dabei sind bereits klassische Delikte wie Beleidigung, üble Nachrede oder Verleumdung gem. §§ 185 ff. StGB⁸ und Bedrohung gem. § 241 StGB⁹ im Internet verwirklicht. Ein spezifischer Straftatbestand „Cybermobbing“ fehlt zwar, doch können hartnäckige Online-Belästigungen als Nachstellung gem. § 238 StGB¹⁰ verfolgt werden. Besonders schwere Fälle von Hassrede lassen sich als Volksverhetzung gem. § 130 StGB¹¹ ahnden.

Eine bedeutsame Rolle spielt im Kontext digitaler Gewalt § 201a StGB, der die Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen unter Strafe stellt.¹² Diese Norm, 2004 eingeführt¹³ und zuletzt 2021 erweitert¹⁴, schützt das Persönlichkeitsrecht in Bezug auf Bildaufnahmen. Strafbar ist gem. (§ 201a Abs. 1 Nr. 1 StGB¹⁵ unter anderem, wer unbefugt Bildaufnahmen von einer Person in deren höchstpersönlichem Lebensbereich, also einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, herstellt oder überträgt und dadurch den höchstpersönlichen Lebensbereich der abgebildeten Person verletzt. Ebenso wird gem. § 201a Abs. 2 StGB¹⁶ bestraft, wer unbefugt von einer anderen Person eine Bildaufnahme, die geeignet ist, dem Ansehen der abgebildeten Person erheblich zu schaden, einem Dritten zugänglich macht. Erfasst werden insbesondere heimliche Aufnahmen im privaten Raum (z.B. Wohnung) oder von einer hilflosen Person, aber auch das Verbreiten solcher Aufnahmen. In der Praxis dient § 201a StGB als zentrales Instrument gegen „revenge porn“ und ähnliche Formen bildbasierter digitaler Gewalt.¹⁷ So fällt etwa das Veröffentlichen intimer Fotos eines Ex-Partners ohne Einwilligung typischerweise unter § 201a StGB, da dadurch der höchstpersönliche Lebensbereich des Opfers verletzt wird.¹⁸ Pornographische Deepfakes – mittels KI erzeugte intime Bildaufnahmen einer Person, insbesondere von Kindern – dürften vom Tatbestand des § 184b Abs. 1 S. 1 Nr. 2 und Abs. 3 StGB erfasst sein.¹⁹ Allerdings greift § 201a StGB nicht in allen Konstellationen. Nicht-pornographische Bildmanipulationen oder das unbefugte Veröffentlichen personenbezogener Daten (Doxing) sind von § 201a StGB nicht ohne Weiteres abgedeckt und fallen, sofern nicht noch die Voraussetzungen des § 126a StGB vorliegen²⁰, in eine Straf-

⁸ König/Schork, in: Schumann/Mosbacher/König, Medienstrafrecht, Kommentar, 2023, StGB § 185; Heinze, in: Schumann/Mosbacher/König, Medienstrafrecht, Kommentar, 2023, StGB § 186.

⁹ Valerius, in: BeckOK StGB, Stand: 1.8.2025, § 241 Rn. 3–8.

¹⁰ Sonnen, in: NK-StGB, Bd. 4, 6. Aufl. 2023, § 238 Rn. 31.

¹¹ Anstötz, in: MüKo-StGB, Bd. 3, 5. Aufl. 2025, § 130 Rn. 39.

¹² Kargl, in: NK-StGB, Bd. 3, 6. Aufl. 2023, § 201a Rn. 9, 10.

¹³ BGBl. I 2004, S. 1950.

¹⁴ BT-Drs. 18/9327; BR-Drs. 226/16.

¹⁵ Kargl, in: NK-StGB, Bd. 3, 6. Aufl. 2023, § 201a Rn. 9.

¹⁶ Kargl, in: NK-StGB, Bd. 3, 6. Aufl. 2023, § 201a Rn. 18.

¹⁷ Terhaag/Schwarz, Influencer-Marketing, Rechtshandbuch, 2. Aufl. 2025, § 3 Rn. 215.

¹⁸ Graf, in: MüKo-StGB, Bd. 4, 4. Aufl. 2021, § 201a.

¹⁹ Diskussionsentwurf des Bundesministeriums der Justiz (13.6.2025), S. 24; Schmidt, KriPoZ 2024, 183.

²⁰ Puschke, in: MüKo-StGB, Bd. 3, 5. Aufl. 2025, § 126a Rn. 12.

barkeitslücke. Upskirting und ähnliche voyeuristische Aufnahmen wurden 2021 durch § 184k StGB²¹ als Sexualdelikt unter Strafe gestellt, weil § 201a StGB solche Fälle zuvor nicht eindeutig erfasste.²² Dennoch bleibt der strafrechtliche Schutz lückenhaft und in verschiedene Tatbestände zersplittert, was die Systematik und Wirksamkeit erschwert.

