Diskussionsentwurf

des Bundesministeriums der Justiz

Entwurf eines Gesetzes zur Stärkung der privaten Rechtsverfolgung im Internet

A. Problem und Ziel

Wer eine Verletzung seiner Rechte erfährt, muss sich selbst effektiv vor Gericht dagegen wehren können. Das gilt auch bei Rechtsverletzungen im digitalen Raum. Das gegenwärtige Recht wird diesem Anspruch nicht hinreichend gerecht. Insbesondere Betroffene von Persönlichkeitsrechtsverletzungen im digitalen Raum (sog. digitale Gewalt) haben zu oft nur unzureichende Möglichkeiten, ihre Rechte selbst durchzusetzen. Häufig scheitert die Durchsetzung ihrer Rechte schon daran, dass es nicht gelingt, zügig und mit vertretbarem Aufwand Auskunft über die Identität des Verfassers rechtswidriger Inhalte zu erlangen. Auch fehlt es im gegenwärtigen Recht an einem effektiven Instrument, bei schwerwiegenden Persönlichkeitsrechtsverletzungen weiteren Rechtsverstößen vorzubeugen.

Die öffentliche Aufgabe, einen respektvollen Umgang im digitalen Raum sicherzustellen, steht in einem verfassungsrechtlichen Spannungsverhältnis. Einerseits ist der offene Austausch im Internet und die Freiheit, Meinungen – auch anonym – zu äußern, für unser demokratisches Gemeinwesen von grundlegender Bedeutung. Andererseits ist es notwendig, dass sich jeder Einzelne gegen rechtswidrige und ihn betreffende Inhalte wie zum Beispiel Beleidigungen und Verleumdungen im Internet effektiv zur Wehr setzen kann. Das Recht muss deshalb bei der Kommunikation im Internet die unterschiedlichen Grundrechtspositionen in Ausgleich bringen: Zu berücksichtigen sind die Meinungsfreiheit des sich Äußernden, das allgemeine Persönlichkeitsrecht der vom jeweiligen Inhalt betroffenen Person und die unternehmerische Freiheit des Diensteanbieters bzw. des Anbieters eines Internetzugangsdienstes. Richtervorbehalte ermöglichen, dass die verschiedenen Grundrechtspositionen in jedem Einzelfall berücksichtigt werden.

Die Bekämpfung digitaler Gewalt erfordert ein ganzheitliches Vorgehen. Dazu gehören eine effektive strafrechtliche Verfolgung und Ahndung von digital begangenen Straftaten, um Täter angemessen zu bestrafen und künftige Täter abzuschrecken. Daneben verpflichtet der Digital Services Act (DSA) soziale Netzwerke, gegen Hassrede vorzugehen und regelt die behördliche Aufsicht und das Compliance-Verfahren. Auf der Ebene des Zivilrechts müssen die Betroffenen von Beleidigungen, Bedrohungen und sonstigen Formen digitaler Gewalt in die Lage versetzt werden, selbst effektiv gegen solche Beeinträchtigungen vorzugehen. Das gegenwärtige Recht wird diesem Anspruch nicht hinreichend gerecht.

Ziel des vorliegenden Entwurfs ist es, die individuelle Rechtsdurchsetzung zu stärken.

An den Spielregeln des demokratischen Diskurses wird der Entwurf nichts ändern: Was heute geäußert werden darf, darf auch künftig geäußert werden. Auch die grundsätzliche Freiheit zur anonymen Meinungsäußerung bleibt gewahrt. Verfahrensmäßige Absicherungen – wie insbesondere Richtervorbehalte – dienen dazu, dass die neuen Rechtsschutzmöglichkeiten nicht eingesetzt werden können, um den offenen Diskurs im Netz zu beschränken.

Dieser Entwurf steht im Kontext der Erreichung der Ziele der Resolution der Generalversammlung der Vereinten Nationen vom 25. September 2015 „Transformation unserer Welt:

die UN-Agenda 2030 für nachhaltige Entwicklung“. Der Entwurf trägt insbesondere zur Erreichung des Nachhaltigkeitsziels 16 bei, den gleichberechtigten Zugang aller zur Justiz zu gewährleisten, leistungsfähige Institutionen auf allen Ebenen aufzubauen und die Grundfreiheiten zu schützen.

B. Lösung

Das Gesetz gegen digitale Gewalt (GgdG) soll Schutzlücken im Auskunftsverfahren gemäß § 21 Absatz 2 bis 4 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes schließen und einzelne Rechte im Betroffenen-Plattform-Verhältnis in einem neuen Stammgesetz bündeln. Personen, deren Persönlichkeitsrechte im digitalen Raum durch bestimmte strafwürdige Verhaltensweisen verletzt sind, sollen von Diensteanbietern und Anbietern von Internetzugangsdiensten einfacher und weitergehend Auskunft über die Identität der rechtswidrig handelnden Nutzer erhalten können als dies bisher der Fall war. Zudem soll das Auskunftsverfahren durch eine frühestmögliche gerichtliche Anordnung zur Speicherung der einschlägigen Daten bei den Diensteanbietern und den Anbietern von Internetzugangsdiensten einem Datenverlust vorbeugen. Mit der Normierung richterlich angeordneter Sperrungen von Nutzerkonten soll ein neues Instrument geschaffen werden, um schwerwiegende Rechtsverletzungen zu verhindern oder abzustellen. Dadurch können auch künftige Rechtsverletzungen unterbunden werden, selbst wenn der Verletzer nicht identifiziert werden kann. Solche Sperrungen verhindern, dass über einzelne Accounts eines Internetdienstes fortwährend schwerwiegende Rechtsverletzungen begangen werden. Soziale Netzwerke, die keinen Sitz in einem Mitgliedstaat der Europäischen Union haben, sollen auch nach Inkrafttreten des DSA über einen inländischen Zustellungsbevollmächtigten verfügen.

C. Alternativen

Keine.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Keine.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Für Bürgerinnen und Bürger entsteht ein geringfügiger laufender Erfüllungsaufwand in Folge zusätzlicher Beantragungen von Auskunftsverfahren und richterlich angeordneten Accountsperren.

E.2 Erfüllungsaufwand für die Wirtschaft

Für die Wirtschaft erhöht sich der jährliche Erfüllungsaufwand in Höhe von rund 53 000 Euro, die gänzlich auf Bürokratiekosten aus Informationspflichten entfallen. Diese Belastung stellt ein „In“ im Sinne der One in, one out-Regelung der Bundesregierung dar. Die Kompensation kann im Wege der Entlastungen durch das vierte Gesetz zur Entlastung der Bürgerinnen und Bürger, der Wirtschaft sowie der Verwaltung von Bürokratie (BEG IV) erfolgen.

E.3 Erfüllungsaufwand der Verwaltung

Der Verwaltung entsteht kein Erfüllungsaufwand.

F. Weitere Kosten

Aufgrund zusätzlicher richterlicher Anordnungen zur Durchsetzung von Auskunftsverfahren und Accountsperren sowie daraus folgenden Beschwerdeverfahren nach dem GgdG entstehen den Ländern jährliche Mehrkosten im justiziellen Kernbereich in Höhe von rund 194 000 Euro.

Referentenentwurf des Bundesministeriums der Justiz

Entwurf eines Gesetzes zur Stärkung der privaten Rechtsverfolgung im Internet

Vom ...

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Gesetz gegen digitale Gewalt

(GgdG)

§ 1

Begriffsbestimmungen

(1) Eine Rechtsverletzung im Sinne dieses Gesetzes liegt vor, wenn eine Person durch Nutzung von Diensten eines Diensteanbieters (Nutzer) eine Tat begeht, die den Tatbestand der folgenden Vorschriften erfüllt und nicht gerechtfertigt ist:

1. der §§ 111, 126, 126a, 130, 130a, 131, 140, 166, 176a, 176b, 184 bis 184c, 184k, 185 bis 189, 192a, 201, 201a, 238 oder 241 des Strafgesetzbuches,

2. des § 33 des Gesetzes betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie oder

3. des § 42 des Bundesdatenschutzgesetzes.

(2) Diensteanbieter im Sinne dieses Gesetzes sind: Anbieter von

1. Online-Plattformen im Sinne des Artikels 3 Buchstabe i der 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) (ABl. L 277 vom 27.10.2022, S. 1; L 30 vom 1.12.2023, S. 17), die zuletzt durch die Delegierte Verordnung (EU) 2024/436 (ABl. L, 2024/436, 2.2.2024) geändert worden ist, in der jeweils geltenden Fassung, oder

2. Hosting-Dienste im Sinne des Artikel 3 Buchstabe g Ziffer iii der Verordnung (EU) 2022/2065, die es ihren Nutzern ermöglichen, Websites im Internet zu veröffentlichen und zugänglich zu machen (Web-Hosting-Dienste), oder

3. Hosting-Dienste im Sinne des Artikel 3 Buchstabe g Ziffer iii der Verordnung (EU) 2022/2065, die es ihren Nutzern ermöglichen, Dateien im Internet zu speichern, zu teilen und darauf zuzugreifen (Cloud-Hosting-Dienste).

(3) Internetzugangsdienste im Sinne dieses Gesetzes sind Dienste im Sinne des Artikels 2 Absatz 2 Nummer 2 der Verordnung (EU) 2015/2120 des Europäischen Parlaments und des Rates vom 25. November 2015 über Maßnahmen zum Zugang zum offenen

Internet und zu Endkundenentgelten für regulierte intra-EU-Kommunikation sowie zur Änderung der Richtlinie 2002/22/EG und der Verordnung (EU) Nr. 531/2012 (ABl. L 310 vom 26.11.2015, S. 1), die zuletzt durch die Verordnung (EU) 2024/1309 (ABl. L, 2024/1309, 8.5.2024) geändert worden ist.

(4) Soziale Netzwerke im Sinne dieses Gesetzes sind Online-Plattformen, deren Hauptzweck oder wesentliche Funktion darin besteht, dass ihre Nutzer miteinander kommunizieren und interagieren, indem sie Inhalte mit anderen Nutzern teilen oder der Öffentlichkeit zugänglich machen.

(5) Inhaltemoderation im Sinne dieses Gesetzes ist die Moderation von Inhalten im Sinne des Artikels 3 Buchstabe t der Verordnung (EU) 2022/2065.

§ 2

Auskunft über Daten

(1) Diensteanbieter und Anbieter von Internetzugangsdiensten, deren Dienste zur Begehung einer Rechtsverletzung genutzt wurden, dürfen Auskunft über Daten erteilen, soweit dies zur Durchsetzung von zivilrechtlichen Ansprüchen wegen einer Rechtsverletzung erforderlich ist. In diesem Umfang sind sie gegenüber dem von der Rechtsverletzung Betroffenen zur Auskunft verpflichtet. Für die Erteilung der Auskunft ist eine vorherige richterliche Anordnung über die Zulässigkeit der Auskunftserteilung auf Antrag des Betroffenen erforderlich.

(2) Die nach Absatz 1 Satz 1 erforderlichen Daten umfassen

1. die folgenden Daten, die bei dem im Antrag benannten Diensteanbieter hinterlegt oder gespeichert sind:

   a) die Personalien des Nutzers, wie den Namen, das Geburtsdatum, die Anschrift, die E-Mail-Adresse und die Telefonnummer,

   b) die gespeicherte Internetprotokoll-Adresse einschließlich der Portnummer, die bei der Rechtsverletzung verwendet wurde, und den Zeitpunkt des Zugriffs unter Angabe der zugrunde liegenden Zeitzone und

   c) die gespeicherte Internetprotokoll-Adresse einschließlich der Portnummer, die vor der Zustellung der gerichtlichen Anordnung bei Nutzung des betreffenden Nutzerkontos zuletzt verwendet wurde, und den Zeitpunkt des letzten Zugriffs unter Angabe der zugrunde liegenden Zeitzone,

2. die Personalien des Nutzers, die bei einem Anbieter eines Internetzugangsdienstes hinterlegt sind, wie den Namen, das Geburtsdatum, die Anschrift, die E-Mail-Adresse und die Telefonnummer.

(3) Der Antragsteller hat in seinem Antrag an das Gericht glaubhaft zu machen, dass die Voraussetzungen des Absatz 1 Satz 1 vorliegen. Dazu hat er die Tatsachen darzulegen, aus denen sich ergibt, dass ein ihm unbekannter Nutzer eine Rechtsverletzung begangen hat und dass er gegen diesen Nutzer zivilrechtliche Ansprüche geltend macht.

(4) Das Gericht entscheidet in einem Verfahren über die Auskunftspflicht des im Antrag benannten Diensteanbieters und des Anbieters eines Internetzugangsdienstes. Sofern der Antrag nicht ausdrücklich auf die Anordnung der Zulässigkeit der Auskunftserteilung nach Absatz 1 Satz 1 beschränkt ist, entscheidet das Gericht zugleich über die Verpflichtung zur Auskunftserteilung nach Absatz 1 Satz 2.

(5) Durch Absatz 1 wird das Grundrecht des Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) eingeschränkt.

§ 3

Sicherungsanordnungen

(1) Sobald ein Verfahren nach § 2 gegen einen Diensteanbieter anhängig ist und zureichende tatsächliche Anhaltspunkte für eine Rechtsverletzung vorliegen, ordnet das zuständige Gericht gegenüber diesem Anbieter unverzüglich an, dass die vorhandenen Daten des Nutzers im Sinne des § 2 Absatz 2 Nummer 1, der die mögliche Rechtsverletzung begangen hat, nicht gelöscht werden und eine Kopie des angegriffenen rechtsverletzenden Inhalts erstellt wird.

(2) Neben der Anordnung nach Absatz 1 ordnet das Gericht außerdem an, dass der Diensteanbieter die Daten des Nutzers und die Kopie des rechtsverletzenden Inhalts dem Gericht unverzüglich in Textform mitteilt. Eine Mitteilung der nach Satz 1 vom Diensteanbieter erhaltenen Daten an den Antragsteller ist nicht statthaft. Insoweit ist eine Akteneinsicht des Antragstellers ebenfalls ausgeschlossen.

(3) Nach Eingang der Daten nach Absatz 2 Satz 1 ordnet das Gericht gegenüber dem von dem Auskunftsersuchen betroffenen Anbieter eines Internetzugangsdienstes unverzüglich an, dass die bei diesem Anbieter vorhandenen Daten des Nutzers im Sinne von § 2 Absatz 2 Nummer 2 nicht gelöscht werden.

(4) Daten dürfen von dem Diensteanbieter und dem Anbieter eines Internetzugangsdienstes, die vom Auskunftsersuchen betroffen sind, zur Erfüllung der Pflichten aus der Sicherungsanordnung verarbeitet werden. Die gesicherten Daten dürfen zum Zweck der Strafverfolgung auch an die Strafverfolgungsbehörden übermittelt werden. Für andere Zwecke dürfen diese Daten nicht verwendet werden.

(5) Der Antrag auf Erteilung einer Auskunft gemäß § 2 Absatz 1 Satz 3 gilt zugleich als Antrag auf Erlass von Sicherungsanordnungen nach den Absätzen 1 und 3.

(6) Sobald das Auskunftsverfahren rechtskräftig abgeschlossen ist, teilt das Gericht dies dem jeweiligen Diensteanbieter und dem jeweiligen Anbieter des Internetzugangsdienstes mit. Wenn die Anbieter zur Auskunft verpflichtet werden, haben sie die Daten und die Kopie des rechtsverletzenden Inhalts nach Erteilung der Auskunft irreversibel zu löschen oder die irreversible Löschung sicherzustellen. Wenn die Anbieter nicht zur Auskunft verpflichtet werden, haben sie die Daten und die Kopie des rechtsverletzenden Inhalts bereits nach der Mitteilung nach Satz 1 irreversibel zu löschen oder die irreversible Löschung sicherzustellen. Sonstige Befugnisse oder Pflichten, die Daten zu speichern, bleiben unberührt.

(7) Durch die Absätze 1 bis 4 wird das Grundrecht des Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) eingeschränkt.

§ 4

Anspruch auf richterlich angeordnete Sperrung des Nutzerkontos

(1) Begeht ein Nutzer in einem sozialen Netzwerk eine Rechtsverletzung, die den Betroffenen in seinem Persönlichkeitsrecht schwerwiegend beeinträchtigt, so kann der Betroffene von dem Anbieter des sozialen Netzwerks verlangen, dass dieser alle bekannten

Konten des Nutzers, der die Rechtsverletzung begangen hat, für einen angemessenen Zeitraum sperrt. Die Sperrung muss erforderlich sein, um künftige Rechtsverletzungen zu verhindern.

(2) Ein Nutzerkonto ist gesperrt, wenn der Nutzer keine Inhalte veröffentlichen, kommentieren und teilen kann. Die passive Nutzung des Nutzerkontos im Lesemodus soll weiterhin möglich sein. Die Sperrung bezieht sich auch auf künftige Nutzerkonten, die der Nutzer innerhalb des in Absatz 1 Satz 1 genannten Zeitraums eröffnet.

(3) Die Sperrung ist in der Regel erforderlich, wenn

1. der Nutzer die Abgabe einer strafbewehrten Unterlassungserklärung, die die Rechtsverletzung nach Absatz 1 Satz 1 betrifft, verweigert hat,

2. der Nutzer gegen eine von ihm unterzeichnete strafbewehrte Unterlassungserklärung, die die Rechtsverletzung nach Absatz 1 Satz 1 betrifft, verstoßen hat oder

3. andere als die in den Nummern 1 und 2 genannten Anhaltspunkte eine weitere Rechtsverletzung befürchten lassen.

Bei der Beurteilung der Erforderlichkeit ist auch zu berücksichtigen, ob das soziale Netzwerk eine mildere Form der Inhaltemoderation anbietet, die geeignet ist, weitere Rechtsverletzungen wirksam zu verhindern.

(4) Für die Sperrung des Nutzerkontos nach Absatz 1 ist eine vorherige gerichtliche Anordnung erforderlich, die von dem von der Rechtsverletzung Betroffenen zu beantragen ist. Das Gericht ordnet mit der Sperrung die Entfernung der rechtsverletzenden Inhalte an. Satz 1 steht der Sperrung eines Nutzerkontos ohne richterliche Anordnung aufgrund der Allgemeinen Geschäftsbedingungen des sozialen Netzwerks oder aufgrund der Verpflichtung aus Artikel 23 Absatz 1 der Verordnung (EU) 2022/2065 nicht entgegen.

§ 5

Verfahren

(1) Für das gerichtliche Verfahren nach diesem Gesetz gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend.

(2) Die Anbieter sind als Beteiligte zu den Verfahren nach den §§ 2 und 4 hinzuzuziehen.

(3) Soweit den Anbietern Dokumente formlos übermittelt werden sollen, kann dies durch E-Mail an die nach Artikel 11 Absatz 1 der Verordnung (EU) 2022/2065 benannte zentrale Kontaktstelle der Anbieter erfolgen.

(4) Gegen die Endentscheidung des Landgerichts in Verfahren nach diesem Gesetz ist die Beschwerde statthaft. Die Beschwerde ist innerhalb einer Frist von zwei Wochen einzulegen.

