Republikanischer Anwältinnen- und Anwälteverein e.V.
Gneisenaustr. 2a | 10961 Berlin
Tel 030.417 235 55 | Fax 030.417 235 57
www.rav.de | kontakt@rav.de

Stellungnahme des RAV

zum Entwurf eines Gesetzes zur Stärkung des zivilrechtlichen und strafrechtlichen Schutzes vor digitaler Gewalt, Geschäftszeichen: IIIB7-611722#00002#0027

Verfasser*innen: Laura Leogrande und Petra Sußner

Vorbemerkung

Die Gesetzesnovelle zur Bekämpfung digitaler Gewalt trifft auf ein gesellschaftliches Phänomen, das längst kein Randproblem einzelner internetbezogener Konflikte mehr darstellt. Digitale Gewalt[1] ist Teil gesellschaftlicher Macht- und Ungleichheitsverhältnisse und betrifft insbesondere Frauen, queere Personen und andere marginalisierte Gruppen überproportional häufig. Eine Auseinandersetzung mit dem Gesetzesentwurf bedarf daher notwendigerweise auch einer feministischen und herrschaftskritischen Perspektive, die digitale Gewalt nicht lediglich als individuelle Grenzüberschreitung, sondern als strukturell geschlechtsspezifisches Gewaltphänomen versteht. Digitale Gewalt dient der gewaltsamen (Wieder)Herstellung einer binären Geschlechterordnung. Ihr ist als solcher zu begegnen.

Die Erscheinungsformen digitaler Gewalt sind vielfältig. Sie reichen von Überwachung, Kontrolle und Einschüchterung im Kontext partnerschaftlicher Gewalt bis hin zu öffentlichkeitswirksamen Angriffen im digitalen Raum, etwa in Form koordinierter Hasskampagnen, sexualisierter Herabwürdigung oder der Verbreitung manipulierter Inhalte gegenüber Personen, die in sozialen Medien oder der Öffentlichkeit sichtbar sind.

Breitenwirksame Debatten positionieren – wie die jüngsten Fälle Collien Fernandes oder Grok zeigen – Gewalt- und Datenschutz als Gegenpole. Auch Meinungsfreiheit und Gewaltschutz gelten vielfach als Spannungsfeld. Die positive Dimension der Meinungsfreiheit, der ihr inhärente Gleichheitsanspruch und die Gefahr, vulnerable Stimmen im (digitalen) Forum demokratischer Meinungsbildung zu verlieren, geraten darüber ins Hintertreffen. Wie schon die (rechts)politische Debatte um die so genannte Kölner Silvesternacht gezeigt hat, birgt solch binäres Denken die Gefahr, (queer)feministische Ansprüche in der Sache auszuhöhlen und als Stützpfeiler weiterer Grundrechtseinschränkungen und Repressionen zu funktionalisieren. Eine entsprechende Gefahr geht auch mit dem gegenständlichen Gesetzesentwurf einher. Er fokussiert strafrechtliche Verschärfungen und baut auf die in § 176 TKG-E vorgesehene unterschieds- und anlasslose IP-Datenspeicherung auf.

1 Digitale Gewalt ist kein legaldefinierter Begriff. Für die Zwecke dieser Stellungnahme wird das in der Gesetzesbegründung (S. 19) gewählte Verständnis von „Handlungen im digitalen Raum oder mit digitalen Mitteln [gewählt], die in rechtlich geschützte Güter, oft Persönlichkeitsrechte, eingreifen. Kennzeichnend ist die Nutzung digitaler Kommunikationsmittel und informationstechnischer Infrastrukturen“.