2. Zivilrechtliche Ansprüche und Lücken im Online-Kontext

Neben dem Strafrecht gewährt das deutsche Recht den Opfern persönlicher Rechtsverletzungen Ansprüche auf Unterlassung, Beseitigung und Schadensersatz. Insbesondere bei Verletzungen des allgemeinen Persönlichkeitsrechts gem. Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG²³, zu dem der Schutz des eigenen Bildes und der Intimsphäre gehört, stehen zivilrechtliche Unterlassungsansprüche zur Verfügung. So kann etwa das unbefugte Veröffentlichen von Bildern einer Person im Internet zivilrechtlich untersagt und, gestützt auf § 1004 BGB²⁴ analog i.V.m. § 22 KUG²⁵ bzw. dem Allgemeinen Persönlichkeitsrecht (APR)²⁶, deren Löschung verlangt werden. In der Praxis erwirken Betroffene rechtswidriger Inhalte häufig einstweilige Verfügungen gegen die Plattformbetreiber, um beleidigende Posts, diffamierende Behauptungen oder intime Fotos kurzfristig entfernen zu lassen. Allerdings richtet sich ein solcher Unterlassungsanspruch zunächst nur gegen den Plattformbetreiber als Störer, nicht unmittelbar gegen den unbekannten Täter. Die Plattformregulierung, insbesondere das Netzwerkdurchsetzungsgesetz (NetzDG) für die Zulassung eines sozialen Netzwerkes²⁷ und die Verpflichtung nach Art. 9 des DSA (Digital Services Act) zur Anordnung zum Vorgehen gegen rechtswidrige Inhalte verpflichtet soziale Netzwerke zwar zur raschen Löschung eindeutig rechtswidriger Inhalte und schafft behördlichen Durchsetzungsdruck.²⁸ Doch für das *individuelle* Rechtsschutzinteresse der Opfer – etwa Genugtuung durch Bestrafung des Täters oder Schadensersatz – greift das nicht weit genug.

Ein zentrales Problem war bislang die Identifizierung anonymer oder pseudonymer Täter im Netz. Ohne Kenntnis von Name oder Anschrift des Verletzers können Opfer ihre zivilrechtlichen Ansprüche nicht direkt gegen diesen geltend machen. Strafverfahren offenbaren die Täteridentität oft nicht schnell genug oder gar nicht, insbesondere wenn die Taten mangels Priorität nicht intensiv verfolgt werden. Zwar existiert seit 2017 ein gerichtliches Auskunftsverfahren, seit 2021 aus § 21 Telekommunikation-Telemedien-Datenschutz-Gesetz (das TDDDG wurde 2024 in TTDSG umbenannt), TTDSG²⁹, das es Opfern ermöglichen soll, von Plattformbetreibern Auskunft über Bestandsdaten der Nutzer zu erhalten. Dieses Verfahren setzt jedoch voraus, dass der betroffene Inhalt einen bestimmten Straftatbestand aus einem festgelegten Katalog, u.a. Beleidigung, üble Nachrede, Bedrohung, Volksverhetzung, § 201a StGB etc. erfüllt oder absolut geschützte Rechte verletzt.³⁰ Zudem benötigt der Plattformbetreiber seinerseits oft die Mitwirkung des Internetzugangsanbieters

²¹ Heger, in: Lackner/Kühl/Heger, Strafgesetzbuch, Kommentar, 30. Aufl. 2023, § 184k Rn. 1–3.

²² Schmidt, in: Burghardt/Schmidt/Steinl, Sexuelle Selbstbestimmung jenseits des Körperlichen, 2024, S. 181 f.

²³ Barczak, in: Dreier, Grundgesetz, Kommentar, Bd. 1, 4. Aufl. 2023, Art. 2 Abs. 1.

²⁴ Pille, in: Leupold/Wiebe/Glossner, IT-Recht, Handbuch, 4. Aufl. 2021, Teil 15.2 Rn. 13, 14.

²⁵ Fricke, in: Wandtke/Bullinger, UrhR, Kommentar, 6. Aufl. 2022, KUG § 22 Rn. 23, 24.

²⁶ Schmidt, in: Burghardt/Schmidt/Steinl, Sexuelle Selbstbestimmung jenseits des Körperlichen, 2024, S. 181 f.; Specht-Riemenschneider, in: Dreier/Schulze, UrhG, Kommentar, 8. Aufl. 2025, KUG § 22 Rn. 10, 10a.

²⁷ Schmittmann, in: Hoeren/Sieber/Holznagel, Multimedia-Recht, Handbuch, 62. Lfg., Stand: Juni 2024, Teil 9 Rn. 170, 171.

²⁸ Diskussionsentwurf des Bundesministeriums der Justiz (13.6.2025), S. 1.

²⁹ Sesing-Wagenpfeil, in: BeckOK IT-Recht, Stand: 1.4.2025, TTDSG § 21 Rn. 4a, 9–12.

³⁰ § 21 TDDDG.

(Access-Providers), um etwa anhand einer IP-Adresse den tatsächlichen Nutzer zu ermitteln. Das bisherige Auskunftsverfahren erwies sich als umständlich. Es erforderte zwei separate Gerichtsbeschlüsse (gegen Plattform und Access-Provider) und führte häufig nicht zum Erfolg, weil zwischen- durch die nötigen Daten gelöscht wurden. Viele Betroffene standen daher trotz klarer Rechtsverletzungen ohne zivilrechtliche Sanktionsmöglichkeit da.³¹