§ 6

Beteiligung des Nutzers

(1) Der Nutzer, dem eine Rechtsverletzung vorgeworfen wird, ist als Beteiligter zu den Verfahren nach den §§ 2 und 4 hinzuziehen, sofern er dem Gericht bekannt ist.

(2) Ist der Nutzer dem Gericht nicht bekannt, soll es die Anbieter verpflichten, den Nutzer über die Einleitung des Verfahrens zu unterrichten und ihm Gelegenheit zur Stellungnahme bei Gericht zu geben. Die Anbieter haben die Einreichung der Stellungnahme anonym oder unter einem Pseudonym zu ermöglichen. Der Nutzer ist auf Antrag an dem Verfahren zu beteiligen. Die Anbieter haben dem Gericht zu versichern, dass die Unterrichtung des Nutzers erfolgt ist.

§ 7

Zivilgesellschaftliche Organisationen

In Verfahren nach diesem Gesetz können sich die Beteiligten auch durch zivilgesellschaftliche Organisationen als Bevollmächtigte vertreten lassen, wenn

1. es zu den satzungsmäßigen Aufgaben der zivilgesellschaftlichen Organisation gehört, Interessen von Internetnutzern durch unentgeltliche Aufklärung und Beratung wahrzunehmen,

2. die Vertretung nicht im Zusammenhang mit einer entgeltlichen Tätigkeit steht und

3. die zivilgesellschaftliche Organisation durch eine Person mit Befähigung zum Richteramt handelt.

§ 8

Zuständigkeit; Verordnungsermächtigung

(1) Für Anträge, die nach diesem Gesetz gestellt werden, ist das Landgericht ausschließlich zuständig. Örtlich zuständig ist das Gericht, in dessen Bezirk der Antragsteller seinen Wohnsitz, seinen Sitz oder eine Niederlassung hat.

(2) Für Streitigkeiten über Ansprüche aus Rechtsverletzungen, für die zuvor ein Auskunftsverfahren nach § 2 durchgeführt wurde, ist auch das Gericht, welches über diesen Auskunftsanspruch entschieden hat, sachlich und örtlich zuständig.

(3) Die Landesregierungen werden ermächtigt, durch Rechtsverordnung die Auskunftsverfahren einem Landgericht für die Bezirke mehrerer Landgerichte zuzuweisen. Die Landesregierungen können die Ermächtigung durch Rechtsverordnung auf die Landesjustizverwaltungen übertragen.

§ 9

Inländischer Zustellungsbevollmächtigter

(1) Anbieter sozialer Netzwerke, bei denen kein anderer Mitgliedstaat der Europäischen Union Sitzland ist oder als Sitzland gilt, haben im Inland einen

Zustellungsbevollmächtigten spätestens mit Anbieten des Dienstes zu benennen und in ihrem Angebot in leicht erkennbarer und unmittelbar erreichbarer Weise auf ihn aufmerksam zu machen.

(2) An den Zustellungsbevollmächtigten können Zustellungen in gerichtlichen Verfahren bewirkt werden wegen

1. Ansprüchen aus Rechtsverletzungen oder

2. Ansprüchen aus der unbegründeten Annahme von Rechtsverletzungen, insbesondere in Fällen, in denen die Wiederherstellung entfernter oder gesperrter Inhalte oder die Entsperrung gesperrter Nutzerkonten begehrt wird.

Satz 1 gilt auch für die Zustellung von Schriftstücken, die solche Verfahren einleiten oder vorbereiten, und für zivilrechtliche Anspruchsschreiben.

(3) Ein Gericht kann gegenüber Anbietern sozialer Netzwerke, die einen Sitz in einem Mitgliedsstaat der Europäischen Union haben, in Verfahren, die Ansprüche aus Rechtsverletzungen zum Gegenstand haben, anordnen, dass sie innerhalb einer angemessenen Frist für ein anhängiges Gerichtsverfahren einen Zustellungsbevollmächtigten im Inland benennen.

§ 10

Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig entgegen § 9 Absatz 1 einen Zustellungsbevollmächtigten nicht oder nicht rechtzeitig benennt.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfhunderttausend Euro geahndet werden. § 30 Absatz 2 Satz 3 des Gesetzes über Ordnungswidrigkeiten ist anzuwenden.

(3) Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten ist das Bundesamt für Justiz.

§ 11

Übergangsvorschrift

Die Zuständigkeit des Bundesamts für Justiz nach der bis … [einsetzen: Datum des Tages vor Außerkrafttreten nach Artikel 4 Satz 2 dieses Gesetzes] geltenden Fassung des Netzwerkdurchsetzungsgesetzes vom 1. September 2017 (BGBl. I S. 3352), das zuletzt durch Artikel 29 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist, für Bußgeldverfahren bleibt bis zum Abschluss der Verfahren bestehen.

Artikel 2

Änderung des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes

§ 21 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982; 2022 I S. 1045), das zuletzt durch Artikel 8 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist, wird wie folgt geändert:

1. In Absatz 1 wird die Absatzbezeichnung „(1)“ gestrichen.

2. Die Absätze 2 bis 4 werden aufgehoben.

Artikel 3

Änderung des Urheberrechts-Diensteanbieter-Gesetzes

§ 20 des Urheberrechts-Diensteanbieter-Gesetzes vom 31. Mai 2021 (BGBl. I S. 1204, 1215), das durch Artikel 22 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist, wird wie folgt gefasst:

„§ 20

Inländischer Zustellungsbevollmächtigter

Für die Verpflichtung des Diensteanbieters zur Bestellung eines inländischen Zustellungsbevollmächtigten für das gerichtliche Verfahren ist § 9 des Gesetzes gegen digitale Gewalt entsprechend anzuwenden.“

Artikel 4

Inkrafttreten, Außerkrafttreten

Dieses Gesetz tritt am … [einsetzen: Datum des ersten Tages des auf die Verkündung folgenden Quartals] in Kraft. Gleichzeitig tritt das Netzwerkdurchsetzungsgesetz vom 1. September 2017 (BGBl. I S. 3352), das zuletzt durch Artikel 29 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist, außer Kraft.

Begründung

A. Allgemeiner Teil

I. Zielsetzung und Notwendigkeit der Regelungen

Ein relevanter Teil der öffentlichen, politischen und privaten Kommunikation findet im virtuellen Raum statt. Insbesondere in sozialen Netzwerken kommt es immer wieder zu aggressiven, verletzenden und hasserfüllten Äußerungen, die jede und jeden aufgrund der Meinung, Hautfarbe oder Herkunft, der Religion, des Geschlechts oder der sexuellen Orientierung diffamieren. Hasskriminalität und andere strafbare Inhalte, die nicht effektiv bekämpft und verfolgt werden können, bergen eine große Gefahr für das friedliche Zusammenleben in einer freien, offenen und demokratischen Gesellschaft. In diesem Umfeld wagen es viele Nutzerinnen und Nutzer aus Sorge vor derartigen Angriffen nicht, ihre Meinung frei zu äußern. Digitale Kommunikationsforen weisen dabei ein deutlich höheres Verletzungspotenzial auf, da Inhalte innerhalb kürzester Zeit einem unvorhersehbar großen Empfängerkreis zugänglich gemacht werden können und im Netz permanent abrufbar fortleben. Außerdem können Rechtsverletzer im virtuellen Raum weitgehend anonym agieren. Zum Schutz der Meinungsfreiheit im Netz müssen Instrumente, die den Betroffenen an die Hand gegeben werden, um sich gegen solche Verletzungen zu wehren, hohe tatbestandliche Hürden und verfahrensmäßige Absicherungen (z. B. einen Richtervorbehalt) vorsehen.

Die Bekämpfung digitaler Gewalt erfordert ein ganzheitliches Vorgehen. Dazu gehören eine effektive strafrechtliche Verfolgung und Ahndung von digital begangenen Straftaten, um Täter angemessen zu bestrafen und künftige Täter abzuschrecken. Daneben verpflichtet der Digital Services Act (DSA) soziale Netzwerke gegen Hassrede vorzugehen und regelt die behördliche Aufsicht und das Compliance-Verfahren. Darüber hinaus müssen Betroffene von Beleidigungen, Bedrohungen und sonstigen Formen digitaler Gewalt in die Lage versetzt werden, selbst auf zivilrechtlichem Wege effektiv gegen solche Verletzungen vorgehen zu können.

Ziel des vorliegenden Entwurfs ist es, die individuelle Rechtsdurchsetzung zu stärken.

An den Spielregeln des demokratischen Diskurses wird der Entwurf nichts ändern: Was heute geäußert werden darf, darf auch künftig geäußert werden. Auch die grundsätzliche Freiheit zur anonymen Meinungsäußerung bleibt gewahrt. Verfahrensmäßige Absicherungen – wie insbesondere Richtervorbehalte – dienen dazu, dass die neuen Rechtsschutzmöglichkeiten nicht eingesetzt werden können, um den offenen Diskurs im Netz zu beschränken.

Dieser Entwurf steht im Kontext der Erreichung der Ziele der Resolution der Generalversammlung der Vereinten Nationen vom 25. September 2015 „Transformation unserer Welt: die UN-Agenda 2030 für nachhaltige Entwicklung“. Der Entwurf trägt insbesondere zur Erreichung des Nachhaltigkeitsziels 16 bei, den gleichberechtigten Zugang aller zur Justiz zu gewährleisten, leistungsfähige Institutionen auf allen Ebenen aufzubauen und die Grundfreiheiten zu schützen.

II. Wesentlicher Inhalt des Entwurfs

Das Gesetz gegen digitale Gewalt soll die individuelle Rechtsdurchsetzung stärken. Das private Auskunftsverfahren soll es Betroffenen ermöglichen, Rechtsverletzer im virtuellen Raum effektiv zu identifizieren und damit überhaupt erst eine Basis für eine zivilrechtliche

Verfolgung von Rechtsverletzungen zu schaffen. Zur Vermeidung eines drohenden Datenverlusts gibt das angerufene Gericht dem Diensteanbieter und den Anbietern des Internetzugangsdienstes auf, diejenigen Daten, die für die Auskunftserteilung erforderlich sind, bis zum Abschluss des Auskunftsverfahrens zum Zwecke der Auskunftserteilung zu sichern und nicht zu löschen. Gleiches gilt für eine Kopie der betroffenen rechtswidrigen Inhalte, da deren Löschung durch den Dienst selbst die Anspruchsdurchsetzung häufig erschwert. Mit der Normierung eines Anspruchs des von digitaler Gewalt Betroffenen auf eine richterlich angeordnete Sperrung des Nutzerkontos soll ein neues Instrument zur Bekämpfung digitaler Gewalt geschaffen werden. Damit soll verhindert werden, dass über einzelne Accounts eines Internetdienstes fortwährend schwerwiegende Rechtsverletzungen begangen werden.

Soziale Netzwerke, die keinen Sitz in einem Mitgliedstaat der Europäischen Union haben, sollen auch nach Inkrafttreten des DSA weiter über einen inländischen Zustellungsbevollmächtigten erreichbar sein. Die Regelungen sollen zudem auf vorgerichtliche Schreiben ausgeweitet werden. Soziale Netzwerke mit Sitz in der Europäischen Union sollen in Gerichtsverfahren, die die Geltendmachung von Ansprüchen wegen einer Rechtsverletzung zum Gegenstand haben, durch eine Anordnung des Gerichts für das betreffende Verfahren hierzu verpflichtet werden können.

III. Exekutiver Fußabdruck

[Wird nach der Länder- und Verbändebeteiligung ergänzt.]

IV. Alternativen

Keine.

V. Gesetzgebungskompetenz

Die Gesetzgebungskompetenz des Bundes ergibt sich für die an die Diensteanbieter und Anbietern von Internetzugangsdiensten gerichteten Regelungen in Artikel 1 aus Artikel 73 Absatz 1 Nummer 7 des Grundgesetzes (GG; Telekommunikation) sowie aus Artikel 74 Absatz 1 Nummer 11 (Recht der Wirtschaft) in Verbindung mit Artikel 72 Absatz 2 GG. Eine bundesgesetzliche Regelung zu den Auskunfts- und Kontosperrverpflichtungen der betreffenden Diensteanbieter und Anbietern von Internetzugangsdiensten ist zur Wahrung der Rechts- und Wirtschaftseinheit im gesamtstaatlichen Interesse erforderlich (Artikel 72 Absatz 2 GG), um zugunsten der Betroffenen von digitaler Gewalt bundesweit einheitlich die Möglichkeiten der privaten Rechtsverfolgung gegenüber Rechtsverletzern durch begleitende Auskunfts-, Sicherungs- oder Kontosperrpflichten der Diensteanbieter und Anbietern von Internetzugangsdiensten zu stärken. Begleitende Regelungen zu dem Erfordernis einer gerichtlichen Anordnung von Auskünften, Maßnahmen zur Datensicherung oder einer Nutzerkontensperrung beruhen auf der Gesetzgebungskompetenz des Bundes aus Artikel 74 Absatz 1 Nummer 1 GG (Gerichtsverfassung, gerichtliches Verfahren), begleitende Bußgeldregelungen beruhen auf der Gesetzgebungskompetenz des Bundes aus Artikel 74 Absatz 1 Nummer 1 GG (Strafrecht).

Die Änderung in Artikel 2 beruht - wie die zu ändernde Regelung - ebenfalls auf der Gesetzgebungskompetenz des Bundes aus Artikel 74 Absatz 1 Nummer 11 GG (Recht der Wirtschaft) in Verbindung mit Artikel 72 Absatz 2 GG (vgl. BT-Drs. 19/27441, Seite 31), und die Änderung in Artikel 3 - wie die zu ändernde Regelung - auf der Gesetzgebungskompetenz des Bundes aus Artikel 73 Absatz 1 Nummer 9 GG (Urheberrecht; vgl. BT-Drs. 19/27426, Seite 55).

VI. Vereinbarkeit mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen

Die in dem Entwurf vorgesehenen Regelungen sind mit europäischem Recht vereinbar. Dies gilt insbesondere für die Richtlinie 2000/31/EG (E-Commerce-RL) als auch für den Digital Services Act (DSA).

1. Richtlinie 2000/31/EG (E-Commerce-RL)

Artikel 3 Absatz 2 der E-Commerce-RL normiert das Herkunftslandprinzip und gilt grundsätzlich auch nach Inkrafttreten des DSA fort (Artikel 2 Absatz 3 DSA). Die Vorschrift enthält ein grundsätzliches Verbot für die Mitgliedstaaten, den freien Verkehr von Diensten der Informationsgesellschaft aus einem anderen Mitgliedstaat aus Gründen einzuschränken, die in den sogenannten koordinierten Bereich fallen. Dazu gehören nach Artikel 2 Buchstabe i 2. Spiegelstrich E-Commerce-RL unter anderem die von einem Diensteanbieter zu erfüllenden Anforderungen in Bezug auf die Ausübung der Tätigkeit seines Dienstes.

Dem Herkunftslandprinzip unterfallen allerdings nicht „Anordnungen zum Vorgehen gegen rechtswidrige Inhalte“. Dies ergibt sich aus Erwägungsgrund 38 DSA, der diese ausdrücklich vom Herkunftslandprinzip ausnimmt. Weiterhin statuiert Artikel 6 Absatz 4 DSA, dass nationale Justiz- oder Verwaltungsbehörden von einem Hosting-Diensteanbieter verlangen dürfen, bestimmte Verstöße gegen das Recht des jeweiligen Mitgliedstaats abzustellen oder zu verhindern. Solche einzelfallbezogenen Anordnungen beschränken nicht die Freiheit der Anbieter, ihre Dienste grenzüberschreitend zu erbringen. Diese Einschränkung des Herkunftslandprinzips betrifft auch die Vorschriften, die ein Mitgliedstaat erlässt, um entsprechende Anordnungen zum Vorgehen gegen rechtswidrige Inhalte zu ermöglichen.

Aufgrund dieser Einschränkung sind die Auskunft nach § 2 und die Sperrung des Nutzerkontos nach § 4 nicht am Herkunftslandprinzip zu messen. Die Auskunft ist nach § 2 Absatz 1 Satz 1 zur Durchsetzung von zivilrechtlichen Ansprüchen wegen einer Rechtsverletzung im Sinne von § 1 Absatz 1 dieses Gesetzes erforderlich. Das Auskunftsverfahren ist demnach eine Vorschrift, auf deren Grundlage eine „Anordnung zum Vorgehen gegen rechtswidrige Inhalte“ erlassen werden kann. Der Anspruch auf Sperrung des Nutzerkontos steht ebenfalls unter dem Vorbehalt einer gerichtlichen Anordnung und ermöglicht daher ebenfalls eine konkrete Anordnung zum Vorgehen gegen rechtswidrige Inhalte.

Im Hinblick auf die Pflicht nach § 8, einen inländischen Zustellungsbevollmächtigten zu bestellen, verbietet das Herkunftslandprinzip, dass Diensteanbieter mit einem Sitz in anderen Mitgliedstaaten der Europäischen Union generell dazu verpflichtet werden, einen Zustellungsbevollmächtigten in Deutschland zu benennen (vgl. EuGH, Urteil vom 9. November 2023, C-376/22). Daher wird eine solche Pflicht nur aufgrund einer konkreten richterlichen Anordnung im Rahmen eines anhängigen Gerichtsverfahrens eingeführt. Damit stellt die Anordnung zur Benennung eines Zustellungsbevollmächtigten in § 8 Absatz 3 GgdG ebenfalls eine „Anordnung zum Vorgehen gegen rechtswidrige Inhalte“ dar, die dem Herkunftslandprinzip nicht unterfällt. Im Hinblick auf Diensteanbieter, die keinen Sitz in der Europäischen Union haben, gilt die E-Commerce-RL und damit auch das Herkunftslandprinzip nicht.

2. Richtlinie 2010/13/EU (AVMD-RL)

Von dem Gesetz gegen digitale Gewalt werden auch Videosharingplattform-Dienste erfasst. Dies ist mit der geänderten Richtlinie 2010/13/EU (AVMD-RL) vereinbar. Die AVMD-RL lässt gemäß Artikel 28a Absatz 5 die Regelungen nach Artikel 3 und 6 DSA unberührt (der Verweis auf Artikel 14 E-Commerce-RL ist gemäß Artikel 89 Absatz 2 DSA als Verweis auf Artikel 6 DSA zu lesen).

3. Verordnung (EU) 2022/2065 (DSA)

Die vorgesehenen Regelungen sind auch mit dem DSA vereinbar.

Der DSA sieht bereits eine Reihe von Instrumenten vor, die zur Regulierung der Anbieter von digitalen Diensten angewandt werden können. Die Verantwortlichkeit von Vermittlern und die Frage, ob nationale Maßnahmen möglich sind, bestimmt sich nicht mehr nach Artikel 12 bis 15 der E-Commerce Richtlinie, denn durch das Inkrafttreten des DSA wurden gemäß Artikel 89 Absatz 1 DSA die Artikel 12 bis 15 der E-Commerce Richtlinie gestrichen. Verweise auf diese Artikel gelten nun als Verweise auf Artikel 4 ff. DSA.

