Berlin, 22.05.2026

STELLUNGNAHME

Deutscher Juristinnenbund e.V.

Vereinigung der Juristinnen,
Volkswirtinnen und Betriebswirtinnen

Geschäftsstelle / Office:
Kronenstr. 73 ● D-10117 Berlin
Telefon: +49 30 4432700
geschaeftsstelle@djb.de ● https://www.djb.de

zum Referentenentwurf des Bundesministeriums der Justiz und Verbraucherschutz – Entwurf eines Gesetzes zur Stärkung des zivilrechtlichen und strafrechtlichen Schutzes vor digitaler Gewalt

I. Zusammenfassende Bewertung des Entwurfs

Der Deutsche Juristinnenbund begrüßt, dass der vorliegende Gesetzentwurf digitale Gewalt rechtlich regeln möchte und dabei sowohl die strafrechtlichen Lücken als auch Fragen der Rechtsdurchsetzung adressiert. Damit wird eine langjährige Forderung des djb umgesetzt.[1] Der djb beklagt seit Jahren einen lückenhaften Schutz von Frauen vor digitaler Gewalt; die Reform von Straf- und Zivilrecht zum effektiven Schutz ist überfällig.

Denn digitale Gewalt hat gravierende Folgen für die Betroffenen und ihr Umfeld: Sie verletzt individuelle Rechte, wobei hier das Allgemeine Persönlichkeitsrecht im Vordergrund steht, oft in seiner Ausprägung als Recht auf sexuelle Selbstbestimmung. Zudem sind Diskriminierungsverbote zu beachten.

Digitale Gewalt wirkt aber auch darüber hinaus: Sie beschränkt insbesondere Frauen und Mädchen und queere Personen, darunter insbesondere Journalistinnen, Politikerinnen, Wissenschaftlerinnen und Aktivistinnen in ihrer gleichberechtigten Teilhabe am öffentlichen, beruflichen und politischen Leben. Digitale Gewalt bedroht deshalb das gesellschaftliche Miteinander; es ist auch ein strukturelles Problem. Der Kampf gegen digitale Gewalt ist daher nicht allein von den Betroffenen zu führen, sondern eine gesamtgesellschaftliche Aufgabe zur Sicherstellung einer wehrhaften und pluralistischen Demokratie.

Hier bleibt der Entwurf leider hinter dem verfassungs- und menschenrechtlich Erforderlichen zurück. Es fehlt eine hinreichende Anerkennung der strukturellen und insbesondere der geschlechtsspezifischen Dimension digitaler Gewalt.

Zum einen wird digitale Gewalt nur als Summe individueller Rechtsverletzungen behandelt, was die gesamtgesellschaftlichen Auswirkungen nicht beachtet. Digitale Angriffe wirken öffentlichkeitsverdrängend und demokratiegefährdend, und sie haben eine klare Geschlechterdimension. Gerade Antifeminismus, Hass gegen Frauen und queere Menschen finden im Netz Bedingungen, die sich verstärkend auswirken und das Entstehen extremistischer Strömungen begünstigen.

Zum anderen setzt der Entwurf einzig bei der Identifizierung und Inanspruchnahme einzelner Täter an. Für Betroffene ist aber nicht nur das Vorgehen gegen einzelne rechtsverletzende Inhalte und die Strafverfolgung der Tatpersonen entscheidend, sondern der schnelle, effektive und niedrigschwellige

[1] djb, Policy Paper: Zugang zu Recht in Fällen digitaler Gewalt, 11.03.2026, abrufbar unter: https://www.djb.de/fileadmin/user_upload/presse/stellungnahmen/st26-06_70th_CSW_digitale_Gewalt.pdf (letzter Abruf: 15.05.2026).

Schutz vor weiterer Verbreitung, Wiederholung und Eskalation. Das bildet der Entwurf bislang nicht ausreichend ab.

II. Zu den einzelnen Bestimmungen

A. Artikel 1: Gesetz gegen digitale Gewalt (GgdG)

1. § 1 GgdG-E - Begriffsbestimmungen

Der Anwendungsbereich des GgdG-E ist in mehrerlei Hinsicht zu eng gefasst:

a) Strafbarkeitsschwelle der erfassten Rechtsverletzungen

Der djb kritisiert, dass der Anwendungsbereich des GgdG auf Rechtsverletzungen beschränkt ist, die einen der genannten Straftatbestände erfüllen. **Hier sollten auch Äußerungen und andere Handlungen erfasst werden, die absolute Rechte verletzen, ohne einen Straftatbestand zu erfüllen.** Der Anwendungsbereich ist relevant für die Frage, wann ein Anspruch auf Auskunft und auf Accountsperre bestehen kann. Während bei der Accountsperre aufgrund ihres tiefen Eingriffs in die Meinungsfreiheit zurecht eine schwerwiegende Persönlichkeitsrechtsverletzung vorausgesetzt wird (vgl. § 4 GgdG-E), ist dies beim Auskunftsanspruch nicht geboten. Der Anwendungsbereich ist daher hier weiter zu fassen und nur die Accountsperre von dem zusätzlichen Erfordernis der schwerwiegenden Persönlichkeitsrechtsverletzung abhängig zu machen (s.u.).

b) Straftatenkatalog unzureichend

In § 1 Abs. 1 Nr. 2 a) GgdG-E sind die Straftatbestände aufgezählt, die den Anwendungsbereich des GdgG eröffnen, weil sie häufig im digitalen Raum begangen werden und zumindest auch eine Verletzung des Persönlichkeitsrechts bewirken können.[2] **Der Katalog sollte um § 202e StGB-E ergänzt werden.** Der neu zu schaffende § 202e StGB-E kriminalisiert eine erhebliche Verletzung des Persönlichkeitsrechts der überwachten Person mit digitalen Mitteln, die eine lückenlose und ständige Überwachung einer Person erst ermöglichen.

Auch § 232 StGB sollte wie der vom Katalog des Art. 1 § 1 Abs. 1 Nr. 2 a) GgdG-E bereits erfasste § 176b StGB aufgenommen werden. Denn ähnlich wie beim Cybergrooming, das nach § 176b StGB strafbar ist, werden Personen zum Zweck der Ausbeutung im Sinne des § 232 StGB regelmäßig digital angeworben und Betroffene auch auf Onlineplattformen zur Ausbeutung angeboten.

c) Messengerdienste und SaaS-Dienste erfassen

Aus Sicht des djb muss sich der Anwendungsbereich des Gesetzes gegen digitale Gewalt auch auf Messengerdienste erstrecken. Der Messengerdienst WhatsApp etwa ermöglicht nicht nur den Austausch privater Nachrichten zwischen Individuen, sondern auch das Abonnieren von Kanälen nicht persönlicher Kontakte und den Austausch in großen Communities. Es macht sowohl wertungsmäßig als auch aus Betroffenensicht keinen Unterschied, ob ein rechtsverletzender Inhalt über einen Instagram Account oder WhatsApp Kanal an ein breites Publikum gepostet wird. Zudem schlagen Messengerdienste wie WhatsApp und Telegram ihren Nutzende Kanäle vor und greifen so aktiv in den Meinungsmarkt ein. Die Verbreitung digitaler Gewalt liegt daher auch in ihren Händen. Ihre Privilegierung ist unbegründet. **Deshalb sollten Messengerdienste in die Definition des Diensteanbieters nach § 1 Abs. 2 GgdG-E aufgenommen werden.**

[2] RefE S. 42 f.

Um Cyberstalking wirksam einzudämmen, sollten die Auskunftsansprüche auch für Software as a Service-Anwendungen (SaaS-Anwendungen) gelten. SpyApps und Tracker (wie z.B. Airtags) sind regelmäßig einem Account (z.B. Google oder Apple) zugeordnet, mit dem der Standort abgerufen werden kann. Betroffene müssen auch bei dieser Form digitaler Gewalt in der Lage sein zu erfahren, von wem das Cyberstalking ausgeht, also wer Inhaber des verbundenen Accounts ist. Die bisher in § 1 Abs. 2 Nr. 2 und 3 GgdG-E enthaltenen Web-Hosting-Dienste und Cloud-Hosting-Dienste erfassen die SaaS-Anwendungen nicht. **Deshalb sollen Software-as-a-Service-Dienste in die Definition des Diensteanbieters nach § 1 Abs. 2 GgdG-E aufgenommen werden.**

d) Definition des sozialen Netzwerks

§ 1 Abs. 4 GgdG-E schafft eine neue Definition für den Begriff des „sozialen Netzwerks". Der Anspruch auf Accountsperren und Zustellungsbevollmächtigte bezieht sich allein auf soziale Netzwerke, nicht auch auf andere Online-Plattformen im Sinne von § 1 Abs. 2 Nr. 1 GgdG-E, wozu etwa Online-Marktplätze zählen. Eine Ungleichbehandlung ist nicht angezeigt. Insbesondere die Plattform OnlyFans dürfte als Online-Marktplatz eingestuft werden, weil Hauptzweck das Angebot von Waren ist, nicht die Interaktion mit den Nutzenden. Auch Dating-Apps sind nicht erfasst. Dabei werden jegliche Online-Plattformen dazu genutzt, um Gewaltbetroffene zu stalken und ihnen anstößige Bilder zuzusenden (Cyberflashing). Schließlich ist denkbar, dass andere Online-Marktplätze wie Vinted oder Kleinanzeigen eine Kommentar- oder andere Funktionen einfügen, die digitale Gewalt in breitem Ausmaß ermöglichen. **Die Definition des sozialen Netzwerks in § 1 Abs. 4 GgdG-E sollte gestrichen und der Anwendungsbereich von §§ 4 und 9 GgdG-E sollte sich auf alle Online-Plattformen im Sinne des § 1 Abs. 2 Nr. 1 GgdG-E erstrecken.**

2. § 2 GgdG-E – Auskunft über Daten

Die neue Regelung zum Auskunftsanspruch verkürzt einerseits den *de lege lata* bestehenden Anwendungsbereich der Auskunftsansprüche nach § 21 Abs. 2 TDDDG erheblich, dehnt ihn aber andererseits mit § 2 Abs. 2 lit. b) GgdG-E auf IP-Adressen aus. Beides ist abzulehnen, sofern die Erweiterung auf IP-Adressen eine Vorratsdatenspeicherung voraussetzt, die dann die Nachverfolgung von Online-Verhalten ermöglichen soll. Es sollten stattdessen alle Mittel erschöpft werden, die einen wirksamen Schutz vor digitaler Gewalt ermöglichen.

a) Keine Strafbarkeitsschwelle für Auskunftsanspruch

In § 1 GgdG-E ist der Anwendungsbereich auf Rechtsverletzungen beschränkt, die einen der enumerierten Straftatbestände erfüllen. Der jetzige Entwurf bleibt damit hinter dem Auskunftsanspruch nach § 21 Abs. 2 TDDDG zurück, verkürzt also den bereits existierenden Auskunftsanspruch für Bestandsdaten. Denn § 21 Abs. 2 TDDDG greift bis dato bei der Verletzung absoluter Rechte durch audiovisuelle Medien, wozu auch die Verletzung des allgemeinen Persönlichkeitsrechts gehört. Eine Kürzung des Anwendungsbereichs konterkariert das Schutzziel. Tatsächlich erfüllen viele Formen digitaler Gewalt keinen Straftatbestand, können aber für Betroffene mit erheblichen persönlichen Auswirkungen und tiefgehenden Verletzungen etwa ihres allgemeinen Persönlichkeitsrechts und Rechts auf informationelle Selbstbestimmung verbunden sein: Das Offenbaren der sexuellen Orientierung oder einer schweren Erkrankung gegen den Willen der betroffenen Person etwa – um nur zwei Beispiele zu nennen.

