Stellungnahme von SUPERRR Lab zum Eckpunktepapier für ein Gesetz gegen digitale Gewalt

Mai 2023

SUPERRR Lab SL gGmbH
Oranienstr. 58 A
10969 Berlin

1. Einleitung

Als Organisation, die sich für feministische digitale Zukünfte einsetzt, begrüßt SUPERRR Lab den Vorstoß des Bundesministeriums der Justiz, sich mit digitaler Gewalt als Phänomen zu befassen.

Digitale Gewalt wird oft im Kontext von Gewalt gegen Frauen betrachtet, betrifft aber viele Menschen und insbesondere Menschen mit mehrfacher Marginalisierungserfahrung.[1] Die Konsequenzen sind gesellschaftlich spürbar: Weil sie beispielsweise Ziel von Hass- und Verleumdungskampagnen online waren, ziehen sich Betroffene aus dem digitalen Raum zurück.[2] Daher braucht es für den deutschen Kontext Maßnahmen, die die Besonderheiten der verschiedenen Betroffenengruppen im Blick haben und ihnen schnell, verhältnismäßig und effektiv helfen. Dies ist auch so im Koalitionsvertrag der Bundesregierung festgehalten. Dort steht, die Regierung wird „eine ressortübergreifende politische Strategie gegen Gewalt entwickeln, die Gewaltprävention und die Rechte der Betroffenen in den Mittelpunkt stellt." Dazu zählt eine „verlässliche Finanzierung von Frauenhäusern". Zudem plant die Regierung, „die Istanbul-Konvention [...] auch im digitalen Raum und mit einer staatlichen Koordinierungsstelle vorbehaltlos und wirksam um[zusetzen]."

Das Bundesministerium der Justiz hat vor diesem Hintergrund ein Eckpunktepapier für ein Gesetz gegen digitale Gewalt vorgestellt, welches diesen Erwartungen jedoch nicht umfassend gerecht wird.

2. Fehlende Definition von digitaler Gewalt

Eine Leerstelle in den Eckpunkten zum geplanten Gesetz gegen digitale Gewalt ist die fehlende Definition des Anwendungsfeldes. Es lassen sich vor allem zwei Formen digitaler Gewalt unterscheiden: Plattformbasierte digitale Gewalt und technologiebasierte digitale Gewalt. Formen von plattformbasierter digitaler Gewalt umfassen unter anderem Belästigung, Cybermobbing, Cyberstalking, Doxxing, Gewaltandrohungen. Technologiebasierte digitale Gewalt bezeichnet beispielsweise das Installieren von Spy- und Stalkerware, die Nutzung von Überwachungskameras und Apps, um Betroffene auszuspionieren, heimlich zu filmen oder zu tracken.

Das Eckpunktepapier bezieht sich ausschließlich auf Teilbereiche der plattformbasierten digitalen Gewalt, konkret auf Persönlichkeitsverletzungen wie Beleidigungen, Bedrohungen und Verleumdungen, nicht aber auf andere Aspekte wie z. B. Volksverhetzung. Gleichzeitig erstreckt das Eckpunktepapier den digitalen Gewaltbegriff auf alle Fälle, die eine Verletzung absoluter Rechte darstellt – und stellt so nebenbei sicher, dass Restaurants vor negativen Kommentaren nicht nur geschützt werden, sondern dass die Auskunftsansprüche von Wirtschaftsinteressen geleitet werden (können).

Ohne fehlende Definition wird verkannt, wer besonders oft von digitaler Gewalt betroffen ist: Digitale Gewalt betrifft vor allem Menschen mit

[1] https://undocs.org/en/A/76/258 II B 19.

[2] https://undocs.org/en/A/HRC/47/25 II C 27.

Marginalisierungserfahrung, insbesondere mehrfach marginalisierte Menschen. Ohne einen differenzierten Blick, gegen wen und mit welchen Mitteln welche Arten von digitaler Gewalt gerichtet werden, kann keine differenzierte Evaluation und sinnvolle Priorisierung von Maßnahmen stattfinden.

Eine klare Definition von digitaler Gewalt und ihren unterschiedlichen Ausprägungen ist deshalb dringend notwendig und den Betroffenen geschuldet.

3. Auskunftsverfahren

Den Fokus auf die Auskunft über IP-Adressen sehen wir kritisch, da die Verhältnismäßigkeit zwischen Nutzen und potenziell schwerwiegendem Grundrechtseingriff nicht proportional ist.