3. Plattformregulierung und europäische Entwicklungen

Parallel zum nationalen Straf- und Zivilrecht beeinflusst das Europarecht den Rahmen für den Kampf gegen digitale Gewalt. Die EU hat mit der Verordnung (EU) 2022/2065³², bekannt als Digital Services Act (DSA), ein umfassendes Regelwerk geschaffen, das Pflichten großer Online-Plattformen im Umgang mit illegalen Inhalten festlegt. Der DSA belässt es jedoch im Kern bei der schon unter der E-Commerce-Richtlinie geltenden „notice-and-takedown“-Logik: Plattformen haften nicht für fremde Inhalte, müssen aber bei Kenntnis oder behördlicher Anordnung illegales Material entfernen.³³ Eine unmittelbare Identifikationspflicht für Nutzer enthält der DSA nicht; im Gegenteil wird die Möglichkeit anonymer Online-Nutzung auf Unionsebene grundsätzlich anerkannt.³⁴ Allerdings erlaubt der DSA weiterhin, dass nationale Gerichte oder Behörden gem. Art. 9 DSA in Einzelfällen Anordnungen erlassen, um Rechtsverletzungen abzustellen oder Informationen herauszugeben. Die Mitgliedstaaten dürfen also prozedurale Mechanismen wie das Auskunftsverfahren oder Accountsperrern vorsehen, solange diese im Rahmen der DSA-Vorgaben (Transparenz, Verhältnismäßigkeit, Achtung der Grundrechte) erfolgen.³⁵ Deutschland hat zur Umsetzung des DSA bereits Anpassungen vorgenommen, u.a. Umbenennung des TTDSG zu TDDDG und Klarstellungen im Auskunftsrecht.³⁶

Darüber hinaus ist auf EU-Ebene eine Ausweitung der „EU-Strafrechtsbereiche“ im Gespräch. Ein Initiativvorschlag zielt darauf ab, Hasskriminalität und Hassrede als neue Bereiche gem. Art. 83 Abs. 1 AEUV³⁷ zu definieren, um in Zukunft unionsweit harmonisierte Mindeststandards der Strafverfolgung zu ermöglichen.³⁸ Dies unterstreicht den grenzüberschreitenden Charakter digitaler Gewalt und den Willen, auf europäischer Ebene abgestimmte Gegenstrategien zu entwickeln. Bis entsprechende EU-Richtlinien erlassen und umgesetzt sind, liegt es jedoch in der Verantwortlichkeit der nationalen Gesetzgeber, durch effektive Gewaltschutzgesetze die bestehenden Schutzlücken zu schließen.

III. Dogmatische Analyse des BMJ-Entwurfs „Digitale Gewalt“

1. Überblick über die Neuerungen des Gesetzentwurfs

Der Diskussionsentwurf des BMJ für ein Gesetz gegen digitale Gewalt (GdG-DiskE) verfolgt das Ziel, die private Rechtsdurchsetzung bei Persönlichkeitsrechtsverletzungen im Internet zu stärken. Hierzu

³¹ Gesellschaft für Freiheitsrechte, Stellungnahme der Gesellschaft für Freiheitsrechte e.V. (GFF), 2023, (13.6.2026), S. 1.

³² Verordnung (EU) 2022/2065.

³³ Diskussionsentwurf des Bundesministeriums der Justiz (13.6.2025), S. 1.

³⁴ Schulte, KriPoZ (JuP) 2024, 3 (13).

³⁵ Diskussionsentwurf des Bundesministeriums der Justiz (13.6.2025), S. 15.

³⁶ § 21 TDDDG.

³⁷ Vogel/Eisele, in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, 85. Lfg., Stand: Mai 2025, AEUV Art. 83 Rn. 34, 35.

³⁸ Diskussionsentwurf des Bundesministeriums der Justiz (13.6.2025), S. 24.

sollen die zersplitterten Auskunfts- und Abwehransprüche in einem neuen Stammgesetz gebündelt und effizienter ausgestaltet werden.³⁹ Zentral sind dabei drei Neuerungen:

a) Erweiterter Auskunftsanspruch gegenüber Diensteanbietern und Access-Providern

Künftig soll eine von digitaler Gewalt betroffene Person einfacher Auskunft über die Identität eines unbekannten Täters erhalten können. Der Anwendungsbereich des Auskunftsanspruchs wird inhaltlich erweitert – erfasst werden alle oben genannten Straftatbestände (u.a. §§ 185 ff., 201a StGB, § 126a StGB, § 176b StGB) sowie sonstige rechtswidrige Inhalte, die absolut geschützte Rechte verletzen. Damit geht der Entwurf über die bisherige Limitierung auf bestimmte Delikte hinaus und schließt z.B. auch Fälle ein, in denen durch Bild- oder Wortbeiträge das Persönlichkeitsrecht verletzt wird, ohne dass ein spezieller Straftatbestand einschlägig ist. Ferner soll sich der Auskunftsanspruch auf alle wesentlichen Beteiligten erstrecken. Neben den Plattformen („Diensteanbietern“) werden ausdrücklich auch Messenger-Dienste und Internetzugangsdienste (ISP) einbezogen.⁴⁰ Das ist wichtig, weil häufig erst der Access-Provider die Auflösung einer IP-Adresse zu einem Klarnamen ermöglicht. Schließlich sieht der Entwurf eine frühzeitige richterliche Sicherung der Daten vor. Schon zu Beginn des Verfahrens kann das Gericht anordnen, dass die relevanten Bestands- und Verkehrsdaten von Plattform und Access-Provider vorläufig gespeichert werden, um einen Datenverlust während der Auskunftsbeschaffung zu verhindern.⁴¹ Dieses Element einer „quick freeze“-Anordnung stellt ein Novum im Zivilrecht dar und entspricht in etwa der Idee einer Beweissicherungsmaßnahme. Formell bleibt es beim Richtervorbehalt, d.h., die Auskunft wird nur auf richterliche Anordnung erteilt, wobei der Antrag des Opfers beim Landgericht gestellt werden muss.⁴²

