Bundesverband
Frauenberatungsstellen
und Frauennotrufe

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

Berlin | 22.05.2026

Ansprechpartnerin: Elizabeth Ávila González
Petersburger Straße 94, 10247 Berlin | T +49(0)30/32 29 95 00 | digitalegewalt@bv-bff.de | aktiv-gegen-digitale-gewalt.de

Bundesverband
Frauenberatungsstellen
und Frauennotrufe

Im bff: Bundesverband Frauenberatungsstellen und Frauennotrufe sind aktuell über 235 ambulante Fachberatungsstellen aus dem gesamten Bundesgebiet zusammengeschlossen. Diese unterstützen und beraten Frauen und Mädchen, die von sexualisierter, körperlicher, psychischer oder digitaler Gewalt betroffen sind. Digitale Gewalt ist dabei häufig eng mit Gewalt im sozialen Nahraum verbunden – insbesondere in (Ex-)Partnerschaften. Sie umfasst Formen wie Cyberstalking, digitale Überwachung, Bedrohung, sexualisierte Belästigung, die Verbreitung intimer Bilder ohne Zustimmung oder Identitätsmissbrauch im Netz. Täter nutzen digitale Technologien gezielt, um Kontrolle auszuüben und Betroffene einzuschüchtern. Das hat schwerwiegende Folgen für die Betroffenen – von sozialer Isolation bis hin zu langfristigen psychischen und wirtschaftlichen Belastungen. Die Fachberatungsstellen des bff bieten kostenfreie und auf Wunsch anonyme Beratung für Betroffene von digitaler Gewalt an. Sie helfen bei der psychosozialen Bewältigung der Gewalterfahrungen, beraten zu technischen Schutzmaßnahmen, unterstützen bei rechtlichen Schritten und begleiten Betroffene in Verfahren.
Der bff arbeitet seit 2017 mit der Projektreihe *aktiv gegen digitale Gewalt* an der Bekämpfung digitaler geschlechtsspezifischer Gewalt.

Der Bundesverband Frauenberatungsstellen und Frauennotrufe (bff) begrüßt den Gesetzesentwurf als wichtigen und längst überfälligen Schritt zur Anerkennung digitaler Gewalt als eigenständiges Unrecht. Die ausdrückliche strafrechtliche Erfassung neuer Gewaltformen wie bildbasierter sexualisierter Gewalt und digitaler Überwachung ist ein notwendiger Fortschritt.

Gleichzeitig steht der Gesetzgeber in der Verantwortung, die Vorgaben der EU-Richtlinie 2024/1385 zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt vollständig und wirksam umzusetzen. Diese verpflichtet die Mitgliedstaaten, auch digitale Gewaltformen wie Cyberstalking, nicht-einvernehmliche Verbreitung oder Herstellung intimer Inhalte, Cybermobbing und weiteren Formen von digitaler Gewalt umfassend zu erfassen und effektive Schutzmechanismen bereitzustellen.

Aus Sicht der Beratungspraxis wird deutlich: Der vorliegende Entwurf wird den tatsächlichen Bedarfen der Betroffenen nicht gerecht und bildet zentrale und aufkommende Gewaltrealitäten nur unzureichend ab. Der Referentenentwurf benennt zwar verschiedene Erscheinungsformen digitaler Gewalt in seiner Begründung, führt jedoch zahlreiche dieser Gewaltformen nicht ausdrücklich im Gesetzestext selbst auf oder erfasst sie nur unvollständig. Es handelt sich daher nicht um ein umfassendes Gesetz gegen digitale Gewalt, sondern vor allem um eine punktuelle Schließung einzelner Schutzlücken. Für Betroffene bedeutet dies, dass auch weiterhin erhebliche Schutzlücken bestehen bleiben – obwohl die EU-Richtlinie 2024/1385 einen deutlich umfassenderen Schutz vor geschlechtsspezifischer (digitaler) Gewalt vorsieht. Dies wiegt umso schwerer vor dem Hintergrund der unionsrechtlichen Vorgaben: Bis zum Ablauf der Umsetzungsfrist der Richtlinie verbleiben nur noch rund dreizehn Monate, in denen die übrigen Verpflichtungen umgesetzt werden müssten. Hierzu zählen insbesondere der Ausbau spezialisierter Hilfsangebote für Betroffene, umfassende Fortbildungsmaßnahmen für Polizei, Staatsanwaltschaft und Justiz, präventive Maßnahmen einschließlich der Förderung digitaler Kompetenzen sowie systematische Erhebung disaggregierter Daten.

Ansprechpartnerin: Elizabeth Ávila González
Petersburger Straße 94, 10247 Berlin | T +49(0)30/32 29 95 00 | digitalegewalt@bv-bff.de | aktiv-gegen-digitale-gewalt.de

Zugleich zeigt die Praxis, dass strafrechtliche Regulierung allein nicht ausreicht. Viele Betroffene erleben erhebliche Hürden im Zugang zu Recht. Studien zeigen, dass nur ein sehr geringer Anteil digitaler Gewalt tatsächlich zur Anzeige gebracht wird (ca. 2,4%).[1] Gründe hierfür sind unter anderem fehlendes Vertrauen in die Wirksamkeit staatlicher Maßnahmen, hohe Belastungen durch Verfahren, mangelnde Unterstützung sowie die Sorge vor weiterer Eskalation. Strafrechtliche Normen entfalten daher in vielen Fällen keine tatsächliche Schutzwirkung für Betroffene.

Der Schutz vor digitaler Gewalt erfordert daher eine umfassende Gesamtstrategie. Diese muss insbesondere beinhalten:

- Präventive Maßnahmen und gesellschaftliche Sensibilisierung
- Ein nachhaltiger Aufbau und Absicherung spezialisierten Beratungsstrukturen
- Sowie effektive Maßnahmen zur schnellen Entfernung rechtswidriger Inhalte

Gerade letzteres ist für Betroffene oft entscheidend. Der bff hat in seinem Policy Paper zum DSA unter dem Titel „Plattformregulierung muss Gewaltschutz priorisieren“[2] aufgezeigt, dass Plattformen ihrer Verantwortung bislang vielfach nicht gerecht werden. Meldeverfahren sind komplex, intransparent und für Betroffene häufig nicht zugänglich. Inhalte werden oft zu spät oder gar nicht entfernt. Ein wirksamer Gewaltschutz muss daher Strafrecht und Plattformregulierung konsequent zusammendenken.

Dabei darf die Verantwortung von Schutz vor digitaler Gewalt nicht allein auf die europäische Ebene verlagert werden. Zwar schafft der Digital Services Act einen unionsrechtlichen Rahmen, die praktische Umsetzung und Durchsetzung liegt jedoch wesentlich auch bei den Mitgliedstaaten. Deutschland verfügt über erhebliche Einfluss- und Gestaltungsmöglichkeiten, etwa bei der Ausgestaltung nationaler Verfahren, der Benennung und Ausstattung zuständiger Behörden, der gerichtlichen Durchsetzung von Betroffenenrechten sowie der Kontrolle von Plattformen.

