# Referentenentwurf

## des Bundesministeriums der Justiz und für Verbraucherschutz

## Entwurf eines Gesetzes zur Stärkung des zivilrechtlichen und strafrechtlichen Schutzes vor digitaler Gewalt

## A. Problem und Ziel

Die digitale Transformation hat die Kommunikation und den öffentlichen Diskurs revolutioniert. Es ist Menschen aus aller Welt möglich, miteinander in Kontakt zu treten und Informationen in Echtzeit zu verbreiten, Diskussionen anzustoßen, Meinungen auszutauschen und hierdurch gesellschaftliche Veränderungen zu erwirken. Gerade Soziale Medien können Aufmerksamkeit für wichtige Themen schaffen und Menschen mobilisieren.

Zugleich hat die digitale Transformation einen neuen, virtuellen Raum zur Begehung von Rechtsgutsverletzungen mit digitalen Mitteln eröffnet und damit neue Formen der Gewalt – die „digitale Gewalt“ – ermöglicht.

Erscheinungsformen digitaler Gewalt sind beispielsweise „Hate Speech“ (abwertende, bedrohliche, gewaltverherrlichende oder zu Straftaten aufrufende Beiträge in sozialen Netzwerken, Blogs oder Foren), „Doxing“ (das unerlaubte Veröffentlichen personenbezogener Daten wie Adresse oder Telefonnummer), „Cyberflashing“ (das unerwünschte Zusenden von Bildmaterial, das Gewalttätigkeiten und/oder Pornographie („Dick Pics“) enthält), „Cybergrooming“ (das gezielte Ansprechen und Manipulieren Minderjähriger im Internet, um sexuelle Kontakte anzubahnen oder sexuelle Handlungen zu fördern), bildbasierte sexualisierte Gewalt, „Cyberstalking“ (das Verfolgen, Belästigen und/oder Überwachen einer Person mit digitalen Technologien), „Cybermobbing“ (das Beleidigen, Bedrohen, Bloßstellen oder Belästigen über digitale Kommunikationsmedien) und der Identitätsmissbrauch (das Kommunizieren unter einem Fake-Profil zum Nachteil einer real existierenden Person).

Dieser Entwurf zielt darauf ab, den Schutz vor digitaler Gewalt rechtsgebietsübergreifend zu verbessern. Das Konzept beruht auf zwei Säulen: passgenauen Regelungen zur effektiven Durchsetzung zivilrechtlicher Ansprüche sowie einer Effektivierung des Strafrechts durch Schließung bestehender Strafbarkeitslücken.

Für einen effektiven Schutz der Betroffenen soll die zivilrechtliche Rechtsdurchsetzung wesentlich erleichtert werden: Wenn Betroffene im Netz mit Beleidigungen oder weiteren Straftaten konfrontiert werden, soll ihnen künftig nach dem Gesetz gegen digitale Gewalt ein einfacher durchzuführendes gerichtliches Auskunftsverfahren zur Verfügung stehen – eine wesentliche Voraussetzung für die erfolgreiche Geltendmachung und Durchsetzung von Unterlassungs- und Schadensersatzansprüchen. Wenn die Schwere der Rechtsverletzungen dies rechtfertigt, soll das Gericht auch eine Accountsperre anordnen können. Dabei soll zugleich angeordnet werden können, dass der rechtswidrige Inhalt entfernt wird. Der vorgesehene Richtervorbehalt soll dabei sicherstellen, dass die Strafbarkeit der Äußerung als Voraussetzung für eine Auskunftserteilung eingehend geprüft wird und dadurch das Recht der freien Meinungsäußerung aus Artikel 5 Absatz 1 des Grundgesetzes stets Beachtung findet. Damit schützt das Gesetz gegen digitale Gewalt das Grundrecht noch umfassender als dies bei Sperrungen im Nutzer-Plattform-Verhältnis der Fall ist. Meinungsäußerungen, die nicht strafrechtlich relevant sind, sollen im demokratischen Rechtsstaat anonym bleiben. Eine Auskunft zur Identifizierung soll in diesen Fällen nicht erteilt werden.

Zugleich soll das Strafrecht an die neuen Phänomene des digitalen Zeitalters anpasst werden. Mit diesem Entwurf sollen neue Straftatbestände in das Strafgesetzbuch (StGB) eingeführt werden: Die Herstellung und Verbreitung von sexualisierten Deepfakes soll ebenso erfasst werden wie die Verbreitung von sonstigen (nicht sexualbezogenen) Deepfakes, die die Persönlichkeitsrechte einer anderen Person verletzen. Ferner soll auch die Verwendung von Kommunikations- und Informationstechnik (zum Beispiel von GPS-Trackern) zur heimlichen Überwachung anderer Personen in einer neuen Strafvorschrift geregelt werden.

## B. Lösung

Auf dem Gebiet des Zielrechts soll das Gesetz gegen digitale Gewalt einen effektiven Rahmen für die zivilrechtliche Rechtsdurchsetzung schaffen: 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.

Im Strafrecht soll § 184k StGB zur zentralen Vorschrift zum Schutz der Intimsphäre vor Verletzungen durch Bildaufnahmen erweitert werden. Ferner soll zum Schutz der Persönlichkeitsrechte durch täuschende Inhalte ein neuer § 201b StGB eingefügt werden. Der neue § 202e StGB soll künftig die unbefugte Überwachung mittels Informations- oder Kommunikationstechnik erfassen.

Dieser Entwurf steht im Kontext der gefährdeten rechtzeitigen Erreichung der Ziele der Resolution der Generalversammlung der Vereinten Nationen vom 25. September 2015 „Transformation unserer Welt: die UN-Agenda 2030 für nachhaltige Entwicklung“ (UN-Agenda 2030). Der Entwurf soll insbesondere zur Erreichung der Nachhaltigkeitsziele 5 „Geschlechtergleichstellung erreichen und alle Frauen und Mädchen zur Selbstbestimmung befähigen“ und 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“ beitragen.

## 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. Diese Belastung stellt ein „In“ im Sinne der One in, one out-Regelung der Bundesregierung dar.

### Davon Bürokratiekosten aus Informationspflichten

Der Erfüllungsaufwand in Höhe von 53 000 Euro entfällt gänzlich auf Bürokratiekosten aus Informationspflichten.

## 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 Gesetz gegen digitale Gewalt entstehen den Ländern jährliche Mehrkosten im justiziellen Kernbereich in Höhe von rund 194 000 Euro.

# Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz

## Entwurf eines Gesetzes zur Stärkung des zivilrechtlichen und strafrechtlichen Schutzes vor digitaler Gewalt

**Vom ...**

Der Bundestag hat das folgende Gesetz beschlossen:

## Artikel 1

## Gesetz gegen digitale Gewalt

## (GgdG)

§ 1

**Begriffsbestimmungen**

(1) Als Rechtsverletzung im Sinne dieses Gesetzes gilt jede Tat,

1. für die der Dienst eines Diensteanbieters nach Absatz 2 genutzt wurde,

2. die den Tatbestand der folgenden Vorschriften erfüllt:

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

   b) des § 33 des Gesetzes betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie oder

   c) des § 42 des Bundesdatenschutzgesetzes und

3. die nicht gerechtfertigt ist.

(2) Diensteanbieter im Sinne dieses Gesetzes sind Anbieter von

1. Online-Plattformen im Sinne des Artikels 3 Buchstabe i der Verordnung (EU) 2022/2065,

2. Hosting-Diensten im Sinne des Artikels 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-Diensten im Sinne des Artikels 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.

(4) Soziale Netzwerke im Sinne dieses Gesetzes sind Online-Plattformen im Sinne des Artikels 3 Buchstabe i der Verordnung (EU) 2022/2065, 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.

(6) Nutzer im Sinne dieses Gesetzes ist, wer die Dienste eines Diensteanbieters nach Absatz 2 nutzt.

(7) Ein Nutzerkonto im Sinne dieses Gesetzes ist

1. ein Konto, das einem einzelnen Nutzer für den Zugang zu einem sozialen Netzwerk zugewiesen ist, oder

2. ein Unterkonto, das einem Konto (Nummer 1) untergeordnet ist und die selbstständige Veröffentlichung von Inhalten ermöglicht.

§ 2

**Auskunft über Daten**

(1) Diensteanbieter und Anbieter von Internetzugangsdiensten, deren Dienste zur Begehung einer Rechtsverletzung nach § 1 Absatz 1 genutzt wurden, dürfen Auskunft über die in Absatz 2 genannten 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 gegenüber dem Gericht erforderlich.

(2) Die für das Auskunftsersuchen nach Absatz 1 Satz 1 erforderlichen Daten umfassen

1. die folgenden Daten, die bei dem 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 auf den Dienst unter Angabe der zugrunde liegenden Zeitzone sowie

   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, und

3. eine Kopie des angegriffenen Inhalts.

(3) Der Antragsteller hat

1. die Tatsachen glaubhaft zu machen, aus denen sich ergibt, dass ein ihm unbekannter Nutzer ihm gegenüber eine Rechtsverletzung begangen hat, und

2. seine Absicht zu bekunden, gegen diesen Nutzer zivilrechtliche Ansprüche geltend zu machen.

(4) Über die Auskunftspflicht des im Antrag benannten Diensteanbieters und des Anbieters eines Internetzugangsdienstes sowie über die Zulässigkeit der Auskunftserteilung durch dieselben ist zusammen zu verhandeln und zu entscheiden. Sofern der Antrag nicht ausdrücklich auf die richterliche Anordnung über die Zulässigkeit der Auskunftserteilung nach Absatz 1 Satz 1 beschränkt ist, ist er dahingehend auszulegen, dass er zugleich den Antrag umfasst, über die Verpflichtung zur Auskunftserteilung nach Absatz 1 Satz 2 zu entscheiden.

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

## § 3

## Beweissichernde Anordnungen

(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 unverzüglich an, dass

1. die bei dem Diensteanbieter vorhandenen Daten nach § 2 Absatz 2 Nummer 1 über den Nutzer, der die mögliche Rechtsverletzung begangen hat, nicht gelöscht werden und

2. eine Kopie des angegriffenen Inhalts erstellt wird.

(2) Neben der Anordnung nach Absatz 1 ordnet das Gericht außerdem an, dass ihm der Diensteanbieter die Daten des Nutzers und die Kopie des rechtsverletzenden Inhalts unverzüglich in Textform übermittelt. Eine Mitteilung der nach Satz 1 vom Diensteanbieter erhaltenen Daten an den Antragsteller sowie eine Akteneinsicht des Antragstellers sind nicht statthaft, solange seinem Antrag auf Auskunftserteilung nicht rechtskräftig stattgegeben worden ist.

(3) Nach Eingang der Daten nach Absatz 2 Satz 1 beim Gericht ordnet dieses gegenüber dem von dem Auskunftsersuchen betroffenen Anbieter eines Internetzugangsdienstes zur Vorbereitung der Auskunft nach § 2 Absatz 1 unverzüglich an,

1. die übermittelten Daten nach § 2 Absatz 2 Nummer 1 Buchstabe b und c dem Anschlussinhaber zuzuordnen und

2. die anhand dieser Zuordnung erlangten Daten nach § 2 Absatz 2 Nummer 2 bis zu einer Mitteilung nach Absatz 5 Satz 1 zu speichern.

(4) Daten nach § 2 Absatz 2 dürfen von dem Diensteanbieter und dem Anbieter eines Internetzugangsdienstes, die vom Antrag auf Auskunftserteilung nach § 2 Absatz 1 betroffen sind, zur Erfüllung der Pflichten aus den Anordnungen nach Absatz 1 Nummer 1 und Absatz 3 verarbeitet werden. Diese Daten dürfen zum Zweck der Strafverfolgung auch an die Strafverfolgungsbehörden übermittelt werden. Für andere Zwecke dürfen diese Daten nicht verwendet werden.

(5) Sobald das Auskunftsverfahren rechtskräftig abgeschlossen ist, teilt das Ausgangsgericht 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, so 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.

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

§ 4

**Sperrung von Nutzerkonten in sozialen Netzwerken**

(1) Begeht ein Nutzer in einem sozialen Netzwerk eine Rechtsverletzung, die den Betroffenen in seinem Persönlichkeitsrecht schwerwiegend beeinträchtigt, so kann der Betroffene von dem betroffenen Diensteanbieter verlangen, dass dieser alle dem Diensteanbieter bekannten Nutzerkonten des Nutzers für einen angemessenen Zeitraum sperrt, wenn dies erforderlich ist, um künftige Rechtsverletzungen zu verhindern. Nicht gesperrt werden diejenigen Nutzerkonten, über die die Rechtsverletzung nicht begangen wurde, wenn nicht zu erwarten ist, dass während des nach Satz 1 festzulegenden Zeitraums über diese eine entsprechende Rechtsverletzung begangen werden wird.

(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. Versucht der Nutzer innerhalb des nach Absatz 1 Satz 1 festzulegenden Zeitraums neue Nutzerkonten zu eröffnen und zu betreiben, hat der Diensteanbieter die Eröffnung und den Betrieb während dieses Zeitraums zu unterbinden, soweit ihm dies technisch und wirtschaftlich möglich und zumutbar ist.

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

1. der Nutzer innerhalb einer ihm gesetzten angemessenen Frist keine die Rechtsverletzung nach Absatz 1 Satz 1 betreffende strafbewehrte Unterlassungserklärung abgibt oder diese verweigert,

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 einer Sperrung des Nutzerkontos ist auch zu berücksichtigen, ob das soziale Netzwerk eine mildere Form der Inhaltemoderation anbietet, die geeignet wäre, weitere Rechtsverletzungen wirksam zu verhindern.

(4) Die Sperrung des Nutzerkontos nach Absatz 1 erfolgt nur auf gerichtliche Anordnung, die von dem von der Rechtsverletzung Betroffenen zu beantragen ist. Das Gericht ordnet mit der Sperrung gleichzeitig die Entfernung der rechtsverletzenden Inhalte an. Satz 1 steht der Sperrung eines Nutzerkontos durch den Diensteanbieter auf Verlangen des Betroffenen ohne richterliche Anordnung aufgrund vertraglicher Rechte des

Diensteanbieters gegen den Inhaber des Nutzerkontos oder aufgrund einer Verpflichtung aus Artikel 23 Absatz 1 der Verordnung (EU) 2022/2065 nicht entgegen.

§ 5

**Gerichtliches 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, soweit in diesem Gesetz nicht abweichend geregelt.

(2) Die betroffenen 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) Entscheidungen nach § 2 Absatz 4 sowie § 4 Absatz 4 werden mit Rechtskraft wirksam.

(5) Gegen die erstinstanzliche Endentscheidung 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 hinzuzuziehen, sofern er dem Gericht bekannt ist.

(2) Ist der Nutzer dem Gericht nicht bekannt, so hat es den betroffenen Diensteanbieter zu verpflichten, den Nutzer unverzüglich über die Einleitung des Verfahrens mit folgendem Inhalt zu unterrichten:

1. Angabe des anhängigen Verfahrens auf Auskunftserteilung oder Sperrung des Nutzerkontos,

2. Bezeichnung der angegriffenen Inhalte unter Angabe des jeweiligen Datums der Veröffentlichung,

3. Screenshots der angegriffenen Inhalte,

4. welche Anträge nach den §§ 2 und 4 gestellt worden sind und

5. von dem Gericht gesetzte Frist zur Stellungnahme des Nutzers.

Der Diensteanbieter nach Satz 1 hat die Einreichung der Stellungnahme anonym oder unter einem Pseudonym zu ermöglichen. Der Nutzer ist auf seinen Antrag hin als Beteiligter an dem Verfahren im Verfahren hinzuziehen. Der Diensteanbieter hat dem Gericht zu versichern, dass die Unterrichtung des Nutzers erfolgt ist. Er hat bei ihm eingegangene Stellungnahmen des Nutzers unverzüglich an das Gericht weiterzuleiten.

(3) Die schriftliche Bekanntgabe des Beschlusses gemäß § 41 Absatz 1 Satz 1 und Absatz 2 Satz 4 des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit erfolgt unter Schwärzung der Personalien des Nutzers.

§ 7

**Vertretung durch 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) § 348a der Zivilprozessordnung gilt entsprechend.

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

(4) Für Streitigkeiten über Ansprüche aus Rechtsverletzungen, die zuvor Gegenstand eines Verfahrens über die Sperrung eines Nutzerkontos nach § 4 waren, ist auch das Gericht, welches über den Antrag auf Sperrung des Nutzerkontos entschieden hat, sachlich und örtlich zuständig.

(5) Die Landesregierungen werden ermächtigt, durch Rechtsverordnung die Anträge, die nach diesem Gesetz gestellt werden, einem Landgericht für die Bezirke mehrerer Landgerichte zuzuweisen. Die Landesregierungen können die Ermächtigung durch Rechtsverordnung auf die Landesjustizverwaltungen übertragen.

§ 9

**Inländischer Zustellungsbevollmächtigter**

(1) Diensteanbieter, die soziale Netzwerke betreiben, bei denen kein Mitgliedstaat der Europäischen Union Sitzland ist oder als Sitzland gilt, haben spätestens mit Anbieten des Dienstes im Inland einen Zustellungsbevollmächtigten 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, sowie zivilrechtliche Anspruchsschreiben.

(3) Ein Gericht kann gegenüber Diensteanbietern, die soziale Netzwerke betreiben, die ihren 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 dem Inkrafttreten nach Artikel 14 dieses Gesetzes] geltenden Fassung des Netzwerkdurchsetzungsgesetzes vom 1. September 2017 (BGBl. I S. 3352), das zuletzt durch Artikel 12 des Gesetzes vom … [einsetzen: Ausfertigungsdatum und Fundstelle dieses Gesetzes] geändert worden ist, für Bußgeldverfahren bleibt bis zum Abschluss der Verfahren bestehen.

# Artikel 2

## Änderung des Strafgesetzbuches[1]

Das Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch Artikel 13 des Gesetzes vom 11. Januar 2026 (BGBl. 2026 I Nr. 9) geändert worden ist, wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:

   a) Die Angabe zu § 184k wird durch die folgende Angabe ersetzt:

   „§ 184k Verletzung der Intimsphäre durch Bildaufnahmen“.

   b) Nach der Angabe zu § 201a wird die folgende Angabe eingefügt:

   „§ 201b Verletzung von Persönlichkeitsrechten durch täuschende Inhalte“.

   c) Nach der Angabe zu § 202d wird die folgende Angabe eingefügt:

   „§ 202e Unbefugte Überwachung mittels Informations- oder Kommunikationstechnik“.

2. § 127 Absatz 1 Satz 2 Nummer 2 Buchstabe a wird durch den folgenden Buchstaben a ersetzt:

   „a) den §§ 86, 86a, 91, 130, 147 und 148 Absatz 1 Nummer 3, den §§ 149, 152a und 176a Absatz 2, § 176b Absatz 2, § 180 Absatz 2, § 184b Absatz 1, § 184c Absatz 1, § 184l Absatz 1 und 3, den §§ 202a, 202b, 202c, 202d, 202e, 232 und 232a Absatz 1, 2, 5 und 6, nach § 232b Absatz 1, 2 und 4 in Verbindung mit § 232a Absatz 5, nach den §§ 233, 233a, 236, 259 und 260, nach § 261 Absatz 1 und 2 unter den in § 261 Absatz 5 Satz 2 genannten Voraussetzungen sowie nach den §§ 263, 263a, 267, 269, 275, 276, 303a und 303b,“.

3. § 184b Absatz 1 Satz 1 Nummer 3 wird durch die folgende Nummer 3 ersetzt:

   „3. einen kinderpornographischen Inhalt, der ein tatsächliches oder wirklichkeitsnahes Geschehen wiedergibt, herstellt oder“.

4. § 184c Absatz 1 Nummer 3 wird durch die folgende Nummer 3 ersetzt:

   „3. einen jugendpornographischen Inhalt, der ein tatsächliches oder wirklichkeitsnahes Geschehen wiedergibt, herstellt oder“.

5. § 184k wird durch den folgenden § 184k ersetzt:

---

[1] Artikel 2 dient der Umsetzung der Richtlinie (EU) 2024/1385 des Europäischen Parlaments und des Rates vom 14. Mai 2024 zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt (ABl. L, 2024/1385, 24.5.2024).

„§ 184k

Verletzung der Intimsphäre durch Bildaufnahmen

(1) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer unbefugt eine Bildaufnahme herstellt oder einer dritten Person zugänglich macht, die

1. eine sexuelle Handlung einer anderen Person abbildet,

2. die unbekleideten Genitalien, das unbekleidete Gesäß oder die unbekleidete weibliche Brust einer anderen Person abbildet,

3. in sexuell bestimmter Weise die bekleideten Genitalien, das bekleidete Gesäß oder die bekleidete weibliche Brust einer anderen Person abbildet, oder

4. mittels eines Computerprogramms so verändert, umgestaltet oder mit weiteren Inhalten verbunden wurde, dass der Anschein erweckt wird, dass sexuelle Handlungen oder die unbekleideten Genitalien, das unbekleidete Gesäß oder die unbekleidete weibliche Brust einer anderen Person abgebildet seien.

(2) Ebenso wird bestraft, wer eine Bildaufnahme, die die Nacktheit einer anderen Person unter achtzehn Jahren zum Gegenstand hat,

1. herstellt oder anbietet, um sie einer dritten Person gegen Entgelt zu verschaffen, oder

2. sich oder einer dritten Person gegen Entgelt verschafft.

(3) Die Tat wird nur auf Antrag verfolgt, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

(4) Die Absätze 1 und 2 gelten nicht für Handlungen, die in Wahrnehmung überwiegender berechtigter Interessen erfolgen, namentlich der Kunst oder der Wissenschaft, der Forschung oder der Lehre, der Berichterstattung über Vorgänge des Zeitgeschehens oder der Geschichte oder ähnlichen Zwecken dienen.

(5) Die Bildträger sowie Bildaufnahmegeräte oder andere technische Mittel, die der Täter oder Teilnehmer verwendet hat, können eingezogen werden. § 74a ist anzuwenden.“

6. § 201a wird wie folgt geändert:

a) Absatz 3 wird durch den folgenden Absatz 3 ersetzt:

„(3) Absatz 1 Nummer 2 und 3, auch in Verbindung mit Absatz 1 Nummer 4 oder 5, sowie Absatz 2 gelten nicht für Handlungen, die in Wahrnehmung überwiegender berechtigter Interessen erfolgen, namentlich der Kunst oder der Wissenschaft, der Forschung oder der Lehre, der Berichterstattung über Vorgänge des Zeitgeschehens oder der Geschichte oder ähnlichen Zwecken dienen.“

b) Absatz 4 wird gestrichen.

c) Absatz 5 wird zu Absatz 4.

