Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
19(23)117

SVe Katja Grieger

Bundesverband Frauenberatungsstellen und Frauennotrufe | Frauen gegen Gewalt e.V.
Federal Association of Women's Counselling and Rape Crisis Centres (bff)

STELLUNGNAHME

Zum Fragenkatalog für die öffentliche Anhörung des Ausschusses Digitale Agenda

am 24. März 2021 zum Thema

a) Digitale Gewalt gegen Frauen und Mädchen (Selbstbefassung);
b) Antrag der Abgeordneten Anke Domscheit-Berg, Cornelia Möhring, Doris Achelwilm, weiterer Abgeordneter und der Fraktion DIE LINKE.: Digitale Gewalt gegen Frauen BT-Drucksache 19/25351

Berlin, 19.03.2021

Hintergrund

Im bff sind über 200 ambulante Fachberatungsstellen aus dem gesamten Bundesgebiet zusammengeschlossen. Diese unterstützen und beraten Frauen und Mädchen, die von sexualisierter, körperlicher, psychischer oder digitaler Gewalt betroffen und bedroht sind. Häufig handelt es sich um Gewalt im sozialen Nahraum, z.B. in (Ex)Partnerschaften. Die Erfahrung der Beratungsstellen zeigt, dass zunehmend eine Digitalisierung geschlechtsspezifischer Gewalt gegen Frauen zu beobachten ist. In vielen Fällen tritt eine Kombination aus analoger und digitaler Gewalt auf.

Der bff arbeitet mit seinem Projekt "Aktiv gegen digitale Gewalt" an der Sensibilisierung von Öffentlichkeit und relevanten Berufsgruppen, der (Weiter)Qualifizierung der Beratungsstellen und einem besseren Zugang zu Recht, Unterstützung und Informationen für Betroffene geschlechtsspezifischer digitaler Gewalt.

1. Was ist Digitale Gewalt gegen Frauen? Was ist digitale Gewalt gegen Mädchen?

Unter geschlechtsspezifischer digitaler Gewalt versteht der bff Gewalthandlungen, die sich technischer Hilfsmittel und digitaler Medien (Handy, Apps, Internetanwendungen, Mails etc.) bedienen sowie Gewalt, die im digitalen Raum, z.B. auf Online-Portalen oder sozialen Plattformen stattfindet. Wir gehen davon aus, dass digitale Gewalt nicht getrennt von „analoger Gewalt“ funktioniert, sondern meist eine Fortsetzung oder Ergänzung von Gewaltverhältnissen und -dynamiken darstellt. 7 von 10 Frauen, die digitale Gewalt erleben, sind auch von sexualisierter oder körperlicher Gewalt betroffen.

Der bff beobachtet seit mehreren Jahren die Zunahme von Fällen digitaler geschlechtsspezifischer Gewalt. Diese ist keine singuläre Gewaltform, vielmehr ist eine zunehmende Digitalisierung geschlechtsspezifischer Gewalt festzustellen. So berichten die Beratungsstellen im bff, dass vermehrt online Kommunikation, digitale Medien sowie technische Anwendungen und Software starken Einfluss auf (Ex)Partnerschaftsgewalt, sexualisierte Gewalt und Stalking haben. Dies kann beispielsweise bei Stalking oder dem Einsatz von Stalkerware in Trennungssituationen sowie in Form von bildbasierter sexualisierter Gewalt der Fall sein. Digitale geschlechtsspezifische Gewalt ist geprägt von schnelllebigen technologischen Entwicklungen und unterliegt denselben Dynamiken wie analoge Formen geschlechtsspezifischer Gewalt. Hierzu gehört, dass die Gewalt oft von (einst) vertrauten Personen aus dem direkten sozialen Umfeld ausgeht und den Betroffenen häufig eine Mitschuld (victim blaming) an der erlebten Gewalt zugeschrieben wird.

Die rechtlichen und technischen Hürden sind hoch und voraussetzungsvoll. So entsteht der Eindruck, dass Betroffenen in der Durchsetzung ihrer Rechte bei Polizei und Strafverfolgungsbehörden und/oder beim Melden von digitaler geschlechtsspezifischer Gewalt an Soziale Netzwerke, Seitenbetreiber*innen, Anbieter*innen von Online-Diensten (wie pornografischen Websites) sowie Software- und Produktentwickler*innen (wie Stalkerware, Dual-Use-Software oder Smarthomes) nicht ernst genommen werden.

2. Wie würden Sie den Begriff „Cybercrime“ definieren und würden Sie digitale Gewalt oder Teilbereiche der digitalen Gewalt dazu zählen?

Fast jede Form geschlechtsspezifischer Gewalt ist von den Auswirkungen der Digitalisierung betroffen; manche Formen der Gewalt sind nur durch Nutzung von IKT möglich. Für die zahlreichen Phänomene, die mit diesem Prozess einhergehen, wurde in den vergangenen Jahren der Oberbegriff »digitale Gewalt« geprägt.
Unter Cybercrime können zunächst grundsätzlich alle Straftaten verstanden werden, die unter Ausnutzung der Informations- und Kommunikationstechnik begangen werden. Der Begriff »Cybercrime« ist in Deutschland besonders stark durch den Straftatbestand des Computerbetrugs (§ 263a StGB) bzw. die Polizei und die Strafverfolgungsbehörden geprägt. Darunter fällt Internet-Kriminalität wie etwa: Datendiebstahl durch Hacken, Datendiebstahl mittels Social Engineering, Identitätsdiebstahl, Online-Betrug, Kreditkartenbetrug, Hack- und Virenangriffe auf Geräte mit und ohne IoT- Funktionen, Angriffe von Schadprogrammen auf Computer und Server mit Botnetzwerken sowie Installation von Schadsoftware (englisch malware).

Die Lageberichte zur IT-Sicherheit in Deutschland des Bundesamts für Sicherheit in der Informationstechnik bestätigen den Trend zur Kommerzialisierung und Professionalisierung der Internetkriminalität. Betroffene sind vor allem Behörden, Unternehmen, Banken und auch Privatanwender*innen (vgl. BSI 2019: 7ff.).

