STELLUNGNAHME

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

HateAid gGmbH
Kontakt: legal@hateaid.org
22. Mai 2026

# Inhalt


**1 Digitale Gewalt als Massenphänomen und Gefahr für die Demokratie ... 3**

**2 Zivilrecht als Instrument für Betroffene gegen digitale Gewalt ... 4**

2.1 Katalog von Straftaten, § 1 Abs. 1 Nr. 2 lit. a)-c) – GgdG-E ... 5

2.2 Diensteanbieter, § 1 Abs. 2 GgdG-E ... 5

2.3 Auskunft über Daten, § 2 GgdG-E ... 6

2.4 Sperrung von Nutzerkonten in sozialen Netzwerken ... 9

2.5 Digitale Antragstellung ... 10

2.6 Vertretung durch zivilgesellschaftliche Organisationen ... 10

2.7 Pflicht zur Benennung von inländischen Zustellungsbevollmächtigten für soziale Netzwerke ... 10

**3 Strafrecht als notwendiger Bestandteil des Schutzes vor digitaler Gewalt ... 11**

3.1 Wirkung über die Bestrafung von Tatpersonen hinaus ... 12

3.2 Einführung eines neuen § 184k StGB ... 13

3.3 Einführung eines neuen § 201b StGB ... 19

3.4 Einführung eines neuen § 202e StGB ... 20

**Die gemeinnützige Organisation HateAid** wurde 2018 gegründet und hat ihren Hauptsitz in Berlin. Sie setzt sich für Menschenrechte im digitalen Raum ein und engagiert sich auf gesellschaftlicher wie politischer Ebene gegen digitale Gewalt und deren Folgen. HateAid unterstützt Betroffene konkret psychosozial durch Beratung und im Rahmen der Prozesskostenfinanzierung bei der Rechtsdurchsetzung. HateAid hat in mehr als 150 Fällen Betroffene digitaler Gewalt bei der gerichtlichen Durchsetzung ihrer Persönlichkeitsrechte unterstützt. Hierdurch konnte die Organisation umfangreiche Erfahrungswerte aus dem Eilrechtsschutz, der Durchsetzung von Unterlassungsansprüchen und Geldentschädigungen, sowie in Auskunftsverfahren nach dem TTDDDG sammeln.

# 1. Digitale Gewalt als Massenphänomen und Gefahr für die Demokratie

Digitale Gewalt ist längst kein Einzelfall mehr, sondern ein weitverbreitetes Massenphänomen. Täglich sind unzählige Menschen in sozialen Netzwerken, Kommentarspalten oder Messenger-Diensten Anfeindungen, Hassrede, Bedrohungen und gezielten Einschüchterungen ausgesetzt. 45 % der Internetnutzenden haben bereits Hass im Netz wahrgenommen. Oftmals handelt es sich hierbei um rechtswidrige Äußerungen, die wenigstens persönlichkeitsrechtsverletzend und häufig sogar strafbar sind.

Darüber hinaus verletzt digitale Gewalt nicht nur individuelle Persönlichkeitsrechte, sondern hat auch gesamtgesellschaftliche Auswirkungen. Sie entfaltet einen sogenannten *Silencing Effect*: Menschen ziehen sich aus öffentlichen Debatten zurück, verzichten auf Meinungsäußerungen oder politische Teilhabe, weil sie Anfeindungen befürchten. 54 % der Internetnutzenden bekennen sich seltener zu ihrer politischen Meinung und 47 % beteiligen sich insgesamt seltener an Diskussionen im Internet. Besonders häufig betrifft dies Frauen, queere Menschen, People of Color sowie Personen in politischen oder journalistischen Funktionen.

## 2. Zivilrecht als Instrument für Betroffene gegen digitale Gewalt

Für Betroffene digitaler Gewalt stellt der Zivilrechtsweg in der Theorie ein effektives Mittel des Rechtsschutzes dar. Er ist für Betroffene die einzige Möglichkeit, die Entfernung rechtsverletzender Inhalte gerichtlich durchzusetzen. Unterlassungstitel bieten zudem einen umfassenden, strafbewehrten und sogar in die Zukunft gerichteten Schutz vor der Verbreitung rechtsverletzender Inhalte durch bestimmte Verfasser*innen oder Plattformen. In Fällen krasser Persönlichkeitsrechtsverletzungen können auch Geldentschädigungen geltend gemacht werden. Zudem gelten im Zivilrecht andere Haftungsmaßstäbe als im Strafrecht. Auf diese Weise können Zivilgerichte Schutzbehauptungen im Wege der freien Beweiswürdigung begegnen und ggf. zu einer Beweislastumkehr gelangen. Dies geschieht regelmäßig, wenn z. B. Accountinhaber*innen behaupten, einen Kommentar nicht gepostet zu haben und stattdessen hypothetische Arbeitskolleg*innen, anonyme Familienmitglieder oder gar Fremde als potenzielle Tatpersonen ins Feld führen. Anders als Strafgerichte haben Zivilgerichte im Wege der sekundären Darlegungslast die Möglichkeit, mutmaßlichen Verfasser*innen substantiierten Vortrag und Beweise, bspw. für die Fremdnutzung ihres Accounts, abzuverlangen.

Trotz vieler Vorteile bestehen in der Praxis hohe Hürden für die zivilrechtliche Rechtsdurchsetzung. Dies ist vor allem auf anonyme Verfasser*innen, hohe Streitwerte und Kostenrisiken, sowie lange Verfahrenslaufzeiten zurückzuführen. Nur sehr wenige Betroffene können diesen Weg ohne Unterstützung beschreiten. Den meisten mangelt es an Wissen oder Ressourcen. Wir verfolgen die aktuellen zivilprozessualen Entwicklungen daher mit großem Interesse.

Der Referentenentwurf sieht vor, die aktuell im TDDDG geregelten Auskunftsansprüche zu reformieren und das neue Instrument gerichtlich angeordneter Accountsperren einzuführen. Darüber hinaus soll die Erreichbarkeit von Online-Plattformen mit Hauptsitz im Ausland im Rahmen der europarechtlichen Vorgaben verbessert werden.

HateAid begrüßt diese Maßnahmen, die geeignet erscheinen punktuelle Verbesserungen bei der Rechtsdurchsetzung in Fällen digitaler Gewalt zu bewirken. Die Organisation betont jedoch, dass viele Hürden bei der Rechtsdurchsetzung in Hauptsacheverfahren bestehen bleiben.

Grundlegende Hürden der zivilrechtlichen Rechtsdurchsetzung bleiben jedoch bestehen. So wird auch künftig ein auf Unterlassung und Geldentschädigung gerichtetes Verfahren mehrere Monate bis Jahre in Anspruch nehmen. Wegen der hohen, am Presserecht orientierten Streitwerte von EUR 10.000,00 pro angegriffener Äußerung, wird sich das Kostenrisiko weiterhin auf EUR 2812,50 für die eigenen Kosten der anwaltlichen Vertretung und Gerichtskosten belaufen. Diese Kosten sind in der Regel vorzustrecken. Eine anwaltliche Vertretung ist zudem wegen der hohen Streitwerte und der damit verbundenen zwingenden Zuständigkeit der Landgerichte verpflichtend.