7. Nach § 201a wird der folgende § 201b eingefügt:

„§ 201b

Verletzung von Persönlichkeitsrechten durch täuschende Inhalte

(1) Wer einer dritten Person einen mittels eines Computerprogramms erstellten oder veränderten Inhalt (§ 11 Absatz 3), der den Anschein erweckt, ein tatsächliches Geschehen in Bezug auf eine andere Person wiederzugeben, und der geeignet ist, dem Ansehen dieser Person erheblich zu schaden, unbefugt zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist. Dies gilt auch dann, wenn sich die Tat nach Satz 1 auf eine verstorbene Person bezieht.

(2) § 201a Absatz 3 und 4 gilt entsprechend.“

8. Nach § 202d wird der folgende § 202e eingefügt:

„§ 202e

Unbefugte Überwachung mittels Informations- oder Kommunikationstechnik

Wer den Aufenthaltsort oder die Tätigkeit einer anderen Person wiederholt oder ständig mittels Informations- oder Kommunikationstechnik unbefugt überwacht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Satz 1 ist nur anzuwenden, wenn die Handlung wahrscheinlich dazu führt, dass dieser Person schwerer Schaden zugefügt wird.“

9. § 205 wird wie folgt geändert:

a) Absatz 1 wird durch den folgenden Absatz 1 ersetzt:

„(1) In den Fällen des § 201 Absatz 1 und 2 sowie der §§ 202, 203 und 204 wird die Tat nur auf Antrag verfolgt. Dies gilt auch in den Fällen der §§ 201a, 201b, 202a, 202b, 202d und 202e, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.“

b) In Absatz 2 Satz 4 wird nach der Angabe „Satz 2“ die Angabe „sowie des § 201b Absatz 1 Satz 2“ eingefügt.

## Artikel 3

## Änderung des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes

Das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz vom 23. Juni 2021 (BGBl. I S. 1982; 2022 I S. 1045), das zuletzt durch Artikel 10 des Gesetzes vom 9. Januar 2026 (BGBl. 2026 I Nr. 7) geändert worden ist, wird wie folgt geändert:

§ 21 wird wie folgt geändert:

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

2. Die Absätze 2 bis 4 werden gestrichen.

## Artikel 4

## Änderung der Strafprozessordnung

Die Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 3 des Gesetzes vom 11. Januar 2026 (BGBl. 2026 I Nr. 9) geändert worden ist, wird wie folgt geändert:

§ 374 Absatz 1 Nummer 2a wird durch die folgenden Nummern 2a und 2b ersetzt:

„2a. eine Verletzung der Intimsphäre durch Bildaufnahmen (§ 184k Absatz 1 des Strafgesetzbuches) oder eine Verletzung des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten durch Bildaufnahmen (§ 201a Absatz 1 und 2 des Strafgesetzbuches),

2b. eine Verletzung von Persönlichkeitsrechten durch täuschende Inhalte (§ 201b des Strafgesetzbuches),“.

## Artikel 5

## Änderung des Bundeszentralregistergesetzes

Das Bundeszentralregistergesetz in der Fassung der Bekanntmachung vom 21. September 1984 (BGBl. I S. 1229, 1985 I S. 195), das zuletzt durch Artikel 5 des Gesetzes vom 19. Juli 2024 (BGBl. 2024 I Nr. 245) geändert worden ist, wird wie folgt geändert:

In § 32 Absatz 5, § 34 Absatz 2 in der Angabe vor Nummer 1, § 41 Absatz 2 Satz 2, § 46 Absatz 1 Nummer 1a in der Angabe vor Buchstabe a und § 69 Absatz 4 wird jeweils nach der Angabe „201a Absatz 3“ die Angabe „in der bis einschließlich … [einsetzen: Datum des Tages vor dem Tag des Inkrafttretens nach Artikel 14 dieses Gesetzes] geltenden Fassung“ eingefügt.

## Artikel 6

## Änderung des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit

Das Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit vom 17. Dezember 2008 (BGBl. I S. 2586, 2587), das zuletzt durch Artikel 3 des Gesetzes vom 3. Februar 2026 (BGBl. 2026 I Nr. 27) geändert worden ist, wird wie folgt geändert:

In § 158a Absatz 2 Satz 2 wird nach der Angabe „201a Absatz 3“ die Angabe „in der bis einschließlich … [einsetzen: Datum des Tages vor dem Tag des Inkrafttretens nach Artikel 14 dieses Gesetzes] geltenden Fassung“ eingefügt.

## Artikel 7

## Änderung des Urheberrechts-Diensteanbieter-Gesetzes

Das Urheberrechts-Diensteanbieter-Gesetz 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 geändert:

§ 20 wird durch den folgenden § 20 ersetzt:

„§ 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 8

## Änderung des Achten Buches Sozialgesetzbuch

Das Achte Buch Sozialgesetzbuch – Kinder- und Jugendhilfe – in der Fassung der Bekanntmachung vom 11. September 2012 (BGBl. I S. 2022), das zuletzt durch Artikel 2 des Gesetzes vom 3. April 2025 (BGBl. 2025 I Nr. 107) geändert worden ist, wird wie folgt geändert:

In § 72a Absatz 1 Satz 1 wird nach der Angabe „201a Absatz 3“ die Angabe „in der bis einschließlich … [einsetzen: Datum des Tages vor dem Tag des Inkrafttretens nach Artikel 14 dieses Gesetzes] geltenden Fassung“ eingefügt.

## Artikel 9

## Änderung des Neunten Buches Sozialgesetzbuch

Das Neunte Buch Sozialgesetzbuch vom 23. Dezember 2016 (BGBl. I S. 3234), das zuletzt durch Artikel 13 des Gesetzes vom 16. Januar 2026 (BGBl. 2026 I Nr. 14) geändert worden ist, wird wie folgt geändert:

In § 124 Absatz 2 Satz 3 wird nach der Angabe „201a Absatz 3“ die Angabe „in der bis einschließlich … [einsetzen: Datum des Tages vor dem Tag des Inkrafttretens nach Artikel 14 dieses Gesetzes] geltenden Fassung“ eingefügt.

## Artikel 10

## Änderung des Zwölften Buches Sozialgesetzbuch

Das Zwölfte Buch Sozialgesetzbuch – Sozialhilfe – (Artikel 1 des Gesetzes vom 27. Dezember 2003, BGBl. I S. 3022, 3023), das zuletzt durch Artikel 15 des Gesetzes vom 16. Januar 2026 (BGBl. 2026 I Nr. 14) geändert worden ist, wird wie folgt geändert:

In § 75 Absatz 2 Satz 3 wird nach der Angabe „201a Absatz 3“ die Angabe „in der bis einschließlich … [einsetzen: Datum des Tages vor dem Tag des Inkrafttretens nach Artikel 14 dieses Gesetzes] geltenden Fassung“ eingefügt.

## Artikel 11

## Änderung des Telekommunikationsgesetzes

Das Telekommunikationsgesetz vom 23. Juni 2021 (BGBl. I S. 1858), das zuletzt durch Artikel 12 des Gesetzes vom 9. Januar 2026 (BGBl. 2026 I Nr. 7) geändert worden ist wird wie folgt geändert:

§ 174 Absatz 5 wird wie folgt geändert:

1. In Nummer 8 wird die Angabe „unterstützen.“ durch die Angabe „unterstützen,“ ersetzt.

2. Nach Nummer 8 wird die folgende Nummer 9 eingefügt:

   „9. den von einer Rechtsverletzung nach § 1 Absatz 1 des Gesetzes gegen digitale Gewalt Betroffenen, soweit dies zur Durchsetzung zivilrechtlicher Ansprüche erforderlich und nach § 2 Absatz 1 Satz 3 des Gesetzes gegen digitale Gewalt richterlich angeordnet worden ist.“

## Artikel 12

## Änderung des Netzwerkdurchsetzungsgesetzes

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, wird wie folgt geändert:

Nach § 6 wird der folgende § 7 eingefügt:

„§ 7

Außerkrafttreten

Dieses Gesetz tritt mit Ablauf des … [einsetzen: Datum des Tages vor dem ersten Tag des auf die Verkündung folgenden Quartals] außer Kraft.“

## Artikel 13

## Einschränkung eines Grundrechts

Das Fernmeldegeheimnis (Artikel 10 Absatz 1 des Grundgesetzes) wird nach Maßgabe des Artikels 11 Nummer 2 (§ 174 Absatz 5 Nummer 9 des Telekommunikationsgesetzes) eingeschränkt.

## Artikel 14

## Inkrafttreten

Dieses Gesetz tritt am … [einsetzen: Datum des ersten Tages des auf die Verkündung folgenden Quartals] in Kraft.

**EU-Rechtsakte:**

1. 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 vom 29. April 2024 (ABl. L, 2024/1309, 8.5.2024; 2024/90315, 24.5.2024) geändert worden ist

2. 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 310 vom 1.12.2023, S. 17; L, 2025/90880, 5.11.2025), die zuletzt durch die Delegierte Verordnung (EU) 2025/2050 vom 1. Juli 2025 (ABl. L, 2025/2050, 9.10.2025) geändert worden ist

# Begründung

## A. Allgemeiner Teil

### I. Zielsetzung und Notwendigkeit der Regelungen

Ein relevanter Teil der öffentlichen, politischen und privaten Kommunikation findet mittlerweile im virtuellen Raum statt. Insbesondere in sozialen Netzwerken kommt es jedoch immer wieder zu rechtswidrigen Äußerungen oder Inhalten wie Bedrohungen, Beleidigungen oder bildbasierter sexualisierter Gewalt wie KI-generierten pornographischen Deepfakes.

Diese Phänomenbereiche werden in der Regel dem Oberbegriff „digitale Gewalt“ zugerechnet. Digitale Gewalt ist allerdings weder einheitlich noch abschließend definiert. Es handelt sich um keinen eigenständigen Rechtsbegriff, sondern um einen Sammelbegriff aus dem gesellschaftlichen und politischen Diskurs für Handlungen im digitalen Raum oder mit digitalen Mitteln, die in rechtlich geschützte Güter, oft Persönlichkeitsrechte, eingreifen. Kennzeichnend ist die Nutzung digitaler Kommunikationsmittel und informationstechnischer Infrastrukturen. Nach der Gewaltschutzstrategie der Bundesregierung (Strategie der Bundesregierung zur Prävention und Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt nach der Istanbul-Konvention 2025-2030, Seite 81) umschreiben die Begriffe „Cybergewalt“/„digitale Gewalt“ Persönlichkeitsrechtsverletzungen, die im digitalen Raum begangen werden. Sie umfassen insbesondere die Nutzung von Informations- und Kommunikationstechnologien zur Herabsetzung, Belästigung, Diskriminierung, Nötigung und Verursachung oder Androhung von Gewalt gegen andere Menschen, die zu körperlichem, sexuellem oder wirtschaftlichem Schaden oder psychologischem Leid führt (oder führen kann) und die Ausnutzung der Umstände, Merkmale oder Schwachstellen der Person einschließen kann. Digitale und analoge Gewalt verstärken und ergänzen sich oft gegenseitig. Erscheinungsformen digitaler Gewalt sind insbesondere

– „Hate Speech“, also abwertende, bedrohliche, gewaltverherrlichende oder zu Straftaten aufrufende Beiträge in sozialen Netzwerken, Blogs oder Foren, die unter anderem als öffentliche Aufforderung zu Straftaten (§ 111 des Strafgesetzbuches – StGB), als Störung des öffentlichen Friedens durch Androhung von Straftaten (§ 126 StGB), als Volksverhetzung (§ 130 StGB), als Anleitung zu Straftaten (§ 130a StGB), als Belohnung oder Billigung von Straftaten (§ 140 StGB), als Beschimpfung von Bekenntnissen, Religionsgesellschaften und Weltanschauungsvereinigungen (§ 166 StGB) oder als Ehrdelikt (§§ 185 und folgende StGB) strafbar sein können;

– „Identitätsmissbrauch“ zum Nachteil des Betroffenen, also das Kommunizieren unter einem Fake-Profil einer real existierenden Person, das unter anderem nach § 185 StGB (Beleidigung), § 238 Absatz 1 Nummer 6 bis 8 StGB (Nachstellung), § 42 des Bundesdatenschutzgesetzes (BDSG) oder § 33 KunstUrhG strafbar sein kann;

– „Doxing“, also das unerlaubte Veröffentlichen personenbezogener Daten wie Adresse oder Telefonnummer, das insbesondere als gefährdendes Verbreiten personenbezogener Daten (§ 126a StGB) oder nach § 42 BDSG strafbar sein kann;

– „Cyberflashing“, also das unerwünschte Zusenden von Bildmaterial, das Gewalttätigkeiten und/oder Pornographie („Dick Pics“) enthält, und insbesondere als Gewaltdarstellung (§ 131 StGB) oder als Pornographiedelikt (§§ 184 bis 184c StGB) strafbar sein kann;

– „Cybergrooming“, also das gezielte Ansprechen und Manipulieren Minderjähriger im Internet, um sexuelle Kontakte anzubahnen oder sexuelle Handlungen zu fordern, das insbesondere als sexueller Missbrauch von Kindern ohne Körperkontakt mit dem Kind (§ 176a StGB) oder als Vorbereitung des sexuellen Missbrauchs von Kindern (§ 176b StGB) strafbar sein kann;

– die bildbasierte sexualisierte Gewalt, die unter anderem die Erscheinungsformen der Rachepornographie („Revenge Porn“), also das nicht-einvernehmliche Verbreiten intimer Aufnahmen, ferner das nicht-einvernehmliche Herstellen von intimen Bildern und Videos, das Verbreiten künstlich generierter oder manipulierter intimer Bilder oder Videos („sexualisierte Deepfakes“) und die Drohung mit einem Verbreiten entsprechender intimer Inhalte („Sextortion“) umfasst und unter anderem als Verletzung des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten durch Bildaufnahmen (§ 201a StGB), als Bedrohung (§ 241 StGB) oder nach § 33 des Gesetzes betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (KunstUrhG) strafbar sein kann;

– „Cyberstalking“, also das Verfolgen, Belästigen und/oder Überwachen einer Person mit digitalen Technologien, das unter anderem als Nachstellung (§ 238 StGB) strafbar sein kann; und

– „Cybermobbing“, also das Beleidigen, Bedrohen, Bloßstellen oder Belästigen über digitale Kommunikationsmedien, das unter anderem als Ehrdelikt (§§ 185 und folgende StGB) oder Bedrohung (§ 241 StGB) strafbar sein kann.

Digitale Gewalt führt nicht nur zu gravierenden physischen und psychischen Belastungen, sondern stellt auch grundlegende Menschenrechte, wie das Recht auf körperliche und seelische Unversehrtheit sowie die sexuelle Selbstbestimmung, infrage. Digitale Gewalt unterscheidet sich in ihrer Wirkung und ihre Wirkweite grundlegend von analoger Gewalt. Sie kann sich in kürzester Zeit global verbreiten, bleibt oft dauerhaft verfügbar und entzieht sich der vollständigen Kontrolle der Betroffenen, was die Belastung für Betroffene erheblich verstärkt. Zudem sind digitale und analoge Lebenswelten eng miteinander verknüpft, sodass Übergriffe im Netz reale psychische, soziale und körperliche Folgen haben können. Die häufige Anonymität, kollektive Dynamiken und algorithmische Verstärkung erschweren eine rein individuelle oder rechtliche Ahndung. Gleichzeitig sind bestimmte gesellschaftliche Gruppen überproportional betroffen, was bestehende Diskriminierungen vertieft.

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. Das gegenwärtige Recht wird diesem Anspruch nicht hinreichend gerecht. Insbesondere Betroffene von Persönlichkeitsrechtsverletzungen im digitalen Raum 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, spezifisch auf die Besonderheiten des Internets ausgerichteten 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 insbesondere 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.

Zum Ausgleich der unterschiedlichen Grundrechtspositionen und Gewährleistung der durch Artikel 5 Absatz 1 des Grundgesetzes (GG) geschützten Meinungsfreiheit, müssen Instrumente, die den Betroffenen an die Hand gegeben werden, um sich gegen solche Verletzungen zu wehren, hohe tatbestandliche Hürden und verfahrensmäßige Absicherungen (zum Beispiel einen Richtervorbehalt) vorsehen.

### 1. Zivilrecht

Der zivilrechtliche Teil des Entwurfs (Gesetz gegen digitale Gewalt) erfasst bestimmte strafrechtlich relevante Persönlichkeitsrechtsverletzungen, die mittels Online-Plattformen oder (sonstigen) Hosting-Diensten begangen werden. Das allgemeine Persönlichkeitsrecht als Rahmenrecht schützt die soziale Geltung und die persönliche Integrität auch vor jenen Handlungen, die mittels informationstechnischer Infrastrukturen auf die Herabsetzung oder psychische Destabilisierung von Personen abzielen. Die Besonderheit liegt hierbei in der digitalen Begehungsweise: Durch die Ubiquität und Dauerhaftigkeit digitaler Inhalte erfahren Eingriffe in rechtlich geschützte Güter oft eine Intensivierung, die über analoge Beleidigungen oder Belästigungen hinausgeht.

Das Gesetz gegen digitale Gewalt erfasst Verletzungen des allgemeinen Persönlichkeitsrechts und sonstige Rechtsgutsverletzungen dann, wenn sie zugleich ein Strafgesetz verletzen; insoweit wird auf die Darstellung der einzelnen Phänomene und die in Betracht kommende Straftatbestände unter A.I. Bezug genommen.

Die Durchsetzung von Ansprüchen aus § 823 des Bürgerlichen Gesetzbuches (BGB) oder § 1004 BGB analog im Kontext mit digitaler Gewalt stößt in der Praxis oft auf erhebliche Hürden. Ein zentrales Hindernis ist die Identifizierung der schädigenden Person: Da die Täter oft unter Pseudonymen bei den Diensteanbietern registriert sind, bleibt dem Betroffenen die für eine Klage notwendige ladungsfähige Anschrift ohne Schaffung einer gerichtlichen Hilfe verborgen. Betroffene sind daher häufig auf kostspielige und langwierige Vorbereitungen angewiesen, die das Kosten-Nutzen-Verhältnis einer Klage nach § 823 BGB oder § 1004 BGB analog insbesondere bei Privatpersonen ins Negative verkehren. In der aktuellen Rechtspraxis führt das Fehlen der Nutzerdaten dazu, dass Betroffene von digitaler Gewalt oft den Umweg über das Strafverfahren wählen müssen, bevor sie eine zivilrechtliche Klage erheben können. Betroffene erstatten deshalb Strafanzeige – verbunden mit der Hoffnung, zu einem späteren Zeitpunkt mittels Akteneinsicht die von den Strafverfolgungsbehörden ermittelte Identität des Täters zu erfahren. Allerdings: Erst wenn die Strafverfolgungsbehörden die Daten (zum Beispiel über eine Bestandsdatenabfrage anhand der IP-Adresse) erhoben haben, kann ein Rechtsanwalt über § 406e der Strafprozessordnung (StPO) Akteneinsicht beantragen, um den Namen und die Anschrift für eine zivilrechtliche Klage nach § 823 BGB oder § 1004 BGB analog zu erfahren. Dieser Weg über die Ermittlungsbehörden und die anschließende Akteneinsicht ist jedoch mit erheblichen Hürden verbunden. Zwar gebietet das Legalitätsprinzip, dass die Ermittlungsbehörden bei einem Anfangsverdacht tätig werden müssen. Als Ausnahme vom Legalitätsprinzip erlaubt es das Opportunitätsprinzip jedoch, in gewissen Fällen von der Verfolgung abzusehen oder auf den Privatklageweg zu verweisen. Hinzu tritt der Faktor Zeit: Inhalte im Internet können in kürzester Zeit vervielfältigt werden oder von weiteren Nutzerinnen und Nutzern heruntergeladen worden sein, sodass ein erhebliches Interesse an einer möglichst schnellen Löschung besteht.

Das Gesetz gegen digitale Gewalt soll es Betroffenen von bestimmten Persönlichkeitsrechtsverletzungen daher erleichtern, Auskunft über die Identität der Rechtsverletzer zu erhalten, um in einem zivilrechtlichen Verfahren Ansprüche geltend machen zu können.

Darüber hinaus soll mit der Schaffung eines Anspruchs auf Accountsperre den Betroffenen ein einfaches und kostengünstiges Mittel an die Hand gegeben werden, sich bei scherwiegenden Fällen digitaler Gewalt vor wiederholten Begehungen zu schützen. Mit der Sperrung soll verhindert werden, dass über einzelne Nutzerkonten eines Internetdienstes fortwährend schwerwiegende Rechtsverletzungen begangen werden. 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 „Lesemodus“ 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 – soweit ersichtlich – 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. Außerhalb eines Vertrages dürfte ein Anspruch auf Accountsperre auch auf § 1004 BGB analog gestützt werden können (vergleiche Hinweisbeschluss des OLG Rostock, K&R 2021, 671), wenn dem Anbieter bekannt ist, dass ein Account für Rechtsverletzungen genutzt wird und die Gefahr weiterer Verletzungen besteht. Gegenüber der Störerhaftung bietet der neue Anspruch dem Geschädigten allerdings eine Reihe von Erleichterungen bei der Sperrung von Nutzerkonten: Durch die Anwendbarkeit der Vorschriften des FamFG trifft den Betroffenen keine Beweisführungslast, da das Gericht gemäß § 26 FamFG die zur Feststellung der entscheidungserheblichen Tatsachen erforderlichen Ermittlungen amtswegig durchführen muss. Zudem trägt der Betroffene ein geringeres Kostenrisiko, da zum einen keine Gerichtsgebühren anfallen. Im Übrigen sieht § 81 Absatz 1 Satz 1 FamFG vor, dass das Gericht die Kosten des Verfahrens nach billigem Ermessen den Beteiligten ganz oder zum Teil auferlegen kann. Die Sperrung des Nutzerkontos muss in jedem Einzelfall verhältnismäßig sein. Zudem soll der Richtervorbehalt sicherstellen, dass auch die Grundrechte des Rechtsverletzers, insbesondere aus Artikel 5 GG, geschützt werden. Vor diesem Hintergrund trägt § 4 dem Schutz der Meinungsfreiheit noch intensiver Rechnung als Deaktivierungen von Nutzerkonten im Nutzer-Plattform-Verhältnis mit nachträglicher Rechtsschutzmöglichkeit.