Der RAV solidarisiert sich entschieden mit den Betroffenen von digitaler Gewalt und begrüßt staatliche Schutzinitiativen. Gleichzeitig stellt er sich gegen eine Instrumentalisierung von Gewaltschutz im Prozess einer zusehenden Einschränkung informationeller Freiheit. Vor diesem Hintergrund konzentriert sich die Stellungnahme auf (1) Aspekte der unterschieds- und anlasslosen IP-Adressspeicherung ("Vorratsdatenspeicherung") und (2) eine kritische Auseinandersetzung mit den strafrechtlichen Verschärfungen. In beiden Gesichtspunkten spricht die Stellungnahme Leerstellen und Handlungsbedarf an, die sich aus der Anerkennung von Gewalt als Ausdruck gesellschaftlicher Macht- und Herrschaftsverhältnisse ergeben.

1.

§ 2 GgDG und Speicherung von IP-Adressen

§ 2 GgDG-E sieht einen Anspruch auf Auskunft über IP-Adressen, Portnummern sowie Zeitstempel vor. Diese Auskunft setzt eine unterschieds- und anlasslose Speicherung dieser Daten (Vorratsdatenspeicherung) voraus, wie sie mit dem § 176 TKG-E[2] am 22.4.2026 im Kabinett für eine Dauer von drei Monaten beschlossen wurde. Deren Rechtsmäßigkeit ist Voraussetzung für die Rechtmäßigkeit der in § 2 GdDG-E vorgesehene Datenverarbeitung (Art. 5 I a DSGVO).

Die Rechtsprechung von BVerfG und EuGH setzen einer solchen Vorratsdatenspeicherung enge Grenzen. Bereits in BVerfG, 1 BvR 256/08 vom 2. März 2010 hat das Bundesverfassungsgericht die damals in RL 2006/25/EG vorgesehene sechsmonatige Vorratsdatenspeicherung für mit Art. 10 GG unvereinbar erklärt und die Möglichkeit einer Erstellung von **Bewegungsprofilen** mit dem Erfordernis einer hohen Eingriffsschwelle verknüpft. In der Entscheidung EuGH, C-793/19 und C-794/19 vom 22.September 2022 – SpaceNet hat der Gerichtshof zuletzt betont, dass eine anlass- und unterschiedslose Speicherung von IP-Adressen grundsätzlich nur dann mit Art. 7, 8 und 11 GrCH („chilling effects") vereinbar ist, wenn diese zur Bekämpfung schwerer Kriminalität und Verhütung schwerer Bedrohungen der öffentlichen Sicherheit auf einen absolut notwendigen Zeitraum beschränkt ist. Zudem bedarf es einer materiell- und verfahrensrechtlichen Einhegung sowie eines effektiven Missbrauchsschutzes. Zu C-470/21 vom 30. April 2024 – La Quadrature de Net u.a. hat der EuGH nun eine Präzisierung vorgenommen, die der GgdG-E als Lockerung aufgegriffen haben dürfte.

Tatsächlich hat der Gerichtshof in La Quadrature de Net u.a. den Zusammenhang von Eingriffsintensität, Profilbildung und Rechtsgutschutz bzw. Verfolgung von Gemeinwohlzielen fokussiert. Er geht davon aus, dass eine anlass- und unterschiedslose IP-Adressspeicherung nicht nur zur Bekämpfung schwerer Kriminalität, sondern auch bei der Bekämpfung von Straftaten im Allgemeinen grundrechtskonform erfolgen kann, *sofern* die **Eingriffsintensität** nicht als hoch einzustufen ist. Um die Intensität des Eingriffs zu bemessen, orientiert sich der EuGH an tatsächlichen Möglichkeiten zur **Profilbildung**: Erfolgt eine Speicherung von IP-Adressen in der Funktion eines Identitätsdatums (Bestandsdatum), ist nicht von einem schweren Eingriff auszugehen. Das bedeutet, es ist sicher zu stellen, dass keine Verknüpfungen mit Verkehrs- oder Standortdaten stattfinden, sondern ausschließlich auf die Identifikation der betreffenden Person abgestellt wird.

