Stellungnahme

von Ann Cathrin Riedel, LOAD e.V. - Verein für liberale Netzpolitik, für die öffentliche Anhörung "Digitale Gewalt gegen Frauen und Mädchen" des Ausschusses Digitale Agenda am 24. März 2021 (Drs. 19/25351)

LOAD e.V.
Verein für liberale Netzpolitik

Reinhardtstraße 5
10117 Berlin

Fon: (030) 69203242
Fax: (030) 2000 3893

info@load-ev.de
www.load-ev.de

Vorsitzende:
Ann Cathrin Riedel

Berlin, 24.03.2021

Allgemeines

Formen digitaler Gewalt richten sich prinzipiell gegen jeden. Jede Person jeglicher geschlechtlichen Identität kann hiervon Opfer werden. Es ist jedoch zu beobachten, dass Frauen und Mädchen deutlich stärker Opfer von digitaler Gewalt werden, auch und insbesondere aufgrund ihres Geschlechts.

Unter digitaler Gewalt lassen sich mehrere Phänomene fassen. Leider wird in der politischen und medialen Debatte, wenn überhaupt, vornehmlich über das Problem von "Hate Speech" im digitalen Raum, insbesondere auf Social-Media-Plattformen diskutiert, obgleich der digitale Raum und das Internet weit mehr umfasst als soziale Medien. Dabei ist "Hate Speech" kein klar juristisch definierter Begriff, es müsste vielmehr von Beleidigungen, Verleumdungen, etc. gesprochen werden. Der Begriff soll dennoch im Folgenden Stellvertretend für diese Straftatbestände genutzt werden.

Folgende Taten müssen – nicht abschließend – unter dem Begriff "digitale Gewalt" diskutiert werden:

- Cybermobbing; Mobbing im digitalen Raum (öffentlich oder in geschlossenen Räumen, z.B. Messenger),
- Cybergrooming; Anbahnung, sexuelle Belästigung, insb. von Minderjährigen
- Doxing, Veröffentlichung von persönlichen/privaten Informationen (Adresse, Fotos, Dokumente, Nachrichten, etc.),
- Einsatz von Stalkerware, digitales Stalking; Einsatz von Apps/Technologie um z.B. Smartphones und die über sie laufende Kommunikation auszuspähen/mitzulesen, Verfolgung durch GPS-Signale, Mitlesen von Informationen durch Zugriff auf Nutzerkonten,
- Versenden sog. "Dickpics"; Versenden von Bilder entblößter männlicher Genitalien,
- Hacking von Smart-Home-Geräten; Fremdsteuerung von Geräten (z.B. Lichter, Rollladen, vergleichbar mit "Telefonterror"),

- Revenge-Porn; Veröffentlichung intimer/sexueller Aufnahmen ohne das Einverständnis der betroffenen Person,
- Einsatz von Deep Fakes / Bildmanipulationen; Manipulation von pornografischem Material (mit Hilfe von künstlicher Intelligenz), indem Identitäten betroffener Person auf die Körper der Darstellerinnen und Darsteller pornografischer Inhalte manipuliert werden.

Vorhandene Studien zeigen, dass Frauen deutlich häufiger als Männer Opfer von Stalking generell sind[1], Opfer von Revenge-Porn und pornografischen Bildmanipulationen/Deep Fakes[2], sowie partnerschaftlicher Gewalt allgemein[3]. Auch zeigen Untersuchungen, dass Frauen deutlich häufiger und insbesondere aufgrund ihres Geschlechts Opfer von sogenannter "Hate Speech" sind. Dabei darf außerdem nicht unterschlagen werden, dass Frauen, die zudem einer Minderheit angehören, d.h. Schwarz oder Frauen of Colour sind, jüdischen oder muslimischen Glaubens sind, und/oder nicht-heterosexuell sind, sowie Transpersonen allgemein, ein deutlich höheres Risiko haben, Opfer digitaler Gewalt zu werden. Dazu gehört "Hate Speech", aber auch das Doxing privater Informationen, wie zum Beispiel der Klarname oder die Privatanschrift.

Frauen werden durch digitale Gewalttaten wie "Hate Speech" und Doxing systematisch versucht aus dem öffentlichen Raum zu verdrängen, der auch im Digitalen ist. Dabei sind vor allem Frauen, die sich für Frauenrechte (z.B. Reproduktions- und Abtreibungsrechte), aber auch die Rechte von Minderheiten (z.B. Gleichstellung, oder gegen Rassismus, Antisemitismus, Antiziganismus, Diskriminierung allgemein, etc.) einsetzen, betroffen. Die Bandbreite reicht hier von Berufspolitikerinnen, über ehrenamtlich Engagierte bis hin zu Aktivistinnen, Journalistinnen und einfachen Bürgerinnen, die sich im Netz äußern möchten. Dieses sogenannte "Silencing"[4], also das mundtot-machen insbesondere von Frauen, muss deutlich stärker als Angriff auf die freiheitliche, liberale, demokratische Gesellschaft gewertet werden. Außerdem muss deutlich stärker erkannt und benannt werden, dass Frauenhass, d.h. Misogynie, nebst Antisemitismus und Rassismus eines von drei großen Leitmotiven von Rechtsextremisten ist[5]. Veröffentlichte Manifeste von rechtsextremistischen Terroristen geben dies wider. Auch die Bedeutung der sogenannten "Incel-Bewegung" darf hier nicht unterschlagen werden[6].

