In wessen Namen?

Zur Verknüpfung von Gewaltschutz und IP-Adressspeicherung

Petra Sußner

12.06.2026 doi: 10.59704/57d5fc48e8e0e84a

Am 16. April 2026 hat das Bundesministerium für Justiz und Verbraucherschutz den Referentenentwurf des Gesetzes zur Stärkung des zivil- und strafrechtlichen Schutzes vor digitaler Gewalt veröffentlicht. Er folgt auf breit diskutierte Fälle wie den von Collien Fernandes oder des KI Chatbots Grok. Im – auch kritischen – Fokus stehen strafrechtliche Verschärfungen. Zivilrechtlich sollen Betroffene zukünftig mit mehr Auskunftsansprüchen ausgestattet sein. Diese Erweiterung umfasst insbesondere einen gerichtlich angeordneten Zugriff auf – unterschieds- und anlasslos gespeicherte – IP-Adressen, Portnummern und Zeitstempel. Die Vorratsdatenspeicherung ist also zurück. Mit ihr eine funktionale Verknüpfung von informationellen Grundrechtseingriffen und Gewaltschutz hergestellt, die rechtspolitisch vertraut wirkt. Evidenzbasiert ist sie nicht. Und grundrechtlich dürfte sie Probleme aufwerfen.

Der (neue) Auskunftsanspruch im Zivilverfahren

Auf den ersten Blick wirkt das Gesetz zur Stärkung des zivil- und strafrechtlichen Schutzes vor digitaler Gewaltwie Anlassgesetzgebung. Eine solche Einordnung übersieht jedoch historische Kontinuitäten und unionsrechtliche Rahmung des Gesetzesvorhabens: Bereits im Jahr 2023, zur Zeit der Ampelregierung, hat das Bundesministerium der Justiz Eckpunkte zum Gesetz gegen digitale Gewalt veröffentlicht. Sie sahen im zivilrechtlichen Bereich, ähnlich wie der aktuelle Entwurf, Maßnahmen wie richterlich angeordnete Accountsperren (aktuell § 4 GgdG-E) oder Sicherungsanordnungen („*Quick Freeze*“, aktuell § 3 GgdG-E) vor. Mit Ablauf der Umsetzungsfrist der RL 2024/1385 (GewaltschutzRL) am 14.6.2027 soll die nicht einvernehmliche Herstellung und Veröffentlichung von sexualisierten Deepfakes in den Mitgliedstaaten (ohnehin) unter Strafe stehen (Art. 5 I b iVm Erwägungsgrund 19 der GewaltschutzRL).

Was neu und auf den ersten Blick leicht zu übersehen ist: § 2 GgdG-E sieht einen gegenüber dem geltenden § 21 II-IV TDDDG hinausgehenden zivilrechtlichen Auskunftsanspruch vor. Das ist angesichts des fragmentarisch ausgestalteten § 21 III TDDDG im Sinn des Rechtsschutzes begrüßenswert. Derzeit setzt ein Auskunftsanspruch voraus, dass absolute Rechte entweder aufgrund rechtswidriger audiovisueller Inhalte verletzt oder aufgrund spezifisch genannter Katalogstraftaten verletzt werden. Sofern es sich also z.B. „nur“ um ein Foto oder eine Textnachricht handelt, bedarf es der rechtswidrigen Verwirklichung einer Katalogstraftat. Mit §§ 185 oder 201a StGB – Beleidigung und Verletzung des höchstpersönlichen Lebensbereichs und höchstpersönlicher Rechte durch Bildaufnahmen – fallen typische digitale Gewaltphänomene unter die Katalogstraftaten. Ebenso einschlägig, aber nicht erfasst sind etwa die §§ 126a und 184k StGB: Sie betreffen die Phänomene *Doxing, Downblousing* und *Upskirting*. Diese Ausdifferenzierung ist historisch gewachsen. Für Betroffene dürfte sie ohne Weiteres weder ermittelbar noch nachvollziehbar sein.

Neben einer Vereinheitlichung auf der Basis von Rechtsverletzungen im Sinn des § 1 Abs. 1 S. 2 a-c GgdG-E sieht § 2 GgdG-E auch eine Erweiterung der auskunftsfähigen Daten vor. Bisher stellt § 21 TDDDG auf Bestandsdaten ab. In Zukunft werden neben den Bestandsdaten auch IP-Adresse, Zeitstempel und Portnummer erfasst sein (§ 2 Abs. 2 GgdG-E). Dem liegen die bereits am 22. April 2026 im Kabinett beschlossenen Änderungen der §§ 174ff TKG-E zugrunde (vgl. insbesondere § 174 V 9 TKG-E). Sie sehen u.a. eine unterschieds- und anlasslose Speicherung der genannten Daten für die Dauer von drei Monaten vor. Damit

ist das Thema Vorratsdatenspeicherung erneut auf dem Tisch. Dabei dürfte die Gesetzgebung von einer Lockerung der grundrechtlichen Anforderungen durch die Entscheidung EuGH, C-470/21 vom 30. April 2024 – *La Quadrature de Net* u.a. ausgegangen sein.