Bereits an dieser Stelle ergeben sich grundrechtliche Schwierigkeiten mit § 2 GgdG-E in der derzeit vorgesehenen Fassung. Dieser sieht in Abs 2 lit a-c nicht nur die Speicherung von IP-Adressen, sondern auch von Portnummern und Zeitstempel vor (vgl. § 176 I 1-4 TKG-E). Dies ermöglicht nicht nur die

2 Unerheblich dürfte in diesem Zusammenhang sein, dass § 2 GgdG-E Auskünfte zum Zweck ziviler Rechtsverfolgung vorsieht. Auch der Entscheidung C-470/21 lag ein zivilrechtliches Auskunftsersuchen zu Grunde.

Identifikation von Geräten im mobilen Netz und öffentlichen WLAN, sondern auch eine Erstellung von Standort- und Bewegungsprofilen. Dass § 2 GgDG-E dafür keine Eingriffsgrundlagen schafft, ist für die Beurteilung der Eingriffsintensität unerheblich. Der EuGH stellt auf tatsächliche Möglichkeiten ab, und die **Intensität** der in Betreff **stehenden informationellen Eingriffe** ist als **hoch** einzustufen. Eine Rechtfertigung wird damit nur mehr zum Zweck der Bekämpfung schwerer Kriminalität und Verhütung schwerer Bedrohungen der öffentlichen Sicherheit denkbar sein.

Ergänzend ist darauf hinzuweisen, dass der EuGH zur Senkung der Eingriffsintensität eine getrennte Speicherung von Datenkategorien vorsieht (also etwa Identitätsdaten getrennt von Verkehrs- und Standortdaten). Diese Trennung ist auch bei einer Verknüpfung mit Identitätsdaten gegenüber allen anderen Datenkategorien wirksam aufrecht zu erhalten. § 176 TKG-E sieht eine entsprechende Trennung, Missbrauchsschutz und Löschpflichten vor. § 176 IV TKG-E ermächtigt zur näheren Ausgestaltung der Pflichten durch RechtsVO und stattet die Bundesnetzagentur mit Überprüfungskompetenzen aus. Es ist zumindest zu hinterfragen, ob damit – angesichts der intensiven Grundrechtseingriffe – **Wesentlichkeitsgebot und Bestimmtheitsgrundsatz** sowie das vom EuGH postulierte Wirksamkeitsgebot gewahrt sind. Eine Einbeziehung der Bundesdatenschutzbeauftragen wäre in grundrechtlicher Hinsicht wünschenswert.

Ist die Eingriffsintensität im Fall des § 2 GgdG-E als hoch einzuordnen, stellt sich die Frage, wo die Grenze zwischen Bekämpfung schwerer Kriminalität und Verhütung schwerer Bedrohungen der öffentlichen Sicherheit und der Bekämpfung von Straftaten im Allgemeinen zu ziehen ist – und in welchen Bereich die hier gegenständlichen Delikte des § 1 I 2 a-c GgDG-E fallen. Die erste Frage bemisst sich dem EuGH zu Folge – soweit es keine einschlägigen Unionrechtsregelungen gibt – nach dem Recht der Mitgliedstaaten. Maßgeblich sind dabei sich aus den Art. 7, 8, 11, 51 I GrCH ergebende Verhältnismäßigkeitsanforderungen. Jedenfalls ist es nach dem EuGH unzulässig, Straftaten als im genannten Sinn schwer zu qualifizieren, wenn „es sich angesichts der vorherrschenden gesellschaftlichen Bedingungen in dem betreffenden Mitgliedstaat nicht um schwere Straftaten handelt“ (EuGH, C-178/22 vom 30.4.2024).

