

# Zugang zu Recht in Fällen digitaler Gewalt

11.03.2026



## **Abstract**

Digitale Gewalt gegen Frauen und Mädchen ist eine Ausprägung geschlechtsspezifischer Gewalt und heute eine zentrale gleichstellungsrechtliche Herausforderung. Sie reicht von bildbasierter sexualisierter Gewalt und Deepfakes über Cyberstalking und Hatespeech bis hin zu Doxing und koordinierten Angriffen in misogynen Online-Milieus. Die aktuellen Zahlen belegen einen drastischen Anstieg entsprechender Delikte; zugleich werden weniger als fünf Prozent der Taten angezeigt. Dabei bestehen für Betroffene häufig erhebliche Hürden beim Zugang zu Recht, die eine effektive Rechtsdurchsetzung erschweren. Digitale Gewalt bleibt dadurch in weiten Teilen unsichtbar und wird nur selten geahndet. Für Betroffene hat dies erhebliche psychische, soziale und berufliche Folgen; sehr oft bewirkt es den Rückzug aus digitalen und insgesamt gesellschaftlichen Räumen.

Deutschland ist völker- und europarechtlich verpflichtet, geschlechtsspezifische Gewalt auch im digitalen Raum wirksam zu verhindern, zu verfolgen und zu sanktionieren. Maßstäbe ergeben sich aus der CEDAW, der EMRK, der Istanbul-Konvention, dem Digital Services Act sowie aus der EU-Gewaltschutz-Richtlinie 2024. Sie alle konkretisieren, was das Grundgesetz ohnehin fordert: Die tatsächliche Durchsetzung der Gleichberechtigung und die Beseitigung bestehender Nachteile, so fordert Art. 3 Abs. 2 GG, die auch hier erschreckend oft zulasten von Frauen gehen.

Vor diesem Hintergrund ergeben sich drei Handlungsprioritäten:

1. Konsequente Umsetzung internationaler und europäischer Standards, insbesondere der EU-Gewaltschutz-Richtlinie.
2. Entwicklung eines ganzheitlichen Konzepts aus Prävention, Schutz und effektiver Rechtsverfolgung.
3. Regelmäßige, systematische und intersektional aufgeschlüsselte Datenerhebung.

# Inhalt

1.	Einleitung.....	1
2.	Begriffliche Einordnung und Erscheinungsformen digitaler Gewalt .....	2
I.	Formen digitaler geschlechtsspezifischer Gewalt .....	2
II.	Geschlechtsspezifische Dimension und Intersektionalität .....	2
III.	Die Manosphäre .....	3
3.	Internationaler und europäischer Rechtsrahmen .....	3
I.	UN-Frauenrechtskonvention .....	3
II.	UN-Übereinkommen gegen Cyberkriminalität.....	4
III.	Europäische Menschenrechtskonvention .....	4
IV.	Istanbul-Konvention .....	5
V.	Europäische Union.....	6
1.	EU-Gewaltschutz-Richtlinie .....	6
2.	Digital Services Act .....	7
3.	Datenschutzgrundverordnung.....	7
4.	Nationaler Rechtsrahmen in Deutschland.....	8
I.	Strafrecht.....	8
II.	Zivilrecht .....	8
5.	Sachgerechte Forderungen des djb .....	9
I.	Schließung gesetzlicher Schutzlücken .....	9
II.	Verbesserung von Ermittlungs- und Verfahrensstrukturen.....	11
III.	Konsequente Umsetzung der EU-Gewaltschutz-Richtlinie 2024.....	11
IV.	Stärkere Plattformverantwortung.....	12
V.	Bessere Unterstützung und Schutz von Betroffenen.....	12
VI.	Datenerhebung.....	13
6.	Schlussbemerkung und Ausblick .....	13

# 1. Einleitung

Dieses Positionspapier des Deutschen Juristinnenbunds e.V. (djb) gibt einen Überblick über die Problematik des Zugangs zum Recht in Fällen digitaler Gewalt und verdeutlicht angesichts bestehender Verpflichtungen Deutschlands nach europäischem und internationalem Recht nach wie vor bestehenden Handlungsbedarf. Auf Umsetzungsdefizite hat der djb bereits wiederholt hingewiesen und Vorschläge formuliert, um digitaler Gewalt wirksam zu begegnen.<sup>1</sup> Das [Event](#) des djb in Kooperation mit dem Bundesministerium für Bildung, Familie, Senioren, Frauen und Jugend (BMBFSJ) „Access to justice in cases of digital violence. Countering the manosphere“ anlässlich der 70. Commission on the Status of Women vom 9. bis 20. März 2026 unterstreicht die Aktualität und Relevanz des Themas.

Digitale Gewalt gegen Frauen und Mädchen ist nicht nur eine immer weiter verbreitete Form der Gewalt. Sie stellt auch ein strukturelles Gleichstellungs- und Rechtsproblem dar, denn viele Formen digitaler Gewalt sind keine isolierten Einzelhandlungen, sondern die Fortsetzung patriarchaler Kontroll- und Einschüchterungsmechanismen im digitalen Raum.<sup>2</sup> In Deutschland ist ein deutlicher Anstieg digitaler Gewalt zu verzeichnen. Im Jahr 2024 wurden bereits 18.224 weibliche Opfer registriert.<sup>3</sup> Im Fünfjahresvergleich entspricht dies einer Zunahme um +110,6%.<sup>4</sup> Dunkelfeldstudien etwa von BMBFSJ, Bundesministerium des Innern (BMI) und Bundeskriminalamt (BKA) zeigen zudem, dass weniger als fünf Prozent der digitalen Gewalterfahrungen überhaupt zur Anzeige gebracht werden.<sup>5</sup>

Auch wenn in den letzten Jahren vermehrt Rechtsakte, wie etwa die EU-Gewaltschutz-Richtlinie<sup>6</sup> erlassen wurden, um digitale Gewalt zu adressieren, fehlt es nach wie vor an einem hinreichenden Verständnis der unterschiedlichen Erscheinungsformen digitaler Gewalt und deren weitreichenden, gravierenden Konsequenzen für Betroffene. Ein solches Verständnis ist jedoch unabdingbar, um auch hier für Gleichberechtigung zu sorgen und die Verpflichtungen Deutschlands nach internationalem und europäischem Recht umfassend und effektiv umzusetzen. Dies wirkt sich insbesondere auf den Zugang zu Recht in Fällen digitaler Gewalt aus.

Vor diesem Hintergrund wird im Folgenden zunächst der Begriff der geschlechtsspezifischen digitalen Gewalt eingeordnet und verschiedene Erscheinungsformen, die insbesondere in der sog. Manosphäre auftreten, benannt. Sodann wird der internationale und europäische Rechtsrahmen zum Schutz vor digitaler Gewalt und die sich daraus ergebenden staatlichen Handlungspflichten dargestellt. So lassen sich Umsetzungsdefizite und Schutzlücken im deutschen Recht aufzeigen. Daraus ergeben sich konkrete Vorschläge des djb, um einen tatsächlich effektiven Schutz Betroffener vor jeglichen Formen digitaler Gewalt zu erreichen.

---

<sup>1</sup> Vgl. Pressemitteilungen und Stellungnahmen des djb, jeweils abrufbar unter <https://www.djb.de/fokusthemen/digitale-gewalt> (zuletzt aufgerufen am 25.02.2026).

<sup>2</sup> Siehe hierzu bereits djb, Policy Paper: Das Netz als antifeministische Radikalisierungsmaschine, 09.09.2021, [https://www.djb.de/fileadmin/user\\_upload/presse/stellungnahmen/st21-18\\_Antifeminismus\\_im\\_Netz.pdf](https://www.djb.de/fileadmin/user_upload/presse/stellungnahmen/st21-18_Antifeminismus_im_Netz.pdf) (zuletzt aufgerufen am 25.02.2026).

<sup>3</sup> *Bundeskriminalamt*, Bundeslagebilder - Geschlechtsspezifisch gegen Frauen gerichtete Straftaten 2024, 20.01.2026, S. 33 f.

<sup>4</sup> *Ebd.*, S. 34.

<sup>5</sup> *Bundeskriminalamt*, Ergebnisse der Dunkelfeldstudie „Lebenssituation, Sicherheit und Belastung im Alltag (LeSuBiA)“, Themenheft I, 10.2.2026, abrufbar unter <https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2026/02/lesubia.html> (zuletzt aufgerufen am 25.02.2026), S. 101.

<sup>6</sup> Richtlinie 2024/1385 des Europäischen Parlaments und des Rates zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt, ABl. L.2024/1385, 24.05.2024.