b) Gerichtliche Accountsperre

Als zweites zentrales Instrument führt der Entwurf einen Anspruch des Opfers auf Sperrung des Nutzerkontos des Täters ein. Diese Maßnahme greift, wenn ein Nutzer über sein Konto schwerwiegende Rechtsverletzungen begeht und die konkrete Gefahr weiterer Verletzungen besteht. War bislang die Deaktivierung von Accounts primär eine freiwillige Maßnahme der Plattformbetreiber, etwa nach wiederholten Verstößen gegen Gemeinschaftsstandards, soll nun ein Gericht auf Antrag der verletzten Person die Sperre vornehmen können. Die Voraussetzungen orientieren sich an der Schwere und Wiederholungsgefahr, wobei bereits eine erstmalige gravierende Rechtsverletzung genügen kann, sofern weitere Übergriffe zu befürchten sind.⁴³ Damit trägt der Entwurf Bedenken Rechnung, man dürfe kein „einmaliges Recht auf Beleidigung“ einräumen.⁴⁴ Die Accountsperre wird per gerichtlicher Verfügung angeordnet und direkt an die Plattform adressiert, welche das Nutzerkonto zeitweise oder dauerhaft zu deaktivieren hat. Durch diese Konstellation fungiert die Accountsperre als eine Art präventive Unterlassungsverfügung, die – anders als herkömmliche Unterlassungsgebote – nicht nur bestimmte Inhalte verbietet, sondern die weitere Partizipation des Täters auf der Plattform unterbindet. Sie zielt damit ausdrücklich auch auf Fälle ab, in denen der Täter unbekannt bleibt oder sich

³⁹ Diskussionsentwurf des Bundesministeriums der Justiz (13.6.2025), S. 1/2.

⁴⁰ Schulte, KriPoZ (JuP) 2024, 3.

⁴¹ Diskussionsentwurf des Bundesministeriums der Justiz (13.6.2025), S. 2/26.

⁴² § 21 TDDDG.

⁴³ Diskussionsentwurf des Bundesministeriums der Justiz (13.6.2025), S. 19.

⁴⁴ Gesellschaft für Freiheitsrechte, Stellungnahme der Gesellschaft für Freiheitsrechte e.V. (GFF), 2023, (13.6.2026), S. 1.

im Ausland befindet. Selbst wenn keine Strafverfolgung greift, kann wenigstens dessen schädigen-
des Online-Treiben unterbrochen werden.⁴⁵

c) Zustellungsbevollmächtigter für Auslandsplattformen

Drittens verpflichtet das Gesetz soziale Netzwerke ohne Sitz in der EU, einen inländischen Zustellungsbevollmächtigten zu benennen.⁴⁶ Dies knüpft an bereits bestehende Verpflichtungen aus dem NetzDG an und soll sicherstellen, dass gerichtliche Schriftstücke wie etwa die genannten Anordnungen, wirksam zugestellt werden können. Dies gewährleistet eine effektive Durchsetzung auch gegenüber Plattformen im Ausland und ergänzt die Vorgaben des DSA.

2. Verfassungsrechtliche Einordnung der Auskunftsansprüche

Die vorgeschlagene Erweiterung der Auskunftsansprüche nach dem GgdG-Diskussionsentwurf berührt mehrere Grundrechte. Zunächst ist das Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 GG⁴⁷ der von einer Auskunft betroffenen Nutzer tangiert. Die Herausgabe von Bestandsdaten wie etwa Klarnamen, E-Mail-Adressen oder IP-Adressen ohne Einwilligung stellt einen Eingriff in das personenbezogene Datengeheimnis dar.⁴⁸ Das BVerfG betonte 2020, dass ein Auskunftsverfahren nur bei hinreichend qualifizierten Rechtsverletzungen und mit Richtervorbehalt verfassungsgemäß ist. Im Urteil „Bestandsdatenauskunft II“ erklärte das Gericht damalige Regelungen teilweise für nichtig, weil sie u.a. keinen hinreichenden Richtervorbehalt vorsahen und die Abfrage von Passwörtern ermöglichten⁴⁹ – beides Punkte, die im vorliegenden GgdG-Entwurf so nicht enthalten sind. Aus der Entscheidung lässt sich jedoch entnehmen, dass eine Auskunftsanordnung immer nur zum Schutz gewichtiger Rechtsgüter zulässig ist und mit effektiven Verfahrensgarantien wie Richtervorbehalt und Benachrichtigungspflichten versehen sein muss.⁵⁰

Allerdings erscheint der Auskunfts-Anwendungsbereich als zu weit gefasst. Kritiker warnen, dass darunter auch Fälle ohne Bezug zur eigentlichen digitalen Gewalt fallen könnten, etwa wenn Unternehmen auf diesem Wege anonyme Portal-Kritiker enttarnen lassen.⁵¹ Hier wären die Grenzen des Bestimmtheitsgebots erreicht; der Gesetzgeber muss klarstellen, dass nur gravierende Persönlichkeitsangriffe erfasst sind.

Neben dem Datenschutzgrundrecht ist die Meinungsfreiheit gem. Art. 5 Abs. 1 S. 1 Var. 1 GG berührt.⁵² Die Möglichkeit, online anonym oder unter Pseudonym seine Meinung zu äußern, genießt Verfassungsrang. Die Aussicht, im Falle einer (behaupteten) Rechtsverletzung identifiziert zu werden, kann eine abschreckende Wirkung auf potenzielle Äußernde haben – der genannte chilling effect. Dieses Phänomen hat das Bundesverfassungsgericht zwar nicht ausdrücklich im Kontext privater Auskunftsansprüche behandelt, doch lässt sich aus seiner Rechtsprechung ableiten, dass die Gesetzesausgestaltung diesen Effekt minimieren muss. Insbesondere muss der Auskunftsanspruch

⁴⁵ Diskussionsentwurf des Bundesministeriums der Justiz (13.6.2025), S. 2.

