Stellungnahme

zum

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

Mainz, 20.05.2026

Kontakt:
WEISSER RING Gemeinnütziger Verein zur Unterstützung von Kriminalitätsopfern und zur Verhütung von Straftaten e. V., Weberstraße 16, 55130 Mainz

Der WEISSE RING bedankt sich für die Gelegenheit, im Rahmen der Verbändebeteiligung Stellung zum Entwurf des Bundesministeriums der Justiz und für Verbraucherschutz im oben genannten Gesetzgebungsverfahren zu nehmen.

A. Stellungnahme zum konkreten Gesetzesentwurf

Die Verbreitung von KI-generierten Deepfakes, bei denen andere Personen nackt oder in pornographischen Positionen ohne deren Einwilligung dargestellt werden, ist ohne Zweifel strafwürdiges Unrecht. Der WR begrüßt die zivilrechtliche und strafrechtliche Verankerung des Rechtsschutzes bei Rechtsgutsverletzungen, die mit digitalen Mitteln begangen werden. Der populistische Begriff „digitale Gewalt“, der sich in den Medien hierfür etabliert hat, ist als Sammelbegriff für die Vielfalt der Erscheinungsformen (s. Entwurfsbegründung S. 19 f.) vertretbar. Da er nur in der Gesetzesüberschrift und nicht in den Gesetzestexten verwendet wird, ist eine Auflösung des traditionellen strafrechtlichen Begriffs der Gewalt nicht zu befürchten.

Die Strafbarkeitslücken sind allerdings nicht so gravierend wie in manchen Medien suggeriert wird. Die meisten der im Entwurf angesprochenen Rechtsgutsverletzungen sind schon nach bisherigem Recht strafbar. Neben der Verletzung des Rechts am eigenen Bild gem. §§ 22 KunstUrhG (strafbar mit Geldstrafe oder mit Freiheitsstrafe bis zu einem Jahr gem. § 33 KunstUrhG), der Verletzung des höchstpersönlichen Lebensbereichs durch unbefugte Bildaufnahmen gem. § 201a StGB (strafbar mit Geldstrafe oder mit Freiheitsstrafe bis zu zwei Jahren) oder der Nachstellung gem. § 238 StGB bei wiederholten Aktivitäten (strafbar mit Geldstrafe oder mit Freiheitsstrafe bis zu drei Jahren) liegt in der Regel auch eine strafbare Verleumdung gemäß § 187 StGB vor, die bei öffentlicher Tatbegehung oder bei Verbreitung ihres Inhalts mittels Informations- oder Kommunikationstechnik mit Freiheitsstrafe bis zu 5 Jahren oder mit Geldstrafe geahndet werden kann (§ 187 StGB).

Denn die Verbreitung eines Nacktfotos oder einer pornographischen Darstellung einer anderen Person in deren Namen beinhaltet die konkludente Behauptung, dass die oder der Geschädigte diese Verbreitung will.[1] Damit wird wider besseres Wissen eine unwahre Tatsache behauptet oder verbreitet, welche geeignet ist, diese Person verächtlich zu machen oder in der öffentlichen Meinung herabzuwürdigen (§ 187 StGB).

Die vielfach geäußerte Ansicht, dass es zu einschlägigen Verurteilungen bisher nicht oder extrem selten gekommen sei, hängt damit zusammen, dass die Verleumdung (ebenso wie einfache Beleidigung oder üble Nachrede) ein Privatklagedelikt gemäß § 374 Abs. 1 Nummer 2 StPO ist, bei dem die Staatsanwaltschaft und die Polizei nicht zur Mitwirkung an der Strafverfolgung verpflichtet sind.

Der WEISSE RING fordert daher schon seit vielen Jahren die Streichung der Verleumdung aus dem Katalog der Privatklagedelikte, um sie wie die Vergewaltigung oder die gefährliche Körperverletzung zu einem Offizialdelikt zu machen, bei dem die Polizei und die Staatsanwaltschaft von Amts wegen verpflichtet sind, Ermittlungen durchzuführen.[2]

Zumindest die öffentlich begangene Verleumdung (§ 187 Halbsatz 2 StGB) sollte als Offizialdelikt ausgestaltet werden.

[1] Eine konkludente Behauptung steht einer ausdrücklichen Behauptung gleich, vgl. Tübinger Kommentar StGB, 31. Aufl. 2025, Eisele/Schittenhelm, 30. Aufl. 2019, § 186 Rn. 7, § 187 Rn. 2, zur Geltung bei Deepfakes MüKo StGB/Regge/Pegel 5. Aufl. 2025, Rn. 17.