## 2. Begriffliche Einordnung und Erscheinungsformen digitaler Gewalt

### I. Formen digitaler geschlechtsspezifischer Gewalt

Digitale Gewalt umfasst eine Vielzahl von Handlungen, die unter Nutzung digitaler Technologien, insbesondere sozialer Medien, Smartphones sowie zunehmend auch Künstlicher Intelligenz, begangen werden. Dabei handelt es sich nicht um ein einheitliches Delikt, sondern um ein breites Spektrum an Verhaltensweisen.<sup>7</sup>

Besonders hervorzuheben ist bildbasierte sexualisierte Gewalt, die sich in Form des nicht einvernehmlichen Aneignens, Anfertignens oder Erstellens intimer Aufnahmen, deren Verbreitung oder Verwendung ohne Zustimmung der betroffenen Person sowie die Androhung einer Veröffentlichung zeigen kann.<sup>8</sup> Eine zunehmend relevante Erscheinungsform stellen zudem sog. *Deepfakes* dar, bei denen mittels Künstlicher Intelligenz täuschend echte sexualisierte Bild- oder Videoaufnahmen generiert werden, um Betroffene zu erniedrigen, zu erpressen oder öffentlich zu diskreditieren.<sup>9</sup>

Digitale Gewalt kann so gravierende Auswirkungen auf die psychische und soziale Lebensrealität der Betroffenen entfalten. Sie steht zudem häufig in einem Zusammenhang mit Gewalt in intimen Beziehungen.<sup>10</sup>

Eine Sonderform ist die digitalisierte Gewalt. Dies ist die Verbreitung von Bild- und Videomaterial realer sexueller Übergriffe oder Vergewaltigungen und damit die nachträgliche digitale Verstärkung physischer Gewalt.<sup>11</sup>

### II. Geschlechtsspezifische Dimension und Intersektionalität

Die Opferzahlen verdeutlichen, dass digitale Gewalt in besonderer Weise geschlechtsspezifisch geprägt ist.<sup>12</sup> Die aktuellen Zahlen des Bundeskriminalamts zeigen, dass Frauen signifikant häufiger betroffen sind als Männer; im Verhältnis von 61,2 % zu 38,8 %<sup>13</sup>. So knüpft digitale Gewalt an patriarchale Machtstrukturen an und ist häufig durch Sexualisierung und Verdinglichung weiblicher Körper sowie durch gesellschaftliche Stigmatisierung der Betroffenen geprägt. Digitale Gewalt reproduziert damit bestehende geschlechtsspezifische Macht- und Kontrollverhältnisse im virtuellen Raum und wirkt als Verlängerung und Verstärkung struktureller Ungleichheiten.

Besonders betroffen sind zudem mehrfach diskriminierte Personen, deren Vulnerabilität sich aus dem Zusammenwirken verschiedener Diskriminierungsmerkmale ergibt, etwa aufgrund ihres Berufs –

<sup>7</sup> Bundeskriminalamt, Bundeslagebilder - Geschlechtsspezifisch gegen Frauen gerichtete Straftaten 2024, 20.01.2026, S. 32.

<sup>8</sup> Bildbasierte sexualisierte Gewalt umfasst Phänomene wie digitalen Voyeurismus, also das Aufnehmen von Nacktbildern oder sexualbezogenen Bildinhalten mittels bspw. Spy Cams, sowie Upskirting und Downblousing (das heimliche Fotografieren unter den Rock oder in den Ausschnitt), Sextortion und somit die Drohung, intime oder sexualisierte Aufnahmen Dritten zugänglich zu machen. Darunter fallen auch das Teilen einvernehmlich hergestellter intimer oder sexualisierter Aufnahmen ohne Einwilligung der abgebildeten Person sowie KI-generierte Aufnahmen (sog. Deep-Fakes); vgl. McGlynn/Rackley, Image-Based Sexual Abuse, Oxford Journal of Legal Studies Vol. 37:3 (2017) 534, 534; djb, Policy Paper: Bekämpfung bildbasierter sexualisierter Gewalt, 07.06.2023, <https://www.djb.de/presse/pressemitteilungen/detail/st23-17> (zuletzt aufgerufen am 25.02.2026).

<sup>9</sup> Aufsehen erregte in letzter Zeit dabei insbesondere der KI-Chatbot Grok von Elon Musks Plattform X; Frankfurter Allgemeine, Musks KI erzeugt immer noch sexualisierte Bilder, 03.02.2026, <https://www.faz.net/aktuell/feuilleton/medien-und-film/mediapolitik/grok-erzeugt-weiter-sexualisierte-bilder-200502477.html> (zuletzt aufgerufen am 25.02.2026).

<sup>10</sup> Amnesty International, Amnesty reveals alarming impact of online abuse against women, 2019, [www.amnesty.org/en/latest/press-release/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women](https://www.amnesty.org/en/latest/press-release/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women) (zuletzt aufgerufen am 25.02.2026).

<sup>11</sup> Bundeskriminalamt, Bundeslagebilder - Geschlechtsspezifisch gegen Frauen gerichtete Straftaten 2024, 20.01.2026, S. 32.

<sup>12</sup> So auch GREVIO, General Recommendation No. 1 on the digital dimension of violence against women, GREVIO(2021)20, 2021.

<sup>13</sup> Bundeskriminalamt, Bundeslagebilder - Geschlechtsspezifisch gegen Frauen gerichtete Straftaten 2024, 20.01.2026, S. 34.

Politikerinnen und andere Personen des öffentlichen Lebens – oder in Überschneidung mit Rassismus, Queerfeindlichkeit und Ableismus. Auch im digitalen Raum fehlt es in Deutschland jedoch an einer disaggregierten Datenerhebung und damit an der präzisen Erfassung intersektionaler Betroffenheiten, sodass spezifische Risikolagen vielfach unsichtbar bleiben, was die Entwicklung gezielter Schutz- und Präventionsmaßnahmen erschwert.

### III. Die Manosphäre

Zunehmend relevant für die Verbreitung digitaler geschlechtsspezifischer Gewalt ist die sog. Manosphäre.<sup>14</sup> Darunter werden lose verbundene Online-Communities verstanden, in denen misogynie Narrative verbreitet und tradierte Geschlechterrollen insbesondere mit einer aggressiven Männlichkeit und untergeordneten Weiblichkeit verfestigt werden. Diese Räume fungieren häufig auch als Orte der politischen Radikalisierung im autoritären Spektrum und tragen zur Normalisierung frauenfeindlicher Ideologien bei.

In diesen digitalen Milieus werden antifeministische Deutungsmuster verstärkt, wird Gleichstellungspolitik delegitimiert und Frauen werden pauschal als Bedrohung männlicher Identität konstruiert. Die dort verbreiteten Narrative knüpfen nicht selten an gesellschaftliche Polarisierungsdynamiken an und stabilisieren Vorstellungen von männlicher Anspruchs- und Kontrollberechtigung.<sup>15</sup>

Die Manosphäre trägt damit zur ideologischen Fundierung geschlechtsspezifischer Gewalt bei, indem sie Misogynie normalisiert. In ihrer extremsten Form können solche digitalen Radikalisierungsräume zum Nährboden für eine Entgrenzung von Gewalt werden.<sup>16</sup>

## 3. Internationaler und europäischer Rechtsrahmen

### I. UN-Frauenrechtskonvention

Die UN-Frauenrechtskonvention<sup>17</sup> (CEDAW) erwähnt digitale Gewalt nicht ausdrücklich, doch stellte der zuständige CEDAW-Ausschuss früh klar, dass jede Form geschlechtsbasierter Gewalt gegen Frauen als Diskriminierung im Sinne von Art. 1 CEDAW gilt. Darunter versteht er jede Form der Gewalt, die sich gegen Frauen richtet, weil sie Frauen sind, oder die sie unverhältnismäßig betrifft.<sup>18</sup> In seiner Allgemeinen Empfehlung Nr. 35 (2017) betonte der Ausschuss, dass solche Gewalt in allen Lebensbereichen vorkommt – auch in technologisch vermittelten und digitalen Räumen. Er verweist dabei ausdrücklich auf Online-Gewalt und stellt klar, dass diese sowohl von Staaten als auch von privaten oder nichtstaatlichen Akteuren, auch extraterritorial, ausgehen kann.<sup>19</sup>

Damit ist geschlechtsbasierte Gewalt gegen Frauen im digitalen Raum als Diskriminierung im Sinne des Art. 1 CEDAW anzusehen und löst die in Art. 2 der Konvention geregelten Pflichten aus. Danach haben die Konventionsstaaten mit allen geeigneten Mitteln und ohne Verzögerung eine Politik zur Beseitigung der Diskriminierung von Frauen, einschließlich geschlechtsspezifischer Gewalt gegen Frauen, zu

---

<sup>14</sup> Zur Übersicht siehe UN Women, Die Manosphäre – HeForShe als feministischer Gegenpol, Oktober 2025, <https://unwomen.de/heforshe-themen-manosphaere/> (zuletzt aufgerufen am 25.02.2026).