Die geschlechtsspezifische digitale Gewalt, mit der die Fachberatungsstellen des bff konfrontiert sind, wird von den Strafverfolgungsbehörden in der Regel nicht als Cybercrime betrachtet und dementsprechend nicht in den dafür vorgesehenen Abteilungen behandelt.

3. Was ist über das Ausmaß, die Täter und die Betroffenen von digitaler Gewalt bekannt?

Die Datenlage in Deutschland zum Thema (geschlechtsspezifische) digitale Gewalt ist spärlich. Aus vereinzelten Studien zu einzelnen Unterformen digitaler Gewalt oder aus dem Ausland können jedoch einige Erkenntnisse gezogen werden.

So hat eine Erhebung aus den USA beispielsweise ergeben, dass 90% aller Betroffenen von bildbasierter Gewalt Frauen sind.
Für die FRA wurde 2014 bei einer Studie über Gewalt gegen Frauen „Cyberstalking“ und „Belästigung im Internet“ abgefragt. In dieser Studie bestätigt die besondere Vulnerabilität bei jungen Frauen zwischen 18 und 29 Jahren. Die Gefahr, von digitaler Gewalt betroffen zu sein, ist für junge Frauen im Alter zwischen 18 und 29 Jahren zweimal so hoch, wie für Frauen im Alter zwischen 40 und 49 Jahren und mehr als dreimal so hoch wie für Frauen im Alter zwischen 50 und 59 Jahren (vgl. FRA 2014: 32).

Mädchen und besonders junge Frauen erleben aufgrund ihres Geschlechts digitale Gewalt, mit der zusätzlichen Erfahrung von Mehrfachdiskrimierung, erleben sie häufiger verstärkte digitaler Gewalt.

Die Umfrage des Welt-Mädchenberichts 2020 „Free to be online? Erfahrungen von Mädchen und jungen Frauen mit digitaler Gewalt“ ergab, dass 58 % der Befragten angaben, dass sie bereits digitale Gewalt auf Social-Media-Plattformen erfahren

haben. Die meisten Mädchen und jungen Frauen erleben erstmals digitale Gewalt zwischen 14 und 16 Jahren.

Eine eigene Erhebung des bff unter seinen Mitgliedorganisationen von 2017 legt nahe, dass digitale Gewalt an bestehende Gewaltdynamiken anschließt und somit ein ähnliches Bild von Tätern und Opfern zu erwarten ist, wie bei anderen Formen von geschlechtsspezifische Gewalt.

Andere betroffenen Gruppen von digitaler Gewalt sind trans, nonbinary und queere Personen und auch Menschen, die Mehrfachdiskriminierung erfahren wie beispielsweise Frauen mit Rassismuserfahrungen oder trans Personen mit Behinderungen (vgl. Amnesty International 2017).

4. Welche Formen digitaler Gewalt gegen Frauen gibt es, welche sind (vergleichsweise) neu, welche nehmen zu und was zeichnet die unterschiedlichen Erscheinungsformen aus?

Seit Jahren lässt sich ein Anstieg geschlechtsspezifischer digitaler Gewalt in den verschiedensten Formen erkennen: Stalking und die Anwendung von Spionage-Software, heimliches Filmen und sogenannte Deepfakes, wo Bilder der Betroffenen auf pornografische Inhalte gefaked werden. Außerdem das Kontrollieren von Cloud-Diensten, Hacking oder auch Identitätsdiebstahl. Internationale Studien weisen darauf hin, dass sich digitale Gewalt aktuell vor allem in Richtung bildbasierte Gewalt entwickelt: Noch unter Einverständnis aufgenommene Bilder werden ohne Zustimmung ins Internet gestellt oder auch zur Nötigung benutzt. Auch heimliches Filmen und Bildmanipulationen nehmen zu. Der bff unterscheidet derzeit zwischen einer Vielzahl an Formen digitaler Gewalt und unterschiedlichen konkreten Methoden und Strategien der Gewaltausübung.

Durch die Geschwindigkeit der Technikentwicklung ist es wahrscheinlich, dass sich bestehende Gewaltformen verändern und weitere Gewaltformen in der Zukunft auftreten werden. Für einen niedrigschwelligen Überblick siehe auch bff: Aktiv gegen digitale Gewalt: https://www.aktiv-gegen-digitale-gewalt.de/de/

Hate Speech ist Gewalt im öffentlichen digitalen Raum. Vor allem qualitative Aspekte kennzeichnen geschlechtsspezifische Hate Speech. Frauen, aber auch nicht-binäre / trans Personen sind häufiger Ziel sexualisierter Formen von Hate Speech wie beispielsweise Vergewaltigungsandrohungen oder sexualisierten Demütigungen. Bei geschlechtsspezifischem Hate Speech geht es in der Regel darum, die Betroffenen zum Schweigen zu bringen, sie einzuschüchtern und sie bzw. ihre öffentlichen digitalen Äußerungen zu diffamieren.

Cyberharassement ist als Sammelbegriff zu verstehen für unterschiedliche Formen der Belästigung, Beleidung, Bedrohung und Diffamierung im Netz. Die geschlechtsspezifische Komponente äußert sich dabei vor allem durch den oft sexualisierten, sexistischen, misogynen Charakter der Äußerungen. Die Methoden umfassen u.a. das Streuen von Gerüchten und Falschinformationen über Betroffene, das Kopieren von Profilen, Rufschädigungen, das Versenden von Direktnachrichten mit Beleidigungen und Drohungen gegen die Betroffene oder eine Person die ihr nahesteht, unfreiwilliges Zusenden pornografischer Inhalte, das Schalten von Anzeigen im Namen der Betroffenen z.B. auf Datingplattformen mit

sexualisierten Aufrufen zur Kontaktaufnahme oder Slut-Shaming, d.h. das Diffamieren wegen tatsächlicher oder vermeintlicher Abweichung von der sexuellen Norm. Auch durch tatsächliche Profile auf Dating-Plattformen werden Frauen zum Ziel von Cyberharassment und gegebenenfalls erleben sie auch analoge sexualisierte Gewalt, wenn es zu einem Treffen kommt.