[2] Strafrechtspolitische Forderungen des WEISSEN RINGS, Forderung Nr. 11, https://weisser-ring.de/experten/recht/strafrecht.

Auch die neuen im Entwurf vorgeschlagenen Straftatbestände §§ 184k Abs.1, 201b, StGB-E sollten nicht, wie in § 374 Abs. 1 Nr. 2a und 2 e StPO-E vorgesehen, den Privatklagedelikten zugeordnet werden.

Die Ausgestaltung als Antragsdelikte (§§ 194, 205 StGB) ist dagegen sachgerecht.

Eine Privatperson ist in aller Regel nicht in der Lage, den Täter solcher Deepfakes zu ermitteln. Auch eine einzelne Polizeidienststelle, bei der die Anzeige erstattet wird, dürfte hierzu in der Regel nicht befähigt sein. Daran ändert auch der zivilrechtliche Teil des Entwurfs nichts oder nur wenig, denn zur Durchsetzung der Ansprüche auf Auskunft über Daten, beweissichernde Anordnungen oder Sperrung von Benutzerkonten in sozialen Netzwerken gemäß §§ 2-4 GgdG-E wären in der Regel nur höchstspezialisierte Rechtsanwaltskanzleien in der Lage, die sich Normalverdiener kaum leisten könnten. Ob die in §7 GgdG-E vorgesehenen zivilgesellschaftlichen Organisationen dazu in der Lage sind, ist zweifelhaft, da nicht jede Person mit der Befähigung zum Richteramt befähigt ist, derart komplexe Verfahren erfolgreich zu gestalten.

Deshalb sind Ermittlungen durch die Staatsanwaltschaften geboten, die sich hierfür – wie bei der Verfolgung von Kinderpornographie – auf die Zuständigkeitskonzentration bei den Landeskriminalämtern stützen können.

Der Referentenentwurf aus dem Bundesministerium der Justiz vom 22.12.2025 zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren verspricht eine effektivere Strafverfolgung, da er eine Speicherung der Internetprotokoll-Adressen (IP-Adressen) bis zu 3 Monaten ermöglichen soll (§ 176 Telekommunikationsgesetz-E). Auch der vom Bundesministerium der Justiz vorgelegte Referentenentwurf „digitale Ermittlungsmaßnahmen“ vom 12.3.2026 dürfte zur Effektivität der Strafverfolgung beitragen, da er eine Ermächtigungsgrundlage für den automatisierten Abgleich biometrischer Daten aus einem Strafverfahren mit im Internet öffentlich zugänglichen Daten vorsieht (§§ 98d, e StPO-E).

Die neuen Strafnormen §§ 184k Abs. 1 Nr. 4, 201b und 202e StGB-E sind geeignet, eventuell bestehende Strafbarkeitslücken zu schließen und das Unrechtsbewusstsein bei Rechtsgutsverletzungen im virtuellen Raum zu schärfen.

Bei der neuen Strafvorschrift des § 184k Abs. 1 Nr. 4 StGB-E könnte es verfassungsrechtlich problematisch sein, dass bereits das Herstellen von KI-generierten sexualisierten Deepfakes mittels eines Computerprogramms strafbar sein soll. Denn anders als beim Verbreiten entsprechender Bilder werden hierdurch keine fremden Rechtsgüter verletzt. Im Hinblick auf fremde Rechtsgüter handelt es sich allenfalls um eine strafrechtlich neutrale Vorbereitungshandlung. Solche Vorbereitungshandlungen werden nur in Fällen extremer Rechtsgutsgefährdung unter Strafe gestellt, z. B. bei der Verabredung eines Verbrechens (§ 30 Abs. 2 StGB), der Gründung einer kriminellen oder terroristischen Vereinigung (§§ 129, 129a StGB) oder bei der Herstellung kinderpornographischer Inhalte (§ 184b Abs. 1 Nr. 4 StGB). Der Gesetzgeber hat schon im 4. Strafrechtsreformgesetz vom 23.11.1973 entschieden, dass einfache Pornographie nicht schon wegen ihrer Unmoral bestraft werden soll, sofern sie lediglich in der höchstpersönlichen Privatsphäre eines Bürgers hergestellt oder verwendet wird.