Ohne die Einordnung der in § 1 I 2 a-c GgDG-E abschließend vorzunehmen, ist auf folgendes hinzuweisen: Lediglich ein Bruchteil der genannten Delikte sind Bestandteil der Katalogstraftaten des § 100a II 1 StPO (wie z.B. §§ 130, 184b, 184c II StGB). Zumindest die §§ 131, 184, 184a, 184c, 185, 186, 241 StGB sehen eine Strafmindestmaß unter einem Jahr Freiheitsstrafe vor, es handelt sich also um Vergehen iSd § 12 StGB. Bei den §§ 185, 186, 201a, 201b, 238 und 241 StGB handelt es sich um Antragsdelikte. Auch dem Gesetzesentwurf (S. 42f) ist nicht zu entnehmen, dass eine Zuordnung zur Bekämpfung schwerer Kriminalität und Verhütung schwerer Bedrohungen der öffentlichen Sicherheit maßgebliches Aufzählungskriterium gewesen wäre. Vielmehr ist als entscheidend ausgewiesen, dass die „genannten Straftaten häufig im digitalen Raum begangen [werden] und eine besondere Nähe zum allgemeinen Persönlichkeitsrecht [aufweisen]“. Im Ergebnis dürfte das verfolgte Gemeinwohlziel daher (zumindest auch) die Bekämpfung von Straftaten im Allgemeinen sein.[2] Die gewählte Eingriffsintensität ist jedoch als hoch einzustufen, woraus sich eine schon nach der Judikatur des EuGH **grundrechtswidrige Zweck-Mittel Relation** ergibt.

Dazu treten schließlich weitere Verhältnismäßigkeitserwägungen. Mit Blick auf online begangene oder durch das Internet in der Begehung oder Verbreitung erleichterte Straftaten – also die hier einschlägigen digitalen Straftaten – berücksichtigt der EuGH in La Quadrature de Net u.a., dass eine anlass- und unterschiedslose IP-Adressspeicherung als effektivste und grundrechtsschonendste Maßnahme zu werten sein kann. Maßgeblichen Abwägungsumstand ist für den Gerichtshof die Gefahr systematischer Straflosigkeit bei fehlendem Zugang zu IP Adressen (Rz 119). Selbst angesichts einer solchen drohenden Gefahr ist die Speicherung jedoch auf das zeitlich absolut Notwendige zu beschränken.

Schon die Gefahr systematischer Straflosigkeit vermögen die relevanten Gesetzesentwürfe nicht evidenzbasiert zu begründen. Die jüngst veröffentlichte LeSuBiA Studie zeigt im digitalen

Gewaltbereich eine signifikant niedrige Anzeigequote (2,4 Prozent unter Frauen / 0,9 Prozent unter Männern, Themenheft 1 S. 11). Im Zuge medialer Aufmerksamkeitskonjunkturen – wie rund um den Fall Collien Fernandes oder die Ki Chatbot Grok – werden Sensibilisierungs- und Kompetenzbedarf bei Ermittlungsbehörden sichtbar. Es fehlt nach wie vor an zentralen Zuständigen im Bereich digitale Gewalt, demokratiefördernde Projekte werden gestrichen. All diese Faktoren indizieren eine Begünstigung von systematischer Straflosigkeit. Es ist nicht ersichtlich, dass eine unterschieds- und anlasslose Speicherung von IP-Adressen dieser Gefahr wirksam und umfassend begegnen könnte. Dies trifft umso mehr auf die vorgesehene Dauer von drei Monaten zu. Es ist nicht ersichtlich, inwiefern diese Dauer ein zeitlich absolut notwendiges Minimum repräsentiert.

2.

Änderung und Erweiterung des Straf- und Strafprozessrechts

Der Gesetzesentwurf umfasst die Neufassung des § 184k StGB, wonach auch Aufnahmen bekleideter Intimbereiche in "sexuell bestimmter Weise" sowie sexualisierte KI-generierte oder manipulierte Inhalte (sog. Deepfakes) strafbar sein sollen, die Einführung von § 201b StGB-E, wovon Deepfakes erfasst sind, die den Eindruck eines realen Geschehens vermitteln und geeignet sind, dem Ansehen einer Person erheblich zu schaden, die Einführung von § 202e StGB-E, wonach insbesondere digitale Überwachung mittels Informations- oder Kommunikationstechnik (GPS-Tracker, Spyware oder ähnliche Technologien) strafbar werden soll und eine Anpassung im Strafprozessrecht zur stärkeren Einbindung von Plattformen und Diensteanbietern zur Identifizierung von Beschuldigten sowie einer teilweisen Erweiterung der Nebenklage- und Privatklagemöglichkeiten.