Aus Sicht des bff besteht die Gefahr, dass bestehende Handlungsspielräume auf europäische Regulierungsprozesse verschoben werden. Effektiver Gewaltschutz erfordert jedoch auch auf nationaler Ebene klare Zuständigkeiten, wirksame Durchsetzung und eine konsequente Priorisierung der Rechte von Betroffenen.

Die vorliegende Stellungnahme nimmt vor diesem Hintergrund eine integrierte Bewertung des Gesetzesentwurf vor. Zunächst werden die zivilrechtlichen Regelungen analysiert, da diese für Betroffene häufig den unmittelbarsten Zugang zu Schutz bieten. Anschließend erfolgt eine Bewertung der strafrechtlichen Vorschriften, insbesondere auf ihre praktische Umsetzbarkeit und ihre Vereinbarkeit mit den Vorgaben der

[1] Ergebnisse der Dunkelfeldstudie „Lebenssituation, Sicherheit und Belastung im Alltag (LeSuBiA), s. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/Forschungsergebnisse/260210_LeSuBiA_Ergebnisse_I.html?nn=261272

[2] Bundesverband der Frauenberatungsstellen und Frauennotrufe, „Plattformregulierung muss Gewaltschutz priorisieren“, s. https://www.frauen-gegen-gewalt.de/de/studien-und-positionspapiere/policy-paper-zum-digital-services-act-und-digitaler-geschlechtsspezifischer-gewalt-2026.html

Ansprechpartnerin: Elizabeth Ávila González
Petersburger Straße 94, 10247 Berlin | T +49(0)30/32 29 95 00 | digitalegewalt@bv-bff.de | aktiv-gegen-digitale-gewalt.de

EU-Richtlinie 2024/1385. Abschließend wird der Entwurf in den europarechtlichen Kontext eingeordnet, insbesondere im Zusammenspiel mit dem Digital Services Act (DSA) sowie der KI-Verordnung (AI Act).

## I. Querschnittsproblem: Fehlende Sensibilisierung und Spezialisierung

Die praktische Wirksamkeit gesetzlicher Regelungen gegen digitale Gewalt hängt maßgeblich davon ab, ob Polizei, Staatsanwaltschaften, Gerichte und zuständige Behörden über ausreichende Kenntnisse zu digitalen Gewaltformen, ihren technischen Erscheinungsformen sowie ihren geschlechtsspezifischen Dynamiken verfügen. Die Beratungspraxis zeigt jedoch, dass digitale Gewalt häufig nicht als zusammenhängendes Gewaltgeschehen erkannt oder in ihrer Schwere unterschätzt wird, insbesondre im Kontext von Gewalt im sozialen Nahraum.

Zugleich erfordern viele Erscheinungsformen digitaler Gewalt spezifisches technisches Wissen, etwa zu Spyware, Plattformmechanismen, KI-generierten Inhalten, Smart-Home-Technologien oder digitaler Überwachung. Ohne entsprechende Spezialisierung besteht die Gefahr, dass bestehende und neue Schutzinstrumente in der Praxis nur eingeschränkt wirksam sind.

Die EU-Richtlinie 2024/1385 hebt die Bedeutung spezialisierter Schulungen ausdrücklich hervor. Aus Sicht des bff braucht es daher flächendeckende und verpflichtende Fortbildungsmaßnahmen für Polizei, Staatsanwaltschaften, Richter*innen und weitere zuständige Stellen. Dies umfasst insbesondere Kenntnisse zu:

- Digitaler Gewalt im sozialen Nahraum
- geschlechtsspezifische Gewaltverhältnisse
- technische Überwachungs- und Manipulationsmöglichkeiten,
- Auswirkungen digitaler Gewalt auf Betroffene,
- Sowie intersektionalen Betroffenheiten.

Darüber hinaus sollte geprüft werden, spezialisierte Zuständigkeiten und Schwerpunkte für digitale Gewalt flächendeckend auszubauen.

## II. Zur Änderung des Zivilrechts

Zivilrechtliche Instrumente sind für Betroffene digitaler Gewalt von zentraler Bedeutung. Während strafrechtliche Verfahren häufig langwierig sind und hohe Hürden aufweisen, bieten zivilrechtliche Ansprüche die Möglichkeit, schnell auf fortdauernde Gewalt zu reagieren – insbesondere durch die Entfernung von Inhalten, die Unterbindung weiterer Übergriffe und die Inanspruchnahme der verantwortlichen Personen oder Plattformen.

Aus Sicht der Beratungspraxis zeigt sich jedoch, dass Betroffene bislang vielfach keinen effektiven Zugang zu zivilrechtlichem Schutz haben. Verfahren sind komplex, kostenintensiv und setzen voraus, dass

Ansprechpartnerin: Elizabeth Ávila González
Petersburger Straße 94, 10247 Berlin | T +49(0)30/32 29 95 00 | digitalegewalt@bv-bff.de | aktiv-gegen-digitale-gewalt.de

betroffene Inhalte selbst dokumentieren und Beweise sichern. Dies führt vielfach dazu, dass Betroffene sich wiederholt mit retraumatisierenden Inhalten auseinandersetzen, was erheblich belastend wirken kann.

### 1. *Verknüpfung mit anlassloser Speicherung von IP-Adressen und Portnummern für 3 Monate*

Die geplante Verknüpfung zivilrechtlicher Auskunftsansprüche mit einer anlasslosen Speicherung von IP-Adressen und Portnummern für einen Zeitraum von drei Monaten (s. Gesetz zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse im Strafverfahren[3]) wird aus Sicht des bff kritisch bewertet.

Zwar verfolgt die Maßnahme das legitime Ziel, die Identifizierung von Tätern zu erleichtern. In der Praxis bestehen jedoch erhebliche Zweifel an ihrer Wirksamkeit. In vielen Fällen, in denen Tatpersonen unerkannt bleiben wollen, nutzen sie technische Möglichkeiten zur Verschleierung, etwa durch VPN-Dienste, geteilte Netzwerke oder öffentliche WLAN-Zugänge. Insbesondere bei mobilen Datenverbindungen ist eine eindeutige Zuordnung oft nicht möglich. In vielen anderen Fällen digitaler Gewalt besteht kein Identifikationsproblem, weil die Tatpersonen mit Klarnamen auftreten.

Die anlasslose Speicherung von IP-Adressen von Nutzer*innen bedeutet einen weitreichenden Eingriff in die Rechte aller Internet-Nutzer*innen, ohne dass sich daraus ein verlässlicher Schutzgewinn für Betroffene ergibt. Gerade für Betroffener geschlechtsspezifischer Gewalt ist die Möglichkeit, sich anonym im Netz zu bewegen, oft existenziell, da sie Schutz vor weiterer Überwachung, Kontrolle und Eskalation durch (Ex-)Partner oder anderer Täter bietet und überhaupt erst den Zugang zu Information, Beratung und Unterstützung eröffnet. Dies betrifft insbesondere Betroffene von Stalking oder digitaler Überwachung, die häufig gezielt versuchen müssen, ihre digitalen Spuren zu minimieren, Aufenthaltsorte zu verschleiern oder anonyme Kommunikationswege zu nutzen, um sich vor weiterer Gewalt zu schützen.