Cyberstalking bezeichnet das Nachstellen mit digitalen Mitteln, d.h. das beharrliche, andauernde und hartnäckige Verhalten, das mittels Informations- und Kommunikationstechnologie ausgeübt wird, um eine Person zu belästigen, ihr zu schaden, sie zu verfolgen und zu terrorisieren. Die Täter sind den Betroffenen häufig bekannt. I.d.R. wird Cyberstalking von (Ex-)Partnern ausgeübt oder von Personen (i.d.R. Männer), deren Beziehungswunsch nicht erwidert wird. Für Cyberstalking verwenden Täter teils Daten aus dem öffentlichen digitalen Raum (d.h. öffentliche Social Media-Profile). Diese Möglichkeit steht auch unbekannten Tätern offen. Ebenfalls gibt es Fälle, bei denen der Täter sich Zugang zu Accounts der Betroffenen verschafft (z.B. mit durch Erpressung erlangten Passwörtern). Im Fall von Cyberstalking durch (Ex-)Partner werden auch zunächst freiwillig geteilte digitale Infrastrukturen, wie ein gemeinsames Bankkonto, eine gemeinsame E-Mail-Adresse, etc. verwendet. Im Kontext von (Ex-)Beziehungen wird oft Software zur Nachstellung verwendet, die in diesem Kontext als **Dual-Use-Software** bezeichnet wird. Damit ist Software gemeint, die vordergründig anderen Zwecken dient, wie der Überwachung des Standorts eines Kindes oder der vordergründig auf einen anderen Zweck gerichteten Übermittlung von Standortdaten z.B. bei Heimweg-Apps, Dating-Apps, Fitness-Tracking-Software. Es gibt jedoch auch **dedizierte Stalkerware**, die vermarktet wird mit dem erkennbaren Zweck, die Partnerin zu überwachen. Cyberstalking kann das Abfangen folgender Daten beinhalten. Die Liste ist notwendigerweise unvollständig:

- Der Standort des Geräts (i.d.R. Smartphone, ggf. auch andere vernetzte Gegenstände wie Auto, Fitness-Tracker, ...)
- Verbindungsdaten, d.h. wer wann die Betroffene kontaktiert hat
- Mitlesen von E-Mails und anderen Nachrichten durch Kontrolle über E-Mail- und Social Media-Accounts
- Den Browserverlauf: Welche Websites aufgerufen wurden
- Daten aus dem sog. "Smart Home"
- Screenshots
- Fotos mithilfe der Kameras an Smartphone oder Laptop
- Tonmitschnitte
- Nachrichten, auch aus vielen verschlüsselten Messengern

Identitätsdiebstahl kann je nach Kontext als alleinstehende Form digitaler Gewalt betrachtet werden, hat jedoch große Schnittmengen mit Cyberstalking und Doxxing. Unter Identitätsdiebstahl wird v.a. verstanden, dass z.B. im Namen der Betroffenen Waren bestellt werden, Notrufe getätigt werden, die zu Polizeieinsätzen führen und vergleichbares.

Doxing (auch: Doxxing) ist das Sammeln und Verbreiten von privaten Informationen über die betroffene Person. In Chaträumen, Massen-E-Mails, auf Social Media-Portalen, Blogs und Homepages kann der Täter persönliche (Kontakt-)Daten der Betroffenen an andere Internetnutzer*innen weitergeben. Hierfür werden z.B.

Newsletterabos oder Eintragungen in Plattformen wie z.B. Kleinanzeigen- oder Dating-Portalen vorgenommen. Zudem können intime Details verbreitet werden, beispielsweise über die (vermeintliche) Sexualität, den gesundheitlichen oder finanziellen Status der betroffenen Person. Hierbei werden intime und/oder manipulierte Bilder/Videos an alle Kontakte verschickt, in den meisten Fällen in Verbindung mit diffamierenden Lügen und Gerüchten. Durch die Veröffentlichung solcher Informationen im Netz wird die Betroffene u.a. in die Gefahr gebracht, dass Dritte ihr nachstellen und auflauern. Darüber hinaus sind Folgen von Doxing die Verletzung ihres Rufes und soziale Isolation. Die Konsequenzen können auch unmittelbare negative Folgen für den finanziellen und sozialen Status sein, wenn beispielsweise Betroffene aufgrund der veröffentlichten (Falsch-)Informationen keine Wohnung oder keine Arbeitsstelle bekommen.

Bildbasierte Gewalt ist ein Problem seit es Handys mit Kamera und Schnittstelle zur Datenübertragung gibt. Begriffe wie revenge porn oder non-consensual Porn sind insofern problematisch, da sie die Gewaltdynamiken verschleiern. Daher verwendet der bff den Begriff "bildbasierte sexualisierte Gewalt", in Anlehnung an die englische Terminologie "image-based sexual abuse" nach Clare McGlynn and Erika Rackley (vgl. McGlynn/Rackley 2017) und fasst darunter unterschiedliche Gewalthandlungen zusammen. Die folgende Aufzählung von Formen bildbasierter Gewalt ist keinesfalls vollständig, gibt jedoch nach Einschätzung des bff einen Überblick, der geeignet ist, Verständnis für die Diversität der Problematik zu schaffen.

Die Veröffentlichung zunächst einvernehmlich erstellter Fotos und Videos, z.B. um die Ex-Partnerin nach der Trennung zu beschämen und zu "bestrafen". Unbefugte Aneignung von Bildmaterial, z.B. in einer schlecht gesicherten Cloud oder zuvor gemeinsam genutzten oder durch die Nutzung ungesicherter Passwörter bzw. der Manipulation zur Herausgabe von Passwörtern, durch Personen die der Betroffenen bekannt oder fremd sein können.
Die Verwendung und Veröffentlichung heimlich erstellter Aufnahmen, in der Wohnung bei Partnerschaftsgewalt, ebenso wie durch Fremde in öffentlich zugänglichen Räumen (Festival-Toiletten, Saunen, Umkleidekabinen, aber auch sogenanntes Upskirting, d.h. Fotografieren unter den Rock, im ÖPNV). Filmen von (sexualisierter) Gewalt mit anschließender Veröffentlichung.

Es gibt Fälle in denen Bildmaterial direkt und ohne Kenntnis der Betroffenen veröffentlicht wird. Teils wird auch nicht-sexuelles Bildmaterial sich angeeignet, das z.B. auf Social Media öffenlich oder für einen größeren Personenkreis einsehbar ist, und in bestimmten Foren / Imageboards bzw. auf bestimmten Websites veröffentlich mit Slut-Shaming-Aufrufen. Dies geschieht auch in Verbindung mit Doxing.