## 2.1. Katalog von Straftaten, § 1 Abs. 1 Nr. 2 lit. a)-c) – GgdG-E

Das BMJV stellt im vorliegenden Referentenentwurf für ein Gesetz gegen digitale Gewalt darauf ab, dass dieses für einen Katalog von Straftaten anwendbar sein soll. Dies hat zur Folge, dass die Auskunft über Nutzerdaten nach § 2 GgdG-E nur dann beantragt werden kann, wenn sich der Antrag auf die Verfasser*innen strafrechtlich relevanter Inhalte bezieht. Dies führt zu einem Widerspruch. Denn auf diese Weise ist der Anspruch auf die Auskunft von Accountinhaber*innendaten an strengere Voraussetzungen geknüpft als die zivilrechtliche Rechtsdurchsetzung, die er ausdrücklich ermöglichen soll. Für die Durchsetzung von Entfernungs- oder Unterlassungsansprüchen ist nämlich eine Persönlichkeitsrechtsverletzung ausreichend. Diese kann auch unterhalb der Strafbarkeitsschwelle beginnen.
Die Gründe für diesen Widerspruch sind nicht selbsterklärend. Sie könnten möglicherweise daraus resultieren, dass der Wunsch besteht, eine ausufernde Anwendung des Auskunftsanspruchs auf alle denkbaren Rechtsverletzungen zu verhindern. Insbesondere mag dahinter die Intention stehen, z. B. Fälle der Durchsetzung von Unternehmenspersönlichkeitsrechten, etwa bei negativen Restaurantbewertungen auszuschließen. Diese wäre wohl nach dem allgemeinen Verständnis nicht mehr unter den Oberbegriff „digitale Gewalt“ zu subsumieren. Dieser mögliche Anwendungsbereich war jedenfalls nach der Veröffentlichung des in dieser Hinsicht weiter gefassten Eckpunktepapiers zu diesem Gesetz kritisiert worden. Obschon andere Wege denkbar wären, den Anwendungsbereich einzugrenzen, ist nach dem Dafürhalten von HateAid ein Straftatenkatalog eine gangbare Möglichkeit. Hierdurch werden die meisten der Fälle digitaler Gewalt, erfasst, die HateAid regelmäßig über die Betroffenenberatung erreichen. HateAid empfiehlt dennoch über den aktuellen Katalog hinaus die Straftatbestände der Nötigung (§ 240 StGB) und der Erpressung (§ 253 StGB) auszuweiten. Hierüber könnten bspw. Fälle der Nötigung unter Androhung der Veröffentlichung sexualisierter Deepfakes ("Sextortion") ebenfalls erfasst werden.

## 2.2. Diensteanbieter, § 1 Abs. 2 GgdG-E

Die Regelungen des Gesetzes sollen ausschließlich für Online-Plattformen, sowie Web- und Cloud-Hosting-Anbieter gelten. Diese Regelung führt zu Abgrenzungsschwierigkeiten in Fallkonstellationen digitaler Gewalt, z. B. in sehr großen Gruppen von hunderten oder gar tausenden Mitgliedern oder sogar in öffentlich einsehbaren Kanälen von Messengerdiensten. Diese werden teilweise wie Online-Plattformen behandelt. Es mangelt jedoch an klar abgrenzbaren Kriterien der Funktionalitäten, für die das gelten soll, z. B. der Anzahl der Mitglieder in Gruppen. Diese Funktionen sind vor allem für die Verbreitung bildbasierter digitaler Gewalt von hoher Relevanz. Nach der aktuell vorgesehenen Regelung wäre es unklar, ob eine Betroffene einen Auskunftsanspruch gegen Nutzende einer WhatsApp oder Telegramm-Gruppe mit 600 Mitgliedern geltend machen kann oder nicht. Wird dies offengelassen, wäre diese Frage durch die Gerichte oder künftigen Leitlinien der EU-Kommission zur Behandlung von Messengerdiensten unter dem Digital Services Act zu beantworten. Hiermit geht eine erhebliche Rechtsunsicherheit für Nutzende einher, die durch eine Klarstellung im Gesetz beseitigt werden könnte.

## 2.3. Auskunft über Daten, § 2 GgdG-E

HateAid begrüßt besonders die Reform der Auskunftsansprüche, die bisher im TDDDG geregelt sind. Diese haben sich in ihrer aktuellen Ausgestaltung als praktisch nutzlos erwiesen. Dies liegt vor allem darin begründet, dass die im Rahmen des Verfahrens zu beauskunftenden Daten für Privatpersonen nicht brauchbar sind. Richtigerweise soll die Auskunft von Accountinhaber*innendaten auch künftig dem Richtervorbehalt unterstehen.

### a) Beschränkung des Auskunftsanspruchs

HateAid empfiehlt den Auskunftsanspruch auf Telekommunikationsanbieter und E-Mailprovider verwertbar zu machen. Auf diese Weise könnten die zu beauskunftenden E-Mailadressen und Telefonnummern für eine Identifizierung von Verfasser*innen herangezogen werden.
Es ist nicht nachvollziehbar, warum der Anspruch gemäß § 2 Abs. 1 GgdG-E auf Internetzugangsdienste und Dienste, die zur Begehung einer Katalogtat verwendet wurden, beschränkt werden soll. Es würde die Wahrscheinlichkeit der Identifizierung von Accountinhaber*innen wesentlich erhöhen, wenn der Anspruch sich auch auf Telekommunikations- und E-Mail-Diensteanbieter erstrecken würde. Ohne diese Öffnung können gemäß § 2 Abs. 2 Nr. 1 lit. a), Nr. 2 GgdG-E beauskunftete Telefonnummern und E-Mailadressen, nicht durch eine Abfrage beim jeweiligen Anbieter ihren jeweiligen Inhaber*innen zugeordnet und so für eine zivilrechtliche Rechtsdurchsetzung verwertbar gemacht werden. Dies ist verschenktes Potenzial. Denn insbesondere die Telefonnummer ist in der EU ein Datum, welches häufig die Zuordnung zu einem Anschlussinhaber zulässt. Innerhalb der EU erfordert nämlich selbst die Anschaffung einer Prepaid-Karte die Verifikation von Daten, z.B. durch ein Ausweisdokument per Post-Ident. Gleichzeitig sind E-Mailadressen und Telefonnummern oftmals die einzig verifizierten Daten, die Online-Plattformen vorliegen. Sie werden u.a. zur Einrichtung von Accounts oder Verwendung einer Zwei-Faktor-Authentifizierung genutzt.

### b) Reichweite der Auskunft, § 2 Abs. 2 GgdG-E

Zu begrüßen ist, dass künftig auch die IP-Adresse wieder von der Auskunft erfasst sein soll. Als besonders begrüßenswert hervorzuheben ist, dass sich der Anspruch auf Auskunft anders als seine Vorgängerregelungen explizit nicht nur auf die IP-Adresse und Portnummer des Uploads, sondern auch des letzten Logins erstrecken soll (Art. 2 Abs. 2 Nr. 1 lit. c) GgdG-E). Denn die IP-Adresse des Uploads des strafbaren Inhalts, wird selbst mit einer gesetzlich geregelten Mindestspeicherdauer, oftmals nicht mehr abrufbar sein. Aus diesem Grund ist vor allem die IP-Adresse des letzten Logins ein vielversprechendes Datum zur Identifizierung der Anschlussinhaber*innen.
Ausdrücklich zu begrüßen ist auch die in Art. 2 Abs. 2 Nr. 3 vorgesehene Regelung, wonach eine Kopie des angegriffenen Inhalts durch die Plattform erstellt und übermittelt werden muss. Zu beachten ist hierbei, dass es sich bei dieser Kopie um einen Screenshot handeln muss, der alle zur weiteren Rechtsverfolgung erforderlichen Angaben enthält. Diese sollte zudem auch elektronisch und nicht etwas in Papierform übermittelt werden müssen, damit sie nach der Einsicht durch Antragstellende auch für weitere Rechtsdurchsetzung verwendet werden kann. Hierzu zählen Datum und Uhrzeit des Screenshots, sowie

Datum und Uhrzeit des angegriffenen Inhalts und ggf. auch der Ausgangsinhalt, wenn sich die Rechtsverletzung nur aus dem Kontext ergibt. Diese Beweissicherung wird Betroffenen von digitaler Gewalt bewusst erschwert, in dem die Angaben gerade nicht auf einem einfachen Bildschirmfoto enthalten sind. Darüber hinaus sind sie in der Regel nur in der Desktopversion und nicht etwa in der App sichtbar, was nicht dem üblichen Nutzungsverhalten entspricht. Die meisten Nutzenden nutzen Online-Plattformen heutzutage hauptsächlich über Apps auf ihrem Smartphone.