An den Spielregeln des demokratischen Diskurses wird der Entwurf nichts ändern: Was heute geäußert werden darf, darf auch künftig geäußert werden. Der Entwurf begründet weder neue materielle Beschränkungen für Meinungsäußerungen, noch schafft er eine neue Kategorie unzulässiger Kommunikation. Ziel ist ausschließlich die effektivere Durchsetzung bestehenden Rechts bei gravierenden Rechtsverletzungen. Die Anknüpfung an einen Straftatenkatalog begrenzt dabei die Reichweite der vorgesehenen Maßnahmen. Hierdurch wird eine gewisse Intensität der Persönlichkeitsrechtsverletzung vorausgesetzt; weniger stark ausgeprägte Formen der Persönlichkeitsrechtsverletzungen reichen für die geregelten Maßnahmen nicht aus.

Zugleich bleibt die Möglichkeit anonymer oder pseudonymer Meinungsäußerung gewahrt. Enge tatbestandliche Voraussetzungen und der Richtervorbehalt dienen dem Schutz der Grundrechte – insbesondere aus Artikel 5 Absatz 1 GG – des in Anspruch Genommenen und gewährleisten die Wahrung des Verhältnismäßigkeitsgrundsatzes. Die Maßnahmen dienen allein dem Zweck der Rechtsdurchsetzung des Betroffenen und sind auf das hierfür erforderliche Maß begrenzt.

2. **Strafrecht**

Die strafrechtlichen Ergänzungen betreffen mehrere Phänomene. Im Einzelnen:

**a) Bildbasierte sexualisierte Gewalt**

Mit diesem Entwurf sollen Strafbarkeitslücken bei bildbasierter sexualisierter Gewalt geschlossen werden. Der Begriff der „bildbasierten sexualisierten Gewalt“ beruht auf einer Übersetzung der erstmals im Oktober 2015 von der australischen Tageszeitung „Sydney Morning Herald“ verwendeten Bezeichnung „image-based sexual abuse“ und charakterisiert ein kriminologisches Phänomen, das verschiedene Arten der missbräuchlichen Herstellung und Verwendung von Nacktaufnahmen umschreibt (vergleiche McGlynn/Rackley, Image-Based Sexual Abuse, in: Oxford Journal of Legal Studies, 2017 (37), S. 534 ff.). Die dem Phänomen unterfallenden Erscheinungsformen werden im deutschen Recht von verschiedenen Tatbeständen des Kern- und Nebenstrafrechts erfasst, wobei die Vorschriften jeweils unterschiedliche Anknüpfungspunkte haben. Einige Tatbestände setzen eine räumliche Begrenzung beziehungsweise einen Sichtschutz voraus (§ 201a Absatz 1 Nummer 1 StGB, § 184k StGB), andere erfassen im Wesentlichen pornographische Inhalte (§§ 184 und folgende StGB). Teilweise schützen die Vorschriften nur Kinder und Jugendliche (§§ 184b, 184c, 201a Absatz 3 StGB) oder stellen auf einen ehrverletzenden Charakter ab (§§ 185 und folgende, 201a Absatz 2 StGB). Ein Teil der Vorschriften erfasst zudem nur das Verbreiten bzw. Zugänglichmachen (§ 33 in Verbindung mit § 22 KunstUrhG, § 201a Absatz 2 StGB) und nicht auch das Herstellen von Bildaufnahmen. Infolgedessen wird der strafrechtliche Bildnisschutz als „Flickenteppich“ wahrgenommen (Deutsches Institut für Menschenrechte, „Monitor Gewalt gegen Frauen – Umsetzung der Istanbul-Konvention in Deutschland. Erster Periodischer Bericht“, S. 352 f.), der ein homogenes Konzept strafrechtlicher Vorschriften für unbefugte Nacktaufnahmen vermissen lasse (Eisele NStZ 2025, 613, 614), und lückenhaft sei (Völzmann ZUM 2025, 493, 500). Nicht strafbar ist beispielsweise die Herstellung intimen Materials von Erwachsenen, das in öffentlich zugänglichen Bereichen hergestellt wird (zum Beispiel Aufnahmen in der Sauna oder am Strand). Das unbefugte Zugänglichmachen solchen Materials ist nicht strafbar, wenn eine Eignung zur Ansehensschädigung im Sinne des § 201a Absatz 2 StGB oder ein sonstiger ehrverletzender Charakter (§§ 185 und folgende StGB) nicht gegeben oder die geschädigte Person, etwa im Falle der Abbildung einzelner intimer Körperteile, nicht zu erkennen ist (§ 201a StGB und § 33 in Verbindung mit § 22 KunstUrhG scheiden aus). Das Verbreiten im Sinne der §§ 184a, 184b oder 184c StGB zielt auf einen größeren, nicht mehr kontrollierbaren Personenkreis ab, das heißt die Weitergabe an nur eine oder mehrere bestimmte Personen genügt hierfür nicht.

Im materiellen Strafrecht wird der Bildnisschutz in § 201a StGB vor allem für die Themen Tod, Krankheit und Sexualität aufgegriffen (Graf, in: Münchener Kommentar zum Strafgesetzbuch, 5. Auflage 2025, § 201a Rn. 10); dabei wird teilweise nach thematischen und teilweise nach räumlichen Sphären differenziert (vergleiche Eisele, in: Tübinger Kommentar, 31. Aufl. 2025, § 201a Rn. 8). Der Schutz der Intimsphäre durch Bildaufnahmen in § 184k StGB beschreibt mit dem „Upskirting“ und „Downblousing“ bislang nur einen Teil der in Betracht kommenden Rechtsgutverletzungen. So sind Bildaufnahmen von bekleideten Geschlechtsteilen in § 184k StGB aufgeführt, nicht aber etwa von unbekleideten intimen Körperteilen oder sexuellen Handlungen. Die Pornographiedelikte wiederum dienen in erster Linie dem Kinder- und Jugendschutz und dem Schutz der Allgemeinheit vor ungewollter Konfrontation mit Pornographie und schützen die Persönlichkeitsrechte und die sexuelle Selbstbestimmung der abgebildeten Kinder und Jugendlichen nur, soweit die Tathandlungen „Besitz“ und „Herstellen“ im Vorfeld des eigentlichen „Verbreitens“ unter Strafe gestellt sind.

Das Anfertigen von Bildern oder Videos von einer Person ohne ihre Einwilligung stellt einen Eingriff in ihr allgemeines Persönlichkeitsrecht dar. Der Eingriff wiegt umso schwerer, je intimer die Körperteile sind, die abgebildet werden. Mit technischen Mitteln wie Smartphones, Smart Glasses oder Kameras mit hochauflösenden Teleskop-Funktionen ist es heutzutage leicht möglich, aus beliebiger Entfernung scharfe Bild- oder Videoaufnahmen von Personen zu erstellen, ohne dass diese es bemerken. Mithilfe künstlicher Intelligenz können gewöhnliche Abbildungen von Personen zudem ohne ihr Zutun verändert und

gegebenenfalls mit sexuellen Inhalten verbunden werden. Nicht zuletzt bedarf es angesichts moderner Kommunikationsmittel so gut wie keiner Anstrengungen mehr, entsprechende Bilder oder Videos einer Vielzahl von Personen zugänglich zu machen. Vor diesem Hintergrund ergibt sich – auch unter Berücksichtigung des Ultima-Ratio-Gedankens im Strafrecht – die Notwendigkeit, den strafrechtlichen Bildnisschutz im 13. Abschnitt erneut umfassend in den Blick zu nehmen.

In anderen europäischen Ländern gibt es zahlreiche Beispiele für Strafvorschriften zur Sanktionierung bildbasierter sexualisierter Gewalt.

In Belgien etwa ist nach einer weitreichenden Reform des Sexualstrafrechts (in Kraft getreten im Juni 2022, u. a. Implementierung von „Nur-ja-heißt-ja“) und der Verabschiedung eines neuen Strafgesetzbuches (angenommen 2024, in stufenweiser Umsetzung) in Artikel 417/8 des belgischen Strafgesetzbuches ein eigener Tatbestand des Voyeurismus geregelt. Voyeurismus besteht nach dieser Vorschrift darin, eine Person zu beobachten oder beobachten zu lassen oder eine Bild- oder Tonaufnahme von ihr zu machen oder machen zu lassen, direkt oder mit technischen oder anderen Mitteln, ohne die Zustimmung dieser Person oder ohne ihr Wissen, während diese Person nackt ist oder sich einer expliziten sexuellen Handlung hingibt, und während sich diese Person in einer Situation befindet, in der sie vernünftigerweise davon ausgehen kann, dass sie vor unerwünschten Blicken geschützt ist. Als entblößte Person gilt eine Person, die ohne ihre Zustimmung oder ohne ihr Wissen einen Teil ihres Körpers zeigt, der aufgrund ihrer sexuellen Integrität verborgen geblieben wäre, wenn diese Person gewusst hätte, dass sie beobachtet oder visuell oder akustisch aufgezeichnet wird. Diese Straftat wird mit einer Freiheitsstrafe von sechs Monaten bis zu fünf Jahren bestraft.

In Frankreich macht sich nach Artikel 226-1 Nummer 2 des französischen Strafgesetzbuchs strafbar, wer ohne Einwilligung eine Person aufnimmt, aufzeichnet oder überträgt, die sich an einem privaten Ort befindet. Für den Fall, dass sich die Aufnahmen auf Äußerungen oder Bilder sexueller Natur beziehen, die an einem öffentlichen oder privaten Ort aufgenommen wurden, erhöht sich die Strafe gemäß Artikel 226-1-2 auf zwei Jahre Freiheitsentzug und eine Geldstrafe von 60 000 Euro. Mit denselben Strafen wird bestraft, wer ohne Zustimmung der betroffenen Person Aufzeichnungen oder Dokumente mit sexuellen Äußerungen oder Darstellungen, die mit ausdrücklicher oder vermuteter Zustimmung der betroffenen Person oder von dieser selbst durch eine der in Artikel 226-1 vorgesehenen Handlungen erlangt wurden, der Öffentlichkeit oder einem Dritten zugänglich macht.

In England und Wales wurden Lücken im strafrechtlichen Bildnisschutz durch den Data (Use and Access) Act 2025 mit Wirkung zum 6. Februar 2026 geschlossen. Der Sexual Offences Act, der in Section 67 bereits Tatbestände für Voyeurismus und Upskirting enthält, wurde u. a. in Section 66E um einen Tatbestand für Deepfakes ergänzt. Danach begeht eine Person A eine Straftat, wenn (a) A vorsätzlich ein angebliches intimes Bild einer anderen Person (B) erstellt, (b) B der Erstellung des angeblichen intimen Bildes nicht zustimmt und (c) A nicht vernünftigerweise davon ausgehen kann, dass B zustimmt. Ein „angebliches intimes Bild” einer Person ist ein Bild, das (a) wie eine Fotografie oder ein Film der Person aussieht oder eine solche enthält (aber keine oder nicht nur eine Fotografie oder ein Film der Person ist), (b) wie ein Erwachsener aussieht und (c) die Person in einer intimen Situation zu zeigen scheint.

In Irland stellt der Harassment, Harmful Communications and Related Offences Act 2020, bekannt als „Coco’s Law“, die Herstellung und Verbreitung von intimen Bildern ohne Einwilligung unter Strafe. Dies schließt mit der weiten Definition der „intimen Bilder“ in § 1 als „jede visuelle Darstellung (einschließlich begleitender Tonaufnahmen oder Dokumente), die mit beliebigen Mitteln erstellt wurde, darunter fotografische, filmische, videografische oder digitale Darstellungen“, KI-generierte Bilder und Deepfakes ein. Nach § 3 Absatz 1 Buchstabe a dieses Gesetzes macht sich strafbar, wer ohne Zustimmung einer anderen Person intime Bilder dieser Person aufzeichnet, verbreitet oder veröffentlicht und diese

Aufzeichnung, Verbreitung oder Veröffentlichung die Ruhe und Privatsphäre dieser anderen Person ernsthaft beeinträchtigt oder dieser anderen Person Angst, Stress oder Schaden zufügt.

In den Niederlanden kann die Erstellung und Verbreitung von „visuellen Darstellungen sexueller Natur“ mit bis zu zwei Jahren Freiheitsstrafe bestraft werden. So macht sich nach Artikel 254ba Absatz 1 des niederländischen Strafgesetzbuches strafbar, wer vorsätzlich und rechtswidrig eine visuelle Darstellung sexueller Natur von einer Person anfertigt (Buchstabe a) oder über eine visuelle Darstellung im Sinne von Buchstabe a verfügt, obwohl er weiß oder vernünftigerweise vermuten muss, dass diese durch oder infolge einer unter Buchstabe a strafbaren Handlung erlangt wurde (Buchstabe b). Nach Artikel 254ba Absatz 2 wird bestraft, wer eine visuelle Darstellung im Sinne von Absatz 1 Buchstabe a veröffentlicht, obwohl er weiß oder vernünftigerweise vermuten muss, dass diese durch oder infolge einer in Absatz 1 Buchstabe a strafbaren Handlung erlangt wurde (Buchstabe a) oder eine visuelle Darstellung sexueller Natur von einer Person veröffentlicht, obwohl er weiß, dass diese Veröffentlichung für diese Person nachteilig sein kann (Buchstabe b).

In Italien wird gemäß Artikel 612 ter des italienischen Strafgesetzbuches mit einer Freiheitsstrafe von einem bis zu sechs Jahren und einer Geldstrafe von 5 000 bis 15 000 Euro bestraft, wer nach deren Erstellung oder Entwendung Bilder oder Videos mit sexuell eindeutigem Inhalt, die privat bleiben sollen, ohne die Zustimmung der abgebildeten Personen versendet, übergibt, weitergibt, veröffentlicht oder verbreitet.

### b) Nicht-sexualisierte Deepfakes

Auch nicht-sexualisierte Deepfakes, verstanden als mit Methoden generativer künstlicher Intelligenz veränderte oder erstellte Inhalte, können gravierende nachteilige Konsequenzen für betroffene Personen haben, wenn sie unbefugt dritten Personen zugänglich gemacht werden. Sie treten in verschiedenen Erscheinungsformen auf, zum Beispiel als Bildaufnahmen, in denen Gesichter von Personen ausgetauscht oder einer Person mittels Lippensynchronisation fingierte Aussagen in den Mund gelegt werden, oder als Ganzkörper-Deepfakes, die den gesamten Körper einer Person in eine fiktive, durch künstliche Intelligenz generierte Umgebung versetzen (vergleiche Heckmann/Paschke, in: Stern/Sodan/Möstl, Das Staatsrecht der Bundesrepublik Deutschland im europäischen Staatenverbund, 2. Auflage 2022, § 121 Rn. 68). Durch sich stetig verbessernde technologische Möglichkeiten sind Deepfakes heute kaum noch von realen Bild- und Tonaufnahmen zu unterscheiden. Nicht selten werden derartige Deepfakes gerade zu dem Zweck weitergegeben, die dargestellte Person zu diskreditieren oder fingierte, etwa obszöne oder gewaltverherrlichende Aussagen als Äußerungen dieser Person auszugeben. Für die dargestellte Person handelt es sich auch hier um einen Eingriff in das allgemeine Persönlichkeitsrecht aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG, das nicht nur unter anderem die persönliche Ehre und das Recht am eigenen Bild und am (gesprochenen) Wort schützt, sondern auch ein Recht auf Schutz vor Zuschreibung nicht getätigter oder verfälschter Äußerungen beinhaltet (vergleiche BVerfG, Beschluss vom 3. Juni 1980 – 1 BvR 185/77 –, BVerfGE 54, 148 [155 f.]; Eichberger, in: Huber/Voßkuhle, Grundgesetz, 8. Auflage 2024, Artikel 2 Rn. 259 f.).

Das geltende Recht erfasst das unbefugte Zugänglichmachen von ansehensschädigenden Deepfakes bereits. So ist die missbräuchliche Weitergabe von Deepfakes nach geltendem Recht bereits strafbar. Insbesondere können die Tatbestände der Verleumdung (§ 187 StGB), der Verletzung des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten durch Bildaufnahmen (§ 201a StGB) und § 33 KunstUrhG einschlägig sein. Handelt es sich bei den Deepfakes um Darstellungen mit pornographischem Inhalt, kommt eine Strafbarkeit nach § 184 StGB (Verbreitung pornographischer Inhalte), § 184a StGB (Verbreitung gewalt- oder tierpornographischer Inhalte), § 184b StGB (Verbreitung, Erwerb und Besitz kinderpornographischer Inhalte) oder § 184c StGB (Verbreitung, Erwerb und Besitz

jugendpornographischer Inhalte) in Betracht. Das Verbreiten von Deepfakes kann zudem zivilrechtliche Ansprüche auf Unterlassung und gegebenenfalls Geldentschädigung analog § 1004 BGB in Verbindung mit § 823 Absatz 1 und 2 BGB, den §§ 22 folgende KunstUrhG begründen (vergleiche zu Unterlassungsansprüchen gegen einen Hostprovider wegen eines auf einer Internetseite veröffentlichten Deepfake-Videos OLG Frankfurt a. M., Beschluss vom 4. März 2025 – 16 W 10/25 –, GRUR-RS 2025, 3551). Angesichts des Fehlens einer die unbefugte Verbreitung von Deepfakes spezifisch adressierenden Regelung und des Nebeneinanders verschiedener Straftatbestände wird die bisherige Rechtslage allerdings als wenig kohärent und unübersichtlich kritisiert (vergleiche etwa Bundestagsdrucksache 21/1383, Seite 11 f.; Lantwin, MMR 2020, 78, 81). Es entspricht daher einem rechtspolitischen Bedürfnis, das spezifische Tatunrecht dieser Handlungen künftig in einem eigenständigen Tatbestand abzubilden und so strafrechtlich noch präziser zu erfassen.

### c) Verwendung von Informations- und Kommunikationstechnik zur heimlichen Überwachung

Die wiederholte oder ständige Überwachung einer Person greift in deren allgemeines Persönlichkeitsrecht ein. Mithilfe von Informations- und Kommunikationstechnik können aus der Ferne die Bewegungsdaten des Opfers erhoben, sowie Ton- und Videoaufnahmen angefertigt werden. Mittels (untergeschobener) Ortungsgeräte („Tracker“), die die Position von Objekten oder Personen ermitteln, können detaillierte Bewegungsprofile erstellt werden. Erfolgt ein Zugriff auf von Smart-Home-Produkten erhobene Daten, können vielfältige Informationen zu überwachten Personen und ihren Lebensgewohnheiten gesammelt werden. Erfolgt die Überwachung wiederholt oder ständig, kann der Täter Kontrolle über das Opfer gewinnen und dieses ängstigen und zu Verhaltensänderungen zwingen.

Artikel 6 der Richtlinie (EU) 2024/1385 zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt verpflichtet die Mitgliedstaaten der Europäischen Union dazu, die wiederholte oder ständige Überwachung einer anderen Person ohne deren Einwilligung oder ohne rechtliche Genehmigung mittels Informations- und Kommunikationstechnologien unter Strafe zu stellen, sofern diese Handlungen wahrscheinlich dazu führen, dass dieser Person schwerer Schaden zugefügt wird. Das in Artikel 6 der Richtlinie (EU) 2024/1385 beschriebene Verhalten ist abhängig von den Umständen des Einzelfalls bereits nach geltendem Recht strafbar. So ist etwa eine heimliche Überwachung einer Person mittels eines Ortungsgerätes zur Erstellung persönlicher Bewegungsprofile durch eine Detektei, die gegen Entgelt handelt, nach § 42 BDSG strafbar (vergleiche BGH, Urteil vom 4. Juni 2013 – 1 StR 32/13 zu § 44 BDSG a. F. = NJW 2013, 2530). Strafbar ist auch ein entsprechendes Handeln in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen (vergleiche im Einzelnen etwa Bieber, in: v. Heintschel/Heinegg (Hrsg.), BeckOK StGB, 66. Edition Stand 1. August 2025, § 42 BDSG Rn. 28.1; zur Verwendung eines an der Unterseite des PKW des neuen Lebensgefährten der Exfrau angebrachten GPS-Trackers vergleiche LG Aachen, Urteil vom 18. Februar 2011 – 71 Ns-504 Js 506/09-129/10, BeckRS 2011, 20917, zu § 44 BDSG der alten Fassung). Abhängig von den Umständen des Einzelfalls kommen weitere Straftatbestände in Betracht, etwa § 202a StGB (Ausspähen von Daten), § 202b StGB (Abfangen von Daten) und § 238 StGB (Nachstellung). Auch wenn von Artikel 6 der Richtlinie (EU) 2024/1385 erfasstes Verhalten nach deutschem Recht bereits strafbar ist, soll mit § 202e StGB (Unbefugte Überwachung durch Informations- oder Kommunikationstechnik) klargestellt und bekräftigt werden, dass das deutsche Recht den Richtlinienvorgaben entspricht. Darüber hinaus sollen Rechtsanwender durch einen gesonderten Tatbestand für die erheblichen Gefahren sensibilisiert werden, die von einer wiederholten oder ständigen Überwachung für die Persönlichkeitsrechte betroffener Personen ausgehen.

### 3. Nachhaltigkeitsaspekte

Der Entwurf steht im Einklang mit den Leitgedanken der Bundesregierung zur nachhaltigen Entwicklung im Sinne der Deutschen Nachhaltigkeitsstrategie (DNS), die der Umsetzung der Agenda 2030 (UN-Agenda 2030) für nachhaltige Entwicklung der Vereinten Nationen dient und trägt zur Förderung der Erreichung der Nachhaltigkeitsziele 5 und 16 der UN-Agenda 2030 bei. Er leistet insbesondere einen Beitrag zur Erreichung der Unterziele 5.2 „Alle Formen von Gewalt gegen alle Frauen und Mädchen im öffentlichen und im privaten Bereich einschließlich des Menschenhandels und sexueller und anderer Formen der Ausbeutung beseitigen“ und 16.1 „Alle Formen der Gewalt und die gewaltbedingte Sterblichkeit überall deutlich verringern“ der UN-Agenda 2030, weil strafrechtliche Normen auch immer präventiv wirken.