Insbesondere bei bildbasierter Gewalt durch (Ex)-Partner kommt es vor, dass Personen mit Bildmaterial zunächst genötigt werden, z.B. wenn ein Partner damit droht, zunächst einvernehmlich erstellte Bilder zu veröffentlichen, wenn die Partnerin die Beziehung beendet.

Eine Studie von Powell et al. 2019, mit Datenerhebung in Australien, Neuseeland und Großbritannien, stellt fest, dass 90 % der Betroffenen den Täter kannten, 60,9 % der Täter waren Ex-Partner*innen.

Zunehmend relevant wird die Erstellung von Bildmanipulationen, bei denen Laien kaum erkennen können, dass es sich um Montagen handelt: sogenannte Deep Fakes. Diese werden vornehmlich verwendet, um die Gesichter von Personen in pornografisches Material zu implementieren.

5. Sind Mädchen bzw. Frauen besonders von digitaler Gewalt betroffen und wenn ja, inwiefern und warum?

Digitale Gewalt wird grundsätzlich gegen viele unterschiedliche Betroffenengruppen angewendet, beispielsweise rassistische digitale Gewalt gegen von Rassismus betroffene Personen, antisemitische digitale Gewalt gegen Jüd*innen, transfeindliche digitale Gewalt gegen trans Personen, rechtsextremistische digitale Gewalt gegen Personen, die sich für eine offene Gesellschaft engagieren, usw.. Häufig kommen auch Mehrfachdiskriminierungen vor.

Wie bereits erwähnt machen die im bff organisierten Beratungsstellen seit vielen Jahren die Erfahrung, dass sich die bereits bekannte geschlechtsbezogene Gewalt, die sie seit ihrer Gründung bearbeiten, digitalisiert. Diese Gewalt basiert auf dem tradierten Machtverhältnis zwischen den Geschlechtern (s.u., Frage 9), ihre zunehmend digitale Anwendung bringt jedoch stetig neue Formen hervor. Frauen (und Mädchen) sind von dieser Gewalt deshalb besonders betroffen, weil der Kern dieser Gewalt sich auf ihr Geschlecht bezieht.

In der Altersgruppe der 12- bis 19-Jährigen geben 37 % an, dass in ihrem Bekanntenkreis schon einmal jemand im Internet fertig gemacht oder belästigt worden ist. Mädchen haben dies mit 42 Prozent schon häufiger mitbekommen als Jungen (31 %). Je älter die Jugendlichen sind, desto höher ist der Anteil derer, die schon von so einem Fall erfahren haben (vgl. JIM-Studie 2017).

Die Spezifik von digitaler Gewalt, die Frauen erleben, liegt darin, dass sie anders als bei vielen anderen Formen digitaler Gewalt oft von Personen aus dem sozialen Nahraum begangen wird und / oder dass sie sexualisiert ist. Hatespeech gegen Frauen findet im digitalen öffentlichen Raum statt (s.o.), ist aber häufig ebenfalls sexualisiert und offenbart ein großes Ausmaß an Misogynie, zielt also ebenfalls auf das Geschlecht und darauf, speziell Frauen zum Schweigen zu bringen.

6. Welche wissenschaftlichen Analysen zu welchen Fragestellungen sind notwendig, um die Herausforderungen von digitaler Gewalt genauer zu verstehen und konsistent zu untersuchen?

Siehe Frage 8

7. Welche weiteren Gewaltformen gehen ggf. damit einher? Was bedeutet das Erleben von digitaler Gewalt für die Betroffenen?

Das Erleben digitaler Gewalt ist für Betroffene oft mit dem Gefühl großer Ohnmacht verbunden. Sie sehen sich nicht "nur" dem oder den jeweiligen Täter*innen ausgeliefert, sondern zusätzlich noch schwer nachvollziehbaren Technologien und/oder Akteuren wie Plattformen und Internetdiensten. Die zeitliche und räumliche Entgrenzung digitaler Räume führt auch dazu, dass Gewalterlebnisse sich

entgrenzen. Das Erleben digitaler Gewalt bewirkt, dass Betroffene im Umgang mit digitalen Geräten und Technologien verunsichert werden, oft auch noch lange Zeit nach den Angriffen. Dies wiederum kann die (digitale) gesellschaftliche Teilhabe der Betroffenen nachhaltig einschränken. So gelangt der Welt-Mädchenbericht von plan International zu dem Ergebnis, dass 38% der Betroffenen digitaler Übergriffe aufgrund von Online-Belästigungen ihr Verhalten auf Social Media änderten, z.B. Plattformen seltener nutzten, seltener ihre Meinung sagten oder das jeweilige Netzwerk komplett verließen (plan International, #FreeToBeOnline).

Im Falle von digitalem Stalking, beispielsweise in einer Trennungsphase oder nach einer Trennung, befinden sich Betroffene oft in einem Empfinden kontinuierlicher Bedrohung, Überwachung und Unsicherheit. Sie wissen meist zunächst nicht, welche Geräte und Techniken benutzt werden, ob auch Kameras installiert wurden und können kaum Momente oder Orte finden, an denen sie sich sicher fühlen und zu Kräften kommen können.

Im Falle von bildbasierter sexualisierter Gewalt, beispielsweise dem Veröffentlichen von intimen Aufnahmen, haben die Betroffenen mit Gefühlen extremer Scham zu kämpfen, die zu sozialer Isolierung führen können. Die Betroffenen erfüllen häufig die Forderungen der Täter (Zurücknahme der Trennung, Nichtanzeige von sexualisierter Gewalt, Geldleistungen) in der Hoffnung, diese würden aufhören oder ihre Drohung nicht wahr machen.

Einer Studie von Amnesty International zufolge leiden 60% der Frauen, die digitale Gewalt erlebt haben, an Schlafproblemen, Konzentrationsschwierigkeiten, Panikattacken und Angstzuständen (vgl. Amnesty International 2017). Auch die Beratungspraxis zeigt, dass digitale Gewalt schwere Folgen für viele Betroffene haben kann. Besonders fatal ist der häufige und verständliche Impuls des sozialen Rückzugs von Betroffenen.