Nach Artikel 6 Absatz 1 DSA haften Hosting-Diensteanbieters für die im Nutzerauftrag gespeicherten Informationen nicht, wenn sie keine Kenntnis von der rechtswidrigen Tätigkeit haben oder nach Kenntniserlangung zügig tätig werden. Im Umkehrschluss bedeutet dies, dass Anbieter aber haften können, wenn sie trotz Kenntnis die rechtswidrigen Inhalte nicht löschen. Nach Artikel 6 Absatz 4 DSA bleibt die Möglichkeit unberührt, „dass eine Justiz- oder Verwaltungsbehörde nach dem Rechtssystem eines Mitgliedsstaats vom Anbieter verlangt, eine Zuwiderhandlung abzustellen oder zu verhindern“. Zu beachten ist ferner Erwägungsgrund 46, wonach „diese Richtlinie die Möglichkeit der Mitgliedstaaten unberührt“ lässt, „spezifische Anforderungen vorzuschreiben, die vor der Entfernung oder der Sperrung des Zugangs unverzüglich zu erfüllen sind.“ Dementsprechend eröffnet der Erwägungsgrund 31 den Mitgliedstaaten die Möglichkeit, gegen Vermittlungsdienste Anordnungen zu erlassen, um gegen rechtswidrige Inhalte vorzugehen.

Das in § 4 normierte Verfahren zur Sperrung eines Nutzerkontos kann auf Artikel 6 Absatz 4 DSA gestützt werden, wonach eine Justiz- oder Verwaltungsbehörde nach dem Rechtssystem des Mitgliedsstaats vom Diensteanbieter verlangen kann, eine Zuwiderhandlung abzustellen oder zu verhindern. Das in § 4 normierte Verfahren ist auch mit Artikel 8 DSA vereinbar. Danach wird Vermittlungsdiensten keine allgemeine Verpflichtung auferlegt, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder aktiv nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hindeuten. Einem Gericht eines Mitgliedstaats ist es aus Artikel 8 DSA nicht verwehrt, einem Diensteanbieter aufzugeben, die von ihm gespeicherten Informationen, die den wortgleichen oder sinngleichen Inhalt haben wie Informationen, die zuvor für rechtswidrig erklärt worden sind, zu entfernen oder den Zugang zu ihnen zu sperren (vgl. EuGH, Urteil vom 03.10.2019 – C-18/18 – Glawischnig-Piesczek). Mit einer Sperrung des Nutzerkontos wird gerade keine Überwachungs- oder Nachforschungspflicht eines Diensteanbieters bezüglich bestimmter Inhalte eines Nutzerkontos begründet, sondern derartige an den Diensteanbieter gerichtete Pflichten werden durch den Ausschluss des Inhalte-Verfassers von der Plattform zur Verhinderung der weiteren Verbreitung rechtswidriger Inhalte gerade obsolet. Der Regelungsgehalt von Artikel 8 DSA ist auch nicht insoweit betroffen, als dem Diensteanbieter mit der Sperrung gemäß § 4 Absatz 4 die Verpflichtung auferlegt wird, Umgehungsversuche der Sperrung des Nutzerkontos im Rahmen des für ihn Zumutbaren ebenfalls zu verhindern. Auch eine solche Verpflichtung des Diensteanbieters stellt keine allgemeine Überwachungspflicht im Sinne des Artikels 8 DSA dar.

Artikel 23 DSA gibt Anbietern von Online-Plattformen vor, wie sie die missbräuchliche Verwendung ihrer Dienste verhindern sollen und nennt dabei in Absatz 1 die Aussetzung der Dienste. Artikel 23 Absatz 1 DSA regelt aber nicht die Anordnung einer Sperrung eines Nutzerkontos aufgrund eines zivilrechtlichen Anspruchs. Dem DSA ist ein vollharmonisierender Ansatz, der gerichtlich angeordnete Sperrungen eines Nutzerkontos in einem Verfahren zwischen zwei Privaten ausschlösse, jedenfalls nicht zu entnehmen. Der DSA setzt das Vorliegen von materiellen Grundlagen für Auskunftsansprüche sowie Beseitigungs- und Unterlassungsansprüche in Einzelfällen vielmehr ausdrücklich voraus und lässt die Ausgestaltung nationalen Zivilrechts bezüglich der Beseitigung beziehungsweise der zukünftigen Unterlassung von Rechtsverletzungen unberührt. Dies ergibt sich auch aus Erwägungsgrund 34, wonach "[d]ie zuständigen nationalen Behörden […] solche Anordnungen gegen als rechtswidrig erachtete Inhalte oder Auskunftsanordnungen auf der Grundlage des Unionsrechts oder nationaler Rechtsvorschriften […] erlassen“. Hierfür spricht

auch Erwägungsgrund 25 des DSA, wonach die im DSA festgelegten Haftungsausschlüsse gerichtliche oder behördliche Anordnungen unberührt lassen, die die Abstellung oder Verhinderung einer Zuwiderhandlung verlangen, einschließlich der Entfernung rechtswidriger Inhalte oder der Sperrung des Zugangs zu ihnen.

Auch die Regelung zum inländischen Zustellungsbevollmächtigten, die zwischen sozialen Netzwerken mit Sitz in Drittstaaten und mit Sitz in der EU differenziert, ist mit dem DSA vereinbar. Der DSA enthält zwar Regelungen zu elektronischen Kontaktstellen (Artikel 11 und 12 DSA) sowie gesetzlichen Vertretern (Artikel 13 DSA). Diese Kontaktstellen beziehungsweise gesetzlichen Vertreter stehen allerdings im DSA nicht im Kontext mit der förmlichen Zustellung von Dokumenten. In Erwägungsgrund 42 heißt es ausdrücklich, dass die Kontaktstelle der „reibungslosen und wirksamen Kommunikation“ und „operativen Zwecken“ dient. Die Zustellung von Schriftstücken, die für Gerichtsverfahren erforderlich ist, ist nicht eine bloße Kommunikation, sondern ein förmlicher Akt, an den bestimmte Rechtsfolgen geknüpft sind. Ferner nennt Artikel 9 Absatz 2 DSA bestimmte Mindestanforderungen, die die Anordnungen durch Justiz- oder Verwaltungsbehörden erfüllen müssen. Zur Zustellung werden hier jedoch ebenfalls keine Regelungen getroffen. Diese Mindestanforderungen haben jedoch keinen abschließenden Charakter. Nach Erwägungsgrund 31 werden lediglich „Mindestanforderungen“ harmonisiert. Und nach Erwägungsgrund 32 bleiben zusätzliche nationale Bedingungen möglich. Vielmehr wird in Artikel 9 Absatz 6 ausdrücklich normiert, dass das nationale Zivil- und Strafprozessrecht davon unberührt bleibt.

Gegen eine abschließende Regelung durch den DSA hinsichtlich eines Zustellungsbevollmächtigten spricht auch, dass an die elektronische Kontaktstelle im Sinne von Artikel 11 DSA auf absehbare Zeit keine förmliche Zustellung erfolgen kann. Nach Erwägungsgrund 42 des DSA benötigt die elektronische Kontaktstelle nach Artikel 11 DSA (im Gegensatz zu dem gesetzlichen Vertreter nach Artikel 13 DSA) keinen physischen Standort. An eine elektronische Adresse ist jedoch grundsätzlich keine förmliche Zustellung von Dokumenten wie einer Klageschrift möglich. Zwar gibt es für die Zustellung in andere EU Mitgliedstaaten Sondervorschriften. Nach § 183 Absatz 1 Nummer 1 der Zivilprozessordnung (ZPO) richtet sich die Zustellung in anderen EU Mitgliedsstaaten nach der Verordnung (EU) Nr. 2020/1784 (EuZVO). Gemäß Artikel 19 EuZVO kann die Zustellung durch elektronische Mittel erfolgen, die nach dem Recht des Forummitgliedstaats vorgesehen sind. Dies steht jedoch unter der Voraussetzung, dass die Schriftstücke mittels eines qualifizierten Dienstes (im Sinne von Artikel 44 Verordnung (EU) Nr. 910/2014) empfangen werden. Ein qualifizierter Dienst erfordert unter anderem, dass das Absenden und Empfangen der Daten durch eine fortgeschrittene elektronische Signatur oder ein fortgeschrittenes elektronisches Siegel eines qualifizierten Vertrauensdiensteanbieters auf eine Weise gesichert ist, dass die Möglichkeit einer unbemerkten Veränderung der Daten ausschließt. Der DSA setzt nicht voraus, dass die elektronische Kontaktstelle diese Voraussetzungen erfüllt. Daher wird in der Regel auch keine förmliche Zustellung an die elektronische Kontaktstelle erfolgen können.

Insofern besteht unionsrechtlich eine Regelungslücke, die durch nationales Recht gefüllt werden kann. Die Schaffung der Voraussetzungen für eine förmliche Zustellung an eine elektronische Adresse mit Sitz in der EU ist dabei – ohne vorherige Einwilligung des Zustellungsempfängers – auch nicht in der Verordnung über die Digitalisierung der justiziellen Zusammenarbeit und des Zugangs zur Justiz in grenzüberschreitenden Zivil-, Handels- und Strafsachen und zur Änderung einiger Rechtsakte im Bereich der justiziellen Zusammenarbeit (sog. Digitalisierungs-VO) vorgesehen. Gerade wegen der erheblichen Marktmacht sozialer Netzwerke ist es dringend erforderlich, insbesondere zur gerichtlichen Abwehr von rechtswidrigen Internetinhalten weiterhin eine schnelle und sichere Zustellungsvariante zur Verfügung zu haben, um den Betroffenen ein schnelles rechtliches Einschreiten zu ermöglichen. Ein Zustellungsbevollmächtigter im Heimatstaat des sozialen Netzwerks kann eine sichere und zügige Zustellung nicht in gleichem Maße gewährleisten, selbst wenn per Einschreiben zugestellt werden könnte. Die bisher gegen soziale Netzwerke geführten Zivilprozesse haben gezeigt, dass die europäischen Zustellungsmechanismen (Einschreiben

mit Rückschein in Zivilverfahren) generell nicht ausreichen, da entsprechende Zustellungen regelmäßig zwei bis drei Wochen dauern. Eine solche Zustellungsdauer wird der Dynamik von Internetsachverhalten nicht gerecht.

4. Verordnung (EU) 2020/1784

Die Möglichkeit, gegenüber sozialen Netzwerken nach Zustellung des verfahrenseinleitenden Schriftstücks im Einklang mit den Regelungen der EuZVO für ein konkretes Verfahren einen inländischen Zustellungsbevollmächtigten anzuordnen, ist für Anbieter mit Sitz in anderen EU-Mitgliedstaaten mit der EuZVO vereinbar. Es besteht ein sachliches Bedürfnis für die Verpflichtung zur Benennung eines inländischen Zustellungsbevollmächtigten, weil auch nach Inkrafttreten der Neuregelungen der EuZVO eine zivilgerichtliche oder außergerichtliche Zustellung an die Kontaktstelle beziehungsweise den gesetzlichen Vertreter nicht kurzfristig bewirkt werden kann. Auch für zivilgerichtliche Verfahren gegen Anbieter mit Sitz in anderen EU-Mitgliedstaaten sind die vorgesehenen Regelungen zum inländischen Zustellungsbevollmächtigten mit der EuZVO vereinbar, da bei Nichteinhaltung der Verpflichtung keine gesetzliche Zustellungsfiktion greift (siehe zur Ablehnung einer Zustellungsfiktion bei Zustellungsbevollmächtigten EuGH zur alten Fassung der EuZVO in der Rechtssache C-325/11 "Alder" und auch die Literatur zur neuen EuZVO u. a Fabig/Windau, NJW 2022, 1977 u. Gottwald, MDR, 2022, 1185 (1186)).

5. Richtlinie 2002/58/EG (E-Privacy-RL) und Verordnung (EU) 2016/ 679 (DS-GVO)

Die vorgesehenen gesetzlichen Maßnahmen sind sowohl mit der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) („E-Privacy-RL“) als auch mit der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, „DS-GVO“) vereinbar.

Gemäß Artikel 5 Absatz 1 Satz 1 E-Privacy-RL stellen die Mitgliedstaaten die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten durch innerstaatliche Vorschriften sicher. Gemäß Artikel 15 Absatz 1 E-Privacy-RL können die Mitgliedstaaten Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5 beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG für die nationale Sicherheit, (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zweck können die Mitgliedstaaten unter anderem durch Rechtsvorschriften vorsehen, dass Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden. Die E-Privacy-RL, insbesondere deren Artikel 15 Absatz 2, schließt dabei nicht die Möglichkeit der Mitgliedsstaaten aus, eine Pflicht zur Weitergabe personenbezogener Daten im Rahmen eines zivilrechtlichen Verfahrens vorzusehen (EuGH, Urteil vom 29. Januar 2008, C-275/06, Promusicae, Rn. 54).

Vor dem EuGH wurde bereits geklärt, dass nationale Regelungen, die eine Auskunftspflicht über Nutzungsdaten statuieren, grundsätzlich mit der DS-GVO und der E-Privacy-RL vereinbar sind (EuGH GRUR 2021, 1067, Rn. 115 ff., 132). Artikel 6 Absatz 4, 23 Absatz 1 Buchstabe j) erlauben grundsätzlich eine Zweckänderung nach nationalen Rechtsvorschriften, die insbesondere in notwendiger und verhältnismäßiger Weise die Durchsetzung zivilrechtlicher Ansprüche sicherstellen. Bei § 21 Absatz 2 und 3 TDDDG (bzw. der Vorgängernorm § 14 TMG a.F.) handelt es sich um eine solche Rechtsvorschrift im Sinne des Artikels

6 Absatz 4 DS-GVO (BGH BeckRS 2019, 28976 Rn. 40; OLG Schleswig GRUR-RS 2022, 5901 Rn. 35 mwN – Fake Account).

Die vorgesehene Speicherung von Daten auf gerichtliche Anordnung ist zur zivilrechtlichen Rechtsverfolgung insbesondere mit der Entscheidung des EuGH zur Vorratsdatenspeicherung (EuGH, Urteil vom 20. September 2022 – verb. C-793/19, C-794/19 – BRD/SpaceNet AG bzw. Telekom Deutschland GmbH) vereinbar.

So unterscheidet sich die vorgesehene Verpflichtung zur anlassbezogenen Speicherung einzelner IP-Datensätze hinsichtlich der Tiefe des damit verbundenen datenschutzrechtlichen Eingriffs bereits im Ansatz von dem der allgemeinen und unterschiedslosen Vorratsdatenspeicherung, die ohne Anlass erfolgt. In der Entscheidung BRD/SpaceNet wurde betont, dass sich die dortige Schwere des Eingriffs aus der Gefahr ergibt, dass die auf Vorrat gespeicherten Daten insbesondere in Anbetracht ihrer Menge und Vielfalt es in ihrer Gesamtheit ermöglichen, sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten gespeichert wurden, zu ziehen (EuGH, s.o., Rn. 87). Die Vorratsdatenspeicherung erfasst allgemein und unterschiedslos die gesamte Bevölkerung, ohne dass der Einzelne einen Anlass für die Speicherung seiner Daten gegeben hätte. Demgegenüber werden nach dem vorliegenden Entwurf nur gezielt ausgewählte Informationen im Zusammenhang mit einer konkreten Äußerung gespeichert, wenn tatsächliche Anhaltspunkte vorgetragen werden, dass diese eine Rechtsverletzung darstellt. Ob diese Voraussetzungen im konkreten Fall vorliegen, wird zudem durch ein Gericht geprüft. Es handelt sich also nicht um eine allgemeine und unterschiedslose Vorratsspeicherung.

Überdies hat der BGH einen Anspruch auf Unterlassung der Löschung von Verkehrsdaten zur Absicherung des Auskunftsanspruchs bei Verletzungen von Rechten des geistigen Eigentums aus der Verpflichtung zur effektiven Durchsetzung solcher Rechte (Richtlinie 2004/48/EG) sowie der „Natur der Sache“ hergeleitet, dass die Löschung der benötigten und vom Diensteanbieter bereits erhobenen Verkehrsdaten vorläufig unterbleiben darf und muss, soweit die Daten für die Auskunftserteilung erforderlich sind (BGH, ZUM 2018, 136, Rn. 59 und 62). Europarechtliche Bedenken hiergegen wurden bislang nicht geäußert.

6. Dienstleistungsfreiheit

Vorbehaltlich spezieller sekundärrechtlicher Bestimmungen ist eine nationale Regelung zur Verbesserung der privaten Rechtsverfolgung und Rechtsdurchsetzung gegenüber Diensteanbietern und Anbietern von Internetzugangsdiensten an den unionsrechtlichen Grundfreiheiten zu messen, sobald ein grenzüberschreitender Bezug besteht. Davon ist hier auszugehen. Die vorgesehenen gesetzlichen Maßnahmen richten sich nicht ausschließlich an inländische Anbieter und umfassen auch nicht nur deren Dienstleistung im Inland, sondern betreffen ebenso Betreiber aus anderen EU-Mitgliedstaaten beziehungsweise die Erbringung von Dienstleistungen durch inländische Betreiber an Nutzer in anderen EU-Mitgliedstaaten.

Berührt wird hier die Grundfreiheit des freien Dienstleistungsverkehrs (Artikel 56 des Vertrags über die Arbeitsweise der Europäischen Union). Eine Beschränkung lässt sich hier nur rechtfertigen, wenn sich erweist, dass sie zwingenden Gründen des Allgemeininteresses entspricht, geeignet ist, die Erreichung des mit ihr verfolgten Ziels zu gewährleisten, und nicht über das hinausgeht, was zur Erreichung dieses Ziels erforderlich ist. Dabei ist insbesondere zu begründen, warum das harmonisierende Sekundärrecht in dem entsprechenden Bereich nicht ausreicht und weitergehende nationale Beschränkungen erforderlich sind.

Als zwingendes Gemeinwohlinteresse ist die mit dem Gesetz gegen digitale Gewalt erfolgende Verbesserung der zivilrechtlichen Rechtsverfolgung und Rechtsdurchsetzung zur Verhütung und Bekämpfung von digitaler Gewalt anzusehen, welche mit dem vorliegenden

Entwurf aus den in der Begründung dargelegten erforderlichen und geeigneten Gründen ergänzt und fortentwickelt werden.

Zur Verhütung und Bekämpfung von digitaler Gewalt sind sowohl die schnelle Identifizierung der digitalen Rechtsverletzer als auch effektive Maßnahmen gegen diese Personen zur Unterbindung rechtswidriger Handlungen erforderlich. Hierzu leisten die im Gesetz gegen digitale Gewalt vorgesehenen Maßnahmen einen effektiven Beitrag, ohne dass es in harmonisiertem Sekundärrecht bereits entsprechende Maßnahmen gibt.