In der Entwurfsbegründung (S. 67 f.) wird ausgeführt, dass die Herstellung fiktiver Nacktbilder oder pornographischer Darstellungen „zum Zwecke der eigenen sexuellen Erregung“ zur Vermeidung von Wertungswidersprüchen der entsprechenden Regelung bei der

Kinderpornographie (§ 184b Abs. 1 Nr. 4 StGB) und Jugendpornographie (§ 184c Abs. 1 Nr. 4 StGB) gleichgestellt werden müsse. Dies sei trotz der geringeren Rechtsgutsverletzung geboten, weil bei solchen Darstellungen der reale Bezug dadurch hergestellt werde, dass in der Regel der fiktiven Körperdarstellung das Gesicht einer Person hinzugefügt werde. Das lässt außer Acht, dass auch die gesamte Darstellung fiktiv sein kann. Die Strafbarkeit einer solchen Darstellung ist bei der Kinder- und Jugendpornographie im Hinblick auf die Rechtsgutsgefährdung durch pädophile Netzwerke gerechtfertigt, nicht aber bei der fiktiven Darstellung von Körpern erwachsener Personen, die Gegenstand des vorliegenden Entwurfs ist.

Es sollte geprüft werden, ob die berechtigten Anliegen des vorliegenden Entwurfs möglicherweise durch die Risiken einer verfassungsgerichtlichen Beanstandung der Strafbarkeit des Herstellens von KI-generierten Nacktbildern beeinträchtigt werden könnten.

B. Generelle Überlegungen zur Digitalen Gewalt

Um konsequent gegen digitale Gewalt vorgehen zu können, braucht es einen effektiven rechtlichen Schutz von Betroffenen. Dazu gehören konsistente Strafnormen zur Erfassung digitaler Gewaltformen, erleichterte zivilrechtliche Durchsetzung sowie systematische und nachhaltige Durchsetzungsmöglichkeiten gegenüber Plattformbetreibern.

Aus präventiver Sicht ist darüber hinaus sicherzustellen, dass Betroffene ihre Rechte tatsächlich wirksam wahrnehmen können. In der Praxis bestehen weiterhin erhebliche Zugangsbarrieren, insbesondere durch komplexe Verfahren, Kostenrisiken und begrenzte Transparenz hinsichtlich zuständiger Stellen und Abläufe. Eine **wirksame Ausgestaltung des Rechtsrahmens** sollte daher auch auf eine Vereinfachung und Beschleunigung von Verfahren, niedrigschwellige und standardisierte Anzeige- und Meldewege sowie eine bessere Unterstützung und Information von Betroffenen abzielen. Dies kann wesentlich dazu beitragen, die Inanspruchnahme rechtlicher Möglichkeiten zu erhöhen und präventive Wirkung zu entfalten.

Rechtliche Regelungen haben nicht nur einen bestrafenden Charakter und eine abschreckende Wirkung, sondern sie gestalten auch aktiv mit, welches gesellschaftliche Verhalten gewollt ist. Rechtliche Regelungen alleine reichen jedoch nicht aus, um digitale Gewalt zu verhindern. Es braucht eine **Kombination aus rechtlichen, präventiven, politischen und gesellschaftlichen Ansätzen**.

Über den rechtlichen Rahmen hinaus ist es erforderlich, **digitale Resilienz und Medienkompetenz** in jedem Alter zu fördern. Zur systematischen Förderung digitaler Handlungskompetenzen zählen das Wissen über digitale Gewalt- und Betrugsphänomene, Kenntnisse zu Datenschutz, IT-Sicherheit und digitaler Beweissicherung, zielgruppenspezifische Schulungsformate für besonders vulnerable Gruppen sowie Sensibilisierung für Täterstrategien. Dabei ist zu berücksichtigen, dass Selbstschutzmaßnahmen strukturelle Verantwortlichkeiten nicht ersetzen dürfen, sondern komplementär zu verstehen sind.

Da digitale Gewalt strukturell in digitale Kommunikationsumgebungen eingebettet ist, sind **technische und regulatorische Maßnahmen** zentral, wie transparente und effiziente Beschwerdemechanismen, proaktive Erkennung und Unterbindung missbräuchlicher Inhalte, Schutzmechanismen gegen wiederholte Verbreitung. Darüber hinaus ist es sinnvoll bei der Konzeption und Entwicklung digitaler Produkte und Dienste „Safety by Design“-Prinzipien zu implementieren. So können Missbrauchsrisiken minimiert werden, z. B. proaktive Risikoanalysen, sichere Voreinstellungen sowie niedrigschwellige und wirksame Melde- und

Beschwerdemechanismen. Die Verantwortlichkeit der Plattformbetreiber muss als integraler Bestandteil präventiver Gesamtstrategien betrachtet werden.