Digitale Gewalt kann auch tödlich enden. Quantitative Forschung ist dem bff nicht bekannt, jedoch gibt es gut dokumentierte Fälle, in denen Betroffene von Belästigung, bildbasierter Gewalt, Doxxing und anderen Formen digitaler Gewalt, versucht haben sich zu suizidieren (vgl. UN-Special Rapporteur on Violence Against Women 2018: Abs. 78).

Oft gehen den Tötungen von Frauen häusliche Gewalt oder Stalking und eine Beziehung voraus, die geprägt ist von Kontrolle, starker Eifersucht, psychischer Gewalt oder einer starken Isolierung. Eine aktuelle Studie der Kriminologin Monckton-Smith aus Großbritannien, in der über 300 Tötungen von Frauen untersucht wurden, bestätigt das. Immer häufiger sind digitales Stalking oder digitale Überwachung Bestandteile solcher Partnerschaften. Eine australische Studie dokumentiert, dass 17 Prozent der Betroffenen von häuslicher Gewalt von ihrem Partner oder Ex-Partner permanent durch Apps wie „Find My Friends“ getrackt worden sind.

Der bff gibt deshalb zu bedenken, dass Fälle von digitaler Gewalt auch zu Femiziden führen können und deshalb äußerst erst genommen werden müssen, wenn Betroffene um Unterstützung suchen.

8. Ist das Ausmaß von digitaler Gewalt durch die bestehenden

Erfassungsmöglichkeiten erkennbar? Wenn nicht, wo bestehen Defizite und was muss sich ändern? Denken Sie, dass die PKS zu erweitern und ein jährliches Lagebild zu Gewalt an Frauen inkl. digitaler Gewalt zu erstellen, die Statistiken der Justiz zu erweitern und eine wissenschaftliche Studie zu Gewalt an Frauen zu erstellen, zielführend und ausreichend sind? Gibt es darüber hinaus noch Handlungsbedarfe?

Über das Ausmaß von geschlechtsspezifischer digitaler Gewalt ist in Deutschland bisher nur wenig bekannt. Eine Erfassung in der PKS findet bislang bei einzelnen Delikten über das Kriterium "Tatmittel Internet" statt, wobei dieses nur angegeben wird, wenn das Internet das hauptsächliche Tatmittel ist. Eine kombinierte Tabelle, die für einzelne Straftatbestände sowohl Informationen zum "Tatmittel Internet" als auch zu Geschlecht von Opfer und Täter enthält, gibt es nicht.

Zu berücksichtigen ist, dass die Erfassung polizeilicher Meldungen immer nur das polizeiliche Hellfeld abbildet. Sie ermöglicht also nur Aussagen über das Anzeigeverhalten, nicht über das tatsächliche Vorkommen der Tatbestände. Sowohl bei geschlechtsspezifischer Gewalt generell als auch bei ihrer digitalen Komponente wählen Betroffene häufig nicht den Weg, sich an die Polizei zu wenden[1]. Insofern würde eine bessere Erfassung geschlechtsspezifischer digitaler Gewalt in der PKS nur einen begrenzten Beitrag zur Aufhellung des Phänomens digitale Gewalt leisten, der angesichts der schlechten Forschungslage in Deutschland aber keinesfalls zu vernachlässigen wäre. Ein jährliches Lagebild zum Thema Gewalt an Frauen kann hilfreich sein, um für die Geschlechterdimension dieser Gewalt zu sensibilisieren, die aus der bisher existierenden jährlichen Auswertung zu Partnerschaftsgewalt kaum hervorgeht.

Mangels einer Verlaufsstatistik der Strafverfolgung in Deutschland sind ganz allgemein keine Aussagen zum Ausgang von Strafverfahren (z.B. Verurteilungsquoten) bezogen auf einzelne Delikte möglich. Insofern sind auch keine Daten vorhanden, die eine Aussage erlauben, ob digitale Straftaten in der Regel zu unterschiedlichen Verfahrensausgängen führen als analoge Straftaten.

Ganz grundsätzlich besteht ein hoher Bedarf, die Forschungslage in Deutschland zum Thema (geschlechtsspezifische) digitale Gewalt zu verbessern. So müssen z.B. Prävalenzstudien durchgeführt werden, die auf das Dunkelfeld abzielen. Die letzte repräsentative Studie in Deutschland zum Thema Gewalt gegen Frauen wurde im Jahr 2004 veröffentlicht, das Thema digitale Gewalt kommt dementsprechend dort (bis auf Stalking per E-Mail) nicht vor. In künftigen Studien zu geschlechtsspezifischer Gewalt sollte unbedingt auch die digitale Komponente differenziert miterfasst werden, aber auch die in der Praxis häufig beobachtete Kombination aus analogen und digitalen Gewalthandlungen und Übergriffen. Auch gibt es bislang keine tiefergehenden Forschungserkenntnisse über Täter geschlechtsspezifischer digitaler Gewalt und die Frage, inwieweit und unter welchen Bedingungen diese auch analoge Gewalttaten begehen, was aber in der Praxis häufig beobachtet wird.

[1] Die Gründe dafür sind vielfältig: eine polizeiliche Anzeige ist mit der Offenlegung intimer und schambesetzter Inhalte verbunden; Betroffene erhoffen sich keinen Nutzen von einem Strafverfahren und haben Sorge, dass ihnen nicht geglaubt wird; Betroffene haben Angst, dass eine Anzeige zu Racheakten des Täters führen kann oder er hat dies explizit angedroht; Betroffene fürchten die lange Dauer und die Belastungen eines Strafverfahrens, usw..

9. Inwieweit ist es sinnvoll, bei der Erfassung digitaler Gewalt und bei Maßnahmen gegen sie zwischen den Geschlechtern zu unterscheiden?