## c) Beweissichernde Anordnungen, § 3 GgdG-E

HateAid begrüßt ausdrücklich die angedachte Regelung zu beweissichernden Anordnungen. Diese können entscheidend dazu beitragen, dass Auskunftsansprüche nicht wegen eines Datenverlusts ins Leere laufen. Dies setzt jedoch voraus, dass die Gerichte Anordnungen unverzüglich übermitteln. Insbesondere sind die vorgesehenen Regelungen auf diese Weise nicht auf Speicherfristen für IP-Adressen angewiesen. Dies gilt insbesondere, weil sich die beweissichernde Anordnung auch auf die IP-Adresse des letzten Logins vor Zustellung der Anordnung erstrecken soll (§ 3 Abs. 1 Nr. 1, Abs. 2 iVm § 2 Abs. 2 GgdG-E). Dies erhöht die Wahrscheinlichkeit, dass die beauskunftete IP-Adresse einem Anschlussinhaber zugeordnet werden kann. Eine Garantie ist dies jedoch nicht. Denn die Speicherdauer von IP-Adressen hängt allein von den internen Geschäftsvorgängen der Hostingprovider ab. Laut Bundeskriminalamt schwanken diese zwischen 0 und bis zu 7 Tagen (nicht Werktage!). Es ist daher entscheidend, dass die Abfrage von IP-Adressen bei Hostingprovidern durch die Gerichte schnellstmöglich nach Erhalt geschieht. Dies muss seitens der Gerichtsverwaltung sichergestellt werden.

## d) Fristen zur Mitwirkung der Diensteanbieter

HateAid empfiehlt darüber hinaus dringend Fristen für die Mitwirkung der Diensteanbieter und Internetzugangsdienste, sowie etwaigen Drittanbieter gesetzlich zu regeln. Andernfalls droht ein Datenverlust, der das gesamte Auskunftsverfahren obsolet machen könnte. Als empfehlenswert wird eine Regelung erachtet, wonach die Sicherungskopie (§ 3 Abs. 1 GgdG-E) unverzüglich, spätestens jedoch spätestens nach 12 Stunden zu erstellen und an das Gericht zu übermitteln ist. Die Übermittlung der Bestands- und Verkehrsdaten durch die Diensteanbieter an das Gericht (§ 3 Abs. 2 GgdG-E), sollte unverzüglich, spätestens jedoch nach 24 Stunden erfolgen. Gleiches gilt für die Sicherung der IP-Adresse durch den Internetzugangsdienst (§ 3 Abs. 3 GgdG-E), welche nicht mehr als 12 Stunden dauern darf. Ist eine Frist nicht gesetzlich geregelt, steht ein Datenverlust durch eine zu langsame Mitwirkung der Diensteanbieter und Internetzugangsdienste zu befürchten. Aus anderen Kontexten, u.a. dem Digital Services Act, ist bekannt, dass unbestimmte Formulierungen sehr unterschiedlich ausgelegt werden. So bedeutet „unverzüglich“ im Sinne des Art. 16 Abs. 5 DSA in der Praxis nach der Erfahrung von HateAid 30 Minuten bis 14 Tage.

## e) Entfernung von Inhalten

Der Entwurf sieht in § 4 Abs. 4 GgdG-E vor, dass mit einer Profilsperre gleichzeitig die Entfernung rechtswidriger Inhalte angeordnet werden soll. HateAid empfiehlt dringend, dies auch für die Geltendmachung des Auskunftsanspruchs zu regeln. Dem steht jedenfalls der Art. 6 des Digital Services Acts nicht entgegen. Spätestens mit Einreichen eines Antrags auf Auskunftserteilung, hat der beteiligte Diensteanbieter positive Kenntnis des rechtsverletzenden Inhalts und ist ohnehin zur Prüfung verpflichtet. Aus der Erfahrung von HateAid führt die Anstrengung eines Auskunftsverfahrens jedoch in der Regel nicht auch zu einer Entfernung der Inhalte durch die Diensteanbieter. Dies also direkt im gerichtlichen Verfahren anzuordnen, welches ohnehin die Strafbarkeit der Inhalte feststellen muss, wäre nur konsequent.
Es erschließt sich nicht, warum die Anträge diesbezüglich nicht gleichbehandelt werden sollten, insbesondere da beide Verfahren der freiwilligen Gerichtsbarkeit nach dem FamFG sind und den gleichen prozessualen Vorschriften unterliegen. Betroffene digitaler Gewalt sind oftmals vorrangig an der Entfernung von Inhalten interessiert, damit sich diese nicht weiterverbreiten können. Einen nachhaltig wirkenden Unterlassungsanspruch können sie naturgemäß erst nach Abschluss des Auskunftsverfahrens durchsetzen. Betroffene könnten vorher allenfalls die Plattform im einstweiligen Rechtsschutz auf Entfernung in Anspruch nehmen. Dies müsste jedoch parallel zum Auskunftsverfahren geschehen, da ansonsten die Dringlichkeitsfrist verstreicht. Der späteren Geltendmachung eines Unterlassungsanspruchs gegen Verfasser*innen stünde die Entfernungsanordnung nach Abschluss des Auskunftsverfahrens jedenfalls nicht entgegen. So könnten Betroffene in Ruhe das Auskunftsverfahren abwarten und anschließend eruieren, welche Ansprüche sie in einem möglichen Klageverfahren geltend machen möchten. Ein etwaiger Unterlassungsanspruch würde auch deshalb nicht vorweggenommen werden, da ein gerichtlicher Titel auf Unterlassung umfassender in seiner Wirkung ist als eine Entfernungsanordnung und insbesondere auch in die Zukunft wirkt.

HateAid warnt zudem davor, dass durch die in § 8 Abs. 2 GgdGE getroffene Zuständigkeitsregelung eine für Antragstellende nachteilige Verengung eintreten könnte. Diese könnte sie nach der derzeitigen Formulierung fliegenden Gerichtsstands berauben und künftig für die Durchsetzung von auf einen Auskunftsanspruch folgenden Unterlassungsansprüchen an ihren Wohnsitz binden

## f) Kosten der Auskunft

Der Entwurf stellt in Bezug auf die Kosten eines solchen Auskunftsverfahrens allein auf die Geltung des § 81 Abs. 1 FamFG ab. Diese stellt die Kostenverteilung ins Ermessen des Gerichts. Der Entwurf geht ferner davon aus, dass das Verfahren gebührenfrei ist.

Zu begrüßen ist, dass künftig die ausdrückliche Anordnung der Kostentragung des § 21 Abs. 3 TDDDG entfallen soll. Diese führte bisher dazu, dass Antragstellende die Gerichtsgebühren, sowie auch die Kosten der anwaltlichen Vertretung der beteiligten Plattform zu tragen hatten. Dies galt stets, obwohl für das Verfahren nach dem FamFG kein Anwaltszwang besteht. Die Kosten beliefen sich insgesamt auf ca. EUR 900,00 pro Äußerung. Diesen Zustand aufrechtzuerhalten wäre fatal, da künftig zusätzlich auch die Internetzugangsdienste Beteiligte sein sollen. Demzufolge kämen weitere Kosten hinzu. Diese Kosten übersteigen die Gerichtskosten und fallen daher besonders erheblich ins Gewicht.