Die in § 2 vorgesehene Regelung zum Auskunftsverfahren ist mit der ergänzenden Befugnis zu Sicherungsanordnungen (§ 3) erforderlich, weil harmonisiertes Sekundärrecht solche Verfahren nicht enthält. So setzt Artikel 10 Absatz 1 DSA Rechtsgrundlagen zum Erlass von Auskunftsanordnungen voraus, ohne selbst eine Rechtsgrundlage hierfür zu bieten. Auch der in § 4 vorgesehene Anspruch zur Sperrung eines Nutzerkontos ist erforderlich. Zwar enthält Artikel 23 Absatz 1 DSA regulatorische und im Wege der Aufsicht durchsetzbare Vorgaben für die „Aussetzung der Dienste“, nicht aber eine zivilrechtliche Anspruchsgrundlage für die Anordnung einer Sperrung eines Nutzerkontos durch ein Gericht. Auch die in § 8 Absatz 3 vorgesehene Anordnungsmöglichkeit, einen inländischen Zustellungsbevollmächtigten in Deutschland und damit einen „Briefkasten“ im Inland vorzuhalten, kann (weiterhin) sowohl geeignet als auch erforderlich im Hinblick auf eine wirksame zivilrechtliche Rechtsverfolgung zur Bekämpfung von digitaler Gewalt im Internet sein. Eine effektive Verfolgung von auf sozialen Netzwerken begangenen Rechtsverletzungen setzt nämlich voraus, dass der gerichtsfeste Nachweis einer Kenntniserlangung des Anbieters des sozialen Netzwerks im Hinblick auf einen auf dem sozialen Netzwerk zirkulierenden rechtswidrigen Inhalt für einen Zeitpunkt möglichst kurz nach Kenntniserlangung beim Betroffenen erbracht wird. So besteht auch nach Inkrafttreten des DSA und Neuregelungen der EuZVO ein sachliches Bedürfnis für die Verpflichtung von Anbietern sozialer Netzwerker zur Benennung eines inländischen Zustellungsbevollmächtigten, da zivilgerichtliche oder außergerichtliche Zustellungen an eine Kontaktstelle beziehungsweise einen gesetzlichen Vertreter auch weiterhin nicht kurzfristig bewirkt werden können. Die in der Vergangenheit gegen soziale Netzwerke geführten Zivilprozesse haben dabei gezeigt, dass die europäischen Zustellungsmechanismen (Einschreiben mit Rückschein in Zivilverfahren) vor dem Hintergrund der besonderen Verbreitungs- und Speicherdynamik des Internets für eine effektive private Rechtsverfolgung generell nicht ausreichen. Gerade wegen der erheblichen Marktmacht sozialer Netzwerke ist es daher dringend erforderlich, dem von rechtswidrigen Inhalten Betroffenen zur zivilgerichtlichen Rechtsverfolgung eine schnelle und sichere Zustellungsvariante zur Verfügung zu stellen, um ein schnelles rechtliches Einschreiten zu ermöglichen. Ein Zustellungsbevollmächtigter im Heimatstaat des sozialen Netzwerks kann eine sichere und zügige Zustellung nicht in gleichem Maße gewährleisten, selbst wenn per Einschreiben zugestellt werden könnte.

Die durch das Gesetz gegen digitale Gewalt vorgesehenen Maßnahmen gehen dabei durch entsprechende Vorgaben auf Tatbestands- und Rechtsfolgenseite allesamt nicht über das für die effektive Verhütung und Bekämpfung digitaler Gewalt erforderliche Maß hinaus. Dies betrifft insbesondere die Ausgestaltung der Regelungen zur Sperrung eines Nutzerkontos. Um den grundrechtlichen Positionen aller Beteiligten – der antragstellenden Person, des Accountinhabers und des Anbieters eines sozialen Netzwerks – Rechnung zu tragen, wird die Sperrung an mehrere Bedingungen geknüpft. Unter anderem muss die Sperrung im Einzelfall verhältnismäßig sein. Diesem Ziel dienen auch strenge tatbestandliche Voraussetzungen. Erforderlich ist, dass eine sonstige Form der Inhaltemoderation als milderes Mittel nicht ausreicht und die Gefahr der Wiederholung schwerwiegender Rechtsverletzungen durch von einem spezifischen Account veröffentlichte Inhalte besteht. Die Sperrung soll dabei jeweils nur für einen angemessenen Zeitraum ergehen können. Vor Entscheidung des Gerichts über die Sperrung des Nutzerkontos muss der betroffene Accountinhaber vom Gericht oder, bei fehlender Kenntnis der Identität des Accountinhabers, vom Anbieter des sozialen Netzwerks auf ein anhängiges Sperrersuchen hingewiesen und ihm Gelegenheit zur Stellungnahme gegeben werden. Dies kann auch über die Kommunikationskanäle des

sozialen Netzwerks selbst erfolgen. Auf diese Weise können auch anonyme Nutzer erreicht werden. Damit eine Sperrung des Nutzerkontos effektiv ist, soll der Anbieter des sozialen Netzwerks dazu verpflichtet werden, Umgehungsversuche durch den Accountinhaber im Rahmen des für ihn Zumutbaren zu unterbinden.

7. Notifizierungspflicht nach der Richtlinie (EU) 2015/1535

Die geplante Regelung ist notifizierungspflichtig nach der Richtlinie (EU) 2015/1535 vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft.

VII. Gesetzesfolgen

Der Gesetzentwurf wirkt sich vor allem dahingehend aus, dass wesentliche Maßnahmen der privaten Rechtsverfolgung im Internet zukünftig in einem Stammgesetz geregelt werden. Unbeabsichtigte Gesetzesfolgen sind nicht erkennbar.

1. Rechts- und Verwaltungsvereinfachung

Der Entwurf dient der Rechts- und Verwaltungsvereinfachung. Der Gesetzentwurf sorgt für Rechtsklarheit im Hinblick auf wesentliche Maßnahmen der privaten Rechtsverfolgung im Internet, indem er diese in einem eigenen Stammgesetz zusammenfasst und transparent ausgestaltet.

2. Nachhaltigkeitsaspekte

Der Entwurf steht im Einklang mit den Leitgedanken der Bundesregierung zur nachhaltigen Entwicklung im Sinne der Deutschen Nachhaltigkeitsstrategie, die der Umsetzung der UN-Agenda 2030 für nachhaltige Entwicklung der Vereinten Nationen dient.

Indem der Entwurf die Rechte der von digitaler Gewalt betroffenen Personen stärkt, leistet er einen Beitrag zur Verwirklichung von Nachhaltigkeitsziel 16 „Friedliche und inklusive Gesellschaften für eine nachhaltige Entwicklung fördern, allen Menschen Zugang zur Justiz ermöglichen und leistungsfähige, rechenschaftspflichtige und inklusive Institutionen auf allen Ebenen aufbauen“. Dieses Nachhaltigkeitsziel verlangt mit seiner Zielvorgabe 16.3, die Rechtsstaatlichkeit auf nationaler und internationaler Ebene zu fördern und den gleichberechtigten Zugang aller zur Justiz zu gewährleisten. Der Entwurf fördert die Erreichung dieser Zielvorgabe, indem er das Auskunftsverfahren gegenüber den Diensteanbietern und Anbieters von Internetzugangsdiensten effektiver ausgestaltet, insbesondere durch die Normierung eines Anspruchs auf richterlich angeordnete Sperrung des Nutzerkontos bereits nach erstmaliger schwerer Rechts-verletzung mit Wiederholungsgefahr. Damit versetzt der Entwurf Betroffene von digitaler Gewalt in die Lage zu versetzen, selbstständig, zeitnah und effektiv gegen Beleidigungen, Bedrohungen und sonstige Persönlichkeitsrechtsverletzungen im Netz gezielt vorzugehen. Indem der Entwurf das Auskunftsverfahren gegenüber den Diensteanbietern und Anbieters von Internetzugangsdiensten effektiver ausgestaltet, leistet er einen Beitrag zur Verwirklichung von Zielvorgabe 16.6, die verlangt, leistungsfähige, rechenschaftspflichtige und transparente Institutionen auf allen Ebenen aufzubauen. Der Entwurf fördert die Erreichung dieser Zielvorgabe, indem er das Auskunftsverfahren nach dem in der freiwilligen Gerichtsbarkeit geltenden Amtsermittlungsgrundsatz bei den Landgerichten gerichtskostenfrei regelt und damit insbesondere die Sicherung der Bestands- und Nutzerdaten mutmaßlicher Verfasser rechtswidriger Inhalte bei den Dienstanbietern in einem frühen Verfahrensstadium ermöglicht.

Indem der Entwurf die grundsätzliche Freiheit zur anonymen Meinungsäußerung bewahrt, leistet er außerdem einen Beitrag zur Erreichung von Zielvorgabe 16.10, die verlangt, den öffentlichen Zugang zu Informationen zu gewährleisten und die Grundfreiheiten zu

schützen. Der Entwurf fördert die Erreichung dieser Zielvorgabe, indem er insbesondere die richterlich angeordnete Accountsperre als ein neues Instrument zur Bekämpfung digitaler Gewalt an die tatbestandsrechtliche Voraussetzung der schwerwiegenden Persönlichkeits-rechtsverletzung mit Wiederholungsgefahr knüpft und dabei die grundrechtlichen Positionen aller Beteiligten und den Verhältnismäßigkeitsgrundsatz berücksichtigt.

Im Sinne des systemischen Zusammendenkens der Nachhaltigkeitsziele leistet der Entwurf damit gleichzeitig einen Beitrag zur Erreichung von Zielvorgabe 5.c, die verlangt, durchsetzbare Rechtsvorschriften zur Förderung der Gleichstellung der Geschlechter auf allen Ebenen zu beschließen und zu verstärken. Der Entwurf fördert die Erreichung dieser Zielvorgabe, indem er dazu beiträgt, Diskriminierungen auch wegen des Geschlechts durch Hasskriminalität und andere rechtswidrigen Inhalten im virtuellen Raum insbesondere auf den Plattformen sozialer Netzwerke wirksam zu begegnen, um so das friedliche Zusammenleben in einer freien, offenen und demokratischen Gesellschaft zu fördern. Damit berücksichtigt der Entwurf die Querverbindungen zwischen den Zielen für nachhaltige Entwicklung und deren integrierenden Charakter, der für die Erfüllung von Ziel und Zweck der UN-Agenda 2030 von ausschlaggebender Bedeutung ist.

Der Entwurf folgt damit den Prinzipien der Deutschen Nachhaltigkeitsstrategie „(1.) Nachhaltige Entwicklung als Leitprinzip konsequent in allen Bereichen und bei allen Entscheidungen anwenden“ und „(5.) Sozialen Zusammenhalt in einer offenen Gesellschaft wahren und verbessern“.

3. Haushaltsausgaben ohne Erfüllungsaufwand

Keine.

4. Erfüllungsaufwand

4.1. Erfüllungsaufwand für Bürgerinnen und Bürger

Vorgabe 4.1.1: Auskunft über Daten und Accountsperre, §§ 2 und 4 GgdG

Durch das verbesserte Auskunftsverfahren wird eine Zunahme von 1 400 zusätzlichen Verfahren (Herleitung: s. Vorgabe 4.2.1) sowie die Beantragung von 810 Accountsperren (s. Vorgabe 4.2.2) geschätzt. Aufgrund der geschätzten Fallzahl (i.e. rund 2 200) wird ein geringfügiger Mehraufwand für Bürgerinnen und Bürger erwartet.

4.2. Erfüllungsaufwand der Wirtschaft nach Vorgaben

Vorgabe 4.2.1 (Informationspflicht): Auskunft über Daten, § 2 GgdG

Veränderung des jährlichen Erfüllungsaufwands:

Fallzahl	Zeitaufwand pro Fall (in Minuten)	Lohnsatz pro Stunde (in Euro)	Sachkosten pro Fall (in Euro)	Personalkosten (in Tsd. Euro)	Sachkosten (in Tsd. Euro)
6 400	10	49,30	0	53	0
Änderung des Erfüllungsaufwands (in Tsd. Euro)					53

Aktuell werden Auskunftsverfahren zur Identifizierung von Personen, die Rechtsverletzungen im digitalen Raum begehen, nach § 21 Absatz 2 bis 4 TDDDG geregelt. Jedoch scheitert die Rechtsdurchsetzung von betroffenen Personen häufig daran, dass die Identität der rechtsverletzenden Person nicht festgestellt werden kann (vgl. https://www.bmj.de/SharedDocs/Downloads/DE/Gesetzgebung/Eckpunkte/Digitale_Gewalt_Eckpunkte.pdf?__blob=publicationFile&v=2). Nach § 2 GgdG soll der Auskunftsumfang

bezüglich der Herausgabe von Bestandsdaten um die Herausgabe bestimmter Nutzungsdaten (IP-Adresse und Portnummer) erweitert werden. Dadurch wird zusätzlicher Erfüllungsaufwand durch zwei Effekte vermutet. Zum einen werden zusätzlich zu den betroffenen Onlinediensten auch Anbieter von Internetzugangsdiensten zur Auskunft verpflichtet. Andererseits wird aufgrund verbesserter Rechtsdurchsetzung ein moderater Anstieg des Verfahrensaufkommens erwartet.

Eine zentrale statistische Erfassung der Anzahl an Auskunftsverfahren liegt nicht vor. Näherungsweise wird auf Anfragen der Sicherheitsbehörden pro Jahr zurückgegriffen, die maximal 4 000 umfassen. (s. Drs. 19/25294: S. 39, unter: https://dserver.bundestag.de/btd/19/252/1925294.pdf). Unterstellt man diese Anzahl für den zivilrechtlichen Bereich und nimmt an, dass aufgrund der Rechtsänderung in 90 Prozent der Fälle eine parallele Abfrage der Internetzugangsdienste hinzukommt – in manchen Fällen liegen bei den Diensteanbietern ausreichend Daten vor –, ist allein aufgrund der Ausweitung des Normadressatenkreises mit 3 600 zusätzlichen Anfragen zu rechnen. Diese Größenordnung entspricht auch der bekannten Anzahl an Verfahren nach den § 101 Absatz 9 UrhG, § 19 Absatz 9 MarkenG und §140b Absatz 9 PatentG. So werden z. B. im Rahmen der gerichtlichen Auskunftsanordnung nach § 101 Absatz 9 UrhG jährlich ca. 2 000 Verfahren (vgl. Statistischer Bericht – Zivilgerichte – 2023, unter: https://www.destatis.de/DE/Themen/Staat/Justiz-Rechtspflege/_inhalt.html#_edff98645) durchgeführt. Der Auskunftsanspruch setzt voraus, dass eine offensichtliche Verletzung eines nach dem Urheberrechtsgesetz geschützten Rechts vorliegt oder bereits Klage gegen den Verletzer erhoben worden ist und fällt somit in seinem Anwendungsbereich hinter § 2 GgdG zurück. Die Annahme von 3 600 zusätzlichen Verfahren durch Ausweitung des Anwendungsbereichs des § 2 GdgG auf Internetzugangsdiensteanbieter und IP-Adressen lässt sich somit auch anhand der bekannten Anzahl an Verfahren nach den § 101 Absatz 9 UrhG plausibel darlegen.

Ferner wird ein moderater Anstieg der Anzahl an durchgeführten Verfahren erwartet, welcher näherungsweise mittels der PKS-Statistik „Tatmittel Internet“ der Jahre 2022 und 2023 (BKA, 2022 & 2023, T05 Grundtabelle - Straftaten mit Tatmittel „Internet“ - Fälle (V1.0), unter: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/pks_node.html) geschätzt wird. Dazu wurden die Daten gemäß der relevanten Tatbestände nach § 1 Abs. 1 Satz 1 GgdG sortiert und gemittelt. Insgesamt wurden pro Jahr im Mittel rund 97 000 Tatbestände erfasst und rund 83 000 Fälle aufgeklärt. Somit ergibt sich, dass circa 14 000 Fälle im Jahr unaufgeklärt bleiben. Unter der Annahme, dass das verbesserte Auskunftsverfahren zu einer Steigerung der Aufklärungsquote um 10% führen wird, würden dadurch rund 1 400 zusätzlichen Auskunftsfällen für betroffene Online-Dienste und Internetzugangsdienste jährlich hinzukommen. Somit ergibt sich eine Fallzahl von 6 400 zusätzlichen Auskunftsanfragen im Jahr (= 3 600 Bestandsdatenabfragen an Internetzugangsdiensten + [1 400 * 2] zusätzliche Anfragen nach der neuen Rechtslage).

Für die Übermittlung der Daten und sonstige im Zuge des Auskunftsverfahrens anfallende Prozesse, einschließlich der Umsetzung von Sicherungsanordnungen nach § 3 GgdG, wird ein Zeitaufwand von 10 Minuten pro Fall angesetzt. Herangezogen wurde dieser Zeitwert aus einer vergleichbaren Vorgabe der Online Datenbank des Erfüllungsaufwands (s. OnDEA, unter: https://www.ondea.de/SiteGlobals/Functions/Datenbank/Vorgaben/Einzelansicht/Vorgabe_Einzelansicht.html?idVorgabe=116830).

Bei einer geschätzten Steigerung um rund 6 400 Fälle pro Jahr, einem Zeitaufwand von 10 Minuten pro Fall und einem durchschnittlichen Lohnsatz der Wirtschaft von 49,30 Euro pro Stunde (vgl. Leitfaden Anhang 7, Zeile J, S. 65f.) entsteht der Wirtschaft zusätzlicher laufender Erfüllungsaufwand aus Informationspflichten von rund 53 000 Euro im Jahr.

Vorgabe 4.2.2: richterlich angeordnete Accountsperre, § 4 GgdG

Die Neueinführung des § 4 GgdG sieht ein neues Instrument zur Bekämpfung digitaler Gewalt vor. Dadurch besteht künftig die Möglichkeit einzelne Nutzerkonten aufgrund fortwährender schwerwiegender Rechtsverletzungen temporär – durch richterliche Anordnung – zu sperren, auch wenn die Identität des rechtsverletzenden Nutzers unbekannt ist.

In wie vielen Fällen die Sperrung eines Accounts durch richterliche Anordnung künftig notwendig sein wird, kann nur grob geschätzt werden. Angenommen wird, dass jährlich rund 810 Accountsperren angeordnet werden.

Da der fallbezogene Zeitaufwand für das Sperren und das spätere Entsperren eines Nutzerkontos unter Berücksichtigung des hohen Grades an Automatisierung in den betroffenen Unternehmen gering eingeschätzt wird, ergibt sich hieraus nur ein geringfügiger – nicht näher zu beziffernder – Erfüllungsaufwand.

Vorgabe 4.2.3: Zustellungsbevollmächtigter, § 9 GgdG

Der neue § 9 GgdG ist weitestgehend deckungsgleich mit der bisherigen geltenden Regelung in § 5 NetzDG, weshalb keine Änderungen des Erfüllungsaufwands der Wirtschaft zu erwarten sind. Durch § 9 Abs. 3 GgdG wird nun zusätzlich die Möglichkeit eingeführt, dass ein Gericht im Einzelfall anordnen kann, dass Anbieter aus dem Ausland für ein anhängiges Gerichtsverfahren einen Zustellungsbevollmächtigten im Inland benennen müssen. Diese Neuerung dürfte, wenn überhaupt, nur im Ausnahmefall Anwendung finden, da bekannte, im Anwendungsbereich des Gesetzes liegende Anbieter, sich bereits regelmäßig von einem Prozessbevollmächtigten im Inland vertreten lassen, an den das Gericht zustellen kann. Ferner kann den betroffenen Unternehmen aus dem Empfang zusätzlicher Schreiben nach Absatz 2 Satz 2 GgdG im Einzelfall und abhängig von der gewählten Benennungspraxis des Zustellungsbevollmächtigten ein voraussichtlich geringfügiger Erfüllungsaufwand anfallen.