<sup>15</sup> Vgl. zu dieser Problematik auch bereits ausführlich djB, Policy Paper: Das Netz als antifeministische Radikalisierungsmaschine, 09.09.2021, [https://www.djb.de/fileadmin/user\\_upload/presse/stellungnahmen/st21-18\\_Antifeminismus\\_im\\_Netz.pdf](https://www.djb.de/fileadmin/user_upload/presse/stellungnahmen/st21-18_Antifeminismus_im_Netz.pdf) (zuletzt aufgerufen am 25.02.2026).

<sup>16</sup> Ebd.

<sup>17</sup> Convention on the Elimination of the Discrimination against Women, U.N.T.S. Vol. 1249 (1979), S. 13, BGBl. 1985 II Nr. 17, 647.

<sup>18</sup> CEDAW Committee, General Recommendation No. 19: Violence against Women (1992), A/47/38, Rn. 6.

<sup>19</sup> CEDAW Committee, General Recommendation No. 35 on gender-based violence against women, updating general recommendation No. 19 (26 July 2017), UN Doc. CEDAW/C/GC/35, Rn. 20.

verfolgen.<sup>20</sup> Dazu gehört, das Verhalten privater Akteure zu regulieren sowie effektiven Rechtsschutz zu ermöglichen.<sup>21</sup> Dabei empfiehlt der Ausschuss unter anderem, Hindernisse bei der Sammlung von Beweisen für Verletzungen der Rechte von Frauen abzubauen, die online und durch die Nutzung von Informations- und Kommunikationstechnik und neuen sozialen Medien begangen werden.<sup>22</sup>

## II. UN-Übereinkommen gegen Cyberkriminalität

Zudem verpflichtet das UN-Übereinkommen gegen Cyberkriminalität<sup>23</sup> die Vertragsstaaten, erforderliche Maßnahmen gegen den Verkauf, die Verbreitung, die Übermittlung, die Veröffentlichung oder die sonstige Bereitstellung eines intimen Bildes einer Person mittels eines Informations- und Kommunikationstechnologiesystems, ohne die Zustimmung der abgebildeten Person unter Strafe zu stellen, sofern diese Handlungen vorsätzlich und widerrechtlich begangen wurden (Art. 16 (1)). Die Konvention ist noch nicht in Kraft getreten; dies erfolgt 90 Tage nachdem vierzig Staaten das Instrument ratifiziert haben.<sup>24</sup>

## III. Europäische Menschenrechtskonvention

Die Europäische Menschenrechtskonvention<sup>25</sup> (EMRK) enthält ebenfalls keine explizite Regelung zu digitaler Gewalt. Doch legt der Gerichtshof die Konvention nach der *living-instrument*-Doktrin<sup>26</sup> auch mit Blick auf technologische Entwicklungen dynamisch aus.<sup>27</sup> Es ist also davon auszugehen, dass auch digitale Gewalt von den Normen erfasst ist, die Staaten zum Schutz vor Gewalt verpflichten.

Die Menschenrechte der EMRK stellen dabei insbesondere nicht nur Abwehrrechte des Individuums gegen den Staat dar, sondern verpflichten die Konventionsstaaten auch dazu, Privatpersonen konkret zu schützen.<sup>28</sup> Die Verletzung eines Konventionsrechts liegt insoweit vor, wenn ein Staat es unterlässt, dieser Schutzpflicht nachzukommen.<sup>29</sup> Nach der Rechtsprechung des EGMR bestehen hinsichtlich Gewalt nach Art. 2, 3 und 8 EMRK (Recht auf Leben, Folterverbot und Recht auf Privatsphäre) prozedurale Pflichten nationaler Behörden, erstens einen legislativen Rahmen zu schaffen, zweitens hinreichende Schutzmaßnahmen zu ergreifen und drittens strafrechtlicher Ermittlungen aufzunehmen.<sup>30</sup>

Der Gerichtshof hat auch in mehreren Fällen digitaler Gewalt solche Pflichten anerkannt: Im Fall *Buturugă v. Rumänien* befand der Gerichtshof erstmals, dass digitale Gewalt in Form von Cybermobbing einen Aspekt von häuslicher Gewalt darstellt und sah eine Verletzung von Art. 3 und

---

<sup>20</sup> Ebd., Rn. 21.

<sup>21</sup> Art. 2(e) CEDAW; CEDAW Committee, General Recommendation No. 35 on gender-based violence against women, updating general recommendation No. 19 (26 July 2017), UN Doc. CEDAW/C/GC/35, Rn. 24.

<sup>22</sup> CEDAW Committee, General Recommendation No. 33 on women's access to justice (3 August 2015), UN Doc. CEDAW/C/GC/33, Rn. 25.

<sup>23</sup> United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes, enthalten in United Nations (UN) Generalversammlung, Resolution 79/243 (24 Dezember 2024), UN Doc. A/RES/79/243.

<sup>24</sup> Die Europäische Union (EU) hat die Konvention unterzeichnet und den Mitgliedstaaten empfohlen, ihr darin zu folgen, siehe Rat der Europäischen Union, Beschluss (EU) des Rates 2025/2307 vom 13. Oktober 2025 über die Unterzeichnung – im Namen der Europäischen Union – des Übereinkommens der Vereinten Nationen gegen Cyberkriminalität, ABl. L 2025/2307 (11.11.2025) Erwägungsgrund (20). Deutschland ist dem jedoch bisher nicht nachgekommen.

<sup>25</sup> Convention for the Protection of Human Rights and Fundamental Freedoms, ETS No. 005, 03.09.1953, BGBl. II 1952, 685.

<sup>26</sup> Erstmals EGMR, *Tyrer v. Vereinigtes Königreich*, Nr. 5856/72, 1978.

<sup>27</sup> Zur Übersicht siehe EGMR, *Guide to the Case-Law of the European Court of Human Rights Data protection*, (Stand 31.08.2025), [https://ks.echr.coe.int/documents/d/echr-ks/guide\\_data\\_protection\\_eng](https://ks.echr.coe.int/documents/d/echr-ks/guide_data_protection_eng) (zuletzt aufgerufen am 25.02.2026).

<sup>28</sup> Ausführlich dazu siehe Stoyanova, *Positive Obligations under the European Convention on Human Rights: Within and Beyond Boundaries*, 2023.

<sup>29</sup> In Bezug auf den digitalen Raum kann diese Pflicht auch verletzt sein, wenn der Gesetzgeber inaktiv bleibt und keine adäquaten Gesetze erlässt. Dazu gehört beispielsweise die Strafbarkeit des Filmens Minderjähriger, EGMR, *Söderman v. Schweden*, Nr. 5786/08, 2013, Rn. 117, oder die Identifizierungspflicht des Internetproviders im Falle anstößiger Werbung auf einer Datingplattform gegenüber Minderjährigen, EGMR, *K.U. v. Finnland*, Nr. 2872/02, 2008, Rn. 49.

<sup>30</sup> EGMR, *X et al. v. Bulgarien*, Große Kammer, Nr. 22457/16, 2021, Rn. 178; EGMR, *Botoyan v. Armenien*, Nr. 5766/17, 2022, Rn. 91 ff.