## II. Wesentlicher Inhalt des Entwurfs

Der Entwurf beruht auf zwei Säulen: der Gewährleistung einer wirksamen zivilrechtlichen Rechtsverfolgung und der Schaffung eines effektiven Strafrechtsschutzes.

### 1. Zivilrecht

Der zivilrechtliche Teil des Gesetzes 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.

### 2. Strafrecht

Von den Erscheinungsformen des Phänomens der bildbasierten sexualisierten Gewalt greift § 184k des Strafgesetzbuches in der Entwurfsfassung (StGB-E) das unbefugte Herstellen und Zugänglichmachen von intimem Bildmaterial auf. Die Strafbarkeit soll künftig nicht mehr an räumliche Begrenzungen oder die Individualisierbarkeit der Person anknüpfen und bereits mit der unbefugten Herstellung oder der unbefugten Zugänglichmachung entsprechenden Materials an eine einzige andere Person gegeben sein. Unter § 184k StGB-E fallen künftig etwa Vergewaltigungsvideos in Vergewaltigungsnetzwerken, voyeuristische Nacktaufnahmen in öffentlich zugänglichen Bereichen (FKK-Strand, Sauna) und voyeuristische Aufnahmen von bekleideten Geschlechtsteilen, zudem enthält der Tatbestand eine eigene Regelung für das unbefugte Herstellen und Teilen von manipulierten Bildinhalten („sexualisierte Deepfakes“). Darüber hinaus wird mit § 184k StGB eine Vorschrift

im 13. Abschnitt des Strafgesetzbuches und damit im Kernstrafrecht geschaffen. Dies hat zur Folge, dass der Tatbestand der Bedrohung in § 241 StGB, der Straftaten der sexuellen Selbstbestimmung bereits heute in Bezug nimmt, die Drohung mit entsprechenden Verhaltensweisen („Sextortion“) künftig umfassend erfasst.

Nach § 201a StGB (Verletzung des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten durch Bildaufnahmen) wird § 201b StGB (Verletzung von Persönlichkeitsrechten durch täuschende Inhalte) eingefügt. Der neue Tatbestand dient der Klarstellung der bisherigen Rechtslage. Er setzt ein klares gesetzgeberisches Signal gegen die Gefahren, die von derartigen Inhalten für die Persönlichkeitsrechte der dargestellten Personen ausgehen, und schärft insofern das Bewusstsein der Rechtsanwender.

Nach § 202d StGB (Datenhehlerei) wird § 202e StGB (Unbefugte Überwachung mittels Informations- oder Kommunikationstechnik) eingefügt. Dadurch wird eine vollständige Umsetzung von Artikel 6 der Richtlinie (EU) 2024/1385 gewährleistet und klargestellt, dass strafwürdige Fälle elektronischer Überwachung strafrechtlich erfasst sind.

## III. Exekutiver Fußabdruck

[Wird nach der Länder- und Verbändebeteiligung gegebenenfalls 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 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-, Datenspeicherungs- 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 in Artikel 1 sowie die Änderungen im Straf- und Strafprozessrecht in den Artikeln 2, 4 und 5 beruhen auf der Gesetzgebungskompetenz des Bundes aus Artikel 74 Absatz 1 Nummer 1 GG (Strafrecht, gerichtliches Verfahren).

Die Änderung in Artikel 3 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 (vergleiche Bundestagsdrucksache 19/27441, Seite 31), und die Änderung in Artikel 7 – wie die zu ändernde Regelung – auf der Gesetzgebungskompetenz des Bundes aus Artikel 73 Absatz 1 Nummer 9 GG (Urheberrecht; vergleiche Bundestagsdrucksache 19/27426, Seite 55).

Die Änderung in Artikel 11 beruht auf der Gesetzgebungskompetenz des Bundes aus Artikel 73 Absatz 1 Nummer 7 GG (Telekommunikation).

Im Übrigen handelt es sich um Folgeänderungen.

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

Der Entwurf ist mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen, die die Bundesrepublik Deutschland abgeschlossen hat, vereinbar.

### 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 § 9, 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 (vergleiche 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 § 9 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 und folgende 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 (vergleiche 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-Mitgliedstaaten 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 bei einer Zustellung nach Artikel 19 Absatz 1 Buchstabe a EuZVO 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. Auch eine Zustellung nach Artikel 19 Absatz 1 Buchstabe b EuZVO dürfte in der Praxis nicht möglich sein. Zum einen dürfte die erforderliche ausdrückliche Zustimmung des Empfängers gegenüber dem Gericht zur Versendung von E-Mails in dem konkreten Verfahren nicht vorliegen. Zum anderen dürfte keiner der erforderlichen, in § 130a ZPO aufgeführten sicheren Übermittlungswege zu den betroffenen Diensteanbietern bestehen.

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 (sogenannte 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, (das heißt 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, um Rechtsinhabern die Möglichkeit zu geben, bei einem Zivilgericht eine Schadensersatzklage wegen eines Schadens zu erheben, der von diesen Nutzern verursacht worden sein soll, 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) der DS-GVO 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 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes (TDDDG) (bzw. der Vorgängernorm § 14 des Telemediengesetzes (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 mit weiteren Nachweisen – Fake Account).

Dies gilt auch, soweit für die Auskunftserteilung auf bei einem Telekommunikationsanbieter vorratsgespeicherte IP-Adressen zurückgegriffen wird. Nach der Rechtsprechung des EuGH ist ein solcher Zugriff schon zur Erreichung eines mit der Bekämpfung von Straftaten im Allgemeinen verbundenen Ziels möglich, wenn durch Wahrung bestimmter Speichermodalitäten tatsächlich ausgeschlossen ist, dass diese Speicherung schwere Eingriffe in das Privatleben des Betroffenen zur Folge haben kann, die darauf beruhen, dass insbesondere durch eine Verknüpfung dieser IP-Adressen mit einem von den Betreibern ebenfalls gespeicherten Satz von Verkehrs- oder Standortdaten die Möglichkeit besteht, genaue Schlüsse auf das Privatleben der Personen zu ziehen (vergleiche EuGH [Plenum], Urteil vom 30. April 2024, Rs. C-470/21, Quadrature du Net II – Hadopi, Rn. 82 ff.). Der EuGH billigt auch bei einer Verletzung des Eigentumsrechts dem Betroffenen zu, sich im Rahmen eines zivilrechtlichen Verfahrens um dessen Schutz zu bemühen (vergleiche EuGH [GK], Urteil vom 29. Januar 2008, Rs. C-275/06, Promusicae, Rn. 53; EuGH, Urteil vom 17. Juni 2021, Rs. C 597/19, Mircom, Rn. 116 f.). Nichts anderes kann für den – dem Schutz des Eigentums mindestens gleichgewichtigen – Schutz des Allgemeinen Persönlichkeitsrechts und seiner besonderen Ausprägungen wie dem Recht am eigenen Bild, der informationellen Selbstbestimmung oder der sexuellen Selbstbestimmung durch private Rechtsverfolgung gelten.

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 beweissichernden Anordnungen (§ 3 GgdG) 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 § 9 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 Diensteanbieters 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 Diensteanbieters – Rechnung zu tragen, wird die Sperrung an mehrere Bedingungen geknüpft. Insbesondere 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 kann jeweils nur für einen angemessenen Zeitraum ergehen. Vor Entscheidung des Gerichts über die Sperrung des Nutzerkontos muss der betroffene Accountinhaber vom Gericht oder, bei fehlender Kenntnis der Identität des Accountinhabers, vom Diensteanbieter 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 Diensteanbieter dazu verpflichtet werden, Umgehungsversuche durch den Accountinhaber im Rahmen des für ihn Zumutbaren zu unterbinden.

## 7. **Richtlinie (EU) 2024/1385 (Gewalt gegen Frauen und häusliche Gewalt)**

Der Entwurf dient auch der weiteren Umsetzung der Artikel 5 und 6 der Richtlinie (EU) 2024/1385 des Europäischen Parlaments und des Rates vom 14. Mai 2024 zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt. Nach Artikel 5 Absatz 1 Buchstabe a der Richtlinie sind die Mitgliedstaaten aufgefordert, Handlungen unter Strafe zu stellen, bei denen ohne Einverständnis der betreffenden Person Bilder, Videos oder vergleichbares Material, welches eindeutig sexuelle Handlungen oder intime Körperteile dieser Person darstellt, mittels Informations- und Kommunikationstechnologien der Öffentlichkeit zugänglich gemacht wird, sofern diese Handlungen wahrscheinlich dazu führen, dass der betreffenden Person schwerer Schaden zugefügt wird. Nach Auffassung der Kommission kommt es bei der Abbildung intimer Körperteile nicht auf die Individualisierbarkeit der dargestellten Person an, die nach geltendem Recht häufig Voraussetzung für eine Strafbarkeit ist. Artikel 6 der Richtlinie (EU) 2024/1385 verpflichtet die Mitgliedstaaten der Europäischen Union dazu, die wiederholte oder ständige Überwachung einer anderen Person ohne deren Einwilligung oder ohne rechtliche Genehmigung mittels Informations- und Kommunikationstechnologien unter Strafe zu stellen, sofern diese Handlungen wahrscheinlich dazu führen, dass dieser Person schwerer Schaden zugefügt wird.

## 8. **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 Entwurf 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 Rechtsvereinfachung. Der Entwurf sorgt für Rechtsklarheit im Hinblick auf wesentliche Maßnahmen der privaten Rechtsverfolgung im Internet, indem er diese in einem eigenen Stammgesetz zusammenfasst und transparent ausgestaltet.

Aspekte der Verwaltungsvereinfachung sind von dem Entwurf nicht betroffen.

### 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 Rechtsverletzung 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 Persönlichkeitsrechtsverletzung 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 rechtswidrige Inhalte 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.

Soweit Änderungen des materiellen Strafrechts vorgeschlagen werden, steht der Entwurf im Kontext der gefährdeten rechtzeitigen Erreichung der Ziele der Resolution der Generalversammlung der Vereinten Nationen vom 25. September 2015 „Transformation unserer Welt: die Agenda 2030 für nachhaltige Entwicklung“ und trägt insbesondere zur Erreichung ihrer Nachhaltigkeitsziele 5.2 und 16.1 bei, alle Frauen und Mädchen zur Selbstbestimmung zu befähigen sowie friedliche und inklusive Gesellschaften im Sinne einer nachhaltigen Entwicklung zu fördern.

Konflikte mit anderen Nachhaltigkeitszielen sind nicht erkennbar.

## 3. Haushaltsausgaben ohne Erfüllungsaufwand

Zusätzliche Haushaltsausgaben ohne Erfüllungsaufwand sind nicht zu erwarten. Soweit die von den neuen Straftatbeständen der §§ 201b und 202e StGB und dem erweiterten § 184k StGB erfassten Verhaltensweisen im Zusammenhang mit bereits nach geltendem Recht strafbaren Handlungen stehen, entsteht kein zusätzlicher Aufwand, weil insoweit ohnehin bereits Strafverfahren eingeleitet und geführt werden. Im Übrigen sind die Tatbestände als relative Antragsdelikte ausgestaltet und allenfalls dem Bereich der mittleren Kriminalität zuzuordnen. Eine Vollstreckung von Freiheitsstrafen, die höhere Kosten für den Strafvollzug zur Folge hätte, ist damit regelmäßig nicht zu erwarten. Soweit durch die neuen Tatbestände künftig bislang nicht strafbare Konstellationen erfasst werden, ist anzunehmen, dass entsprechende Verfahren aufgrund entsprechender Strafanzeigen bereits bislang schon eingeleitet und geführt wurden. Soweit diese anders als bislang nicht aus rechtlichen Gründen eingestellt werden, ist allenfalls mit geringfügigen Mehrkosten bei den Strafverfolgungsbehörden und den Strafgerichten der Länder zu rechnen.

## 4. Erfüllungsaufwand

### 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.

### 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 (vergleiche 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 (siehe Bundestagsdrucksache 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 zum Beispiel im Rahmen der gerichtlichen Auskunftsanordnung nach § 101 Absatz 9 UrhG jährlich ca. 2 000 Verfahren (vergleiche 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 Absatz 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 beweissichernden Anordnungen 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 (siehe 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 (vergleiche 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 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 Absatz 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.

**Erfüllungsaufwand der Verwaltung**

Für die Verwaltung entsteht kein Erfüllungsaufwand.

Soweit Änderungen des materiellen Strafrechts vorgeschlagen werden, entsteht oder entfällt kein Erfüllungsaufwand für die Bürgerinnen und Bürger, die Wirtschaft und die Verwaltung.

## 5. Weitere Kosten

Durch die neugeregelten Auskunftsverfahren (§ 2 GgdG) sowie die neue Möglichkeit zur Durchsetzung einer Accountsperre (§ 4 GgdG) ergeben sich im justiziellen Kernbereich laufende Mehrkosten für die Justiz der Länder. Für das Auskunftsverfahren einschließlich der beweissichernden Anordnungen (§ 3) 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 (vergleiche 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 beweissichernde Anordnung (§ 3 GgdG) erlassen. Informationen zum fallbezogenen Aufwand einer beweissichernden Anordnung liegen nicht vor. Es ist zu erwarten, dass das Gericht zum Erlass einer beweissichernden Anordnung zwei Kommunikationsvorgänge (einmal an Plattformbetreiber und Onlinedienste zur Ermittlung der mit dem Rechtsverstoß verbundenen IP-Adresse und Nutzerdaten und einmal an Internetzugangsdienste zur Durchsetzung der beweissichernden Anordnung) aufsetzen muss sowie die von der Plattform übermittelte IP-Adresse einem zuständigen Internetzugangsdienst zuordnen muss, sodass insgesamt 10 Minuten pro Datenspeicherungsanordnung (vergleiche Leitfaden, Anhang 8, Standardaktivitäten 3 und 4 in einfacher Komplexität) anfallen. Durch die neu hinzukommenden beweissichernden Anordnungen 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 (vergleiche 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 (vergleiche 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 (vergleiche Leitfaden, Anhang 9) entstehen jährliche Mehrkosten von rund 53 000 [= 220 * 223/60 * 65,20] Euro.

Für den justiziellen Kernbereich ist durch die Einführung der neuen Straftatbestände der §§ 201b und 202e StGB und die Erweiterung des § 184k StGB kein erheblicher Mehraufwand zu erwarten. Die neu geschaffenen beziehungsweise erweiterten Delikte sind allenfalls dem Bereich der mittleren Kriminalität zuzuordnen und lassen daher die Vollstreckung von Freiheitsstrafen in aller Regel nicht erwarten. Sie sind zudem als relative Antragsdelikte ausgestaltet. Entsprechende Verhaltensweisen stehen in einer Vielzahl der Fälle mit bereits nach geltendem Recht strafbarem Verhalten im Zusammenhang, so dass die Einleitung entsprechender Ermittlungs- und Strafverfahren bereits nach geltendem Recht erfolgen dürfte. Soweit nicht strafbare Verhaltensweisen künftig infolge der Neuregelungen strafbar sind, kann dies zu geringfügigen Mehrkosten bei den Strafverfolgungsbehörden und den Strafgerichten der Länder führen.

## 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 hinsichtlich seines zivilrechtlichen Teils 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.

Eine Befristung oder Evaluierung der strafrechtlichen Regelungen ist nicht vorgesehen.

# 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 einen der folgenden Tatbestände erfüllen und nicht gerechtfertigt sind:

1. Aus dem Strafgesetzbuch:

   – § 111 Öffentliche Aufforderung zu Straftaten,

   – § 126 Störung des öffentlichen Friedens durch Androhung von Straftaten,

   – § 126a Gefährdendes Verbreiten personenbezogener Daten,

   – § 130 Volksverhetzung,

   – § 130a Anleitung zu Straftaten,

- § 131 Gewaltdarstellung,
- § 140 Belohnung und Billigung von Straftaten,
- § 166 Beschimpfung von Bekenntnissen, Religionsgesellschaften und Weltanschauungsvereinigungen,
- § 176a Sexueller Missbrauch von Kindern ohne Körperkontakt mit dem Kind,
- § 176b Vorbereitung des sexuellen Missbrauchs von Kindern,
- § 184 Verbreitung pornographischer Inhalte,
- § 184a Verbreitung gewalt- oder tierpornographischer Inhalte,
- § 184b Verbreitung, Erwerb und Besitz kinderpornographischer Inhalte,
- § 184c Verbreitung, Erwerb und Besitz jugendpornographischer Inhalte,
- § 184k-E Verletzung der Intimsphäre durch Bildaufnahmen,
- § 185 Beleidigung,
- § 186 Üble Nachrede,
- § 187 Verleumdung,
- § 188 Gegen Personen des politischen Lebens gerichtete Beleidigung, üble Nachrede und Verleumdung,
- § 189 Verunglimpfung des Andenkens Verstorbener,
- § 192a Verhetzende Beleidigung,
- § 201 Verletzung der Vertraulichkeit des Wortes,
- § 201a Verletzung des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten durch Bildaufnahmen,
- § 201b StGB-E Verletzung von Persönlichkeitsrechten durch täuschende Inhalte,
- § 238 Nachstellung oder
- § 241 Bedrohung.

2. Aus strafrechtlichen Nebengesetzen:

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

Die genannten Straftaten werden häufig im digitalen Raum begangen und weisen eine besondere Nähe zum allgemeinen Persönlichkeitsrecht auf, da die zugrundeliegenden Handlungen auch die Verletzung des Persönlichkeitsrechts bewirken können.

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 mit weiteren Nachweisen).

Der Straftatenkatalog orientiert sich am früheren § 1 Absatz 3 Netzwerkdurchsetzungsgesetz, enthält jedoch einige Änderungen. Auf die Straftatbestände der §§ 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 Deepfakes – 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 den §§ 126a, 185 und folgende, 201a StGB, § 33 KUG, § 42 BDSG. Damit sollen im Gegensatz zum früheren Netzwerkdurchsetzungsgesetz (vergleiche LG Koblenz, Urteil vom 25. August 2025, 2 O 1/25) nunmehr auch Fälle erfasst werden, in denen gefälschte Nutzerkonten mit unbefugter Verwendung von Bildern anderen Personen betrieben werden. Außerdem soll das gezielte Ansprechen im Internet von Kindern, um sexuellen Kontakt anzubahnen, das gemäß § 176b StGB strafbar ist, in den Anwendungsbereich des Gesetzes fallen. Erfasst sind damit gängige Ausprägungen digitaler Gewalt (vergleiche oben A.I.).

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 sogenannte Revenge-Porns auf eigens dafür erstellten Internetseiten veröffentlicht.

**Zu Nummer 3**

Cloud-Hosting-Dienste stellen eine weitere Unterkategorie von Hosting-Diensten dar und umfassen sogenannte 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 Telekommunikationsgesetz (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 zum Beispiel 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, zum Beispiel Herabstufung, Demonetisierung, Sperrung des Zugangs oder Entfernung, oder in Bezug auf die Fähigkeit der Nutzer, solche Informationen bereitzustellen, zum Beispiel Schließung oder Aussetzung des Kontos eines Nutzers.

**Zu Absatz 6**

Absatz 6 definiert den Begriff des Nutzers. Nutzer sind nur solche Personen, die die Dienste von Diensteanbieter nutzen.

**Zu Absatz 7**

Absatz 7 definiert den Begriff des Nutzerkontos. Dieser soll sämtliche von einem Nutzer betriebene Konten erfassen, einschließlich Unterkonten, auf denen unabhängig vom Konto eigene Inhalte veröffentlicht werden können. Hierdurch soll gewährleistet werden, dass sich gerichtliche Entscheidungen nach § 4 auf die jeweiligen Konten und Unterkonten beziehen und die Frage der Sperre für die jeweilige Einheit isoliert prüfen. Ein Konto oder Unterkonto darf nur dann mit einer Sperre belegt werden, wenn von dieser isoliert zu betrachtenden Einheit eine Wiederholungsgefahr ausgeht.

**Zu § 2 (Auskunft über Daten)**

§ 2 setzt auf den Bestimmungen zur Auskunft über Bestandsdaten von § 21 Absatz 2 bis 4 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes (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. Für diese Auskunft sollen – in Abhängigkeit des Fortgangs des Referentenentwurfs eines Gesetzes zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren (siehe dazu näher in Begründung zu Artikel 11) – die Internetzugangsdiensteanbieter künftig auch vorsorglich gespeicherte IP-Adressen verwenden können. Das stellt § 174 Absatz 5 Nummer 9 TKG-E klar, der insoweit § 2 Absatz 1 ergänzt.

**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 zum Beispiel 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 Bundestagsdrucksache 18/13013, S. 24 zu Nummer 2). Das TDDDG enthält keine dem § 15 Absatz 5 Satz 4 TMG a.F. vergleichbare Vorschrift.

Die Meinungsfreiheit und das allgemeines Persönlichkeitsrecht sind Grundrechte, die ihre privaten Träger zuvörderst als Abwehrrechte gegen den grundrechtsgebundenen Staat in Stellung bringen können, etwa gegen überschießende Strafverfolgung oder zu weit reichende Überwachungsmaßnahmen.

Beeinträchtigungen des allgemeinen Persönlichkeitsrechts können jedoch nicht nur vom Staat, sondern auch von privaten Dritten ausgehen, insbesondere in Form von Behauptungen oder Darstellungen mit beleidigendem oder unwahrem Inhalt. Es obliegt dem Staat für ein hinreichendes Maß an positivem Schutz hiergegen Sorge zu tragen; der Gesetzgeber hat dabei einen Einschätzungs-, Wertungs-, und Gestaltungsspielraum (vergleiche BVerfG, Beschluss vom 10. November 1998 – 1 BvR 1531/96 –, BVerfGE 99, 185-202, Rn. 45; BVerfG, Urteil vom 26. Februar 2020 – 2 BvR 2347/15 –, BVerfGE 153, 182-310, Rn. 224). Diesem Erfordernis kommt der Gesetzgeber auf einfachgesetzlicher Ebene, u.a. durch das (Beleidigungs-)Strafrecht, das die äußersten Grenzen der Meinungsfreiheit markiert, nach.