4.3. Erfüllungsaufwand der Verwaltung

Für die Verwaltung entsteht kein Erfüllungsaufwand.

5. Weitere Kosten

Durch die neugeregelten Auskunftsverfahren (§ 2 GgdG) sowie die neue Möglichkeit zur Durchsetzung einer Accountsperre (§ 4 GgdG) ergeben sich laufende Mehrkosten für die Justiz der Länder. Für das Auskunftsverfahren einschließlich der Sicherungsanordnungen und für Ansprüche, die auf die Sperrung des Nutzerkontos gerichtet sind, sind die Landgerichte zuständig. Entsprechend der Fortschreibung der Basiszahlen zur Personalbedarfsbemessung für die Ordentliche Gerichtsbarkeit und die Staatsanwaltschaften im Jahr 2014 wird eine mittlere Bearbeitungszeit pro Fall an dem Landgericht in Höhe von 34 Minuten angesetzt (s. PEBB§Y-Fortschreibung 2014, S. 187, unter: https://justiz.thueringen.de/fileadmin/TMMJV/Service/pebbsy/fortschreibung2014_anlagenband.pdf). Bei geschätzt rund 2 210 notwendigen richterlichen Anordnungen (= 1 400 Auskunftsverfahren und 810 Accountsperren), einem geschätzten Zeitaufwand von 34 Minuten pro Fall und einem durchschnittlichen Lohnsatz des höheren Dienstes der Länder von 65,20 Euro pro Stunde (vgl. Leitfaden, Anhang 9) verursachen die notwendigen richterlichen Anordnungen zur Durchsetzung von Auskunftsverfahren und Accountsperren Mehrkosten von rund 82 000 [= 2 210 * 34 Minuten / 60 Minuten * 65,20 Euro] Euro jährlich für die Länder.

Darüber hinaus wird im Rahmen des Auskunftsverfahrens in nahezu allen Fällen eine Sicherungsanordnung (§ 3 GgdG) erlassen. Informationen zum fallbezogenen Aufwand einer Sicherungsanordnung liegen nicht vor. Es ist zu erwarten, dass das Gericht zum Erlass einer Sicherungsanordnung zwei Kommunikationsvorgänge (einmal an

PlattformbetreiberOnlinedienste zur Ermittlung der mit dem Rechtsverstoß verbundenen IP-AdresseNutzerdaten und einmal an Internetzugangsdienste zur Durchsetzung der Sicherungsanordnung) aufsetzen muss sowie die von der Plattform übermittelte IP-Adresse einem zuständigen Internetzugangsdienst zuordnen muss, sodass insgesamt 10 Minuten pro Sicherungsanordnung (vgl. Leitfaden, Anhang 8, Standardaktivitäten 3 und 4 in einfacher Komplexität) anfallen. Durch die neu hinzukommenden Sicherungsanordnungen im Zuge der künftig 5 400 jährlich geschätzten Auskunftsverfahren entstehen bei einem Zeitaufwand von 10 Minuten pro Fall und einem Lohnsatz von 65,20 Euro pro Stunde rund 59 000 [= 5 400 * 10 Minuten /60 Minuten * 65,20 Euro] Euro Mehraufwand.

Gegen die zusätzlichen Auskunftsverfahren ist die Beschwerde gemäß § 5 Absatz 4 GdgG statthaft. Nach dem statistischen Bericht der Zivilgerichte 2023 wurden insgesamt 293 642 vor dem Landgericht in erster Instanz erledigte Zivilprozesssachen und 29 939 vor dem Landgericht in der Berufungsinstanz erledigte Zivilprozesssachen geführt (vgl. Statistischer Jahresbericht Zivilgerichte 2023, unter: https://www.destatis.de/DE/Themen/Staat/Justiz-Rechtspflege/Publikationen/Downloads-Gerichte/statistischer-bericht-zivilgerichte-2100210237005.html), was eine Anwendung zulässiger Rechtsmittel in rund 10 Prozent [= 29 939 / 293 642 * 100] der Fälle bedeutet. Folglich wird vermutet, dass in 10 Prozent der zusätzlichen Auskunftsverfahren und der richterlich angeordneten Accountsperren – also rund 220 Fällen [= 2 210 * 10%] – eine Beschwerde erwirkt wird. Bei einem durchschnittlichen Zeitaufwand von 223 Minuten pro Beschwerde (vgl. PEBB§Y-Fortschreibung 2014, S. 188, unter: https://justiz.thueringen.de/fileadmin/TMMJV/Service/pebbsy/fortschreibung2014_anlagenband.pdf), 220 Fällen und einem Lohnsatz von 65,20 pro Stunde (vgl. Leitfaden, Anhang 9) entstehen jährliche Mehrkosten von rund 53 000 [= 220 * 223/60 * 65,20] Euro.

6. Weitere Gesetzesfolgen

Gleichstellungspolitische Belange

Das Gesetzesvorhaben hat Auswirkungen von gleichstellungspolitischer Bedeutung. Der Entwurf trägt dazu bei, Diskriminierungen auch wegen des Geschlechts durch Hasskriminalität und andere rechtswidrige Inhalte im virtuellen Raum, insbesondere auf den Plattformen sozialer Netzwerke, wirksamer zu bekämpfen. Unbeabsichtigte Gesetzesfolgen sind nicht erkennbar.

Gleichwertigkeits-Check

Das Gesetzesvorhaben hat Auswirkungen auf die Gleichwertigkeit der Lebensverhältnisse der Menschen. Ungleiche Lebensverhältnisse sollen verringert, nicht verfestigt oder verstärkt werden. Ein wichtiger Beitrag besteht darin, rechtliche Hürden zur effektiven Rechtsdurchsetzung bei digitaler Gewalt abzubauen. Insbesondere durch die kostengünstige Ausgestaltung der Verfahren soll es Personen unabhängig von ihren wirtschaftlichen Verhältnissen erleichtert werden, ihre Rechte bei Betroffenheit von digitaler Gewalt durchzusetzen.

VIII. Befristung; Evaluierung

Dieses Gesetz sollte spätestens fünf Jahre nach Inkrafttreten evaluiert werden. Dabei wird die Bundesregierung in fachlich geeigneter Weise prüfen, ob und inwieweit die beabsichtigten Wirkungen erreicht worden sind. Die Bundesregierung wird ferner untersuchen, wie sich der Erfüllungsaufwand für Bürger und Wirtschaft entwickelt hat und ob die Entwicklung in einem angemessenen Verhältnis zu den festgestellten Regelungswirkungen steht. Die Evaluierung wird die Frage nach unbeabsichtigten Nebenwirkungen sowie nach der Akzeptanz und Praktikabilität der Regelungen einschließen.

B. Besonderer Teil

Zu Artikel 1 (Gesetz gegen digitale Gewalt)

Artikel 1 enthält das Gesetz gegen digitale Gewalt. Das Gesetz gegen digitale Gewalt soll vorhandene Schutzlücken im Auskunftsverfahren gemäß § 21 Absatz 2 bis 4 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes (TDDDG) schließen und einzelne Rechte im Betroffenen-Plattform-Verhältnis in einem neuen Stammgesetz bündeln und regeln.

Zu § 1 (Begriffsbestimmungen)

Zu Absatz 1

Der Begriff der Rechtsverletzung stellt einen zentralen Anknüpfungspunkt des Entwurfs dar. Rechtsverletzungen im Sinne dieses Gesetzes sind Straftaten, die den Tatbestand der §§ 111, 126, 126a, 130, 130a, 131, 140, 166, 176a, 176b, 184 bis 184c, 184k, 185 bis 189, 192a, 201, 201a, 238 oder 241 des Strafgesetzbuches, des § 33 des Gesetzes betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie oder des § 42 des Bundesdatenschutzgesetzes erfüllen und nicht gerechtfertigt sind. Die genannten Straftaten werden häufig im digitalen Raum begangen, weisen eine besondere Nähe zum Persönlichkeitsrecht auf und schützen daher auch subjektive Rechte. Durch die Anknüpfung an konkrete Straftatbestände wird verdeutlicht, dass nicht bei jeder Verletzung eines absolut geschützten Rechts oder bei jeder Verletzung eines Schutzgesetzes das Auskunftsverfahren durchgeführt werden und der Anspruch auf eine Sperrung des Nutzerkontos bestehen soll. Erfasst werden ausschließlich Handlungen, die den Tatbestand eines oder mehrerer der in Absatz 1 genannten Strafgesetze erfüllen und rechtswidrig, aber nicht notwendigerweise schuldhaft begangen werden. Zudem ist es unerheblich, ob ein Delikt auf konkurrenzrechtlicher Ebene verdrängt wird. Beispielsweise ist eine Rechtsverletzung nicht deswegen abzulehnen, weil neben der Bedrohung auch eine Nötigung erfüllt ist, obwohl diese nach herrschender Auffassung die Bedrohung verdrängt (*Valerius*, in: BeckOK, StGB, § 241 Rn. 13 mwN).

Der Straftatenkatalog orientiert sich am früheren § 1 Absatz 3 Netzwerkdurchsetzungsgesetz, enthält jedoch einige Änderungen. Auf die Straftatbestände §§ 86, 86a, 89a, 91, 100a, 129 bis 129b und 269 StGB wird verzichtet, weil diese nicht typischerweise mit der zumindest mittelbaren Verletzung eines subjektiven Rechts einhergehen, sondern ausschließlich kollektive Rechtsgüter schützen. Ähnlich verhält es sich mit den §§ 89a, 91, 129 bis 129b StGB, bei denen es sich um Vorfeld- bzw. Organisationsdelikte handelt, die für eine Strafbarkeit keine individuelle Rechtsgutsverletzung voraussetzen. Neu hinzu kommen die §§ 126a, 130a, 176a, 176b, 184, 184a, 184c, 184k, 188, 192a, 201, 238 StGB, § 33 KUG, § 42 BDSG. Neben dem wichtigen Anwendungsfall der Hassrede sollen weitere Formen von digitaler Gewalt, insbesondere strafrechtlich relevante Deep Fakes – realistisch wirkende Medieninhalte, die durch Techniken der Künstlichen Intelligenz erzeugt worden sind – und Doxing – unberechtigtes Veröffentlichen personenbezogener Daten – erfasst sein. Diese Phänomene könnten unter anderem strafbar sein nach §§ 126a, 185 ff., 201a StGB, § 33 KUG, § 42 BDSG. Außerdem soll das gezielte Ansprechen im Internet von Kindern, um sexuellen Kontakt anzubahnen (sogenanntes Cybergrooming), das gemäß § 176b StGB strafbar ist, in den Anwendungsbereich des Gesetzes fallen.

Zusätzlich muss für die Rechtsverletzung der Dienst eines Diensteanbieters genutzt werden, um den kausalen Beitrag des Diensteanbieters zur Rechtsverletzung sicherzustellen und zugleich die Taten, die ausschließlich in der analogen Welt begangen werden, auszuschließen.

Zu Absatz 2

Diensteanbieter im Sinne dieses Gesetzes sind Online-Plattformen, Web-Hosting- und Cloud-Hosting-Dienste. Diese Dienste stellen Unterkategorien von Hosting-Diensten dar. Hosting-Dienste bestehen gemäß Artikel 1 Absatz 1 Buchstabe g Ziffer iii DSA darin, von einem Nutzer bereitgestellte Informationen in dessen Auftrag zu speichern. Erfasst werden von diesem Gesetz dabei nur jene Unterkategorien, die regelmäßig einen Begehungsort von digitaler Gewalt darstellen. Dies sind Online-Plattformen sowie Web- und Cloud-Hostingdienste, deren Dienste für die Begehung einer Rechtsverletzung genutzt werden.

Dienste der reinen Durchleitung (wie zum Beispiel VPN-Netzwerke) und Caching-Dienste werden folglich nicht erfasst, da diese keine Hosting-Dienste darstellen. Ebenfalls nicht erfasst werden Suchmaschinen sowie rein interpersonelle Kommunikationsdienste wie zum Beispiel Messenger- und E-Mail-Hosting-Dienste, Videokonferenzen und Internettelefonie.
.

Zu Nummer 1

Online-Plattformen stellen gemäß Artikel 1 Absatz 1 Buchstabe i DSA eine Unterkategorie von Hosting-Diensten dar. Die zentrale Eigenschaft von Online-Plattformen ist die öffentliche Verbreitung von Informationen im Auftrag des Nutzers. Online-Plattformen umfassen insbesondere soziale Netzwerke, Video-Sharing-Plattformen und Marktplätze. Auch öffentliche Gruppen oder Kanäle von Kommunikationsdiensten sind Online-Plattformen, sofern diese gerade nicht für eine rein interpersonelle Kommunikation zwischen einer endlichen, vom Absender bestimmten Anzahl von Personen verwendet werden, sondern die Bereitstellung von Informationen für eine potentiell unbegrenzte Zahl von Nutzern ermöglichen. Abzugrenzen sind Online-Plattformen hingegen von rein interpersonellen Kommunikationsdiensten wie Messenger- und E-Mail-Diensten.

Zu Nummer 2

Web-Hosting-Dienste stellen eine Unterkategorie von Hosting-Diensten dar. Diese Dienste stellen Serverressourcen bereit, um Webseiten im Internet zu hosten. Nutzer registrieren eine Domain, die mit dem Web-Hosting-Anbieter verknüpft wird. Der Web-Hosting-Anbieter weist dem Nutzer Speicherplatz auf ihren Servern zu. Durch das Erstellen und Veröffentlichen von Internetseiten können ähnlich wie auf Online-Plattformen rechtsverletzende Inhalte anonym verbreitet werden. Oft werden etwa sog. Revenge-Porns auf eigens dafür erstellten Internetseiten veröffentlicht.

Zu Nummer 3

Cloud-Hosting-Dienste stellen eine weitere Unterkategorie von Hosting-Diensten dar und umfassen sog. File-Hosting-Services. Nutzer können auf ihre Dateien von verschiedenen Geräten aus zugreifen, sei es über Webbrowser, Desktop-Anwendungen oder mobile Apps. Diese Dienste ermöglichen es regelmäßig, Inhalte etwa durch Erstellung und Versendung eines Links mit einem unbestimmten Adressatenkreis zu teilen und somit rechtsverletzende Inhalte zu verbreiten. Diese Cloud-Hosting-Dienste stellen damit neben Online-Plattformen und Web-Hosting-Diensten einen weiteren Schauplatz für digitale Gewalt dar.

Zu Absatz 3

Für den Begriff des Internetzugangsdienstes wird auf den durch Unionsrecht harmonisierten Begriff, der auch im TKG verwendet wird, Bezug genommen.

Zu Absatz 4

Absatz 4 definiert den Begriff des sozialen Netzwerks. Eine Definition ist notwendig, weil sich der Anspruch auf eine richterlich angeordnete Sperrung des Nutzerkontos und die Pflicht, einen Zustellungsbevollmächtigten zu benennen, allein auf soziale Netzwerke bezieht. Die Definition lehnt sich an die frühere Definition aus § 1 Absatz 1 Netzwerkdurchsetzungsgesetz (NetzDG) an und konkretisiert sie insoweit, als dass Nutzer auf sozialen Netzwerken miteinander kommunizieren und interagieren, indem sie Inhalte teilen oder veröffentlichen. Dies betont den kommunikativen Charakter von sozialen Netzwerken und ist bei Bezugnahme auf den nach DSA definierten Begriff der Online-Plattform notwendig, um soziale Netzwerke etwa von Online-Marktplätzen abzugrenzen, auf denen zwar ebenfalls Nutzerinhalte veröffentlicht werden können, Hauptzweck aber das Angebot von Waren oder Dienstleistungen ist. Die Interaktion der Nutzer nimmt bei diesen Diensten nur eine untergeordnete Rolle ein, um den Hauptzweck zu erreichen. Die zu teilenden oder zu veröffentlichenden Inhalte können in jeglichen Informationen bestehen, insbesondere in reinem Text, aber beispielsweise auch in Videos, Fotos und Empfehlungen.

Anders als nach der Definition im NetzDG sollen nicht nur beliebige Inhalte umfasst und damit Plattformen zur Verbreitung von spezifischen Inhalten ausgeschlossen werden. Das Nutzerverhalten auf Online-Plattformen hat sich dahingehend entwickelt, dass z.B. auch themenspezifische Plattformen wie Berufs- und Gaming-Plattformen sowie Plattformen, die vorwiegend zur Verbreitung pornographischer Nutzerinhalte bestimmt sind, Schauplätze von digitaler Gewalt darstellen können.

Zu Absatz 5

Für den Begriff der Inhaltemoderation wird auf Artikel 3 Buchstabe t DSA Bezug genommen. Danach bezeichnet die Moderation von Inhalten die – automatisierten oder nicht automatisierten – Tätigkeiten der Anbieter von Vermittlungsdiensten, mit denen insbesondere rechtswidrige Inhalte oder Informationen, die von Nutzern bereitgestellt werden und mit den allgemeinen Geschäftsbedingungen des Anbieters unvereinbar sind, erkannt, festgestellt und bekämpft werden sollen, darunter auch Maßnahmen in Bezug auf die Verfügbarkeit, Anzeige und Zugänglichkeit der rechtswidrigen Inhalte oder Informationen, z. B. Herabstufung, Demonetisierung, Sperrung des Zugangs oder Entfernung, oder in Bezug auf die Fähigkeit der Nutzer, solche Informationen bereitzustellen, z. B. Schließung oder Aussetzung des Kontos eines Nutzers.

Zu § 2 (Auskunft über Daten)

§ 2 setzt auf den Bestimmungen zur Auskunft über Bestandsdaten von § 21 Absatz 2 bis 4 TDDDG auf und erweitert diese Bestimmung um einzelne Aspekte. Betroffene, die Opfer von Hasskriminalität und anderen Straftaten im Internet werden, die häufig mit Persönlichkeitsrechtsverletzungen einhergehen, sollen die Identität des Rechtsverletzers ermitteln können, um gegen diesen gerichtlich vorgehen zu können.

Die Auskunft soll sich anders als bisher unter § 21 Absatz 2 bis 4 TDDDG nicht nur auf Bestandsdaten, sondern neben den Personalien des Nutzers auch auf die IP-Adressen einschließlich der Portnummern zum Zeitpunkt der Verletzung und des vor Entscheidungsverkündung letzten Zugriffs erstrecken. Deshalb wird der Begriff der Daten zusammengefasst.

Dies hat zur Folge, dass neben bestimmten Anbietern von Hosting-Diensten, die regelmäßig Schauplatz digitaler Gewalt darstellen (Diensteanbieter im Sinne dieses Gesetzes), über die IP-Adresse auch Anbieter von Internetzugangsdiensten zur Auskunft verpflichtet werden können, weil sie die relevanten Daten haben, um die IP-Adresse einer konkreten Person zuzuordnen.