Für einen wirksamen Schutz vor digitaler Gewalt ist es erforderlich, dass jede Verletzung des Allgemeinen Persönlichkeitsrechts zur Auskunft über die Tatperson berechtigt. Eine Erheblichkeitsschwelle braucht es für den Auskunftsanspruch nicht. Dabei übersieht der djb nicht, dass die Möglichkeit, sich im Netz anonym zu äußern, besonders schützenswert ist, weil sie die öffentliche Debatte fördert und die Meinungsäußerungsfreiheit sichert. Der Meinungsäußerungsfreiheit kann im Rahmen der Abwägung mit dem allgemeinen Persönlichkeitsrecht ausreichend Rechnung getragen werden. Der Auskunftsanspruch dient gerade dazu, zivilrechtliche Ansprüche der Betroffenen vorzubereiten. Bei

Einführung einer Strafbarkeitsschwelle würde ein riesiger rechtsfreier Raum entstehen, den der Gesetzesentwurf gegen digitale Gewalt gerade verhindern möchte: Die Betroffenen könnten sich gerade nicht gegen die Tatperson, sondern nur gegen die Betreibende sozialer Netzwerke wenden und Löschung verlangen. Vor einer erneuten Veröffentlichung der rechtsverletzenden Inhalte wären sie nicht geschützt. Für das sog. Notice-and-Take-down Schreiben müssten Betroffene selbst aufkommen.

b) Gewaltschutz als Vorwand für die Vorratsdatenspeicherung

Der djb begrüßt, dass sich der Auskunftsanspruch in § 2 Abs. 2 GgdG-E u.a. auf die Personalien der Nutzenden, wie den Namen, das Geburtsdatum, die Anschrift, die E-Mail-Adresse und die Telefonnummer erstreckt. Auch die Erstreckung auf die IP-Adresse kann sich als wertvoll erweisen, um die Tatperson bei digitaler Gewalt zu ermitteln.

Der djb hat jedoch erhebliche Bedenken, den Auskunftsanspruch auf IP-Adresse, Portnummern und Zeitstempel zu erweitern, soweit die Herausgabe dieser Daten eine anlasslose Vorratsdatenspeicherung voraussetzt und diese die Nachverfolgung des Online-Verhaltens ermöglicht. Eine solche ist im begleitenden „Entwurf eines Gesetzes zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren“ des BMJV geregelt.

EuGH und BVerfG haben in der Vergangenheit enge Maßstäbe für die Zulässigkeit einer Vorratsdatenspeicherung aufgestellt.[3] Sie kann u.a. nur zulässig sein, wenn ausgeschlossen ist, dass Schlüsse auf das Privatleben gezogen werden können. In seiner jüngsten Rechtsprechung zur Vorratsdatenspeicherung aus dem Jahr 2024 nimmt der EuGH ausführlich zur Möglichkeit der IP-Adressspeicherung Stellung.[4] Sofern durch Speicher- und Zugriffsmodalitäten sichergestellt ist, dass keine Nachverfolgung der besuchten Internetseiten möglich ist, kann die IP-Adressspeicherung auch zur Verfolgung von Straftaten im Allgemeinen zulässig sein. Hierauf nimmt auch die Begründung des Gesetzentwurfs zur IP-Adressspeicherung Bezug.[5] Der Gesetzgeber verkennt aber, dass nach seinem Entwurf nicht lediglich IP-Adressen gespeichert werden sollen, sondern zusätzlich auch Portnummern und Zeitstempel. Das ist aus Ermittlungssicht erforderlich, um bestimmen zu können, wer zum Tatzeitpunkt gehandelt hat. Aus der Kombination von IP-Adresse, Portnummer und Zeitstempel ist allerdings auch eine Nachverfolgung der besuchten Internetseiten möglich. U**nter Zugrundelegung der Maßstäbe des EuGH erscheint die vorgeschlagene Vorratsdatenspeicherung unzulässig.** Für die Bewertung der Eingriffsintensität kommt es auf die Gesamtschau der existierenden Überwachungsmaßnahmen an (sog. Überwachungsgesamtrechnung).[6] Dabei sind Einschüchterungseffekte (sog. Chilling Effects) zu berücksichtigen. Ein Gefühl ständiger Überwachung kann dazu führen, dass Bürgerinnen und Bürger auf die Wahrnehmung ihrer Grundrechte verzichten.[7] Eine besondere Gefahr besteht dabei für die Meinungs- und Pressefreiheit, Art. 5 Abs. 1 GG, aber auch für die Versammlungs- und Vereinigungsfreiheit und die Mitwirkung in der Politik. Gerade die demokratischen Grundrechte sind für Menschen besonders wichtig, die nicht der Mehrheit angehören bzw. bei denen die Gefahr besteht, dass ihre Belange außen vor bleiben. Dazu

---

[3] BVerfG Urt. v. 2. 3. 2010 - 1 BvR 256/08 u.a. = NJW 2010, 833 - Vorratsdatenspeicherung; EuGH, Urt. v. 21.12.2016 - C-203/15, C-698/15 (Tele2/Sverige) = NVwZ 2017, 1025; EuGH, Urt. v. 20.9.2022 – C-793/19 und C-794/19 (BRD/SpaceNet AG bzw. Telekom Deutschland GmbH) = NJW 2022, 3135; EuGH Urt. V. 30.4.2024 – C-470/21 (La Quadrature du Net u.a./ Premier ministre u.a.) - GRUR-RS 2024, 8831.

[4] EuGH Urt. V. 30.4.2024 – C-470/21 (La Quadrature du Net u.a./ Premier ministre u.a.) - GRUR-RS 2024, 8831 Rn. 101 - 115.

[5] Entwurf eines Gesetzes zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren vom 20.04.2026, S. 67.

[6] Vgl. hierzu *Witting*, Stellungnahme für den Rechtsausschuss des Deutschen Bundestages zum Antrag IP-Adressen rechtssicher speichern und Kinder vor sexuellem Missbrauch schützen (BT-Drucksacke 20/3687), abrufbar unter: https://www.bundestag.de/resource/blob/970442/Stellungnahme-Witting.pdf (letzter Abruf: 18.05.2026).

[7] BVerfG Urt. v. 2. 3. 2010 - 1 BvR 256/08 u.a. = NJW 2010, 833 Rn. 212, 233 und 241.

gehören auch Frauen. Der Schutz vor Einschüchterung steht deshalb auch im Zusammenhang damit, dass der Staat für die tatsächliche Gleichstellung Sorge tragen muss (Art. 3 Abs. 2 Satz 2 GG). Darauf zielt auch das aktuelle Gesetzgebungsvorhaben gegen digitale Gewalt, das durch eine Maßnahme, die einschüchternd wirkt, nicht konterkariert werden sollte. In Anbetracht der zahlreichen und tiefgreifenden Beeinträchtigungen liegt vielmehr ein schwerwiegender Grundrechtseingriff vor.

Keine der Begründungen zum Entwurf vermag bislang evidenzbasiert zu begründen, wie der mit der Anzeigepraxis einhergehenden Gefahr effektiv begegnet werden soll. Die Zahlen zur Erforderlichkeit der Vorratsdatenspeicherung für die Bekämpfung digitaler Gewalt[8] genügen so nicht.[9] Besonders zu betonen ist hier, dass die Vorratsdatenspeicherung ohnehin nur in Fällen weiterhelfen könnte, in denen die Betroffene innerhalb der vorgesehenen Speicherfrist Kenntnis von der Tat erlangt und rechtzeitig den Antrag auf Auskunft stellt und damit eine Beweissicherung erwirkt.[10] Die vorgeschlagene IP-Adressspeicherung von drei Monaten kann überhaupt nur rechtsverletzende Inhalte erfassen, die innerhalb dieses Zeitraums online gestellt wurden. Die IP-Adresse gibt nur Auskunft über die Anschlussinhabenden und das Endgerät, mit dem die Rechtverletzung vorgenommen wurde. Es bleibt bei dem beweisrechtlichen Problem, dass eine andere Person Zugriff auf das Endgerät gehabt haben kann. Schließlich können die Tatpersonen, die bewusst die Anonymität des Internets zur Begehung von Straftaten nutzen wollen, durch einfache technische Mittel (wie etwa VPN-Dienste) die Nachverfolgung verhindern.

c) Zielgerichtete und wirksame Maßnahmen

Effektiver Schutz vor digitaler Gewalt erfordert keine massenhafte Datenspeicherung. Es gibt zahlreiche zielgerichtete Maßnahmen, die Betroffene wirksam schützen würden, welche als mildere Mittel auszuschöpfen sind. Mit der Login-Falle[11] und dem Quick-Freeze-Modell sind zwei Mittel vorgeschlagen worden, die ebenfalls die IP-Adresse einer Tatperson sichtbar machen und deutlich weniger stark in die Grundrechte Dritter eingreifen.

Nach dem Quick-Freeze-Modell können Ermittlungsbehörden eine richterliche Anordnung zum Einfrieren bestimmter Verbindungsdaten erwirken. Nach einer Erhebung des BKA aus dem Jahr 2023 speichern Telekommunikationsanbieter IP-Adressen bereits bis zu sieben Tage lang.[12] Quick-Freeze hilft dann weiter, wenn die betroffene Person unverzüglich Kenntnis von der Rechtsverletzung erhält und die Justiz schnell handelt, was hohe Fachkompetenz und damit entsprechende Fortbildung voraussetzt. Eine massenhafte Vorratsdatenspeicherung ist dann nicht erforderlich.

Die Login-Falle wird aufgrund einer (im Idealfall elektronisch gestellten) Anzeige von der einen Anfangsverdacht bejahenden Ermittlungsbehörde scharf gestellt. Sobald der Kontoinhaber erneut eine Verbindung mit dem Plattform-Server aufbaut (etwa durch Öffnen der App auf dem Smartphone) wird in Echtzeit die IP-Adresse an die Ermittlungsbehörde übermittelt. Erforderlich ist hierfür eine Justiz-Schnittstelle, über die die Datenanfrage sicher und schnell erfolgen kann. Die Login-Falle ist folglich deutlich wirksamer bei Rechtsverletzungen, die über ein Nutzerkonto begangen werden. Das ist bei digitaler Gewalt, die über soziale Netzwerke ausgeübt wird, stets der Fall. Daher bietet sie sich gerade hier als Alternative an.

---

[8] *Bundeskriminalamt (BKA)*, Positionspapier zu erforderlichen Speicherfristen von IP-Adressen, 23.6.2023.

[9] Vgl. Kritik von Puschke GSZ 2024, 23, 26.

[10] Vgl. hierzu die die Begründung zu § 3 RefE, S. 49.

[11] Vgl. ausführlich zum Vorschlag der Login-Falle von D64 - Zentrum für digitalen Fortschritt, abrufbar unter: https://d-64.org/login-falle/ (letzter Abruf: 18.05.2026).

[12] *BKA*, Mindestspeicherfristen, abrufbar unter: https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/230623_Mindestspeicherfristen_IP-Adressen.html (letzter Aufruf: 13.05.2026).

Zudem sind zuvor weitere Maßnahmen zu ergreifen. **Dazu gehören vor allem eine bessere personelle und technische Ausstattung sowie präzisere Ermittlungsinstrumente für die Behörden. Allem voran sind sexualisierende Bildinhalte konsequent zu löschen, um ein weiteres Verbreiten zu verhindern. Digitale Schnittstellen zwischen Plattformen und Justiz sind einzuführen, Meldewege sind einfacher auszugestalten und nicht den Plattformen zu überlassen.** Insofern wird die Bundesregierung aufgefordert, ihren Einfluss auf europäischer Ebene auszuüben.