Grundsätzlich ist es aus feministischer Perspektive begrüßenswert, dass erkannt wird, dass in Anbetracht der Vielseitigkeit geschlechtsspezifischer Gewalt gesetzgeberischer Handlungsbedarf besteht. Zugleich lässt sich jedoch beobachten, dass sich die Entwicklung des Sexualstrafrechts und angrenzender Schutzdelikte im vergangenen Jahrzehnt durch eine hohe Normdichte und Unübersichtlichkeit auszeichnet. Zwar kann dem entgegengehalten werden, dass dies erforderlich sei, um jeglichen Auswüchsen geschlechtsspezifischer und sexueller Gewaltformen gerecht zu werden. Allerdings spricht dies jedoch eher dafür, dass die gesetzgeberischen Reformen häufig als Reaktion auf gesellschaftliche und mediale Aufmerksamkeit für bestimmte Gewaltphänomene erfolgen, anstatt auf einer systematisch durchdachten Gesamtkonzeption des Schutzes vor geschlechtsspezifischer Gewalt zu beruhen.

Eine tiefgreifende Auseinandersetzung mit den zugrundeliegenden gesellschaftlichen Macht- und Gewaltverhältnissen tritt dabei auch hinsichtlich der vorliegenden Novelle in den Hintergrund. Der Eindruck verschärft sich dadurch, dass der Gesetzesentwurf selbst keine vorliegenden Alternativen sowie einen vergleichsweise geringen Kosten- und Erfüllungsaufwand ausweist. Die Reform zielt mithin primär auf eine rechtliche Nachsteuerung ab, ohne zugleich umfassende institutionelle oder strukturelle Maßnahmen zur nachhaltigen Bekämpfung geschlechtsspezifischer Gewalt zu etablieren.

Die neuen bzw. abgeänderten Straftatbestände sind im Übrigen stark durch normative Tatbestandsmerkmale geprägt, die eine erhebliche Einzelfallabhängigkeit der Rechtsanwendung zur Folge haben und somit dem strafrechtlichen Bestimmtheitsgebot nicht hinreichend gerecht werden. So knüpfen die Tatbestände an unbestimmte Rechtsbegriffe an, etwa im Fall des § 184k StGB-E an die Abbildung bekleideter Intimbereiche „in sexuell bestimmter Weise", wobei dieser Begriff ersichtlich an die aus § 184i StGB bekannte Formulierung anknüpft. Nach der hierzu entwickelten Rechtsprechung erfolgt die Einordnung „in sexuell bestimmter Weise" anhand einer objektiven Gesamtbetrachtung des äußeren Erscheinungsbildes der Handlung, während eine rein subjektive sexuelle Motivation des Täters für sich genommen nicht ausreicht. Maßgeblich ist vielmehr, ob sich die Sexualbezogenheit nach außen hin im Gesamtzusammenhang der Handlung manifestiert. Diese an einer wertenden Gesamtbetrachtung orientierte Strafbarkeitsvoraussetzung führt dazu, dass die tatbestandliche Einordnung im Ergebnis wesentlich von der richterlichen Würdigung des Einzelfalls abhängt, insbesondere in Grenz- und Ambivalenzfällen, in denen die Sexualbezogenheit nicht eindeutig

hervortritt und die Abgrenzung zwischen sozialadäquatem Verhalten und strafrechtlich relevanter Handlung stark kontextabhängig ist. Vergleichbare Wertungsspielräume bestehen auch etwa bei dem Tatbestandsmerkmal der „Erheblichkeit“ der Ansehensschädigung im Rahmen des § 201b StGB-E, die ebenfalls eine einzelfallbezogene und stark normativ geprägte Bewertung der konkreten Rechtsgutsverletzung erfordert.

