VEREINIGUNG BERLINER STRAFVERTEIDIGER*INNEN e.V.

STRAFVERTEIDIGER VEREINIGUNG-NRW E.V.

Gemeinsame STELLUNGNAHME

der Vereinigung Berliner Strafverteidiger*innen e.V. und der Strafverteidigervereinigung NRW e.V. zum

Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz „Entwurf eines Gesetzes zur Stärkung des zivilrechtlichen und strafrechtlichen Schutzes vor digitaler Gewalt"

Berlin, Mai 2026

Berichterstatter*innen:

Rechtsanwältin Nina Wittrowski, Berlin

Rechtsanwalt Clemens Hof, Berlin

Rechtsanwältin Astrid Aengenheister, Bonn

I. Vorbemerkung

Die Vereinigung Berliner Strafverteidiger*innen e.V. nimmt Stellung zu dem Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV) vom 16. April 2026 für ein „Gesetz zur Stärkung des zivilrechtlichen und strafrechtlichen Schutzes vor digitaler Gewalt" (nachfolgend: RefE oder GgdG-E).

Die Vereinigungen vertreten die Interessen von Strafverteidiger*innen und ihrer Mandant*innen. Aus dieser Perspektive beobachten wir mit erheblicher Besorgnis Gesetzesentwürfe, die – ungeachtet ihrer Einkleidung als zivilrechtliche Instrumente – mittelbar in das Gefüge strafprozessualer Garantien eingreifen, die Datengrundlage für Strafverfolgungsmaßnahmen erweitern und dabei die Verteidigungsrechte der Betroffenen strukturell schwächen.

Der vorliegende Entwurf vereinigt mehrere solcher Eingriffe: Er schafft ein gerichtliches Auskunftsverfahren, das ohne die Schutzstandards der Strafprozessordnung auskommt; er erlaubt die Nutzung anlasslos auf Vorrat gespeicherter IP-Adressen und knüpft damit unmittelbar an ein verfassungsrechtlich hochproblematisches Parallelprojekt der Bundesregierung an; er führt neue und

teils konturenlose Straftatbestände ein, die die Verteidigung in ihrer praktischen Arbeit erheblich belasten. Weiter erzeugt er eine Mehrbelastung der Justiz, die der Entwurf selbst unzureichend erfasst.

Die Vereinigung Berliner Strafverteidiger*innen e.V. und die Strafverteidigervereinigung NRW e.V. lehnen den Referentenentwurf in seiner Gesamtheit ab und fordern eine grundlegende Überarbeitung, die das Fernmeldegeheimnis (Art. 10 GG), den Schutz vor anlassloser Datenspeicherung, die Verfahrensrechte der Beschuldigten und die Funktionsfähigkeit der Justiz in angemessener Weise berücksichtigt.

Strafrecht muss stets Ultima Ratio bleiben: Die geplanten neuen Straftatbestände wären also ohnehin nur dann zu rechtfertigen, wenn mildere Mittel nicht ausreichten; der Entwurf selbst bekennt sich zum Ultima-Ratio-Gedanken – daran muss er sich messen lassen.

Gesetzgebung darf auch nicht vom Einzelfall getrieben sein; wo der Entwurf selbst „*hohe tatbestandliche Hürden*“ und den Richtervorbehalt als Schutz der Meinungsfreiheit betont, bleiben weit gefasste, wertungsoffene Straftatbestände und streubreite Datennutzungssysteme systemwidrig und unverhältnismäßig. Der Entwurf verschiebt damit die Eingriffsschwellen nach vorn (zivilrechtliches Vorfeld), erweitert das Strafrecht in unklarer Breite und erzeugt faktische Vorwirkungen – all dies widerspricht dem eigentlichen Anspruch, die Meinungsfreiheit zu schützen und das Strafrecht nur als letztes Mittel einzusetzen.

II. Verfassungsrechtliche Einwände: Vorratsdatenspeicherung durch die Hintertür

1. Das Auskunftsverfahren nach § 2 GgdG-E und seine datenschutzrechtliche Grundlage

§ 2 GgdG-E verpflichtet Diensteanbieter und Anbieter von Internetzugangsdiensten, auf richterliche Anordnung hin einem Betroffenen Auskunft über Bestands- und Nutzungsdaten zu erteilen. Zu diesen Daten gehören nach § 2 Abs. 2 Nr. 1 lit. b GgdG-E insbesondere die bei der Rechtsverletzung verwendete IP-Adresse einschließlich Portnummer sowie – nach lit. c – die zuletzt vor Zustellung der Anordnung verwendete IP-Adresse.

Der Entwurf selbst räumt ein, dass Anbieter von Internetzugangsdiensten diese Daten in der Praxis nur wenige Tage oder überhaupt nicht gespeichert halten. Er verweist deswegen ausdrücklich auf das Parallelprojekt einer Vorratsdatenspeicherung: Artikel 11 GgdG-E fügt § 174 Abs. 5 Nr. 9 TKG-E ein und ermächtigt Internetzugangsdiensteanbieter, für die Erfüllung der Auskunftspflicht auf „vorsorglich gespeicherte" IP-Adressen zurückzugreifen (vgl. Begründung zu Artikel 11 RefE). Die Formulierung „vorsorglich gespeicherte Daten" ist nichts anderes als ein Euphemismus für die anlasslose Vorratsdatenspeicherung.