---

[1] Vgl. https://weisser-ring-stiftung.de/system/files/domains/weisser_ring_stiftung/downloads/praevalenzvonstalkingergebnisse2018.pdf

[2] Vgl. http://dip21.bundestag.de/dip21/btd/19/156/1915657.pdf

[3] Vgl. https://www.bmfsfj.de/bmfsfj/themen/gleichstellung/frauen-vor-gewalt-schuetzen/haeusliche-gewalt/haeusliche-gewalt-80642#:~:text=Demnach%20wurden%202019%20insgesamt%20141.792,Vors%C3%A4tzliche%2C%20einfache%20K%C3%B6rperverletzung%3A%2069.012%20F%C3%A4lle

[4] Vgl. https://hateaid.org/sexistische-digitale-gewalt/

[5] Vgl. https://www.sueddeutsche.de/politik/antifeminismus-rechtspopulismus-schutzbach-meinung-1.4798085?reduced=true

[6] Vgl. https://www.ndr.de/kultur/Incel-Subkultur-Frauen-nichts-anderes-als-Sexobjekte,incels104.html

Gewalt, auch digitale Gewalt gegen Frauen, darf kein “Frauenproblem” sein, sondern muss immer als ein gesamtgesellschaftliches Problem betrachtet werden, das es gesamtgesellschaftlich zu lösen gilt. Dabei gilt es außerdem anzuerkennen, dass die digitale und analoge Welt miteinander interagieren und nicht losgelöst voneinander betrachtet werden können. Digitale Gewalt hat Ursachen außerhalb der digitalen Sphäre und ebenso Auswirkungen außerhalb der digitalen Sphäre.

Während zurecht darüber diskutiert wird, ob und wenn ja, wie Social-Media-Plattformen ein sogenanntes “Deplatforming”[7] betreiben dürfen und welche regulatorischen Grundlagen es hierfür ggf. braucht, darf nicht unterschlagen werden, dass aufgrund mangelnder Rechtsdurchsetzung im digitalen Raum zahlreiche Frauen selbständig “Deplatforming” ihrer eigenen Person im Netz betreiben, da die Gewalterfahrungen bzw. analogen Gefahren für sie nicht mehr erträglich sind. Dass Frauen so aus dem öffentlichen Diskurs gedrängt werden, sollte uns als demokratische Gesellschaft mindestens genauso intensiv beschäftigen, wie das aktive “Deplatforming” durch Plattformen.

Handlungsfelder, die es beim Thema digitale Gewalt gegen Frauen und Mädchen zu berücksichtigen gilt, sind – nicht abschließend – aus vorrangig netzpolitischer Sicht, die Folgenden:

1. **Rechtsdurchsetzung im digitalen Raum / Fähigkeiten im Justizwesen und bei den Ermittlungsbehörden**

Generell muss bezüglicher der Bekämpfung von Straftaten im digitalen Raum sowohl das Justizwesen, als auch die Ermittlungsbehörden deutlich besser aufgerüstet und aus- bzw. fortgebildet werden. Dabei geht es aber explizit nicht um weitere Befugnisse. Die Modernisierung und damit auch die Digitalisierung der Justiz und der Polizei muss dringend stärker fokussiert werden und mit finanziellen Mitteln unterstützt werden. Dies ist nicht nur notwendig für eine zeitgemäße Ausstattung und damit Ermittlung (für jegliche Straftaten), sondern auch, um Verfahren beschleunigen zu können. Zeit ist oftmals ein kritischer Faktor in der Beweissicherung. Akten müssen sicher elektronisch geführt werden können und dürfen nicht auf Papier hin und her verschickt werden. Eine Modernisierung ist auch aus Sicherheitsaspekten für das Justizwesen selber von hoher Bedeutung (Stichwort: Hack des Kammergerichts in Berlin).