Die signifikante Verlagerung des öffentlichen Diskurses auf Online-Plattformen (vergleiche Artikel 3 Buchstabe i) DSA) und in sozialen Netzwerken (vergleiche § 1 Absatz 1 Satz 1 NetzDG) fordert auch den Gesetzgeber heraus, die Möglichkeiten der Rechtsverfolgung im Spannungsfeld der Grundrechte von Meinungsfreiheit und allgemeinem Persönlichkeitsrecht neu auszubalancieren. Die technische Entwicklung hat dazu geführt, dass Meinungen, Tatsachen und andere Äußerungen auch und insbesondere von „Normalbürgern“ heutzutage – auf Online-Plattformen – viel leichter öffentlichkeitswirksam kundgetan werden können als in der Vergangenheit, in der der öffentliche Diskurs vornehmlich durch Meinungskundgaben in Rundfunk und Presse geprägt war. Meinungskundgaben auf Online-Plattformen können zudem – aus guten Gründen – auch anonym erfolgen, was bisweilen zu einer Verrohung von Diskursen und zum Absenken von Hemmschwellen für diffamierende Äußerungen führt. Äußerungen auf Online-Plattformen erzielen durch den potenziell unbegrenzten Adressatenkreis zudem eine viel stärkere Breitenwirkung. Eine Verletzung des allgemeinen Persönlichkeitsrechts durch einen öffentlich sichtbaren Post auf einer Online-Plattform wiegt wegen ihrer schriftlichen Perpetuierung und des erreichten bzw.

erreichbaren Adressatenkreises dabei in der Regel schwerer als eine flüchtige mündliche Beleidung auf der Straße oder im Klassenraum. Zu den zu berücksichtigenden Umständen können insbesondere Inhalt, Form, Anlass und Wirkung der betreffenden Äußerung sowie Person und Anzahl der Äußernden, der Betroffenen und der Rezipienten gehören. Das bei der Abwägung anzusetzende Gewicht der Meinungsfreiheit ist umso höher, je mehr die Äußerung darauf zielt, einen Beitrag zur öffentlichen Meinungsbildung zu leisten, und umso geringer, je mehr es hiervon unabhängig lediglich um die emotionalisierende Verbreitung von Stimmungen gegen einzelne Personen geht (vergleiche in diesem Sinne BVerfGE 152, 152 <204 f. Rn. 125> – Recht auf Vergessen I; BVerfG, Beschluss der 2. Kammer des Ersten Senats vom 19. Mai 2020 – 1 BvR 1094/19 –, Rn. 27; Beschluss der 2. Kammer des Ersten Senats vom 19. Dezember 2021 – 1 BvR 1073/20 –, Rn. 30, 31, 35).

Die skizzierte Entwicklung wirkt sich dabei unter anderem auf die Möglichkeiten privater Rechtsdurchsetzung aus, insbesondere bei anonym getätigten Äußerungen. Denn erst wenn die Identität eines Rechtsverletzers bekannt ist, kann dieser im Wege privater Rechtsdurchsetzung zum Beispiel auf Unterlassung oder Schadensersatz in Anspruch genommen werden. Der hier geregelte Auskunftsanspruch ist eine Reaktion darauf, dass Äußerungen, die Verletzungen des allgemeinen Persönlichkeitsrechts darstellen, zunehmend auch unter dem Deckmantel der Anonymität erfolgen. Er soll es ermöglichen, die Anonymität in begründeten Einzelfällen aufzuheben, um bestehende zivilrechtliche Ansprüche gerichtlich durchzusetzen; damit wird zugleich der Justizgewährungsanspruch (Artikel 20 Absatz 3 in Verbindung mit Artikel 2 Absatz 1 GG) gefördert.

Die datenschutzrechtliche Erlaubnis der Datenherausgabe wird unter den Vorbehalt einer richterlichen Gestattung (Richtervorbehalt) gestellt. Ein Richter entscheidet hierzu auf Antrag des Betroffenen in einem Hauptsacheverfahren, ob der Anspruch auf Auskunft nach § 2 Absatz 1 besteht. Das wird nur dann der Fall sein, wenn die verfahrensgegenständliche Äußerung eine Rechtsverletzung im Sinne von § 1 Absatz 1 GgdG darstellt. Mit dem Richtervorbehalt 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. Der Richtervorbehalt wird Einschüchterungseffekte auf die Ausübung der Meinungsfreiheit in diesem eng begrenzten Bereich 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 Satz 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. Nutzerkonten bei Diensteanbietern werden häufig unter Pseudonymen ohne Angabe einer ladungsfähigen Anschrift erstellt; in der Regel genügt die Angabe eines (fiktiven) Namens und einer E-Mail-Adresse. Folglich reicht die Mitteilung der bei dem Diensteanbieter vorhandenen Daten zur Identifizierung in der Regel nicht aus. Um eine effektive Rechtsverfolgung und den grundrechtlich gebotenen Rechtsschutz zu ermöglichen, ist daher die Zuordnung der beim Diensteanbieter protokollierten dynamischen IP-Adresse durch den jeweiligen Internetzugangsanbieter unter Berücksichtigung des exakten Zeitstempels zwingend erforderlich, da eine Identifizierung auf anderem Wege regelmäßig ausscheidet.

**Zu Nummer 3**

Der Anbieter soll dem Antragsteller eine Kopie des rechtsverletzenden Inhalts zur Verfügung stellen, um einerseits Beweisführungsschwierigkeiten des Antragstellers im Folgeverfahren, zum Beispiel aufgrund eines Manipulationsvorwurfs hinsichtlich selbsterstellter Screenshots, zu vermeiden und um andererseits tatsächliche Manipulationen solcher Screenshots durch den Antragsteller zu verhindern.

**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. 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 Halbleiterschutzgesetzes, § 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.

Voraussetzung für eine Entscheidung des Gerichts ist ein entsprechender Antrag des Betroffenen.

**Zu Nummer 1**

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. Diese Antragsvoraussetzungen müssen durch den Antragsteller glaubhaft gemacht werden, um keine ausufernde Amtsermittlungspflicht des Gerichts zu begründen.

**Zu Nummer 2**

Da die Herausgabe der Daten allein zum Zweck der Geltendmachung zivilrechtlicher Ansprüche gegen den Nutzer statthaft ist, muss der Antragsteller im Zeitpunkt der Antragstellung die Absicht haben, gegen den Nutzer zivilrechtlich vorzugehen und diese Absicht in dem Antrag mitteilen. Es sind Fälle denkbar, in denen der Betroffene nach Kenntniserlangung von der Identität des Nutzers aus nachvollziehbaren Gründen (zum Beispiel Verwandtschaft oder enge persönliche Beziehungen) keine Ansprüche mehr geltend machen möchte. Daher dürfte im Zeitpunkt der Antragstellung nur eine vorläufige Intention und noch kein endgültiger Entschluss zur Geltendmachung zivilrechtlicher Ansprüche vorliegen. Das Absehen einer Weiterverfolgung dieser Ansprüche lässt daher nicht zwingend auf einen missbräuchlichen Antrag schließen.

**Zu Absatz 4**

Das Gericht soll in einem Verfahren über die Herausgabe sämtlicher erforderlichen Daten entscheiden, es ist lediglich ein einheitlicher Antrag erforderlich. Das Gericht hat hierbei zu prüfen, ob die Voraussetzungen des § 2 Absatz 1 Satz 1 und 2 vorliegen. 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 Absatz 1 ermöglicht auch den Zugriff auf Daten, die vom Schutzbereich des Fernmeldegeheimnisses erfasst sind. Die Vorschrift trägt dem Zitiergebot nach Artikel 19 Absatz 1 Satz 2 GG Rechnung.

**Zu § 3 (Beweissichernde Anordnungen)**

§ 3 enthält gerichtliche, für die Dauer des Auskunftsverfahrens befristete beweissichernde Anordnungen hinsichtlich der im Fall eines rechtskräftigen stattgebenden Auskunftsbeschlusses an den Antragsteller herauszugebende Daten. Dadurch soll verhindert werden, dass die Auskunft nach § 2 durch Löschung der Daten zwischen Antragstellung und rechtskräftigem Abschluss des Gestattungs- und Auskunftsverfahrens seitens der Anbieter vereitelt wird.

Ab Zeitpunkt der Rechtsverletzung bis zum rechtskräftigen Abschluss des Verfahrens vergehen bei Betroffenheit eines anderen EU-Mitgliedstaats (wegen der entsprechenden Niederlassung des Anbieters der Online-Plattform häufig Irland) mehrere Wochen. Ein erster Zeitverlust kann dadurch eintreten, dass der Betroffene von dem rechtsverletzenden Inhalt nicht gleich am Tag der Veröffentlichung, sondern gegebenenfalls erst Wochen später Kenntnis erlangt. Nach Kenntnis wird er Überlegungen anstellen, ob er gegen den rechtswidrigen Inhalt rechtlich vorgehen will. Hierbei wird er vernünftigerweise eine Beratungsstelle oder einen Rechtsanwalt einbeziehen, was zusätzlich Zeit kostet. Hat der Betroffene sich zu einem rechtlichen Vorgehen entschieden, ist ein Schriftsatz zu erstellen und dieser dem Gericht zu übermitteln. Dieser Prozess der Entscheidung und Antragstellung kann durchaus ein, zwei Wochen in Anspruch nehmen. Nach Eingang des Antrags bei Gericht wird dieser der zuständigen Kammer vorgelegt, die den Antrag prüft und die prozessleitenden Verfügungen veranlasst. Sodann muss die Zustellung an den Anbieter der Online-

Plattform oder des Hosting-Dienstes – in der Regel in einem anderen Mitgliedstaat – erfolgen. Eine Zustellung nach der EU-Zustellungsverordnung (EU) 2020/1784 soll zwar so rasch wie möglich und in jedem Fall binnen eines Monats nach Eingang des Schriftstücks bei der Empfangsstelle des Staates, in dem die Zustellung bewirkt werden soll, erfolgen. In der Praxis kann dies aber auch länger dauern. Alternativ kann auch ein Ersuchen an das zuständige Gericht in dem Mitgliedstaat nach der EU-Beweisaufnahmeverordnung (EuBVO – VO (EU) 2020/1783) gestellt werden, auch dieser Weg nimmt mehrere Wochen in Anspruch. Sodann muss der Diensteanbieter den Beschluss umsetzen, also die geforderten Daten heraussuchen, speichern und – wiederum grenzüberschreitend – an das deutsche Gericht übersenden. Die Kammer muss danach den Anbieter des Internetzugangsdienstes kontaktieren und die Zuordnung sowie die Speicherung verlangen. Nach Entscheidung des erstinstanzlichen Gerichts tritt die Rechtskraft nach weiteren zwei Wochen ein, was der Zeitpunkt ist, zu dem die Anbieter dem Betroffenen im Falle des Obsiegens die Daten zur Identität des Urhebers des rechtswidrigen Inhalts herauszugeben haben. Angesichts der geschilderten Abläufe ist es nicht unwahrscheinlich, dass die Auskunft erst nach Ablauf von drei Monaten zu erteilen ist und die für die Zuordnung einer IP-Adresse zu einem Nutzer erforderlichen Daten beim Anbieter des Internetzugangsdienstes nicht mehr vorhanden sind.

Sollte ein Beteiligter des Verfahrens Rechtsmittel einlegen, muss außerdem die Entscheidung des Oberlandesgerichts abgewartet werden. Dies dürfte nochmals einige Wochen in Anspruch nehmen. Hier ist offensichtlich, dass eine rechtskräftige Entscheidung binnen drei Monaten kaum zu erzielen ist und die Daten vom Anbieter von Internetzugangsdiensten ohne Datenspeicherung gelöscht wären.

**Zu Absatz 1**

Absatz 1 enthält formale und materiell-rechtliche Regelungen zur Sicherung der Drittauskunft und orientiert sich dabei an der Rechtsprechung zum Urheberrecht (vergleiche 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 im Wege einer verfahrensleitenden Anordnung aufgeben können, vorhandene Daten des Verletzers bis zur endgültigen gerichtlichen Entscheidung über die Verpflichtung zur Auskunftserteilung nicht zu löschen.

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 im Wege einer verfahrensleitenden Anordnung 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.

Zur Umsetzung der gerichtlichen Anordnungen in einem anderen Mitgliedstaat stehen dem Gericht zwei Wege zur Verfügung: Zum einen kann es das nach der EuBVO zuständige Gericht in dem betroffenen Mitgliedstaat um Umsetzung der Maßnahmen ersuchen. Das Gericht des Mitgliedstaats wendet dann sein eigenes nationales Recht an und kann die gleichen Zwangsmittel nutzen wie in seinen eigenen nationalen Verfahren. Zum anderen kann das hiesige Gericht auch den direkten Weg wählen und die Anordnung unmittelbar an den Empfänger im anderen Mitgliedstaat zustellen; Zwangsmaßnahmen stehen dann allerdings nicht zur Verfügung (EuGH, Beschluss vom 24. Februar 2022, C-188/22, Rn. 33; EuGH, Urteil vom 21. Februar 2013, C-332/11, Rn. 47 f.; EuGH, Urteil vom 6. September 2012, C-170/11, Rn. 31, 38).

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. Die Unstatthaftigkeit der Mitteilung der Daten an den Antragsteller gilt dabei nur für das Datenspeicherungsverfahren und bei Abweisung des Auskunftsersuchens nach § 2. Bei einem erfolgreichen Auskunftsverfahren gemäß § 2 sind diese Daten herauszugeben. Satz 3 regelt klarstellend das insoweit beschränkte Akteneinsichtsrecht, da die Daten auch nicht auf diesem Wege eingesehen werden dürfen. Im Fall des Stattgebens des Antrags auf Auskunftserteilung liegt allerdings kein Grund mehr vor, die Akteneinsicht weiterhin einzuschränken.

**Zu Absatz 3**

Absatz 3 enthält nach Anhängigkeit des Auskunftsantrags die gerichtliche Verpflichtung, eine beweissichernde Anordnung gegenüber dem vom Auskunftsersuchen betroffenen Anbieter des Internetzugangsdienstes als verfahrensleitende Anordnung 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 beweissichernde Anordnung 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 leerläuft. 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. Die beweissichernde Anordnung soll dabei auch verhindern, dass eine Bestandsdatenauskunft des Internetzugangsdienstes unter Verwendung von vorsorglich gespeicherten IP-Adressen (§ 2 Absatz 1 in Verbindung mit § 174 Absatz 5 Nummer 9 TKG-E), die – in Abhängigkeit des Fortgangs des Referentenentwurfs eines Gesetzes zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren (siehe dazu näher in Begründung zu Artikel 11) – voraussichtlich für drei Monate zu speichern sind, wegen Datenverlustes scheitert. Je nach Zeitpunkt der Antragstellung und Dauer des Verfahrens können auch in diesen Fällen die Daten wegen Zeitablaufs verlustig gehen.

Absatz 3 regelt daher, dass der Anbieter eines Internetzugangsdienstes anhand der durch den Diensteanbieter an das Gericht übermittelten Daten nach § 2 Absatz 2 Nummer 1 Buchstabe b und c, also anhand Internetprotokoll-Adresse einschließlich Portnummer, die

Zuordnung zum Anschlussinhaber unverzüglich vornehmen muss. § 174 Absatz 1 Satz 3 in Verbindung mit Absatz 5 Nummer 9 TKG-E, der die in § 2 Absatz 1 Satz 1 geregelte Befugnis zur Datenverarbeitung ergänzt, berechtigt den Internetzugangsdienst, hierbei – neben sämtlichen unternehmensinternen Datenquellen – auch die nach § 177 Absatz 1 TKG-E vorsorglich gespeicherten Daten zu verwenden und das Ergebnis der Zuordnung in einem Zwischenschritt der Bestandsdatenauskunft betriebsintern zu speichern. Die so ermittelten (Identitäts-)Daten (vergleiche § 2 Absatz 2 Nummer 2) sind gemäß § 3 Absatz 5 erst nach Rechtskraft eines stattgebenden Beschlusses an den Antragsteller herauszugeben oder aber ohne Herausgabe zu löschen. Die Löschverpflichtung nach Abschluss des Verfahrens ergibt sich ebenfalls aus Absatz 5.

**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 beweissichernden Anordnungen 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 nationalen Strafverfolgungsbehörden herausgegeben werden. Hinsichtlich der Herausgabe an Strafverfolgungsbehörden der Mitgliedstaaten gelten gesonderte Regelungen (E-Evidence). Für andere Zwecke dürfen die Daten jedoch nicht verwendet werden.

**Zu Absatz 5**

Absatz 5 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 beweissichernden Anordnung 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 6**

Die Neuregelung in § 3 Absatz 1 bis 4 ermöglicht auch den Zugriff auf Daten, die vom Schutzbereich des Fernmeldegeheimnisses erfasst sind. Die Vorschrift trägt dem Zitiergebot nach Artikel 19 Absatz 1 Satz 2 GG Rechnung.

**Zu § 4 (Sperrung von Nutzerkonten in sozialen Netzwerken)**

§ 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 betroffenen Person einen Diensteanbieter. dazu verpflichten, ein spezifisches Nutzerkonto zeitweise zu sperren, um zukünftige Rechtsverletzungen zu verhindern. Der Begriff des Diensteanbieters umfasst auch den Anbieter eines sozialen Netzwerks (§ 1 Absatz 2 Nummer 1, Absatz 4). Die Sperrung des Nutzerkontos muss in jedem Einzelfall verhältnismäßig sein. Da sich der Antrag gegen den Dienstanbieter richtet, ist es möglich, gegen Nutzer vorzugehen, deren Identität nicht bekannt ist.

Kontosperrungen werden nach gegenwärtiger Praxis von Plattformbetreibern auf vertraglicher Basis, ausgehend von den jeweiligen Nutzungsbedingungen ausgesprochen. Diese sehen bei Vertragsverletzungen, also Verstößen gegen die jeweiligen Nutzerbedingungen, oft eine Deaktivierung des Accounts vor. Soweit Rechte Dritter beeinträchtigt werden, die kein Vertragsverhältnis mit dem Plattformbetreibern haben, scheiden vertragliche Ansprüche des Betroffenen auf Accountsperren gegenüber dem Plattformbetreibern allerdings aus. In Betracht kommen insofern zwar deliktische Ansprüche aus § 1004 BGB analog. Insoweit fehlt es allerdings bisher an gerichtlichen Entscheidungen, so dass die Anforderungen durch die Rechtsprechung bisher nicht konturiert sind. Eine spezialgesetzliche Regelung schafft demgegenüber klare Voraussetzungen für den schnellen und effektiven Schutz der Persönlichkeitsrechte im Internet. Sie definiert präzise, in welchen Fällen und unter welchen Voraussetzungen ein beschleunigtes Eingreifen zulässig ist, und vermeidet dadurch sowohl eine Überdehnung als auch eine unklare Rechtsanwendung. Dem Betroffenen soll mit § 4 zusätzlich ein Mittel an die Hand gegeben werden, mit geringem Kostenrisiko und mit wenig prozessualen Hürden weitere schwerwiegende Rechtsverletzungen zu verhindern. Bei drohenden wiederholten Fällen von schweren Online-Persönlichkeitsrechtsverletzungen ist ein besonders schnelles Einschreiten erforderlich. Um der besonderen Gefährdungslage gerecht zu werden, ist die Schaffung einer speziellen Regelung erforderlich, die zum einen die Voraussetzungen für eine Sperre eindeutig definiert und zum anderen geringe prozessuale Hürden für die prozessuale Durchsetzung vorsieht.

Mit der Nutzung eines Accounts bei sozialen Netzwerken wird die grundrechtlich geschützte Meinungsfreiheit wahrgenommen und am grundrechtlich geschützten Meinungsstreit teilgenommen. Die Nutzung eines Accounts bei sozialen Netzwerken fällt damit in den Schutzbereich des Artikel 5 GG. Zudem können – je nach Fallgestaltung – auch weitere Grundrechte des Nutzes betroffen sein (zum Beispiel Artikel 4 und 12 GG). Auf Seiten des (kommerziellen) Plattformbetreibers ist die Berufsausübungsfreiheit (Artikel 12 Absatz 1 GG) berührt. Eine gesetzliche Bestimmung, die die gerichtliche Anordnung einer Sperrung des Nutzerkontos erlaubt, unterliegt daher verfassungsrechtlichen Grenzen. Dabei ist in Rechnung zu stellen, dass der Staat anders als die privaten Plattformbetreiber einer unmittelbaren Bindung an die Grundrechte des Nutzers unterliegt, sich gleichzeitig aber nicht selbst auf Grundrechte berufen kann. Aus der bislang ergangenen Judikatur zu privatrechtlichen Accountsperren lassen sich daher nur sehr eingeschränkt Rückschlüsse auf die Zulässigkeit staatlich angeordneter Sperrungen des Nutzerkontos ziehen.

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). Zudem kann, je nach Fallkonstellation, auch das Recht auf Pressefreiheit sowie die Freiheit der Berichterstattung durch Rundfunk und Film aus Artikel 5 Absatz 1 Satz 2 GG zu berücksichtigen sein.

Auf Seiten des Diensteanbieters 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 (vergleiche BGH ZUM-RD 2017, 515 Rn. 24 und BGHZ 202, 242 = ZUM-RD 2015, 154 Rn. 28 m. w. N.).

**Zu Absatz 1 und Zu Absatz 2**

Absatz 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 betroffenen Diensteanbieter.

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 (vergleiche BGH, Urt. v. 22.02.2022, VI ZR 1175/20, GRUR 2022, 735; 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 (vergleiche § 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. Aufgrund der gefestigten Rechtsprechung ist eine Aufnahme von Regelbeispielen in den Tatbestand nicht erforderlich. Eine solche liefe vielmehr Gefahr, die erforderliche Flexibilität der Rechtspraxis, gegebenenfalls auch kurzfristig auf neue Ausprägungen von Persönlichkeitsrechtsverletzungen im sich dynamisch entwickelnden digitalen Raum reagieren und Nachjustierungen hinsichtlich der Anforderungen vornehmen zu können, zu sehr einzuschränken.

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 eröffnen und betreiben möchte. Damit wird der Diensteanbieter 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. Absatz 1 Satz 2 behandelt den Fall, dass ein Nutzer mehrere Konten führt. In diesem Fall muss das Gericht prüfen, ob die Sperrung der einzelnen Nutzerkonten oder Unterkonten erforderlich ist (siehe auch OLG Bamberg, Urteil vom 28.07.2025 – 4 U 62/25 e). Dabei sind auch die Art und inhaltliche Ausgestaltung des jeweiligen Kontos zu berücksichtigen, also ob es sich zum Beispiel um ein ausschließlich für (rechtmäßige) geschäftliche Zwecke genutztes Konto handelt.