Es ist aus Sicht von HateAid jedoch fraglich, ob allein der Wegfall der Kostenanordnung in § 21 Abs. 3 TDDDG eine maßgebliche Verbesserung zur Folge haben wird. Denn die dem Entwurf zugrundeliegende Annahme, das Verfahren sei gebührenfrei, ist nichtzutreffend. In jedem von HateAid im Rahmen der Prozesskostenfinanzierung unterstützten Auskunftsverfahren, wurden Gerichtsgebühren erhoben. Dementsprechend ist davon auszugehen, dass Gerichte grundsätzliche an der Praxis, Gebühren zu erheben und diese nach eigenem Ermessen den Antragstellenden aufzuerlegen festhalten können.
HateAid empfiehlt daher dringend die Gebührenfreiheit des Verfahrens im Gesetz zu verankern und zudem anzuordnen, dass die Beteiligten ihre Kosten selbst zu tragen haben. Insbesondere bei beteiligten Unternehmen wird eine anwaltliche Vertretung regelmäßig nicht erforderlich sein. Sofern diese dennoch auch ohne Anwaltszwang in Anspruch genommen wird, darf dies nicht zu Lasten der Antragstellenden gehen.

### g) Internationale Zuständigkeit

Der Entwurf geht davon aus, dass für ein Auskunftsverfahren in der Regel der deliktische Gerichtsstand gemäß Art. 7 Nr. 2 EuGVVO geltend wird. Dies ist zwar wünschenswert, steht jedoch der gerichtlichen Praxis in Deutschland entgegen. Die Gerichte nehmen nämlich regelmäßig für Verfahren nach § 21 TDDDG keine deliktische Zuständigkeit an. Allenfalls denkbar ist daher ein Abstellen auf den Verbrauchergerichtsstand gemäß Art. 17, 18 EuGVVO, um den internationalen Gerichtsstand in Deutschland zu begründen. Dies kommt allerdings nur für diejenigen in Betracht, die Online-Plattformen rein in ihrer Eigenschaft als Privatpersonen nutzen. Dies scheidet nach gefestigter Rechtsprechung der Gerichte bereits dann aus, wenn die berufliche oder ehrenamtliche Tätigkeit im Profil referenziert oder gelegentlich in Inhalten thematisiert wird. Hiervon wären daher mit hoher Wahrscheinlichkeit vor allem besonders von digitaler Gewalt betroffene Personen des politischen Lebens, Journalist*innen, Aktivist*innen tangiert. Zugleich wären automatisch ganze Plattformen vom Auskunftsanspruch ausgeschlossen, z.B. die Berufsnetzwerke LinkedIn und Xing.
Diese maximale und lebensfremde Verengung des Verbrauchergerichtsstandes durch die deutschen Gerichte gefährdet nicht nur die effektive Durchsetzung von Auskunftsansprüchen, sondern die Rechtsdurchsetzung gegenüber Plattformen insgesamt. Die Bundesregierung sollte sich daher dringend für eine europäische Regelung einsetzen, die dem entgegenwirkt.

## 2.4. Sperrung von Nutzerkonten in sozialen Netzwerken

Die in § 4 GgdG-E vorgesehene Einrichtung eines gerichtlichen Verfahrens zur vorübergehenden Sperrung von Profilen, ist grundsätzlich zu begrüßen. Die Profilsperre kann ein sinnvoller ergänzender Baustein zum oftmals herausfordernden Umgang mit digitaler Gewalt sein. HateAid sieht die Relevanz dieses Anspruchs vor allem bei Fällen, in denen der Accountinhaber zwar bekannt, aber im Ausland ansässig und deswegen weder für die Strafverfolgungsbehörden noch für die Zivilgerichte erreichbar ist.

Wie bereits beim Diskussionsentwurf ist nicht nachvollziehbar, warum die Profilsperre bereits bei einer schwerwiegenden Beeinträchtigung der Persönlichkeitsrechte erfolgen kann, die Auskunft jedoch die Begehung einer Straftat erfordert. Die Eingriffsintensität beider Verfahren ist wohl vergleichbar.

Die Praxisrelevanz des Anspruchs wird maßgeblich davon abhängen, ob der Anspruch wirklich gebühren- und auch ansonsten kostenfrei durchgesetzt werden kann. Andernfalls ist nicht zu erwarten, dass Betroffene eine Incentivierung haben ein Verfahren zur vorübergehenden Profilsperre überhaupt anzustrengen. Andernfalls könnte der einstweilige Rechtsschutz gerichtet auf die dauerhafte Entfernung und Unterlassung von Inhalten gegen die Plattform für Betroffene vorzugswürdig sein. Zur Kostenregelung gilt das oben unter Punkt f. Gesagte.

Darüber erachtet HateAid die Umgehungsgefahr einer solchen Profilsperrung nach wie vor als sehr hoch. Die Einrichtungen der Plattformen zur Erkennung von Mehrfachprofilen können leicht umgangen werden. Daher ist nach unserer Auffassung unklar, wie die Regelung aus Art. 4 Abs. 2 GgdG-E technisch umgesetzt werden soll.

## 2.5. Digitale Antragstellung

Sowohl dem Auskunftsanspruch als auch der Profilsperre könnte eine digitale Antragstellung zu mehr Praxisrelevanz verhelfen. Diese könnte dem Mahnverfahren nachempfunden sein. Angesichts dessen, dass bei der freiwilligen Gerichtsbarkeit der Amtsermittlungsgrundsatz gilt, wäre dies ohne Weiteres möglich. Insbesondere wäre nicht zu befürchten, dass Antragstellende mit mangelhaftem oder unvollständigem Vortrag präkludiert sind.

## 2.6. Vertretung durch zivilgesellschaftliche Organisationen

HateAid begrüßt ausdrücklich, dass künftig auch zivilgesellschaftliche Organisationen im Hinblick auf den Auskunftsanspruch vertretungsbefugt sein sollen. Eine anwaltliche Vertretung ist kostenpflichtig, und zwar nicht gesetzlich vorgeschrieben, dennoch trauen sich Betroffene selten den Gang zum Gericht allein zu. Es erscheint daher mehr als sachgerecht Organisationen mit der notwendigen juristischen Expertise zur Vertretung in diesen als kostenlos angedachten Verfahren zu befähigen. Aufgrund des in der freiwilligen Gerichtsbarkeit geltenden Amtsermittlungsgrundsatzes ist das Haftungsrisiko zudem gering.

## 2.7. Pflicht zur Benennung von inländischen Zustellungsbevollmächtigten für soziale Netzwerke

Erwartungsgemäß sieht der Referentenentwurf eine modifizierte Regelung eines Zustellungsbevollmächtigten im Rahmen der europarechtlichen Grenzen vor. Diese Grenzen werden durch die angedachte Regelung wohl angemessen ausgeschöpft. Nicht nachvollziehbar erscheint, warum sich die Norm nur auf „soziale Netzwerke“ im Sinne des § 1 Abs. 4 GgdG-E erstrecken soll. Auch wenn die Legaldefinition des GgdG-E weiter gefasst ist als die des NetzDG, könnten hier Abgrenzungsschwierigkeiten entstehen. Unklar ist z. B. ob pornografische Plattformen hierunter fallen.

# 3. Strafrecht als notwendiger Bestandteil des Schutzes vor digitaler Gewalt

HateAid begrüßt ausdrücklich das Vorhaben des Gesetzgebers Schutzlücken im Bereich der bildbasierten digitalen Gewalt zu schließen. Dies gilt insbesondere für nicht-einvernehmliche sexualisierte Deepfakes, deren Erstellung und Verbreitung erhebliche Folgen für Betroffene haben können.