Unionsrechtliche Grundlagen und Grenzen

Vorratsdatenspeicherung kann gerade in Deutschland auf eine lebhafte Rechtshistorie zurückblicken. Die Rechtsprechung von BVerfG und EuGH setzt ihr 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.

In *La Quadrature de Net* u.a. hat der EuGH nun eine Präzisierung vorgenommen. Dabei fokussiert er den Zusammenhang von Eingriffsintensität, Profilbildung und Rechtsgutschutz bzw. Verfolgung von Gemeinwohlzielen. Der EuGH geht davon aus, dass eine anlass- und unterschiedslose IP-Adressspeicherung nicht nur zur Bekämpfung schwerer Kriminalität, sondern auch bei der Bekämpfung von Straftaten imAllgemeinen 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 sicherzustellen, dass keine Verknüpfungen mit Verkehrs- oder Standortdaten stattfinden, sondern ausschließlich auf die Identifikation der betreffenden Person abgestellt wird. Dreh- und Angelpunkt ist also auch hier – weiterhin – die Profilbildung.

Bereits an dieser Stelle ergeben sich grundrechtliche Schwierigkeiten mit § 2 GgdG-E. Über die Integration von Portnummern und Zeitstempel (vgl. § 176 Abs. 1 1-4 TKG-E) ermöglicht die Bestimmung nicht nur die Identifikation von Geräten im mobilen Netz und öffentlichen WLAN, sondern auch eine Erstellung von Standort- und Bewegungsprofilen. Dass es sich dabei um keine Ermächtigungsgrundlage, sondern lediglich um eine tatsächliche Möglichkeit für Profilbildung handelt, ist unionsrechtlich unerheblich. Der EuGH stellt genau auf tatsächliche Möglichkeiten ab, wenn er Profilbildung mit hoher Eingriffsintensität verbindet. Eine Rechtfertigung wird damit nur mehr zum Zweck der Bekämpfung schwerer Kriminalität und Verhütung schwerer Bedrohungen der öffentlichen Sicherheit denkbar sein.

Damit 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 nunmehr über die Vereinheitlichung relevanten Delikte des § 1 Abs. 1 S. 2 a-c GgdG-E fallen. Die erste Frage bemisst sich dem EuGH zufolge – soweit es keine einschlägigen Unionsrechtsregelungen 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. April 2024). Ohne die Einordnung der in § 1 Abs. 1 S. 2 a-c GgdG-E abschließend vorzunehmen, ist auf Folgendes hinzuweisen: Lediglich ein Bruchteil der genannten Delikte ist 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 ein 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 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. Eine grundrechtskonforme Zweck-Mittel-Relation dürfte der Gesetzesentwurf verfehlen.

Spitzfindigkeiten angesichts systematischer Straflosigkeit?

Sind das nicht alles nur Spitzfindigkeiten angesichts der grassierenden digitalen Gewalt? Diese Frage kann sich auch mit Blick auf die weiteren Verhältnismäßigkeitserwägungen des EuGH stellen: So berücksichtigt auch *La Quadrature de Net* u.a., mit Blick auf online begangene oder durch das Internet in der Begehung oder Verbreitung erleichterte Straftaten – also die hier einschlägigen digitalen Straftaten, dass eine anlass- und unterschiedslose IP-Adressspeicherung als effektivste und grundrechtsschonendste Maßnahme zu werten sein kann. Maßgeblicher Abwägungsumstand ist für den Gerichtshof dabei die Gefahr systematischer Straflosigkeit bei fehlendem Zugang zu IP-Adressen (Rz 119).