Zu Absatz 1

Absatz 1 enthält in Satz 1 die datenschutzrechtliche Ermächtigungsnorm aus § 21 Absatz 2 TDDDG. Satz 2 ermöglicht wie schon § 21 Absatz 2 Satz 2 TDDDG, dass der Auskunftsanspruch und die datenschutzrechtliche Zulässigkeit dieser Auskunft in einem Verfahren beantragt werden können. Auskunftsanspruch und die datenschutzrechtliche Zulässigkeit unterliegen dabei gleichermaßen zwei einschränkenden Voraussetzungen.

Zum einen muss der Dienst, des betroffenen Diensteanbieters zur Begehung einer Rechtsverletzung genutzt werden. Der Dienst muss somit einen Bezug zur Rechtsverletzung aufweisen. Damit wird ausgeschlossen, dass ein Anbieter verpflichtet werden kann, Auskunft über Daten von Nutzern, die über seine Dienste keine Rechtsverletzung begangen haben, zu erteilen. Das betrifft z.B. Besucher einer Website oder Nutzer, die Daten in einer Cloud lediglich lesen, ohne sie weiterzuverbreiten oder zu speichern. Zum anderen wird das Auskunftsverfahren ausdrücklich auf Daten des Rechtsverletzers erstreckt, soweit die Kenntnis der Daten zur privaten Rechtsverfolgung erforderlich ist. Dies betrifft maßgeblich Fälle, in denen der Betroffene von einem Diensteanbieter die Herausgabe der dynamischen IP-Adresse verlangt, die dem Rechtsverletzer zu einem bestimmten Zeitpunkt auf einer Internetplattform zugeordnet war. Da die Herausgabe der Bestandsdaten seitens der Hosting-Dienste häufig wertlos und Nutzungsdaten des Verletzers andernfalls aufwändig und kompliziert über den Weg über eine Strafanzeige und nachfolgender Akteneinsicht erlangt werden können, besteht ein sachliches Bedürfnis für einen derartigen durchsetzbaren zivilrechtlichen Auskunftsanspruch. In der Praxis führt häufig nur die Herausgabe der IP-Adresse und Zugriffszeit zur erfolgreichen privaten Rechtsverfolgung. Die Rechtsprechung hatte vor Inkrafttreten des TDDDG (früher TTDSG) die Gestattung der Erteilung einer solchen Auskunft als Auskunft über Nutzungsdaten gewertet, die aufgrund des Verweises auf § 14 Absatz 2 bis 5 des Telemediengesetzes (TMG) a.F. in § 15 Absatz 5 Satz 4 TMG a.F. zulässig war (OLG Celle, Beschluss vom 07.12.2020, Az. 13 W 80/20, Bl. 28, juris mit Verweis auf BT-Drs. 18/13013, S. 24 zu Nr. 2). Das TDDDG enthält keine dem § 15 Absatz 5 Satz 4 TMG a.F. vergleichbare Vorschrift.

Die datenschutzrechtliche Erlaubnis der Datenherausgabe wird unter den Vorbehalt einer richterlichen Gestattung (Richtervorbehalt) gestellt. Damit wird verfahrensrechtlich sichergestellt, dass es nicht vorschnell zur Herausgabe von Daten kommt, sondern der Herausgabe immer eine richterliche Prüfung und Anordnung vorausgeht. Eine entsprechende Absicherung erscheint in den erfassten Fällen deswegen notwendig, weil die behaupteten Rechtsverletzungen sich oft im Kontext heftiger Debatten und Auseinandersetzungen abspielen können. Sie betrifft einen Kernbereich der Ausübung der durch Artikel 5 Absatz 1 Satz 1 GG geschützten Meinungsfreiheit. Der Richtervorbehalt wird Einschüchterungseffekte auf die Ausübung der Meinungsfreiheit in diesem eng begrenzten Bereich besonders grundrechtssensibler Kommunikation verhindern. Insbesondere sollen Teilnehmer von Debatten und Diskussionen nicht mit der Angst leben müssen, dass Anbieter vorschnell und ohne richterliche Prüfung, gegebenenfalls aufgrund falscher Angaben eines Dritten, ihre Anonymität aufdecken.

Zu Absatz 2

In Absatz 2 werden die Daten genannt, die regelmäßig für die erfolgreiche Durchsetzung der zivilrechtlichen Ansprüche erforderlich sind. Vor dem Hintergrund des Grundsatzes der Datensparsamkeit nach Artikel 5 Absatz 1 Buchstabe c DS-GVO sind im Einzelfall nur einzelne dieser Daten herauszugeben, wenn diese bereits zur Durchsetzung der zivilrechtlichen Ansprüche ausreichen.

Zu Nummer 1

Zunächst sind die Daten erforderlich, die der Anbieter des Hosting--Dienstes gespeichert hat.

Zu Buchstabe a)

Zu den bei dem Diensteanbieter gespeicherten Bestandsdaten gehören die von dem Nutzer hinterlegten Personalien, wie Name, Geburtsdatum, Anschrift und E-Mail-Adresse.

Zu Buchstabe b)

Außerdem ist regelmäßig die Auskunft über die IP-Adresse und die Portnummer erforderlich, die dem Nutzer, der die Rechtsverletzung begangen hat, zum Zeitpunkt der Rechtsverletzung zugewiesen war. Die Portnummer ist hilfreich, wenn verschiedenen Internetnutzern dieselbe IP-Adresse zugewiesen war.

Zu Buchstabe c)

Da die Auskunft möglicherweise zu einem Zeitpunkt geltend gemacht wird, in dem die IP-Adresse und die Portnummer, die dem Nutzer zum Zeitpunkt der Rechtsverletzung zugewiesen war, bereits gelöscht wurde, ist zusätzlich die IP-Adresse und die Portnummer des zum Zeitpunkt der Zustellung der gerichtlichen Anordnung letzten Logins herauszugeben. Auch dies sind erforderliche Daten, um zivilrechtliche Ansprüche geltend zu machen (so auch das LG Berlin zu § 14 Absatz 3 TMG a.F. in Verbindung mit § 15 Absatz 5 S.4 TMG a.F., Beschluss vom 21. Januar 2020 – 27 AR 17/19 –, juris Rn. 38). Dies hat den weiteren Vorteil, dass dadurch auch Rechtsverletzer identifiziert werden können, die zum Zeitpunkt der Rechtsverletzung in einem öffentlichen WLAN eingeloggt waren. Anhand der IP-Adresse, die ihnen während der Rechtsverletzung zugewiesen war, ist eine Identifizierung in diesen Fällen ansonsten nicht möglich.

Zu Nummer 2

In einem zweiten Schritt sind regelmäßig die bei dem Anbieter von Internetzugangsdiensten hinterlegten Bestandsdaten erforderlich, wenn die bei dem Diensteanbieter hinterlegten Daten nicht zur Identifizierung des Nutzers, dem die Rechtsverletzung vorgeworfen wird, ausreichen.

Zu Absatz 3

Absatz 3 übernimmt, ergänzt durch Absatz 1 Satz 3 und § 5, grundsätzlich die verfahrensrechtlichen Regelungen zum Auskunftsverfahren aus § 21 Absatz 3 TDDDG.

Voraussetzung für eine Entscheidung des Gerichts ist ein entsprechender Antrag des Betroffenen. Der Betroffene muss die Tatsachen darlegen, aus denen sich eine Rechtsverletzung im Sinne von § 1 Absatz 1 GgdG ergibt. Hierzu gehört auch die Benennung des jeweiligen Anbieters, durch dessen Dienst die Rechtsverletzung begangen worden sein soll.

Verfahrensrechtliche Regelungen im Zusammenhang mit spezialgesetzlichen Auskunftsansprüchen (insbesondere § 140b Absatz 9 des Patentgesetzes, § 24b Absatz 9 des Gebrauchsmustergesetzes, auch in Verbindung mit § 9 Absatz 2 des Halbleiter-schutzgesetzes, § 19 Absatz 9 des Markengesetzes, § 101 Absatz 9 des Urheberrechtsgesetzes, § 46 Absatz 9 des Designgesetzes und § 37b Absatz 9 des Sortenschutzgesetzes, Artikel 15 DS-GVO) bleiben unberührt.

Zu Absatz 4

Das Gericht soll in einem Verfahren über die Herausgabe sämtlicher erforderlichen Daten entscheiden. Satz 2 enthält die Klarstellung, dass das Gericht eine isolierte Entscheidung über die Gestattung der Auskunft nur dann entscheidet, wenn der Antrag ausdrücklich hierauf beschränkt wurde.

Zu Absatz 5

Die Neuregelung in § 2 ermöglicht auch den Zugriff auf Daten, die vom Schutzbereich des Fernmeldegeheimnisses erfasst sind (vgl. BVerfGE 155, 119, 168). Ein Eingriff in Artikel 10 Absatz 1 GG löst dabei das Zitiergebot aus Artikel 19 Absatz 1 Satz 2 GG aus, unbeschadet der Möglichkeit, dass Artikel 10 GG im Einzelfall nicht betroffen sein mag, weil der fragliche Kommunikationsvorgang diesen grundrechtlichen Schutz nicht genießt.

Zu § 3 (Sicherungsanordnungen)

Zu Absatz 1

Absatz 1 enthält formale und materiell-rechtliche Regelungen zur Sicherung der Drittauskunft und orientiert sich dabei an der Rechtsprechung zum Urheberrecht (vgl. BGH, ZUM 2018, 136). Das für das Auskunftsverfahren zuständige Gericht soll unverzüglich nach Einleitung des Auskunftsverfahrens zur Vermeidung eines drohenden Datenverlusts dem vom Auskunftsersuchen betroffenen Diensteanbieter aufgeben können, vorhandene Daten des Verletzers bis zur endgültigen gerichtlichen Entscheidung über die Verpflichtung zur Auskunftserteilung nicht zu löschen. Dadurch wird verhindert, dass der Auskunftsanspruch durch die Löschung der Daten bis zum rechtskräftigen Abschluss des Gestattungs- und Auskunftsverfahrens seitens des Anbieters vereitelt wird. Die Daten, die für die Identifizierung des Rechtsverletzers benötigt werden, werden ansonsten bestenfalls wenige Tage bei den Anbietern gespeichert.

Außerdem müssen Diensteanbieter eine Kopie des rechtsverletzenden Inhalts erstellen. Diese Kopie soll den Betroffenen die Beweisführung ermöglichen, dass die Rechtsverletzung tatsächlich stattfand, auch wenn der Inhalt in der Zwischenzeit gelöscht wurde. Zwar werden Betroffene in aller Regel ihrem Antrag einen Screenshot beifügen, der die behauptete Rechtsverletzung beweisen soll. Allerdings kann es vorkommen, dass der rechtsverletzende Inhalt bis zur Entscheidung des Gerichts gelöscht wird. In einem solchen Fall ist der Beweisführer regelmäßig dem Vorwurf ausgesetzt, den Screenshot gefälscht oder manipuliert zu haben. Diesem Einwand kann mit der vom Diensteanbieter erstellten Kopie entgegengetreten werden, sodass ein Gericht dem Screenshot einen höheren Beweiswert zusprechen kann.

Zu Absatz 2

Nach Absatz 2 verpflichtet das Gericht den vom Auskunftsverfahren betroffenen Diensteanbieter zur frühzeitigen Übermittlung der Daten und der Kopie des rechtsverletzenden Inhalts ausschließlich an das für das Auskunftsverfahren zuständige Gericht. Die Mitteilungen haben nach Satz 1 unverzüglich zu erfolgen. Im Regelfall ist daher davon auszugehen, dass das Gericht den betroffenen Anbieter eines Hosting-Dienstes zur sofortigen Mitteilung auffordern oder hierfür eine Frist von höchstens wenigen Tagen setzen wird. Denn die Identifizierung eines Verletzers wird in der Regel erfordern, in einem zweiten Schritt die bei dem Internetzugangsanbieter vorhandenen Datensätze über die Zuordnung einer IP-Adresse zu einem bestimmten Kunden zu erfragen. Diese Daten werden beim Internetzugangsanbieter bestenfalls wenige Tage gespeichert. Satz 2 enthält die klarstellende Regelung, dass eine Mitteilung der vom Anbieter gemäß Satz 1 erhaltenen Daten seitens des Gerichts an den Betroffenen nicht statthaft ist.

Zu Absatz 3

Absatz 3 enthält nach Anhängigkeit des Auskunftsantrags die gerichtliche Verpflichtung, eine Sicherungsanordnung gegenüber dem vom Auskunftsersuchen betroffenen Anbieter des Internetzugangsdienstes zu erlassen, um die Löschung der Daten des Nutzers zu verhindern. Dafür hat das Gericht den Internetzugangsdienst zu ermitteln. Dies ist anhand der IP-Adresse über allgemein verfügbare Datenbanken im Internet (wie beispielsweise www.ripe.net) möglich. Die für die Vergabe von öffentlichen IP-Adressen zuständigen Organisationen halten auf ihren Internetseiten eine Suchfunktion bereit, mit Hilfe derer die IP-Adresse einem Anbieter eines Internetzugangsdienstes zugeordnet werden kann. Für Europa ist die RIPE (franz. Réseaux IP Européens) zuständig. Durch gesonderte Sicherungsanordnung an den vom Auskunftsersuchen betroffenen Internetzugangsdienst, die innerhalb eines Auskunftsverfahrens durch Erfassung eines weiteren Verfahrensbeteiligten erfolgen soll, soll im Sinne eines effektiven Rechtsschutzes gewährleistet werden, dass das Auskunftsersuchen nicht beim Anbieter des Internetzugangsdienstes wegen einer dortigen Löschung der Daten leer läuft. Die Identifizierung eines Verletzers wird nämlich regelhaft erfordern, dass beim Internetzugangsanbieter diejenigen Datensätze vorhanden sind, die darüber Aufschluss geben, welchem Kunden des Internetzugangsdienstes eine bestimmte IP-Adresse zu einem bestimmten Zeitpunkt zugeordnet war. Dieser Datensatz wird beim Internetzugangsdienst ebenfalls bestenfalls wenige Tage gespeichert.

Zu Absatz 4

Absatz 4 enthält eine klarstellende Regelung, dass die Anbieter die Daten des Rechtsverletzers verarbeiten dürfen, um ihre Pflichten aus der gemäß den Absätzen 1 bis 3 erlassenen Sicherungsanordnungen zu erfüllen. Daher dürfen sie die Daten zunächst speichern und im Falle einer gerichtlichen Anordnung an das Gericht oder auf gerichtliche Anordnung an den Betroffenen herausgeben. Die gesicherten Daten dürfen zum Zweck der Strafverfolgung auch an die Strafverfolgungsbehörden herausgegeben werden. Für andere Zwecke dürfen die Daten jedoch nicht verwendet werden.

Zu Absatz 5

Absatz 5 enthält die Fiktion, dass mit einem Antrag auf Auskunft nach § 2 zugleich die Anträge auf Erlass einer Sicherungsanordnung nach Absatz 1 und 3 gestellt werden. Die Sicherungsanordnungen nach Absatz 1 und 3 müssen daher nicht eigenständig beantragt werden. Bezüglich der Anordnung nach Absatz 2 ist kein eigenständiger Antrag erforderlich, da diese – anders als die Anordnungen nach Absatz 1 und 3 – als Mitwirkungshandlung zu qualifizieren ist, die nicht gesondert zu beantragen ist.

Zu Absatz 6

Absatz 6 enthält die Regelung, dass die Befugnis zur Speicherung der Daten und der Kopie des rechtsverletzenden Inhalts gemäß Absatz 4 nur bis zu Erfüllung der Pflichten aus der Sicherungsanordnung gilt und die entsprechend gespeicherten Daten nach Wegfall des Speicherungsgrunds vom Anbieter unverzüglich zu löschen sind. Damit wird den datenschutzrechtlichen Grundsätzen der Datensparsamkeit entsprochen. Eine vergleichbare Regelung ist beispielsweise in § 176 Absatz 8 TKG enthalten.

Die Löschung der Daten hat irreversibel zu erfolgen, das heißt, es muss sichergestellt werden, dass auf den Speichermedien keine Fragmente oder gar die gesamten Daten noch vorhanden sind und etwa mit technischen Mitteln wieder rekonstruiert werden können. Die irreversible Löschung der Daten muss daher nach dem Stand der Technik gewährleistet werden.

Zu Absatz 7

Absatz 7 trägt dem Zitiergebot nach Artikel 19 Absatz 1 Satz 2 GG Rechnung.

Zu § 4 (Anspruch auf richterlich angeordnete Sperrung des Nutzerkontos)

§ 4 enthält mit dem Anspruch auf eine richterlich angeordnete Sperrung eines Nutzerkontos ein neues Instrument, um digitale Gewalt zu bekämpfen. Damit soll verhindert werden, dass über einzelne Nutzerkonten eines Internetdienstes fortwährend schwerwiegende Rechtsverletzungen begangen werden. Unter den in Absatz 1 aufgeführten Voraussetzungen kann ein Gericht auf Antrag einer von digitaler Gewalt betroffenen Person einen Anbieter eines sozialen Netzwerks dazu verpflichten, ein spezifisches Nutzerkonto zeitweise zu sperren, um zukünftige Rechtsverletzungen zu verhindern. Die Sperrung des Nutzerkontos muss in jedem Einzelfall verhältnismäßig sein. Da sich der Antrag gegen das soziale Netzwerk richtet, ist es möglich, gegen Nutzer vorzugehen, deren Identität nicht bekannt ist.

Bislang werden Sperrungen der Nutzerkonten von den Anbietern nach eigenem Ermessen in Gestalt von regelmäßig 30-tägigen Teil-Deaktivierungen (der Account wird für diesen Zeitraum im „read-only-modus“ geführt) auf Basis der jeweiligen Nutzungsbedingungen vorgenommen. Diese enthalten zumeist Regelungen zur Möglichkeit der Deaktivierung von Accounts im Falle des Verstoßes gegen Nutzerbedingungen. Folglich gibt es eine Vielzahl von Gerichtsentscheidungen zur Rechtslage im Nutzer-Plattform-Verhältnis nach bereits erfolgter Deaktivierung eines Nutzerkontos durch die Plattform. Zu der Möglichkeit und den Voraussetzungen der Erzwingung einer solchen Sperrung seitens des Betroffenen gibt es hingegen keine Rechtsprechung. Da nicht zwangsläufig davon auszugehen ist, dass ein Vertrag zwischen dem Betroffenen und der Plattform besteht, kann der Betroffene nicht auf die Nutzungsbedingungen verwiesen werden. Auch wenn es in der Rechtsprechung vereinzelt Hinweise darauf gibt, dass eine Sperrung eines Nutzerkontos möglicherweise auch auf § 1004 BGB analog gestützt werden kann (vgl. OLG Rostock, K&R 2021, 671), wurde (auch) diese Anspruchsgrundlage bislang noch nicht als Grundlage für einen solchen Anspruch herangezogen.

Dem Grundsatz der praktischen Konkordanz folgend sind im Rahmen der Ausgestaltung der materiellen und der verfahrensrechtlichen Regelungen sowie deren Auslegung im konkreten Einzelfall die grundrechtlichen Positionen der Beteiligten derart auszugleichen, dass die Grundrechte aller Beteiligten möglichst weitgehend geschützt werden. Mit den hohen Tatbestandsvoraussetzungen in Absatz 1 und in Absatz 3 soll der mit einer Sperrung des Nutzerkontos einhergehende Eingriff in grundrechtliche Positionen, unter anderem in das Recht auf Meinungsfreiheit, auf das erforderliche und angemessene Maß begrenzt werden.