Auch Betroffene politisch motivierter digitaler Gewalt – etwa Aktivist*innen, Journalist*innen, Wissenschaftler*innen oder feministische und queere Personen – sind vielfach auf Anonymität angewiesen, um sich vor Doxxing, Einschüchterung, Hasskampagnen oder koordinierten digitalen Angriffen zu schützen. Die Möglichkeit anonymer oder pseudonymer Nutzung digitaler Räume ist für viele Betroffene daher nicht nur Ausdruck informationeller Selbstbestimmung, sondern konkrete Sicherheitsvoraussetzung.

Aus Perspektive der Beratungspraxis besteht daher die Gefahr, dass erhebliche Ressourcen in eine Maßnahme fließen, die in vielen Fällen keine effektive Unterstützung bietet, während gleichzeitig andere, für Betroffene zentrale Instrumente unzureichend ausgestaltet bleiben.

[3] Bundesministerium der Justiz und Verbraucherschutz, Regierungsentwurf-Entwurf eines Gesetzes zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren, s. https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/2025_IP_Speicherung.html

Ansprechpartnerin: Elizabeth Ávila González
Petersburger Straße 94, 10247 Berlin | T +49(0)30/32 29 95 00 | digitalegewalt@bv-bff.de | aktiv-gegen-digitale-gewalt.de

### 2. *Zu §2: Auskunft über Daten*

Der vorgesehene Auskunftsanspruch stellt grundsätzlich ein wichtiges Instrument dar, um Betroffenen die Durchsetzung ihrer Rechte zu ermöglichen.

Die Praxis zeigt jedoch, dass solche Auskunftsansprüche für viele Betroffene nicht im Zentrum ihrer Bedürfnisse stehen. In akuten Gewaltsituationen geht es Betroffenen in erster Linie darum, die Gewalt schnell zu stoppen: also Inhalte entfernen zu lassen, Kontaktmöglichkeiten zu unterbinden oder weitere Übergriffe zu verhindern. Die Identifizierung von Tätern und die Durchsetzung von Ansprüchen treten häufig erst in einem späteren Schritt in den Vordergrund, wenn überhaupt.

Der Gesetzesentwurf setzt jedoch einen starken Fokus auf Auskunftsansprüche und die Identifizierbarkeit von Tätern. Damit wird ein Instrument priorisiert, das für viele Betroffene in der konkreten Situation nicht die dringendste Unterstützung bietet. Gleichzeitig bleibt die Verantwortung, diesen Anspruch zu nutzen, weitgehend bei den Betroffenen selbst. Sie müssen Verfahren anstoßen, rechtliche Schritte einleiten und sich mit komplexen Anforderungen befassen, oft ohne ausreichende psychosoziale Unterstützung.

Die Erlangung von Auskünften über personenbezogene Daten birgt auch Risiken für die Betroffene. In Konstellation digitaler Gewalt im sozialen Nahraum kann die Offenlegung oder gerichtliche Verarbeitung sensibler Daten unbeabsichtigte Rückwirkungen haben, etwa wenn Verfahren eskalieren oder Täter Gegenmaßnahmen ergreifen. So kann bereits die Kenntnis darüber, dass eine betroffene Person rechtliche Schritte eingeleitet hat, zu weiterer Einschüchterung, verstärkter Überwachung oder einer Eskalation von Gewalt führen. In Stalking-Konstellationen besteht zudem die Gefahr, dass Täter versuchen, über Verfahren oder Unterlagen neue Informationen über Aufenthaltsorte, Kommunikationswege oder Unterstützungsstrukturen der Betroffenen zu erlangen. Es ist daher wichtig, dass entsprechende Verfahren besonders sorgfältig ausgestaltet und sensibel gehandhabt werden.

Für die praktische Umsetzung kommt es entscheidend auf ausreichend sensibilisierte und spezialisierte Stellen an (s. Abschnitt I. "Querschnittsproblem: Fehlende Sensibilisierung und Spezialisierung).

Zudem ist sicherzustellen, dass die Verfahren kostenfrei oder zu mindestens mit keinem erheblichen Kostenrisiko verbunden sind. Bereits die Aussicht auf hohe Verfahrenskosten stellt in der Praxis eine erhebliche Hürde dar und führt dazu, dass Betroffene von der Geltendmachung ihrer Rechte absehen.

Für Betroffene bedeutet dies, dass sie erneut auf sich gestellt sind, obwohl sie sich in einer ohnehin belastenden Situation befinden. Der bff hält es daher für notwendig, den Fokus stärker auf Maßnahmen zu legen, die unmittelbar zu Beendigung von Gewalt beitragen. Auskunftsansprüche sollten sinnvoll eingebettet sein, dürfen jedoch nicht zulasten effektiver, niedrigschwelliger Schutzmechanismen priorisiert werden.

### 3. *Zu §4: Sperrung von Nutzerkonten in sozialen Netzwerken*

Die Möglichkeit, Accounts sperren zu lassen, ist für Betroffene digitaler Gewalt zentral. Besonders bei bildbasierter sexualisierter Gewalt werden Accounts genutzt, um intime Inhalte zu verbreiten oder Betroffene

Ansprechpartnerin: Elizabeth Ávila González
Petersburger Straße 94, 10247 Berlin | T +49(0)30/32 29 95 00 | digitalegewalt@bv-bff.de | aktiv-gegen-digitale-gewalt.de

weiter zu belästigen. In Stalking-Konstellationen werden Accounts eingesetzt, um Kontakte aufzunehmen, Betroffene zu überwachen oder einzuschüchtern.

Aus der Beratungspraxis zeigt sich, dass Betroffene Inhalte und Accounts oft wiederholt melden, ohne dass Plattformen zeitnah reagieren. Werden einzelne Accounts gesperrt, erstellen Täter häufig innerhalb kurzer Zeit neue Accounts und setzen die Gewalt fort. Eine einmalige Accountsperre reicht deshalb in vielen Fällen nicht aus. Es braucht wirksame Maßnahmen, erneute Übergriffe tatsächlich zu erschweren.

Vor diesem Hintergrund ist eine gesetzliche Regelung zur Accountsperre grundsätzlich zu begrüßen. Entscheidend ist jedoch, dass sie als frühzeitige Schutzmaßnahme ausgestaltet wird: Aus Sicht der Betroffenen geht es darum, Gewalt schnell zu beenden. Accountsperren dürfen daher nicht erst am Ende langer Verfahren greifen, sondern müssen frühzeitig möglich sein - auch ohne vollständige Identifizierung des Täters.

Accountsperre greifen erheblich in Grundrechte ein und erfordern daher eine sorgfältige und spezialisierte Prüfung (s. Abschnitt I. "Querschnittsproblem: Fehlende Sensibilisierung und Spezialisierung).

Aus Sicht der Praxis bleiben die vorgesehenen Schutzmechanismen jedoch unzureichend. Betroffene müssen weiterhin wiederholt neue Accounts dokumentieren, Anträge stellen und sich erneut mit retraumatisierenden Inhalten auseinandersetzen. Gerade in Stalking- oder koordinierten Angriffskonstellationen führt dies zu erheblichen Belastungen.