3. § 3 GgdG-E – Beweissichernde Anordnungen

a) Klare Frist zur Datenspeicherung und Auskunftserteilung

Das schnell eskalierende Verbreitungspotential digitaler Gewalt kann nur durch klare, kurze Fristen eingedämmt werden. Der Gesetzesentwurf macht in § 3 Abs. 1 GgdG-E keine Vorgaben, binnen welcher Frist die Dienste die Daten speichern sollen. **Hier ist eine gesetzliche Regelung erforderlich, damit Gerichte nicht unterschiedlich lange Fristen setzen.** Für die Datenspeicherung erscheint es sinnvoll, eine Frist "binnen 24 Stunden ab Zugang der gerichtlichen Mitteilung (unabhängig von Werk- oder Feiertag)" vorzusehen. Hinsichtlich der Auskunftserteilung erklärt der Entwurf in § 3 Abs. 2 Satz 1 GgdG-E lediglich, dass diese "unverzüglich" zu erfolgen habe. Auch hier droht uneinheitliche Rechtsanwendung durch die Dienste. Angemessen wären hier „72 Stunden ab Zugang der gerichtlichen Mitteilung (unabhängig von Werk- oder Feiertag)".

b) Rein digitale Datenübermittlung

Der Gesetzesentwurf sieht in § 3 Abs. 2 Satz 1 GgdG-E lediglich vor, dass die Dienste die Auskunft in Textform übermitteln können. Sie können damit selbst entscheiden, wie sie Daten übermitteln, z.B. auch in ausgedruckter Form auf dem Postweg. Das verzögert Schutz. **Um dem Eskalationspotential digitaler Gewalt zu begegnen, sollten die Dienste verpflichtet werden, die Daten in digitaler Form per E-Mail binnen der genannten Frist zu übermitteln.** Ein Medienbruch führt lediglich zu Zeitverlust.

Die Vorgabe „in Textform" wird den tatsächlichen Erscheinungsformen digitaler Gewalt nicht gerecht. Gerade geschlechtsspezifische digitale Gewalt greift häufig auf visuelle oder audiovisuelle Herabwürdigungen zurück, deren diskriminierende, sexualisierte oder einschüchternde Wirkung sich nicht adäquat in einer bloßen textlichen Beschreibung abbilden lässt. Die Gefahr einer Verharmlosung oder Entkontextualisierung solcher Inhalte wird durch eine rein textbasierte Übermittlung erheblich verstärkt. Manipulationsgrad, Reichweite und Wirkungsdimension audiovisueller Inhalte lassen sich regelmäßig nur anhand des Originalformats zuverlässig beurteilen. Besonders problematisch erscheint dies vor dem Hintergrund des § 3 Abs. 5 GgdG-E, wonach Diensteanbietende verpflichtet sind, die gesicherte Kopie des rechtsverletzenden Inhalts nach Erteilung der Auskunft irreversibel zu löschen. Damit wird die Verantwortung für die Sicherung zentraler Beweismittel auf die Betroffenen verlagert, die sich Manipulationsvorwürfen ausgesetzt sehen werden.

Der djb fordert daher, das Gesetz technologieneutral zu fassen und die Übermittlung rechtsverletzender Inhalte ausdrücklich auch in audio- und visuellen Formaten zu ermöglichen. Ergänzend sollte eine sichere elektronische Infrastruktur geschaffen werden, über die Diensteanbietende entsprechende Inhalte unmittelbar und beweissicher an Gerichte übermitteln können. Eine solche Ausgestaltung trüge den Realitäten digitaler Gewalt besser Rechnung und so zu einer geschlechtergerechten und diskriminierungssensiblen Rechtsdurchsetzung bei.

4. § 4 GgdG-E – Sperrung von Nutzerkonten in sozialen Netzwerken

Der djb begrüßt die Einführung von Accountsperren in § 4 GgdG-E. Auch hier besteht jedoch Nachbesserungsbedarf.

a) Zu hohe Anforderung an Accountsperre

Nach derzeitigem Stand ist der Anwendungsbereich des Gesetzentwurfs auf Rechtsverletzungen beschränkt, die einen der in § 1 Abs. 1 Nr. 2 GgdG-E genannten Straftatbestände erfüllen. Sofern es sich

– anders als der djb annimmt – nicht um ein redaktionelles Versehen hält, ist die weitere Forderung es müsse eine schwerwiegende Persönlichkeitsrechtsverletzung vorliegen, nicht zu erklären. Sollte der Gesetzgeber tatsächlich am Strafbarkeitserfordernis festhalten, ist kein Mehrwert darin zu erkennen, zusätzlich eine schwere Persönlichkeitsrechtsverletzung zu fordern. Vielmehr bestünde sogar die Gefahr, dass gegen Gruppen oder Bevölkerungsteile gerichtete Volksverhetzung (§ 130 Abs. 1 Var. 1 und 2 StGB) mangels persönlicher Betroffenheit einzelner Personen nicht zu einer Sperrung führen würde. **Bei Erfüllung der Straftatbestände aus § 1 Abs. 1 Nr. 2 a)-c) GgdG-E ist eine Accountsperre auch ohne die zusätzliche Anforderung der schwerwiegenden Persönlichkeitsrechtsverletzung verhältnismäßig.**

Der Anwendungsbereich in § 1 Abs. 1 Nr. 1 GgdG-E ist allerdings auf die Verletzung absoluter Rechte zu erweitern. Zur Wahrung der Verhältnismäßigkeit ist die Accountsperre dann von dem zusätzlichen Erfordernis einer schwerwiegenden Rechtsverletzung abhängig zu machen. Der djb begrüßt insofern, dass S. 54 der Begründung des Entwurfs für die Beurteilung der Schwere die Rechtsprechung zur Geldentschädigung bei der Verletzung des allgemeinen Persönlichkeitsrechts heranziehen möchte.

b) Wirkung der Accountsperre unklar

Nach dem Entwurf ist unklar, welche Wirkung eine Accountsperre konkret hat. Zum Schutz der Betroffenen muss jedoch gesetzlich klargestellt werden, ob ein gesperrter Account für Dritte weiterhin sichtbar ist, ob er als gesperrt gekennzeichnet wird und ob Inhalte des Accounts weiterhin abrufbar bleiben. **Eine Accountsperre, die zwar Nutzungshandlungen unterbindet, aber rechtsverletzende Inhalte weiterhin öffentlich sichtbar lässt, ist unzureichend.**

Es bleibt zudem unklar, ob nicht-öffentliche Funktionen, wie etwa der Austausch privater Nachrichten (Chat-Funktion), möglich bleiben. Zum Schutz vor digitaler Gewalt sollte **auch das Versenden privater Nachrichten gesperrt werden**. Dies wäre auch durch eine Klarstellung zu erreichen, wonach das Verfassen und Versenden privater Nachrichten unter den Begriff des „Veröffentlichen“ des § 4 Abs. 2 Satz 1 GgdG-E fällt.

c) Zumutbarkeitsgrenze als potenzielles Schlupfloch

Nach dem derzeitigen § 4 Abs. 2 Satz 3 GgdG-E sollen Maßnahmen in Bezug auf neue Nutzerkonten nur dann erfolgen, soweit sie technisch und wirtschaftlich zumutbar und möglich sind. Das ist unzureichend. Diese Einschränkung birgt die erhebliche Gefahr, dass Plattformen sich unter Verweis auf technische oder wirtschaftliche Hindernisse ihrer Verantwortung entziehen. Dies wird von großen Plattformen immer wieder vorgebracht, wenn es darum geht, kerngleiche Inhalte zu löschen. Doch gerade große Plattformen verfügen über erhebliche technische, personelle und wirtschaftliche Ressourcen. **Die Zumutbarkeit darf nicht so ausgestaltet werden, dass sie faktisch zur Einwendung gegen effektiven Rechtsschutz wird.** Hier ist zu beachten, dass Plattformen mit ihren Algorithmen digitale Gewalt gerade befeuern. Wenn das Geschäftsmodell darauf basiert, Gewaltinhalte auszuspielen – weil schockierende Inhalte die Menschen länger auf der Plattform halten und ihnen so mehr Werbung ausgespielt werden kann –, sind besonders strenge Anforderungen daran zu stellen, wann eine Sperrung unzumutbar ist. § 4 Abs. 2 Satz 3 GgdG-E ist insofern ein Beispiel für eine zahnlose Digitalpolitik: Gesetze werden Geschäftsmodellen angepasst – nicht Geschäftsmodelle der Rechtsordnung, wie sonst. Wenn Gewalt auf Plattformen nicht wirksam eingedämmt werden kann, muss das Geschäftsmodell gescheitert sein, nicht die Demokratie.

d) Regelbeispiele systemwidrig

§ 4 Abs. 1 Satz 1 GgdG-E macht die Sperre davon abhängig, dass sie zur Vermeidung weiterer Rechtsverletzungen erforderlich sein muss. Dies wird in § 4 Abs. 3 GgdG-E in Regelbeispielen konkretisiert. So soll die Sperrung in der Regel erforderlich sein, wenn der Nutzende bzgl. der konkreten Rechtsverletzung die Abgabe einer strafbewehrten Unterlassungserklärung verweigert, gegen eine von ihm unterzeichnete strafbewehrte Unterlassungserklärung verstoßen hat oder andere Anhaltspunkte eine weitere Rechtsverletzung befürchten lassen.

Die Regelung ist **zu streichen**. § 4 Abs. 3 GgdG-E widerspricht der unterlassungsrechtlichen Dogmatik. Denn nach ständiger höchstrichterlicher Rechtsprechung indiziert eine bereits getätigte Rechtsverletzung die Gefahr weiterer Rechtsverletzungen; dem Hinzutreten weiterer Umstände bedarf es gerade nicht. I**n Bezug auf die Erforderlichkeit der Accountsperre nach § 4 Abs. 1 Satz 1 GgdG-E genügt ein Verweis im Entwurf auf die etablierte Rechtsprechung zur Ausräumung der Wiederholungsgefahr.** Systemkonform wäre allenfalls eine ausdrückliche gesetzliche Feststellung, wann die nach ständiger Rechtsprechung bestehende Vermutung der erneuten Rechtsverletzung entfällt, wie durch die Abgabe einer angemessen strafbewehrten Unterlassungserklärung. **So wäre auch sichergestellt, dass die Accountsperre nicht fordert, weitere Rechte geltend zu machen.** Denn in der Praxis kommt es immer wieder vor, dass die digital rechtsverletzenden Inhalte von Tätern stammen, die auch physisch gewaltbereit sind, was dazu führt, dass Opfer nach Aufklärung der Identität des Täters aus berechtigter Furcht vor diesem von der direkten Kontaktaufnahme und Aufforderung zur Abgabe einer strafbewehrten Unterlassungserklärung absehen, eine gerichtlich angeordnete Accountsperre indes begrüßen.