Für den Betroffenen streitet das grundrechtlich gemäß Artikel 2 Absatz 1 GG in Verbindung mit Artikel 1 Absatz 1 Satz 1 GG geschützte allgemeine Persönlichkeitsrecht. Dabei schützt das allgemeine Persönlichkeitsrecht „den engeren persönlichen Lebensbereich und die Erhaltung seiner Grundbedingungen“ (BVerfGE 121, 69/90; 72, 155/170; 96, 56/61), damit der Einzelne „seine Individualität entwickeln und wahren kann“ (BVerfGE 79, 256/268; 117, 202/225). Der Einzelne soll „selbst darüber befinden dürfen, wie er sich gegenüber Dritten oder der Öffentlichkeit darstellen will“ (BVerfGE 63, 131/142). Damit ist auch der Schutz vor Äußerungen verbunden, die sich negativ auf das Ansehen der Person auswirken (BVerfGE 152, 152/186).

Auf Seiten des von einem Sperrersuchen betroffenen Nutzerkontoinhabers ist das Grundrecht auf freie Meinungsäußerung aus Artikel 5 Absatz 1 Satz 1 GG zu berücksichtigen. Artikel 5 Absatz 1 Satz 1 GG gibt das Recht, die eigene Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten. Eine Sperrung des Nutzerkontos greift tief in die grundrechtliche Position des Nutzerkontoinhabers ein, weil ihm für den Zeitraum der Sperrung jegliche Form der Meinungsäußerung über den vom Sperrersuchen betroffenen Dienst untersagt wird. Die Meinungsfreiheit tritt jedoch insbesondere im Falle der Schmähkritik hinter

das allgemeine Persönlichkeitsrecht zurück, wenn also „nicht mehr die Auseinandersetzung in der Sache, sondern die Diffamierung der Person im Vordergrund steht“ (BVerfG NJW 1995, 3303, 3304 – Soldaten sind Mörder).

Auf Seiten des Anbieters des sozialen Netzwerks ist das Grundrecht auf Berufsausübungsfreiheit aus Artikel 12 Absatz 1 Satz 1, 19 Absatz 3 GG und die unternehmerische Freiheit aus Artikel 16 GRC (Grundrechtecharta – Charta der Grundrechte der Europäischen Union (2010/C 83/02)) zu berücksichtigen. Die Berufsausübungsfreiheit aus Artikel 12 Absatz 1 Satz 1 GG sichert die Teilhabe am Wettbewerb, mithin die wirtschaftliche Dispositionsfreiheit. Sie umfasst das Recht der am Markt Tätigen, die Bedingungen ihrer Marktteilhabe selbst festzusetzen. Ferner ist auf Seiten des Diensteanbieters das Grundrecht auf freie Meinungsäußerung aus Artikel 5 Absatz 1 Satz 1 GG und Artikel 11 GRC zu berücksichtigen, denn Artikel 5 Absatz 1 Satz 1 GG schützt auch den Kommunikationsprozess als solchen, weshalb die Mitteilung einer fremden Meinung oder Tatsachenbehauptung selbst dann in den Schutzbereich des Grundrechts fallen kann, wenn der Mitteilende sich diese weder zu eigen macht noch sie in eine eigene Stellungnahme einbindet (vgl. BGH ZUM-RD 2017, 515 Rn. 24 und BGHZ 202, 242 = ZUM-RD 2015, 154 Rn. 28 m. w. N.).

Zu Absatz 1 und Absatz 2

Die Absätze 1 und 2 enthalten Tatbestand und Rechtsfolge einer richterlich angeordneten Sperrung des Nutzerkontos. Es handelt sich dabei um die spezialgesetzliche Kodifizierung eines zivilrechtlichen Unterlassungsanspruchs des von digitaler Gewalt Betroffenen gegen den Anbieter eines sozialen Netzwerks.

Die tatbestandlichen Voraussetzungen in Absatz 1 berücksichtigen, dass mit einer Sperrung eines Nutzerkontos in die Meinungsfreiheit eingegriffen wird. Über die Rechtsverletzung im Sinne des § 1 Absatz 1 hinausgehend muss der Betroffene in seinem Persönlichkeitsrecht schwerwiegend beeinträchtigt sein. Bei der Beurteilung, ob eine Verletzung schwerwiegend ist, kann sich das Gericht unter anderem an der Rechtsprechung zur Geldentschädigung für die Verletzung des allgemeinen Persönlichkeitsrechts orientieren, für die ebenfalls eine schwerwiegende Verletzung verlangt wird. Der Bundesgerichtshof zieht hierfür in ständiger Rechtsprechung neben dem Ausmaß der Verbreitung der Veröffentlichung auch die Nachhaltigkeit und Fortdauer der Interessen- oder Rufschädigung des Betroffenen, den Anlass und Beweggrund des Rechtsverletzers sowie den Grad seines Verschuldens als Kriterien heran (BGH, Urt. v. 22.01.1985, VI ZR 28/83, NJW 1985, 1617 (1619)). In Bezug auf die Beweggründe des Rechtsverletzers kann das Gericht beispielsweise berücksichtigen, ob die Rechtsverletzung bestimmte Diskriminierungsmerkmale erfüllt. Das Grundgesetz verbietet in Artikel 3 Absatz 3, dass jemand wegen des Geschlechtes, der Abstammung, der Rasse, der Sprache, der Heimat und Herkunft, des Glaubens, der religiösen oder politischen Anschauungen oder wegen einer Behinderung benachteiligt wird. Diese Wertentscheidung hat auch Orientierungsfunktion im Strafrecht (vgl. § 46 Absatz 2 StGB) und im Zivilrecht und kann daher für eine schwerwiegende Persönlichkeitsverletzung sprechen. Eine Sperrung des Nutzerkontos kann nur als ultima ratio vom Plattformbetreiber eingefordert werden. Sie muss daher erforderlich sein, um künftige Rechtsverletzungen zu verhindern.

Die Sperrung führt dazu, dass von dem betroffenen Nutzerkonto für einen bestimmten Zeitraum keine Inhalte veröffentlicht, geteilt oder kommentiert werden können. Eine passive Nutzung, ein sogenannter Lesemodus, soll weiterhin möglich sein. Damit wird dem Verhältnismäßigkeitsgrundsatz Rechnung getragen. Die richterliche Anordnung einer dauerhaften Sperrung ist aus Verhältnismäßigkeitsgründen nicht möglich.

Die Sperrung bezieht sich auch auf künftige Konten, die der Nutzer innerhalb des für die Sperrung maßgeblichen Zeitraums eröffnet. Damit wird der Anbieter eines sozialen Netzwerks dazu verpflichtet, Versuche des Nutzerkontoinhabers, eine Sperrung zu umgehen, im Rahmen des für ihn Zumutbaren zu unterbinden. Diesbezüglich soll der Anbieter im

Sperrzeitraum weitere Account-Anmeldungen, bei denen beispielsweise die dem betroffenen Anbieter bekannte Telefonnummer oder E-Mail-Adresse des jeweiligen Nutzers verwendet werden, unterbinden. Dies kann jedoch nur dann verlangt werden, soweit dies dem Anbieter im Einzelfall technisch und wirtschaftlich zumutbar ist.

Zu Absatz 3

Absatz 3 konkretisiert die Anforderungen an die Erforderlichkeit der Sperrung, um künftige Rechtsverletzungen des Nutzers zu verhindern. Die in den Nummern 1 und 2 angeführten Voraussetzungen sind dabei Beispiele, bei dessen Vorliegen regelmäßig von der Erforderlichkeit der Sperrung ausgegangen werden kann. Nummer 3 bietet einen Auffangtatbestand, um dem Gericht zu ermöglichen, auch weitere Anhaltspunkte zu berücksichtigen, die die Erforderlichkeit positiv indizieren können. Sofern keine der Voraussetzungen aus den Nummern 1 bis 3 vorliegt, bedeutet dies im Umkehrschluss nicht automatisch, dass keine Erforderlichkeit gegeben ist. Insbesondere kann bei einer besonders schwerwiegenden Rechtsverletzung die Erforderlichkeit auch ohne positives Vorliegen der in Nummer 1 bis 3 genannten Voraussetzungen gegeben sein. Dabei ist auch zu berücksichtigen, inwieweit der Anbieter eines sozialen Netzwerks eine Verhinderung weiterer Rechtsverletzung durch andere Methoden gewährleisten kann. Wenn der Anbieter den rechtsverletzenden Inhalt bereits gelöscht hat, kann im Einzelfall trotzdem eine Anordnung zur Sperrung des Nutzerkontos erforderlich sein.

Dem Gericht wird damit ausreichend Ermessen eingeräumt, um die Umstände des jeweiligen Einzelfalls berücksichtigen zu können.

Zu Absatz 4

Absatz 4 Satz 1 regelt, dass für die Sperrung des Nutzerkontos eine gerichtliche Anordnung erforderlich ist. Damit wird sichergestellt, dass ein Gericht die grundrechtlichen Positionen miteinander abwägt. Allerdings schließt der Richtervorbehalt nicht aus, dass das soziale Netzwerk ein Nutzerkonto aufgrund eines Verstoßes gegen die allgemeinen Geschäftsbedingungen ohne eine richterliche Anordnung sperrt oder seine Dienste nach Artikel 23 Absatz 1 DSA aussetzt. Dies ist in Absatz 4 Satz 3 klargestellt.

Nach Absatz 4 Satz 2 ordnet das Gericht mit der Sperrung als Nebenfolge zusätzlich an, dass der jeweilige rechtsverletzende Inhalt dauerhaft gesperrt wird, damit die Rechtsverletzung nicht im Lesemodus oder nach der späteren Wiederherstellung des Kontos fortdauert. Andernfalls müsste der Betroffene in einem gesonderten Verfahren die Beseitigung des rechtsverletzenden Inhalts einklagen, obwohl ein Gericht bereits festgestellt hat, dass ein Inhalt auf einem sozialen Netzwerk einen Straftatbestand erfüllt, rechtswidrig ist und zugleich eine schwerwiegende Persönlichkeitsrechtsverletzung vorliegt.

Bei dieser Anordnung durch das Gericht handelt sich nicht um einen selbständigen Löschanspruch des Betroffenen. Solche selbständigen, unabhängig von einer Sperrung geltend gemachten Unterlassungs- und Beseitigungsansprüche gegen das soziale Netzwerk und gegen den jeweiligen Nutzer, der die Rechtsverletzung begangen hat, ergeben sich aus § 1004 BGB analog in Verbindung mit § 823 BGB und müssen in einem gesonderten Verfahren geltend gemacht werden. Eine Kodifizierung der sogenannten Störerhaftung geht daher mit dieser Regelung nicht einher.

Zu § 5 (Verfahren)

Zu Absatz 1

Die Vorschriften über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit (FamFG) gelten für Ansprüche nach diesem Gesetz, die gerichtlich geltend gemacht werden, entsprechend. Dies gilt insbesondere auch für die Vorschrift

des § 32 Absatz 3 FamFG, wonach das Gericht in geeigneten Fällen die Sache mit den Beteiligten im Wege der Bild- und Tonübertragung in entsprechender Anwendung des § 128a ZPO erörtern soll.

Hinsichtlich des Auskunftsverfahrens war dies bereits nach der bisherigen Rechtslage gemäß § 21 Absatz 3 Satz 6 TDDDG der Fall. Dies hat sich bewährt und soll daher beibehalten werden. Nach dem FamFG gilt der Untersuchungsgrundsatz. In den Auskunftsverfahren des geistigen Eigentums ist das FamFG für die Entscheidung über die Zulässigkeit der Herausgabe von Verkehrsdaten ebenfalls anwendbar (vergleiche § 101 Absatz 9 UrhG, § 19 Absatz 9 MarkenG, § 140b Absatz 9 PatentG).

Das FamFG soll auch für Verfahren gelten, in denen eine Sperrung eines Nutzerkontos beantragt wird. Dies hat den Vorteil, dass dadurch derselbe Spruchkörper, der auch über das Auskunftsverfahren entscheidet, über die Sperrung des Nutzerkontos entscheiden kann. Diese Expertise des Spruchköpers kann die Verfahren beschleunigen.

Für das Auskunftsverfahren nach § 2 und für die Sperrung des Nutzerkontos nach § 4 sind die verfahrensrechtlichen Regelungen aus dem FamFG und aus diesem Gesetz abschließend. Sofern Artikel 9 DSA und Artikel 10 DSA etwas abweichendes regeln, finden sie grundsätzlich keine Anwendung, weil das nationale Zivilprozessrecht nach Artikel 9 Absatz 6 DSA und Artikel 10 Absatz 6 DSA unberührt bleibt. Nach § 13 GVG gehören Angelegenheiten der freiwilligen Gerichtsbarkeit ebenfalls zu den Zivilsachen, sodass auch das FamFG unberührt bleibt.

Antragsteller, die befürchten, dass ihre Anonymität durch das Auskunftsverfahren gefährdet wird, können entsprechend der Praxis bei Verfahren nach dem Gewaltschutzgesetz in ihrem Antrag darauf hinweisen, dass die Geheimhaltung des Aufenthaltsortes notwendig ist. Dies gilt auch für den Rechtsverletzer, sofern dieser am Verfahren beteiligt ist. In der Folge stellt das Gericht durch entsprechende Aktenführung sicher, dass die Daten gegenüber den anderen Verfahrensbeteiligten nicht bekannt werden. Nach § 13 Absatz 1 FamFG besteht ein Akteneinsichtsrecht nur, soweit nicht schwerwiegende Interessen eines Beteiligten oder eines Dritten entgegenstehen. Auch die Übermittlung des verfahrenseinleitenden Antrags nach § 23 Absatz 2 FamFG kann im Einzelfall aufgrund schwerwiegender Interessen eines Beteiligten eingeschränkt werden.

Anders als § 21 Absatz 3 TDDDG enthält Absatz 1 keine Abweichung von der allgemeinen Vorschrift des § 81 Absatz 1 Satz 1 FamFG, wonach das Gericht die Kosten des Verfahrens nach billigem Ermessen den Beteiligten ganz oder zum Teil auferlegen kann.

Für die Durchführung des Auskunftsverfahrens nach § 21 Absatz 2 bis 4 TDDDG gibt es bisher keinen Gebührentatbestand. An diesem Rechtszustand soll auch unter Geltung des Gesetzes gegen digitale Gewalt festgehalten werden. Die Gebührenfreiheit soll zusätzlich auch für Verfahren für eine richterlich angeordnete Sperrung des Nutzerkontos gelten.

Zwar hätte die betroffene Person einen Erstattungsanspruch für die angefallenen Kosten, die sie von dem Rechtsverletzer in einem Folgeprozess geltend machen könnte. Ein solcher Erstattungsanspruch könnte jedoch faktisch wertlos sein, wenn der Rechtsverletzer nicht zahlungsfähig ist. Zudem wird es vorkommen, dass trotz einer richterlichen Anordnung im Auskunftsverfahren, nach der Diensteanbieter und Anbieter von Internetzugangsdiensten Daten herauszugeben haben, die Identität des Rechtsverletzers tatsächlich nicht ermittelt werden kann, z.B. weil das Nutzerkonto auf einem sozialen Netzwerk unter einem Decknamen betrieben wird und die IP-Adresse bereits gelöscht ist oder jemand ein öffentliches WLAN genutzt hat. Dann haben die Betroffenen keine Möglichkeit, vom Rechtsverletzer Erstattung der Gerichtskosten zu verlangen.

Zu Absatz 2

Nach § 6 Absatz 2 sind die jeweiligen Diensteanbieter und Anbieter von Internetzugangsdiensten zwingend Beteiligte des Verfahrens. Hierbei handelt es sich um ein Gesetz im Sinne von § 7 Absatz 2 Nummer 2 FamFG.

Zu Absatz 3

Nach Artikel 11 DSA haben Anbieter von Vermittlungsdiensten eine zentrale Kontaktstelle zu benennen, damit sie auf elektronischem Weg unmittelbar mit den Behörden der Mitgliedstaaten kommunizieren können. An die elektronische Kontaktstelle kann zwar nicht zugestellt werden, da sie keinen sicheren Übermittlungsweg im Sinne von § 193a Absatz 1 Nummer 1 ZPO und Artikel 19 Absatz 1 Buchstabe a EuZVO darstellt. Sie kann aber für formlose Mitteilungen an den Anbieter genutzt werden, sofern eine Bekanntgabe nicht geboten ist (§ 15 Absatz 3 FamFG).

Zu Absatz 4

Statthaftes Rechtsmittel gegen die Entscheidung ist die Beschwerde gemäß §§ 58 ff. FamFG. Die Beschwerde ist abweichend von § 63 Absatz 1 FamFG binnen einer Frist von zwei Wochen einzulegen.

Zu § 6 (Beteiligung des Nutzers)

Zu Absatz 1

Der Nutzer, dem eine Rechtsverletzung vorgeworfen wird, ist sowohl im Auskunftsverfahren als auch im Verfahren auf Sperrung seines Accounts als Beteiligter nach § 7 Absatz 2 Nummer 1 FamFG hinzuzuziehen, sofern dem Gericht die Identität der Person bekannt ist.

Zu Absatz 2

Sofern die Identität des betroffenen Nutzers dem Gericht nicht bekannt ist, soll der betroffene Anbieter verpflichtet werden, den Nutzer zu unterrichten. Damit soll gewährleistet werden, dass dem Nutzer die Möglichkeit gewährt wird, bei Gericht eine Stellungnahme einzureichen. Die Schriftform ist abweichend von § 25 FamFG nicht vorgeschrieben. Der Anbieter soll dafür seine eigenen Kommunikationswege nutzen. Es ist dabei nicht erforderlich, dass der betroffene Nutzer seine Identität preisgibt. Aufgrund des Amtsermittlungsgrundsatzes muss das Gericht auch eine Stellungnahme, die anonym abgegeben wurde, berücksichtigen. Das Gericht hat gemäß § 7 FamFG in Verbindung mit Artikel 103 Absatz 1 GG in geeigneter Weise – etwa durch Einholung einer entsprechenden Versicherung des Anbieters – sicherzustellen, dass der betroffene Nutzer über die Einleitung des Verfahrens unterrichtet worden ist.

Zu § 7 (Zivilgesellschaftliche Organisationen)

In Angelegenheiten der freiwilligen Gerichtsbarkeit besteht kein Rechtsanwaltszwang (vergleiche § 10 Absatz 1 FamFG). § 10 Absatz 2 bis 5 FamFG nennt, wer als Bevollmächtigter der Beteiligten auftreten darf. Nach § 10 Absatz 2 Nummer 2 FamFG ist die Vertretung durch Personen mit Befähigung zum Richteramt möglich, wenn die Vertretung nicht im Zusammenhang mit einer entgeltlichen Tätigkeit steht. In Verfahren nach diesem Gesetz sollen abweichend von den in § 10 Absatz 2 FamFG genannten Personen auch zivilgesellschaftliche Organisationen als Bevollmächtigte auftreten dürfen, wenn die Vertretung nicht im Zusammenhang mit einer entgeltlichen Tätigkeit steht und die zivilgesellschaftliche Organisation durch eine Person mit Befähigung zum Richteramt handelt.