Art. 8 EMRK.<sup>31</sup> In *Volodina v. Russland (Nr. 2)* aus 2021 entschied der EGMR, dass die Untätigkeit der Behörden bei der wiederholten Erstellung von Fake-Profilen durch den Ehemann der Beschwerdeführerin in ihrem Namen, die Veröffentlichung ihrer Intimfotos, der Verfolgung ihrer Bewegung mittels GPS-Tracker und Todesdrohungen via sozialen Medien einen Verstoß gegen Art. 8 darstelle.<sup>32</sup> Im Verfahren *M.Ş.D. v. Rumänien* aus 2024 befand der EGMR, dass auch die Verbreitung von *revenge pornography* (Intimfotos und/oder -videos einer früheren Intimpartnerin gegen deren Willen) eine Schutzpflicht in Gestalt eines legislativen Rahmens und effektiver strafrechtlicher Ermittlungen begründet.<sup>33</sup>

Insgesamt erkennt der Gerichtshof damit digitale Gewalt als eine Form von Gewalt gegen Frauen und Mädchen an, die in engem Zusammenhang zu körperlicher Gewalt stehen kann und Schutzpflichten der Staaten begründet.<sup>34</sup>

#### IV. Istanbul-Konvention

Das Übereinkommen zur Verhütung und Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt des Europarats<sup>35</sup> (Istanbul-Konvention) stellt das bislang umfassendste völkerrechtliche Instrument zur Bekämpfung geschlechtsspezifischer Gewalt in Europa dar. Die Istanbul-Konvention versteht Gewalt gegen Frauen als eine Form geschlechtsspezifischer Gewalt, die strukturell in gesellschaftlichen Machtverhältnissen verankert ist und Frauen aufgrund ihres Geschlechts unverhältnismäßig betrifft.<sup>36</sup> Insbesondere fasst die Konvention Gewalt realistisch, indem sie ausdrücklich über körperliche Gewalt hinausgeht und auch psychische, sexualisierte sowie ökonomische Gewaltformen einbezieht.<sup>37</sup> Damit bietet die Konvention einen normativen Rahmen, der auch für digitale Erscheinungsformen geschlechtsspezifischer Gewalt von zentraler Bedeutung ist.

Die Istanbul-Konvention verfolgt zudem einen ganzheitlichen Ansatz: Sie verpflichtet die Vertragsstaaten nicht nur zur Strafverfolgung, sondern auch zu umfassenden Präventions-, Schutz- und Unterstützungsmaßnahmen.<sup>38</sup> Dabei kommt der in Art. 5 verankerten staatlichen Sorgfaltspflicht (*due diligence*) eine besondere Bedeutung zu, wonach die Vertragsstaaten auch geschlechtsspezifische Gewalt durch Private wirksam verhüten, untersuchen, sanktionieren und wiedergutmachen müssen. Gerade im digitalen Kontext wird geschlechtsspezifische Gewalt häufig durch private Nutzer\*innen digitaler Plattformen ausgeübt.<sup>39</sup>

In Konkretisierung von Art. 5 verpflichtet Art. 33 die Vertragsstaaten, vorsätzliche Handlungen unter Strafe zu stellen, die durch Zwang oder Drohungen schwerwiegende psychische Beeinträchtigungen verursachen. Diese Norm eröffnet wichtige Anknüpfungspunkte für digitale Gewaltformen, bei denen

---

<sup>31</sup> EGMR, *Buturugă v. Rumänien*, Nr. 56867/15, 2020, Rn. 74. Die Beschwerdeführerin zeigte ihren Ex-Partner wegen körperlicher Gewalt an und wies die Behörden explizit darauf hin, auch den Familiencomputer zu durchsuchen. Der Ex-Partner hatte sich gegen ihren Willen in ihre Konten, u.a. Facebook, eingeloggt und private Nachrichten, Dokumente und Fotos gespeichert. Der Gerichtshof betonte, dass die Behörden bei ihren Ermittlungen jegliche Form von Gewalt, auch digitale Gewalt, hätten berücksichtigen müssen, ebd., Rn. 74-78.

<sup>32</sup> EGMR, *Volodina v. Russland*, Nr. 40419/19, 2021.

<sup>33</sup> EGMR, *M.Ş.D. v. Rumänien*, Nr. 28935/21, 2024, Rn. 158.

<sup>34</sup> Ebd., Rn. 118-120.

<sup>35</sup> Convention on preventing and combating violence against women and domestic violence, U.N.T.S. Vol. 3010 (2014), S. 107, BGBl. 2017 II, S. 1026 f., 2018 II, S. 119.

<sup>36</sup> Siehe Präambel der Istanbul Konvention.

<sup>37</sup> Im Sinne dieses Übereinkommens wird der Begriff „Gewalt gegen Frauen“ als eine Menschenrechtsverletzung und eine Form der Diskriminierung der Frau verstanden und bezeichnet alle Handlungen geschlechtsspezifischer Gewalt, die zu körperlichen, sexuellen, psychischen oder wirtschaftlichen Schäden oder Leiden bei Frauen führen oder führen können, einschließlich der Androhung solcher Handlungen, der Nötigung oder der willkürlichen Freiheitsentziehung, sei es im öffentlichen oder privaten Leben, Art. 3 lit. a Istanbul-Konvention.

<sup>38</sup> Art. 4 Abs. 2, Art. 5 ff., Art. 12 ff., Art. 18 ff., Art. 49 ff. der Istanbul Konvention.

<sup>39</sup> Council of Europe, Explanatory Report to the Council of Europe Convention on preventing and combating violence against women and domestic violence, Rn. 57-60.

Betroffene häufig nicht körperlich verletzt werden, jedoch durch fortgesetzte Überwachung, Bedrohungen oder öffentliche Diffamierung erheblichen psychischen Belastungen ausgesetzt sind.<sup>40</sup>

Darüber hinaus sind die Vertragsstaaten nach Art. 34 verpflichtet, vorsätzliches, wiederholtes Nachstellen unter Strafe zu stellen, sofern dies bei der betroffenen Person ernsthafte Furcht auslöst. Die Konvention selbst differenziert dabei nicht zwischen analogen und digitalen Handlungsformen. In der Auslegung durch die Expert\*innengruppe zur Umsetzung der Istanbul-Konvention (GREVIO) wird jedoch betont, dass Nachstellung auch unter Einsatz digitaler Kommunikationsmittel erfolgen kann.<sup>41</sup> Digitale Überwachung, wiederholte Kontaktaufnahmen über Kommunikationsplattformen oder das systematische Beobachten von Online-Aktivitäten können daher in den Anwendungsbereich der Norm fallen. Daneben verpflichtet Art. 40 die Staaten zur Sanktionierung sexualisierter Belästigung. Diese erfolgt heutzutage gerade in sozialen Medien und digitalen Räumen und entfaltet dort spezifische Dynamiken der Entgrenzung und Verstärkung.

Die Vertragsstaaten sind nach Art. 17 ferner dazu verpflichtet, den privaten Sektor, insbesondere Informations- und Kommunikationstechnologieunternehmen, zur Mitwirkung an der Prävention von Gewalt gegen Frauen anzuhalten. Damit wird anerkannt, dass digitale Plattformen nicht nur Tatorte, sondern als regulierungsrelevante Akteure im Kontext geschlechtsspezifischer Gewalt ebenfalls in präventive Strategien einzubeziehen sind.<sup>42</sup>

Digitale Gewalt ist jedoch nicht allein als strafrechtliches Problem zu behandeln. Auch die weiteren Präventions- und Schutzpflichten der Konvention sind auf den digitalen Raum anwendbar. Insbesondere müssen die Staaten einen ausreichenden Zugang zu Rechtsberatung gewährleisten.<sup>43</sup> Daneben verpflichtet Art. 11 die Staaten zur Erhebung aufgeschlüsselter Daten zu geschlechtsspezifischer Gewalt. Insgesamt stellt die Istanbul-Konvention somit einen wichtigen Referenzrahmen dar, um digitale geschlechtsspezifische Gewalt sichtbar zu machen, rechtlich einzuordnen und wirksam zu bekämpfen.

## V. Europäische Union

### 1. EU-Gewaltschutz-Richtlinie

Die EU-Gewaltschutz-Richtlinie<sup>44</sup> ist der erste umfassende Rechtsakt der EU zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt und schafft dafür einen unionsweit einheitlichen Rechtsrahmen. Die Richtlinie enthält Vorgaben im Bereich des Strafrechts, des Zugangs zur Justiz, des Opferschutzes, der Opferhilfe, der Prävention und Intervention sowie zur Koordinierung und Zusammenarbeit. Der Begriff der Gewalt gegen Frauen ist auch hier realistisch gefasst. Er umfasst nach Art. 2 lit. a insbesondere Handlungen, die zu körperlichen, sexuellen, psychischen oder wirtschaftlichen Schäden oder Leiden führen oder führen können.

Die Richtlinie nennt auch Gewalthandlungen mit digitalem Bezug, die die Mitgliedstaaten unter Strafe stellen müssen. Dazu gehören die Verbreitung intimer oder sexueller Bilder oder Videos sowie die Erstellung und Verbreitung manipulierten Bildmaterials, unter anderem *Deepfakes* (Art. 5),

---

<sup>40</sup> GREVIO, General Recommendation No. 1 on the digital dimension of violence against women, GREVIO(2021)20, 2021, Rn. 42-44.

<sup>41</sup> Ebd., Rn. 32.

<sup>42</sup> Council of Europe, Explanatory Report to the Council of Europe Convention on preventing and combating violence against women and domestic violence, Rn. 106-109.