Das Merkmal der Erforderlichkeit wirft auch die (ungeklärte) Frage auf, in welchem Verhältnis der Anspruch auf zeitweilige Sperrung eines Accounts und der (ggf. parallel) im einstweiligen Verfügungsverfahren geltend gemachte Unterlassungsanspruch stehen. Lässt eine (vorläufig) verhängte Accountsperre, für die mit der Erforderlichkeit das Bestehen der Wiederholungsgefahr geprüft und bejaht werden muss, dann die Vermutung der Wiederholungsgefahr als materielle Voraussetzung des Unterlassungsanspruchs entfallen? D**ie Accountsperre sollte eine reine Erweiterung der Betroffenenrechte sein und daher keinen Einfluss auf den Unterlassungsanspruch haben. Der djb empfiehlt, dies in der Begründung zum Entwurf klarzustellen.**

Es bietet sich an, zumindest zu ergänzen, dass eine Accountsperre in der Regel erforderlich ist, wenn sich die Tatperson einer schwerwiegenden Persönlichkeitsrechtsverletzung hinter der Anonymität oder Pseudonymität des Accounts verbirgt. Damit fordert der djb keine Klarnamenpflicht für alle Accounts, sondern nur, dass die Accountsperre nicht an die Durchsetzung anderer Betroffenenrechte (Auskunft, Unterlassung, Richtigstellung etc.) geknüpft sein darf. Betroffene sollten den Account zur Eindämmung der von ihm ausgehenden digitalen Gewalt zügig sperren lassen können, ohne das Auskunftsverfahren durchlaufen oder gar weitere Individualrechte geltend machen zu müssen.

e) Inhaltemoderation kein gleich geeignetes Mittel

In § 4 Abs. 3 S. 2 GgdG-E findet sich die Vorstellung, Inhaltemoderation könne regelmäßig ein milderes Mittel gegenüber einer Accountsperre darstellen. Dies überzeugt nicht. Die Praxis zeigt, dass Meldeverfahren auf Plattformen häufig unzureichend funktionieren, intransparent sind, erhebliche Hürden für Betroffene enthalten und nicht selten durch Dark Patterns erschwert werden.[13] Inhaltemoderation allein reicht gerade bei wiederholten, anonymen oder koordinierten Angriffen nicht aus. Es handelt sich im Vergleich zu Accountsperren also meist nicht um ein gleich geeignetes Mittel. **Deshalb sollte in der Begründung zum Entwurf klargestellt werden, dass die derzeitige Inhaltemoderation zum Schutz vor digitaler Gewalt unzureichend ist.**

f) Sperrung von Gruppen

In § 4 GgdG-E sollte der Anspruch auf Sperrung ganzer Gruppen aufgenommen werden, sofern der Zweck der Gruppe die Begehung von Rechtsverletzungen im Sinne des § 1 Abs. 1 GgdG-E ist. Die Folgen digitaler Gewalt sind regelmäßig dann besonders schwerwiegend, wenn es sich um ein koordiniertes Vorgehen handelt. Betroffene haben jedoch bisher nur die Möglichkeit, gegen jede einzelne Äußerung isoliert vorzugehen. Recherchen von NDR zu Vergewaltiger-Netzwerken auf Telegram zeigen

[13] Vgl. *HateAid*, Recht ohne Reichweite, 2025, S. 11, abrufbar unter: https://www.stiftung-mercator.de/content/uploads/2025/12/hateaid-dsa-bilanz-recht-ohne-reichweite-2025-1.pdf (letzter Abruf: 13.05.2026).

das erschreckende Ausmaß digitaler Gewalt gegen Frauen .[14] Gruppen mit zehntausenden Mitgliedern tauschen sich darüber aus, wie sich Frauen für sexuelle Übergriffe unbemerkt betäuben lassen und bieten anderen Nutzenden ihre Partnerinnen zur Vergewaltigung an. Es werden Fotos und Videos betäubter, entkleideter Frauen sowie der sexualisierten Übergriffe an diesen geteilt. Eine Betroffene müsste hier gegen jedes einzelne Mitglied der Gruppe vorgehen, um die Inhalte auf deren Endgeräten löschen zu lassen. Auch Facebook-Gruppen, deren alleiniger Zweck darin besteht, schwerwiegende Persönlichkeitsrechtsverletzungen oder Straftaten zum Nachteil einer Person zu begehen, müssen gesperrt werden können. Hier ist in besonderem Maß das Grundrecht auf Meinungsfreiheit zu berücksichtigen, da die Sperrung – anders als bei einer Accountsperre – auch diejenigen Nutzenden betrifft, die nur lesen oder sich in ihren Posts rechtstreu verhalten. Die Verhältnismäßigkeit einer Gruppensperre ist dann gewahrt, wenn die Gruppe allein das Ziel verfolgt, die schwerwiegende Rechtsverletzungen oder Katalogstraftaten nach § 1 Abs. 1 Nr. 2 a) GgdG-E zu begehen oder wenn die überwiegende Zahl der Beiträge die Rechte der Betroffenen verletzen.[15]

5. § 5 GgdG-E Gerichtliches Verfahren

a. Kosten

Der djb begrüßt, dass der Gesetzesentwurf – anders als § 21 Abs. 3 TDDDG – die Kostenlast des Auskunftsverfahrens nicht der verletzten Person auferlegt. Soweit S. 22 der Begründung auf den Grundsatz des § 81 Abs. 1 S. 1 FamFG verweist, ist darauf hinzuweisen, dass in der Praxis von der Möglichkeit des § 81 Abs. 1 S. 2 FamFG, von der Erhebung der Kosten gänzlich abzusehen, regelmäßig kein Gebrauch gemacht wird. Betroffene müssten daher damit rechnen, die Kosten für das Auskunfts- oder Accountsperreverfahren zu tragen. Das sind nicht nur die Gerichtskosten, sondern auch die Rechtsverfolgungskosten des an den Verfahren beteiligten Dienstes. **Effektiver Schutz vor digitaler Gewalt bedarf einer Regelung, wonach für das Auskunfts- und Accountsperrenverfahren keine Gerichtskosten erhoben werden und an dem Verfahren beteiligte Dienste ihre Kosten selbst tragen müssen.**

a) Schutzinteressen der Betroffenen

Der Text des Gesetzesentwurfs selbst sieht für Antragstellende, die befürchten, dass ihre Anonymität durch das Auskunftsverfahren gefährdet wird, keine Ausnahme von dem Grundsatz vor, dass Betroffene nur mit Angabe ihres Namens und ihrer Anschrift Ansprüche geltend machen können. Lediglich die Begründung verweist auf S. 56 darauf, dass diese besonders vulnerablen Personen entsprechend der Praxis bei Verfahren nach dem Gewaltschutzgesetz in ihrem Antrag darauf hinweisen können, dass die Geheimhaltung des Aufenthaltsortes notwendig ist. Dies soll auch für den Rechtsverletzenden gelten, sofern dieser am Verfahren beteiligt ist. Es sei Aufgabe des Gerichts, durch entsprechende Aktenführung sicherzustellen, dass die Daten gegenüber den anderen Verfahrensbeteiligten nicht bekannt werden; auch das Akteneinsichtsrecht nach § 13 Abs. 1 FamFG bestehe nur, soweit nicht schwerwiegende Interessen eines Beteiligten oder eines Dritten entgegenstehen.

Zielführender wäre es, Betroffene zumindest im Auskunfts- und Accountsperrenverfahren zu berechtigen, eine ladungsfähige c/o-Adresse anzugeben. Das wäre auch bei der Geltendmachung der übrigen Betroffenenrechte (Unterlassung, Richtigstellung etc.) zu begrüßen. Eine ausdrückliche Regelung gibt es dazu bislang nicht. Die Offenbarung der Privatanschrift hindert Betroffene von Gewalt an der Durchsetzung ihrer Rechte: Sie haben gute Gründe, weitere Gewalt zu fürchten. Die Angabe einer Privatadresse ist insbesondere dann nicht erforderlich, wenn die betroffene Person – wie vom djb vorgeschlagen – im Auskunfts- und Accountsperreverfahren im Falle des Unterliegens keine Kosten zu tragen hat. Die Offenbarungspflicht ist insbesondere dann entbehrlich, wenn die betroffene Person

[14] Vgl.: https://www.tagesschau.de/investigativ/ndr/telegram-ko-tropfen-vergewaltigung-netzwerk-100.html (letzter Abruf: 18.05.2026).
[15] Vgl. KG Urt. v. 23.12.2025 – 10 U 190/23, GRUR-RS 2025, 36001 Rn. 23 - Morddrohung.

anwaltlich vertreten ist oder eine Beratungsstelle unterstützt und diese die Anschrift der betroffenen Person kennen. **Insofern regt der djb an, den Gesetzentwurf um die Möglichkeit der Angabe einer c/o-Adresse bei Strafanzeigen sowie bei zivilrechtlichen Verfahren zu ergänzen.**

6. § 6 GgdG-E Beteiligung des Nutzers

Der djb begrüßt, dass der Referentenentwurf nun zur Sicherstellung der Meinungsäußerungsfreiheit der Accountinhabenden die Vorgaben der Anhörung detaillierter ausgestaltet und nicht den jeweiligen Diensten überlässt. Zuvor sollte nicht geregelt werden, welche konkreten Informationen die Dienste den Accountinhabenden bereitstellen müssen und welche Antwortfrist sie ihnen einräumen können. Das würde sich nun ändern.

7. § 7 GgdG-E Vertretung durch Zivilgesellschaft

a) Prozessstandschaft

Die in § 7 GgdG-E vorgesehene Möglichkeit der Vertretung durch zivilgesellschaftliche Organisationen ist ausdrücklich zu begrüßen. Sie trägt dem Umstand Rechnung, dass Betroffene digitaler Gewalt im Rahmen gerichtlicher Verfahren erheblichen Belastungen ausgesetzt sind, und kann auf diese Weise einen wichtigen Beitrag zur Verringerung sekundärer Viktimisierung leisten. Der Mehrwert liegt insbesondere darin, dass spezialisierte Organisationen ihre fachliche Expertise und Beratungserfahrung in das Verfahren einbringen und Betroffene zugleich vor unmittelbarer Konfrontation mit den Tätern schützen können.

Die Prozessstandschaft sollte auf nachgelagerte zivilrechtliche Verfahren erstrecke werden. Der Rechtsschutzbedarf der Betroffenen erschöpft sich nicht im Auskunfts- oder Accountsperrenverfahren, sondern besteht auch zur Geltendmachung von Unterlassungs-, Richtigstellungs-, Geldentschädigungs- und Schadensersatzansprüchen. Beschränkt sich die Möglichkeit der Vertretung auf einen Teil dieser Verfahren, drohen die Schutzwirkungen des § 7 GgdG-E leerzulaufen, da Betroffene in den Folgeverfahren erneut selbst auftreten und sich der belastenden Konfrontation aussetzen müssten.

b) Einführung eines Verbandsklagerechts

Die vorgesehene Regelung reicht zum effektiven Kampf gegen digitale Gewalt allerdings nicht aus. Der starke Fokus auf Individualrechtschutz wird der Lage der Betroffenen und den Folgen digitaler Gewalt für eine demokratische Gesellschaft nicht gerecht. Damit Betroffene ihre Rechte gegen digitale Gewalt durchsetzen und verteidigen können, benötigen sie erhebliche emotionale und finanzielle Ressourcen, die oft fehlen. Der Kampf gegen digitale Gewalt ist indes eine gesamtgesellschaftliche Aufgabe; er darf nicht allein auf den Betroffenen lasten. Wenn Verbraucherschutzverbände im eigenen Namen gegen UWG-Verstöße vorgehen dürfen, sollten zivilgesellschaftliche Organisationen auch im eigenen Namen gegen digitale Gewalt vorgehen können – zum Schutz des demokratischen Zusammenhalts und freien gesellschaftlichen Diskurses im Internet.

Aus Sicht des djb ist daher ein Verbandsklagerecht für zivilgesellschaftliche Organisationen einzuführen. Nur so lässt sich den Belastungen der individuellen Prozessführung gerade in Fällen digitaler Gewalt begegnen. Gerade koordinierte Angriffe, massenhafte Belästigung und sexualisierte Diffamierung verursachen schwere psychische Belastungen für die Betroffenen, die durch Unterstützung abgemildert werden können. Hier würde ein Verbandsklagerecht Betroffene entlasten, aber Verfahren auch effizienter machen. So erkennen Verbände insbesondere auch strukturelle Defizite bei Plattformen und können auch langwierige Prozesse gegen diese führen.