⁴⁶ Diskussionsentwurf des Bundesministeriums der Justiz (13.6.2025), S. 2.

⁴⁷ Barczak, in: Dreier, Grundgesetz, Kommentar, Bd. 1, 4. Aufl. 2023, Art. 2 Abs. 1 Rn. 90.

⁴⁸ Schulte, KriPoZ (JuP) 2024, 3 (13).

⁴⁹ BVerfG, Beschl. v. 27.5.2020 – 1 BvR 1873/13, Rn. 194, 257.

⁵⁰ Schulte, KriPoZ (JuP) 2024, 3 (14).

⁵¹ Gesellschaft für Freiheitsrechte, Stellungnahme der Gesellschaft für Freiheitsrechte e.V. (GFF), 2023, (13.6.2026), S. 1.

⁵² Grabenwarter, in: Dürig/Herzog/Scholz, Grundgesetz, Kommentar, 106. Lfg., Stand: Oktober 2024, Art. 5 Abs. 1 Rn. 23, 24.

eng auf klare Unrechtsgehalte begrenzt sein (z.B. strafbare Inhalte), damit Nutzer nicht die berechnete Furcht haben, schon für grenzwertige oder eigentlich zulässige Äußerungen enttarnt zu werden. Hier zeigt die Dogmatik der Meinungsfreiheit aber auch die Gegenperspektive. Unerkannt agierende Täter können durch extreme Schmähungen oder Drohungen den öffentlichen Diskurs von anderen „säubern“ (silencing effect).⁵³ Ein zu starkes Gewicht auf Anonymität würde also umgekehrt die Meinungsfreiheit der Opfer und vieler Bürger beeinträchtigen, die sich aus Angst zurückhalten. Die Verhältnismäßigkeitsprüfung muss folglich austarieren, ob der Gewinn an effektivem Rechtsschutz und damit mittelbar an Meinungsvielfalt, weil Opfer geschützt werden, den möglichen Abschreckungseffekt für andere Nutzer überwiegt. Im GdG-Entwurf sind wesentliche Sicherungen wie richterliche Kontrolle, Verfahren nach den Regeln der freiwilligen Gerichtsbarkeit, Anhörungsmöglichkeiten für Plattform und ggf. Nutzer eingebaut.⁵⁴ Außerdem bleibt die anonyme Nutzung im Grundsatz erlaubt, es gibt also keine generelle Klarnamenpflicht, was der DSA-konformen Linie entspricht.⁵⁵ Die Maßnahme greift nur im berechtigten Einzelfall. Insofern erscheint der Auskunftsanspruch bei enger Auslegung, beschränkt auf schwerwiegende Rechtsverletzungen und mit hohen Hürden, grundrechtskonform, verlangt aber eine sorgfältige Handhabung durch die Gerichte. Insbesondere sollten Richter die Möglichkeit haben, Anträge abzuweisen, wenn der Eingriff außer Verhältnis zum behaupteten Rechtsverstoß stünde, wie z.B. bei Bagatellen oder zweifelhaften Ansprüchen.

3. Verfassungsrechtliche Einordnung der Accountsperre

Die Account-Aussetzung als neues Instrument berührt vor allem die Meinungsfreiheit der jeweiligen Nutzerin oder des Nutzers. Ein vollständiger Ausschluss von einer Kommunikationsplattform, sei es zeitweise oder endgültig, bedeutet faktisch ein Publikationsverbot in diesem Forum und damit einen Eingriff in Art. 5 Abs. 1 S. 1 Var. 1 GG.⁵⁶ Zwar handelt es sich nicht um ein generelles Berufs- oder Äußerungsverbot, doch gerade große soziale Netzwerke stellen heute zentrale Orte der Meinungsbildung dar; ein dortiges Redeverbot kommt einer erheblichen Beschränkung der individuellen Kommunikationsmöglichkeiten gleich. Entsprechend streng sind die Anforderungen an Normenklarheit und Verhältnismäßigkeit. Der Gesetzgeber muss aufgrund des Bestimmtheitsgebots klar definieren, unter welchen Voraussetzungen ein Gericht eine Accountsperre verhängen darf.⁵⁷ Der Entwurf stellt auf „schwerwiegende Rechtsverletzungen“ ab, belässt aber die inhaltliche Schwerebestimmung weitgehend den Gerichten. Hier könnte etwa durch eine beispielhafte Aufzählung wie Beleidigungen von erheblichem Gewicht, beharrliches Cyberstalking, Verbreitung schwerer Hetze oder intimster Aufnahmen etc. mehr Kontur geschaffen werden. Anknüpfungspunkt wird meist ein bestimmter strafbarer Inhalt sein, der über das betreffende Konto verbreitet wurde. Unklar ist, ob auch kumulativ mehrere weniger gravierende Verstöße eine Sperre rechtfertigen könnten, z.B. anhaltendes „trolling“ unterhalb der Strafbarkeitsgrenze. Fehlt es an Präzision, droht die Norm im Zweifel wegen Bestimmtheitsmangels verfassungswidrig zu sein, da die Bürger nicht vorhersehen können, welches Verhalten zu einer Sperre führen kann.