<sup>43</sup> GREVIO, General Recommendation No. 1 on the digital dimension of violence against women, GREVIO(2021)20, 2021, Rn. 57.

<sup>44</sup> Richtlinie (EU) 2024/1385 des Europäischen Parlaments und des Rates vom 14. Mai 2024 zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt, ABl. L 2024/1385, 24.05.2024 (nachfolgend EU-Gewaltschutz- Richtlinie).

Cyberstalking (Art. 6), Cybermobbing (Art. 7) und die Aufstachelung zur Gewalt oder Hass gegenüber einer geschlechtlich definierten Gruppe oder einzelner Mitglieder im Internet (Art. 8).

Darüber hinaus besteht nach Art. 23 die staatliche Pflicht, dafür zu sorgen, Inhalte, die auf strafrechtlich relevante Weise ins Internet gelangt sind, zu löschen oder die entsprechenden Accounts zu sperren. Nach Art. 11 sollen die Mitgliedstaaten sicherstellen, dass bei der Strafzumessung hinsichtlich der in den Art. 3 bis 8 verankerten Straftaten erschwerende Umstände berücksichtigt werden können. Erschwerende Umstände sind auch die sexuelle Orientierung und das Geschlecht.

Art. 34 sieht ferner die Pflicht zu Präventivmaßnahmen vor. Dabei adressiert Abs. 8 explizit Maßnahmen gegen digitale Gewalt, zum Beispiel die Vermittlung digitaler Kompetenzen. Hervorzuheben ist, dass die Richtlinie in Art. 2 lit. g vorsieht, dass auch „abhängige Personen“, worunter etwa Kinder des Opfers fallen, dieselben Schutzmaßnahmen wie die Opfer selbst erhalten sollen.<sup>45</sup>

Zudem schreibt Art. 12 (3) vor, dass die gerichtliche Zuständigkeit schon dadurch begründet wird, dass von einem Staatsgebiet aus auf die Inhalte im Internet zugegriffen wird, unabhängig davon, wo der Hostingdienst ansässig ist oder in welchem Land das Material hochgeladen wurde. Auf diese Weise sollen Zuständigkeitslücken im Bereich der Cyberkriminalität vermieden werden.

## 2. Digital Services Act

Der Digital Services Act (DSA)<sup>46</sup> ist die zentrale europäische Verordnung zur Regulierung aller in der Europäischen Union tätigen Online-Dienste. Ziel des DSA ist es, digitale Räume sicherer zu machen, Grundrechte zu schützen und systematische Risiken wie Hass, Desinformation und geschlechtsspezifische Gewalt zu reduzieren. Hierfür regelt der DSA digitale Rechte von Nutzenden auf Online-Plattformen. Dazu gehören die Transparenz bei der Entfernung von Inhalten und die Optionen zur Anfechtung von Entscheidungen über die Moderation von Inhalten (Art. 20), die einfache Meldung rechtswidriger Inhalte (Art. 16) sowie der verbesserte Schutz für Minderjährige (Art. 28).

Gerade große Online-Plattformen müssen weitverbreitete Risiken identifizieren und analysieren. Dazu gehört nach Art. 34 insbesondere auch geschlechtsspezifische Gewalt, zudem der Jugendschutz sowie körperliches und geistiges Wohlbefinden. Wurden diese Risiken erkannt, ist der Betreiber der Plattform nach Art. 35 gehalten, sie durch geeignete Maßnahmen zu verringern.

## 3. Datenschutzgrundverordnung

Die Datenschutzgrundverordnung (DSGVO) enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten in der Europäischen Union. Im Dezember 2025 entschied der EuGH mit dem Urteil *Russmedia Digital*<sup>47</sup>, dass Plattformen direkt in Anspruch genommen werden können, um eine Löschung personenbezogener Daten aus dem Internet zu bewirken. Anbieter müssen ihre digitalen Dienste so gestalten, dass Risiken jedenfalls für besonders sensible Daten begrenzt werden.

---

<sup>45</sup> Erwägungsgrund (41) EU-Gewaltschutz-Richtlinie.

<sup>46</sup> Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste), ABl. L 277, 27.10.2022, S. 1.

<sup>47</sup> EuGH, Urteil v. 2.12.2025 - C-492/23, *Russmedia Digital and Inform Media Press*, ECLI:EU:C:2025:935.

## 4. Nationaler Rechtsrahmen in Deutschland

### I. Strafrecht

Das Strafrecht ermöglicht durch Tatbestände wie Beleidigung (§ 185 StGB), Bedrohung (§ 241 StGB), Nachstellung (§ 238 StGB), Pornografiedelikte (§§ 184 ff. StGB), Verletzung des höchstpersönlichen Lebensbereichs (§ 201a StGB) und das Recht am eigenen Bild (§§ 33 KUG) die Verfolgung von Straftaten mit misogynen Beweggründen auch im digitalen Raum. 2021 hat der Gesetzgeber zum Schutz vor geschlechtsspezifischer Gewalt zudem den Straftatbestand der Bedrohung um die Drohung mit einer rechtswidrigen Tat gegen die sexuelle Selbstbestimmung (§ 241 Abs. 1 StGB) erweitert.

Minderjährige sollen vor der sexualbezogenen Wiedergabe in digitalen Inhalten durch die Pornografiedelikte in den §§ 184b, 184c StGB geschützt werden. Neben der Verbreitung und dem Öffentlich-Zugänglichmachen sind insbesondere das Herstellen von Inhalten, die ein tatsächliches Geschehen wiedergeben (reale Inhalte), das Zugänglichmachen oder Besitzverschaffen an andere, sowie der Abruf und das Besitzverschaffen an sich selbst in Bezug auf reale und wirklichkeitsnahe Inhalte verboten. Hinzu kommt mit § 201a Abs. 3 StGB das Verbot, eine Bildaufnahme, die eine minderjährige Person nackt wiedergibt, herzustellen oder anzubieten, um sie einer dritten Person gegen Entgelt zu verschaffen (Nr. 1) oder eine solche Bildaufnahme sich oder einer dritten Person gegen Entgelt verschafft (Nr. 2). Allerdings gibt es eine Regelungslücke: Hier fehlt ein Verbot, (neutrales) Bildmaterial zwecks Herstellung eines *Deepfakes* zu manipulieren.

Zudem fehlt eine vergleichbar weitgehende Regelung zum Schutz Erwachsener. Bildbasierte sexualisierte Gewalt gegen Erwachsene wird bislang nicht als eigens zu regelndes Phänomen angesehen, sondern eher zufällig und nur teilweise in unterschiedlichen Regelungsbereichen erfasst.

### II. Zivilrecht

Der zivilrechtliche Rechtsrahmen gegen bildbasierte Gewalt unterscheidet zwischen dem öffentlichen Zugänglichmachen von Bildaufnahmen einerseits und anderen Formen des unbefugten Gebrauchs (Herstellen, Besitz, privater Weitergabe und Manipulation) andererseits. Das Verbreiten oder öffentlich zur Schau stellen ohne Einwilligung von Bildnissen, auf denen die betroffene Person erkennbar abgebildet ist, ist zivilrechtlich von §§ 823 Abs. 2 iVm §§ 22, 23 Kunsturhebergesetz (KUG) gedeckt und stellt – soweit kein Rechtfertigungsgrund des § 23 Abs 1 KUG vorliegt – eine Verletzung des Rechts am eigenen Bild dar. Im Falle anderer Formen des unbefugten Gebrauchs ist jedoch die Rechtswidrigkeit des Eingriffs in das Allgemeine Persönlichkeitsrecht als Rahmenrecht nicht über § 823 Abs. 2 BGB indiziert, sodass eine Abwägung der widerstreitenden Interessen im Einzelfall nach § 823 Abs. 1 BGB erfolgen muss.<sup>48</sup> Gleiches gilt für Fälle nicht bildbasierter Gewalt, die in die Privatsphäre eingreifen.

Bei *Deepfakes* handelt es sich zivilrechtlich um eine bildliche Lüge, deren Verbreiten und öffentliches zur Schau stellen grundsätzlich der Einwilligung bedarf. Das oben Gesagte gilt hier auch. Allerdings kann die Einordnung als bildliche Lüge entfallen, wenn *Deepfakes* als solche gekennzeichnet werden. Auch hier ergibt sich also eine Schutzlücke. Was daneben aber bleibt ist eine Verletzung des Persönlichkeitsrechts durch die Manipulation. Im Falle sexualisierter Deepfake ist dies regelmäßig die Intimsphäre.