Aus Sicht des bff ist das nicht ausreichend. Schutzmaßnahmen müssen frühzeitig gebündelt und wirksam greifen. Gleichzeitig geht es für Betroffene in vielen Fällen vor allen darum, nicht-einvernehmlich veröffentlichte Inhalte schnell entfernen zu lassen. Gerade bei bildbasierter sexualisierter Gewalt ist eine schnelle Löschung zentral, um weitere Verbreitung und andauernde Belastungen zu verhindern. Dieses Schutzbedürfnis wird im derzeitigen Entwurf jedoch nicht ausreichend adressiert. Stattdessen wird die Verantwortung, gegen immer neue Accounts und Inhalte vorzugehen, weiterhin weitgehend auf die Betroffene verlagert.

### 4. *Zu §7: Vertretung durch zivilgesellschaftliche Organisationen*

Die in §7 vorgesehene Möglichkeit der Vertretung durch zivilgesellschaftliche Organisationen ist grundsätzlich zu begrüßen, bleibt jedoch hinter einem echten Verbandsklagerecht zurück. Die Regelung ermöglicht lediglich eine Bevollmächtigung im Einzelfall und setzt weiterhin voraus, dass Betroffene selbst Verfahren anstoßen, die Belastungen des Verfahrens tragen und individuell gegen Täter oder Plattformen vorgehen.

Gerade bei digitaler Gewalt stößt diese Form individueller Rechtsdurchsetzung jedoch regelmäßig an ihre Grenzen. Viele Betroffene befinden sich in hochbelastenden Situationen, verfügen nicht über die finanziellen oder psychischen Ressourcen für langwierige Verfahren oder sehen sich massiven Machtasymetrien gegenüber großen Plattformen oder Täter ausgesetzt. Zugleich handelt es sich bei digitaler Gewalt häufig nicht um isolierte Einzelfälle, sondern die Gewalt wird durch strukturelle Probleme - etwa unzureichende

Ansprechpartnerin: Elizabeth Ávila González
Petersburger Straße 94, 10247 Berlin | T +49(0)30/32 29 95 00 | digitalegewalt@bv-bff.de | aktiv-gegen-digitale-gewalt.de

Moderationspraktiken, systematische Schutzlücken oder diskriminierende Plattformmechanismen befördert.

Ein Verbandsklagerecht würde es ermöglichen, solche strukturellen Missstände unabhängig vom einzelnen Verfahren gerichtlich überprüfen zu lassen und grundlegende Schutzstandards durchzusetzen. Dadurch würden Betroffene entlastet, Verfahren gebündelt und Rechtsdurchsetzung effektiver gestaltet. Aus Sicht des bff ist ein Verbandsklagrecht daher ein zentraler Baustein für wirksamen Gewaltschutz im digitalen Raum und der vorgeschlagenen Regelung deutlich vorzuziehen.

### 5. *Zu §9: Inländischer Zustellungsbevollmächtigter*

Die Verpflichtung von Plattformen zur Benennung von inländischen Zustellungsbevollmächtigten ist ein wichtiger Schritt zur Verbesserung der Rechtsdurchsetzung. Betroffene stehen derzeit häufig vor erheblichen praktischen Hürden, wenn sie rechtlich gegen Plattformen vorgehen wollen. Zustellungen scheitern, Ansprechpartner*innen sind nicht erreichbar oder Verfahren verzögern sich erheblich. Eine klare und verbindliche Zustellstruktur kann hier zu einer Verbesserung führen. Voraussetzung ist jedoch, dass die benannten Stellen tatsächlich erreichbar sind und Verfahren effizient abgewickelt werden.

### 6. *Zum Datenschutz der Betroffenen*

Der Schutz der Daten von Betroffenen ist ein zentraler Bestandteil eines wirksamen Gewaltschutzes. Viele Betroffene digitaler Gewalt befinden sich in Situationen, in denen ihre Sicherheit konkret gefährdet ist, insbesondere im Kontext häuslicher oder partnerschaftlicher Gewalt. In solchen Fällen kann die Offenlegung von Adressdaten erhebliche Risiken mit sich bringen. Die Möglichkeit c/o-Adressen oder vergleichbare Schutzmechanismen zu nutzen, ist daher essenziell. Aus Sicht der Beratungspraxis ist Datenschutz hier nicht nur eine formale Frage, sondern unmittelbar mit dem Schutz vor weiterer Gewalt verbunden. Regelungen müssen daher sicherstellen, dass Betroffene ihre Rechte durchsetzen können, ohne sich dabei zusätzlichen Gefahren auszusetzen.

### 7. *Fazit*

Die vorgesehenen zivilrechtlichen Regelungen enthalten wichtige Ansätze, bleiben jedoch aus Sicht der Betroffenen in ihrer derzeitigen Ausgestaltung hinter den tatsächlichen Bedarfen zurück.

Der bff fordert daher:

- Eine konsequente Ausrichtung zivilrechtlicher Instrumente auf die schnelle Beendigung von Gewalt
- Frühzeitige, gebündelte und wirksame Accountsperren, auch ohne vollständige Identifizierung von Täter*innen
- Die Einführung eines Verbandsklagerechts, um strukturelle Probleme adressieren zu können
- Sowie niedrigschwellige, zugängliche Verfahren, die die tatsächlichen Handlungsmöglichkeiten von Betroffenen berücksichtigen

Ansprechpartnerin: Elizabeth Ávila González
Petersburger Straße 94, 10247 Berlin | T +49(0)30/32 29 95 00 | digitalegewalt@bv-bff.de | aktiv-gegen-digitale-gewalt.de

## III. Zur Änderung des Strafgesetzbuches

### 1. *Zu §184k StGB-E: Verletzung der Intimsphäre durch Bildaufnahmen*

Die Neuregelung stellt einen wichtigen Schritt dar, die Vorgaben der EU-Richtlinie 2024/1385, die bildbasierte sexualisierte Gewalt regelt, zu erfüllen. Der neu geschaffene §184k StGB trägt der Realität Rechnung, dass bereits die nicht-einvernehmliche Herstellung intimer (manipulierter) Inhalte eine eigenständige Verletzung der sexuellen Selbstbestimmung darstellt.

#### 1.1. *Zu §184k Abs. 1 Nr. 3 StGB-E: digitaler Voyeurismus*

Die Ausweitung des Tatbestands auf Aufnahmen bekleideter Körperteile ist aus gesellschaftlicher Perspektive nachvollziehbar, wirft jedoch erhebliche praktische und rechtliche Umsetzungsprobleme auf.

Im vorliegenden Referenten-Entwurf ist die zentrale Voraussetzung für die Strafbarkeit von sogenanntem digitalem Voyeurismus der Nachweis eines „sexualbezogenen" Handelns bzw. einer entsprechenden Motivation. Dieser Begriff ist jedoch unbestimmt und in der Praxis schwer abzugrenzen. Hinzu kommt ein grundlegendes Beweisproblem: Der Vorsatz ist in Bezug auf eine sexuelle Motivation ist regelmäßig nur schwer nachweisbar. Täter können alternative Motive behaupten, wodurch die Strafbarkeit in vielen Fällen an der Beweisbarkeit scheitert. Es besteht daher die reale Gefahr, dass die Norm in der Praxis weitgehend ins Leere läuft.