Ist die Norm hinreichend bestimmt, muss die konkrete Anordnung verhältnismäßig sein. Hier kommen die eingebauten Hürden des Richtervorbehalts und die Prüfung der Wiederholungsgefahr ins Spiel. Eine Accountdeaktivierung ist nur zulässig, wenn ohne sie fortgesetzte Persönlichkeitsver-

⁵³ Schulte, KriPoZ (JuP) 2024, 3 (14).

⁵⁴ § 21 TDDDG.

⁵⁵ Schulte, KriPoZ (JuP) 2024, 3 (13).

⁵⁶ Schemmer, in: BeckOK GG, Stand: 15.6.2025, Art. 5 Abs. 1 S. 1 Hs. 1 Rn. 11.

⁵⁷ Aust, in: Huber/Voßkuhle, Grundgesetz, Kommentar, Bd. 3, 8. Aufl. 2024, Art. 103 Rn. 98.

letzungen zu erwarten sind. Damit hat die Maßnahme den Charakter einer präventiven Gefahrabwehr. Das BVerfG fordert bei präventiven Maßnahmen, die Grundrechte beschränken, dass sie einem über-
ragend wichtigen Schutzgut dienen und kein milderes Mittel verfügbar ist.⁵⁸ Im Kontext digitaler Gewalt dürfte der Schutz der Persönlichkeit und der öffentlichen Sicherheit wie Schutz vor schweren Straftaten wie etwa andauernde Bedrohungen als legitimer Zweck anerkannt werden. Als milderes Mittel käme z.B. die bloße Löschung einzelner Beiträge in Betracht. Die Accountsperre greift indes weiter, da sie den Nutzer auch an künftigen legalen Äußerungen hindert. Sie sollte daher wirklich ultima ratio sein, was der Entwurf implizit anerkennt, indem er eine Sperre erst bei erheblicher Verletzung und Wiederholungsgefahr erlaubt. Zudem kann die Sperre zeitlich begrenzt werden, etwa bis zur Hauptsacheentscheidung oder für eine bestimmte Dauer, was die Verhältnismäßigkeit wahrt.

Ein besonderer Aspekt ist die Grundrechtsbindung Privater. Formal handelt es sich um einen zivilrechtlichen Unterlassungsanspruch, doch die Vollziehung läuft über private Plattformbetreiber, die den Account schließen. Hier stellt sich die Frage, ob große soziale Netzwerke selbst an Grundrechte gebunden sind oder jedenfalls über das zivilrechtliche Instrumentarium Grundrechte Dritter, also der Gespernten, mittelbar zu berücksichtigen sind. Diese Problematik ist vergleichbar der Diskussion um „Facebook-Urteile“, wo Gerichte über die Zulässigkeit privater Accountsperren entschieden. Wegen der Bedeutung großer Plattformen als Kommunikationsräume muss dem Kontoinhaber vor der Sperrentscheidung rechtliches Gehör gem. Art. 103 Abs. 1 GG gewährt werden,⁵⁹ der Entwurf sieht dementsprechend eine vorherige Stellungnahme des Nutzers vor.

Letztlich dürfte die verfassungsrechtliche Rechtfertigung der Accountsperre auf einer Abwägung zwischen dem Persönlichkeitsrecht des Opfers nach Art. 2 Abs. 1 GG und der Meinungsfreiheit des Täters beruhen. In besonders exzessiven Fällen digitaler Gewalt, wie etwa wiederholte schwerste Beleidigungen, Cyberstalking oder Verbreitung intimster Bilder trotz Untersagung, wird das Persönlichkeitsrecht und das Rechtsgut der Unversehrtheit des Opfers regelmäßig überwiegen. Die Accountsperre beschränkt zwar die Kommunikationsfreiheit, bewahrt aber den offenen Diskurs vor einem „Verstummen“ der Opfer und anderer Nutzer, die von der aggressiven Präsenz des Täters abgeschreckt würden.⁶⁰ Sofern die Maßnahme eng begrenzt bleibt auf evidente und andauernde Rechtsverletzungen, ist sie als notwendiges Schutzmittel im digitalen Raum vertretbar. Gleichwohl bleibt sie ein scharfes Schwert – eine Art digitales Hausverbot – das behutsam eingesetzt werden muss. Es wird Aufgabe der Rechtsprechung sein, klare Kriterien wie etwa Schwellen der „Schwere“ herauszuarbeiten und so für eine einheitliche Anwendung zu sorgen, um dem Bestimmtheitsgrundsatz in der praktischen Handhabung zur Geltung zu verhelfen.

IV. Rechtsprechung

Da das Gesetz gegen digitale Gewalt noch im Entwurfsstadium ist, existiert naturgemäß keine Rechtsprechung speziell zu dessen Vorschriften. Allerdings haben Gerichte bereits in verwandten Bereichen Entscheidungen getroffen, die für die hier diskutierten Fragen wegweisend sind.

1. Auskunftsansprüche und Anonymität

Der Bundesgerichtshof (BGH) hat in mehreren Urteilen Grundsätze zur Abwägung zwischen Persönlichkeitsrechtsschutz und anonymisierter Meinungsäußerung formuliert. Im vielbeachteten Urteil

⁵⁸ BVerfG, Beschl. v. 31.1.2022 – 1 BvR 208/22, Rn. 5.

⁵⁹ Schulze-Fielitz, in: Dreier, Grundgesetz, Kommentar, 3. Aufl. 2018, Art. 103 Abs. 1 Rn. 16, 17.

⁶⁰ Schulte, KriPoZ (JuP) 2024, 3 (14).