---

<sup>48</sup> djb, Policy Paper: Bekämpfung bildbasierter sexualisierter Gewalt, 07.06.2023, <https://www.djb.de/presse/pressemitteilungen/detail/st23-17> (zuletzt aufgerufen am 25.02.2026), S. 10.

Zivilrechtliche Folgen bei Verstößen sind vor allem Unterlassungs- und Beseitigungsansprüche (Löschung). Schadensersatzansprüche können grundsätzlich nur bei kommerzieller Nutzung geltend gemacht werden. Eine Geldentschädigung kommt nur im Fall von schwerwiegenden Beeinträchtigungen des Persönlichkeitsrechts in Betracht.

Zur Verfolgung dieser zivilrechtlichen Ansprüche bedarf es gegenüber anonymen Personen entsprechender Auskunftsansprüche. Doch greift der Anspruch auf Auskunft über vorhandene Bestandsdaten nach § 21 Abs. 2 des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten (TDDDG) gegenüber Anbietern von digitalen Diensten derzeit nur für den Fall, dass die Inhalte die von § 21 Abs. 2 genannten Straftatbestände erfüllen bzw. bei Verletzung absolut geschützter Rechte durch rechtswidrige audiovisuelle Inhalte.

Darüber hinaus sind weitere Schutzlücken zu verzeichnen: So ermöglicht das Bekanntwerden von Wohnadressen verschiedene Formen von Gewalt – von ungewollten Online-Bestellungen über die Versendung von Drohbriefen bis hin zu Stalking oder sogar körperlicher Gewalt am Wohnort. Im Prozessrecht, bei der Impressumspflicht sowie im Melderegisterrecht wird das nicht angemessen adressiert.

Prozessual erachten Gerichte derzeit nur in seltenen Ausnahmefällen die Angabe von c/o-Adressen als zulässig, selbst in Verfahren, in denen es um (digitale) Gewalt geht. Die damit bestehende Gefahr der Adressbekanntgabe kann Betroffene abschrecken, tatsächlich Rechtsschutz zu suchen.

Noch weitergehend zwingt die Impressumspflicht potenziell Betroffene von digitaler Gewalt zur Offenbarung von Adressdaten im Internet. Dies gilt nach § 5 Digitale-Dienste-Gesetz für sämtliche Betreiber von Websites oder Profilen in sozialen Medien, die nicht rein privater Natur sind, sowie nach § 18 des Medienstaatsvertrags für Anbieter journalistisch-redaktioneller Angebote. Besonders für Solo-Selbständige, freischaffende Journalist\*innen und politisch aktive Bürgerinnen und Bürger kann dies abschreckende Wirkung entfalten, überhaupt als Stimme im digitalen Raum aufzutreten.

Problematisch ist auch die aktuelle Regelung der Melderegisterauskunft. Zum einen ist eine Adresse beim Einwohnermeldeamt leicht zu erlangen (§§ 44, 45 Bundesmeldegesetz), zum anderen werden an eine Meldesperre nach § 51 Bundesmeldegesetz sehr hohe Anforderungen gestellt und diese bundesweit sehr uneinheitlich gehandhabt, was die Vulnerabilität potenziell Betroffener für digitale und analoge Gewalt vom Zufall des Wohnorts abhängig macht.

## 5. Sachgerechte Forderungen des djb

### I. Schließung gesetzlicher Schutzlücken

Der strafrechtliche Schutz vor digitaler Gewalt ist derzeit lückenhaft und fragmentarisch.<sup>49</sup> Der Schutz vor bildbasierter sexualisierter Gewalt, insbesondere bei erwachsenen Betroffenen, durch das StGB und KUG ist unzureichend. Das gilt insbesondere für *deepfakes*. Sinnvoll ist es daher ein einheitlicher Regelungskomplex von Straftatbeständen innerhalb des Sexualstrafrechts und außerhalb des Pornografiestrafrechts, der das unbefugte Herstellen, Gebrauchen, Zugänglichmachen und

---

<sup>49</sup> Vgl. dazu bereits die Forderungen des djb, Policy Paper: Das Netz als antifeministische Radikalisierungsmaschine, 09.09.2021, [https://www.djb.de/fileadmin/user\\_upload/presse/stellungnahmen/st21-18\\_Antifeminismus\\_im\\_Netz.pdf](https://www.djb.de/fileadmin/user_upload/presse/stellungnahmen/st21-18_Antifeminismus_im_Netz.pdf), S. 9 ff.; djB, Policy Paper: Bekämpfung bildbasierter sexualisierter Gewalt, 07.06.2023, [https://www.djb.de/fileadmin/user\\_upload/presse/stellungnahmen/st23-17\\_Bildbasierte\\_Gewalt.pdf](https://www.djb.de/fileadmin/user_upload/presse/stellungnahmen/st23-17_Bildbasierte_Gewalt.pdf), S. 4 ff.; djB, Policy Paper: Sexualisierte Gewalt - Schutzlücken und Reformbedarfe, 18.11.2024, [https://www.djb.de/fileadmin/user\\_upload/presse/stellungnahmen/st24-39\\_Sexualisierte\\_Gewalt.pdf](https://www.djb.de/fileadmin/user_upload/presse/stellungnahmen/st24-39_Sexualisierte_Gewalt.pdf) (jeweils zuletzt aufgerufen am 25.02.2026) S. 9 ff.

Manipulieren von Bildaufnahmen unter Strafe stellt, die eine andere erwachsene Person nackt oder sexualbezogen wiedergeben. Die Strafraumen sollten abgestuft nach dem Unrechtsgehalt verhältnismäßig bestimmt werden.<sup>50</sup>

Auch das sog. *Doxing*, die unbefugte Veröffentlichung privater Daten Dritter, was häufig als Begleitakt zu der Weitergabe oder Veröffentlichung sexualbezogener persönlicher Bildaufnahmen geschieht, ist strafrechtlich zu regeln, da die vorhandenen Tatbestände in StGB und BDSG keinen ausreichenden Schutz bieten.<sup>51</sup> Hier bedarf es einer eigenständigen, konsistenten und umfassenden Regelung.<sup>52</sup>

Das Schließen strafrechtlicher Schutzlücken ermöglicht über § 823 II BGB zugleich mehr Schutz auf zivilrechtlicher Ebene, insbesondere Unterlassungs- und Beseitigungsansprüche. Darüber hinaus sollen Persönlichkeitsrechtsverletzungen unterhalb der strafrechtlichen Erheblichkeit zumindest Unterlassungs- und Beseitigungsanspruch auslösen, wobei in der Abwägung widerstreitender Interessen das Persönlichkeitsrecht in Fällen digitaler Gewalt hoch zu gewichten ist, sodass es in der Regel die Interessen des Herstellers oder Besitzers von (manipulierten) Bildern überwiegt. Zu regeln ist insbesondere, dass ein Anspruch auf Löschung auch ursprünglich mit Einwilligung hergestellte sexualisierte Bildaufnahmen und *Deepfakes* betreffen kann, wenn die Einwilligung widerrufen wird.

Um effektive Rechtsverfolgung zu ermöglichen, muss zudem der Auskunftsanspruch nach § 21 Abs. 2 TDDDG um die Tatbestände der § 240 StGB, § 253 StGB, § 202a StGB sowie ggf. § 33 KUG und § 42 BDSG (Veröffentlichung personenbezogener Daten) erweitert werden.<sup>53</sup> Darüber hinaus darf die Möglichkeit des Auskunftsanspruchs bei zivilrechtlichen Ansprüchen wegen der Verletzung absolut geschützter Rechte nicht auf audiovisuelle Inhalte beschränkt sein, sondern sämtliche Formen der digitalen Gewalt umfassen.

Der djb fordert insbesondere zugunsten des wirksamen Schutzes von Frauen vor digitaler Gewalt die Einführung richterlich angeordneter Accountsperrern. Aktuell sehen weder der nationale noch der europäische Rechtsrahmen eine Möglichkeit zu richterlich angeordneten Accountsperrern vor. Digitale Gewalt wird oft von anonymen Accounts ausgeübt. Mit Ausnahme von – häufig genug ergebnislos eingestellten – strafrechtlichen Ermittlungsverfahren, gibt es keine Möglichkeit herauszufinden, wer verantwortlich für den Account ist, um gegen diese Person zivilrechtlich vorzugehen.<sup>54</sup> Um diese Schutzlücke zu füllen, sollten richterlich angeordneten Accountsperrern bei digitaler Gewalt eingeführt werden. Die Sperren sind dabei nicht auf anonyme Accounts zu beschränken, sondern auch auf Accounts, die wiederholte Rechtsverletzungen vornehmen. Da die Accountsperrere ein erheblicher

---

<sup>50</sup> djb, Policy Paper: Bekämpfung bildbasierter sexualisierter Gewalt, 07.06.2023, [https://www.djb.de/fileadmin/user\\_upload/presse/stellungnahmen/st23-17\\_Bildbasierte\\_Gewalt.pdf](https://www.djb.de/fileadmin/user_upload/presse/stellungnahmen/st23-17_Bildbasierte_Gewalt.pdf) (zuletzt aufgerufen am 25.02.2026).