Sexualisierte Deepfakes haben sich im Zuge frei verfügbarer KI-Bildgeneratoren und sogenannter „Nudification"-Angebote zu einer allgegenwärtigen Erscheinungsform digitaler Gewalt entwickelt. Sie sind so auch zu einem dauerhaften Bedrohungsszenario für Nutzende geworden, die stets befürchten müssen, hiervon betroffen zu sein. Betroffen sind dabei insbesondere Frauen und Mädchen. Technische Fachkenntnisse sind zur Erstellung von sexualisierten Bild- und sogar Videoinhalten nicht mehr erforderlich. Mit der Integration entsprechender Funktionen in KI-Systeme wie den Chatbot „Grok" auf der Plattform X hat die gesellschaftliche Normalisierung geschlechtsspezifischer digitaler Gewalt eine neue Dimension erreicht. Analysen[1] zufolge wurden allein im Januar 2026 innerhalb von elf Tagen rund drei Millionen sexualisierte Deepfakes erstellt und verbreitet. Darunter befanden sich mindestens 23.000 Darstellungen von Kindern. Die Erstellung und Verbreitung solcher Inhalte sind bislang nur lückenhaft strafrechtlich erfasst. Angesichts dessen ist es nicht verwunderlich, dass es in der Bevölkerung kaum ein Unrechtsbewusstsein bei der Erstellung sexualisierter Deepfakes gibt. Dies wird nach wie vor meist als harmloser Spaß abgetan.

Aktuell werden Fälle bildbasierter digitaler Gewalt vor allem durch den § 33 Kunsturhebergesetz (KUG), eine Norm des Nebenstrafrechts, erfasst. Diese unterscheidet nicht zwischen der unberechtigten Verbreitung von vollständig bekleideten Personen und der Verbreitung von gestohlenen oder manipulierten Nacktfotos. Zugleich ist die Norm als absolutes Antragsdelikt und als Privatklagedelikt ausgestaltet. Die verlangt Betroffenen daher ab, für jeden einzelnen Fall binnen drei Monaten einen Strafantrag zu stellen. Und selbst wenn sie dem nachkommen, werden Ermittlungsverfahren in der Regel reflexartig unter Verweis auf den Privatklagewegwegen mangelnden öffentlichen Interesses per Beschluss eingestellt. Dieser Beschluss ist für die Betroffenen nicht anfechtbar. Gleichzeitig hat der kostenpflichtige Privatklageweg keine praktische Bedeutung und wird selbst von Anwält*innen mangels Erfolgsaussichten nicht empfohlen.

Die Erstellung von sexualisierten Deepfakes ist aktuell strafrechtlich nicht relevant. Dies gilt selbst, wenn entsprechendes Bildmaterial massenhaft auf einem digitalen Endgerät oder gar in einer Cloud gespeichert wird. Dies ist wohl der Regelfall bei der Nutzung von Nudification-Tools, die frei verfügbar und kostenlos in App-Stores und als Browseranwendung im Internet nutzbar sind. Ihre Verwendung erfordert keinen technischen Sachverstand. Einmal erstellt sind sie nur einen falschen Mausklick, ein Datenleck in der Cloud, einen Hackingangriff oder eine unsachgemäße Entsorgung der Geräte von einer Veröffentlichung entfernt. Solange dies straffrei möglich ist, müssen alle Menschen-insbesondere jedoch Frauen und weiblich gelesene Personen, stets mit dem Kontrollverlust und der Angst davor leben selbst davon betroffen zu sein.

[1] https://counterhate.com/research/grok-floods-x-with-sexualized-images/ , sowie https://www.nytimes.com/2026/01/22/technology/grok-x-ai-elon-musk-deepfakes.html [letzter Zugriff 20.05.2026].

Der gesetzgeberische Handlungsbedarf wird auch durch die gesellschaftliche Erwartung wirksamer Schutzmechanismen bestätigt. Eine repräsentative Civey-Umfrage[2] im Auftrag von HateAid zeigt, dass 79,4 % der Befragten die strafrechtliche Sanktionierung der Erstellung und Verbreitung sexualisierter KI-generierter Inhalte ohne Einwilligung befürworten. 88,7 % sprechen sich zudem für ein Verbot der Monetarisierung entsprechender Inhalte durch Plattformen und Anbieter aus.

## 3.1. Wirkung über die Bestrafung von Tatpersonen hinaus

Die Bedeutung strafrechtlicher Regelungen erschöpft sich nicht in der Sanktionierung einzelner Taten. Strafrechtliche Verbote entfalten zugleich präventive, regulative und gesellschaftliche Wirkungen über das eigentliche Strafverfahren hinaus. So haben zwei der weltweit größten Deepfake-Pornografie-Webseiten nach Ankündigung entsprechender Gesetzesvorhaben im Vereinigten Königreich den Zugriff aus diesem Staat blockiert.[3]

Eine strafrechtliche Regulierung schafft wichtige Anreize für „Safety by Design“[4]-Ansätze bei Plattformen und KI-Anbietern. Diesen ist es durch eine strafrechtliche Regelung schlicht unterwegs ein vollends rechtswidriges Geschäftsmodell anzubieten, welches allein auf das Entkleiden von Frauen gerichtet ist und das Einverständnis der abgebildeten Personen nicht sicherstellt. Hierzu zählen insbesondere technische Schutzmechanismen, die die Erstellung oder Verbreitung sexualisierter Inhalte von dem Nachweis einer Einwilligung der betroffenen Person abhängig machen. Dies ist aus präventiver Sicht von erheblicher Bedeutung. Denn einmal erstellte und verbreitete Inhalte können regelmäßig nicht mehr vollständig aus dem digitalen Raum entfernt werden.

Die strafrechtliche Erfassung ist zudem für die effektive Durchsetzung unionsrechtlicher Schutzmechanismen von zentraler Bedeutung. Rechtswidrige Inhalte im Sinne des Art. 16 DSA bestimmen sich maßgeblich nach nationalem Recht. Eine klare strafrechtliche Normierung schwerwiegender persönlichkeitsrechtsverletzender Inhalte erleichtert daher die Meldung und Entfernung entsprechender Inhalte auf Plattformen. Damit wird der Schutz Betroffener digitaler Gewalt ebenfalls gestärkt.

[2] https://hateaid.org/geschaeft-mit-nicht-einvernehmlichen-sexualisierten-deepfakes-verbieten/ [letzter Zugriff 20.05.2026].

[3] https://www.wired.com/story/the-biggest-deepfake-porn-website-is-now-blocked-in-the-uk/ [letzter Zugriff 20.05.2026].

[4] https://hateaid.org/wp-content/uploads/2026/04/safety-by-design-bericht-wege-zu-sichereren-sozialen-netzwerken-hateaid.pdf?pid=124971

## 3.2. Einführung eines neuen § 184k StGB

## a) Zusammenfassung der zentralen Forderungen von HateAid

Die Anpassungen des § 184k StGB sind ein wichtiger und lang überfälliger Schritt, um Schutzlücken im Bereich der bildbasierten sexualisierten Gewalt zu schließen. Bei dem Entwurf bestehen jedoch aus Sicht von HateAid noch zentrale Defizite in der konkreten Ausgestaltung:

- HateAid begrüßt ausdrücklich die explizite strafrechtliche Erfassung einiger Formen sexualisierter Deepfakes als Tatbestand im Sexualstrafrecht. Dieser ist geeignet den schweren Eingriff in das Recht auf sexuelle Selbstbestimmung Rechnung zu tragen.
- Besonders ist die geplante Einführung der Strafbarkeit der Erstellung bestimmter Formen sexualisierter Deepfakes zu begrüßen.
- Zu begrüßen ist ferner die Einordnung als relatives Antragsdelikt, die künftig eine Strafverfolgung bei besonderem öffentlichem Interesse auch ohne einen Strafantrag ermöglicht.
- Eine Ausgestaltung als Privatklagedelikt ist hingegen strikt abzulehnen, da sie die praktische Relevanz der Norm bereits vor Inkrafttreten der Norm zu untergraben droht.
- Zentraler Änderungsbedarf besteht beim Wortlaut des § 184k Abs. 1 Nr. 4 StGB-E
    - Alle unbefugten sexualisierten Deepfakes, insbesondere entkleidende Darstellungen (Unterwäsche- oder Bikinibilder), müssen im Sexualstrafrecht erfasst werden.
    - Ferner ist der im Entwurf enthaltene „Anschein“-Zusatz zu streichen, da er missverständlich ist und den Anwendungsbereich unzutreffend verengen könnte. Schlecht gemachte oder gekennzeichnete unbefugte sexualisierte Deepfakes dürfen nicht versehentlich aus dem Anwendungsbereich fallen.
    - Schließlich sollten die Tathandlungen der Erstellung und des Zugänglichmachens an Dritte ausdrücklich im Tatbestand des § 184k Abs. 1 Nr. 4 StGB-E genannt werden. Zudem sollte in Erwägung gezogen werden die Tatmodalität des Gebrauchs in § 184k Abs. 1 Nr. 1, 2, 4 StGB-E mit aufzunehmen.
    - Der Tatbestand des § 184k Abs. 1 Nr. 4 StGB-E sollte zudem nicht auf Bildaufnahmen beschränkt bleiben, sondern auf alle Inhalte im Sinne des § 11 Abs. 3 StGB erstreckt werden, um medienübergreifende Schutzlücken zu vermeiden.
- Positiv zu bewerten ist der Schutz anderer berechtigter Interessen, wie der Kunst, der Wissenschaft, der Forschung, Lehre oder Berichterstattung über Vorgänge des Zeitgeschehens