„Spickmich“ aus dem Jahr 2009 wies der BGH die Klage einer Lehrerin ab, die die Identität von anonymen Schülern hinter einem Bewertungsportal ermitteln lassen wollte.⁶¹ Der BGH stellte klar, dass die rein wertenden Äußerungen der Schüler zu den Benotungen von der Meinungsfreiheit gedeckt und nicht rechtswidrig waren und somit folglich kein Anspruch auf Offenlegung der Identität bestand.⁶² Dieses Urteil betont implizit, dass, solange keine Rechtsverletzung vorliegt, Anonymität geschützt bleibt.

In einem jüngeren Fall entschied der BGH 2022, dass soziale Netzwerke keine Klarnamenpflicht gegenüber ihren Nutzern durchsetzen durften, solange das Telemediengesetz (a.F.) Anonymität erlaubte.⁶³ Hier wurde deutlich, dass der Gesetzgeber selbst großen Wert auf das anonyme Online-Kommunizieren legt. Diese Entscheidung stärkt das Vertrauen der Nutzer, dass ihre Daten nicht ohne Weiteres preisgegeben werden. Gleichwohl hat der BGH bereits früher anerkannt, dass bei Vorliegen eindeutiger Rechtsverletzungen die Identitätsfeststellung gerechtfertigt sein kann. So billigte er Auskunftsansprüche in Fällen von geistigem Eigentumsdiebstahl oder Kreditwürdigkeitsverletzungen, soweit sie gesetzlich vorgesehen und verhältnismäßig sind.⁶⁴

Auf oberster Ebene zeigen auch höchstrichterliche Entscheidungen aus dem Zivil- und Verwaltungsrecht eine Tendenz, Auskünfte restriktiv zu handhaben – im Zweifel zugunsten der Meinungsfreiheit, solange kein eindeutiger Rechtsbruch vorliegt.

Final wegweisend ist das BVerfG-Urteil zur Bestandsdatenauskunft II.⁶⁵ Das Gericht befand, dass damalige Vorschriften zur Bestandsdatenabfrage teilweise unverhältnismäßig waren, weil es an effektiven Begrenzungen und unabhängiger Kontrolle fehlte. Diese Maßstäbe dürfte das BVerfG auch an ein künftiges GgdG anlegen.

2. Maßnahmen gegen Online-Hass und -Hetze

Im Bereich der Bekämpfung extremistischer Online-Inhalte gibt es bereits Rechtsprechung, die Parallelen zur Intention des GgdG aufweist. So hat etwa das BVerfG in einem Urteil 2021 bestimmte Vorschriften des NetzDG-Erweiterungsgesetzes vorläufig suspendiert, weil sie vorsahen, dass soziale Netzwerke bestimmte strafbare Inhalte wie Volksverhetzung, Bedrohung etc. *automatisch* dem BKA melden und dabei auch Bestandsdaten (IP-Adresse, Portnummer) übermitteln sollten – *ohne* dass hierzu ein Richterbeschluss erforderlich war.⁶⁶ Das BVerfG sah in diesem automatisierten Meldeverfahren wahrscheinlich einen Verstoß gegen das Recht auf informationelle Selbstbestimmung, weil hier Datenweitergaben an die Strafverfolgung erfolgten, ohne dass der Einzelfall von einer unabhängigen Stelle geprüft wurde. Auch wenn dieser Fall einen staatlich initiierten Informationsfluss an Behörden betraf, unterstreicht er, dass Grundrechtsschutz online sehr ernst genommen wird. Jede Form von Identifizierung oder Sanktionierung muss rechtsstaatlich eingeeht werden.

Ein weiteres potenziell relevantes Feld sind gerichtliche Einstweilige Verfügungen gegen Plattformen, problematisch vor allem bei Accountsperrern oder Inhaltsentfernungen aus privater Initiative. Beispielsweise erstritten einige Nutzer in jüngerer Zeit vor Zivilgerichten die Wiederherstellung ihrer gelöschten Social-Media-Beiträge mit dem Argument, die Plattform habe bei der Löschung ihr

⁶¹ BGH, Urt. v. 23.6.2009 – VI ZR 196/08.

⁶² Schulte, KriPoZ (JuP) 2024, 3 (13).

⁶³ BGH, Urt. v. 27.1.2022 – III ZR 3/21; BGH, Urt. v. 27.1.2022 – III ZR 4/21.

⁶⁴ BGH, Urt. v. 27.1.2022 – III ZR 3/21 (Klarnamenpflicht, Facebook, Ziff. 49).

⁶⁵ BVerfGE 155, 119 = NJW 2020, 2699; Schulte, KriPoZ (JuP) 2024, 3 (14).

⁶⁶ BVerfG, Beschl. v. 19.12.2021 – 1 BvR 1073/20, Rn. 27.

Recht auf freie Meinungsäußerung nicht angemessen berücksichtigt.⁶⁷ Solche Verfahren zeigen eine Bereitschaft der Gerichte, auch die Position der Äußernden zu schützen, und deuten an, dass eine vom Staat veranlasste Accountstilllegung ebenfalls einer strengen Verhältnismäßigkeitskontrolle unterzogen würde.

Im Bereich der Unterlassungsverfügungen gegen Täter selbst, wenn diese bekannt sind, haben die Gerichte mitunter sehr rigide Maßnahmen gebilligt. So bestätigte der BGH in einem Fall, dass bei fortgesetzten Persönlichkeitsverletzungen im Internet notfalls auch Ordnungshaft gegen den Täter verhängt werden kann, um das Unterlassungsgebot durchzusetzen.⁶⁸ Diese Entschlossenheit, den Opferschutz durchzusetzen, stützt im Prinzip die Stoßrichtung des GdG, wenn auch die Accountsperrung als milderes Mittel vor einer Haft sanktionieren würde.