Zusätzlich wird diese Problematik durch technische Entwicklung verschärft. Hochauflösende Kameras und Zoomfunktionen ermöglichen es heute aus weit entfernten oder scheinbar harmlosen Aufnahmen nachträglich intime Details herauszuarbeiten. Dadurch verschiebt sich die Grenze zwischen vermeintlich „neutraler" Aufnahmen und voyeuristischer Nutzung zunehmend in schwer kontrollierbare Bereiche.

Die konsequente Anwendung der Norm würde erhebliche Anforderungen an Ermittlungsbehörden, Staatsanwaltschaften und Gerichte stellen. Ohne spezialisierte Schulungen im Umgang mit digitaler Bildauswertung, Kontextanalyse und technischen Manipulationsmöglichkeiten droht eine uneinheitliche und restriktive Anwendung.

Auch wenn durch das Strafrecht eine gesellschaftliche Signalwirkung entfaltet werden kann, weil Taten als Unrecht benannt werden, ist aufgrund der enormen Umsetzungshürden in diesem Fall das Strafrecht als zentrales Steuerungsinstrument anzuzweifeln. Stattdessen erscheint es sinnvoll, den Blick stärker auf präventive Ansätze zu richten und diese Auszubauen. Eine solche Regelung kann dabei allenfalls als ergänzender Baustein wirken, insbesondere im Zusammenspiel mit Maßnahmen wie:

- Aufklärung über digitale Grenzverletzung und fehlendes digitales Einvernehmen
- Sensibilisierung für sexualisierte Objektivierung und Rollenbilder
- Stärkung von Medienkompetenz im Umgang mit Bildaufnahmen und Weiterverarbeitung
- Gesellschaftliche Auseinandersetzung mit Machtverhältnissen im digitalen Raum
- Spezialisierte Schulungen für Polizei, Staatsanwaltschaften und Gerichte zu digitalen Gewaltformen, sexualisierter Objektivierung und technischen Manipulationsmöglichkeiten

Ansprechpartnerin: Elizabeth Ávila González
Petersburger Straße 94, 10247 Berlin | T +49(0)30/32 29 95 00 | digitalegewalt@bv-bff.de | aktiv-gegen-digitale-gewalt.de

### *1.2. Zu §184k Abs. 1 Nr. 4 StGB-E: Herstellung und Verbreitung sexualisierter Deepfakes*

Die Strafbarkeit der Herstellung sexualisierter Deepfakes ist grundsätzlich zu begrüßen. Der Tatbestand stellt darauf ab, dass mittels eines Computerprogramms Inhalte so verändert, umgestaltet oder mit weiteren Inhalten verbunden werden, dass der Anschein erweckt wird, es seien sexuelle Handlungen oder die unbekleideten Genitalien, das unbekleidete Gesäß oder die unbekleidete weibliche Brust einer anderen Person abgebildet. Aus betroffenenzentrierter Perspektive ist das kritisch zu bewerten.

Die Voraussetzung eines „Anscheins" verengt den Schutzbereich in problematischer Weise. Aus Sicht der Betroffenen liegt der Unrechtsgehalt nicht primär in einer möglichen Täuschungswirkung, sondern in der nicht-einvernehmlichen sexualisierten Darstellung ihrer Person. Entscheidend ist die Verletzung der sexuellen und informationellen Selbstbestimmung, unabhängig davon, ob Inhalte als echt wahrgenommen oder technisch als manipuliert erkennbar sind.

Zudem führt die Beschränkung auf „sexuelle Handlungen" und bestimmte unbekleidete Körperteile zu erheblichen Schutzlücken. Erfasst werden etwa keine Fälle, in denen durch digitale Bearbeitung zwar Kleidung nicht ausgezogen wird, jedoch gravierende Verletzung der Intimsphäre und Selbstbestimmung erfolgt. Dies betrifft etwa die Erstellung oder Veränderung von Bildern in Bikinis oder freizügiger Kleidung sowie KI-generierte Manipulationen, bei denen etwa muslimischen Frauen digital das Kopftuch entfernt wird. Solche Eingriffe stellen klar geschlechtsspezifische Gewalt und Entwürdigung dar.

Vor diesem Hintergrund erscheint eine stärkere Anbindung an den Schutz der Intimsphäre sowie sexuellen Selbstbestimmung sachgerechter. Der bff plädiert für eine betroffenenzentrierte Ausgestaltung, die nicht an enge bildbezogene Kategorien oder den „Anschein der Echtheit" anknüpft, sondern die Verletzung der betroffenen Person in den Mittelpunkt stellt. Dies muss ausdrücklich auch Fälle umfassen, in denen Darstellungen formal als nicht echt gekennzeichnet sind – etwa durch kleine Wasserzeichen oder Hinweise –, die jedoch nichts daran ändern, dass die betroffene Person in ihrer Intimsphäre und sexuellen Selbstbestimmung verletzt wird.

Im Lichte der EU-Richtlinie 2024/1385 zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt ist ein solcher weiter, betroffenenzentrierter Ansatz geboten. Erforderlich ist zudem eine Sensibilisierung von Polizei, Staatsanwaltschaft und Justiz für die vielfältigen Erscheinungsformen digitaler, sexualisierter und geschlechtsspezifischer Gewalt sowie deren intersektionale Dimension.

### *1.3. Weitere Gewaltformen bildbasierter sexualisierter Gewalt: Schutzlücken bei Identitätsmissbrauch und Avataren*

Die Beratungspraxis zeigt, dass bildbasierte sexualisierte Gewalt nicht auf „klassische" Deepfake-Konstellationen beschränkt ist. Ein erheblicher Teil der Fälle betrifft Konstellationen, in denen Täter keine komplexe KI-Technologie einsetzen, sondern Profile im Namen der betroffenen Person erstellen, vorhandene Bilder verwenden oder Inhalte kontextuell verfälschen. Solche Fälle – etwa das Erstellen von Fake-Profilen

Ansprechpartnerin: Elizabeth Ávila González
Petersburger Straße 94, 10247 Berlin | T +49(0)30/32 29 95 00 | digitalegewalt@bv-bff.de | aktiv-gegen-digitale-gewalt.de

zur Initiierung sexualisierter Kommunikation mit Dritten – verdeutlichen, dass die Verletzung bereits darin liegt, dass einer Person ohne ihre Zustimmung eine sexuelle Rolle oder bestimmte sexuelle Handlung zugeschrieben wurde.

Aus Sicht des bff bestehen hier Schutzlücken, weil die geplanten Regelungen teilweise zu eng an Kriterien wie den "Anschein der Echtheit", "täuschende Inhalte" oder bestimmte technische Herstellungsweisen an. Dadurch bleibt unklar beziehungsweise besteht die Gefahr, dass Konstellationen nicht erfasst werden, in denen keine technisch komplexe Manipulation vorliegt, die betroffene Person aber dennoch in sexualisierter Weise digital instrumentalisiert wird.