Die Bundesregierung hat am 22. April 2026 parallel den Gesetzentwurf zur Einführung einer IPAdressspeicherung beschlossen, der Anbieter von Internetzugangsdiensten verpflichtet, IP-Adressen und Portnummern sämtlicher Nutzer drei Monate lang anlasslos zu speichern. Dies ist – nach den Gesetzen von 2007 und 2015 – der dritte Versuch, eine Vorratsdatenspeicherung in Deutschland zu etablieren. Beide Vorgängergesetze wurden von höchsten Gerichten für verfassungs- bzw. europarechtswidrig erklärt.

2. Die Rechtsprechung des Bundesverfassungsgerichts zur Vorratsdatenspeicherung

Mit Urteil vom 2. März 2010 (BVerfGE 125, 260) erklärte das BVerfG die anlasslose Speicherung von Telekommunikationsverkehrsdaten für unvereinbar mit Art. 10 Abs. 1 GG. Es machte die Verhältnismäßigkeit einer solchen Speicherung von strikter Zweckbindung, bereichsspezifischen Verwendungsbeschränkungen, effektiver Datensicherheit und effektivem Rechtsschutz abhängig. Eine Übermittlung auf Vorrat gespeicherter Daten ließ es nur bei überragend wichtigen Rechtsgütern zu (BVerfGE 125, 260, 344 f.); zivilrechtliche Auskunftsansprüche erkannte es nicht als tauglichen Zugangspfad an.

Mit Beschluss vom 15. Februar 2023 (1 BvR 141/16 u.a.) hielt das BVerfG auch das zweite Vorratsdatenspeicherungsgesetz für voraussichtlich europarechtswidrig und legte es dem EuGH vor. Dieser hatte bereits mit Urteil vom 20. September 2022 (C-793/19, C-794/19 – SpaceNet/Telekom) die allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten für unionsrechtswidrig erklärt.

Der Entwurf stützt sich auf das EuGH-Urteil vom 30. April 2024 (C-470/21 – La Quadrature du Net II/Hadopi), das eine auf IP-Adressen beschränkte Vorratsspeicherung zur allgemeinen Verbrechensbekämpfung unter engen Voraussetzungen erlaubt. Diese Entscheidung setzt jedoch voraus, dass eine Verknüpfung der gespeicherten IP-Adressen mit weiteren Verkehrs- oder Standortdaten faktisch ausgeschlossen ist (Rn. 82 ff.). Angesichts der im Entwurf vorgesehenen Verknüpfungsmöglichkeiten mit Bestandsdaten (§ 2 Abs. 2 Nr. 2, § 3 Abs. 3 GgdG-E) ist zweifelhaft, ob diese Voraussetzungen erfüllt sind. Der EuGH betont zudem, dass auch die Vorratsspeicherung von IP-Adressen einen schweren Eingriff in Art. 7 und 8 GRCh darstellen kann, da sie eine umfassende Nachverfolgung der Online-Aktivität von Nutzerinnen und Nutzern ermöglicht.

3. Strukturelle Umgehung der strafprozessualen Schutzsystematik

Das GgdG-E schafft ein zivilrechtliches Auskunftsverfahren – nutzt dabei aber die infrastrukturellen Voraussetzungen einer anlasslosen Massenüberwachung und ermöglicht eine Datenweitergabe an Strafverfolgungsbehörden. § 3 Abs. 4 Satz 2 GgdG-E sieht ausdrücklich vor, dass die im Rahmen des beweissichernden Verfahrens gespeicherten Daten „zum Zweck der Strafverfolgung auch an die Strafverfolgungsbehörden übermittelt werden" dürfen. Damit entsteht ein Parallelkanal zur strafprozessualen Datenbeschaffung, der die Anforderungen der StPO – insbesondere die Anforderungen an die Anordnung von Maßnahmen nach §§ 100j, 100a ff. StPO – unterläuft (Deckers - MAH Strafverteidigung | § 19 Verteidigung bei verdeckten Ermittlungen Rn. 61-68).

Im Strafverfahren bedürfen Maßnahmen zur Erhebung von Verbindungs- und Bestandsdaten einer richterlichen Anordnung nach der StPO, die auf den Verdacht einer konkreten Straftat gestützt sein muss. Das GgdG-E erlaubt hingegen die Erhebung und beweissichernde Speicherung identischer Datenkategorien auf Initiative eines Zivilklägers – mit dem Ergebnis, dass diese Daten sodann an Ermittlungsbehörden weitergegeben werden dürfen. Diese Konstruktion ist eine Umgehung, die das BVerfG im Kontext vergleichbarer Konstruktionen stets missbilligt hat.

Hinzu kommt, dass die Betroffenen – also die Personen, gegen die das Auskunftsverfahren betrieben wird – im Zeitpunkt der beweissichernden Anordnung keine Möglichkeit haben, sich rechtliches Gehör zu verschaffen. § 6 Abs. 2 GgdG-E sieht zwar eine Unterrichtung des Nutzers durch den Diensteanbieter vor. Diese erfolgt jedoch erst nach Anordnung der Datensicherung und setzt lediglich eine (anonyme) Stellungnahme bei Gericht voraus – ohne Anwaltszwang, ohne Akteneinsicht und ohne Kenntnis der vollständigen Antragsunterlagen.

III. Strafprozessrechtliche Dimension und Verteidigungsrechte

1. Das Auskunftsverfahren als strafprozessuales Vorfeld ohne StPO-Garantien

Das GgdG-E ist als zivilrechtliches Verfahren konzipiert, operiert aber in einem Bereich, der in der Praxis häufig zugleich strafrechtlich relevant ist. Die Straftatbestände des § 1 Abs. 1 GgdG-E – namentlich §§ 185 ff. StGB, 238 StGB, 241 StGB sowie die neu einzuführenden §§ 184k, 201b, 202e StGB – sind deckungsgleich mit solchen, die auch Gegenstand strafrechtlicher Ermittlungen sein können.