Folgender Wortlaut wird für einen Absatz 2, der sexualisierte Deepfakes regelt, vorgeschlagen:

*Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer unbefugt einen Inhalt (§ 11 Abs. 3 StGB) mittels eines Computerprogrammes erstellt, der eine andere Person sexualbezogen[5] wiedergibt, insbesondere indem die andere Person bei Vornahme sexueller Handlungen, mit unbekleideten Genitalien, unbekleidetem Gesäß oder unbekleideter weiblicher Brust oder sonst überwiegend nackt dargestellt wird. Ebenso wird bestraft, wer einen durch eine Tat nach Satz 1 hergestellten Inhalt unbefugt besitzt oder einen Inhalt, der in Satz 1 bezeichneten Art unbefugt einer dritten Person zugänglich macht.*

## b) Effektive Rechtsdurchsetzung gewährleisten: kein Verweis auf Privatklageweg und relatives Antragsdelikt

HateAid empfiehlt dringend, die Norm nicht als Privatklagedelikt auszugestalten. Dies droht die praktische Relevanz der Norm zu untergraben. Bereits der § 33 KUG ist ein Privatklagedelikt. Dies hat zur Folge, dass selbst dann, wenn es um die massenhafte Verbreitung sexualisierter Deepfakes im Internet geht, Strafverfolgung so gut wie nie stattfindet. Stattdessen werden Strafverfahren nahezu reflexhaft unter grober Missachtung der Nr. 86 und 87 RiStBV unter Verweis auf den Privatklageweg eingestellt. Diese Entscheidung ist für Betroffene nicht anfechtbar.

KI-Bildgeneratoren werden systematisch und millionenfach zur unbefugten sexualisierten Darstellung, insbesondere von Mädchen und Frauen, genutzt. Dies stellt eine Störung des Rechtsfriedens über den Lebenskreis der jeweiligen betroffenen Person hinaus dar. Jede andere Betrachtungsweise wäre lebensfremd. Es sind keine Einzelfälle. Es handelt sich um ein frauenverachtendes und damit menschenverachtendes Massenphänomen der digitalen Zeit.[6] Der Verweis auf den Privatklageweg wäre damit – selbst, wenn er gesetzlich angelegt wäre – nach Nr. 86 RiStBV nicht zulässig.

Dennoch stellt der Verweis auf den Privatklageverfahren faktisch eine weitere Einstellungsmöglichkeit für überlastete Strafverfolgungsbehörden dar.[7] Der Gesetzgeber muss dem zuvorkommen und das Risiko eines reflexhaften Verweises auf den Privatklageweg vorausschauend vorbeugen. Stattdessen braucht es ausreichende Ressourcen für Strafverfolgungsbehörden, um die Ermittlungen in Fällen bildbasierter digitaler Gewalt aufzunehmen.

Die Einordnung als relatives Antragsdelikt ist hingegen ein wichtiger und sachgerechter Schritt. Bisher mussten Betroffene von bildbasierter sexualisierter Gewalt beispielsweise im Rahmen des §§ 33, 22, 23 KUG für jeden einzelnen Inhalt einen gesonderten Strafantrag stellen. Dies galt selbst dann, wenn es sich um eine

[5] Neben dem Begriff sexualbezogen, den das Strafrecht bereits kennt, kommen die Begriffe sexualisiert oder sexualisierend in Betracht. Letzterer hebt die Objektifizierung der wiedergegebenen Person stärker und sachgerecht hervor.

[6] Studien zufolge sind 98 % aller online Deepfake Inhalte pornographische Inhalte. Davon sind zu 99 % Frauen betroffen. https://www.securityhero.io/state-of-deepfakes/#key-findings [letzter Zugriff 20.05.2026]. Siehe auch: https://www.thedeepfake.report/en/09-digital-rape-en [letzter Zugriff 20.05.2026]

[7] Löwe/Rosenberg/Wenske Vor § 374 Rn. 4.

Vielzahl von Inhalten auf verschiedenen Plattformen handelte oder diese über Jahre wiederholt verbreitet wurden.

Die praktische Bedeutung dieser Entlastung wird durch empirische Befunde unterstrichen: Eine repräsentative Studie[8] des Bundeskriminalamts, des Bundesministeriums für Familie, Senioren, Frauen und Jugend sowie des Bundesministeriums des Innern zeigt, dass digitale Gewalt insgesamt nur äußerst selten angezeigt wird. Die Anzeigequote liegt bei Frauen bei lediglich 2,4 % und bei Männern sogar nur bei 0,9 %. Vor diesem Hintergrund ist eine niedrigschwellige Ausgestaltung als relatives Antragsdelikt praktisch bedeutsam und geeignet das Dunkelfeld zu erhellen. Dies gilt insbesondere bei bildbasierter sexualisierter Gewalt. Die Erfahrung von HateAid zeigt, dass nicht nur die psychische Belastung hierbei besonders hoch ist, sondern auch die Scham Betroffene davon abhält den Kontakt zu den Behörden zu suchen.

### c) Schutz vor unbefugten sexualisierter Deepfakes

Der Gesetzgeber verspricht: „§ 184k StGB soll künftig alle Formen des unbefugten nicht-einvernehmlichen Herstellens und Verbreitens intimen Bildmaterials („bildbasierte sexualisierte Gewalt“) erfassen”.[9] Diesem Versprechen wird er in der derzeitigen Fassung jedenfalls hinsichtlich sexualisierter Deepfakes nicht gerecht.

## Systematische Erfassung unbefugter sexualisierter Deepfakes einschließlich entkleideter Darstellungen

Nach der aktuell geplanten Ausgestaltung des § 184k Abs. 1 Nr. 4 StGB-E braucht es für die Strafbarkeit die Sichtbarkeit von sexuellen Handlungen, der unbekleideten Genitalien, des unbekleideten Gesäßes oder der unbekleideten weiblichen Brust. Das bedeutet: Bilder und Videos, die eine Person stehend in Unterwäsche oder einem Bikini zeigen, sind nicht erfasst. Dies ist nicht nachvollziehbar. Denn das digitale, nicht-einvernehmliche „Entkleiden“ von Personen stellt bereits für sich genommen einen eigenständigen und schwerwiegenden Eingriff in das Recht auf sexuelle Selbstbestimmung dar. Eine repräsentative Civey-Umfrage[10] im Auftrag von HateAid belegt insoweit, dass 77,8 % der Befragten auch die strafrechtliche Erfassung solcher Inhalte befürworten.