**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, so können unter anderem Fälle der Unzustellbarkeit von dieser Nummer erfasst werden. Hierbei kann auf die nicht abschließenden Kriterien für eine missbräuchliche Verwendung in Artikel 23 Absatz 3 DSA zurückgegriffen werden. Demzufolge können zumindest die absolute Anzahl der offensichtlich rechtswidrigen Inhalte, die bereitgestellt wurden, deren relativer Anteil an der Gesamtzahl der bereitgestellten Einzelinformationen, die Schwere der Rechtsverletzung, einschließlich der Art der rechtswidrigen Inhalte, und deren Folgen sowie die von dem Nutzer verfolgten Absichten, sofern diese Absichten ermittelt werden können, berücksichtigt werden. 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 Diensteanbieter 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 zu-gleich 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. Ansprüche aus Störerhaftung können daher auch weiterhin unabhängig von § 4 geltend gemacht werden.

**Zu § 5 (Gerichtliches 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, soweit dieses Gesetz nichts anderweitig regelt. 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. Dem Betroffenen soll bei besonders schwerwiegenden Verletzungen ein einfaches und kostengünstiges Mittel an die Hand gegeben werden, weiteren Verletzungshandlungen entgegenzuwirken.

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 in ihrem Antrag darauf hinweisen, dass die Geheimhaltung des Aufenthaltsortes notwendig ist. Dies gilt auch für den Rechtsverletzer, sofern dieser als Beteiligter zum Verfahren hinzugezogen wurde. In der Folge stellt das Gericht durch entsprechende Aktenführung sicher, dass die Daten gegenüber den anderen Verfahrensbeteiligten nicht bekannt werden. Da nach § 13 Absatz 1 FamFG ein Akteneinsichtsrecht nur besteht, soweit nicht schwerwiegende Interessen eines Beteiligten oder eines Dritten entgegenstehen, hat das Gericht bei Vorliegen dieser Voraussetzungen sicherzustellen, dass die Daten nicht im Rahmen der Akteneinsicht den anderen Verfahrensbeteiligten bekannt 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, zum Beispiel 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**

Die Wirksamkeit der Entscheidung sowohl über die Auskunftserteilung gem. § 2 Absatz 4, als auch über die Accountsperre gem. § 4 Absatz 4 wird an die Rechtskraft gekoppelt (ähnlich wie in § 184 Absatz 1 Satz 1 FamFG).

Grundsätzlich werden Beschlüsse in FamFG-Verfahren gemäß § 40 Absatz 1 FamFG bereits mit Bekanntgabe und damit bereits vor Rechtskraft wirksam. Nach § 86 Absatz 2 FamFG sind Beschlüsse mit Wirksamwerden auch vollstreckbar. Dies könnte sowohl beim Auskunftsverfahren als auch bei der Kontosperre unbillige Folgen nach sich ziehen, wenn eine Beschwerde entweder des Anbieters oder des Nutzers Erfolg hat. Bei der Entscheidung über die Zulässigkeit der Auskunfterteilung und der Verpflichtung zur Auskunfterteilung würde die Wirksamkeit der erstinstanzlichen Entscheidung nämlich dazu führen, dass die Auskunft unmittelbar erteilt werden kann und muss. Die Offenlegung der Identität des Nutzers ist aber irreversibel. Eine erfolgreiche Beschwerde würde in diesem Fall die Auskunfterteilung nicht mehr verhindern können und faktisch ins Leere laufen.

Mit der Koppelung der Wirksamkeit an die Rechtskraft in Bezug auf die Accountsperre soll sichergestellt werden, dass keine auch nur zeitweise unberechtigte Kontosperrung erfolgt, wenn das Beschwerdegericht die Voraussetzungen hierfür als nicht gegeben erachtet. In

Anbetracht der Erheblichkeit der mit einer Kontosperrung verbundenen Folgen muss der Antragsteller die Entscheidung des Beschwerdegerichts abwarten.

**Zu Absatz 5**

Statthaftes Rechtsmittel gegen die Entscheidung ist die Beschwerde gemäß den §§ 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, verpflichtet das Gericht den betroffenen Anbieter, den Nutzer zu unterrichten. Diese Pflicht besteht allerdings nur, soweit die Unterrichtung dem Anbieter auch tatsächlich möglich ist. Aufgrund der Eilbedürftigkeit muss der Anbieter seiner Verpflichtung ohne schuldhaftes Zögern nachkommen. Damit soll gewährleistet werden, dass dem Nutzer die Möglichkeit gewährt wird, bei Gericht eine Stellungnahme einzureichen und sich gegebenenfalls zu verteidigen. Hierfür muss der Nutzer wissen, welches Verhalten bzw. welche Äußerungen ihm genau vorgeworfen werden und welche Maßnahmen ihm drohen. Die Nummern 1 bis 5 enthalten daher Vorgaben zum Inhalt der Unterrichtung des Nutzers. Aufgrund der Eilbedürftigkeit setzt das Gericht gemäß Nummer 5 eine Stellungnahmefrist für den Nutzer. Die Dauer der Frist ist unter Berücksichtigung der Umstände des Einzelfalls zu bemessen. 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. Kommt der Anbieter seinen Verpflichtungen nicht oder nur unzureichend nach, kann das Gericht Zwangsmittel nach § 35 FamFG anwenden. Soweit der Nutzer einen Antrag auf Hinzuziehung als Beteiligter stellt, muss er dem Gericht seine Identität mitteilen, damit aus den Akten unzweifelhaft hervorgeht, wer Beteiligter eines Verfahrens ist und Beteiligtenrechte ausüben kann.

**Zu Absatz 3**

Bei schriftlicher Bekanntgabe des Beschlusses sind im Rubrum die Daten der beteiligten Personen aufgeführt. Die Schwärzungspflicht der Daten des Nutzers soll verhindern, dass der Antragsteller diese Daten erhält, obwohl er keinen Anspruch darauf hat. Eine Schwärzung muss auch bei stattgebendem Beschluss erfolgen, da dieser noch mit der Beschwerde angefochten werden kann.

**Zu § 7 (Vertretung durch 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. Der Begriff der zivilgesellschaftlichen Organisationen umfasst dabei sämtliche juristische Personen des Privatrechts, bei denen die Voraussetzungen der Nummern 1 bis 3 vorliegen. Durch diese weite Auslegung sollen ein zu enges Verständnis, durch das bestimmte Organisationen zum Nachteil des Antragstellers ausgeschlossen werden könnten, sowie eine zusätzliche Belastung der Gerichte aufgrund der Prüfung weiterer, teils mit erheblichem Aufwand zu ermittelnder Voraussetzungen vermieden werden.

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 Verfahrensstandschaft oder eines Verbandsantragsrechts 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 (vergleiche 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 einem Verbandsantragsrecht 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 Anträge, die nach diesem Gesetz gestellt werden, das heißt für die Anträge hinsichtlich der Einleitung des Auskunftsverfahrens einschließlich der beweissichernden Anordnung (§ 3 GgdG) und für Anträge, 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 (vergleiche § 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 – und in bestimmten Fällen auch die örtliche – 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 den §§ 2 und 4 dieses Gesetzes dürfte regelmäßig der deliktische Gerichtsstand nach Artikel 7 Nummer 2 EuGVVO gegeben sein, der sowohl die internationale als auch die örtliche Zuständigkeit regelt.

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 (vergleiche 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 Verbindung mit Artikel 18 Absatz 1 EuGVVO am Wohnsitz des Verbrauchers 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 beweissichernden Anordnung nach § 3 dieses Gesetzes, die innerhalb des Auskunftsverfahrens unverzüglich ergehen soll, dürfte im Regelfall eine Zuständigkeit in der Hauptsache gegeben sein. Daher wird die Wirkung der beweissichernden Anordnung häufig nicht auf den Mitgliedstaat beschränkt sein, in dem sie erlassen wurde (vergleiche Artikel 2 Buchstabe a Unterabsatz 2 EuGVVO). Anderenfalls kann die Zuständigkeit deutscher Gerichte auch mit Artikel 35 EuGVVO begründet werden; die beweissichernde Anordnung wirkt dann jedoch nur im Inland.

Für den Anspruch auf Kontosperrung wird regelmäßig die besondere internationale und örtliche 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 Diensteanbieter, 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, Artikel 6 EuGVVO Rn. 3.1).

**Zu Absatz 2**

Die sich in Konsequenz des § 75 GVG ergebende Vorgabe, alle erstinstanzlichen Verfahren nach dem GgdG stets in Kammerbesetzung durchführen zu müssen, liefe der Zielsetzung des Entwurfs, dem Betroffenen zügig Auskunft über die Identität des Nutzers zu verschaffen, zuwider. Entsprechend der zivilprozessualen Regelung für Streitigkeiten über Ansprüche aus Veröffentlichungen im Internet gemäß § 348 Absatz 1 Satz 2 Nummer 2k ZPO in Verbindung mit § 71 Absatz 2 Nummer 7 GVG ist daher die Möglichkeit der Übertragung auf den Einzelrichter entsprechend § 348a ZPO vorgesehen, um eine flexible, die tatsächliche und rechtliche Schwierigkeit und Bedeutung des Falles im Einzelfall berücksichtigende Handhabung zu ermöglichen. Dabei können auch Nicht-Katalogsachen unter den Voraussetzungen von § 348a Absatz 1 Nummer 1 bis 3 ZPO auf den Einzelrichter übertragen werden (zum Beispiel bei Beleidigungen per Textnachricht, die keine „Veröffentlichung“ im Sinne des § 71 Absatz 2 Nummer 7 GVG in Verbindung mit § 348 Absatz 1 Satz 2 Nummer 2k ZPO darstellen dürften).

**Zu Absatz 3**

Mit Absatz 3 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 Ansprüche aus den Rechtsverletzungen, für die vorher ein Auskunftsverfahren durchgeführt wurde. Hierdurch wird die Möglichkeit eröffnet, dass dieselbe Kammer über weitere Ansprüche entscheiden kann, die aus der Rechtsverletzung resultieren. Dies dient der Prozessökonomie und fördert eine einheitliche Bewertung desselben Sachverhalts.

**Zu Absatz 4**

Mit Absatz 4 wird es dem Betroffenen ermöglicht, nach Abschluss eines Verfahrens bei einem bestimmten Gericht wegen Sperrung des Nutzerkontos nach § 4 bei demselben Gericht materielle Ansprüche geltend zu machen, wenn diese auf derselben Rechtsverletzung beruhen wie der Antrag auf Sperrung des Nutzerkontos. In Betracht kommen dabei Ansprüche gegen den Diensteanbieter auf Löschung gemäß § 1004 BGB analog oder Ansprüche gegen den Rechtsverletzer, wie solche auf Beseitigung, Unterlassung oder Schadensersatz. Im Wesentlichen dürfte das dann relevant sein, wenn ein Antrag auf Sperrung des Nutzerkontos abgewiesen wurde, der Betroffene aber von dem Diensteanbieter die Löschung des rechtswidrigen Inhalts aus § 1004 BGB analog erwirken möchte. Hierdurch wird die Möglichkeit eröffnet, dass dieselbe Kammer über weitere Ansprüche entscheiden kann, die aus derselben Rechtsverletzung resultieren. Dies dient der Prozessökonomie und fördert eine einheitliche Bewertung desselben Sachverhalts.

**Zu Absatz 5**

Mit der Möglichkeit, per Verordnung die Anträge, die nach diesem Gesetz gestellt werden einem Landgericht für den Bezirk mehrerer Landgerichte zuzuweisen, wird auf die Konzentration solcher Verfahren und damit auf die Zusammenfassung des Fallaufkommens bei einem Landgericht 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. Mit gerichtlichem Verfahren sind sämtliche Verfahrensschritte gemeint, einschließlich Vollstreckung.

Die Zustellungsmöglichkeit gilt ebenso für Schriftstücke, die solche Verfahren einleiten oder vorbereiten, und für zivilrechtliche Unterlassungsaufforderungen. 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 (vergleiche § 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 Strafgesetzbuches)**

**Zu Nummer 1**

In die Inhaltsübersicht sollen die Änderung der Überschrift zu § 184k StGB und die Überschriften der neu eingefügten Vorschriften (§§ 201b und 202e StGB) aufgenommen werden.

**Zu Nummer 2**

Es handelt sich um eine Folgeänderung zu Artikel 2 Nummer 8. Die Ergänzung des Katalogs des § 127 Absatz 1 Satz 2 Nummer 2 Buchstabe a StGB ist notwendig, um das Angebot von Waren und Dienstleistungen zur Begehung von Taten nach § 202e StGB, die auf kriminellen Handelsplattformen im Internet angeboten werden, rechtssicher zu erfassen.

**Zu Nummer 3**

Die Herstellung manipulierter Bildinhalte, also Abbildungen, die infolge einer Bearbeitung, Umgestaltung oder Verbindung mit weiteren Inhalten mittels eines Computerprogramms den Anschein erwecken, dass eine Person unter 14 Jahren sexuelle Handlungen vorgenommen hat oder nackt dargestellt ist („sexualisierte Deepfakes“), ist gemäß § 184b Absatz 1 Satz 1 Nummer 4 StGB nur unter weiteren Voraussetzungen – in der Regel einer Verbreitungs- oder Verwendungsabsicht im Sinne der Nummern 1 und 2 der jeweiligen Normen – strafbar. Eine Herstellung solcher manipulierter Bildaufnahmen für den Eigengebrauch ist bislang nicht strafbar. Das Sich-Verschaffen, der Besitz oder Abruf von Bildinhalten ist indes bei kinderpornographischen Inhalten, die ein tatsächliches oder wirklichkeitsnahes Geschehen wiedergeben, nach § 184b Absatz 3 StGB strafbar. Die darin liegende Diskrepanz, dass wirklichkeitsnahe Inhalte, die bei Deepfakes in der Regel gegeben sind, zwar zum Eigengebrauch straflos hergestellt, aber nicht „abgerufen“ oder „besessen“ werden dürfen, soll dadurch beseitigt werden, dass künftig auch die Herstellung von kinderpornographischen Inhalten, die ein wirklichkeitsnahes Geschehen wiedergeben, in § 184b Absatz 1 Satz 1 Nummer 3 StGB aufgenommen wird. Damit ist § 184b Absatz 1 Satz 1 Nummer 3 StGB für „sexualisierte“ Deepfakes als lex specialis im Verhältnis zu § 184k Absatz 1 Nummer 4 StGB-E anzusehen (vergleiche dazu die Begründung zu Nummer 5).

**Zu Nummer 4**

Um die Herstellung von „sexualisierten“ Deepfakes auch bei Jugendlichen zu erfassen, soll auch § 184c Absatz 1 Nummer 3 StGB um „wirklichkeitsnahe Geschehen“ ergänzt werden, wenngleich sich hier die Besitzstrafbarkeit anders als in § 184b Absatz 3 StGB nach § 184c Absatz 3 StGB nur auf Inhalte bezieht, die ein tatsächliches Geschehen wiedergeben. Bei Jugendlichen ist insbesondere auch die Ausschlussklausel des § 184c Absatz 4 StGB zu beachten, nach der § 184c Absatz 1 Nummer 3 StGB nicht anzuwenden ist auf Handlungen von Personen in Bezug auf einen solchen jugendpornographischen Inhalt, den sie ausschließlich zum persönlichen Gebrauch mit Einwilligung der dargestellten Personen hergestellt haben. § 184c StGB ist damit im Anwendungsbereich jugendpornographischer Inhalte – einschließlich Deepfakes – lex specialis zu § 184k StGB.

**Zu Nummer 5 (§ 184k StGB)**

Die Vorschrift soll als neue zentrale Vorschrift im 13. Abschnitt den Schutz vor Verletzungen der Intimsphäre durch Bildaufnahmen regeln. Dabei sollen die verschiedenen Erscheinungsformen des kriminologisch unter dem Begriff der „bildbasierten sexualisierten Gewalt“ oder der „bildbasierten sexuellen Belästigung“ bezeichneten Phänomens erfasst werden. Dies betrifft einerseits die nicht-einvernehmliche Herstellung von intimen Bildern, Videos und mittels Informationstechnik beziehungsweise Künstlicher Intelligenz manipulierten Materials („Deepfakes“). Darunter fällt auch der „digitale Voyeurismus“, also das heimliche

Filmen oder Fotografieren zum Beispiel unter der Kleidung (einschließlich der bisher ausschließlich von § 184k StGB g. F. erfassten Formen des „Upskirting“ und „Downblousing“), in Umkleiden, auf der Toilette, in Saunalandschaften oder am Strand, ferner auch Bildmaterial von nicht-einvernehmlichen, gewalttätigen sexuellen Handlungen (Vergewaltigungsvideos) oder gezielt in sexuell bestimmter Weise erstellte Ausschnitte, die bekleidete intime Körperteile zeigen. Andererseits erfasst werden soll das nicht-einvernehmliche Teilen von einvernehmlich oder nicht-einvernehmlich erlangten Bildern, Videos oder Deepfakes (einschließlich der „Revenge Porns“ als Unterfall). Die Drohung mit der Vornahme entsprechender Handlungen, also insbesondere der Veröffentlichung entsprechenden Materials, auch sexuelle Erpressung oder „Sextortion“ genannt, fällt künftig unter § 241 Absatz 1 StGB (Bedrohung), der bereits in seiner geltenden Fassung rechtswidrige Taten gegen die sexuelle Selbstbestimmung als taugliche Anknüpfungstaten in Bezug nimmt.

**Absatz 1**

Der Begriff der „Bildaufnahme“ erfasst insbesondere Fotos und Videos (*Eisele*, in: Tübinger Kommentar, 31. Auflage 2025, § 201a Rn. 6). Er ist enger als der Begriff der „Abbildung“ oder des „Bildnisses“; Gemälde, Zeichnungen oder Karikaturen sind folglich nicht erfasst. Die Bildaufnahme „einer anderen Person“ muss das Abbild einer natürlichen lebenden Person zeigen (vergleiche BGH NStZ-RR 2019, 143).

Eine sexuelle Handlung einer anderen Person im Sinne des Absatzes 1 Nummer 1 ist eine Handlung im Sinne des § 184h Nummer 1 StGB. Darunter fallen solche, die im Hinblick auf das jeweils geschützte Rechtsgut von einiger Erheblichkeit sind. Bildaufnahmen von sexuellen Handlungen unterfallen unabhängig davon, wo die sexuellen Handlungen stattfinden, der Intimsphäre und damit dem Schutz des allgemeinen Persönlichkeitsrechts.

In Absatz 1 Nummer 2 sollen – dem § 184k StGB g. F. entsprechend – die unbekleideten Genitalien, das unbekleidete Gesäß oder die unbekleidete weibliche Brust konkret genannt werden. Es genügt, wenn eines der genannten Merkmale, etwa im Rahmen einer Ganzkörperaufnahme ganz oder teilweise abgebildet ist. Nicht erforderlich ist, dass die Bildaufnahme explizit nur einen Ausschnitt mit den jeweiligen intimen nackten Körperteilen zeigt. Nicht erfasst werden Abbildungen von Körperteilen, bei denen die in Absatz 1 Nummer 2 genannten Merkmale ganz oder teilweise nicht zu sehen sind, etwa ein nackter Arm, ein nacktes Bein oder ein nackter Rücken. Aus diesem Grund wurde in Absatz 1 das in § 201a Absatz 3 StGB der geltenden Fassung enthaltene Merkmal der „Nacktheit einer anderen Person“ (eingefügt im parlamentarischen Verfahren, vergleiche Bundestagsdrucksache 18/3202, S. 28) nicht aufgegriffen. Bereits zur geltenden Rechtslage stellt sich die Frage, ob diese Formulierung überschießend ist, weil mit der „Nacktheit einer Person“ keine vollständige Nacktheit gemeint sein muss (*Hoven*, Stellungnahme im Rechtsausschuss zur Einführung des § 184k StGB g. F., S. 6) und damit auch Personen in Unterwäsche oder Badebekleidung erfasst sein können. Die Auslegung des Merkmals ist in der strafrechtlichen Literatur jedenfalls umstritten (für die Einbeziehung nicht vollständiger Nacktheit Fischer/Anstötz, in: Fischer, Strafgesetzbuch mit Nebengesetzen, 73. Auflage 2026, § 201a Rn. 37; zweifelnd Graf, in: Münchener Kommentar zum Strafgesetzbuch, 5. Auflage 2025, § 201a StGB Rn. 81). Die die „Nacktheit einer Person“ erfassende Bildaufnahmen sind bislang allerdings nur strafbar, wenn sie Personen unter achtzehn Jahren zum Gegenstand haben und gegen Entgelt verschafft bzw. hergestellt oder angeboten werden und eine Verschaffungsabsicht gegen Entgelt besteht. Für Kinder und Jugendliche kommt es nach dem geltenden Kinder- und Jugendpornographiebegriff des § 184b Absatz 1 Satz 1 Nummer 1 Buchstabe b StGB und § 184c Absatz 1 Nummer 1 Buchstabe b StGB, der auch die Wiedergabe eines teilweise unbekleideten Kindes als ausreichend ansieht, sofern eine aufreizend geschlechtsbetonte Körperhaltung gegeben ist, auf eine vollständige Nacktheit allerdings nicht an. Der Begriff soll daher im Interesse eines umfassenderen Schutzes der Personen unter 18 Jahren für diese beibehalten – und in die hiesige Regelung überführt (vergleiche Absatz 2) – werden.

Für eine Bildaufnahme der in Absatz 1 Nummer 2 genannten intimen Körperteile ist nicht erforderlich, dass die Person, deren Körperteile gezeigt werden, identifizierbar ist, also entweder ihr Gesicht oder andere markante Merkmale in der Darstellung ersichtlich sind. Insofern unterscheidet sich die neue Regelung von § 201a StGB und § 33 in Verbindung mit § 22 KunstUrhG. Artikel 2 Absatz 1 schützt in Verbindung mit Artikel 1 Absatz 1 GG die engere persönliche Lebenssphäre, insbesondere auch den Intim- und Sexualbereich, und gewährleistet das Recht des Einzelnen, grundsätzlich selbst zu bestimmen, aus welchem Anlass und in welchen Grenzen er persönliche Lebenssachverhalte offenbart (vergleiche BVerfGE 120, 224, 238 f.; 65, 88, 87, 97; 65, 1, 43). Die Intimsphäre kann beeinträchtigt sein, wenn Bildmaterial von intimen Körperteilen einer Person ohne deren Einwilligung hergestellt oder verwendet wird. Dies gilt auch für den Fall, dass die abgebildete Person selbst auf den Abbildungen nicht erkennbar sein sollte. Nummer 2 dient ferner der Umsetzung von Artikel 5 Absatz 1 Buchstabe a der Richtlinie (EU) 2024/1385 des Europäischen Parlaments und des Rates vom 14. Mai 2024 zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt (vergleiche VI.).