In der Praxis wird das Auskunftsverfahren nach § 2 GgdG-E daher häufig parallel zu laufenden oder beginnenden Strafverfahren stattfinden oder sogar diesen vorausgehen. Der Betroffene – möglicherweise Beschuldigter eines künftigen Strafverfahrens – wird über das Auskunftsverfahren identifiziert, ohne dass er im Zeitpunkt der Datenweitergabe auch nur Kenntnis von seiner Beschuldigtenstellung hätte. Die im Auskunftsverfahren erhobenen Daten stehen sodann ohne weitere richterliche Kontrolle zur Verfügung der Strafverfolgungsbehörden.

Dies verletzt das Recht auf ein faires Verfahren (Art. 6 EMRK) und das verfassungsrechtlich abgesicherte Recht auf effektive Strafverteidigung (Gaede - MüKoStPO | EMRK Art. 6 Rn. 346, Lohse, Jakobs - KK-StPO | MRK Art. 6 Rn. 42-44). Nach der ständigen Rechtsprechung des Bundesverfassungsgerichts und des Europäischen Gerichtshofs für Menschenrechte muss die Verteidigung in der Lage sein, Kenntnis von allen Informationen zu erlangen, die für die Beurteilung der Schuld oder der Unschuld des Beschuldigten relevant sind – und dies frühzeitig genug, um sich sachgerecht vorbereiten zu können(Valerius - BeckOK StPO | EMRK Art. 6 Rn. 2-30.1; Fischer - KK-StPO | Einleitung Rn. 111).

2. Keine Verteidigerkonsultation im Auskunftsverfahren

Das Auskunftsverfahren nach §§ 2, 3 GgdG-E sieht weder einen Anwaltszwang für den betroffenen Nutzer noch eine Benachrichtigung eines Verteidigers vor. Der Nutzer wird nach § 6 Abs. 2 GgdG-E durch den Diensteanbieter über das Verfahren informiert; es wird ihm lediglich ermöglicht, beim Gericht eine Stellungnahme abzugeben. Die Frist hierfür ist vom Gericht zu setzen und kann aufgrund der „Eilbedürftigkeit" sehr kurz bemessen sein.

In der Praxis wird ein Laie, der eine Nachricht seines Social-Media-Anbieters erhält, die auf ein laufendes Gerichtsverfahren und eine Möglichkeit zur anonymen Stellungnahme hinweist, nicht wissen, dass er sich möglicherweise in einer Situation befindet, die anwaltliche Beratung erfordert. Noch weniger wird er wissen, dass die Daten, die in diesem Verfahren erhoben werden, unmittelbar für ein Strafverfahren gegen ihn genutzt werden können. Dies ist ein strukturelles Verteidigungsdefizit (Gaede - MüKoStPO | EMRK Art. 6 Rn. 1-9).

3. Keine Waffengleichheit im Verfahren

Das GgdG-E ist als Verfahren der freiwilligen Gerichtsbarkeit (FamFG) ausgestaltet. In diesen Verfahren gilt der Amtsermittlungsgrundsatz – dies klingt für den Betroffenen zunächst vorteilhaft. In der Realität jedoch ist das Gericht allein mit dem Antrag des Antragstellers konfrontiert, ohne dass dem Betroffenen – insbesondere wenn dieser anonym bleibt – eine gleichwertige Teilhabe möglich ist. Die Begründung des Entwurfs betont selbst, dass der Betroffene auch anonym Stellung nehmen kann. Dies unterstreicht aber gerade, dass das Verfahren keinen echten kontradiktorischen Charakter hat.

Demgegenüber verfügt der Antragsteller – häufig eine Privatperson oder ein Unternehmen – über alle Informationen zum Sachverhalt, kann anwaltlich vertreten sein und legt die Beweise vor. Der Betroffene kann hingegen nicht Akteneinsicht nehmen (§ 3 Abs. 2 Satz 2 GgdG-E), solange dem Auskunftsantrag nicht rechtskräftig stattgegeben wurde. Diese strukturelle Ungleichheit verletzt das Gebot der Waffengleichheit im Verfahren (Lohse, Jakobs - KK-StPO | MRK Art. 6 Rn. 42-44).

4. Vorverurteilungswirkung der Accountsperre nach § 4 GgdG-E

§ 4 GgdG-E ermöglicht die richterliche Anordnung einer Sperre von Nutzerkonten in sozialen Netzwerken. Diese Maßnahme – die den Betroffenen für einen „angemessenen Zeitraum" an der aktiven Nutzung seines Accounts hindert – kann auch dann angeordnet werden, wenn die Identität des Betroffenen noch nicht bekannt ist. Sie trifft also potentiell eine Person, deren Schuld an einer Straftat noch nicht gerichtlich festgestellt ist, ohne dass diese effektiv Verteidigungsrechte geltend machen kann.

Aus strafprozessualer Sicht ist dies eine nicht akzeptable Vorverurteilungswirkung. Die Unschuldsvermutung (Art. 6 Abs. 2 EMRK, Art. 48 EU-Grundrechtecharta) gilt auch im vorgelagerten zivilrechtlichen Bereich, wenn die Sanktion – wie hier – faktisch pönalen Charakter hat (Hüttemann - von der Groeben/Schwarze/Hatje/Terhechte, Europäisches Unionsrecht | GRC Art. 48 Rn. 1-4). Eine Accountsperre, verbunden mit der öffentlichen Feststellung einer „schwerwiegenden Rechtsverletzung", ist geeignet, den Betroffenen in seinem gesellschaftlichen und beruflichen Ansehen zu beeinträchtigen, bevor auch nur ein Strafgericht über seine Schuld entschieden hat.

