EIN—TEAM.org
Eine Initiative des ITUJ e.V.

Stellungnahme zum „Entwurf eines Gesetzes zur Stärkung des zivilrechtlichen und strafrechtlichen Schutzes vor digitaler Gewalt (GgdG)“ des Bundesjustizministeriums vom 16. April 2026

22. Mai 2026

Digitale Gewalt umfasst neben Hatespeech und bildbasierter Gewalt auch verschiedene Methoden der Ortung, Überwachung und Nötigung mit technischen Mitteln im sozialen Nahfeld. Ein Gesetz, das digitale Gewalt in den Blick nimmt, muss diesen unterschiedlichen Gewaltformen angemessen begegnen.

Die Initiative „Ein Team gegen digitale Gewalt“ und ihr Trägerverein, das Institut für Technik und Journalismus e.V., begrüßen die Verbesserungen, die im aktuellen Diskussionsentwurf gegenüber der Version von 2024 vorgenommen wurden. Dennoch enthält der Entwurf noch gravierende Lücken bei bestimmten Gewaltformen (siehe Abschnitt 1).

Auch die Handlungsmaxime „erst stoppen, dann ermitteln“ wurde unserer Einschätzung nach nicht ausreichend berücksichtigt (siehe Abschnitt 2). Vor allem setzt der Entwurf voraus, dass Verbindungsdaten aller Nutzer*innen dauerhaft von Diensteanbietern vorgehalten werden. Dies entspricht unserer Einschätzung nach einer anlasslosen Vorratsdatenspeicherung, die wir entschieden ablehnen.

1. Bluetooth-Tracker, Stalkerware und IoT-Geräte

Der vorliegende Entwurf führt mit dem Paragrafen §202e GdgG einen neuen Straftatbestand ein, der „unbefugte Überwachung mittels Informations- oder Kommunikationstechnik“ adressiert. Wir begrüßen diese Neuerung ausdrücklich, da sie erstmals eine rechtliche Handhabe für die Gewaltausübung mit technischen Hilfsmitteln wie Bluetooth-Trackern, internetfähigen Kameras oder sogenannter Stalkerware bietet.

> Definition Stalkerware: Smartphone-Apps, die heimlich Standort und Aktivitäten überwachen. Sie verstoßen gegen die Richtlinien der App-Stores, weil sie in der Lage sind, sich auf dem Handy zu tarnen, können aber außerhalb der App-Stores auf den Webseiten der Anbieter von jeder Privatperson erworben und installiert werden.

Institut für Technik und Journalismus e.V. (ITUJ e.V.)
Linienstraße 13 | D-10178 Berlin

Amtsgericht (Charlottenburg) VR 27591 B
GLS Bank | DE59 4306 0967 11020509 00 | GENODEM1GLS

Zivilrechtlicher Weg ist derzeit ausgeschlossen: Allerdings reicht die bloße Etablierung des Straftatbestandes nicht aus. Auch mit der neuen Regelung dürfte eine Strafverfolgung regelmäßig daran scheitern, dass Täter*innen nicht eindeutig identifiziert werden können. Weiterhin liefert die Regelung in der jetzigen Fassung keine Hilfe für Betroffene bei der Durchsetzung ihrer Ansprüche auf zivilrechtlichem Wege (z.B. Unterlassungsansprüche). Insbesondere für Betroffene, die sich aus verschiedenen Gründen nicht an die Polizei wenden wollen, verbessert sich die Situation damit nicht.

Kein Schutz vor Wiederholungen: Die Überwachung durch AirTags, internetfähige Kameras und Stalkerware lässt sich zwar in einigen Fällen temporär beenden, indem man die Geräte, bzw. die Software aufspürt. Es gibt aber keinerlei Schutz vor Wiederholungstaten, da die Überwachungsmittel immer wieder neu platziert werden können. Auch dagegen bietet der Entwurf in der jetzigen Fassung keine Handhabe.

Unserer Einschätzung nach bleibt §202e GdgG damit in seiner jetzigen Form weitgehend wirkungslos.

Diese Mängel ließen sich in vielen Fällen aus dem Weg räumen, wenn es für die in §202e genannten Delikte ebenfalls einen Auskunftsanspruch beim jeweiligen Diensteanbieter sowie eine beweissichernde Anordnung gäbe, wie in §2 und §3 des vorliegenden Entwurfes für andere Tatbestände definiert, sowie – in angepasster Form – eine Möglichkeit zur Accountsperre, wie in §4 GdgG vorgesehen.

Dies ließe sich zum Beispiel umsetzen, indem §202e in den Straftatenkatalog unter §1 (1) 2 GdgG aufgenommen wird, und die Definition der Diensteanbieter um solche Diensteanbieter erweitert würde, die Software as a Service anbieten. Weiterhin müsste die Definition des Nutzerkontos unter §1(7) GdgG entsprechend erweitert werden.

Erläuterung: Bluetooth-Tracker (z.B. AirTags), internetfähige Kameras (z.B. Ring) und andere iOT-Geräte sind keine alleinstehenden Hardware-Geräte. Sie funktionieren in aller Regel nur mit dem zugehörigen Diensteanbieter, der die entsprechende Funktionalität als SaaS-Anbieter (Software as a Service) auf seinen Servern bereitstellt. So funktioniert die Standortüberwachung mittels AirTag beispielsweise nur über den Standortdienst, den Apple bereitstellt. Für die Nutzung ist ein Nutzerkonto notwendig, in diesem Fall ein iCloud-Konto von Apple. Auch Stalkerware wird von Diensteanbietern bereitgestellt und benötigen ein Nutzerkonto, um die Informationen vom überwachten Gerät abzurufen.