Insbesondere bei der Speicherung von IP-Adressen führt ein Auskunftsrecht nicht direkt zu den Inhalteverfasser*innen, sondern zu Anschlussinhaber*innen. Im Fall öffentlicher WLAN-Netze wie z. B. im ÖPNV bieten IP-Adressen ohnehin keinen direkten Anhaltspunkt zur Identifikation. Zudem gibt es ubiquitär verfügbare, einfach zu nutzende technische Mittel, um die IP-Adresse und andere Marker zu verschleiern. Im Fall von Gewalt im sozialen Nahraum ist die IP-Auskunft ohnehin nicht hilfreich: Die Täter*innen, z. B. (Ex-)Partner*innen oder Familienangehörige, sind meist bekannt.

Uns sind keine umfassenden Studien dazu bekannt, wie viele Ermittlungsverfahren zu den im Eckpunktepapier genannten Tatbeständen eingestellt werden müssen, weil die IP-Adresse nicht mehr zugeordnet werden konnte. Für andere Straftatbestände gibt es solche Zahlen jedoch: 2021 scheiterte bei rund bei 3,5 % aller strafrechtlich relevanten Meldungen von dokumentierter sexueller Gewalt gegen Kinder die Identifikation des Anschlusses daran, dass keine IP-Adresse mehr gespeichert war.[3] Deshalb lehnen wir das Auskunftsverfahren ohne vertiefende Forschung dazu, wie groß dieser Faktor im Kontext der „digitalen Gewalt“ ist, ab.

Das Auskunftsverfahren eröffnet neue Gefahren, die bisher unzureichend adressiert wurden: Die Erweiterung des Auskunftsanspruchs auf die Herausgabe auf Nutzungsdaten um „z. B. die IP-Adresse“ auch im Kontext von Messenger- und Internetzugangsdiensten birgt die theoretische Gefahr, durch eine Änderung der Rechtslage oder allein durch gesellschaftlichen Druck auf Kommunikationsdienstleister zu einem Baustein einer ausgeweiteten Vorratsdatenspeicherung auf Anwendungsebene zu werden. Die Ausweitung auf Messenger- und andere Kommunikationsdienste lehnen wir deshalb ab.

Derzeit erläutert nur der Fragenkatalog zum Eckpunktepapier, dass durch diese Regelung keine Anbieter*innen zur Speicherung dieser Nutzungsdaten verpflichtet werden. Dies muss auch in der schriftlichen Fassung des Gesetzentwurfs festgehalten werden, um kein rechtliches Argument für eine gesetzlich mandatierte Datenspeicherung zu liefern.

[3] https://dserver.bundestag.de/btd/20/005/2000534.pdf

4. Ausbau bestehender Kapazitäten statt Kompetenzausweitung zu digitaler Überwachung

Wie im Koalitionsvertrag anerkannt wird, kann digitale Gewalt nicht nur mit juristischen oder gar strafrechtlichen Mitteln angegangen werden. Dieser Fokus verkennt das Ausmaß des Problems. Daher braucht es eine ressortübergreifende Strategie gegen digitale Gewalt, die außerhalb der politischen Silos denkt. Wir brauchen eine Strategie, die mit dem Bundesministerium für Familien, Senioren, Frauen und Jugend (BMFSFJ), dem Bundesministerium für Digitales und Verkehr (BMDV) oder auch der Antidiskriminierungsstelle des Bundes abgestimmt ist und die auch an anderen Stellschrauben als nur juristischen dreht.

Die vielen Institutionen (z. B. Frauenhäuser und andere, nicht staatlich betriebene Anlaufstellen), die schon jetzt Betroffenen vor Ort oder online helfen und juristische sowie technische Hilfe leisten, benötigen strukturelle und nachhaltige Finanzierung, die über Projektfinanzierung hinausgeht. Hier ist ein wichtiger Wirkungshebel, der schnellstmöglich angesetzt werden muss. Im Gegensatz von Polizei und Staatsanwaltschaften sind diese Institutionen häufig staatsfern und knüpfen an sehr unterschiedliche bestehende soziale Strukturen an. Sie sind deshalb besser dazu geeignet, Menschen mit Marginalisierungs- und Diskriminierungserfahrung zu erreichen.

Aus einer intersektionalen feministischen Perspektive müssen Ansätze zur Beseitigung von digitaler Gewalt betroffenenzentriert und evidenzbasiert sein. Um dies zu erreichen, ist grundlegende Forschung und Datenerhebung zu digitaler Gewalt notwendig.