V. Schluss

Zusammenfassend würdigt die Fachliteratur⁶⁹ den BMJ-Entwurf als Schritt in die richtige Richtung, insbesondere was die dringend benötigte Verbesserung der Auskunftsmöglichkeiten angeht. Zugleich werden präzisere Grenzziehungen verlangt, um Missbrauch vorzubeugen und verfassungsgerichtlicher Kontrolle standzuhalten. Die Balance zwischen effektivem Schutz und Freiheit der Kommunikation bleibt der Leitfaden der Kritik. Der Gesetzgeber soll die Waage halten, damit weder Opfer noch (potenziell zu Unrecht beschuldigte) Nutzer unverhältnismäßig benachteiligt werden. In der Summe deutet vieles darauf hin, dass das GdG in modifizierter Form verabschiedet werden könnte, begleitet von flankierenden Maßnahmen und möglicherweise evaluiert, um etwaige Fehlentwicklungen zu korrigieren.

Der Diskussionsentwurf für ein Gesetz gegen digitale Gewalt reagiert auf reale Schutzdefizite im Internet. Indem er den Opfern von Persönlichkeitsrechtsverletzungen, etwa von Hasskommentaren, Drohungen oder der Verbreitung intimer Bilder, schnellere und direktere Rechtsbehelfe an die Hand gibt, schließt er eine Lücke zwischen Strafrecht und Zivilrecht. Besonders die Verknüpfung von erweitertem Auskunftsanspruch und Accountsperrung stellt ein innovatives Instrumentarium dar, um digitalen Übergriffen effektiver zu begegnen. In der Schnittstelle zu § 201a StGB zeigt sich exemplarisch der Mehrwert. Wo die strafrechtliche Verfolgung unbefugter Bildaufnahmen oft zu spät oder gar nicht greift, könnte das neue Gesetz dem Opfer ermöglichen, rasch die Identität des anonymen Verbreiters zu erfahren und dessen Treiben durch Sperrung zu stoppen.

Gleichzeitig darf die Begeisterung über neue Befugnisse nicht die verfassungsrechtlichen Leitplanken übersehen. Der Bestimmtheitsgrundsatz verlangt klare Kriterien, wann welche Maßnahme zulasten eines Nutzers ergehen darf. Hier wird der Gesetzgeber im weiteren Gesetzgebungsverfahren nachjustieren müssen, um unnötige Unschärfen, etwa beim Gewaltbegriff oder der Abgrenzung relevanter Rechtsverletzungen, zu beseitigen. Die Kommunikationsgrundrechte fordern zudem, dass Auskunft und Sperre stets ultima ratio bleiben. Eingriffe in Anonymität und Meinungsfreiheit bedürfen einer strengen Verhältnismäßigkeitsprüfung im Einzelfall. Die vorgesehenen Richtervorbehalte, Anhörungsmöglichkeiten und verfahrensrechtlichen Sicherungen bilden hierfür eine gute Grundlage, müssen aber in der Praxis mit Bedacht angewandt werden.

In der Abwägung ist zu berücksichtigen, dass ein unregulierter Raum der digitalen Gewalt seinerseits Grundrechte gefährdet – nämlich die der Opfer und der Allgemeinheit auf einen freien, von Angst

⁶⁷ OLG Oldenburg, Urt. v. 1.7.2019 – 13 W 16/19.

⁶⁸ BGH, Urt. v. 12.10.2021 – VI ZR 488/19.

⁶⁹ Wiedemann, ZUM 2025, 292 (297, 298); Schäfer, ZUM 2023, 734 (740); Valerius, ZRP 2023, 142 (144); Maurer, NJOZ 2024, 257 (263).

und Einschüchterung unbeeinflussten Diskurs. Das Gesetz gegen digitale Gewalt versucht genau diesen Ausgleich. Es wahrt die anonyme Meinungsäußerung dort, wo sie rechtmäßig erfolgt, und greift dort ein, wo Rechtsbruch erfolgt und der demokratische Austausch zu kippen droht. Sollte der Entwurf, gegebenenfalls nach weiterer Überarbeitung, Gesetz werden, wird seine Umsetzung durch die Gerichte kritisch zu begleiten sein. Mögliche verfassungsgerichtliche Verfahren, etwa von gesperrten Nutzern, sind am Horizont, könnten dem Gesetz aber auch den nötigen Feinschliff geben.

Abschließend lässt sich feststellen, dass die Schnittstellen zu bestehenden Normen wie § 201a StGB und zum europäischen Regime (DSA) grundsätzlich kompatibel sind, sofern das Gesetz gegen digitale Gewalt als spezialgesetzlicher Riegel in dem eng umrissenen Bereich schwerer Persönlichkeitsverletzungen verstanden wird. Es ersetzt kein Strafverfahren, aber es ergänzt den Rechtsschutz durch schnelle, zivilrechtliche Abwehr- und Informationsmittel. Damit setzt es ein wichtiges Signal, dass es rechtsfreie Räume – auch im Internet – nicht geben darf. Für eine endgültige Bewertung wird die konkrete Ausgestaltung im Gesetzgebungsverfahren maßgeblich sein. Der bisherige Diskussionsentwurf zeigt Potenzial, benötigt aber teils präzisere Justierung, um als verfassungskonforme und praxistaugliche Antwort auf digitale Gewalt zu dienen.