Hinzu kommt, dass die Sperrung nach § 4 Abs. 4 Satz 2 GgdG-E stets mit der Anordnung zur Entfernung des rechtsverletzenden Inhalts verbunden ist. Damit können Inhalte dauerhaft gelöscht werden, bevor ein rechtskräftiges Strafurteil vorliegt – eine Maßnahme, die das Beweismaterial für eine eventuelle Verteidigung vernichten kann.

IV. Mehrbelastung der Justiz

Der Referentenentwurf schätzt die Mehrkosten für die Justiz der Länder auf insgesamt rund 194.000 Euro jährlich. Diese Schätzung beruht auf der Annahme von 1.400 zusätzlichen Auskunftsverfahren nach § 2 GgdG-E pro Jahr, 810 richterlich angeordneten Accountsperrungen nach § 4 GgdG-E pro Jahr, 5.400 beweissichernden Anordnungen nach § 3 GgdG-E pro Jahr sowie 220 Beschwerdeverfahren (ca. 10 % der 2.210 Hauptsacheverfahren). Ausgehend von einem Zeitaufwand von 34 Minuten je Hauptsacheverfahren, 10 Minuten je beweissichernder Anordnung und 223 Minuten je Beschwerdeverfahren sowie eines Lohnsatzes des höheren Dienstes der Länder von 65,20 Euro werden Mehrkosten von rund 194.000 Euro jährlich errechnet.

Die Vereinigungen weisen darauf hin, dass diese Schätzung wesentliche Kostenkomponenten unberücksichtigt lässt und die tatsächliche Mehrbelastung der Justiz deutlich höher liegen dürfte. Hierzu zählen insbesondere:

- Der Aufwand für grenzüberschreitende Zustellungen und Rechtshilfe, insbesondere bei Diensteanbietern mit Sitz im EU-Ausland
- Die gerichtliche Koordination zwischen Diensteanbietern und Internetzugangsdiensteanbietern im zweistufigen Verfahren nach § 3 GgdG-E
- Die Berücksichtigung und Abwägung von Nutzerbeteiligungen nach § 6 GgdG-E
- Die Prüfung der Tatbestandsvoraussetzungen der in § 1 Abs. 1 GgdG-E genannten Strafnormen, insbesondere bei Fragen der Abgrenzung von Meinung und Tatsachenbehauptung im Rahmen der §§ 185 ff. StGB

Die spezialisierten Kammern für Veröffentlichungsstreitigkeiten (§ 72a Abs. 1 Nr. 5 GVG) an den Landgerichten sind bereits heute erheblich belastet. Zusätzliche Verfahren werden ihre Kapazitäten übersteigen und zu Verfahrensverzögerungen führen können. Hinzu kommt, dass die neuen Straftatbestände (§§ 184k, 201b, 202e StGB-E) zusätzliche Strafanzeigen, Ermittlungsverfahren und Strafverfahren auslösen werden, die ihrerseits Ressourcen binden.

V. Kritik an den neuen Straftatbeständen

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

Die erhebliche Erweiterung des § 184k StGB durch den Entwurf ist grundsätzlich dem Anliegen geschuldet, Lücken im Bildnisschutz zu schließen. Allerdings weist die Neufassung aus Sicht der Strafverteidigung schwerwiegende Defizite auf.

Die Aufnahme von Bildmaterial, das sexuelle Handlungen abbildet (Abs. 1 Nr. 1), von unbekleideten Genitalien (Nr. 2) sowie von bekleideten Körperteilen „in sexuell bestimmter Weise" (Nr. 3) und von KI-generierten Deepfakes (Nr. 4) in einen einzigen Straftatbestand schafft eine erhebliche Unschärfe. Insbesondere die Tatbestandsalternative des Zugänglichmachens an „eine dritte Person" – also an eine einzige weitere Person – führt dazu, dass die Weitergabe auch in privatem, nicht öffentlichem Rahmen strafbar wird. In Verbindung mit dem Antragsvorbehalt (Abs. 3) besteht die Gefahr, dass dieses Instrument im Beziehungskonflikt instrumentalisiert wird.

Es besteht die ernsthafte Gefahr von Fehlentscheidungen, da die Urheberschaft für derartiges Material in der Regel unklar bleibt und digitale Spuren leicht gefälscht werden können. Weder die Behörden, noch die Gerichte, noch die Verteidigung werden in derartigen Situationen, auch aufgrund der wegen KI fortschreitenden Verbesserung des gefälschten Materials, in der Lage sein, Falschbelastungen als solche zu erkennen. Dies gilt umso mehr als schon das bloße Herstellen von Deepfakes zum Eigengebrauch (Abs. 1 Nr. 4) strafbar sein soll, denn ein derartiger Vorwurf ließe sich dann sehr leicht konstruieren ("Hiermit übersende ich Ihnen ein Deepfake, dass ich auf dem Smartphone meines/meiner Ex gefunden habe, erstatte Strafanzeige und stelle Strafantrag").