Es braucht zudem auf Cybercrime allgemein spezialisierte Beamtinnen und Beamte. Außerdem müssen in der Aus- und Weiterbildung im Justizwesen und in der Polizei Grundlagen dafür vermittelt werden, welche Arten von Cybercrime es gibt (diese müssen deutlich klarer definiert werden, s.o.). Wenn nicht bekannt ist, dass man Personen mittels Stalkerware verfolgen und ausspionieren kann, können Polizeibeamtinnen und -beamte Betroffene hierzu nicht befragen, bzw. die o.g. spezialisierten Beamtinnen und Beamten hinzuziehen. Außerdem muss damit ein Bewusstsein dafür geschaffen werden, dass Straftaten im digitalen Raum ernst genommen werden. Betroffenen darf nicht geraten werden, sich für ein paar Tage von den sozialen Medien

[7] Vgl. https://www.idz-jena.de/forschung/hate-not-found-das-deplatforming-der-extremen-rechten/

abzumelden, bzw. ihre Ahnung verfolgt zu werden, als übertrieben erachtet werden.

Zentralstellen und Spezialstaatsanwaltschaften wie das ZAC in NRW sind sehr zu begrüßen, insbesondere ihre Zusammenarbeit mit diversen Insitutionen. Allerdings gibt es auch hier einen Ressourcenmangel, u.a. an Personal. Außerdem dürfen zivilrechtliche Verfahren nicht zugunsten von anderen Verfahren, wie zum Beispiel der Bekämpfung organisierter Kriminalität an Priorität einbüßen, u.a. aufgrund von einem Ressourcenmangel. Um Fachpersonal anwerben zu können bzw. auch, um ein finanziell attraktiver Arbeitgeber zu sein, müssen die Tarife der Länder bzw. des Bundes für IT-Fachkräfte angepasst werden.

Die Erfassung von geschlechtsspezifischen Daten in der PKS ist zu begrüßen. Nur mit einer empirischen Datenbasis kann das Problem auch durch Präventionsarbeit besser bekämpft werden. Außerdem wird dringend empfohlen, die Erfassung von Cybercrimes[8] (z.B. die eingangs genannten) als solche differenziert zu erfassen, bzw. überhaupt als solche anzuerkennen.

Ganz generell braucht es im Justizwesen und in den Polizeibehörden ein besseres Verständnis davon, dass gerade Frauen im digitalen Raum koordiniert angegriffen werden und Frauenhass kein zu unterschätzendes Problem ist. Hier braucht es dringend eine Sensibilisierung, ebenso wie beim Thema Rassismus. Nicht-weiße Frauen, sowie jüdische oder muslimische Frauen (u.a.) dürfen keine Angst haben, bei der Polizei weitere Diskriminierungserfahrungen zu machen.

Strafanzeigen müssen einfach, online und anonymisiert gestellt werden können. In Zivilprozessen muss es für die Geschädigten möglich sein, das Verfahren auch ohne Nennung der privaten Anschrift zu betreiben, sondern derjenigen der beratenden Kanzlei oder NGO. Dies wird von Gerichten nach Angabe von Betroffenen nicht immer akzeptiert. Es ist aber von essentieller Bedeutung, da ansonsten der Täter über eine Akteneinsicht die Privatanschrift erfahren könnte.

2. Aufklärung / Bildung

Viele Menschen gehen noch immer unachtsam mit ihren persönlichen Daten, insbesondere Zugangsdaten für Online-Accounts um. Stalking kann auch passieren, weil Ex-Partner noch Zugang zu Accounts haben, durch die sie Informationen auf Aufenthaltsorte oder Gesprächsthemen etc. bekommen können. Dass Passwortwechsel nach einer Trennung sinnvoll sein können, ist ggf. noch zu unbekannt. Ebenso Wechsel von Passwörtern am Router bzw. Portalen für Smart-Home-Geräte, damit diese nicht missbraucht werden können (z.B. Anschalten von Lichtern oder Geräten)[9].

Bildungsmaßnahmen für Menschen jeden Alters, die sich im Rahmen einer Bundeszentrale für digitale Bildung u.a. mit den Themen Datenschutz und Cybersicherheit beschäftigen, wurden von mir bereits im Sommer 2019

[8] Vgl. http://dipbt.bundestag.de/dip21/btd/19/061/1906174.pdf
[9] Vgl. https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html

vorgeschlagen[10]. Dass die Staatsministerin für Digitalisierung eine solche Bundeszentrale realisieren möchte, ist daher sehr zu begrüßen und dient der allgemeinen Ermächtigung der Bürgerinnen und Bürger, um sich mündig in einer digitalen Welt zu bewegen.

3. Opferschutz

Die Maßnahmen aus dem Gesetzesvorschlag von Prof. Dr. Dirk Heckmann zum Thema Cybermobbing sind generell, aber auch insbesondere im Bereich des Opferschutzes sehr zu begrüßen[11]. Betroffene von digitaler Gewalt brauchen zudem deutlich mehr Anlaufstellen, an die sie sich wenden können. Finanzielle Hürden für zivilrechtliche Verfahren müssen abgebaut werden. Es darf keine Kostenfrage sein, ob sich Frauen gegen digitale Gewalt rechtlich wehren können oder nicht.