Die Verbreitung von Darstellungen von Personen in Unterwäsche oder Bikini wäre in bestimmten Fällen lediglich von § 201b StGB-E und somit außerhalb des Sexualstrafrechts erfasst. Die Herstellung derartiger Inhalte wäre straflos. Darüber hinaus bräuchte es eine Täuschungskomponente und die Geeignetheit zur erheblichen Ansehensschädigung, was unter Umständen von den Gerichten dann verneint wird, wenn die Darstellung nach allgemeinem Verständnis als “attraktiv(er)” gilt. Dies verschiebt den Schutzfokus

[8] https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/Forschungsergebnisse/260210_LeSuBiA_Ergebnisse_I.html?nn=261272 [letzter Zugriff 20.05.2026].

[9] Anschreiben des BMJV zur Verbändeanhörung.

[10] https://hateaid.org/geschaeft-mit-nicht-einvernehmlichen-sexualisierten-deepfakes-verbieten/.

unzulässig vom Schutz des Rechts auf sexuelle Selbstbestimmung hin in Richtung eines rufschutzorientierten Ansatzes. Zudem führt es (erneut) zu erheblicher Rechtsunsicherheit bei Betroffenen. Viele Fälle, in denen Menschen von sexualisierten Deepfakes betroffen sind, blieben straflos.

Ferner schreibt eine solche dogmatische Anknüpfung faktisch das Narrativ fort, der (teil-)entblößte Körper – insbesondere von Frauen – sei bereits für sich genommen ansehensschädigend. Dies würde den Schutzzweck verfehlen, der nicht in der Bewertung des Körpers, sondern in der Wahrung der autonomen Entscheidung über dessen Darstellung liegt. Eine sexualisierte Darstellung ohne Einwilligung ist daher unabhängig von etwaigen reputationsbezogenen Erwägungen als eigenständiger Eingriff zu erfassen.

Auch kriminalpolitisch spricht vieles für eine klare Einbeziehung entsprechender Inhalte. Andernfalls wird insbesondere das Geschäftsmodell sogenannter „Nudifying"-Anwendungen weiter legitimiert. Vergleichbare Normen in anderen Rechtsordnungen, etwa in England und Irland, stellen demgegenüber zutreffend auf den weiter gefassten Begriff der intimen Inhalte ab, der den Schutzbereich nicht auf Nacktheit bestimmter Körperteile oder sexuelle Handlungen beschränkt.[11]

## Irreführender „Anschein"-Zusatz im Tatbestand

Der im Entwurf verwendete Zusatz, wonach die Bildaufnahme einen „Anschein erwecken" muss, sollte gestrichen werden. Diese Formulierung könnte dazu führen, dass Inhalte die nicht "echt genug" aussehen, aus dem Anwendungsbereich der Norm fallen. Dies könnte u. a. damit begründet werden, dass die Qualität der Fälschung mangelhaft sei oder ein Inhalt als KI-generiert gekennzeichnet ist und somit kein realistisches Geschehen vorgetäuscht wird.

Dies überzeugt weder systematisch noch teleologisch. Der Schutz der sexuellen Selbstbestimmung knüpft nicht an den Täuschungserfolg eines Inhalts an, sondern an die unbefugte sexualisierte Darstellung der betroffenen Person. Eine Differenzierung nach der „Glaubwürdigkeit" eines sexualisierten Deepfakes ist für den Unrechtsgehalt nicht maßgeblich.

Vor diesem Hintergrund erscheint die Formulierung nicht ausreichend klar und sollte gesetzgeberisch präzisiert werden. Anders als etwa § 201b StGB-E, der auf den Anschein eines tatsächlichen Geschehens abstellt, verfolgt § 184k StGB-E keinen täuschungsbezogenen Ansatz. Dies sollte im Wortlaut eindeutig zum Ausdruck kommen, um Auslegungsspielräume und Abgrenzungsprobleme zu vermeiden.

## Tathandlungen: Erstellung, Gebrauch und Zugänglichmachen an Dritte

HateAid empfiehlt dringend in § 184k Abs. 1 Nr. 4 StGB-E nicht lediglich auf das computertechnische Verändern, sondern auf das computertechnische Erstellen und das Zugänglichmachen an Dritte abzustellen.

[11] Siehe dazu die Begründung des Referentenentwurfs, S. 24 f.

HateAid empfiehlt außerdem in Erwägung zu ziehen auch den Gebrauch mit in § 184k Abs. 1 Nr. 1, 2 und 4 StGB-E aufzunehmen.

Die Anknüpfung an „Verändern, Umgestalten oder Verbinden“ mittels Computerprogramms setzt denklogisch ein konkretes Ausgangsmaterial voraus und führt damit zu praktischen Abgrenzungs- und Beweisproblemen. Diese Grundannahme verfehlt zudem die technische Entwicklung: Moderne KI-Systeme sind bereits heute in der Lage, sexualisierte Deepfakes allein auf Prompt Basis (also lediglich durch Texteingabe ohne konkrete Vorlage) zu generieren. Eine derartige Beschränkung würde daher zu erneuten Schutzlücken führen, da die Normanforderungen jedenfalls bei Personen des öffentlichen Lebens unterlaufen werden können. Systematisch sachgerechter wäre eine Anknüpfung an computertechnisch erstellte Inhalte, wie es auch § 201b StGB-E vorsieht.

Die Erfassung der Herstellung als solche ist demgegenüber zu begrüßen und zwingend erforderlich. Bereits die Generierung eines sexualisierten Deepfakes stellt einen eigenständigen Eingriff in die Intimsphäre sowie in die Dispositionsbefugnis über das eigene Bild dar. Bereits die Herstellung begründet ein erhebliches Risiko irreversibler Weiterverbreitung und des Kontrollverlusts.

Defizitär erscheint jedoch, dass nicht auch der Gebrauch derartiger Inhalte nicht explizit vom Tatbestand erfasst sein soll. Die Entscheidung über Existenz und Verbreitung solcher Inhalte sollte allein der betroffenen Person vorbehalten sein. Auch die bestehende Systematik des Strafrechts spricht für eine solche kohärente Ausgestaltung (u. a. § 184k Abs. 1 Nr. 2 StGB, § 201a Abs. 1 Nr. 4 StGB, § 184b Abs. 3 StGB, § 184c Abs. 1 Nr. 2 StGB sowie § 201 Abs. 1 Nr. 2 StGB stellen ebenfalls auf Gebrauch / Besitz[12] ab). Dabei sollte hinsichtlich der Tathandlung des Gebrauchens auf den unbefugten Gebrauch von unbefugt hergestellten Inhalten abgestellt werden. So könnte eine ausufernde Regelung im Hinblick auf einvernehmlich hergestellte oder überlassene Inhalte vermieden werden. Hinsichtlich des unbefugten Zugänglichmachens ist es hingegen nicht relevant, ob die Inhalte ohne Befugnis hergestellt wurden.

## Anknüpfung an Inhalte im Sinne des § 11 Abs. 3 StGB

Der Anwendungsbereich des § 184k Abs. 1 Nr. 4 StGB-E sollte nicht auf Bildaufnahmen beschränkt bleiben, sondern systematisch auf „Inhalte“ im Sinne des § 11 Abs. 3 StGB erstreckt werden. Diese erfassen sowohl Bild- als auch Toninhalte.

Bereits das geltende Strafrecht zeigt, dass nicht-visuelle Inhalte eigenständig erfasst werden können, etwa in § 201 StGB. Potenziell uneinheitliche Auslegungen des gleichen Tatbestandsmerkmales sollten vermieden werden. Auch der § 201b StG-E stellt korrekterweise auf Inhalte ab. Der strafrechtliche Schutz der Intimsphäre sollte daher ebenfalls nicht mediengebunden sein.

[12] Die im Gesetz verschiedentlich verwendeten Tathandlungen des Besitzens und Gebrauchens sind dogmatisch nicht deckungsgleich, aber setzen in der Praxis nahezu die gleichen tatsächlichen Handlungen voraus.