Abgesehen davon ist auch unklar, welches Schutzgut genau von der Herstellung von Deepfakes zum Eigengebrauch betroffen sein soll. Der Entwurf selbst führt aus (S. 67f.: "Das bloße Herstellen manipulierter Bilder zum Eigengebrauch begründet zwar im Vergleich zum Zugänglichmachen an Dritte und auch im Vergleich zur Herstellung in Verbreitungsabsicht eine geringfügigere Rechtsgutverletzung, auch sind die Abbildungen der intimen Körperteile und sexuellen Handlungen, welche die KI-Anwendung erzeugt, nicht real. Gleichwohl wird die betreffende Person, deren reale persönliche Merkmale (in der Regel das Gesicht) für die Erstellung entsprechender Bilder verwendet werden, ohne dass diese Person Einfluss darauf hat, zur sexuellen Stimulation oder zu anderen Zwecken 'benutzt'". Der Gesetzeswortlaut dagegen bestraft die Bearbeitung auf eine Weise, "dass der Anschein erweckt wird, dass sexuelle Handlungen oder die unbekleideten Genitalien, das unbekleidete Gesäß oder die unbekleidete weibliche Brust einer anderen Person abgebildet seien."

Gerade das Gesicht taucht hier also gar nicht mehr auf. Es genügt, dass unbekleidete Genitalien, das unbekleidete Gesäß oder die unbekleidete weibliche Brust abgebildet werden. Diese werden immer den Anschein erwecken können, von einer anderen Person zu stammen. Weshalb aber die KI-Herstellung der Abbildung etwa einer unbekleideten Brust zum Eigengebrauch strafbar sein soll, erschließt sich auch vor dem Hintergrund des Gesetzesziels nicht. Hier erweckt der Entwurf vielmehr den Eindruck, moralische Anzüglichkeiten ohne reale Rechtsgutverletzungen unter Strafe stellen zu wollen. Sowohl ein Moralstrafrecht als auch ein Strafrecht ohne Rechtsgutbezug sind aber abzulehnen.

Die Strafbarkeit bereits des Herstellens *„sexualisierter Deepfakes“* zum Eigengebrauch sowie des Zugänglichmachens an nur *„eine dritte Person“* verlagert damit zwangsläufig private Konflikte in das Strafrecht und begünstigt Instrumentalisierungen bei zugleich erheblichen Beweisproblemen.

2. § 201b StGB-E: Verletzung von Persönlichkeitsrechten durch täuschende Inhalte

Der neue § 201b StGB-E ist tatbestandlich zu weit geraten. Strafbar soll es sein, Dritten einen „mittels eines Computerprogramms erstellten oder veränderten Inhalt" zugänglich zu machen, „der den Anschein erweckt, ein tatsächliches Geschehen in Bezug auf eine andere Person wiederzugeben, und der geeignet ist, dem Ansehen dieser Person erheblich zu schaden". Die Subsidiaritätsklausel (Satz 1 Hs. 2) bewahrt den Tatbestand vor Überschneidungen mit Verleumdungsnormen, löst aber das grundlegende Problem der Unbestimmtheit nicht.

In der digitalen Alltagswirklichkeit werden mit Programmen bearbeitete Inhalte ubiquitär verbreitet – von Fotofiltern über Videobearbeitungen bis hin zu Parodien und Satire. Der Tatbestand stellt nicht auf eine Täuschungsabsicht ab, sondern lediglich auf die objektive Eignung zur Ansehensschädigung. Es fehlt an einem subjektiven Tatbestandsmerkmal, das die Strafbarkeit auf manifestes Unrecht begrenzt. Die Einschränkung über § 201a Abs. 3 StGB-E (Wahrnehmung berechtigter Interessen) und das Erfordernis der Eignung zur „erheblichen" Ansehensschädigung reichen nicht aus, um eine ausreichende Bestimmtheit im Sinne des Art. 103 Abs. 2 GG herzustellen.

Besonders problematisch ist, dass die Frage, ob ein Inhalt „geeignet ist, dem Ansehen einer Person erheblich zu schaden", einer stark subjektiven richterlichen Wertung unterliegt. Dies schafft erhebliche Rechtsunsicherheit für die Betroffenen bzw. Beschuldigten. Die Strafbarkeit knüpft damit ohne eine Täuschungsabsicht vorauszusetzen allein an die *„Eignung“* zur erheblichen Ansehensschädigung an. Diese unpräzise Wertungslage verletzt die Anforderungen aus Art. 103 Abs. 2 GG und schafft erhebliche Rechtsunsicherheit.

3. § 202e StGB-E: Unbefugte Überwachung mittels Informations- oder Kommunikationstechnik

§ 202e StGB-E ist als relatives Antragsdelikt ausgestaltet und setzt eine „wiederholte oder ständige" Überwachung voraus, die wahrscheinlich zu einem „schweren Schaden" führt. Diese Einschränkungen sind im Grundsatz begrüßenswert, lösen aber nicht die strukturellen Probleme des Tatbestands.

I. Das Problem des "besonderen öffentlichen Interesses" bei fehlender RiStBV-Ergänzung

Besonders problematisch ist, dass § 202e StGB-E als relatives Antragsdelikt ausgestaltet wird, ohne dass der Entwurf eine Ergänzung der Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) vorsieht. Dies schafft eine erhebliche Missbrauchsgefahr:

Nach ständiger Rechtsprechung und herrschender Meinung ist die Entscheidung der Staatsanwaltschaft über das Vorliegen eines besonderen öffentlichen Interesses an der Strafverfolgung eine Ermessensentscheidung, die einer gerichtlichen inhaltlichen Überprüfung weitgehend entzogen ist. Das Gericht prüft lediglich formal, ob die Staatsanwaltschaft das besondere öffentliche Interesse bejaht hat, nicht jedoch, ob diese Bejahung sachlich gerechtfertigt ist. Eine Ausnahme bildet lediglich die Willkürkontrolle nach Art. 3 Abs. 1 GG, die jedoch einen äußerst engen Prüfungsrahmen eröffnet.