Ohne Verbandsklagerecht bliebe zudem gegen Gruppen/Bevölkerungsteile gerichtete Volksverhetzung (§ 130 Abs. 1 Var. 1 und 2 StGB) zivilrechtlich ungeahndet. Denn es gibt keine Betroffenen, welche

den Auskunftsanspruch zur Vorbereitung eigener zivilrechtlicher Ansprüche oder eine Accountsperre anmelden und eine zivilgesellschaftliche Organisation mit der Geltendmachung ihrer Rechte bevollmächtigen könnten. Ein Verbandsklagerecht wäre auch mit Art. 86 DSA vereinbar, da dieser nur das Minimum („zumindest“) regelt.

Die Unterstützung durch Verbände müsste auch kostenrechtlich beachtet werden. Daher **fordert der djb eine sichere und ausreichende Finanzierung für Verbände und die Einrichtung eines Rechtshilfefonds, mit dem Verbandsklagen bei hinreichenden Erfolgsaussichten finanziert werden können**.

8. § 8 GgdG-E Zuständigkeit

Der Gesetzesentwurf sieht vor, dass für Anträge das Landgericht ausschließlich zuständig ist, in dessen Bezirk der Antragstellende seinen Wohnsitz, seinen Sitz oder eine Niederlassung hat. Diese Zuständigkeit soll gemäß § 8 Abs. 3 GgdG-E (abweichend von § 32 ZPO) auch für Streitigkeiten über Ansprüche aus Rechtsverletzungen gelten, wenn zuvor ein Auskunftsverfahren nach § 2 durchgeführt wurde. In der Praxis führt dies dazu, dass nicht länger die auf äußerungsrechtliche Ansprüche mit speziellen Kammern ausgestatteten Landgerichte, sondern jeweils die am Sitz der Betroffenen zuständig sind. Eine zu stark divergierende Rechtsprechung wäre jedoch ein Problem. **Der djb regt daher an, von der vorgesehenen Ermächtigung der Landesregierungen Gebrauch zu machen, durch Rechtsverordnung die Auskunftsverfahren einem Landgericht für die Bezirke mehrerer Landgerichte zuzuweisen.**

9. § 9 GgdG-E: Inländische Zustellungsbevollmächtigte

Mit Inkrafttreten des Digitale-Dienste-Gesetzes (DDG) im Mai 2024 wurde das NetzDG weitgehend aufgehoben. Lediglich die Pflicht zur Benennung eines inländischen Zustellungsbevollmächtigten besteht als Restvorschrift fort, allerdings nur noch für Anbietende aus Drittstaaten. Plattformen mit Sitz in einem anderen EU-Mitgliedstaat – also der weit überwiegende Teil der für Betroffene relevanten Anbietenden, einschließlich der über ihre irischen Tochtergesellschaften operierenden VLOPs – fallen aus dem Anwendungsbereich heraus. Hintergrund ist das Urteil des EuGH zum Herkunftslandprinzip.[16] Dieses erfasst jedoch nicht ausdrücklich rein prozessuale Regelungen ohne materielle Beschränkung der Dienstleistungsfreiheit. Auch Art. 13 DSA schließt die Lücke nicht: Der dort vorgesehene EU-Vertretende dient primär aufsichtsrechtlichen Zwecken und ersetzt keinen zivilprozessualen Zustellungsbevollmächtigten.

Für Betroffene entsteht hier eine empfindliche Lücke beim Zugang zum Recht: Zustellungen müssen regelmäßig nach der EU-Zustellungs-VO[17] ins EU-Ausland bewirkt werden, was zu erheblichen Verzögerungen, sprachlichen Hürden und höheren Kosten führt. Das steht im Widerspruch zum Ziel eines schnellen und effektiven Rechtsschutzes. **Der djb regt daher an zu prüfen, ob die Pflicht zur Benennung von inländischen Zustellungsbevollmächtigten – in prozessual ausgestalteter Form – auf sämtliche für Betroffene digitaler Gewalt relevanten Plattformen erstreckt werden kann, unabhängig vom Sitz des Anbietenden.** In dieselbe Richtung hat sich auch der Bundesrat im Gesetzgebungsverfahren zum Digitale-Dienste-Gesetz ausgesprochen.[18]

---

[16] EuGH Urt. v. 9. November 2023 - C-376/22 (Google Irland/KommAustria) = NJW 2024, 201.

[17] Verordnung (EU) 2020/1784 des Europäischen Parlaments und des Rates vom 25. November 2020 über die Zustellung gerichtlicher und außergerichtlicher Schriftstücke in Zivil- oder Handelssachen in den Mitgliedstaaten (Zustellung von Schriftstücken).

[18] BR-Drs. 676/1/23 vom 19. Januar 2024, abrufbar unter: https://www.bundesrat.de/SharedDocs/drucksachen/2023/0601-0700/676-1-23.pdf (letzter Abruf: 18.05.2026).

10. Weitere Regelungslücken in der Durchsetzung

a) Gewaltschutzgesetz

Der djb hält es für geboten, auch das Gewaltschutzgesetz auf digitale Gewaltformen zu erweitern. Digitale Gewalt ist regelmäßig keine isolierte Erscheinung, sondern eine Eskalation analoger Gewalt, die sich in den digitalen Raum verschiebt. Tätlichkeiten, Bedrohungen und Kontrollverhalten setzen sich nahtlos online fort – etwa durch Cyberstalking, GPS-Tracking, Doxing oder die Verbreitung intimer Bildaufnahmen. Eine konsequente Schutzsystematik muss diesem Umstand Rechnung tragen und darf nicht künstlich zwischen analoger und digitaler Gewaltdimension trennen. Wir verweisen insoweit auf die entsprechenden Forderungen des djb.[19]

b) Benennung einer Behörde nach Art. 9 Digital Services Act

Das GgdG sollte die nach Art. 9 Digital Services Act zuständige Behörde ausdrücklich benennen und mit den erforderlichen Befugnissen sowie hinreichenden personellen und sachlichen Ressourcen ausstatten. Die Verzahnung nationaler gerichtlicher Verfahren mit den unionsrechtlichen Verpflichtungen der Plattformen ist klar, effektiv und praxistauglich auszugestalten, um den betroffenen Personen einen wirksamen Rechtsschutz zu gewährleisten. Die zuständige Behörde benötigt präzise und rechtssicher ausgestaltete Ermittlungsbefugnisse, die ihr ein zielgerichtetes Vorgehen gegenüber Plattformen ermöglichen. Nur so kann sichergestellt werden, dass Anordnungen nach Art. 9 DSA nicht an unklaren Kompetenzgrenzen oder unzureichenden Untersuchungsinstrumenten scheitern. Darüber hinaus sollte die Bundesregierung ihren Einfluss auf europäischer Ebene aktiv nutzen, um Plattformen stärker in die Verantwortung zu nehmen und die Durchsetzung des DSA in der Praxis zu stärken.

B. Artikel 2: Änderung des Strafgesetzbuches

1. §§ 184b und 184c StGB-E

Der djb begrüßt, dass in § 184b und 184c StGB Strafbarkeitslücken hinsichtlich des Herstellens sexualisierender Deepfakes, die ein Kind oder eine jugendliche Person sexualbezogen wirklichkeitsnah darstellen, geschlossen werden. Allerdings umfassen die §§ 184b Abs. 1 S. 1 Nr. 1 und 184c Abs. 1 Nr. 1 StGB nur bestimmte pornographische Inhalte. So bleiben Schutzlücken bestehen. Ein persönlichkeitsrechtsverletzender Sexualbezug kann auch gegeben sein, wenn bspw. ein Kind mittels Deepfaketechnologie bis auf Bikini oder Unterwäsche ausgezogen gezeigt wird. Ein solcher Inhalt würde jedoch nur unter § 184b Abs. S. 1 Nr. 1b) StGB fallen, wenn das Kind in aufreizend geschlechtsbetonter Haltung abgebildet wird. Diese Einschränkung ist nicht plausibel, denn das Kind wird bereits durch das „digitale Ausziehen“ sexualisiert. Dies gilt auch für sexualisierende Bildaufnahmen eines Kindes, die es in Bikini, Unterwäsche oder ähnlich zeigen. Diese Regelungslücke wird von §§ 184k, 201b StGB-E nur unzureichend aufgefangen.[20]

2. §§ 184k, 201b StGB-E

Der Referentenentwurf sieht vor, mit einer Änderung des § 184k StGB einen einheitlichen Straftatbestand für Phänomene bildbasierter sexualisierter Gewalt zu schaffen. Der djb begrüßt dies ausdrücklich. Damit wird die schon mehrfach erhobene Forderung umgesetzt, einen einheitlichen Straftatbestand im Sexualstrafrecht außerhalb des Pornographiestrafrechts zu schaffen, der die schwerwiegende

[19] Vgl. *djb,* Policy Paper „Bekämpfung bildbasierter sexualisierter Gewalt", vom 7. Juni 2023, Abschnitt VII (Gewaltschutzgesetz).

[20] Hierzu gleich unter X.2.a.

Verletzung des Persönlichkeitsrechts der Betroffenen, insbesondere als Recht auf sexuelle Selbstbestimmung, Recht am eigenen Bild und Recht auf Nichtdiskriminierung, unter Strafe stellt.[21]

Allerdings bedarf der Entwurf der Nachbesserung, um die Verfügungsbefugnis über Bildinhalte, die eine Person sexualbezogen darstellen, umfassend zu schützen. Die Vorschläge schließen das Anfertigen und Manipulieren, Besitzen oder Gebrauchen und Zugänglichmachen von Bildinhalten, die eine andere Person sexualbezogen darstellen, nicht generell aus. Sie verpflichten aber dazu, dass dies nur im Einvernehmen mit der dargestellten Person geschehen darf.

a) Erfasste Inhalte und Formulierungen

(1) Enumerative Aufzählung

In § 184k StGB-E wird aufgezählt, wie der Sexualbezug eines Bildinhalts beschaffen sein muss, um vom Straftatbestand erfasst zu sein. Durch die abschließende Aufzählung lässt sich zwar Bedenken hinsichtlich einer fehlenden Bestimmtheit des Straftatbestandes begegnen. Doch besteht die Gefahr, dass Inhalte nicht erfasst werden, die strafwürdig sind, weil sie die dargestellte Person bildvermittelt sexuell verobjektivieren. Dies gilt zum Beispiel für Inhalte, die eine Muslima mit bloßem Haar oder nackter Schulter zeigen, die sonst einen Hijab trägt. § 184k Abs. 1 Nr. 2 und 4 StGB-E würden diesen Fall nicht erfassen, weil nicht die dort aufgezählten Körperteile unbekleidet abgebildet werden. Damit entsteht eine Schutzlücke gegenüber Handlungen, die im jeweiligen sozio-kulturellen Kontext eine verobjektivierende Sexualisierung der dargestellten Person bedeuten. Zwar kann es für die Bestimmung der sexuellen Verobjektivierung nicht auf rein subjektive Positionen ankommen, vielmehr ist ein objektiver Maßstab anzuwenden. Dabei spielen aber sozio-kulturelle Aspekte eine wichtige Rolle, die typischerweise eine Sexualisierung der dargestellten Person nahelegen müssen; das wäre hier der Fall.