Die Tatsache, dass die Konkretisierung der zentralen Tatbestandsmerkmale sowie deren Reichweite im Ergebnis den Strafgerichten überlassen wird, ist insbesondere in Hinblick darauf problematisch, als dass nicht sichergestellt werden kann, dass im Einzelfall ein Verständnis für geschlechtsspezifische Machtverhältnisse oder die Spezifität digitaler Gewalt vorhanden ist. Dies zeigt sich schließlich bereits in der Anwendung des bestehenden Sexualstrafrechts, wonach die Bewertung etwa des entgegenstehenden Willens nicht frei ist von tradierten und stereotypischen Geschlechtervorstellungen über Sexualität und Einvernehmlichkeit.

Straftaten im digitalen Raum können erhebliche psychische und gesundheitliche Folgen hervorrufen, die in ihrer Intensität durchaus mit denen physischer Gewalt vergleichbar sein können; zugleich hat das Bundesverfassungsgericht dem sogenannten vergeistigten Gewaltbegriff zurecht eine Absage erteilt. Das Internet ist kein Raum, den Betroffene einfach verlassen können, da Inhalte dauerhaft abrufbar bleiben, sich weiterverbreiten und Rechtsgutsverletzungen auch bei fehlender aktiver Online-Präsenz der betroffenen Person fortwirken. Vor diesem Hintergrund bedarf es statt der bloßen Erweiterung strafrechtlicher Tatbestände verpflichtende Fortbildungen und Sensibilisierung innerhalb der Justiz, um sicherzustellen, dass geschlechtsspezifische Machtverhältnisse sowie die spezifischen Dynamiken und Folgen digitaler Gewalt in der strafgerichtlichen Praxis hinreichend berücksichtigt werden[3].

In der Praxis bestehen die größten Schwierigkeiten nicht in der fehlenden Strafbarkeit einzelner Verhaltensweisen, sondern in der tatsächlichen Durchsetzung von Verletztenrechten und der Verfolgung der Taten. Bereits das Wissen darüber, Opfer geworden zu sein, wird in der Regel zufällig erlangt. Gerade bei Deepfakes, Fake-Profilen oder Veröffentlichungen auf pornographischen Plattformen bleibt das tatsächliche Ausmaß der Verbreitung für die Betroffenen regelmäßig verborgen. Inhalte können dauerhaft gespeichert, weiterverarbeitet, reproduziert und auf verschiedenen Plattformen erneut hochgeladen werden. Gleichzeitig bleibt die eigentliche Beweissicherung in der Regel den Betroffenen überlassen. Screenshots, Chatverläufe, Linksammlungen und Dokumentationen werden regelmäßig eigenständig durch die Verletzten zusammengetragen, während eigeninitiierte digitale Ermittlungen durch die Strafverfolgungsbehörden nur selten erfolgen. Gerade die Komplexität der Verfahren führt zudem dazu, dass Zusammenhänge zwischen einzelnen Handlungen nicht immer erkannt werden. Häufig fehlt es an der Kontextualisierung der Übergriffe seitens der Ermittlungsbehörden: Als geringfügig erachtete Einzelhandlungen werden isoliert betrachtet und nicht in einen Gesamtzusammenhang gesetzt, der Ausdruck gezielter Kontroll-, Einschüchterungs- oder Nachstellungsdynamiken sein kann.