1. Fehlende Konkretisierung durch die RiStBV

Die RiStBV enthalten für andere relative Antragsdelikte – etwa bei Körperverletzung (§ 230 StGB) oder bei Straftaten gegen den Wettbewerb (§ 301 StGB) – konkrete Hinweise, wann ein besonderes öffentliches Interesse an der Strafverfolgung anzunehmen ist (Hardtung - MüKoStGB | StGB § 230 Rn. 25-35; NRW_181_2023_0124). Diese Konkretisierungen dienen als "Anleitung für den Regelfall" und binden die Staatsanwaltschaft als innerdienstliche Weisungen (Hardtung - MüKoStGB | StGB § 230 Rn. 25-35). Für § 202e StGB-E fehlt eine solche Ergänzung der RiStBV vollständig.

2. Missbrauchsgefahr durch unkontrollierte Ermessensausübung

Ohne RiStBV-Konkretisierung besteht die Gefahr, dass die Staatsanwaltschaft das besondere öffentliche Interesse nach § 202e StGB-E willkürlich oder aus rein pragmatischen Erwägungen bejaht. Dies ist insbesondere problematisch, weil:

- Das Gesetz keine Frist für die staatsanwaltschaftliche Ermessensentscheidung vorsieht (Eschelbach - BeckOK StGB | StGB § 230 Rn. 21). Die Bejahung des besonderen öffentlichen Interesses kann noch in der Hauptverhandlung oder sogar in der Revisionsinstanz erfolgen (Eschelbach - BeckOK StGB | StGB § 230 Rn. 21).

- Die Staatsanwaltschaft das besondere öffentliche Interesse auch konkludent erklären kann, indem sich aus einer Prozesshandlung mit hinreichender Deutlichkeit der Verfolgungswille ergibt (Eschelbach - BeckOK StGB | StGB § 230 Rn. 17-23). Dies ermöglicht eine "nachträgliche" Bejahung, wenn sich das Verfahren nicht wie gewünscht entwickelt.

- Die Bejahung des besonderen öffentlichen Interesses bedarf keiner besonderen Form und wird in der Praxis regelmäßig nicht begründet (Eschelbach - BeckOK StGB | StGB § 230 Rn. 17-23). Dies erschwert jede Kontrolle.

II. Unbestimmter Tatbestand

Das Merkmal „wahrscheinlich dazu führt, dass dieser Person schwerer Schaden zugefügt wird" (Satz 2) ist ein objektives Tatbestandsmerkmal, das im Einzelfall schwer zu beurteilen ist. Es stellt sich die Frage, wie die Wahrscheinlichkeit eines „schweren Schadens" abzugrenzen ist von bloß unangenehmen oder lästigen Überwachungssituationen. Die Begründung des Entwurfs gibt insoweit wenig konkrete Orientierung. *„Wiederholt oder ständig“* und insbesondere das objektive Merkmal *„wahrscheinlich … schwerer Schaden“* lassen sich in der Praxis kaum trennscharf anwenden. Damit drohen auch an dieser Stelle Ausuferungen jenseits strafwürdiger Fälle.

III. Wechselwirkung § 202e StGB-E und der vorgesehene Auskunftsanspruch

Darüber hinaus besteht die Gefahr, dass § 202e StGB-E und der ebenfalls im Entwurf vorgesehene Auskunftsanspruch nach § 2 GgdG-E in Wechselwirkung treten: Wer befürchtet, überwacht zu werden, wird zivilrechtliche Auskunftsverfahren einleiten, die ihrerseits zur Speicherung und möglichen Weitergabe der Daten des Beschuldigten an Strafverfolgungsbehörden führen – bevor auch nur eine strafrechtliche Anklage erhoben ist.

Darüber hinaus besteht die Gefahr, dass § 202e StGB-E und der ebenfalls im Entwurf vorgesehene Auskunftsanspruch nach § 2 GgdG-E in problematischer Wechselwirkung treten: Wer befürchtet, überwacht zu werden, wird zivilrechtliche Auskunftsverfahren einleiten, die ihrerseits zur Speicherung und möglichen Weitergabe der Daten des Beschuldigten an Strafverfolgungsbehörden führen – bevor auch nur eine strafrechtliche Anklage erhoben ist.

Diese Wechselwirkung birgt besondere Gefahren:

1. Vorwegnahme der strafrechtlichen Beweiserhebung

Das zivilrechtliche Auskunftsverfahren dient faktisch der strafrechtlichen Beweissicherung, ohne dass die strafprozessualen Garantien gelten. Die Daten des Beschuldigten werden gespeichert und können an Strafverfolgungsbehörden weitergegeben werden, ohne dass ein hinreichender Tatverdacht im strafrechtlichen Sinne besteht.

2. Umgehung der strafprozessualen Eingriffsvoraussetzungen

Durch die Nutzung des zivilrechtlichen Auskunftsverfahrens werden die strengen Voraussetzungen für strafprozessuale Eingriffe (§§ 100a ff. StPO) umgangen. Dies ist besonders gravierend bei § 202e StGB-E, der gerade den Schutz vor unbefugter Überwachung bezweckt.

3. Gefahr der "fishing expeditions"

Die Kombination aus einem weiten Tatbestand des § 202e StGB-E und einem niedrigschwelligen Auskunftsanspruch ermöglicht "fishing expeditions" – die gezielte Suche nach belastendem Material ohne konkreten Anfangsverdacht.