Es ist grundsätzlich bei der Erfassung von Gewaltphänomenen und dem Ergreifen von Gegenmaßnahmen sinnvoll, zwischen den Geschlechtern zu unterscheiden. Andernfalls ist es unmöglich, eine spezifische Betroffenheit, aber auch spezifische Gewaltdynamiken zu bearbeiten. Gemäß der von Deutschland ratifizierten Istanbul-Konvention ist geschlechtsspezifische Gewalt gegen Frauen sowohl als Auswirkung als auch als Ursache von ungleichen Machtverhältnissen zwischen den Geschlechtern zu betrachten. Es geht also bei Gewalt gegen Frauen häufig darum, Macht über Frauen zu demonstrieren, Frauen auf ihren vermeintlichen Platz zu verweisen, Kontrolle über Frauen zu gewinnen oder behalten oder Frauen davon abzuhalten, ein selbstbestimmtes Leben zu führen und aus ihrer vorgesehenen Rolle auszubrechen. Die gesellschaftliche Bedeutung dieser Gewalt ist nicht verstehbar ohne den Hintergrund der bestehenden Geschlechterverhältnisse. Die Erfassung der Kategorie Geschlecht sowie eine Bearbeitung von geschlechtlichen Rollenzuweisungen sind somit wichtige Bestandteile im Umgang mit geschlechtsspezifischer (digitaler) Gewalt.

Bisher leider völlig unerfasst ist die geschlechtsspezifische (digitale) Gewalt gegen nicht-binäre und trans Personen. Obwohl es mittlerweile zumindest die Option eines dritten Geschlechtseintrages gibt, erfassen sämtliche Statistiken bislang diese Personen nicht. Aber auch als Frauen erfasste trans Frauen erleben häufig sowohl Übergriffe aufgrund ihres Frauseins als auch aufgrund ihrer trans Identität (Mehrfachdiskriminierung), die bislang als solche nicht dokumentiert und damit bearbeitbar sind.

10. Was ist zur Struktur der Täter*innen bekannt, und inwieweit kann bzw. sollte man Programme gegen digitale Gewalt darauf abstimmen?

Geschlechtsspezifische digitale Gewalt ist häufig eine Fortsetzung analoger Gewalt. Das gilt insbesondere, wenn Täter und Betroffene miteinander bekannt sind und vor allem im Kontext von Gewalt durch den (Ex-)Partner. Die Täter sind in den überwiegenden Fällen Männer. Dahinter stehen gesellschaftliche Machtstrukturen und problematische Rollenbilder, die Kontrolle und Gewalt durch Männer legitimieren. Die Dynamiken digitaler geschlechtsspezifischer Gewalt sind somit oft die gleichen wie in den dahinterstehenden analog stattfindenden Prozessen.

Da die Gewaltdynamiken weitgehend identisch sind, sind Frauenberatungsstellen und Frauennotrufe für Frauen und Mädchen gute Anlaufstellen mit kompetenten Ansprechparterinnen. Um den zusätzlichen Anforderungen bei Fällen digitalisierter Gewalt gerecht zu werden, müssen den Beratungsstellen zeitliche und finanzielle Ressourcen bereitgestellt werden, um z.B. Fortbildungen in IT-Kompetenz und anderen relevanten Aspekten zu ermöglichen.

Inwiefern sich Täternstrategien jedoch bei digitalisierten Aspekten geschlechtsspezifischer Gewalt unterscheiden, ist noch nicht hinreichend wissenschaftlich erforscht.

11.Was sind die (größten) Probleme bei der Bekämpfung Digitaler Gewalt?

Das größte Problem ist die fehlende Anerkennung der digitalen geschlechts-bezogenen Gewalterfahrungen in ihrer gesellschaftlichen und politischen Bedeutung durch Politik, Justiz, Polizei, Plattformanbieter*innen sowie Entwickler*innen und Produzent*innen im Technologiebereich.

Langfristig erfordert ein effektives Vorgehen gegen digitale Gewalt Expertise und Zusammenwirken diverser staatlicher und nichtstaatlicher Akteur*innen mit dem Ziel, Prävention und Intervention zu verwirklichen. Solch ein effektiveres und verstärktes Vorgehen gegen digitale Gewalt darf jedoch nicht zu Lasten von Privatsphäre der Betroffenen gehen, denn der Online-Raum ist wichtig für gesellschaftliche Teilhabe und Austausch von insbesondere vulnerablen Gruppen, wie Frauen mit unterschiedlichen Diskriminierungserfahrungen und Personen anderer marginalisierter Geschlechter.

12.Welche Probleme sehen Sie im Bereich von Polizei und Justiz? Sind Sie der Meinung, dass eine Fortbildungspflicht für Richter*innen und Staatsanwält*innen zu digitaler und geschlechtsspezifischer Gewalt sowie die Verankerung dieser Themen in die Ausbildung der Polizei notwendig und ausreichend sind? Wie könnte eine vertrauliche Spurensicherung (auch bei Beratungsstellen) beim Verdacht von problematischen Inhalten auf Smartphones verbessert werden?

Die Strafverfolgung digitaler Gewalt steckt noch in den Kinderschuhen, was auch damit zu tun hat, dass die allermeisten Gesetze in einer Zeit formuliert wurden, in der es noch kein Internet gab. Der Prozess, die unterschiedlichen Formen digitaler Angriffe rechtlich einzuordnen, ist in Deutschland noch nicht abgeschlossen. Viele Betroffene, aber auch Täter*innen, haben das Gefühl, dass das Internet ein rechtsfreier Raum ist. Ein weiterer Grund für mangelnde Strafverfolgung sind fehlende spezifische Kenntnisse zu digitalen Phänomenen sowie mangelnde Kapazitäten bei den Strafverfolgungsbehörden. Immer wieder berichten uns Betroffene digitaler Gewalt, dass sie bei der Polizei auf eine große Ratlosigkeit im Umgang mit digitaler Technik getroffen sind, z.B. bei Fragen der Sicherung von Beweisen, die sich auf Smartphones befinden.