Rasch ist man an den Fall Collien Fernandes erinnert, die sich angesichts der Kultur von Straflosigkeit in Deutschland vorerst an die spanischen Instanzen gewandt hatte. Dass sich der angesprochenen Kultur jedoch mit einer unterschieds- und anlasslosen IP-Adressspeicherung effektiv begegnen ließe, vermögen die relevanten Gesetzesentwürfe nicht evidenzbasiert zu begründen. Vielmehr zeigt die jüngst veröffentlichte Dunkelfeldstudie LeSuBiA (auch) im digitalen Gewaltbereich eine signifikant niedrige Anzeigequote (2,4 Prozent unter Frauen / 0,9 Prozent unter Männern). Nach wie vor fehlt es an zentralen Zuständigkeiten und flächendeckenden Weiterbildungen im Bereich digitale Gewalt. Demokratiefördernde Projekte werden gestrichen; die Chance zur Einführung einer Verbandsklage wurde vergeben. All diese Faktoren indizieren eine Begünstigung von systematischer Straflosigkeit, denen sich mit weniger eingriffsintensiven Maßnahmen begegnen ließe: etwa durch die Schaffung zentraler Zuständigkeiten für digitale Gewalt, vergleichbar etwa mit der Zentralen Ansprechstelle Cybercrime für die Wirtschaft (ZAC) in Berlin und einer finanziellen Stärkung zivilgesellschaftlicher Anlaufstellen, wie etwa im Fall der neu geschaffenen Beratungsstelle QueerSafe (ebenfalls Berlin) – potentiell ausgestattet mit Verbandsklagerechten. Dem wäre eine umfassende Erfüllung der durch Art. 11 der Istanbul-Konvention begründeten Verpflichtungen zur Datenerhebung vorzuschalten. Sie ist Voraussetzung für evidenzbasiertes Vorgehen. Und noch einmal anders gedacht: Selbst – wie ursprünglich vorgesehen – erst einmal dem *Quick-Freeze*-Verfahren eine Chance zu geben, hätte die Eskalationsspirale der Eingriffsintensität sanfter gedreht. Warum es notwendig war, unmittelbar zu einer unterschieds- und anlasslosen Speicherung von IP-Adressen zu greifen, wäre noch substantiiert zu begründen. Gleiches gilt für die Speicherdauer. Denn jedenfalls ist eine solche Datenspeicherung nach dem EuGH auf das zeitlich absolut notwendige Minimum zu beschränken. Wieso dieses ausgerechnet bei drei Monaten ansetzen sollte, ist bisher nicht nachvollziehbar dargelegt.

Zurück bleiben Zweifel

Der Gesetzesentwurf versteht digitale Gewalt als „Handlungen im digitalen Raum oder mit digitalen Mitteln, die in rechtlich geschützte Güter, oft Persönlichkeitsrechte, eingreifen. Kennzeichnend ist die Nutzung digitaler Kommunikationsmittel und informationstechnischer Infrastrukturen". Als solche ist sie Ausdruck gesellschaftlicher Macht- und Ungleichheitsverhältnisse. Das bringt auch Justizministerin Hubig zum Ausdruck, wenn sie sich auf Gisèle Pelicot und den Anspruch beruft, dass die Scham die Seite wechseln muss. Neben Frauen sind etwa Queers oder

Rassismusbetroffene besondere Ziele digitaler Gewalt. Strukturell ist sie auf (Wieder)Herstellung einer spezifischen Geschlechterordnung, (Re)Etablierung von Rassismen als Struktur unserer Gesellschaft gerichtet. Im Einzelfall drücken sich diese Versuche als Überwachung, Kontrolle und Einschüchterung – in Form von *Deepfakes, Doxing oder Hate Speech* – aus. Selbst wenn wir (nur) diese Ausdrucksformen bekämpfen wollen, braucht es Auseinandersetzung mit diesen Zusammenhängen. Das zeigen Ergebnisse wie die Dunkelfeldstudie LeSuBiA. Es braucht Fragen nach der positiven Dimension von Meinungsfreiheit (wessen Freiheit schützt der Staat?), nach dem der Meinungsfreiheit inhärenten Gleichheitsanspruch und der Gefahr, vulnerable Stimmen im (digitalen) Forum demokratischer Meinungsbildung zu verlieren. Wie schon Aufarbeitungen der sogenannten Kölner Silvesternacht gezeigt haben, bergen oberflächliche Aufmerksamkeitskonjunkturen die Gefahr, feministische Anliegen als Stützpfeiler von Grundrechtseinschränkungen und Repressionen zu funktionalisieren. Die aktuellen Debatten um digitale Gewalt bieten eine Chance, es anders zu machen. Es wäre schade, sie zu verpassen. Gerade in Zeiten, in denen Rufe nach Schutz unserer Demokratie lauter und lauter werden.

AUTOR*IN

Petra Sußner

Prof. Dr. Petra Sußner hat an die Gastprofessur für Recht, insbesondere Geschlechterfragen im Recht der Hochschule Wirtschaft und Recht Berlin inne.

EMPFOHLENE ZITATION

Sußner, Petra: In wessen Namen?: Zur Verknüpfung von Gewaltschutz und IP-Adressspeicherung, Verfassungsblog, 12.06.2026, doi: 10.59704/57d5fc48e8e0e84a.

Lizensiert unter CC BY-SA 4.0.

Langzeitarchiviert bei IntRechtDok unter: doi.org/10.17176/20260612-190652-0.