Schließlich noch ein prozessualer Aspekt: Zwar ist § 184k StGB ein nebenklagefähiges Delikt, bei der Zulassung der Nebenklage bei Delikten wie §§ 201a, 201b oder 202e StGB ist jedoch weiterhin eine gesonderte Begründung nach § 395 Abs. 3 StPO erforderlich, wobei die Nebenklagezulassung ob der Voraussetzung der besonderen Schwere der Tatfolgen weiterhin von einer gerichtlichen

3 Dass eine allgemeine Fortbildungspflicht mit der richterlichen Unabhängigkeit grundsätzlich vereinbar ist, wurde bereits durch den Wissenschaftlichen Dienst des Bundestages hervorgehoben, vgl.: Zur Verfassungsmäßigkeit einer Fortbildungspflicht für Richter, Aktenzeichen: WD 3 - 3000 - 229/19, https://www.bundestag.de/resource/blob/671952/7b297d8bdab137e5b71cd5a9aff7c7a8/WD-3-229-19-pdf-data.pdf; zuletzt aufgerufen am 19.05.2026.

Einzelfallbewertung abhängig bleibt. Die bloße Erweiterung strafrechtlicher Tatbestände ohne spezialisierte Ermittlungsstrukturen, technische Ausstattung und verpflichtende

Fortbildungsmaßnahmen für Polizei und Justiz ist nicht geeignet, den praktischen Schutz Betroffener nachhaltig zu verbessern.

Hinzu kommt, dass die Reform die Verantwortung für die strafrechtliche Verfolgung digitaler Gewalt in erheblichem Umfang auf die Verletzten verlagert. Die neu geschaffenen bzw. erweiterten Tatbestände der §§ 184k, 201a und 201b StGB-E wurden ausdrücklich in den Katalog der Privatklagedelikte des § 374 StPO-E aufgenommen. Dies steht zum einen in einem deutlichen Spannungsverhältnis zu Art. 55 der Istanbul-Konvention, wonach die Verfolgung geschlechtsspezifischer Gewalt gerade nicht maßgeblich von der Anzeige- und Verfolgungsbereitschaft der Verletzten abhängig gemacht werden soll. Zum anderen offenbart die Aufnahme in den Privatklagekatalog einen grundlegenden Widerspruch der Reform: Während digitale Gewalt kriminalpolitisch als strafwürdiges Unrecht anerkannt wird, wird die Verantwortung für deren konsequente Verfolgung weiterhin maßgeblich auf häufig erheblich belastete Betroffene verlagert, die neben den fortdauernden Folgen der Gewalt zugleich mit Beweissicherung, Dokumentation und strafprozessualen Anforderungen konfrontiert werden.

Allerdings ist es verfehlt, die Erweiterung staatlicher Eingriffs- und Überwachungsbefugnisse sowie die Erweiterung des Strafrechts als vorrangige Stellschraube zur Bekämpfung geschlechtsspezifischer und digitaler Gewalt zu betrachten. Strafrecht und polizeiliche Repression können gesellschaftliche Machtverhältnisse allenfalls punktuell sanktionieren, nicht jedoch die strukturellen Ursachen geschlechtsspezifischer Gewalt nachhaltig beseitigen. Ein tatsächlicher gesellschaftlicher Wandel erfordert vielmehr langfristige Prävention- und Bildungsarbeit (darunter z.B. Unterricht zur Bekämpfung von Frauenfeindlichkeit, wie etwa in Großbritannien nunmehr geplant) sowie eine umfassende Aufklärung über Rechte und Schutzmöglichkeiten im digitalen Raum und Erlernen von Medienkompetenz, einen stärkeren Ausbau von außerstrafrechtlicher Täterarbeit und Unterstützungsstrukturen für Betroffene. Ein nachhaltiger Umgang mit digitaler und geschlechtsspezifischer Gewalt darf nicht zur Folge haben, dass individuelle Freiheitsrechte zugunsten ausufernder staatlicher Kontroll- und Überwachungsbefugnisse zurücktreten. Vielmehr bedarf es dafür eines universalistischen Verständnisses von Freiheits- und Menschenrechten, das sowohl den Schutz vor Gewalt als auch den Erhalt rechtsstaatlicher und individueller Freiheitsgarantien umfasst.

Berlin, 22.5.2026