Seit vielen Jahren gibt es in Deutschland bei Polizei und teils auch Justiz Einheiten, die auf häusliche Gewalt oder Sexualstraftaten spezialisiert sind. Diese sind bestenfalls sensibilisiert im Umgang mit Betroffenen geschlechtsspezifischer Gewalt, kennen sich aber viel zu wenig mit der neu hinzugekommenen digitalen Komponente dieser Gewalt aus. Daneben gibt es Einheiten, die in den letzten Jahren speziell zur Bekämpfung von Cyberkriminalität eingerichtet wurden. In diesen Einheiten befindet sich das wichtige Wissen über IT-Anwendungen und die Möglichkeiten der digitalen Technik, dort werden aber keine Fälle geschlechtsspezifischer digitaler Gewalt bearbeitet, sondern beispielsweise digitale Angriffe auf Wirtschaftsunternehmen. Wir empfehlen dringend, dass diejenigen Personen bei Polizei und Justiz, die mit Fällen geschlechtsspezifischer Gewalt befasst sind, zur digitalen Komponente dieser Gewalt fortgebildet werden müssen und bei Bedarf das Wissen der Kolleg*innen aus den Abteilungen Cybercrime hinzuziehen können.
Auch müssen die Ermittlungs- und Strafverfolgungsbehörden mehr forensische

Kapazitäten aufbauen und ihre technische Ausstattung verbessert werden, damit die digitale Beweissicherung verbessert wird.

In der Praxis kommt es immer wieder vor, dass Betroffene, die sich an die Polizei wenden, die Erfahrung machen, dass die Übergriffe aufgrund ihrer digitalen Begehungsweise als "nicht so schlimm" bewertet werden oder ihnen z.B. geraten wird, die betreffende App "einfach zu löschen und dann ist es vorbei". Das Bewusstsein für die möglichen gravierenden Auswirkungen auch von rein digital begangener Gewalt sollte ganz unbedingt durch Fortbildungen gestärkt werden.

Artikel 49 der Istanbul-Konvention verlangt eine effektive Strafverfolgung geschlechtsspezifischer Gewalt und die Durchführung der Verfahren mit einem "geschlechtsbewussten Verständnis von Gewalt". Dies ist in Deutschland generell in vielen Verfahren geschlechtsspezifischer Gewalt nicht gegeben, sodass der bff seit langer Zeit die Intensivierung der Fortbildung der Polizei sowie die Einführung einer Fortbildungsverpflichtung für die mit derartigen Verfahren befasste Justiz fordert. Bei diesen Fortbildungen sollte selbstverständlich und verstärkt auf die digitalen Aspekte dieser Gewalt eingegangen werden.

Eine vertrauliche Spurensicherung beim Verdacht von problematischen Inhalten auf Smartshones existiert bislang in Deutschland nicht. Sie würde aber dem Bedürfnis vieler Betroffener Rechnung tragen, schnell und unbürokratisch ihre digitalen Endgeräte überprüfen zu lassen, wenn sie einen Verdacht z.B. auf Spionagesoftware haben. Viele Betroffene gehen davon aus, dass die Polizei im Rahmen eines Ermittlungsverfahrens eine solche Überprüfung und ggf. auch Bereinigung übernehmen würde und wenden sich deshalb an die Polizei. In seltenen Fällen führt dies zu einer Überprüfung der Geräte im Ermittlungsverfahren, was aber bedeutet, dass Betroffene z.B. ihr Handy für längere Zeit abgeben müssen. In vielen Fällen findet aber gar keine Überprüfung statt. Mangels anderer Überprüfungs-möglichkeiten versuchen mittlerweile einige wenige Beratungsstellen, z.B. durch das Hinzuziehen von externer IT-Kompetenz, solche Überprüfungen vorzunehmen. In den allermeisten Beratungsstellen ist dies aber bislang nicht möglich, weil dafür schlicht die finanziellen Ressourcen fehlen. Wenn Angebote vertraulicher Beweissicherung sowie dem zusätzlichen Angebot der Bereinigung der Endgeräte nach der Sicherung flächendeckend vorhanden wären, könnte in vielen Fällen Cyberstalking schneller beendet und danach auch effektiver strafverfolgt werden.

13. Halten Sie die Schaffung von Spezialdezernaten und -Staatsanwaltschaften für sinnvoll und wenn ja, warum?

Der bff hält es für unbedingt geboten, dass diejenigen, die mit der Strafverfolgung geschlechtsspezifischer digitaler Gewalt befasst sind, sowohl Kenntnisse und Kompetenzen zu geschlechtsspezifischer Gewalt als auch im Umgang mit digitaler Technik haben.

Seit langer Zeit gibt es vielerorts Spezialdezernate beispielsweise für Sexualdelikte oder für häusliche Gewalt. Dort sind Kenntnisse über die spezifische Situation von Betroffenen dieser Gewalt, zu möglichen Gefährdungspotenzialen oder Täterstrategien bestenfalls vorhanden, die für die Strafverfolgung dieser Fälle wichtig sind. Die Einrichtung von Spezialdezernaten für digitale Gewalt würde ggf.

neue Zuständigkeitsfragen aufwerfen, eine Abgrenzung zu den bereits vorhandenen o.g. Dezernaten müsste sinnhaft hergestellt werden.

14. Was ist nötig, um den Betroffenen die nötige Hilfe zukommen zu lassen?

15. Sind Gewalt- und andere Fachberatungsstellen in der Lage, Fällen von digitaler Gewalt adäquat zu begegnen und wenn nicht: Was ist dazu nötig?

zu 14) & 15)

Die Fachberatungsstellen sind ein wichtiger Anlaufpunkt für Frauen die geschlechtsspezifische Gewalt erleben. Sie sind vor allem psychosozial geschult und leisten einen wichtigen Beitrag dazu, den Frauen eine Verarbeitung des Geschehens zu erleichtern und ihnen ihre Rechte aufzuzeigen. Ziel der Beratung ist es, den Betroffenen zu vermitteln, dass digitale Gewalt beendet werden kann, wenn frühzeitig und gezielt vorgegangen wird. Täter-Opfer-Umkehrungen und andere Dynamiken werden besprochen und Mädchen und Frauen aufgezeigt, dass sie sich adäquat zur Wehr setzen können.

Eine ausreichende, einzelfallunabhängige Finanzierung der Fachberatungsstellen und anderer bewährter Infrastrukturen ist nötig, um geschlechtsspezifischer, analoger sowie digitaler Gewalt zu begegnen. Das gilt sowohl bei der Nachsorge als auch bei der Prävention.