Der djb begrüßt, dass mit der Kriminalisierung nicht einvernehmlicher sexualisierender Deepfakes in § 184k Abs. 1 Nr. 4 StGB-E eine der gravierendsten Strafbarkeitslücken im Bereich bildbasierter sexualisierter Gewalt geschlossen werden soll.[22] Allerdings soll diese Tatvariante nur das Verändern von Bildaufnahmen mittels eines Computerprogramms erfassen, wenn der Anschein erweckt wird, dass sexuelle Handlungen oder die unbekleideten Genitalien, das unbekleidete Gesäß oder die unbekleidete weibliche Brust einer anderen Person abgebildet seien. Auch hier würden Bildinhalte, bei denen mittels KI-Technologie Erwachsene oder Kinder bis auf den Bikini oder Unterwäsche „ausgezogen" werden, nicht unter § 184k Abs. 1 Nr. 4 StGB-E fallen, weil sie keine unbekleideten Genitalien, Gesäß oder weibliche Brust zeigen. Bei Kindern und Jugendlichen entfällt zudem, wie angemerkt, eine Strafbarkeit nach § 184b Abs. 1 S. 1 Nr. 1b), § 184c Abs. 1 Nr. 1b) StGB, wenn das Kind oder die jugendliche Person keine aufreizend geschlechtsbetonte Körperhaltung einnimmt. Diese Schutzlücken müssen beseitigt werden.

Unbefugte sexualbezogene Bildinhalte, die nicht unter § 184k StGB-E (und § 184b StGB) fallen, können zwar von § 201b StGB-E erfasst sein, allerdings würde dieser Straftatbestand nur das Zugänglichmachen als Tathandlung erfassen, nicht auch das Herstellen und Besitzen oder Gebrauchen. Zudem bezieht sich § 201b StGB-E auf Deepfakes, die den Anschein erwecken, ein tatsächliches Geschehen wiederzugeben. Das ist für als solche erkennbare Deepfakes und (etwa mittels eines Wasserzeichens) of-

---

[21] Vgl. *djb*, stn. 26-09, Policy Paper zum rechtlichen Handlungsbedarf bei nicht einvernehmlichen sexualisierenden Deepfakes, abrufbar unter: https://www.djb.de/presse/stellungnahmen/detail/st26-09 (letzter Abruf: 15.05.2026); Vgl. *djb,* stn. 23-17, Policy Paper: Bekämpfung bildbasierter sexualisierter Gewalt, S. 9, abrufbar unter: https://www.djb.de/fileadmin/user_upload/presse/stellungnahmen/st23-17_Bildbasierte_Gewalt.pdf (letzter Abruf: 15.05.2026).

[22] Näher zu den Lücken vgl. *djb*, stn. 26-09, Policy Paper zum rechtlichen Handlungsbedarf bei nicht einvernehmlichen sexualisierenden Deepfakes, S. 6, abrufbar unter: https://www.djb.de/presse/stellungnahmen/detail/st26-09 (letzter Abruf: 28.04.2026).

fengelegte Deepfakes fraglich. Für § 201b StGB-E ist das nachvollziehbar, soweit hier der Täuschungsaspekt im Vordergrund steht. Es würde aber dazu führen, dass die für § 184k StGB-E dargelegten Schutzlücken auch nicht von § 201b StGB-E erfasst werden.

Daher ist zu empfehlen, **den Tatbestand des § 184k Abs. 1 offener zu formulieren, indem auf die Aufzählung konkreter Fallgruppen verzichtet wird oder „die Wiedergabe oder wirklichkeitsnahe Darstellung einer anderen Person in sexuell bestimmter Weise" normiert und in der Begründung erläutert wird**. Genauer sollte in der Begründung ausdrücklich auf die im Referentenentwurf als Tatbestandsvarianten aufgezählten Fallgruppen, die Fälle des digitalen Ausziehens in sexuell bestimmter Weise oder das Abbilden in sexuell bestimmter Weise wie im Beispiel der Muslima ohne Kopftuch Bezug genommen werden. Damit würde eine Formulierung wie „in sexuell bestimmter Weise" zentraler Teil des Tatbestandes. Wie der Referentenentwurf zutreffend festhält, lässt sich letzteres aufgrund der Rechtsprechung zu § 184i StGB hinreichend bestimmen.[23] Nur durch eine offenere Formulierung können auch die Rechte betroffener Personen in Fallgestaltungen effektiv geschützt werden, in denen die Bewertung als sexualbezogenen von einer objektiven Betrachtung der konkreten Umstände in Einzelfall abhängt. Dem Bestimmtheitsgebot wäre Genüge getan und zudem eine Überkriminalisierung vermieden.

Nicht zuletzt lässt sich damit ein Vorsatzproblem umgehen: Wenn jemand den Herstellungsprozess des Bildinhaltes nicht kennt, ihn aber in Kenntnis des Sexualbezugs Dritten unbefugt zugänglich macht und die Person davon ausgeht, dass es sich um einen Deepfake handelt, obwohl es eine authentische Bildaufnahme ist oder umgekehrt, läge nach dem Entwurf ein vorsatzausschließender Tatbestandsirrtum vor.[24] Straflosigkeit wäre aber nicht gerechtfertigt, weil die Tatperson die tatsächlichen Umstände des strafwürdigen Unrechts – das nicht einvernehmliche Zugänglichmachen eines Bildinhalts, der eine andere Person sexualbezogen darstellt – kennt.

(2) § 184k Abs. 1 StGB-E: „Bildaufnahme"

Der djb weist darauf hin, dass in § 184k StGB-E zunächst die Formulierung „Bildaufnahme" verwendet wird, die für alle vier aufgezählten Tatvarianten gilt. Für die sexualbezogene Veränderung von Bildinhalten, die selbst schon manipuliert sind, bspw. ein Deepfake eines Deepfakes, würde § 184k Abs. 1 Nr. 4 StGB-E deshalb nicht gelten. § 201b StGB-E hat auch hier als Auffangtatbestand nicht den gleichen Schutzumfang.

(3) §§ 184k Abs. 1 Nr. 2 und 3 StGB-E: „weibliche Brust"

Der djb weist erneut darauf hin, dass die Formulierung „weibliche Brust" unklar lässt, was hier genau zu subsumieren ist. Vor allem kann dies zu bedenklichem Verteidigungsvorbringen führen: Die Frage, ob eine Brust – u. a. im Hinblick auf nicht binäre Personen – als weiblich angesehen wird oder nicht, als Gegenstand der Beweisaufnahme zuzulassen, birgt die Gefahr diskriminierender und entwürdigender Beweisanträge.[25] In der Begründung des Entwurfs könnte zumindest klargestellt werden, dass dieses Tatbestandsmerkmal unabhängig vom personenstandsrechtlichen Geschlechtseintrag anzuwenden ist. Auch angesichts dieser Schwierigkeiten erscheint nicht ratsam, die vom Tatbestand erfassten Bildinhalte abschließend aufzuzählen.

---

[23] Ausführlicher gleich unter (4).

[24] Vgl. *Schmidt*, Vorschlag zur Kriminalisierung nicht einvernehmlicher Deepfakes als eine Form bildbasierter sexualisierter Gewalt, 2026, S. 45, 52 f.; *Härtlein*, KriPoZ 2025, S. 387 (394).

[25] *djb*, stn. 20-19, Stellungnahme zum Gesetzentwurf der Bundesregierung „Entwurf eines … Gesetzes zur Änderung des Strafgesetzbuches – Verbesserung des Persönlichkeitsschutzes bei Bild aufnahmen", S.3, abrufbar unter: https://www.djb.de/fileadmin/user_upload/presse/stellungnahmen/st20-19_upskirting.pdf (letzter Abruf: 28.04.2026), umfassender zur Problematik dieser Formulierung Schuchmann, Geschlecht im Sexualstrafrecht – Aktuelle Entwicklungen und Reformbedarf, in: Januszkiewicz et al. (Hrsg.), Geschlechterfragen im Recht, 2021, S. 91.

(4) § 184k Abs. 1 Nr. 3 StGB-E: „in sexuell bestimmter Weise"

In § 184k Abs. 1 Nr. 3 StGB-E wird die Formulierung „in sexuell bestimmter Weise" benutzt, um bei Bildaufnahmen, die die bekleideten Genitalien, das bekleidete Gesäß oder die bekleidete weibliche Brust zeigen, neutrale von sexualbezogenen Inhalten abzugrenzen. In der Begründung des Entwurfs wird erläutert, dass die Auslegung in Anlehnung an § 184i StGB erfolgen soll. Damit bestehen keine Bedenken hinsichtlich der Bestimmtheit. Für die Auslegung würde es nicht vordergründig auf die sexuelle Motivation des Täters ankommen, sondern es können auch Motive wie „Wut, Sadismus, Scherz oder die Demütigung des Opfers" eine Rolle spielen.[26] Das ist wichtig. Der djb betont, dass es nicht auf die sexuelle Motivation des Täters ankommen kann, denn für die Rechtsgutsverletzung ist entscheidend, dass die betroffene Person sexuell verobjektiviert wird.

Der djb weist darauf hin, dass **die maßstäblich gängige Position des objektiven Beobachters nicht mit der Perspektive der konkret entscheidenden Justizangehörigen gleichgesetzt werden darf**. Es sollte – auch durch **Fortbildungen** - sichergestellt werden, **dass Justizangehörige kontextspezifische Aspekte sexueller Verobjektivierung im Zusammenhang mit bildbasierter sexualisierter Gewalt kennen** und auf diese Weise zutreffend einschätzen können, was im Einzelfall sexuell verobjektivierend ist und was nicht.

(5) § 184k Abs. 1 Nr. 4 StGB-E: schlechte und offengelegte Deepfakes

Das Recht auf sexuelle Selbstbestimmung und das Recht am eigenen Bild werden – neben dem Recht, nicht diskriminiert zu werden - auch dann verletzt, wenn ein sexualisierender Deepfake schlecht gemacht ist oder offengelegt wird, dass es sich um einen Deepfake handelt. Nach der Formulierung des § 184k Abs. 1 Nr. 4 StGB-E ist erforderlich, dass „der Anschein erweckt wird", dass eine andere Person bei sexuellen Handlungen oder mit nackten sexuell konnotierten Körperteilen abgebildet wird. Einerseits ist diese Formulierung nötig, um näher zu bezeichnen, was ein manipulierter Bildinhalt i. S. d. § 184k Abs. 1 Nr. 4 StGB-E ist, andererseits ist sie ein Einfallstor für eine Auslegung, die diese Tatalternative auf täuschend echte und nicht als solche offengelegte Deepfakes beschränkt. In der Begründung zum Entwurf sollte deshalb **klargestellt werden, dass es für die Anwendung des § 184k Abs. 1 Nr. 4 StGB-E nicht darauf ankommt, ob die Manipulation täuschend echt wirkt oder offengelegt wird**. Eine wirklichkeitsnahe Darstellung reicht aus.

b) Tathandlungen

In § 184k Abs. 1 StGB-E soll das unbefugte Herstellen und Zugänglichmachen, der dort aufgezählten Bildinhalte, unter Strafe gestellt werden. Der djb begrüßt nachdrücklich, dass auch das Herstellen kriminalisiert werden soll, denn jede Person muss selbst entscheiden können, ob und gegebenenfalls welche Bildinhalte es von ihr gibt, die sie sexualbezogen darstellen, wer sie nutzt und wer sie wem zugänglich macht.[27]

Allerdings verlangt ausreichender Schutz, dass auch das nicht einvernehmliche Besitzen oder Gebrauchen unter Strafe gestellt wird, weil es jedenfalls ebenso wie das Herstellen die Verfügungsbefugnis über diese Inhalte verletzt. § 184k StGB-E würde sonst hinter das Schutzniveau der §§ 201a Abs. 1, 184b Abs. 3, 184c Abs. 3 StGB zurückfallen. Auch entstünde eine Strafbarkeitslücke, wenn Inhalte bei einer Person aufgefunden werden, ihr aber nicht nachgewiesen werden kann, dass sie sie hergestellt hat. Zwar ergibt sich eine Strafbarkeit in Fällen, in denen ein strafbarer Inhalt unaufgefordert zugeschickt und nicht sofort gelöscht wird. Allerdings ist es aufgrund des niedrigen Mindeststrafrahmens dann auch möglich, die Strafverfahren einzustellen, so wie dies im Hinblick auf Kinderpornographie

[26] Vgl. RefE S. 66; BGH NJW 2014, 3737, 3738.