<sup>51</sup> djb, Policy Paper: Sexualisierte Gewalt - Schutzlücken und Reformbedarfe, 18.11.2024, [https://www.djb.de/fileadmin/user\\_upload/presse/stellungnahmen/st24-39\\_Sexualisierte\\_Gewalt.pdf](https://www.djb.de/fileadmin/user_upload/presse/stellungnahmen/st24-39_Sexualisierte_Gewalt.pdf) (zuletzt aufgerufen am 25.02.2026).

<sup>52</sup> djb, Policy Paper: Bekämpfung bildbasierter sexualisierter Gewalt, 07.06.2023, [https://www.djb.de/fileadmin/user\\_upload/presse/stellungnahmen/st23-17\\_Bildbasierte\\_Gewalt.pdf](https://www.djb.de/fileadmin/user_upload/presse/stellungnahmen/st23-17_Bildbasierte_Gewalt.pdf) (zuletzt aufgerufen am 25.02.2026).

<sup>53</sup> Vgl. djb, Stellungnahme zum Diskussionsentwurf des Bundesministeriums der Justiz zum Gesetz gegen digitale Gewalt, 14.03.2025, <https://www.djb.de/presse/stellungnahmen/detail/st25-09> (zuletzt aufgerufen am 25.02.2026).

<sup>54</sup> Siehe insbesondere zur Effektivität djb, Stellungnahme zu den Eckpunkten des Bundesministeriums der Justiz zum Gesetz gegen digitale Gewalt. Drei kleine Schritte in die richtige Richtung - mehr aber auch nicht, 26.05.2023, [https://www.djb.de/fileadmin/user\\_upload/presse/stellungnahmen/st23-15\\_Eckpunkte\\_digitale\\_Gewalt.pdf](https://www.djb.de/fileadmin/user_upload/presse/stellungnahmen/st23-15_Eckpunkte_digitale_Gewalt.pdf) (zuletzt aufgerufen am 25.02.2026).

Eingriff in die Meinungsfreiheit darstellen kann, ist diese gesetzlich so auszugestalten, dass Verhältnismäßigkeit garantiert ist.<sup>5556</sup>

## II. Verbesserung von Ermittlungs- und Verfahrensstrukturen

In Fällen von sog. *Hatespeech* im digitalen Raum, die den Straftatbestand der Beleidigung erfüllt, sollte § 194 StGB zum Zwecke einer effektiveren Strafverfolgung dahingehend abgeändert werden, dass kein Strafantrag der verletzten Person erforderlich ist, sofern dies nicht den Interessen der verletzten Person widerspricht.<sup>57</sup>

Die einschlägigen Straftatbestände zur Bekämpfung bildbasierter sexualisierter Gewalt sollten als relative Antragsdelikte ausgestaltet werden. In der RiStBV ist klarzustellen, dass das besondere öffentliche Interesse an den Ermittlungen insbesondere dann angenommen werden sollte, wenn die wiedergegebenen Personen nicht ermittelbar sind. Darüber hinaus sollten sie in den Katalog der Nebenklagedelikte nach § 395 Abs. 1 StPO aufgenommen werden, um die Verfahrensrechte Betroffener weiter abzusichern.<sup>58</sup>

Darüber hinaus besteht erweiterter Schutzbedarf im Hinblick auf die Adressen von potenziellen Betroffenen von digitaler Gewalt. Es muss möglich sein, dass Parteien im Prozess ihre Wohnadresse verbergen können, solange eine Vollstreckung auf andere Weise sichergestellt ist. Zur Erfüllung der Impressumspflicht müssen Intermediäre einsetzbar sein. Meldeämter dürfen Adressen nur mit Einwilligung der betroffenen Person oder bei einem besonders gewichtigen Interesse der antragstellenden Person herausgegeben werden.

Im Übrigen ist es geboten, Polizei, Staatsanwaltschaft und Justiz zu den Formen und Auswirkungen von digitaler Gewalt fortzubilden. Der Rechtsschutz in diesem Bereich lässt sich nur verbessern, wenn Betroffene auch tatsächlich mit Schutz, Unterstützung und Gerechtigkeit durch die Behörden rechnen können.

## III. Konsequente Umsetzung der EU-Gewaltschutz-Richtlinie 2024

Für den deutschen Gesetzgeber besteht die Pflicht, die Vorgaben der EU-Gewaltschutz-Richtlinie bis zum 14. Juni 2027 umzusetzen. Mit Blick auf die Regelungen der Richtlinie zu digitaler Gewalt ergibt sich Handlungsbedarf. So sollte für eine vollständige Umsetzung von Art. 5 Abs. 1 lit. a) und lit. b) RL ein einheitlicher Regelungskomplex von Straftatbeständen im deutschen Recht geschaffen werden, der als Schutzgut das Recht auf sexuelle Selbstbestimmung hat. Um das Cyberstalking in Art. 6 zu erfassen, müssen § 238 StGB sowie die Normen des 15. Abschnitts des StGB angepasst werden. Auch Art. 7 und 8 der RL erfordern umfassende Reformen im Strafgesetzbuch. Art. 15 Abs. 1 und 2 der Richtlinie fordern eine effektive sowie zügige Ermittlung und Strafverfolgung der in der Richtlinie behandelten Delikte sowie eine wirksame Beweissicherung durch die zuständigen Stellen. Die Mitgliedstaaten sollen die

---

<sup>56</sup> Ausführlich GGF, Eckpunkte der Gesellschaft für Freiheitsrechte zum Digitalen Gewaltschutzgesetz – Mit Recht Gegen Digitale Gewalt, Dezember 2022, abrufbar unter: <https://freiheitsrechte.org/uploads/documents/Demokratie/Marie-Munk-Initiative/Eckpunkte-Marie-Munk-Initiative.pdf> (zuletzt aufgerufen am 26.02.2026).

<sup>57</sup> Siehe hierzu bereits djb, Policy Paper: Das Netz als antifeministische Radikalisierungsmaschine, 09.09.2021, [https://www.djb.de/fileadmin/user\\_upload/presse/stellungnahmen/st21-18\\_Antifeminismus\\_im\\_Netz.pdf](https://www.djb.de/fileadmin/user_upload/presse/stellungnahmen/st21-18_Antifeminismus_im_Netz.pdf) (zuletzt aufgerufen am 25.02.2026).

<sup>58</sup> Siehe hierzu bereits djb, Policy Paper: Bekämpfung bildbasierter sexualisierter Gewalt, 07.06.2023, [https://www.djb.de/fileadmin/user\\_upload/presse/stellungnahmen/st23-17\\_Bildbasierte\\_Gewalt.pdf](https://www.djb.de/fileadmin/user_upload/presse/stellungnahmen/st23-17_Bildbasierte_Gewalt.pdf) (zuletzt aufgerufen am 25.02.2026).

Ermittlungs- und Verfolgungsbehörden mit dem notwendigen Fachwissen ausstatten und die erforderlichen Ermittlungsinstrumente, insbesondere in dem neueren Bereich der Cybergewalt, zur Verfügung stellen bzw. entwickeln. Auch dies bedarf der Umsetzung.

#### IV. Stärkere Plattformverantwortung

Es muss sichergestellt werden, dass es auch in der Praxis eine starke Plattformverantwortung gibt. Der DSA setzt diesbezüglich stark auf Eigenverantwortung; es gilt daher, den Rechtsakt konsequent durchzusetzen und weiterzuentwickeln. Für die effektive Rechtsdurchsetzung ist die Einführung einer Verbandsklage bzw. der Prozessstandschaft inklusive Anonymisierungsmöglichkeiten gefordert, mit der Betroffene von digitaler Gewalt bei der Rechtsdurchsetzung unterstützt werden können. Um Selbstschutz gegen Hassattacken zu gewährleisten, sollten die Impressumspflichten angepasst und ein durch staatliche Schutzstellen vermittelter anonymisierter virtueller Raum bereitgestellt werden.

