



GESELLSCHAFT
FÜR INFORMATIK

Berlin, 27. Februar 2025

Stellungnahme

der Gesellschaft für Informatik e.V. (GI)

Entwurf eines Gesetzes zur Stärkung der privaten Rechtsverfolgung im Internet

Stand 09.12.2024



Sachstand

Mit voranschreitender Digitalisierung und zunehmender Nutzung sozialer Medien hat das Phänomen digitaler Gewalt dramatisch an Bedeutung gewonnen. Besonders alarmierend ist, dass Frauen fast doppelt so oft von digitaler Gewalt betroffen sind, etwa von Cyberstalking, Hassnachrichten und Mobbing oder Cybergrooming¹. Gleichzeitig werden auch immer mehr Jugendliche mit digitaler Gewalt konfrontiert². Die Folgen sind gravierend: Knapp jede*r zweite Betroffene zieht sich aus digitalen Räumen zurück, Frauen eher als Männer³.

Das Bundesministerium der Justiz hat nun einen Gesetzentwurf zur „Stärkung der privaten Rechtsverfolgung im Internet“ vorgelegt. Er zielt darauf ab, Betroffenen von digitaler Gewalt bessere Möglichkeiten zu geben, ihre Rechte durchzusetzen und zukünftigen Rechtsverletzungen vorzubeugen. Hierbei stehen insbesondere zwei Aspekte im Vordergrund: Personen hinter Rechtsverletzungen sollen durch verbesserte Auskunftsverfahren leichter identifiziert werden. Außerdem soll es möglich werden, Nutzerkonten bei schwerwiegenden Rechtsverletzungen mit richterlicher Anordnung zu sperren.

Als GI begrüßen wir grundsätzlich legislative Initiativen gegen digitale Gewalt, sehen jedoch bei diesem Entwurf einige Aspekte kritisch. Der Ansatz des Gesetzes ist eine zivilrechtliche Rechtsdurchsetzung. Dies setzt „wehrhafte Betroffene“ voraus und lässt damit besonders vulnerable Gruppen wie Kinder und Jugendliche, Menschen mit kognitiven Einschränkungen oder marginalisierte Gesellschaftsgruppen außen vor.

Zudem ist es fraglich, ob die Ausrichtung auf gerichtliche Verfahren geeignet ist, Betroffene im ersten Schritt vor gewaltausübenden Inhalten im Netz zu schützen. Hier bräuchte es präventive Maßnahmen und niedrigschwellige Interventionsmöglichkeiten.

Die GI sieht ein Missverhältnis zwischen der Einordnung als „Gesetz gegen digitale Gewalt“ und dem tatsächlichen Regelungsinhalt. Der Inhalt des Gesetzes ist im Kern ein Gesetz zur Verbesserung zivilrechtlicher Auskunftsverfahren und Klageerleichterungen, suggeriert aber eine Bekämpfung digitaler Gewalt. Diese Diskrepanz kann in der Öffentlichkeit zu falschen Erwartungen führen.

¹ BKA (2024): Bundeslagebild „Geschlechtsspezifisch gegen Frauen gerichtete Straftaten 2023“. 19.11.2024; https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/241119_BLBStraftatengegen-Frauen2023.html (zuletzt abgerufen 26.02.2025)

² Rieger (2024): Jeder fünfte Schüler wird Opfer von Cybermobbing. Tagesschau. 24.10.2024; <https://www.tagesschau.de/inland/gesellschaft/studie-cybermobbing-102.html> (zuletzt abgerufen 26.02.2025)

³ Rafael (2023): Frauenhass online: Hatespeech und digitale Gewalt. In: Institut für Demokratie und Zivilgesellschaft (Hg.). Wissen schafft Demokratie. Schwerpunkt Antifeminismus & Hasskriminalität, Band 13, Online-Ausgabe. Jena, 294–305. <https://www.idz-jena.de/wsddet/wsd13-24> (zuletzt abgerufen 26.02.2025)



Rechtliche Dimension

Die GI begrüßt eine Stärkung der Rechtsdurchsetzung bei digitaler Gewalt. Das verbesserte Auskunftsverfahren zur Identifizierung von Rechtsverletzer*innen, die Möglichkeit richterlich angeordneter Accountsperrung sowie die Einbindung zivilgesellschaftlicher Organisationen als Prozessvertretungen sind wichtige Fortschritte.

Allerdings bezweifeln wir, dass ein primär zivilrechtlicher Ansatz dem Phänomen digitaler Gewalt wirksam begegnen kann. Besonders vulnerable Personen wie behinderte Personen, die Unterstützung benötigen, brauchen spezialisierte Anlaufstellen. Diese Stellen sowie die zuständigen Ermittlungsbehörden müssen deutlich besser finanziell ausgestattet werden, um der Vielzahl an Vorfällen nachzugehen.