Absatz 1 Nummer 3 erfasst Bildaufnahmen, die in sexuell bestimmter Weise abgebildete bekleidete intime Körperteile einer anderen Person enthalten. Die Vorschrift soll insbesondere die Herstellung und Verbreitung voyeuristischer Bild- oder Filmaufnahmen erfassen. Aufnahmen, die lediglich Ausschnitte von intimen Körperteilen enthalten, unterfallen nach geltendem Recht häufig nicht § 201a StGB oder § 33 in Verbindung mit § 22 KunstUrhG, weil sie das Gesicht der betreffenden Person nicht erkennen lassen und damit eine Identifizierbarkeit regelmäßig nicht gegeben ist. Der strafrechtliche Schutz des § 184k StGB der geltenden Fassung („Upskirting“, „Downblousing“) greift zwar auch dann, wenn Personen nicht erkennbar sind, aber nur, wenn die betreffenden Körperteile grundsätzlich gegen Anblick geschützt sind und der Täter eine Lücke im Anblickschutz – etwa unter dem Rock oder von oben oder seitlich – zur Anfertigung der Bildaufnahmen ausnutzt. Künftig sollen generell Aufnahmen bekleideter intimer Körperteile dem strafrechtlichen Schutz unterfallen, sofern diese Körperteile unbefugt in sexuell bestimmter Weise abgebildet sind. Der Begriff „in sexuell bestimmter Weise“ ist bereits in § 184i Absatz 1 StGB enthalten, so dass auf die hierzu von der Rechtsprechung herausgearbeiteten Grundsätze zurückgegriffen werden kann. Im entsprechenden Kontext kann eine Bildaufnahme, die bekleidete intime Körperteile abbildet sowohl objektiv – nach dem äußeren Erscheinungsbild – als auch subjektiv – nach den Umständen des Einzelfalls – sexuell bestimmt sein (für körperliche Berührungen vergleiche BGHSt 63, 98, 100 ff. m.w.N.). Weist die Bildaufnahme nach dem Inhalt dessen, was abgebildet ist, bereits nach dem äußeren Erscheinungsbild einen sexuellen Charakter auf, ist nicht erforderlich, dass der Täter auch von sexuellen Absichten geleitet ist; insofern genügen auch andere Motive wie Wut, Sadismus, Scherz oder die Demütigung des Opfers (vergleiche BGH NJW 2014, 3737, 3738). Darunter können Bildaufnahmen intimer Körperteile fallen, die etwa aus einer dem begrenzten Raum in öffentlichen Verkehrsmitteln geschuldeten oder eigens vom Täter hergestellten körperlichen Nähe resultieren, etwa die bisherigen Upskirting oder Downblousing-Bildaufnahmen. Darüber hinaus können auch ambivalente Abbildungen, die für sich betrachtet nicht ohne Weiteres einen sexuellen Charakter aufweisen, tatbestandsmäßig sein; in diesem Fall ist im Rahmen der Würdigung aller Umstände zu berücksichtigen, ob der Täter von sexuellen Absichten geleitet war. Abzustellen ist auf das Urteil eines objektiven Betrachters, der alle Umstände des Einzelfalls kennt (BGHSt 63, 98, 103).

Absatz 1 Nummer 4 soll sogenannte „sexualisierte“ oder „pornographische“ Deepfakes erfassen, das heißt, Bildaufnahmen einer Person, die infolge einer Veränderung, Neugestaltung oder Verbindung mit weiteren Inhalten mittels eines Computerprogramms den Anschein erwecken, dass eine Person sexuelle Handlungen vorgenommen hat oder ihre intimen Körperteile nackt dargestellt sind. Gemeint sind damit in aller Regel Anwendungen, die auf künstlicher Intelligenz basieren, aber auch Computerprogramme, die es ohne Verwendung generativer künstlicher Intelligenz ermöglichen, Montagen aus Fotos oder Videos herzustellen. „Weitere Inhalte“ sind solche im Sinne des § 11 Absatz 3 StGB. Bei der

Erstellung eines sexualisierten Deepfakes sind dies in erster Linie weitere Bildinhalte, aber auch Geräusche oder Texte. So kann das Abbild einer Person mit künstlich generierten nackten Körperteilen verbunden und im Falle der Erstellung von Videos mit künstlich generierten Lauten, Geräuschen oder Sätzen unterlegt werden. Für die Verwirklichung des Absatzes 1 Nummer 4 ist allerdings Voraussetzung, dass die Person individualisierbar ist, weil es sich ansonsten um rein fiktive Darstellungen handeln würde, bei denen kein konkretes Rechtsgut verletzt ist. Ist eine Individualisierbarkeit gegeben, ist in den Fällen sexualisierter oder pornographischer Deepfakes bereits mit der Herstellung regelmäßig sowohl ein ehrverletzender Charakter als auch ein Eingriff in das allgemeine Persönlichkeitsrecht der betroffenen Person anzunehmen, weil ihre persönlichen Merkmale in einem von ihr nicht mehr beinflussbaren – zudem sexuellen bzw. intimen – Kontext verwendet werden. Das allgemeine Persönlichkeitsrecht schützt den Einzelnen auch vor verfälschenden oder entstellenden Darstellungen seiner Person in der Öffentlichkeit, die von nicht ganz unerheblicher Bedeutung für die Persönlichkeitsentfaltung sind (BVerfGE 99, 185, 194). Der verfälschende und entstellende Kontext wird mit Herstellung in der Deepfake-Aufnahme perpetuiert und kann vom Hersteller jederzeit sowohl zu eigenen als auch fremden Zwecken verwendet werden. Selbst wenn der Hersteller der Aufnahme diese nur für den eigenen Gebrauch fertigen sollte, geht mit einer Nutzung auf künstlicher Intelligenz beruhender Anwendungen regelmäßig ein Abspeichern der Daten in einer Cloud einher. Entsprechende Daten lägen unter Umständen bei Drittanbietern, wären im Falle mangelhafter Sicherheits- oder Schutzvorkehrungen dem unberechtigten Zugriff Dritter ausgesetzt und könnten gegebenenfalls unbemerkt kopiert werden. Auch unabhängig von den Möglichkeiten und Gefahren im digitalen Raum ist das Risiko einer Verwendung oder Verbreitung einer entsprechenden Deepfake regelmäßig bereits mit der Anfertigung gegeben.

Tathandlungen sind in allen Fällen das unbefugte Herstellen oder das unbefugte Zugänglichmachen an Dritte.

Das Herstellen umfasst sämtliche Handlungen, mit denen optische Informationen auf einem Bild- oder Datenträger abgespeichert werden (vergleiche Bundestagsdrucksache 15/2466, S. 5). Die visuelle Wahrnehmung durch den Täter oder eine dritte Person ist nicht Voraussetzung, es genügt, dass der Aufnahmegegenstand sichtbar gemacht werden kann (Eisele, in: Tübinger Kommentar Strafgesetzbuch, 31. Auflage 2025, § 201a StGB Rn. 13). Die Herstellung einer Bildaufnahme ist im geltenden Recht bereits vorgesehen in § 184b Absatz 1 Satz 1 Nummer 3 StGB und § 184c Absatz 1 Nummer 3 StGB für kinder- und jugendpornographische Inhalte, die ein tatsächliches Geschehen wiedergeben, und in § 201a Absatz 1 Nummer 1 bis 3 StGB für Inhalte, die den höchstpersönlichen Lebensbereich einer Person verletzen, die sich in einem gegen Einblick besonders geschützten Raum befindet, deren Hilflosigkeit zur Schau gestellt wird oder bei in grob anstößiger Weise dargestellten Verstorbenen. Anders als in § 201a Absatz 1 Nummer 1 ist für die in § 184k Absatz 1 genannten intimen Bildinhalte nicht erforderlich, dass sich die Person in einem gegen Einblick besonders geschützten Raum befindet. Somit werden etwa auch Bildaufnahmen in öffentlich zugänglichen Bereichen wie etwa Saunen erfasst, die nach der Rechtsprechung bislang nicht strafbar waren (vergleiche OLG Koblenz NStZ 2009, 268, 269).

Nur unter weiteren Voraussetzungen strafbar ist derzeit das Herstellen von kinder- und jugendpornographischen Inhalten, die rein fiktive und manipulierte Bilder enthalten (§ 184b Absatz 1 Satz 1 Nummer 4, § 184c Absatz 1 Nummer 4 StGB). Soweit nach § 184k Absatz 1 Nummer 1 StGB künftig die bloße Herstellung von sexualisierten „Deepfakes“, das heißt, von mit Methoden generativer künstlicher Intelligenz unter Verwendung realen Ausgangsmaterials manipulierten Inhalten, die den Anschein erwecken, dass eine reale Person sexuelle Handlungen vorgenommen hat oder nackt abgebildet ist, zum Zwecke der eigenen sexuellen Erregung strafbar ist, sind § 184b Absatz 1 Satz 1 Nummer 3 StGB und § 184c Absatz 1 Nummer 3 StGB zur Vermeidung von Widersprüchen entsprechend anzupassen (vergleiche Nummern 3 und 4). Das bloße Herstellen manipulierter Bilder zum Eigengebrauch begründet zwar im Vergleich zum Zugänglichmachen an Dritte und auch im Vergleich zur Herstellung in Verbreitungsabsicht eine geringfügigere Rechtsgutverletzung,

auch sind die Abbildungen der intimen Körperteile und sexuellen Handlungen, welche die KI-Anwendung erzeugt, nicht real. Gleichwohl wird die betreffende Person, deren reale persönliche Merkmale (in der Regel das Gesicht) für die Erstellung entsprechender Bilder verwendet werden, ohne dass diese Person Einfluss darauf hat, zur sexuellen Stimulation oder zu anderen Zwecken „benutzt“.

Der Begriff des Zugänglichmachens an Dritte wird im geltenden Recht bereits in § 176e StGB und § 201a StGB verwendet. Anders als der im Strafgesetzbuch ebenfalls gebräuchliche Begriff des Verbreitens zielt das Zugänglichmachen gegenüber Dritten nicht auf einen größeren, nicht mehr kontrollierbaren Personenkreis ab, sondern es genügt regelmäßig die Weitergabe an nur eine weitere Person. Ebenfalls tatbestandsmäßig ist die unbefugte Weitergabe einer ursprünglich befugt hergestellten Bildaufnahme. Das Zugänglichmachen an Dritte erfasst auch Echtzeitübertragungen; eine Speicherung der Bilder beim Empfänger ist dafür nicht erforderlich (Eisele, in: Tübinger Kommentar Strafgesetzbuch, 31. Auflage 2025, § 201a Rn. 6).

In subjektiver Hinsicht verlangt der Tatbestand vorsätzliches Handeln. Der Vorsatz muss sich insbesondere auf den jeweiligen Bildinhalt erstrecken. Bei „Zufallsfotos“, die an öffentlich zugänglichen Orten gefertigt werden und im Hintergrund versehentlich Inhalte im Sinne des § 184k Absatz 1 StGB-E enthalten, fehlt es daher bereits an einem vorsätzlichen Handeln.

Das Herstellen oder Zugänglichmachen der Bildaufnahme muss ferner unbefugt sein. In anderen Vorschriften stellt die Unbefugtheit nach überwiegender Auffassung einen Verweis auf die allgemeinen Rechtfertigungsgründe dar (Lackner/Kühl/Heger, StGB, 31. Auflage 2025, § 201a Rn. 9 m. w. N., auch zur Gegenauffassung). Entscheidend ist danach, ob die Herstellung oder Zugänglichmachung von einer Einwilligung oder einer sonstigen Befugnisnorm gedeckt ist. Bei Personen über 18 Jahren entfällt bei Vorliegen einer wirksamen Einwilligung damit in der Regel die Rechtswidrigkeit der Tathandlung. Gleiches gilt im Falle der mutmaßlichen Einwilligung. Eine solche kommt insbesondere in Betracht, wenn sich Personen außerhalb gesellschaftlich anerkannter Bereiche wie Saunen oder FKK-Stränden in Bereichen, in denen mit der Anfertigung von Aufnahmen gerechnet werden muss (zum Beispiel Großveranstaltungen, Konzerte, Festivals, Demonstrationen) offensiv in der Öffentlichkeit nackt zeigen oder sexuelle Handlungen vornehmen und dadurch deutlich machen, dass sie auf die Wahrung ihrer Privatheit keinen gesteigerten Wert legen. Gleiches ist anzunehmen, wenn die Aufnahmen vor den Augen und mit Wissen der Betroffenen vorgenommen werden, ohne dass diese dagegen einschreiten, obwohl sie dazu in der Lage wären.

Für Minderjährige findet der Tatbestand des § 184k StGB ohnehin nur Anwendung, soweit nicht die §§ 184b und 184c StGB aufgrund der höheren Strafandrohungen als leges speciales heranzuziehen sind. Ansonsten dürfte es für die Wirksamkeit der Einwilligung nach allgemeinen Grundsätzen darauf ankommen, ob die entsprechende Person nach ihrer Entwicklung und Reife Wesen, Tragweite und Bedeutung der Handlung erfasst hat und ihren Willen entsprechend danach bestimmen konnte. Bei Kindern unter 14 Jahren wird es insoweit regelmäßig auf die Einwilligung des Erziehungsberechtigten ankommen, sofern diese nicht selbst pflichtwidrig ist und den Interessen des Kindes nicht zuwiderläuft. Das Teilen von Familienfotos im Familienkreis bleibt danach weiterhin straflos, nicht im Interesse des Kindes wäre aber etwa ein Teilen von Bildern auf Plattformen, um weitere Bilder von anderen Kindern erhalten zu können.

Im Anwendungsbereich des § 184k Absatz 1 Nummer 1 und – infolge der durch dieses Gesetz vorgenommenen Ergänzung – der Nummer 4 StGB tritt der Tatbestand auf der Konkurrenzebene regelmäßig hinter den §§ 184b und § 184c StGB zurück. Im Anwendungsbereich des § 184k Absatz 1 Nummer 2 und 3 StGB sind, wenngleich der Begriff der Kinder- und Jugendpornographie bereits recht weitreichend die Wiedergabe eines ganz oder teilweise unbekleideten Minderjährigen in aufreizend geschlechtsbetonter Körperhaltung oder

die sexuell aufreizende Wiedergabe der unbekleideten Genitalien oder des unbekleideten Gesäßes eines Minderjährigen umfasst, Fälle denkbar, in denen die Abbildungen nicht unter die §§ 184b oder 184c StGB fallen; in diesen Fällen soll künftig § 184k Absatz 1 StGB greifen.

Ein Teil der von § 184k StGB-E künftig erfassten Bildaufnahmen dürfte weiterhin von § 201a Absatz 1 Nummer 1 StGB oder von § 22 in Verbindung mit § 33 KunstUrhG erfasst werden; insoweit dürfte § 184k StGB künftig regelmäßig lex specialis sein. Entscheidend dürfte es insoweit auf das konkret verletzte Rechtsgut ankommen. § 201a Absatz 2 StGB enthält mit dem Aspekt der Ansehensschädigung einen eher ehrschädigenden Charakter und ergänzt damit strukturell die Ehrdelikte. Verhaltensweisen, die § 184k StGB künftig unterfallen und auch § 201a Absatz 2 StGB oder verschiedene Ehrdelikte erfüllen, dürften regelmäßig in Tateinheit zueinander stehen.

**Absatz 2**

Absatz 2 entspricht § 201a Absatz 3 StGB g. F., der aufgrund des Sachzusammenhangs und des vorrangig geschützten Rechtsguts der sexuellen Selbstbestimmung beziehungsweise des Intimbereichs als Aspekt des allgemeinen Persönlichkeitsrechts in den 13. Abschnitt des StGB übernommen werden soll.

**Absätze 3 bis 5**

Die Absätze 3 bis 5 entsprechen den bisherigen Absätzen 2 bis 4 des § 184k StGB g. F. Auch die neue, erweiterte Vorschrift soll als relatives Antragsdelikt ausgestaltet sein, eine Klausel für die Wahrnehmung berechtigter Interessen, namentlich der Kunst oder der Wissenschaft, der Forschung oder der Lehre, der Berichterstattung über Vorgänge des Zeitgeschehens oder der Geschichte oder ähnlichen Zwecken, enthalten, und die Einziehung von Tatmitteln anordnen.

**Zu Nummer 6**

§ 201a Absatz 3 StGB soll aufgrund des vorrangig geschützten Rechtsguts der sexuellen Selbstbestimmung beziehungsweise der Intimsphäre als Aspekt des allgemeinen Persönlichkeitsrechts in den 13. Abschnitt des StGB übernommen werden. Dadurch werden die bisherigen Absätze 4 und 5 zu den Absätzen 3 und 4. Der im bisherigen Absatz 4 enthaltene Verweis auf Absatz 3 entfällt.

**Zu Nummer 7**

Aus den im Allgemeinen Teil der Begründung genannten Gründen wird nach § 201a StGB § 201b StGB (Verletzung von Persönlichkeitsrechten durch täuschende Inhalte) eingefügt, der künftig das spezifische Tatunrecht des unbefugten Zugänglichmachens ansehensschädigender sogenannter Deepfakes und vergleichbarer technischer Manipulationen zielgenau erfassen soll, das heißt von mittels eines Computerprogramms erstellten oder veränderten Inhalten (§ 11 Absatz 3 StGB), die den Anschein erwecken, ein tatsächliches Geschehen wiederzugeben. Von § 201b StGB werden beispielsweise Fälle erfasst, in denen mittels künstlicher Intelligenz generierte Videos unbefugt zugänglich gemacht werden, durch die der Anschein erweckt wird, dass ein prominenter Mediziner Werbung für Produkte mache und dieser Anschein geeignet ist, ansehensschädigend zu wirken. In Betracht kommt eine Strafbarkeit nach § 201b StGB zudem bei der unbefugten Zugänglichmachung von mittels künstlicher Intelligenz generierten bildlichen Darstellungen von Personen in leichter Badebekleidung, sofern diese Inhalte zur Ansehensschädigung geeignet sind. § 184k Absatz 1 Nummer 4 StGB-E wäre bei bildlichen Darstellungen bekleideter Personen nicht einschlägig, da jene Vorschrift nur anwendbar ist, wenn der Anschein erweckt wird, dass sexuelle Handlungen, die unbekleideten Genitalien, das unbekleidete Gesäß oder die unbekleidete weibliche Brust einer anderen Person abgebildet seien.

§ 201b StGB-E orientiert sich in Struktur und Begrifflichkeiten in erster Linie an § 201a Absatz 2 StGB. Durch die technologieneutrale Formulierung wird gewährleistet, dass der Tatbestand auch künftige technologische Neuerungen erfassen kann, insbesondere im Bereich von mittels künstlicher Intelligenz erstellten Inhalten. Inhalte sind gemäß § 11 Absatz 3 StGB solche, die in Schriften, auf Ton- oder Bildträgern, in Datenspeichern, Abbildungen oder anderen Verkörperungen enthalten sind oder auch unabhängig von einer Speicherung mittels Informations- oder Kommunikationstechnik übertragen werden. Der Kreis tauglicher Tatobjekte ist damit weiter gefasst als bei den von § 184k Absatz 1 Nummer 4 StGB-E erfassten sexualisierten Deepfakes, bei denen es sich um bildliche Darstellungen handeln muss. Der Inhalt muss den Anschein erwecken, ein tatsächliches Geschehen wiederzugeben. Amateurhafte Darstellungen, die für den durchschnittlichen Betrachter eindeutig als nicht reales Geschehen zu erkennen sind, fallen daher selbst dann nicht unter den Tatbestand, wenn sie in täuschender Absicht weitergegeben werden. § 201b StGB-E erfasst etwa vermeintlich reale, tatsächlich aber verfälschte bildliche Darstellungen des äußeren Erscheinungsbildes einer Person, aber auch fingierte Stimmaufnahmen und Filmsequenzen. Durch die Vorgabe, dass sich der Inhalt auf eine andere Person beziehen muss, wird klargestellt, dass § 201b StGB-E nur personenbezogene Deepfakes erfasst. Inhalte, die fingierte anderweitige Geschehnisse wiedergeben, die keinen erkennbaren Bezug zu lebenden oder verstorbenen (§ 201b Absatz 1 Satz 2 StGB-E) Personen haben, sind daher nicht tatbestandsmäßig. Der Inhalt muss mittels eines Computerprogramms erstellt oder verändert worden sein, also mittels einer durch Daten fixierten Arbeitsanweisung an einen Computer (vergleiche Perron, in: Tübinger Kommentar Strafgesetzbuch, 31. Auflage 2025, § 263a Rn. 5, 33; Fischer/Lutz, in: Fischer, Strafgesetzbuch, 73. Auflage 2026, § 263a Rn. 6, 30). In der Praxis wird es sich hierbei im Regelfall um Systeme künstlicher Intelligenz handeln. Ein Inhalt ist erstellt, wenn er (neu) generiert worden ist. Verändert ist ein Inhalt, wenn sein ursprünglicher Aussagegehalt modifiziert worden ist.

§ 201b StGB setzt, anders als der vom Bundesrat auf Bundestagsdrucksache 21/1383 vorgeschlagene Tatbestand „Verletzung von Persönlichkeitsrechten durch digitale Fälschung“, voraus, dass der Inhalt geeignet ist, dem Ansehen der dargestellten Person erheblich zu schaden. Der Begriff der Eignung zur Ansehensschädigung ist wie bei § 201a Absatz 2 StGB an die Ehrverletzungstatbestände der §§ 185 und folgende StGB angelehnt. Zur Ansehensschädigung im Sinne von § 201b Absatz 1 StGB-E ist der Inhalt geeignet, wenn die dargestellte lebende oder verstorbene Person durch ihn verächtlich gemacht oder in der öffentlichen Meinung herabgewürdigt werden kann (BGH, Urteil vom 27. Februar 2024 – 4 StR 401/22, Beck RS 2024, 8894, Rn. 32, m. w. N.). Durch das Merkmal der Eignung zur „erheblichen“ Ansehensschädigung wird sichergestellt, dass die Beeinträchtigung eine gewisse Schwere erreichen muss und nicht mehr als sozial hinnehmbar erscheinen kann (vergleiche Eisele, in: Tübinger Kommentar Strafgesetzbuch, 31. Auflage 2025, § 201a Rn. 41). Maßgeblich ist die Perspektive eines durchschnittlichen Betrachters (vergleiche Bundestagsdrucksache 18/2601, S. 37; BGH, a. a. O., Rn. 32, m. w. N.).