2. Erst Stoppen, dann Ermitteln

Fachkräfte, Verbände und Organisationen, die gewaltbetroffene Menschen unterstützen, fordern seit Jahren einhellig, beim Gewaltschutz der Handlungsmaxime „erst stoppen, dann ermitteln“ zu folgen. Insbesondere bei gewaltausübenden Inhalten, die auf Plattformen und in Messenger-Gruppen verbreitet werden, ist es entscheidend, diese zeitnah und effektiv aus der Öffentlichkeit zu entfernen, um die Gewaltwirkung auf Betroffene zu stoppen und die Weiterverbreitung zu unterbinden.

Hierzu wäre ein schnelles, niedrigschwelliges Verfahren nötig, welches zumindest eine temporäre Accountsperre und damit einhergehende Beseitigung der rechtsverletzenden Inhalte ermöglicht. Der vorliegende Gesetzesentwurf genügt dieser Anforderung unserer Einschätzung nach nicht. Im Gegenteil liegen die Voraussetzungen für eine Accountsperre zu hoch und setzen ein langwieriges Verfahren voraus, bei dem zunächst eine Unterlassungserklärung eingeholt und eine Wiederholungsgefahr erwiesen werden muss. Weiterhin wäre es dringend notwendig, dass Betroffene auch die Löschung von Facebook- und Messenger-Gruppen erwirken können, sofern diese Gruppe zum Zweck einer Rechtsverletzung nach §1 (1) 2 GdgG besteht.

Auch der Vorbehalt der „Zumutbarkeit“, der in § 4 Abs. 2 Satz 3 GdgG formuliert wurde, ist in diesem Kontext kritisch zu betrachten. Es ist zu erwarten, dass Diensteanbieter versuchen werden, sich auf dieser Grundlage der Pflicht zu entziehen, das neue Anlegen von Nutzerkonten zu unterbinden. Eine wirksame Beendigung der Gewalt wird damit unterlaufen.

3. Betroffenenschutz stärken

Der Gesetzesentwurf beinhaltet keine Regelung, die es Betroffenen erlaubt, ein Auskunftsersuchen oder eine Accountsperre zu beantragen, ohne dabei die eigene Privatanschrift offenzulegen.

Dies stellt eine hohe Hürde für Betroffene dar, da diese befürchten müssen, dass durch die Offenlegung der Privatadresse zu der digitalen Gewalt auch physische Gewalt am eigenen Wohnort hinzukommt. Unserer Einschätzung nach wäre die Offenlegung der Privatadresse insbesondere dann nicht zwingend notwendig, wenn Betroffene anwaltlich vertreten werden. Wir empfehlen daher, den Entwurf um eine Möglichkeit zur Angabe einer c/o-Adresse zu ergänzen.

4. Gewaltschutz ist keine Rechtfertigung für Vorratsdatenspeicherung

Das geplante Auskunftsverfahren nach §2 basiert implizit darauf, dass Diensteanbieter die Verbindungsdaten aller Nutzer*innen anlasslos für einen längeren Zeitraum speichern. In unserer Wahrnehmung handelt es sich dabei um eine anlasslose Vorratsdatenspeicherung, welche gravierende negative Auswirkungen auf den freien öffentlichen Diskurs und die demokratische Meinungsbildung hätte und einen tiefen Eingriff in die Grundrechte darstellt.

Der Schutz vor digitaler Gewalt darf nicht als Vorwand dafür dienen, eine solche Vorratsdatenspeicherung einzuführen.

Eine dauerhafte, anlasslose Speicherung von Verbindungsdaten aller Nutzenden ist für das Verfahren „Auskunft über Daten“, wie in §2 GdgG beschrieben, unserer Einschätzung nach nicht notwendig. Insbesondere mit Quick-Freeze und der Login-Falle wurden in der Vergangenheit bereits detaillierte Verfahren beschrieben, die eine deutlich niedrigere Eingriffsintensität haben und gleichwertige Ergebnisse erzielen können.

> Bei der Login-Falle können Diensteanbieter auf richterliche Anordnung hin eine Speicherung der Verbindungsdaten für ein bestimmtes, vom Gericht benanntes Nutzerkonto veranlassen. In dem Moment, in dem sich der*die Nutzende nach dieser Anordnung das nächste Mal ins betreffende Nutzerkonto einloggt, werden die Verbindungsdaten gespeichert und können zur weiteren Identifizierung herangezogen werden.

Da nahezu alle hier adressierten Rechtsbrüche über Diensteanbieter mit Nutzerkonten erfolgen, wäre dieses Verfahren geeignet.

5. Über die Organisation

Die Initiative Ein Team gegen digitale Gewalt schult und berät Beratungsstellen und Frauenhäuser bundesweit zur technischen Sicherheit privater Kommunikationsmittel. Der Trägerverein Institut für Technik und Journalismus e.V. reagiert mit der Initiative auf die seit Jahren bestehende Nachfrage nach Fortbildung im Unterstützungssystem.