Aus Sicht der Betroffenen ist jedoch entscheidend, dass ihre Identität, ihr Körper und ihre sexuelle Selbstbestimmung ohne Einwilligung instrumentalisiert werden – unabhängig davon, ob es sich um ein KI-generiertes Bild, ein bearbeitetes Foto, die Verwendung des Bildes einer täuschend ähnlichen Person im Zusammenhang mit ihrer Identität oder ein vollständig konstruiertes Profil handelt. Gleiches gilt für audio-basierte Manipulationen wie Voice Cloning, bei denen Stimmen von Betroffenen täuschend echt nachgebildet und teilweise für sexualisierte oder herabwürdigende Inhalte verwendet werden.

Dies gilt in besonderem Maße auch für sogenannte Avatare oder künstlich erzeugte Darstellungen, die realen Personen täuschend ähnlichsehen. Derartige Inhalte können gezielt eingesetzt werden, um Betroffene zu sexualisieren, zu diffamieren oder in kontrollierende Gewaltkontexte einzubinden. Der derzeitige Gesetzesentwurf regelt nicht ausdrücklich, ob und in welchen Umfang solche Konstellationen erfasst sind.

Der bff sieht hier eine erhebliche Schutzlücke Der bff fordert daher eine technologieoffene und ausdrücklich umfassende Regelung, die alle Formen des Identitätsmissbrauchs erfasst, bei denen reale Personen in sexualisierter Weise digital dargestellt, zugeschrieben oder instrumentalisiert wird. Entscheidend darf nicht die technische Herstellungsweise oder die Täuschungsqualität sein, sondern die Verletzung der Persönlichkeitsrechte, der sexuellen Selbstbestimmung und der Sicherheit der Personen.

## 2. *Zu §202e StGB-E: Unbefugte Überwachung mittels Informations- oder Kommunikationstechnik*

### *2.1 Verhältnis zu §238 StGB (Nachstellung) und Art. 6 der EU-Richtlinie 2024/1385*

Die Einführung eines eigenen Straftatbestands für digitale Überwachung ist grundsätzlich sinnvoll. Gleichzeitig ist das Verhältnis zu §238 StGB (Nachstellung) unklar.

§238 StGB erfasst bereits heute ein breites Spektrum von Nachstellungshandlungen, die geeignet sind, die Lebensgestaltung der betroffenen Person schwerwiegend zu beeinträchtigen. Digitale Überwachung – etwa durch Tracking oder das Mitlesen von Kommunikation – ist in der Praxis häufig Teil genau solcher Nachstellungsdynamiken im sozialen Nahraum.

Art. 6 der EU-Richtlinie 2024/1385 greift dieses Phänomen auf, indem er „Cyberstalking“ ausdrücklich als wiederholte Überwachung von Aufenthalt und Tätigkeiten mittels Informations- und

Ansprechpartnerin: Elizabeth Ávila González
Petersburger Straße 94, 10247 Berlin | T +49(0)30/32 29 95 00 | digitalegewalt@bv-bff.de | aktiv-gegen-digitale-gewalt.de

Kommunikationstechnologie beschreibt. Allerdings bleibt die Richtlinie in ihrer Formulierung teilweise hinter dem Schutzniveau von §238 StGB zurück, weil sie stärker auf einzelne Handlungen fokussiert und weniger klar die Gesamtwirkung auf die Lebensgestaltung adressiert. Vor diesem Hintergrund besteht die Gefahr eines Rückschritts, wenn digitale Überwachung nicht mehr im Rahmen des bestehenden Nachstellungstatbestands (§238 StGB) mitgedacht wird, sondern in einem eigenständigen und enger gefasst Straftatbestand geregelt wird.

Gleichzeitig zeigt die Beratungspraxis auch Grenzen des bisherigen §238 StGB auf. Nachstellung setzt regelmäßig wederholte Tatbegehungen voraus. Im Bereich digitaler Überwachung können jedoch bereits einzelne Handlungen erhebliche Kontroll- und Einschüchterungswirkungen entfalten. Das heimliche Installieren von Spyware, die Einrichtung eines Ortungssystems oder die Verknüpfung eines Accounts mit Überwachungsfunktionen ermöglichen häufig eine dauerhafte Kontrolle durch nur eine Handlung. Diese digitale Gewaltrealität muss gesetzlich ausdrücklich berücksichtigt werden.

Der bff hält es daher für erforderlich, digitale Überwachung ausdrücklich als Form der Nachstellung in §238 StGB zu verankern und den Tatbestand zugleich an digitale Gewaltrealitäten anzupassen. Dabei sollte klargestellt werden, dass auch einzelne Handlungen erfasst sein können, wenn sie eine fortdauernde Überwachung oder Kontrolle ermöglichen. Eine solche Lösung würde das bestehende Schutzniveau sichern und zugleich die Vorgabe der EU-Richtlinie 2024/1385 progressiv umsetzen.

### 2.2 *„Schwerer Schaden" als zentrale Umsetzungshürde*

Der Entwurf knüpft die Strafbarkeit nach §202e StGB-E daran, dass die Handlung „wahrscheinlich einen schweren Schaden" verursacht.

Diese Voraussetzung ist aus Sicht der Praxis häufig nicht tragfähig und führt zu erheblichen Durchsetzungsproblemen:

- Digitale Überwachung wirkt bereits durch Kontrolle, Einschüchterung und ständige Verfügbarkeit
- Betroffene passen ihr Verhalten an, schränken ihre Bewegungsfreiheit ein und vermeiden soziale Kontakte
- Diese Dynamiken setzen lange vor einem nachweisbaren „schweren Schaden" ein.

Zudem wissen Betroffene häufig zunächst nicht, dass sie überwacht werden, sodass ein Schadensnachweis praktisch kaum möglich ist.

Hinzu kommt, dass der Begriff des "schweren Schadens" im juristischen Kontext häufig mit erheblichen materiellen Schäden oder massiven körperlichen Beeinträchtigungen verbunden wird. Die Folgen digitaler Überwachung liegen aus Sicht der Betroffenen jedoch vielfach im psychosozialen Bereich: dauerhafte Verunsicherung, Angst, sozialen Rückzug, Kommunikationsvermeidung, Kontrollverlust oder die Einschränkung der eigenen Lebensführung. Gerade diese Auswirkungen lassen sich in Verfahren oft nur schwer objektivieren oder nachweisen. Es besteht daher die Gefahr, dass Betroffene gezwungen werden, ihre psychischen Belastungen umfassend darzulegen und durch Gutachten oder andere Nachweise zu belegen. Dies

Ansprechpartnerin: Elizabeth Ávila González
Petersburger Straße 94, 10247 Berlin | T +49(0)30/32 29 95 00 | digitalegewalt@bv-bff.de | aktiv-gegen-digitale-gewalt.de

kann zusätzliche Belastungen, langwierige Verfahren sowie kosten- du kräftezehrende Begutachtungen nach sich ziehen. Gleichzeitig drohen Missverständnisse darüber, welche Formen von Schaden überhaupt als ausreichend angesehen werden. Die Folge ist eine erhebliche Schutzlücke: Gerade typische Fälle digitaler Kontrolle im sozialen Nahraum würden nicht erfasst.

Der bff fordert daher die Streichung des Merkmals „schwerer Schaden". Entscheidend sollte – wie auch bei §238 StGB – die Eignung zur Beeinträchtigung der Lebensgestaltung bzw. zur Erzeugung von Angst und Kontrolle sein.