Der Begriff des unbefugten Zugänglichmachens ist wie in § 201a Absatz 2 StGB zu verstehen und setzt voraus, dass die dritte Person die Möglichkeit eines Zugriffs auf den Inhalt hat (vergleiche Fischer/Anstötz, in: Fischer, Strafgesetzbuch, 73. Auflage 2026, § 201a Rn. 25). Das Zugänglichmachen ist nicht unbefugt, wenn es von einer Einwilligung der dargestellten Person oder einer Befugnisnorm gedeckt ist (vergleiche Bundestagsdrucksache 18/2601, S. 37; Eisele, a. a. O., Rn. 44).

Durch die Subsidiaritätsklausel wird klargestellt, dass § 201b StGB keine Sperrwirkung gegenüber Vorschriften mit schwererer Strafandrohung entfaltet. Insbesondere bleiben die §§ 184 und folgende sowie § 187 letzte Variante StGB auch nach Inkrafttreten von § 201b StGB auf die Verbreitung von pornographischen beziehungsweise verleumderischen Deepfakes anwendbar. § 184k Absatz 1 Nummer 4 StGB ist in seinem Anwendungsbereich lex specialis zu § 201b Absatz 1 StGB.

§ 201b Absatz 2 StGB erklärt § 201a Absatz 3 und 4 StGB für entsprechend anwendbar. § 201b Absatz 2 StGB in Verbindung mit § 201a Absatz 3 StGB-E verweist auf das Erfordernis einer tatbestandlichen Abwägung zwischen dem Schutz der Persönlichkeitsrechte der betroffenen Person und den in § 201a Absatz 3 StGB-E genannten Interessen, namentlich Kunst, Wissenschaft, Forschung, Lehre sowie Berichterstattung über Vorgänge des Zeitgeschehens und der Geschichte (vergleiche Bundestagsdrucksache 18/3202, S. 29).

§ 201b Absatz 2 StGB in Verbindung mit § 201a Absatz 4 StGB-E regelt die Einziehung. Dementsprechend können die von einem Beteiligten verwendeten technischen Mittel nach den §§ 74 und folgende StGB eingezogen werden. Auch eine Dritteinziehung ist möglich (vergleiche § 201b Absatz 2 in Verbindung mit § 201a Absatz 4 Satz 2 StGB-E, § 74a StGB).

**Zu Nummer 8**

§ 202e StGB-E orientiert sich eng an Artikel 6 der Richtlinie (EU) 2024/1385. Nach § 202e Satz 1 StGB-E wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wer unbefugt den Aufenthaltsort oder die Tätigkeiten einer anderen Person wiederholt oder ständig mittels Informations- oder Kommunikationstechnik überwacht. Unter Überwachung ist die zielgerichtete Erhebung von Informationen über den Aufenthaltsort und die Tätigkeiten einer Person zu verstehen. Tatbestandsmäßig ist nur die Überwachung mittels Informations- oder Kommunikationstechnik, also mit Mitteln der technischen Informationsübertragung (vergleiche Bundestagsdrucksache 19/19859, S. 26; siehe zur Verwendung des Begriffs in § 176 StGB der alten Fassung auch Bundestagsdrucksache 18/2601, S. 14). Die Beobachtung durch bloßes Hinsehen oder Hinhören, ohne dass eine technische Informationsübertragung stattfindet, erfüllt § 202e StGB daher nicht. Unter den Tatbestand fallen insbesondere das „Tracking“, das heißt die Verfolgung des Aufenthaltsorts mit technischen Mitteln, und die Verwendung sogenannter Spyware. Erfasst ist lediglich die unbefugte Überwachung. Das Tatbestandsmerkmal „unbefugt“ beschränkt den Tatbestand auf strafwürdige Fälle. Eine Überwachung ist nicht unbefugt, wenn sie durch ein ausdrückliches oder konkludentes Einverständnis des Opfers oder durch eine Befugnisnorm gedeckt ist, beispielsweise bei der Überwachung des Aufenthaltsortes oder der Online-Aktivitäten jüngerer Kinder durch die Eltern, wenn bei gemeinsamem Sorgerecht beide Eltern einverstanden sind und die Kinder in die Entscheidung der Eltern über das Tracking einbezogen wurden (§ 1626 Absatz 2, §§ 1627, 1631 Absatz 1, § 1687 Absatz 1 Satz 1 BGB). § 202e StGB-E setzt voraus, dass die Überwachung wiederholt oder ständig erfolgt. Beide Tatbestandsmerkmale dienen, wie das Tatbestandsmerkmal „unbefugt“, dazu, den Tatbestand auf strafwürdige Fälle der Überwachung zu beschränken. Es muss insoweit eine gewisse Erheblichkeitsschwelle überschritten sein. Wie im Rahmen von § 238 Absatz 1 StGB ist es vom Einzelfall abhängig, wie vieler Wiederholungen es für ein Vorliegen des Tatbestandsmerkmals „wiederholt“ bedarf. Bei schwerer wiegenden Einzelhandlungen kann schon eine geringe einstellige Anzahl von Wiederholungen hinreichend für eine Strafbarkeit sein (vergleiche zum Ganzen Bundestagsdrucksache 19/28679, S. 12; Eisele, in: Tübinger Kommentar Strafgesetzbuch, 31. Auflage 2025, § 238 Rn. 33). Die Überwachung erfolgt „ständig“, wenn sie zwar nicht wiederholt, aber ununterbrochen über einen nicht unerheblichen Zeitraum andauert. Qualitativ ist insoweit ein Verhalten von einigem Gewicht erforderlich, das die tatbestandliche Gleichstellung der „wiederholten“ und der „ständigen“ Überwachung zu rechtfertigen vermag, so beispielsweise beim Aufspielen einer Spyware auf ein Smartphone und der daran anschließenden durchgehenden Überwachung des Aufenthaltsortes und dem Mitlesen von Nachrichten des Opfers für mehrere Tage. Der vorgesehene Strafrahmen orientiert sich an § 42 Absatz 2 BDSG.

In Übereinstimmung mit Artikel 6 der Richtlinie (EU) 2024/1385 ist die Tat gemäß § 202e Satz 2 StGB-E nur dann strafbar, wenn die Handlung wahrscheinlich dazu führt, dass der anderen Person schwerer Schaden zugefügt wird. Auch dieses Kriterium dient dazu, den Tatbestand auf strafwürdige Fälle zu beschränken. Ohne eine solche Beschränkung würden etwa auch Fälle erfasst, in denen die Aufenthaltsorte oder die Tätigkeiten einer anderen

Person durch schlichtes Verfolgen öffentlich zugänglicher Profile in sozialen Medien nachvollzogen werden. Wer sich unter Verwendung eines Computers oder Mobiltelefons lediglich regelmäßig über die Aufenthaltsorte oder die Tätigkeiten etwa seiner Wahlkreisabgeordneten oder seines Lieblingsmusikers informiert, indem er deren Beiträge in sozialen Medien liest, verhält sich nicht strafwürdig. Eine mögliche Strafbarkeit nach Satz 1 ist in jenen Fällen nicht schon dadurch ausgeschlossen, dass die in sozialen Medien veröffentlichenden Personen freiwillig Auskunft über ihre Aufenthaltsorte oder ihre Tätigkeiten geben und dadurch das Tatbestandsmerkmal der Unbefugtheit entfiele. Denn selbst wenn veröffentlichende Personen gerade möchten, dass ihre Mitteilungen auch gelesen werden, dürfte darin regelmäßig kein Einverständnis zur wiederholten oder ständigen Überwachung liegen.

Während § 42 Absatz 2 BDSG in Bezug auf die Schädigung einer anderen Person ein subjektives Tatbestandselement voraussetzt (Schädigungsabsicht), stellt § 202e Satz 2 StGB-E in Übereinstimmung mit Artikel 6 der Richtlinie (EU) 2024/1385 darauf ob, ob objektiv die Zufügung eines schweren Schadens bei der überwachten Person wahrscheinlich ist. Ein Schaden ist die Beeinträchtigung eines jeden rechtlich geschützten Interesses, unabhängig davon, ob diesem ein Vermögenswert zukommt (vergleiche Brodowski, in: BeckOK DatenschutzR, 53. Edition, 1. August 2025, BDSG § 42 Rn. 52). Die Schädigung muss über die reine Verarbeitung personenbezogener Daten hinausgehen, weil sonst das Merkmal der Schadenszufügung leerliefe (vergleiche Bergt, in: Kühling/Buchner, 4. Auflage 2024, BDSG § 42 Rn. 52). Der zu erwartende Schaden muss schwer sein, das heißt, er muss über eine bloß geringfügige Belästigung oder Unannehmlichkeit hinausgehen, indem das Opfer erheblich oder nachhaltig beeinträchtigt wird. Wahrscheinlich ist die Zufügung eines Schadens dann, wenn der Schadenseintritt im Einzelfall in Anbetracht der Gesamtumstände der Tat bei einem regelmäßigen Geschehensablauf naheliegt.

**Zu Nummer 9**

**Zu Buchstabe a**

§ 201b und § 202e StGB-E werden als relative Antragsdelikte ausgestaltet und orientieren sich insoweit am Vorbild der §§ 201a, 202a, 202b und 202d StGB. Taten nach §§ 201b und 202e StGB-E werden also nur auf Antrag und in Fällen verfolgt, in denen die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält. § 205 Absatz 1 Satz 2 StGB wird entsprechend ergänzt.

**Zu Buchstabe b**

Bezieht sich die Tat nach § 201b Absatz 1 Satz 1 StGB-E auf eine verstorbene Person (§ 201b Absatz 1 Satz 2 StGB-E), steht wie in den Fällen des § 201a Absatz 1 Nummer 3 und Absatz 2 Satz 2 StGB das Antragsrecht den in § 77 Absatz 2 StGB bezeichneten Angehörigen zu. § 205 Absatz 2 Satz 4 StGB wird entsprechend ergänzt.

**Zu Artikel 3 (Änderung des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes)**

Artikel 3 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 4 (Änderung der Strafprozessordnung)**

Taten nach § 184k Absatz 1 und § 201b Absatz 1 StGB sollen – wie etwa Taten nach § 201a Absatz 1 und 2 StGB – im Wege der Privatklage verfolgt werden können. § 374 Absatz 1 StPO wird daher in Nummer 2a entsprechend angepasst und um eine neue Nummer 2b ergänzt.

**Zu Artikel 5 (Änderung des Bundeszentralregistergesetzes)**

Es handelt sich um eine redaktionelle Folgeänderung der Übernahme des § 201a Absatz 3 StGB in § 184k Absatz 2 StGB. Auch wenn der Regelungsinhalt des § 201a Absatz 3 StGB in den § 184k Absatz 2 StGB überführt wird, sind einschlägige Straftaten, die vor dem Inkrafttreten des Gesetzes begangen wurden bzw. werden, weiterhin Taten nach § 201a Absatz 3 StGB und entsprechende Verurteilungen als solche im Bundeszentralregister eingetragen. Würde man die Angabe „§ 201a Absatz 3“ lediglich streichen, würden solche Eintragungen, die bislang den besonderen Regelungen der §§ 32 Absatz 5, 34 Absatz 2, 41 Absatz 2 Satz 2 und 46 Absatz 1 Nummer 1a BZRG unterfielen, mit Inkrafttreten des Gesetzes aus dem Anwendungsbereich dieser Regelungen fallen. Dies würde dazu führen, dass entsprechende Entscheidungen – je nach konkreter Fristenlage – unter Umständen sofort tilgungsreif werden oder nicht mehr in ein erweitertes Führungszeugnis aufzunehmen wären. Zudem könnte die Verkettung mehrerer Verurteilungen nach § 38 BZRG dadurch zusammenbrechen. Dies wäre nicht im Interesse des Kinder- und Jugendschutzes. Daher wird hinsichtlich der Eintragungen nach § 201a Absatz 3 StGB klarstellend auf die bis zum Inkrafttreten des Gesetzes geltende Fassung verwiesen. In § 69 Absatz 4 BZRG ist die Ergänzung zwar nicht zwingend, da sich die Vorschrift lediglich auf Verurteilungen bezieht, "die vor dem 1. Juli 2022 in das Zentralregister eingetragen wurden", erscheint jedoch zur Klarstellung ebenfalls vorzugswürdig.

**Zu Artikel 6 (Änderung des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit)**

Es handelt sich um eine redaktionelle Folgeänderung. Wegen der Überführung der bisherigen Regelung des § 201a Absatz 3 StGB in den § 184k Absatz 2 StGB ist klarzustellen, dass in § 158a Absatz 2 Satz 2 FamFG auf die bis zum Inkrafttreten dieses Gesetzes geltende Fassung des § 201a Absatz 3 StGB Bezug genommen wird. Auf die Begründung zu Artikel 25 wird Bezug genommen.

**Zu Artikel 7 (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 8 (Änderung des Achten Buches Sozialgesetzbuch)**

Es handelt sich um eine redaktionelle Folgeänderung der Übernahme des § 201a Absatz 3 StGB in § 184k Absatz 2 StGB. Auf die Begründung zu Artikel 5 wird Bezug genommen.

**Zu Artikel 9 (Änderung des Neunten Buches Sozialgesetzbuch)**

Es handelt sich um eine redaktionelle Folgeänderung der Übernahme des § 201a Absatz 3 StGB in § 184k Absatz 2 StGB. Auf die Begründung zu Artikel 5 wird Bezug genommen.

**Zu Artikel 10 (Änderung des Zwölften Buches Sozialgesetzbuch)**

Es handelt sich um eine redaktionelle Folgeänderung der Übernahme des § 201a Absatz 3 StGB in § 184k Absatz 2 StGB. Auf die Begründung zu Artikel 5 wird Bezug genommen.

**Zu Artikel 11 (Änderung des Telekommunikationsgesetzes)**

Artikel 11 verbessert die Durchsetzbarkeit zivilrechtlicher Ansprüche. Anbieter von Internetzugangsdiensten speichern IP-Adressen entweder überhaupt nicht oder nur bis maximal sieben Tage. Bis eine betroffene Person eine Rechtsverletzung wahrnimmt, anschließend einen Antrag auf Auskunft nach dem GgdG stellt, das Gericht sodann gegenüber dem oft

in einem anderen MS ansässigen Diensteanbieter eine beweissichernde Anordnung nach § 3 GgdG erlässt, der Diensteanbieter die IP-Adresse gegenüber dem Gericht mitteilt, das Gericht anschließend ermittelt, von welchem Telekommunikationsanbieter diese IP-Adresse vergeben wurde, und das Gericht schließlich eine weitere beweissichernde Anordnung gegen den Telekommunikationsanbieter erlässt, damit die der IP-Adresse zugeordneten Daten nicht gelöscht werden, wird die Frist von sieben Tagen in aller Regel schon abgelaufen sein mit der Folge, dass die zur Identifizierung erforderlichen Daten nicht mehr vorhanden sind (wegen der Einzelheiten zum zeitlichen Aufwand wird auf die Begründung zu § 3 Absatz 1 Bezug genommen). Die Auskunftsanordnung gegenüber den Anbietern von Internetzugangsdienten nach § 2 ginge dann in der Regel ins Leere. Artikel 11 dient daher der Effektuierung der Auskunft nach § 2 Absatz 1 des Gesetzes gegen digitale Gewalt, indem er Internetzugangsdiensteanbieter (öffentlich zugängliche Telekommunikationsdienste) auf richterliche Anordnung dazu ermächtigt, die Auskunft über die Identität des potenziellen Rechtsverletzers (Bestandsdatenauskunft) zu erfüllen. Dafür wird § 174 Absatz 5 Nummer 9 TKG geschaffen, der insoweit die Auskunftsberechtigung der Internetzugangsdiensteanbieter nach § 2 Absatz 1 Satz 1 GgdG ergänzt. Nach geltendem Recht können öffentlich zugängliche Telekommunikationsdienste für eine Bestandsdatenauskunft nicht auf Daten aus der Vorratsdatenspeicherung, insbesondere auf IP-Adressen, zurückgreifen (vergleiche BVerwG, Urteil vom 14.08.2023 – 6 C 6.22 – Leitsatz 1). Das soll sich künftig ändern. Der Referentenentwurf eines Gesetzes zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren sieht vor, dass Anbieter von Internetzugangsdiensten wieder verpflichtet werden, insbesondere Internetprotokolladressen für drei Monate vorsorglich zu speichern, sodass für diesen Zeitraum stets eine Auskunft erteilt werden könnte (§ 177 Absatz 3 Satz 1 TKG in der Fassung des genannten Referentenentwurfs mit Verweis auf § 174 Absatz 1 Satz 3 TKG).

§ 174 Absatz 5 Nummer 9 TKG-E ergänzt nicht nur die Auskunftsberechtigung der Internetzugangsdiensteanbieter (s.o.). Die Regelung stellt in Verbindung mit § 174 Absatz 1 Satz 3 TKG zugleich klar, dass vorsorglich zu speichernde IP-Adressen von den Internetzugangsdiensteanbietern nur zur Vornahme einer Bestandsdatenauskunft intern verwendet, nicht aber etwa selbst herausgegeben werden dürfen.

Diese Verarbeitungsbefugnis der Telekommunikationsanbieter (1. Doppeltür), die nach den Vorgaben des verfassungsrechtlichen Doppeltürmodells (vergleiche BVerfGE 130, 151 <184>; 155, 119 <209 f. Rn. 201>) für die Beantwortung der gerichtlichen Anordnung über die Datenauskunft nach dem Gesetz gegen digitale Gewalt (2. Doppeltür) erforderlich ist, begründet einen Eingriff in Artikel 10 Absatz 1 GG bzw. – infolge der Eröffnung des Anwendungsbereichs der Richtlinie 2002/58/EG (im Folgenden: ePrivacy-Richtlinie) und wegen Artikel 51 Absatz 1 GRCh – in die Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union (GRCh). Der Eingriff ist gerechtfertigt.

Das Bundesverfassungsgericht verlangt dafür als legitimen Zweck mindestens den Schutz oder die Bewehrung von Rechtsgütern von hervorgehobenem Gewicht (vergleiche BVerfGE 125, 260 <343 f.>; 155, 119 <200 Rn. 175>), wozu jedenfalls die durch das Strafrecht geschützten Rechtsgüter zählen, bei besonderer Ermittlungsrelevanz der Zuordnung von IP-Adressen aber auch besonders gewichtige Ordnungswidrigkeiten (vergleiche BVerfGE 125, 260 <343 f.>; 155, 119 <201 f. Rn. 178>).

Nach der Rechtsprechung des EuGH zur Auslegung der ePrivacy-Richtlinie ist der mit einer Vorratsdatenspeicherung von IP-Adressen einhergehende Eingriff in Artikel 7 und 8 GRCh ebenfalls schon zur Erreichung eines mit der Bekämpfung von Straftaten im Allgemeinen verbundenen Ziels möglich, wenn tatsächlich ausgeschlossen ist, dass diese Speicherung schwere Eingriffe in das Privatleben des Betroffenen zur Folge haben kann, die darauf beruhen, dass insbesondere durch eine Verknüpfung dieser IP-Adressen mit einem von den Betreibern ebenfalls gespeicherten Satz von Verkehrs- oder Standortdaten die Möglichkeit besteht, genaue Schlüsse auf das Privatleben der Personen zu ziehen. (vergleiche EuGH [Plenum], Urteil vom 30. April 2024, Rs. C-470/21, Quadrature du Net II – Hadopi, Rn. 82

ff.). Insofern sind bestimmte Speichermodalitäten zu wahren. Dies stellen § 175 Absatz 2 Nummer 2 TKG-E und § 176 Absatz 2 Satz 2 Nummer 2 TKG-E sicher.

Dass das vorgenannte Ziel nicht nur im Wege öffentlich-rechtlicher Rechtsdurchsetzung, sondern auch im Wege privatrechtlicher Rechtsdurchsetzung (Durchsetzung zivilrechtlicher Ansprüche im Sinne von Artikel 23 Absatz 1 Buchstabe j DSGVO) verfolgt werden kann, ergibt sich ebenfalls aus der EuGH-Rechtsprechung zur ePrivacy-Richtlinie. Deren Artikel 15 Absatz 1 sieht vor, dass eine Beschränkung der Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absatz 1, 2, 3 und 4 sowie Artikel 9 dieser Richtlinie u.a. gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG (heute: Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 – DSGVO) erfolgen kann. Daraus folgert der EuGH, dass der Schutz des Eigentumsrechts und der Situationen, in denen sich Urheber im Rahmen eines zivilrechtlichen Verfahrens um diesen Schutz bemühen, nie vom Anwendungsbereich des Artikel 15 Absatz 1 der ePrivacy-Richtlinie ausgeschlossen waren (vergleiche EuGH [GK], Urteil vom 29. Januar 2008, Rs. C-275/06, Promusicae, Rn. 53; EuGH, Urteil vom 17. Juni 2021, Rs. C-597/19, Mircom, Rn. 116 f.).

Nichts anderes kann für den – dem Schutz des Eigentums mindestens gleichgewichtigen – Schutz des allgemeinen Persönlichkeitsrechts und seiner besonderen Ausprägungen wie dem Recht am eigenen Bild, der informationellen Selbstbestimmung oder der sexuellen Selbstbestimmung durch private Rechtsverfolgung gelten, den das Gesetz gegen digitale Gewalt bezweckt (vergleiche insb. die relevante Begriffsbestimmung der Rechtsverletzung unter Bezugnahme auf ausgewählte, enumerierte Straftatbestände nach § 1 Absatz 1 GgdG).

**Zu Artikel 12 (Änderung des Netzwerkdurchsetzungsgesetzes)**

Das Netzwerkdurchsetzungsgesetz wird 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.

**Zu Artikel 13 (Einschränkung eines Grundrechts)**

Die Neuregelungen in Artikel 11 Nummer 2 (§ 174 Absatz 5 Nummer 9 des Telekommunikationsgesetzes) ermöglicht auch den Zugriff auf Daten, die vom Schutzbereich des Fernmeldegeheimnisses erfasst sind. Die Vorschrift trägt dem Zitiergebot nach Artikel 19 Absatz 1 Satz 2 GG Rechnung.

**Zu Artikel 14 (Inkrafttreten)**

Artikel 14 enthält die Regelung über das Inkrafttreten dieses Gesetzes.