#### V. Bessere Unterstützung und Schutz von Betroffenen

Gesetzliche Reformen allein genügen aber nicht, um digitale Gewalt zu bekämpfen. Es bedarf eines gesellschaftlichen Umdenkens und Überwindens patriarchaler Vorstellungen von Geschlecht. Dafür bedarf es dringend empirischer Forschung zur Verbreitung digitaler Gewalt, den Betroffenen und den Handelnden, zu Radikalisierung im Netz und der Rolle, die Algorithmen hierbei spielen. Dazu kann die Forschungsförderung des Bundes einen wichtigen Beitrag leisten.

Es braucht darüber hinaus ein ganzheitliches Konzept zur Bekämpfung digitaler geschlechtsspezifischer Gewalt, mit Maßnahmen zur Prävention, Betroffenenenschutz, Medienkompetenz sowie ein effektives und niedrigschwelliges Vorgehen gegen digitale Gewalt im sozialen Nahraum. Bestehende Maßnahmen sind unzureichend:<sup>59</sup> Beratungsstellen verfügen häufig über nicht ausreichende oder fehlende personelle Ressourcen<sup>60</sup>; hinzukommen sowohl bei Beratungsstellen als auch bei Strafverfolgungsbehörden erhebliche Unterschiede in der Fachkompetenz im Umgang mit digitaler Gewalt.<sup>61</sup>

Damit Deutschland der Verpflichtung nachkommen kann, die digitale Dimension geschlechtsspezifischer Gewalt strukturell zu adressieren und in Einklang mit den Empfehlungen von GREVIO zu digitaler Gewalt gegen Frauen zu bringen<sup>62</sup>, werden Kapazitäten gebraucht. Dazu gehört der nachhaltige Ausbau der Beratungsangeboten, flächendeckende qualitativ gesicherte Fortbildung und ein starkes Netzwerk auch mit IT-Fachkräften, um Betroffenen konkrete und wirksame Hilfe bieten zu können.<sup>63</sup> Zudem müssen Kapazitäten für Prävention und Kompetenzvermittlung für alle relevanten Berufsgruppen geschaffen werden, sowie Hotlines und Krisenzentren für Betroffene von sexualisierter Gewalt.<sup>64</sup>

---

<sup>59</sup> Bündnis Istanbul Konvention, Alternativbericht zur Umsetzung des Übereinkommens des Europarats zur Verhütung und Bekämpfung von Gewalt gegen Frauen und häusliche Gewalt, September 2025 (nachfolgend BIK, Alternativbericht Istanbul Konvention) S. 29.

<sup>60</sup> Deutsches Institut für Menschenrechte, Monitor Gewalt gegen Frauen. Umsetzung der Istanbul-Konvention in Deutschland. Erster Periodischer Bericht, Dezember 2024, S. 354.

<sup>61</sup> BIK, Alternativbericht Istanbul Konvention, S. 29.

<sup>62</sup> GREVIO, General Recommendation No. 1 on the digital dimension of violence against women, GREVIO(2021)20, 2021.

<sup>63</sup> BIK, Alternativbericht Istanbul Konvention, S. 30.

<sup>64</sup> Ebd., S. 37.

Derzeit wird die Inanspruchnahme der nach Art. 22 Istanbul Konvention zu gewährleisten den spezialisierten Hilfsdiensten wird durch Zugangsbarrieren erschwert.<sup>65</sup> Fachberatungsstellen müssen zunehmend auch zu digitaler Gewalt arbeiten.<sup>66</sup> Um Jüngere besser zu erreichen, ist mehr Präsenz in den sozialen Medien erforderlich.<sup>67</sup> Damit sind zusätzliche Ressourcen und Schulungen für die Fachkräfte gefragt.<sup>68</sup>

## VI. Datenerhebung

Der djv begrüßt die Erhebung von Daten zu digitaler Gewalt entsprechend der Verpflichtung aus Art. 11 Istanbul-Konvention im aktuellen Lagebild und der Dunkelfeldstudie. Doch bestehen weiterhin Lücken in der Aufschlüsselung der Daten insbesondere hinsichtlich intersektionaler Diskriminierung. Auch sollten Lagebild und Dunkelfeldstudie in regelmäßigen Abständen durchgeführt werden.<sup>69</sup> Bei der Auswertung der Daten ist die in diesem Deliktsbereich geminderte Anzeigebereitschaft und das dadurch große Dunkelfeld zu berücksichtigen.<sup>70</sup>

## 6. Schlussbemerkung und Ausblick

Digitale Gewalt gegen Frauen und Mädchen ist heute eine zentrale menschenrechtliche und gleichstellungspolitische Herausforderung. Mit der fortschreitenden Digitalisierung verlagern sich gesellschaftliche Machtverhältnisse in den virtuellen Raum und werden dort verstärkt, beschleunigt und entgrenzt. Radikalisierte Online-Milieus, wie die sog. Manosphäre, normalisieren Misogynie, delegitimieren Gleichstellung und schaffen Resonanzräume, in denen Einschüchterung, sexualisierte Übergriffe und koordinierte Angriffe gegen Frauen alltäglich werden. Der Zugang zu Recht entscheidet dabei, ob Betroffene Schutz erhalten oder sich aus digitalen Räumen zurückziehen müssen.

Deutschland ist völker- und europarechtlich verpflichtet, auch im digitalen Raum wirksame Prävention, Strafverfolgung und Rechtsschutz zu gewährleisten. Bislang ist der Rechtsschutz lückenhaft: Straftatbestände greifen nur punktuell, zivilrechtliche Ansprüche sind schwer durchsetzbar, Plattformen werden unzureichend in die Verantwortung genommen und spezialisierte Unterstützungsstrukturen fehlen. Für Betroffene bedeutet dies hohe Hürden, langwierige Verfahren und nicht selten sekundäre Viktimisierung. So bleibt der Zugang zu Recht strukturell eingeschränkt.

Erforderlich ist ein kohärenter Gesamtansatz aus klaren gesetzlichen Regelungen, konsequenter Durchsetzung, spezialisierten Ermittlungsstrukturen, verlässlicher Datenerhebung und einer starken Beratungs- und Unterstützungsinfrastruktur. Digitale Gewalt ist eine globale Gleichstellungsfrage und verlangt koordiniertes Handeln auf allen Ebenen. Ein effektiver Zugang zu Recht ist dabei keine Ergänzung, sondern Voraussetzung für digitale Teilhabe und Gleichberechtigung. Das Side Event des djv im Rahmen der 70. Sitzung der Commission on the Status of Women bietet einen wichtigen Raum, um dazu Erfahrungen auszutauschen, voneinander zu lernen und gemeinsame Strategien weiterzuentwickeln.

---

<sup>65</sup> Ebd., S. 85.

<sup>66</sup> Ebd.

<sup>67</sup> Ebd.

<sup>68</sup> Ebd.

<sup>69</sup> Siehe hierzu bereits BIK, Alternativbericht Istanbul Konvention, S. 42.

<sup>70</sup> Vgl. djv, Policy Paper: Sexualisierte Gewalt - Schutzlücken und Reformbedarfe, 18.11.2024, [https://www.djb.de/fileadmin/user\\_upload/presse/stellungnahmen/st24-39\\_Sexualisierte\\_Gewalt.pdf](https://www.djb.de/fileadmin/user_upload/presse/stellungnahmen/st24-39_Sexualisierte_Gewalt.pdf) (zuletzt aufgerufen am 25.02.2026); Rabe, Sexualisierte Gewalt im reformierten Strafrecht. Ein Wertewandel – zumindest im Gesetz, ApuZ 4/2017, <https://www.bpb.de/shop/zeitschriften/apuz/240913/sexualisierte-gewalt-im-reformierten-strafrecht-ein-wertewandel-zumindest-im-gesetz/> (zuletzt aufgerufen am 25.02.2026).



# Impressum

Herausgeber: Deutsche Juristinnenbund e.V. (djb)

Präsidium: Prof. Dr. Susanne Baer, Professorin und Richterin des BVerfG a.D., Berlin (Präsidentin), Dr. Lucy Chebout, M.A., Richterin, RinVerfGH Berlin und Verena Haisch, Rechtsanwältin, Hamburg (Vizepräsidentinnen), Nadine Köster, LL.M., Referatsleiterin, Bonn (Schatzmeisterin), Anke Gimbal, Rechtsassessorin, Berlin (Geschäftsführerin)

Verantwortlich: Valentina Chiofalo, Vorsitzende der djb-Kommission Europa- und Völkerrecht

Bundesgeschäftsstelle  
Kronenstr. 73  
10117 Berlin

Telefon: +49 30 4432700

[https://www.djb.de/  
geschaeftsstelle@djb.de](https://www.djb.de/geschaeftsstelle@djb.de)

AG Dortmund, Vereinsreg.-Nr.: 1444

Berlin, 2026