### *2.3 IoT- und Smart-Home-Gewalt*

Digitales Stalking im sozialen Nahraum erfolgt zunehmend über vernetzte Geräte. Täter manipulieren gezielt Licht, Heizung, Kameras und Zugangssysteme, um Angst zu erzeugen und Kontrolle zu auszuüben.

Diese Form der Gewalt ist Ausdruck eines umfassenden Kontrollverhältnisses und eng mit Nachstellung im Sinne des §238 StGB verknüpft. Der Gesetzesentwurf bildet diese Realität nicht ausreichend ab. Insbesondere greift der Begriff „unbefugt" zu kurz, wenn Täter legitime Zugänge missbrauchen – eine typische Konstellation in Partnerschaften.

### *2.4 Monitoring, Spyware und missbräuchliche Nutzung von Dual-Use-Technologien*

Der Entwurf bleibt hinter den tatsächlichen Erscheinungsformen digitaler Überwachung zurück. Die EU-Richtlinie erfasst ausdrücklich auch „Monitoring" mittels Informations- und Kommunikationstechnologie. Dazu gehört insbesondere das Mitlesen privater Kommunikation durch Spyware oder andere Überwachungssoftware. Diese Formen digitaler Kontrolle werden im Gesetzesentwurf bislang nicht berücksichtigt.

Aus der Beratungspraxis ist bekannt, dass Täter gezielt Spyware, Account-Synchronisierungen oder sogenannte Dual-Use-Apps wie Familien- oder Kinderschutzanwendungen missbrauchen, um private Chats, Nachrichten, Standorte oder Kommunikationsverhalten zu überwachen. Auch das Ausspionieren von Nachrichten über gemeinsam genutzte Accounts oder Geräte spielt in Gewaltkonstellationen eine erhebliche Rolle. Diese Formen digitaler Überwachung beziehen sich nicht nur auf Aufenthaltsorte, sondern auf die gesamte private Kommunikation und Lebensführung er Betroffenen.

Der bff fordert daher, dass das Monitoring- und Überwachungsformen – insbesondere das Mitlesen privater Kommunikation mittels Spyware oder missbräuchlich eingesetzter Dual-Use-technologien – ausdrücklich in den Schutzbereich aufgenommen werden.

## 3. *Praktische Rechtsdurchsetzung und Verfahrensschutz*

Die EU-Richtlinie 2024/1385 zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt betont ausdrücklich, dass Betroffene einen effektiven Zugang zum Recht sowie betroffenenzentriert Verfahren benötigen. Aus Sicht des bff zeigt die Praxis jedoch, dass genau hier die größten Hürden liegen.

Ansprechpartnerin: Elizabeth Ávila González
Petersburger Straße 94, 10247 Berlin | T +49(0)30/32 29 95 00 | digitalegewalt@bv-bff.de | aktiv-gegen-digitale-gewalt.de

Betroffene digitaler Gewalt erleben häufig ein Defizit an tatsächlicher Durchsetzung bestehender strafrechtlichen Normen. Anzeigen führen vielfach nicht zu weiteren Ermittlungen oder werden frühzeitig eingestellt, Beweise werden nicht gesichert oder nicht richtig eingeordnet. Gleichzeitig sind Betroffene oft auf sich allein gestellt, müssen Inhalte selbst dokumentieren und bewegen sich in komplexen, für sie kaum zugänglichen Verfahren.

Ein wirksamer Gewaltschutz erfordert daher zwingend eine Stärkung des Verfahrensrechts und der praktischen Umsetzung von Strafgesetzen.

### *3.1 Nebenklagerecht und Psychosoziale Prozessbegleitung stärken*

Betroffene digitaler Gewalt sind in Strafverfahren häufig in einer besonders vulnerablen Position. Sie stehen Tätern gegenüber, deren Handlungen tief in ihre Intimsphäre und Privatsphäre, sowie sexuelle und informationelle Selbstbestimmung eingreifen und deren Folgen dauerhaft im digitalen Raum fortbestehen können.

Ein Recht auf Nebenklage ermöglicht es Betroffenen, aktiv am Verfahren teilzunehmen, eigene Rechte geltend zu machen und nicht auf die Rolle reiner Zeug*innen reduziert zu werden. Aus Sicht der Beratungspraxis ist dies ein zentraler Baustein, um Betroffene zu stärken und sekundäre Viktimisierung zu vermeiden.

Darüber hinaus kommt der psychosozialen Prozessbegleitung eine zentrale Bedeutung zu. Diese unterstützt Betroffene dabei, die Belastungen eines Strafverfahrens zu bewältigen, informiert über Abläufe und begleitet durch das Verfahren. Gerade bei digitaler Gewalt, die häufig mit anhaltender Sichtbarkeit der Tatfolgen und komplexen technischen sowie rechtlichen Fragen verbunden ist, ist eine solche Unterstützung essenziell. Deswegen ist bei den aktuellen gesetzgeberischen Entwicklungen zur Erweiterung der psychosozialen Prozessbegleitung sicherzustellen, dass Betroffene digitaler Gewalt ausdrücklich in den Anwendungsbereich einbezogen werden.

Aus Sicht des bff ist es erforderlich, Nebenklagerechte und psychosoziale Prozessbegleitung systematisch auch auf digitale Gewalt auszurichten und auszubauen. Nur so kann gewährleistet werden, dass Betroffene ihre Rechte tatsächlich wahrnehmen können und Verfahren nicht zu einer zusätzlichen Belastung werden.

### *3.2 Verjährung an digitale Realitäten anpassen*

Digitale Gewalt folgt anderen Zeitlogiken als analoge Straftaten. Inhalte verschwinden nicht, sondern bleiben oft dauerhaft verfügbar oder tauchen nach Jahren erneut auf. Gleichzeitig erfahren viele Betroffene erst verspätet von der Existenz entsprechender Inhalte.

In der Praxis führt dies dazu, dass Taten verjähren, bevor Betroffene überhaupt die Möglichkeit haben, rechtlich dagegen vorzugehen. Dies untergräbt den Schutzgedanken des Strafrechts und verstärkt das Gefühl von Ohnmacht.

Aus Sicht des bff ist daher zu prüfen, ob entsprechende Taten als Dauerdelikte ausgestaltet oder Verjährungsfristen zu mindestens an die andauernde Betroffenheit angepasst werden. Der bff regt an,

Ansprechpartnerin: Elizabeth Ávila González
Petersburger Straße 94, 10247 Berlin | T +49(0)30/32 29 95 00 | digitalegewalt@bv-bff.de | aktiv-gegen-digitale-gewalt.de

entsprechende gesetzgeberische Anpassungen ausdrücklich in Betracht zu ziehen. Zudem könnte erwogen werden, den Beginn der Verjährung bis zur Kenntnis der betroffenen Person von der Tat hinauszuschieben.

#### *3.3 Beweissicherung realistisch gestalten*

Ein weiteres Praxis-Problem ist die Sicherung digitaler Beweise. Betroffene sind häufig darauf angewiesen, selbst Screenshots anzufertigen oder Inhalte zu dokumentieren, ohne zu wissen, welche Beweise tatsächlich erforderlich sind oder wie diese rechtssicher gesichert werden können.