[27] Vgl. *djb*, stn. 26-09, Policy Paper zum rechtlichen Handlungsbedarf bei nicht einvernehmlichen sexualisierenden Deepfakes, S. 5, abrufbar unter: https://www.djb.de/presse/stellungnahmen/detail/st26-09 (letzter Abruf: 28.04.2026).

praktiziert wird. Der djb fordert deshalb, **die Tathandlung des Gebrauchens oder Besitzens mit in den Straftatbestand aufzunehmen**.

c) Strafdrohung und fehlende Qualifikationen

Der Referentenentwurf sieht für § 184k StGB-E eine Strafdrohung von bis zu zwei Jahren Freiheitsstrafe oder Geldstrafe vor. Das entspricht den Strafrahmen in § 201a StGB und dem bisherigen § 184k StGB, steht aber in einem deutlichen Spannungsverhältnis zu den Strafrahmen in § 184b Abs. 1 StGB, obwohl bei authentischen sexualbezogenen Bildaufnahmen und sexualisierenden Deepfakes im Kern das Recht auf sexuelle Selbstbestimmung und das Recht am eigenen Bild unabhängig vom Alter der dargestellten Person verletzt werden, auch wenn es graduelle Unterschiede im Unrecht bezüglich des Alters geben mag.

Insbesondere für das Abbilden oder manipulative Darstellen eines sexuellen Übergriffs an einer jugendlichen oder erwachsenen Person, der mit dem Abbilden des sexuellen Missbrauchs eines Kindes vergleichbar ist, erscheint der Strafrahmen unangemessen. Der djb fordert deshalb einen **Qualifikationstatbestand für das nicht einvernehmliche Herstellen, Besitzen / Gebrauchen und Zugänglichmachen eines Bildinhaltes, der einen sexuellen Übergriff wiedergibt oder wirklichkeitsnah darstellt**.[28]

Ein **Qualifikationstatbestand sollte zudem für das sog. Doxing**, also das unbefugte Zugänglichmachen persönlicher Daten mit dem sexualbezogenen Bildinhalt, vorgesehen werden. Auch dies ist ein massiver Datenkontrollverlust für die betroffene Person, der sie weiteren Gefahren aussetzt.[29]

Zudem sollte erwogen werden, **für das unbefugte Zugänglichmachen an Dritte einen höheren Strafrahmen vorzusehen als für das Herstellen und Gebrauchen**. Aufgrund der einfachen digitalen Verbreitungs- und Speichermöglichkeiten steigt mit dem unbefugten Zugänglichmachen an Dritte die Gefahr immens, dass ein Inhalt unbefugt verbreitet wird und nie gänzlich aus dem Netz gelöscht werden kann.[30]

d) Sozialadäquanzklausel

In § 184k Abs. 4 StGB-E soll nach einer Sozialadäquanzklausel die Strafbarkeit bei Handlungen entfallen, „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“. Zur gleichlautenden Klausel im geltenden § 184k Abs. 3 StGB besteht weitgehend Einigkeit, dass kaum ein Fall vorstellbar ist, in dem ein berechtigtes Interesse am unbefugten Herstellen, Gebrauchen und Zugänglichmachen einer sexualbezogenen Bildaufnahme besteht, das die Rechte der sexualbezogen abgebildeten Person überwiegt.[31] Tatsächlich ist ein **solches berechtigtes Interesse nur in eng umgrenzten Einzelfällen** denkbar, etwa wenn in einer Satire ein nicht einvernehmlicher und als solcher erkennbarer sexualisierender Deepfake am unteren Rand des strafwürdigen Unrechts zugänglich gemacht wird. Das sollte **in der Begründung klargestellt** werden.

e) Relatives Antragsdelikt

Der djb begrüßt, dass der Straftatbestand als relatives Antragsdelikt ausgestaltet werden soll. Dies ermöglicht es, von der Strafverfolgung in Fällen geringen Unrechts oder mangelnden Interesses der betroffenen Person an der Strafverfolgung abzusehen, und es ermöglicht die Strafverfolgung in Fällen, in

---

[28] Vgl. bereits djb, stn. 26-09, Policy Paper zum rechtlichen Handlungsbedarf bei nicht einvernehmlichen sexualisierenden Deepfakes, S. 10, abrufbar unter: https://www.djb.de/presse/stellungnahmen/detail/st26-09 (letzter Abruf: 28.04.2026).
[29] Vgl. bereits djb, stn. 26-09, Policy Paper zum rechtlichen Handlungsbedarf bei nicht einvernehmlichen sexualisierenden Deepfakes, S. 10, abrufbar unter: https://www.djb.de/presse/stellungnahmen/detail/st26-09 (letzter Abruf: 28.04.2026).
[30] Umfassender zu den Strafrahmen Schmidt (Fn. 3), S. 41 f., 55 ff.
[31] Vgl. u. a. Schmidt (Fn. 25), S. 57; Renzikowski, MüKo-StGB, § 184k Rn. 23; Eisele, TK-StGB, § 184k Rn. 21; Noltenius, SK-StGB§ 184k Rn. 21; Bosch, SSW-StGB, § 184k Rn. 8; Schumann, NK-StGB, § 184k Rn. 11; Seidl / Wittschurky, NStZ 2023, S. 392 (395).

denen es sich bspw. um Wiederholungstaten handelt und die Betroffenen nicht ermittelt werden können, unabhängig von einem Strafantrag.[32] Dabei sollte ermöglicht werden, **Strafanträge nicht nur per Mail, sondern auch bundeseinheitlich über Meldeportale sicher online einzureichen**. Es bedarf rechts- und datensicherer Verfahren für das Hochladen von Screenshots mit besonders sensiblen Inhalten.[33]

3. § 202e StGB-E

Der djb begrüßt die Einführung eines eigenen Straftatbestands zur Erfassung der unbefugten Ortung und Überwachung als Aspekte von Cyberstalking. Mit § 202e StGB-E setzt der Gesetzgeber zur Schließung einer wesentlichen Lücke im deutschen Strafrecht auch mit Blick auf die Vorgaben von Art. 6 der Richtlinie (EU) 2024/1385 an.

a) Als Cyberstalking erfasst Tathandlungen

Bei der Formulierung des Straftatbestands hat sich der Gesetzgeber ausdrücklich an Art. 6 der Richtlinie orientiert.[34] Durch den Straftatbestand wird neben der heimlichen Ortung mit technischen Mitteln, worunter sogenannte „AirTags“ fallen, auch anderweitige technische Überwachung mittels Spyware[35] als strafbares Unrecht tatbestandlich erfasst. Das Überwachen muss unbefugt erfolgen, darf also nicht von einem Einverständnis oder einer Befugnisnorm gedeckt sein. Der djb begrüßt, dass auf diese Weise auch strafwürdige Verhaltensweisen wie das Überwachen einer Person mit an sich legalen Ortungsdiensten wie ”AirTags”, der missbräuchlichen Nutzung von ”dual use"-Software oder das Aufspielen einer Stalkerware mit einem bekannten Passwort für das Smartphone strafbar wäre. Diese Begehungsweisen sind bislang nicht von § 238 Abs. 1 Nr. 5, Abs. 2 Nr. 4 StGB erfasst. Anders als im Referentenentwurf angegeben[36] hat die Änderung damit nicht nur deklaratorische Wirkung.

b) Schwerer Schaden

Aus Art. 6 der Gewaltschutz-RL soll die Formulierung übernommen werden, dass die Überwachung wahrscheinlich dazu führen muss, dass der Person schwerer Schaden zugefügt wird. Im Referentenentwurf wird dazu ausgeführt, dass der Schaden über die Verarbeitung der Daten hinausgehen muss und schwer sei, wenn er „über eine bloß geringfügige Belästigung oder Unannehmlichkeit hinausgeh[t], indem das Opfer erheblich oder nachhaltig beeinträchtigt wird”; die Zufügung eines Schadens soll wahrscheinlich sein, „wenn der Schadenseintritt im Einzelfall in Anbetracht der Gesamtumstände der Tat bei einem regelmäßigen Geschehensablauf naheliegt“.[37] Das genügt nicht.

Mit dem Merkmal soll eine ausufernde Strafbarkeit verhindert werden, also ein sinnvolles Anliegen verfolgt. Doch hat die Rechtsanwendung negative Erfahrungen mit der ähnlich lautenden ursprünglichen Erheblichkeitsschwelle (schwerwiegende Beeinträchtigung) in § 238 StGB gemacht.[38] Daher **sollte die Beeinträchtigungsschwelle der des § 238 StGB - der Eignung zur nicht unerheblichen Beeinträchtigung der Lebensgestaltung - angepasst werden**. Gerade bei der heimlichen Überwachung liegt der Schaden typischerweise schon in der gefährlichen Überwachung selbst, weil die Tatperson

---

[32] Vgl. insoweit zu § 184k BT-Drs. 19/15825, S. 18.

[33] Vgl. u. a djb, stn. 26-09, Policy Paper zum rechtlichen Handlungsbedarf bei nicht einvernehmlichen sexualisierenden Deepfakes, S. 10, abrufbar unter: https://www.djb.de/presse/stellungnahmen/detail/st26-09 (letzter Abruf: 28.04.2026).

[34] S. RefE S. 71.

[35] S. RefE S. 71.

[36] RefE S. 26.

[37] RefE S. 72.

[38] I.d.F. vom 1.3.2017 durch das Gesetz zur Verbesserung des Schutzes gegen Nachstellungen, BGBl. I 386: „geeignet, deren Lebensgestaltung schwerwiegend zu beeinträchtigen“; djb, stn. 21-06, Stellungnahme zum Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz/Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches – effektivere Bekämpfung von Nachstellungen und bessere Erfassung des Cyberstalkings, S.1, abrufbar unter: https://www.djb.de/fileadmin/user_upload/presse/stellungnahmen/st21-06_ (letzter Abruf: 06.05.2026).

eine andere Person kontrolliert. Das Persönlichkeitsrecht schützt hier die Freiheitssphäre der betroffenen Person vor dem Zugriff anderer.[39] In der heimlichen Überwachung liegt typischerweise auch ein erhebliches Gefahrenpotential, etwa wenn die Ortung die Adresse eines Frauenhauses offenbart oder einen (womöglich tödlichen) Angriff auf die betroffene Person ermöglicht. Die europarechtlichen Vorgaben stehen dem nicht entgegen; die Gewaltschutz-RL enthält nur Mindestvorgaben für die Strafbarkeit.[40]

c) Ständige Überwachung

Zutreffend stellt der Referentenentwurf nicht nur auf das wiederholte, sondern auch auf das ständige Überwachen ab. So werden auch Fälle erfasst, bei denen die Tatperson einmalig eine Stalkerware installiert oder einen "AirTag" platziert, die eine dauerhafte Überwachung ermöglichen. Doch ist das Merkmal "ständig" problematisch. Es verlangt, dass die Überwachung von gewisser Dauer ist. In der Begründung des Referentenentwurfes heißt es auf S. 71, dass zwar keine wiederholte Tatbegehung erforderlich ist, sie aber einen nicht unerheblichen Zeitraum andauern muss, wie „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". Es kann jedoch auch schon bei einer einstündigen Überwachung zu schweren Schäden kommen, bspw. wenn der bislang unbekannte Aufenthaltsort einer schutzsuchenden Frau bekannt wird. Daher sollte auch **das Überwachen einer Person mit Informations- und Kommunikationstechnik erfasst werden, wenn hierdurch ein schwerer Schaden droht**. Bei den Tatalternativen des wiederholten und ständigen Überwachens liegt der Verzicht auf das Merkmal des schweren Schadens ohnehin nahe.

d) Verortung

Die Einordung von § 202e StGB-E erscheint im 15. Abschnitt des besonderen Teils des StGB nicht passend. Zwar lässt sich die heimliche Überwachung gut im 15. Abschnitt verorten.[41] Thematisch liegt der Bezug zum Straftatbestand der Nachstellung in § 238 StGB im 18. Abschnitt jedoch näher, insbesondere angesichts der eindeutigen Übernahme von Merkmalen aus Art. 6 der Gewaltschutz-RL (Cyberstalking). Im 18. Abschnitt des Besonderen Teils des StGB wird die persönliche Freiheit geschützt. In dieser ist eine Person bereits betroffen, wenn eine Person überwacht wird, weil sie damit zu jedem Zeitpunkt auffindbar ist.