Eine wirksame Präventionsstrategie erfordert **klare Umsetzungsstrukturen und eine enge Zusammenarbeit relevanter Akteure**, insbesondere von Sicherheitsbehörden, Bildungseinrichtungen, Plattformbetreibern und Zivilgesellschaft. Ergänzend zu langfristigen Bildungsmaßnahmen sind auch situative Präventionsansätze erforderlich, die Tatgelegenheiten reduzieren und missbräuchliches Verhalten frühzeitig unterbinden. Dazu zählen insbesondere möglichst niedrigschwellige und nutzerfreundliche Meldeverfahren, technische Mechanismen zur Verlangsamung und bewussten Bestätigung potenziell schädigender Handlungen sowie Maßnahmen zur Begrenzung der schnellen Verbreitung problematischer Inhalte. Eine abgestimmte Umsetzung kann die Wirksamkeit dieser Maßnahmen nachhaltig erhöhen.

Langfristige Prävention digitaler Gewalt erfordert **norm- und wertebezogene Interventionen** auf gesellschaftlicher Ebene. Digitale Gewalt ist häufig Ausdruck bestehender Macht- und Ungleichheitsverhältnisse; präventive Strategien müssen diese strukturellen Dimensionen adressieren. Besonders wirkungsorientiert zeigen sich dabei Medien- und Demokratiebildung in schulischen und außerschulischen Kontexten sowie Programme zur Förderung digitaler Zivilcourage. Digitale Gewalt ist ebenfalls als **geschlechtsspezifische Gewalt** einzuordnen, Frauen, Mädchen und queere Personen sind überproportional von bildbasierter sexualisierter Gewalt, Cyberstalking und geschlechtsbezogener Hassrede betroffen. Präventionsstrategien dürfen sich daher nicht auf individuelle Schutzkompetenzen beschränken, sondern müssen strukturelle Bedingungen adressieren. Neben querfeministischer Arbeit, die diese strukturelle Gewalt in ihren Ausformungen beschreibt, braucht es gezielt geschlechtersensible Präventionskonzepte, wie Jungen- und Männerarbeit für eine strukturelle Veränderung.

Eine nachhaltige Präventionsstrategie setzt letztendlich auch auf **kontinuierliche Datenerhebung, interdisziplinäre Forschung sowie die Evaluation bestehender Maßnahmen**. Die systematische Einbeziehung von Betroffenenperspektiven ist dabei sowohl ethisch geboten als auch erkenntnisleitend.

Zudem sollten präventive Maßnahmen auch aus gesundheitlichen Aspekten aus dem Leitsatz Prävention vor Rehabilitation verfolgt werden. Es ist wissenschaftlicher Konsens, dass erlebte digitale sexualisierte Gewalt für Betroffene ganz reale Gesundheitsfolgen haben kann, da ein solches Erleben zu posttraumatischem Stress, Angstzuständen oder Depressionen führen kann.[3] Mit wirksamen Strategien könnten somit auch mögliche psychische Folgeerkrankungen verhindert werden. Vor dem Hintergrund der zunehmenden Fallzahlen digitaler Gewalt ist mit dem Blick auf die solidarisch getragenen Kosten der Gesundheitsversorgung möglicherweise betroffener Personen auch eine gesellschaftliche Entlastung zu vermuten.

Zudem sollten geeignete Präventionsstrategien insbesondere auch auf den sozialen Nahraum abzielen, da digitale Gewalt auch als Phänomen partnerschaftlicher Gewalt zu bewerten ist – insbesondere bei lebensjüngeren Menschen.[4]

[3] Patel, U. & Roesch, R. (2020). The Prevalence of Technology-Facilitated Sexual Violence: A Meta-Analysis and Sys-tematic Review. TRAUMA, VIOLENCE, & ABUSE, 23(2), S. 1-16. https://doi.org/10.1177/1524838020958057.

[4] Løkkeberg, S. T., Ihlebæk, C., Brottveit, G., & Del Busso, L. (2023). Digital Violence and Abuse: A Scoping Review of Adverse Experiences Within Adolescent Intimate Partner Relationships. Trauma Violence Abuse, 25(3), S. 1954–1965. doi: 10.1177/15248380231201816.