Gleichzeitig fehlt es bei Ermittlungsbehörden oft an ausreichender Expertise, um digitale Spuren korrekt auszuwerten. Dabei gehen wichtige Informationen verloren oder werden in den Ermittlungen nicht berücksichtigt.

Der bff fordert daher:

- Niedrigschwellige, bundesweit zugängliche Möglichkeiten zur Online-Anzeige
- Klare Standards zur Sicherung digitaler Beweise
- Sowie eine proaktive Unterstützung der Betroffenen durch die Behörden

Beweissicherung darf nicht auf die Betroffenen verlagert werden.

### 4. *Fazit*

Der Gesetzesentwurf stellt einen wichtigen Schritt dar, indem er digitale Gewalt ausdrücklich als strafrechtlich relevantes Unrecht anerkennt und neue Tatbestände, insbesondere im Bereich bildbasierter sexualisierter Gewalt und digitaler Überwachung, einführt. Allerdings zeigen sich aus Sicht des bff Schutzlücken und Umsetzungsprobleme.

Der bff fordert daher:

- die Streichung der Voraussetzung eines „schweren Schadens“ in §202e StGB-E
- Eine systematische Einbindung digitaler Überwachung in §238 StGB (Nachstellung)
- Ausweitung des Schutzbereichs bei bildbasierter Gewalt, insbesondere bei Deepfakes
- Schließung von Schutzlücken bei Identitätsmissbrauch und neuen Gewaltformen
- Sowie eine konsequente Stärkung der Verfahrensrechte und Umsetzungskapazitäten (Nebenklage, Verjährung, Beweissicherung, Spezialisierung)

## IV. Europarechtliche Einordnung

### 1. *EU-Richtlinie 2024/1385 zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt*

Die EU-Richtlinie 2024/1385 setzt erstmals verbindliche Mindeststandards für den Schutz vor geschlechtsspezifische Gewalt, einschließlich digitaler Gewaltformen. Sie verpflichtet die Mitgliedstaaten insbesondere dazu, Straftatbestände wie Cyberstalking, die nicht-einvernehmliche Weitergabe oder Herstellung intimer Inhalte sowie weiterer Formen digitaler Gewalt wirksam zu erfassen und zu sanktionieren.

Ansprechpartnerin: Elizabeth Ávila González
Petersburger Straße 94, 10247 Berlin | T +49(0)30/32 29 95 00 | digitalegewalt@bv-bff.de | aktiv-gegen-digitale-gewalt.de

Zugleich geht die Richtlinie über das Strafrecht hinaus und verlangt einen umfassenden, betroffenenzentrierten Ansatz. Dieser umfasst neben strafrechtlichen Regelungen insbesondere auch Betroffenenschutz, Prävention, den Ausbau von Strafverfolgungskapazitäten sowie die Verpflichtung zur systematischen Disaggregierter Daten. Besonders hervorzuheben ist, dass digitale Gewalt ausdrücklich als Teil eines Kontinuums von Gewalt im sozialen Nahraum anerkannt wird. Vor diesem Hintergrund ist der nationale Gesetzgeber gehalten, die Richtlinie nicht nur formal umzusetzen, sondern ihr Schutzniveau effektiv auszuschöpfen.

Aus Sicht des bff bleibt der vorliegende Entwurf hinter diesen Anforderungen zurück. Gewaltformen werden nicht vollständig erfasst, Schutzschwellen werden zu hoch angesetzt und die praktische Durchsetzbarkeit der Regelungen ist nicht ausreichend gewährleistet. Eine richtlinienkonforme Umsetzung erfordert daher insbesondere eine Absenkung von Zugangshürden, eine umfassendere Erfassung digitaler Gewaltrealitäten sowie eine konsequente Ausrichtung am Schutzbedarf der Betroffenen.

### 2. *Digital Services Act (DSA)*

Der Digital Services Act stellt einen zentralen Rahmen für die Regulierung von Plattformen dar und ist für den Schutz vor digitaler Gewalt von erheblicher Bedeutung. Plattformen sind verpflichtet, rechtswidrige Inhalte zu entfernen und systemische Risiken zu adressieren.

Der Digital Services Act schafft wichtige regulatorische Verpflichtungen für Plattformen. Aus Sicht des bff bestehen jedoch weiterhin erhebliche Defizite bei der praktischen Umsetzung, insbesondere bei Meldewegen, Erreichbarkeit von Plattformen und der systematischen Risikoanalyse.

### 3. *KI-Verordnung*

Die europäische KI-Verordnung ist ebenfalls anzusprechen, wenn es um den Schutz vor digitaler Gewalt geht. Technologien wie generative KI ermöglichen neue Formen von Gewalt, insbesondere durch die einfache Erstellung und Verbreitung manipulierter Inhalte, wie sexualisierter Deepfakes.

Aus Sicht der Betroffenen ist entscheidend, dass diese Risiken bereits auf Ebene der Technologie berücksichtigt werden. Anbieter von KI-Systemen müssen Verantwortung für mögliche Missbrauchsszenarien übernehmen, und Schutzmechanismen müssen integraler Bestandteil der Systeme sein.

Die Regulierung von KI darf daher nicht isoliert betrachtet werden, sondern muss eng mit Fragen des Gewaltschutz verknüpft werden.

### 4. *Fazit*

Die europarechtlichen Vorgaben verdeutlichen, dass der Schutz vor digitaler Gewalt einen ganzheitlichen Ansatz erfordert, der Strafrecht, Zivilrecht und Plattformregulierung miteinander verbindet. Der

Ansprechpartnerin: Elizabeth Ávila González
Petersburger Straße 94, 10247 Berlin | T +49(0)30/32 29 95 00 | digitalegewalt@bv-bff.de | aktiv-gegen-digitale-gewalt.de

vorliegende Gesetzesentwurf greift wichtige Aspekte auf, bleibt jedoch in seiner Ausgestaltung hinter den Möglichkeiten und Anforderungen des europäischen Rechtsrahmens zurück.

Aus Sicht des bff ist es erforderlich, die nationalen Regelungen konsequent an den Zielen der EU-Richtlinie 2024/1385, des Digital Services Act und der KI-Verordnung auszurichten. Dies bedeutet insbesondere:

- Eine umfassende und realitätsnahe Erfassung digitaler Gewaltformen,
- Effektive und niedrigschwellige Schutzmechanismen für Betroffene,
- Eine verbindliche und überprüfbare Verantwortung von Plattformen,
- Sowie die frühzeitige Berücksichtigung von Gewaltrisiken in technologischen Entwicklungen

Nur wenn diese Elemente zusammengedacht und konsequent umgesetzt werden, kann ein wirksamer Schutz vor digitaler Gewalt gewährleitet werden. Andernfalls besteht die Gefahr, dass rechtliche Fortschritte auf dem Papier bestehen bleiben, ohne die Situation der Betroffenen tatsächlich zu verbessern.

Ansprechpartnerin: Elizabeth Ávila González
Petersburger Straße 94, 10247 Berlin | T +49(0)30/32 29 95 00 | digitalegewalt@bv-bff.de | aktiv-gegen-digitale-gewalt.de