Ein weiteres und bekanntes Problem ist die internationale Dimension: Viele Plattformbetreiber haben ihren Sitz außerhalb der EU. Der Gesetzentwurf adressiert dies zwar mit inländischen Zustellungsbevollmächtigten (§9), bietet jedoch keine ausreichenden Durchsetzungsmechanismen bei verweigerter Kooperation. Dies ist problematisch, da digitale Gewalt mit einfachen Mitteln gegen viele Opfer ausgeübt werden kann, während sich Plattformbetreiber häufig nicht zuständig fühlen.

Angesichts der Privilegien, die Plattformbetreiber und -nutzende genießen (Nichthaftung nach DSA, Recht auf Anonymität) und der zunehmenden digitalen Gewalt ist fraglich, ob zivilrechtliche Instrumente für eine gesellschaftlich wünschenswerte Balance ausreichen, zumal die Verhinderung von Gewalt nicht Aufgabe des Zivilrechts ist.

Die GI fordert aus diesem Grund eine verpflichtende Zusammenarbeit von Plattformen mit Opferschutzverbänden, um wirksame Präventions- und Interventionsstrategien zu entwickeln.

Zudem muss die hohe Dynamik digitaler Kommunikation durch beschleunigte Wirksamkeitsanalysen der getroffenen Maßnahmen berücksichtigt werden.

Technische Dimension

Auf der technischen Ebene sehen wir mehrere Hürden, die eine effektive Wirksamkeit des Gesetzes verhindern. Neue Bedrohungen wie KI-Deepfakes, Smart-Home-Missbrauch und biometrische Datenmanipulation erfordern ein dynamisches Regulierungskonzept. Die GI fordert daher, die Definition relevanter Diensteanbieter (§1) häufiger als im Fünf-Jahres-Turnus zu aktualisieren.

Eine Beweissicherung erst nach der Einleitung eines Auskunftsverfahrens (§2, §3) kommt zu spät. Eine temporäre Sicherung sollte bereits bei Verdachtsmeldungen erfolgen. Ebenso setzt sich die GI dafür ein, dass Pseudonymisierung für beschuldigte Personen (§6) und Betroffene gleichermaßen implementiert wird, um letztere vor zukünftiger Gewalt zu schützen.



Eine Begrenzung der Kontosperrung mit Lesezugang (§4) auf 30 Tage greift bei Fällen wie Stalking zu kurz. Wiederholte Verstöße sollten stärkere Konsequenzen wie Pflichtschulungen oder verstärkte Inhaltskontrolle nach sich ziehen. Zudem stellt sich die Frage nach einer standardisierten Erfassung von Vorfällen durch

zentrale und dezentrale technische Anlaufstellen mit ausreichend geschultem Personal sowie standardisierte Schnittstellen für Meldung und Dokumentation von Vorfällen. Die GI setzt sich daher für niedrighschwellige, teilautomatisierte Meldemöglichkeiten ein. Plattformen sollten mit technischer Unterstützung zur Erleichterung der Rechtsverfolgung beitragen. Zudem sprechen wir uns für eine öffentlich einsehbare Dokumentation nachgewiesener Verstöße bei Diensteanbietern aus.

Gesellschaftliche Dimension

Die GI unterstützt die Ergänzung von Cybergrooming in den Straftatenkatalog des Gesetzes und begrüßt, dass der Gesetzesentwurf zentrale gesellschaftliche Herausforderungen erkennt: Er betont die Gefährdung demokratischen Zusammenlebens durch Hasskriminalität und zielt darauf ab, Diskriminierung zu bekämpfen und die Geschlechtergleichstellung zu fördern.

Die GI kritisiert jedoch, dass Instrumente wie Auskunftsverfahren und Kontosperrungen zwar wichtige rechtliche Handlungsmöglichkeiten bieten, der Gesetzesentwurf jedoch wenig präventiv denkt. Wir sprechen uns daher für wirksamen Schutz vulnerabler Gruppen, Diskriminierungsbekämpfung und Förderung demokratischer Teilhabe durch geeignete Maßnahmen aus: Dazu gehören niedrighschwellige Meldemechanismen, psychosoziale Unterstützungsangebote, systematische Prävention, spezifische Schutzmaßnahmen für besonders gefährdete Gruppen sowie digitale Teilhabeförderung. Besonders besorgniserregend sind die langfristigen gesellschaftlichen Folgen: Der Rückzug aus digitalen Räumen führt zu einer demokratischen Teilhabekrise, vor allem für marginalisierte Gruppen. Besonders politisch aktive Frauen schränken ihr öffentliches Engagement ein. Solche Rückzüge haben starke Auswirkungen auf die Diversität politischer Debatten⁴.