Die Vertretung durch zivilgesellschaftliche Organisationen ermöglicht, da eine anwaltliche Vertretung ansonsten nicht vorgesehen ist, zum einen eine Professionalisierung des Verfahrens und wirkt dadurch entlastend auf die Gerichte. Zum anderen erleichtert sie es Personen, die im Internet Rechtsverletzungen erlitten haben, sich auch ohne anwaltliche Vertretung mit kompetenter Vertretung gegen solche Verletzungen zur Wehr zu setzen.

Die Möglichkeit einer Prozessstandschaft oder Verbandsklage hinsichtlich volksverletzender Inhalte wurde geprüft und verworfen. Zum einen können Einzelne als Mitglied eines Kollektivs in ihrem Persönlichkeitsrecht verletzt sein (BGH NJW 1989, 1365 – Kollektive Beleidigung von Soldaten). Zum anderen können auch juristische Personen des Privatrechts selbst Träger von Persönlichkeitsrechten sein (vgl. BGH NJW 2005, 279; BGH NJW 2009, 1872). In beiden Fällen können die Ansprüche auf Auskunft und Accountsperre gerichtlich geltend gemacht werden. Ferner soll das Gesetz gegen digitale Gewalt die individuelle Rechtsdurchsetzung von privatrechtlichen Ansprüchen stärken und erweitern. Bei einer Verbandsklage würde der Verband jedoch fremde Rechte wahrnehmen, ohne von der betroffenen Person dazu beauftragt worden zu sein, so dass es dabei gerade nicht um die Durchsetzung individueller Rechte ginge.

Zu § 8 (Zuständigkeit; Verordnungsermächtigung)

Zu Absatz 1

Nach Absatz 1 ist für Verfahren nach diesem Gesetz, das heißt für das Auskunftsverfahren einschließlich der Sicherungsanordnungen und für Ansprüche, die auf die Sperrung des Nutzerkontos gerichtet sind, sachlich ausschließlich das Landgericht zuständig. Bereits bisher waren für das Auskunftsverfahren nach § 21 Absatz 3 Satz 3 TDDDG die Landgerichte streitwertunabhängig zuständig. Daran soll festgehalten werden, da die Landgerichte bereits mit den Auskunftsverfahren vertraut sind. Außerdem bestehen an den Landgerichten spezialisierte Kammern für Veröffentlichungsstreitigkeiten (vgl. § 72a Absatz 1 Nummer 5 GVG). Diese Kammern verfügen über die erforderliche Expertise bei der für eine Entscheidung erforderlichen Abwägung der Grundrechte.

Eine örtliche Zuständigkeit besteht am Wohnsitz, Sitz oder Ort der Niederlassung des Betroffenen. Damit soll es dem Antragsteller möglichst einfach gemacht werden, seine Ansprüche zeitsparend, kostengünstig und effizient durchzusetzen.

Die internationale Zuständigkeit richtet sich nach Verordnung (EU) 1215/2012 des Europäischen Parlaments und des Rates vom 12. Dezember 2012 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen (EuGVVO oder Brüssel-Ia-Verordnung). Beklagte mit Wohnsitz in einem EU-Mitgliedstaat dürfen in anderen EU-Mitgliedstaaten nur nach den Vorschriften der Verordnung verklagt werden.

In den Verfahren nach §§ 2 und 4 dieses Gesetzes dürfte regelmäßig der deliktische Gerichtsstand nach Artikel 7 Nummer 2 EuGVVO gegeben sein.

Dies gilt für das Auskunftsverfahren jedenfalls dann, wenn ein eigener deliktischer Anspruch gegen den Anbieter geltend gemacht werden kann, etwa aufgrund der Verletzung von Prüf- oder Löschpflichten. In Anlehnung an die Rechtsprechung des BGH zum Auskunftsanspruch gegen Nichtverletzer im Urheberrecht (vgl. BGH Urteil vom 13.10.2022 – I ZR 111/21, MMR 2023, 124, Rn. 48 – DNS-Sperre) ist der deliktische Gerichtsstand im Sinne von Artikel 7 Nummer 2 EuGVVO darüber hinaus bereits dann einschlägig, wenn der Beitrag im Inland über eine Internetseite öffentlich zugänglich ist und der auf Auskunft in Anspruch genommene Anbieter als Mittelsperson einen kausalen Beitrag zur Verbreitung des rechtswidrigen Inhalts geleistet hat. Die Annahme eines deliktischen Gerichtsstands widerspricht nicht den Feststellungen des BGH in seinem Beschluss vom 28. September 2023 (Az. III ZB 25/21), in dem die internationale Zuständigkeit deutscher Gerichte aufgrund

eines deliktischen Gerichtsstandes abgelehnt wurde. In dem der Entscheidung zugrunde liegenden Fall begehrte der Antragsteller gemäß § 21 Absatz 2 bis 4 TTDSG (nunmehr: TDDDG) gegenüber einer Verkaufsplattform mit Sitz in Luxemburg Auskunft darüber, wer ihn bei der Verkaufsplattform „angeschwärzt“ und so die zweitweise Sperrung seines Nutzerkontos herbeigeführt hatte. Die vorgeblichen Falschbehauptungen waren jedoch nicht auf der Plattform des in Anspruch genommenen Anbieter veröffentlicht worden. Dem Anbieter wurden weder etwaige Prüf- oder Sorgfaltspflichtverstöße vorgeworfen, noch wurde ein rechtsverletzender Inhalt im Inland öffentlich zugänglich gemacht, der Anbieter leistete damit auch keinen kausalen Beitrag zu einer Rechtsverletzung. Die Feststellungen des BGH sind daher nicht auf die für das Auskunftsverfahren nach § 2 maßgebliche Fallkonstellation übertragbar, die es Betroffenen ermöglichen soll, gegen im digitalen Raum verbreitete Rechtsverletzungen vorzugehen.

Des Weiteren kommt für das Auskunftsverfahren nach diesem Gesetz auch die besondere Zuständigkeit zugunsten von Verbrauchern nach Artikel 17 Absatz 1 Buchstabe c EuGVVO in Betracht, wenn die Betroffenen im Zeitpunkt der Antragstellung in vertraglicher Beziehung mit dem jeweiligen Anbieter stehen. Im Übrigen ist auch eine rügelose Einlassung nach Artikel 26 Absatz 1 Satz 1 EuGVVO möglich (BGH GRUR 2020, 101, Rn. 15). Hinsichtlich der Sicherungsanordnung nach § 3 dieses Gesetzes, die innerhalb des Auskunftsverfahrens unverzüglich ergehen soll, kann die Zuständigkeit deutscher Gerichte auch mit Artikel 35 EuGVVO begründet werden. Da im Regelfall eine Zuständigkeit in der Hauptsache gegeben ist, wird die Wirkung der Sicherungsanordnung häufig nicht auf den Mitgliedstaat beschränkt sein, in dem sie erlassen wurde (vgl. Artikel 2 Buchstabe a Unterabsatz 2 EuGVVO).

Für den Anspruch auf Kontosperrung wird regelmäßig die besondere Zuständigkeit für deliktische Ansprüche eröffnet sein. Denn hierbei handelt es sich um die spezialgesetzliche Kodifizierung eines zivilrechtlichen Unterlassungsanspruchs des von digitaler Gewalt Betroffenen gegen den Anbieter eines sozialen Netzwerks, mithin um einen deliktischen Anspruch. Somit kann auf Kontosperrung auch vor dem Gericht des Ortes geklagt werden kann, an dem das schädigende Ereignis eingetreten ist oder einzutreten droht (Artikel 7 Nummer 2 EuGVVO).

Für Beteiligte, die keinen Wohnsitz im Sinne des Artikels 63 EuGVVO innerhalb der EU haben, gelten nach Artikel 6 Absatz 1 EuGVVO (wie auch für Sachverhalte ohne grenzüberschreitenden Bezug) die nationalen Zuständigkeitsvorschriften (Dörner in Saenger, Zivilprozessordnung, 10. Auflage 2023, Art. 6 EuGVVO Rn. 3.1).

Zu Absatz 2

Mit Absatz 2 wird ermöglicht, dass der Betroffene nach Abschluss des Auskunftsverfahrens bei demselben Gericht auch die materiellen Beseitigungs-, Unterlassungs- und Schadensersatzansprüche geltend machen kann, welche aus der Rechtsverletzung im Sinne des § 1 Absatz 1 dieses Gesetzes resultieren. Insoweit wird die Möglichkeit für ein One-Stop-Shop-Forum geschaffen. Diese besondere Zuständigkeit gilt nur für die Ansprüche, für die vorher ein Auskunftsverfahren durchgeführt wurde. Dadurch kann, abhängig vom Geschäftsverteilungsplan des Gerichts, dieselbe Kammer eines Landgerichts über weitere Ansprüche entscheiden, die aus der Rechtsverletzung resultieren. Dies dient der Prozessökonomie und fördert eine einheitliche Bewertung desselben Sachverhalts.

Zu Absatz 3

Mit der Möglichkeit, per Verordnung die Auskunftsverfahren einem Landgericht in einem OLG- oder LG-Bezirk zuzuweisen, wird auf die Einrichtung spezialisierter Spruchkörper bei den zuständigen Gerichten hingewirkt. Damit soll die Bündelung von Know-how ermöglicht

werden, sodass Gerichte über rechtsverletzende Sachverhalte im Internet schnell entscheiden können.

Zu § 9 (Inländischer Zustellungsbevollmächtigter)

Zu Absatz 1

§ 9 sieht Vorgaben zur Benennung eines inländischen Zustellungsbevollmächtigten vor.

Die bisher gegen soziale Netzwerke geführten Zivilprozesse haben gezeigt, dass die Zustellung in Drittstaaten mehrere Wochen dauert. Gerade wegen der erheblichen Marktmacht sozialer Netzwerke ist es weiterhin erforderlich, dass zur gerichtlichen Abwehr von Rechtsverletzungen eine schnelle und praktikable Zustellungsvariante besteht, die den Betroffenen ein schnelles rechtliches Einschreiten ermöglicht. Die vormalige Verpflichtung zur Bestellung eines inländischen Zustellungsbevollmächtigten gemäß § 5 Absatz 1 NetzDG hat sich nach Aussagen von Betroffenenorganisationen in der Praxis bewährt und Opfern digitaler Gewalt den Zugang zum Recht erheblich erleichtert.

Abweichend von der bisherigen Regelung in § 5 Absatz 1 NetzDG differenziert § 9 allerdings zwischen Drittstaaten (Absatz 1) und EU-Mitgliedstaaten (Absatz 3). Während die Pflicht zur Benennung eines Zustellungsbevollmächtigten gegenüber Drittstaaten unverändert fortgeführt wird, wird diese Pflicht für EU-Mitgliedstaaten von einer gerichtlichen Anordnung abhängig gemacht. Hintergrund dieser Differenzierung ist das Urteil des EuGH vom 9. November 2023 in der Rechtssache C-376/22. Der EuGH hat entschieden, dass ein Mitgliedstaat dem Anbieter eines Dienstes der Informationsgesellschaft, der in einem anderen Mitgliedsstaat niedergelassen ist, keine abstrakt-generellen Verpflichtungen hinsichtlich der Ausübung des Dienstes auferlegen darf. Anders als der Herkunftsmitgliedstaat dürften andere Mitgliedstaaten nur Maßnahmen ergreifen, die sich auf einen individualisierten Dienst beziehen. Durch die Differenzierung zwischen Drittstaaten und EU-Mitgliedstaaten wird der Rechtsprechung des EuGH entsprochen. Gegenüber in anderen Mitgliedstaaten niedergelassenen Anbietern besteht keine abstrakt-generelle Pflicht zur Bestellung eines Zustellungsbevollmächtigten. Vielmehr ist diese Pflicht von einer individuellen gerichtlichen Anordnung in einem konkreten Gerichtsverfahren abhängig.

In sachlicher Hinsicht wird der Anwendungsbereich auf Gerichtsverfahren vor deutschen Gerichten beschränkt. Die Anwendbarkeit auf aufsichtsrechtliche Verfahren und Bußgeldverfahren entfällt, da in den Artikeln 11 und 13 DSA diesbezüglich ein ausreichendes Instrumentarium zur Verfügung steht.

Zu Absatz 2

An den Zustellungsbevollmächtigten können Zustellungen in Gerichtsverfahren vor deutschen Gerichten wegen Ansprüchen aus der begründeten oder unbegründeten Annahme eines Anspruchs aus einer Rechtsverletzung bewirkt werden. Von dem letzten Fall sind insbesondere Wiederherstellungsklagen erfasst, mit denen die Wiederherstellung eines vom sozialen Netzwerk entfernten Inhaltes begehrt wird oder die Unzulässigkeit einer darauf gestützten Sperrung eines Nutzerkontos geltend gemacht wird.

Die Zustellungsmöglichkeit gilt ebenso für Schriftstücke, die solche Verfahren einleiten oder vorbereiten, und für zivilrechtliche Unterlassungsaufforderungen. c hat. Die Zustellung an den inländischen Briefkasten ermöglicht den rechtsverbindlichen Nachweis, dass und zu welchem Zeitpunkt das soziale Netzwerk von dem angegriffenen Inhalt Kenntnis erlangt hat und deshalb bei positiver Feststellung einer Rechtsverletzung im Fall einer Nicht-Löschung haftet.

Zu Absatz 3

Gegenüber sozialen Netzwerken, die einen Sitz in einem Mitgliedsstaat der Europäischen Union haben, kann ein Gericht in einem Verfahren, das einen Anspruch aus einer Rechtsverletzung zum Gegenstand hat, anordnen, dass sie innerhalb einer angemessenen Frist für ein anhängiges Gerichtsverfahren einen Zustellungsbevollmächtigten im Inland benennen müssen. Dann müsste lediglich diese Anordnung ins Ausland zugestellt werden. Eine Zustellungsfiktion kann hingegen nicht vorgesehen werden (EuGH, Urteil vom 19. Dezember 2012, C-325/11 – Alder). Sonstige gerichtliche Schriftstücke können formlos per E-Mail übermittelt werden, sofern eine Bekanntgabe nicht geboten ist (§ 15 Absatz 3 FamFG). Hierzu kann die elektronische Kontaktstelle der Anbieter (Artikel 11 DSA) genutzt werden.

Zu § 10 (Bußgeldvorschriften)

Zu Absatz 1

Durch Absatz 1 wird ein Verstoß gegen die Verpflichtung des sozialen Netzwerks gemäß § 9 Absatz 1, einen inländischen Zustellungsbevollmächtigten zu benennen, als Ordnungswidrigkeit verfolgbar. Es reicht aus, dass die Verstöße fahrlässig begangen worden sind.

Zu Absatz 2

Absatz 2 enthält den Bußgeldrahmen für die Verstöße gemäß Absatz 1.

Für den Verstoß gegen Absatz 1 ist eine Bußgelddrohung von bis zu fünfhunderttausend Euro vorzusehen. Es handelt sich um die Verletzung einer förmlichen Pflicht, die eine erleichterte Zustellung ermöglichen soll und daher einen geringen Unrechtsgehalt aufweist.

Bei der Festsetzung der konkreten Geldbuße ist die Bedeutung der Ordnungswidrigkeit und der Vorwurf, der den Täter trifft, zu berücksichtigen. Daher ist ein weiter Bußgeldrahmen vorzusehen, der der Verfolgungsbehörde die notwendige Flexibilität bei der Bußgeldbemessung im Einzelfall gibt. In jedem Fall kommt es auf den Unrechtsgehalt der Tat an. Außerdem soll sich die Geldbuße am wirtschaftlichen Vorteil, den der Betroffene durch die begangene Ordnungswidrigkeit erlangt hat, orientieren (vgl. § 17 Absatz 4 OWiG).

Absatz 2 Satz 2 verweist auf § 30 Absatz 2 Satz 3 OWiG und führt dadurch bei der nach § 30 Absatz 1 OWiG möglichen Festsetzung einer Geldbuße gegen die das soziale Netzwerk betreibende juristische Person oder Personenvereinigung dazu, dass sich das Höchstmaß der nach diesem Gesetz angedrohten Geldbuße auf 5.000.000 Euro verzehnfacht. Mit dem Verweis soll der Tatsache Rechnung getragen werden, dass es sich bei den Adressaten der Verpflichtung vielfach um große und besonders finanzstarke Unternehmen handelt. Diese müssen wirksam vor einer Erfüllung der Tatbestände abgeschreckt werden. Auch handelt es sich bei den betroffenen Ordnungswidrigkeitstatbeständen um solche, die typischerweise vom Personenkreis des § 30 Absatz 1 Nummer 1 bis 5 OWiG unter Verletzung von Pflichten, welche das Unternehmen treffen, erfüllt werden.

Zu Absatz 3

Absatz 3 bestimmt als Bußgeldbehörde für die in diesem Gesetz bezeichneten Ordnungswidrigkeiten das Bundesamt für Justiz. Aufgabe des Bundesamtes ist es, Gesetzesverstöße im Rahmen des durch § 47 Absatz 1 OWiG eingeräumten Ermessens zu verfolgen und zu ahnden.

Zu § 11 (Übergangsvorschrift)

Da das NetzDG aufgehoben wird, wird in Anlehnung an die bisherige Übergangsvorschrift aus dem NetzDG geregelt, dass die Zuständigkeit des BfJ für Verfahren, die nach dem

NetzDG eingeleitet wurden, fortbesteht. Dies betrifft sowohl Verfahren, die unter dem NetzDG in seiner bis zum 5. Mai 2024 geltenden Fassung als auch Verfahren, die unter dem NetzDG in seiner ab dem 6. Mai 2024 geltenden Fassung eingeleitet wurden.

Zu Artikel 2 (Änderung des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes)

Artikel 2 enthält die Aufhebung des in § 21 Absatz 2 bis 4 des TDDDG enthaltenen Auskunftsverfahrens nach Schaffung einer entsprechenden Norm in § 2 im Gesetz gegen digitale Gewalt.

Zu Artikel 3 (Änderung des Urheberrechts-Diensteanbieter-Gesetzes)

§ 20 des Urheberrechts-Diensteanbieter-Gesetz vom 31. Mai 2021 (BGBl. I S. 1204, 1215) verweist bisher für die Regelung des Zustellungsbevollmächtigten auf „§ 5 des Netzwerkdurchsetzungsgesetzes“. Dieser Verweis muss angepasst werden.

Zu Artikel 4 (Inkrafttreten, Außerkrafttreten)

Absatz 1 enthält die Regelung über das Inkrafttreten dieses Gesetzes.

Zugleich wird das Netzwerkdurchsetzungsgesetz aufgehoben. Mit Inkrafttreten des DSA ist das Netzwerkdurchsetzungsgesetz bereits weitgehend aufgehoben worden. Allerdings ist § 5 NetzDG, die Regelung zum Zustellungsbevollmächtigten, übergangsweise in Kraft geblieben. Dieser Norm bedarf es aufgrund der Regelung eines Zustellungsbevollmächtigten im Gesetz gegen digitale Gewalt nun nicht mehr.