## Besonders schwere Fälle

Sofern für die Ausgestaltung des § 184k StGB-E Strafzumessungsregelungen in Erwägung gezogen werden, sollten folgende vier Konstellationen berücksichtigt werden: Doxxing (das Veröffentlichen von personenbezogenen Daten zusammen mit dem sexualisierten Inhalt), Abhängigkeitsverhältnisse (wie Beratungs-, Behandlungs- oder Betreuungsverhältnis oder das Ausnutzen einer Amtsstellung), digitale Darstellungen von analogen Gewalttaten (insbesondere Vergewaltigungen) sowie Inhalte über Minderjährige. In der Beratung von HateAid melden sich regelmäßig Menschen, die nicht nur von der unbefugten Veröffentlichung intimen Bildmaterials belastet sind, sondern auch von der Tatsache, dass weitere Informationen, wie ihr Wohnort oder ihr Name, mit veröffentlicht werden. Das erhöht das Risiko der betroffenen Person substanziell weitere digitale und analoge Gewalt zu erfahren.

### d) Klausel für die Wahrnehmung berechtigter Interessen

HateAid begrüßt, dass der Schutz der Wahrnehmung berechtigter Interessen als Ausnahmeregelung im jetzigen § 184k Abs. 3 StGB weiterhin erhalten bleiben soll. Dadurch bleiben insbesondere Kunst, Wissenschaft, Forschung, Lehre, Berichterstattung sowie die Darstellung von Vorgängen des Zeitgeschehens weiterhin privilegiert. Dies ist im Hinblick auf die Meinungs-, Presse- und Kunstfreiheit von erheblicher Bedeutung und verhindert eine unangemessen weite Kriminalisierung.

### e) Im Übrigen zu § 184k Abs. 1 StGB-E

Die materiellrechtliche Ausgestaltung des § 184k StGB-E ist grundsätzlich geeignet, den Schutz der sexuellen Selbstbestimmung im digitalen Raum zu stärken. Der Ansatz, das Recht auf sexuelle Selbstbestimmung im Sexualstrafrecht unabhängig von bestimmten Schutzräumen[13] umfassender zu stärken, ist zu begrüßen.

Es ist jedoch nicht nachvollziehbar, dass ein auslegungsbedürftiger und subjektiv geprägter Begriff wie in „sexuell bestimmter Weise“ wie in § 184 Abs. 1 Nr. 3 StGB-E verwendet wird. Die Formulierung, die wohl vor allem vor sexualisierten Bildaufnahmen im öffentlichen Raum schützen soll, birgt erhebliche Abgrenzungsprobleme. Sie droht eine ausufernde Strafbarkeit von Bildaufnahmen im öffentlichen Raum zu begründen oder – bei restriktiver Auslegung – gar keine Relevanz zu haben. Die Formulierung „in sexuell bestimmter Weise“ birgt erhebliche Abgrenzungsschwierigkeiten und liegt – im wahrsten Sinne – im Auge des Betrachters. Es ist gleichzeitig nicht nachvollziehbar, wieso eine möglicherweise als sexualisiert wahrgenommene Bildaufnahme eines bekleideten Gesäßes im öffentlichen Raum im Sexualstrafrecht geregelt werden soll, ein KI-generiertes Bild in Reizwäsche hingegen nicht. Um eine dem Bestimmtheitsgebot

[13] § 201a StGB knüpft an räumliche und situative Schutzbereiche an.

entsprechende Strafnorm zu schaffen, die gleichzeitig den berechtigten Schutzinteressen vor voyeuristischen Aufnahmen Rechnung trägt, bedarf es dringend einer Nachschärfung.

## 3.3. Einführung eines neuen § 201b StGB

Der vorgeschlagene § 201b StGB-E ist grundsätzlich zu begrüßen. Der Tatbestand erscheint geeignet, erhebliche Ansehensschädigungen durch täuschende digitale Inhalte wirksam zu erfassen.
Positiv hervorzuheben ist, dass der Gesetzentwurf ein spezifisches Unrecht ausdrücklich normiert und präzisiert. Zwar geht die Gesetzesbegründung selbst davon aus, dass das Zugänglichmachen ansehensschädigender Deepfakes bereits heute teilweise durch bestehende Vorschriften – etwa § 187 StGB oder § 33 KUG – erfasst werden kann. Gleichwohl schafft der neue Tatbestand mehr Klarheit und Sichtbarkeit für die besondere Gefährdungslage, die von täuschend erzeugten oder veränderten digitalen Inhalten ausgeht. Dies kann auch zur besseren Rechtsdurchsetzung und zu einer stärkeren Sensibilisierung beitragen.
Ebenfalls positiv ist, dass die Ausnahme zur Wahrnehmung berechtigter Interessen aus § 201a Abs. 3 StGB übernommen wird. Dadurch bleiben insbesondere Kunst, Wissenschaft, Forschung, Lehre, Berichterstattung sowie die Darstellung von Vorgängen des Zeitgeschehens weiterhin privilegiert. Dies ist im Hinblick auf die Meinungs-, Presse- und Kunstfreiheit von erheblicher Bedeutung und verhindert eine unangemessen weite Kriminalisierung.

Zu begrüßen ist ferner die technologieneutrale Formulierung des Tatbestands. Der Entwurf vermeidet eine Beschränkung auf bestimmte technische Verfahren oder konkrete KI-Systeme und bleibt damit anpassungsfähig gegenüber zukünftigen technologischen Entwicklungen.

Positiv hervorzuheben ist außerdem, dass der Entwurf ausdrücklich eine Subsidiaritätsklausel enthält und damit keine Sperrwirkung gegenüber bestehenden Straftatbeständen entfaltet. Dies gilt insbesondere im Verhältnis zu § 187 StGB. Der neue Tatbestand tritt nicht an die Stelle bestehender Ehrschutzdelikte, sondern ergänzt diese dort, wo täuschend erzeugte oder manipulierte Inhalte ein eigenständiges Unrecht begründen. Dadurch wird vermieden, dass die Einführung des § 201b StGB-E als abschließende Sonderregelung verstanden wird, die die Anwendung allgemeiner Ehrschutzvorschriften einschränkt. Die gewählte Konstruktion trägt damit zu einem kohärenten Verhältnis zwischen bestehendem Persönlichkeits- und Ehrschutz und den neuen Herausforderungen bei.

Kritisch zu sehen ist jedoch die Formulierung in der Gesetzesbegründung, wonach der Inhalt „den Anschein erwecken [muss], ein tatsächliches Geschehen wiederzugeben“ und „amateurhafte Darstellungen, die für den durchschnittlichen Betrachter eindeutig als nicht reales Geschehen zu erkennen sind“, selbst bei täuschender Absicht nicht vom Tatbestand erfasst sein sollen. Diese Einschränkung überzeugt nicht. Auch schlecht gemachte oder als manipuliert erkennbare Deepfakes können für Betroffene erhebliche Persönlichkeitsverletzungen darstellen. In der Praxis könnte dies zu Schutzlücken führen: Ein erkennbar künstlich erzeugtes „Bikini-Fake“ etwa wäre möglicherweise weder von § 184k StGB-E in seiner derzeitig angedachten Form noch von § 201b StGB-E erfasst, obwohl die Belastung für die betroffene Person erheblich sein kann. Für die Intensität der Rufschädigung ist es aus Sicht der Betroffenen nicht zwingend

entscheidend, ob sämtliche Betrachter den Inhalt für authentisch halten. Dies sollte im weiteren Gesetzgebungsverfahren nochmals überprüft werden.

## 3.4. Einführung eines neuen § 202e StGB

Mit dem neuen Tatbestand des § 202e StGB-E sollen die Vorgaben des Artikel 6 der Richtlinie (EU) 2024/1385 zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt umgesetzt werden. Das deutsche Strafrecht wird insofern klargestellt und Rechtsanwender für das spezifische Unrecht sensibilisiert. Das ist zu begrüßen.