VI. Zur Verwendung der Bezeichnung „digitale Gewalt“

Neben den vorstehenden inhaltlichen Bedenken ist letztlich auch ein normentheoretischer Gesichtspunkt zu erörtern:

Der Gesetzentwurf übernimmt die Bezeichnung „digitale Gewalt” aus dem politischen Raum. Wie der Entwurf aber selbst – insoweit zutreffend – feststellt, handelt es sich insoweit um keine rechtliche Begrifflichkeit. So heißt es auf S. 19 des Entwurfes: *„Digitale Gewalt ist allerdings weder einheitlich noch abschließend definiert. Es handelt sich um keinen eigenständigen Rechtsbegriff, sondern um einen Sammelbegriff aus dem gesellschaftlichen und politischen Diskurs für Handlungen im digitalen Raum oder mit digitalen Mitteln, die in rechtlich geschützte Güter, oft Persönlichkeitsrechte, eingreifen.”*

Damit wird die Problematik der Übernahme von Begrifflichkeiten aus dem vorlegislativen, politischen Raum in den Bereich der Gesetzgebung deutlich: Diese sind oft mit Blick auf eine „griffige” Öffentlichkeitskommunikation angelegt, aber eben nicht definiert (instruktiv dazu Rath in taz vom 20.04.2026.). Rechtsbegriffe dagegen sollen so genau wie möglich zu definieren sein, damit in der Rechtsanwendung deutlich wird, welche Sachverhalte dem Gesetz unterfallen und welche nicht. Gerade im Strafrecht hat dies entscheidende Bedeutung: Die Bürger sollen ja wissen, was erlaubt und was verboten ist, um ihr Verhalten daran ausrichten zu können. Auch wenn die Gerichte Grenzfälle entscheiden sollen, muss ich aus dem Gesetz selbst bereits die Beschreibung des verbotenen Verhaltens ergeben. Diese Transparenz wird aber verdunkelt, wenn unklare, nicht definierte Begrifflichkeiten eingeführt werden.

Ein Musterbeispiel für diese Problematik ist gerade der Begriff der „Gewalt” selbst, der einen der umstrittensten Begriffe des Strafrechts darstellt. Gerade an ihm hat sich gezeigt, wozu unklare Begrifflichkeiten führen können: Von dem ursprünglichen Verständnis dessen, was „Gewalt” im Rechtssinne ist, nämlich die in Anwendung von Körperkraft erfolgende Einwirkung auf den Körper des Opfers zur Überwindung eines Widerstandes (RGSt 56, 88), entfernten sich die Gerichte in ihrem Bedürfnis zu strafen so weit, dass der BGH auch Sachverhalte ohne jegliche physische Zwangswirkung als „Gewalt” ansah („Laepple-Urteil (BGH 2 StR 171/69). Unter Geltung dieser Rechtsprechung war es fast schon willkürlich den Gerichten überlassen, wann sie einen Sachverhalt als strafbare Gewalt ansahen und wann nicht. Das BVerfG musste schließlich korrigierend eingreifen.

Um derartig letztlich verfassungswidrige Entwicklungen gar nicht erst aufkommen zu lassen, ist es als gute gesetzgeberische Praxis nötig, jedenfalls betreffend die Gesetze selbst von politisch-medialen PR-Begrifflichkeiten Abstand zu nehmen.

Ein Gesetz, dass aber seinerseits im Titel eine Vermengung von Begrifflichkeiten im Sinne von „digitaler Gewalt" verwendet und damit weiter verdunkelt, ob es hier wirklich um „Gewalt" gehen soll oder nicht vielmehr (so dann ja der Inhalt des Gesetzes) um digitales Unrecht anderer Art, ist unter dieser Bezeichnung – jenseits der inhaltlichen Bedenken, siehe oben – abzulehnen. Der Gesellschaft als Ganzes ist mit dem Beschreiten einer derartigen gesetzgeberischen Praxis nicht gedient. Oder, wie es Rath (s.o.) ausdrückt: „Eine Ausweitung des Gewaltbegriffs ist jedenfalls nicht per se ein Fortschritt. Wenn fast alles Gewalt sein kann, verliert der Begriff sein Gewicht.

VII. Fazit und Forderungen

Die Vereinigung Berliner Strafverteidiger*innen e.V. und die Strafverteidigervereinigung NRW e.V. lehnen den Referentenentwurf des BMJV zum „Gesetz gegen digitale Gewalt" aus den dargelegten Gründen ab. Im Einzelnen:

- Das Auskunftsverfahren nach § 2 GgdG-E in Verbindung mit der anlasslosen IP-Adressspeicherung (Artikel 11 GgdG-E, § 174 Abs. 5 Nr. 9 TKG-E) ist verfassungsrechtlich nicht tragfähig. Es widerspricht der ständigen Rechtsprechung des Bundesverfassungsgerichts zu Art. 10 GG(BVerfG 1 BvR 256, 263, 586/08)(BVerfG 1 BvR 256, 263, 586/08) und des EuGH zur ePrivacy-Richtlinie (Urteil des Gerichtshofs (Große Kammer) vom 20. September 2022, Verbundene Rechtssachen C-793/19, C-794/19) - 2.). Zwei Vorgängergesetze zur Vorratsdatenspeicherung wurden bereits für verfassungs- bzw. europarechtswidrig erklärt (BVerfG 1 BvR 141/16). Der dritte Versuch leidet an denselben strukturellen Defiziten.