Institutionen, die sich um Frauen kümmern, die Opfer von Gewalt sind, sind generell unterfinanziert. Gerade für den Bereich digitale Gewalt und die Fortbildung der Mitarbeiterinnen und Mitarbeiter in den Beratungsstellen, um betroffenen Frauen eine erste Hilfe zu ermöglichen, braucht es dringend mehr finanzielle Unterstützung. Ebenso für präventive Aufklärungsarbeit.

4. Forschung

Auch, weil die Erfassung von o.g. Cybercrimes nicht erfolgt , ebenso wie die geschlechtsspezifische Erfassung in der PKS, fehlt es an Forschungsdaten. Forschung in diesem Bereich muss dringend gefördert werden und mit Institutionen, die bereits in diesem Bereich intensiv arbeiten und Erfahrung, sowie eigene Daten mitbringen, wie z.B. HateAid, zusammengearbeitet werden. Institutionen aus Deutschland dürfen sich nicht lediglich auf Erhebungen aus dem Ausland verlassen können müssen.

5. Gesetzgebung

Ein generelles Verbot von Stalkingsoftware ist abzulehnen, ebenso wie ein Verbot von Kamera- oder Audio-Funktionen in Haushaltsgeräten. Es kann Zwecke geben, in denen diese Technologie sinnvoll ist. Die Gesetzgebung in § 202b und § 202c StGB halte ich für ausreichend, um gegen Missbrauch vorzugehen. Eine Durchsetzung der security und privacy-by-design Ansätze ist hier deutlich sinnvoller.

Generell sollte die Bundesregierung davon absehen, Gesetze zu erlassen, die die IT-Sicherheit schwächen. So ist eine Ende-zu-Ende-Verschlüsselung essentiell. Vorhaben, sog. Backdoors für Ermittlungsbehörden vorzuschreiben, müssen unterlassen werden. Kriminelle können und werden diese ausnutzen, auch, aber nicht nur, um digitale Gewalt gegen Frauen und Mädchen auszuüben. Ein Recht auf Verschlüsselung ist daher notwendig.

---

[10] Vgl. https://www.freiheit.org/de/deutschland/mehr-digitale-bildung

[11] Vgl. https://www.arag.com/de/presse/pressemitteilungen/group/00448/

Ebenso dürfen Sicherheitslücken nicht offen gehalten werden, Hersteller von Smart-Home-Geräten müssen Sicherheitsupdates während der üblichen Nutzungsdauer zur Verfügung stellen und angeben, bis zu welchem Zeitpunkt sie sich verpflichten, Geräte mit Updates zu versorgen, damit diese sicher sind. Ein verpflichtender security-by-design Ansatz ist daher notwendig. Außerdem muss durch Produkthaftung und Schadensansprüche sichergestellt werden, dass Hersteller Anreize haben, Produkte sicher, d.h. ohne Sicherheitslücken und mit regelmäßigen Updates, auf den Markt zu bringen.

6. Medien / öffentlicher Diskurs

(Digitale) Gewalt gegen Frauen wird auch durch ein öffentliches Klima, das dies möglich macht ge- und befördert. So ist es nicht selten, dass Cybermobbing-Attacken insb. gegen Frauen von Medien befeuert werden. Hier bedarf es gesellschaftlich stärkere Verurteilungen und Kritik an solcher "Medienarbeit"[12].

Auch in Anbetracht der bevorstehenden Bundestagswahlen sollten Parteien intern darauf hinwirken, dass auch im Digitalen ein fairer Wahlkampf stattfindet und darauf aufmerksam machen bzw. dahingehend sensibilisieren, dass Frauen deutlich stärker und sexualisiert angegriffen werden. Weiblichen Parteimitgliedern muss jegliche Unterstützung bei Verfahren gegen Täterinnen und Tätern zukommen. Fehlverhalten – intern, als auch extern – muss deutlich adressiert und ggf. sanktioniert werden. Politische Akteure haben nicht nur im Wahlkampf Vorbildfunktion.

Über LOAD e.V.

LOAD e.V. - Verein für liberale Netzpolitik, ist ein unabhängiger Verein, der sich für den Erhalt eines freien Internets einsetzt und Bürgerinnen und Bürger dazu ermächtigt, ihre Grundrechte zu verwirklichen. LOAD e.V. möchte den gesellschaftlichen digitalen Wandel konstruktiv unterstützen. Der Verein finanziert sich ausschließlich durch die Mitgliedsbeiträge seiner Mitglieder. Der Verein wurde 2014 gegründet und hat seinen Sitz in Berlin.

[12] Vgl. https://www.ndr.de/fernsehen/sendungen/zapp/Kasia-Lenhardt-Gejagt-vom-Boulevard,zapp12884.html