Fazit und Forderungen

Die GI begrüßt die Bestrebung, dem drängenden Problem digitaler Gewalt entgegenzutreten. Der vorgelegte Entwurf greift jedoch zu kurz und weist eine Diskrepanz zwischen Anspruch und Wirklichkeit auf: Die Einordnung des Entwurfs als „Gesetz gegen digitale Gewalt“ suggeriert umfassende Maßnahmen zur Bekämpfung dieses vielschichtigen Phänomens. Hier handelt es sich im Kern jedoch um ein Gesetz zur Verbesserung zivilrechtlicher Auskunftsverfahren, das vorrangig die wirtschaftlichen Interessen verschiedener Akteure austariert. Diese Einordnung weckt falsche Erwartungen und lenkt davon ab, dass umfassendere, präventive Maßnahmen notwendig sind.

⁴ bidt (2025): Neue Studie: Digitale Gewalt schreckt Menschen ab, politische Verantwortung zu übernehmen. 17.01.2025; <https://www.bidt.digital/neue-studie-digitale-gewalt-schreckt-menschen-ab-politische-verantwortung-zu-uebernehmen/> (zuletzt abgerufen 26.02.2025)



Wir fordern daher für ein besseres, präventives Angebot gegen digitale Gewalt:

1. **Digitale Gewaltprävention in Bildungseinrichtungen und Aufbau resilienter Räume:** Aufklärung und Sensibilisierung müssen systematisch in Lehrpläne und pädagogische Konzepte integriert werden, wobei die Schnittstelle zwischen digitalem und physischem Raum besondere Beachtung verdient. Notwendig sind durchdachte Konzepte, die digitale Teilhabe fördern und gleichzeitig vor Risiken schützen. Medienkompetenz darf nicht im Klassenzimmer enden, sondern muss allen Generationen vermittelt werden, um eine resiliente Gesellschaft zu gestalten.
2. **Eine neue Verantwortung für digitale Plattformen:** Das gegenwärtige Plattformprivileg führt zu einer Machtasymmetrie zwischen Täter*innen und Opfern. Dieses Privileg muss überarbeitet und der Umgang mit digitaler Gewalt international harmonisiert werden, um Opfer zu unterstützen.
3. **Entwicklung spezifischer Schutzkonzepte für besonders gefährdete Gruppen:** Die Konzepte müssen den digitalen wie auch den physischen Raum berücksichtigen und ihre Wechselwirkungen einbeziehen.

Angebot der GI zur Zusammenarbeit

Die GI als größte Vereinigung von Informatikerinnen und Informatikern im deutschsprachigen Raum bietet ausdrücklich ihre Expertise an, um bei der Weiterentwicklung des Gesetzesentwurfs und der Implementierung technischer Lösungen mitzuwirken. Wir sind überzeugt, dass nur ein ganzheitlicher und interdisziplinärer Ansatz dem komplexen Phänomen digitaler Gewalt wirksam begegnen kann.

Unsere Fachpersonen aus den Bereichen IT-Sicherheit, Datenschutz, Plattformarchitektur und algorithmische Systeme stehen bereit, um:

- Standardisierungskonzepte für Melde- und Dokumentationsschnittstellen mitzuentwickeln,
- technische Konzepte für Pseudonymisierungs- und Identifizierungsmechanismen zu erarbeiten,
- in einem interdisziplinären Expertengremium die dynamische technologische Entwicklung zu begleiten,
- Empfehlungen für technische Schutzmaßnahmen zu entwickeln, die Grundrechte wahren und gleichzeitig effektiven Schutz bieten



GESELLSCHAFT
FÜR INFORMATIK

Kontakt

Nikolas Becker
Leiter Politik & Wissenschaft
Gesellschaft für Informatik e.V. (GI)
Geschäftsstelle Berlin im Spreepalais am Dom
Anna-Louisa-Karsch-Str. 2, 10178 Berlin
E-Mail: Nikolas.Becker@gi.de
Tel: +49 1767 322 404 3

Über die Gesellschaft für Informatik e.V. (GI)

Die Gesellschaft für Informatik e.V. (GI) ist die größte Fachgesellschaft für Informatik im deutschsprachigen Raum. Seit 1969 vertritt sie die Interessen der Informatikerinnen und Informatiker in Wissenschaft, Gesellschaft und Politik und setzt sich für eine gemeinwohlorientierte Digitalisierung ein. Mit 14 Fachbereichen, über 30 aktiven Regionalgruppen und unzähligen Fachgruppen ist die GI Plattform und Sprachrohr für alle Disziplinen in der Informatik. Weitere Informationen finden Sie unter www.gi.de.