- Der Eingriff in Art. 10 GG durch die Struktur der §§ 2, 3 GgdG-E und die Möglichkeit der Nutzung „*vorsorglich*" gespeicherter IP-Adressen ist nur unter engsten, gesetzlich präzisierten Voraussetzungen tragfähig; an einer solchen normenklaren, verhältnismäßigen Ausgestaltung fehlt es. Die unionsrechtliche Zulässigkeit beschränkter IP-Speicherung setzt strikte Speichermodalitäten und faktische Entkopplung von Verkehrs-/Standortdaten voraus; die im Entwurf vorgesehenen Verknüpfungen mit Bestandsdaten unterlaufen diese Grenzen.

- Das Auskunftsverfahren umgeht die strafprozessualen Schutzstandards der StPO. Die explizite Ermächtigung zur Datenweitergabe an Strafverfolgungsbehörden (§ 3 Abs. 4 Satz 2 GgdG-E) schafft einen Parallelkanal der Datenerhebung ohne die Garantien der §§ 100j, 100a ff. StPO (Deckers - MAH Strafverteidigung | § 19 Verteidigung bei verdeckten Ermittlungen Rn. 61-68). Dies ist mit dem Gebot eines fairen Verfahrens (Art. 6 EMRK) und dem Recht auf effektive Strafverteidigung unvereinbar (Gaede - MüKoStPO | EMRK Art. 6 Rn. 1-9).

- Die im Entwurf enthaltene Schätzung der Mehrbelastung der Justiz (194.000 Euro p.a.) ist erheblich zu niedrig. Unter Berücksichtigung des Aufwands für grenzüberschreitende Zustellungen, die zweistufige Koordination zwischen Diensteanbieter und Internetzugangsanbieter, die Nutzerbeteiligung und die durch neue Straftatbestände ausgelösten Strafverfahren ist von einer deutlich höheren Mehrbelastung auszugehen. Die Landgerichte, insbesondere deren Kammern für Veröffentlichungsstreitigkeiten, sind bereits heute erheblich ausgelastet.

- Die Accountsperre nach § 4 GgdG-E hat faktisch pönalen Charakter und entfaltet eine Vorverurteilungswirkung, die mit der Unschuldsvermutung (Art. 6 Abs. 2 EMRK, Art. 48 EU-Grundrechtecharta) nicht vereinbar ist (Hüttemann - von der Groeben/Schwarze/Hatje/Terhechte, Europäisches Unionsrecht | GRC Art. 48 Rn. 1-4). Gleichzeitig kann die zwingend angeordnete Inhaltsentfernung Beweise vernichten.

- Die neuen Straftatbestände (§§ 184k, 201b, 202e StGB-E) sind teils zu unbestimmt, um den Anforderungen des Art. 103 Abs. 2 GG zu genügen, und werden erhebliche

Auslegungsprobleme in der Strafverteidigung erzeugen. Insbesondere § 201b StGB-E entbehrt eines ausreichenden subjektiven Tatbestandsmerkmals und ist in seiner Reichweite schwer abgrenzbar.

Wir fordern das BMJV auf, den Entwurf in seiner Gesamtheit zurückzuziehen und eine grundlegende Überarbeitung vorzunehmen. Dabei sollten folgende Maßnahmen berücksichtigt werden:

- Strikte Trennung von zivilrechtlichen Auskunftsverfahren und strafprozessualen Ermittlungsmaßnahmen: Eine Datenweitergabe an Strafverfolgungsbehörden auf der Grundlage von § 3 Abs. 4 Satz 2 GgdG-E ist vollständig zu streichen.

- Kein Rückgriff auf anlasslos auf Vorrat gespeicherte IP-Adressen: Artikel 11 GgdG-E und der parallele IP-Adressspeicherungs-Gesetzentwurf sind mit Art. 10 GG und dem europäischen Datenschutzrecht unvereinbar und müssen aufgegeben werden (Urteil des Gerichtshofs (Große Kammer) vom 20. September 2022, (Verbundene Rechtssachen C-793/19, C-794/19) - 2.).

- Stärkung der Verteidigungsrechte im Auskunftsverfahren: Einführung eines Anwaltszwangs für betroffene Nutzer, effektives Akteneinsichtsrecht und ausreichende Stellungnahmefristen (Gaede - MüKoStPO | EMRK Art. 6 Rn. 1-9).

- Überarbeitung der neuen Straftatbestände: § 201b StGB-E bedarf eines ausreichenden subjektiven Tatbestandsmerkmals; § 202e StGB-E muss klarer konturiert werden.

- Eine Ergänzung der RisBV mit konkreten Kriterien für das Vorliegen eines besonderen öffentlichen Interesses bei § 202e StGB-E.

- Die Einführung einer Begründungspflicht für die Bejahung des besonderen öffentlichen Interesses;

- Die Begrenzung der konkludenten Bejahung auf klar definierte Ausnahmefälle.

- Die Sicherstellung, dass zivilrechtliche Auskunftsverfahren nicht zur Umgehungstrafprozessualer Garantien genutzt werden können.

- Realistische Folgenabschätzung für die Justiz: Eine unabhängige Evaluation der Justizkapazitäten ist vor einer etwaigen Neuvorlage des Entwurfs durchzuführen.

Berlin, Mai 2026

Rechtsanwältin Nina Wittrowski und

Rechtsanwalt Clemens Hof für die Vereinigung Berliner Strafverteidiger*innen e.V.

Rechtsanwältin Astrid Aengenheister für die Strafverteidigervereinigung NRW e.V.