C. Artikel 4: Änderung der Strafprozessordnung

§ 184k StGB-E darf **nicht als Privatklagedelikt eingeordnet werden,** denn das wird dem Schutzziel nicht gerecht. Es handelt sich bei Phänomenen bildbasierter sexualisierter Gewalt nicht typischerweise um Bagatelldelikte, die untereinander geklärt werden können.

Der djb interpretiert den Referentenentwurf so, dass § 184k StGB-E weiterhin zum Katalog der Nebenklagedelikte in § 395 Abs. 1 Nr. 1 StPO gehört und begrüßt dies ausdrücklich. Damit wird den Betroffenen eine gesicherte Position als Beteiligte im Strafverfahren ermöglicht.[42]

Auch hier muss Kompetenz gesichert werden. Fälle bildbasierter sexualisierter Gewalt können nur dann effektiv strafrechtlich verfolgt werden, wenn damit befasste Justizangehörige sich des Phänomens, seines Unrechtscharakters und seiner geschlechtsspezifischen Dimension bewusst sind. Der djb fordert deshalb erneut, **Fortbildungsverpflichtungen für Justizangehörige im gesamten Verfahren** vorzusehen. Zudem sollten praktisch **flächendeckend Schwerpunktstaatsanwaltschaften oder zumindest spezialisierte Sonderabteilungen in Staatsanwaltschaften** eine effektive Verfolgung bildbasierter

[39] Vgl. VGH Hessen NJW 1994, 1750 (1751), OVG RhPf NJW 1986, 2659 (2660); NJW 2008, 822 (824).
[40] Vgl. EG 18 RL 2024/1385.
[41] Zu dieser Einschätzung vgl. auch *Leffler/Weber,* DuD 2022, 137, 142.
[42] Vgl. u. a. *djb*, stn. 26-09, Policy Paper zum rechtlichen Handlungsbedarf bei nicht einvernehmlichen sexualisierenden Deepfakes, S. 10, abrufbar unter: https://www.djb.de/presse/stellungnahmen/detail/st26-09 (letzter Abruf: 28.04.2026).

sexualisierter Gewalt ermöglichen, insbesondere im Falle von unbefugten Bildaufnahmen sexueller Übergriffe.[43]

D. Artikel 11: Änderung des Telekommunikationsgesetzes

Der djb begrüßt, dass erstmals auch Cyberstalking als digitale Gewaltform anerkannt werden soll. Die Strafnorm allein reicht jedoch nicht aus, um Betroffene wirksam vor dieser Gewaltform zu schützen. Gerade Cyberstalking ist oft ein Delikt, das heimlich durchgeführt wird und nur wenige Spuren hinterlässt. Aus diesem Grund sind ergänzende rechtliche Maßnahmen erforderlich. Digitale Gewalt wird häufig durch technische Hilfsmittel ermöglicht, die unter dem Deckmantel legitimer Nutzung vertrieben und beworben werden – etwa als „Familien-Sicherheits-App" oder „Diebstahlschutz".

Dazu **sollte das Verbot von Spionageanlagen nach § 90 TKG a.F.** – das nach Aufhebung des TKG 2004 derzeit nur über die Übergangsvorschrift des § 230 TKG fortgilt – **in eine konsolidierte Nachfolgeregelung überführt und auf Apps und Software ausgeweitet werden.**[44] Die Norm erfasst bislang ausschließlich Hardware, während Stalkerware in der Praxis digitaler Gewalt eine viel größere Bedeutung hat. Ein Verbot von Stalkerware würde dann auch mit einem Verbot der Bewerbung dieser Dienstleistung einhergehen. Es sind zudem klare Regeln zu Dual Use Technologien aufzustellen.

Zusätzlich **sollte ein Verbot des Tarnmodus – also der Funktion, eine App auf dem Endgerät der überwachten Person zu verbergen – eingeführt werden, grundsätzlich mit klar definierten Ausnahmen.** Die meisten AppStores lassen schon jetzt keine Apps zu, die einen Tarnmodus anbieten. Dies sollte jedoch gesetzlich verankert sein. Tarnmodi sind das zentrale technische Merkmal von Stalkerware. Sie können aber in eng umgrenzten Kontexten auch dem Schutz Betroffener dienen: So bietet etwa der Verein Gewaltfrei in die Zukunft e.V. eine getarnte Schutz-App für Betroffene häuslicher Gewalt an. Die **Ausnahmen sollten sich auf zertifizierte Schutz- und Beratungsanwendungen beschränken.**

E. Zusammenfassung

Ein wirksames Gesetz gegen digitale Gewalt muss Betroffene schützen und entlasten, Plattformen in die Verantwortung nehmen und digitale Gewalt als das behandeln, was sie ist: ein Angriff auf die Persönlichkeit, auf die Gleichberechtigung und Teilhabe an der demokratischen Öffentlichkeit.

Der djb begrüßt, dass erstmals ein Gesetz geschaffen werden soll, dass sich explizit den Defiziten in der zivilrechtlichen Durchsetzung widmet. Es ist jedoch erkennbar, dass das Phänomen digitale Gewalt viel zu eng gedacht wird. Nach dem Entwurf werden etwa Rechtsverletzungen unterhalb der Strafbarkeitsschwelle nicht erfasst. Damit gibt es weniger Schutz als mit der geltenden Rechtslage. Zudem kann der vom Entwurf versprochene Schutz nicht schnell genug erlangt werden. Auskunftsanspruch und Accountsperren brauchen klare und kurze Fristen, keine zusätzlichen Hürden für die Betroffenen. Betroffene sind nur dann wirksam geschützt, wenn die Erreichbarkeit rechtsverletzender Inhalte schnellstmöglich verhindert wird. Zudem werden Betroffene weiterhin allein gelassen mit der Verfolgung ihrer Rechte. Der djb begrüßt insofern die neu zu schaffende Möglichkeit der Prozessstandschaft. Um die strukturelle Dimension digitaler Gewalt adressieren zu können, braucht es aber ein echtes Verbandsklagerecht. Es braucht umfassende Regelungen zu Stalkerware und Trackern sowie einen umfas-

---

[43] Vgl. *djb*, stn. 26-09, Stellungnahme: Rechtlicher Handlungsbedarf bei nicht-einvernehmlichen sexualisierenden Deepfakes. S. 11, abrufbar unter https://www.djb.de/presse/stellungnahmen/detail/st26-09 (letzter Abruf: 28.04.2026); djb, stn. 23-17 Policy Paper: Bekämpfung bildbasierter sexualisierter Gewalt, S. 9, abrufbar unter https://www.djb.de/fileadmin/user_upload/presse/stellungnahmen/st23-17_Bildbasierte_Gewalt.pdf (letzter Abruf: 28.04.2026).

[44] Köver, Der Feind in der eigenen Tasche – Stalkerware und digitale Überwachung im Kontext von Partnerschaftsgewalt, in: Bundesverband Frauenberatungsstellen und Frauennotrufe, Nivedita Prasad (Hg.), Geschlechtsspezifische Gewalt in Zeiten der Digitalisierung, Bielefeld 2021, S. 227.

senden Adressschutz. Die Instrumentalisierung von digitaler Gewalt für ausufernde Überwachungsmaßnahmen ist abzulehnen. Stattdessen sind zielgerichtete und wirksame Instrumente zur Ermittlung der Tatperson einzuführen.

In strafrechtlicher Hinsicht begrüßt der djb ausdrücklich, dass ein Straftatbestand geschaffen werden soll, der Phänomene bildbasierter sexualisierter Gewalt einschließlich nicht einvernehmlicher sexualisierter Deepfakes systematisch adressiert. Damit sind Betroffene deutlich besser vor einer schwerwiegenden Verletzung des Rechts auf sexuelle Selbstbestimmung, des Rechts am eigenen Bild und des Rechts auf Nichtdiskriminierung geschützt. Allerdings sind im Referentenentwurf weder alle strafwürdigen Bildinhalte noch das unbefugte Gebrauchen oder Besitzen als Tathandlung erfasst. Auch bei den Strafrahmen bedarf er der Nachbesserung, insbesondere sollten Strafschärfungen für die Wiedergabe eines sexuellen Übergriffs und für das unbefugte Zugänglichmachen persönlicher Daten zusammen mit einem sexualbezogenen Bildinhalt vorgesehen werden. Zu begrüßen ist zudem, dass der Referentenentwurf vorsieht, Strafbarkeitslücken beim Überwachen einer Person mit digitalen Mitteln zu schließen. Allerdings sollte hier die Erheblichkeitsschwelle an die des § 238 StGB – Eignung zur nicht unerheblichen Beeinträchtigung der Lebensgestaltung – angepasst werden, zudem sollte auch die kurzzeitige Überwachung unter Strafe gestellt werden, wenn dadurch ein erheblicher Schaden droht. Der djb betont erneut, dass es einer Fortbildungsverpflichtung für Justizangehörige im gesamten Verfahren und spezialisierter Sonderabteilungen in Staatsanwaltschaften bedarf, um eine effektive Verfolgung bildbasierter sexualisierter Gewalt zu ermöglichen.

Beim rechtlichen Vorgehen gegen digitale Gewalt sind nicht nur die Anonymität der Tatpersonen und der bislang fehlende, alle Formen strafwürdiger bildbasierter sexualisierter Gewalt umfassende Straftatbestand problematisch, sondern auch die schnelle und starke Verbreitung von Inhalten im Netz, die Rechte von Individualpersonen verletzen. Oft übersteigt es die finanziellen und persönlichen Ressourcen der Betroffenen, sich mit rechtlichen Mitteln angemessen dagegen zur Wehr zu setzen. Damit werden sie mit diesem Entwurf eines Gesetzes zur Stärkung des zivilrechtlichen und strafrechtlichen Schutzes vor digitaler Gewalt weitgehend allein gelassen. Das zeigt sich insbesondere in der fehlenden Förderung von Beratungsstrukturen. Der djb weist deshalb noch einmal nachdrücklich darauf hin, dass das Unterstützungsnetz für Betroffene durch zivile Verbände und Vereinigungen flächendeckend und dauerhaft finanziert und ausgebaut werden muss, um spezifische und schnell wirksame psychologische, rechtliche und soziale Beratung für Betroffene digitaler Gewalt zu ermöglichen.[45]

[45] Vgl. u. a. djb, stn. 26-09, Stellungnahme: Rechtlicher Handlungsbedarf bei nicht-einvernehmlichen sexualisierenden Deepfakes. S. 11, abrufbar unter https://www.djb.de/presse/stellungnahmen/detail/st26-09 (letzter Abruf: 28.04.2026).; djb, stn. 23-17 Policy Paper: Bekämpfung bildbasierter sexualisierter Gewalt, S. 14, abrufbar unter https://www.djb.de/fileadmin/user_upload/presse/stellungnahmen/st23-17_Bildbasierte_Gewalt.pdf (letzter Abruf: 28.04.2026).