Derzeit besteht ein Mangel an finanziellen und personellen Ressourcen. Das gilt insbesondere, da die Erweiterung geschlechtsspezifischer Gewalt ins Digitale die Anforderungen an das Wissen und die Kompetenzen der Beraterinnen erhöhen, bei gleichbleibender - oft unzureichender - Finanzierung. Der Bedarf nach Weiterbildung und -qualifizierung ist enorm. Der bff erhält regelmäßig mehr Anfragen zu Fortbildungen für die Beratung bei Fällen digitaler Gewalt, als er bedienen kann. Teils wäre für eine adäquate Beratung externe Expertise nötig, beispielsweise die Konsultation von IT-Forensiker*innen, um festzustellen, ob ein Gerät durch Stalkerware kompromittiert ist und diese gegebenenfalls zu entfernen.

16. Denken Sie, dass der Aufbau von Technik-Kompetenzzentren eine sinnvolle Unterstützung der Beratungsstellen und Frauenhäuser sein könnte? Welche Kompetenzen sollten dort gebündelt werden?

Der bff begrüßt den Aufbau von Technik-Kompetenzzentren, wenn diese in Zusammenarbeit mit Fachberatungsstellen und Frauenhäusern fungieren und konzipiert werden.

Es ist unstrittig, dass ohne ein Grundverständnis digitaler Gewaltphänomene gute Unterstützung bei geschlechtsspezifischer Gewalt künftig nicht mehr möglich sein wird. Bereits jetzt gibt es Formen geschlechtsspezifischer Gewalt, wie beispielsweise Stalking, die fast immer auch IKT nutzen. Eine fehlende Expertise über geschlechtsspezifische Gewalt und IKT kann für die Betroffenen eine unzureichende Unterstützung zur Folge haben.

Momentan diskutieren einige Fachberatungsstellen verschiedene Modelle zur Kompetenzerweiterung und Unterstützung bei geschlechtsspezifischer digitaler Gewalt. So erproben einige die Zusammenarbeit mit IT-Unternehmen, die bei

technisch herausfordernden Beratungsprozessen hinzugezogen werden können. Auch wird vorgeschlagen, dass es für jede Beratungsstelle und jedes Frauenhaus eine Technik-Beauftragte geben sollte, die dafür zuständig ist, den jeweils aktuellen Stand der digitalen Angriffsmöglichkeiten und Möglichkeiten der Gegenwehr zu kennen. Ein weiterer Vorschlag ist die Einrichtung von Kompetenzzentren für geschlechtsspezifische digitale Gewalt, z.B. auf der Ebene der Bundesländer, deren Expertise durch die Mitarbeiter*innen von Beratungsstellen und Frauenhäusern bei Bedarf hinzugezogen und möglicherweise auch für Weiterbildungen genutzt werden kann.

17. Welche Regelungsdefizite gibt es?

18. Was sind die aus Ihrer Sicht drängendsten Schritte zur Bekämpfung von digitaler Gewalt gegen Frauen (Forschung, Beratung, Aufmerksamkeit, Kompetenzen der Behörden, Kompetenzen der Nutzer*innen, rechtliche Nachbesserungen, etc.)?

Die Fragen 17 und 18 werden gemeinsam beantwortet.

Forschung: siehe Frage 8.

Beratung: Es sollte garantiert werden, dass es eine angemessene Unterstützung und Beratung von gewaltbetroffenen Frauen und Mädchen durch ausfinanzierte Fachberatungsstellen gibt. Bestehende Unterstützungsangebote müssen finanziell in die Lage versetzt werden, der Digitalisierung der Gewalt auch in ihrer Beratung Rechnung zu tragen.

Aufmerksamkeit: Für eine größere Sichtbarkeit des Themas digitale geschlechtsspezifische Gewalt, wie beispielsweise durch die große bff-Social Media Kampange » digital + real« aus dem Jahr 2020, ist notwendig. Noch zu selten werden digitale Taten in ihrer für die Betroffenen realen Dimension erkannt.

Kompetenzen der Behörden: Behörden brauchen im Umgang mit Betroffenen von digitaler Gewalt spezifische Kompetenzen, um den Betroffenen angemessen zu begegnen und sie zu unterstützen. Dies umfasst einerseits psychosoziale Kompetenzen z.B. Wissen über Trauma-Erlebnisse, andererseits ein Verständnis für informationstechnische Geräte, Software-Anwendungen und die Dynamiken des Internets. Diese Kompetenzen müssen Behörden-Mitarbeiter*innen, die direkten Kontakt mit Betroffenen haben, in Fortbildungen vermittelt werden.

Kompetenzen der Nutzer*innen: Die ungleiche Verteilung von Wissen über Informationstechnik und dem mündigen Umgang mit Medien ist auch bei der Prävention geschlechtsspezifischer digitaler Gewalt ein Problem. Technikberufe sind weiterhin von Männern dominiert, wodurch das Gefühl der Hilflosigkeit und des Ausgeliefertseins für betroffene Frauen sich häufig verstärkt. Um dieses Ungleichgewicht zu beenden und z.B. auch Frauen und Mädchen zu empowern, einen selbstbewussten Umgang mit Geräten und Software zu entwickeln, sind Maßnahmen zur Förderung der IT-Kompetenz und digitalen Mündigkeit geboten. Darüber hinaus, wäre es hilfreich, IT- und Medienkompetenz bereits ab dem Grundschulalter in das Curriculum aufzunehmen. Das ist eine wichtige Investition in den mündigen Umgang mit digitalen Medien. Ein Bewusstsein für die Dynamiken des

Internets und sozialer Medien und die Möglichkeiten technischer Geräte können die Möglichkeiten der „digitalen Selbstverteidigung“ erhöhen.

Rechtliche Nachbesserung: Bei Gewalt die mit Hilfe digitaler Plattformen (Social Media, insbesondere aber auch Porno-Websites) begangen wird, müssen Täter und Plattformen in die Verantwortung genommen werden.

Plattformregulierung: Insbesondere um die Betroffenen von bildbasierter Gewalt zu entlasten ist es nötig, Plattformen in die Pflicht zu nehmen, sowohl präventiv tätig zu werden als auch betroffenengerecht zu intervenieren. Dazu gehören:

- Gut auffindbare, einheitliche, niedrigschwellige und tatsächlich funktionierende Möglichkeiten der Kontaktaufnahme
- Schnelle Reaktion der Plattformbetreiber*innen
- Vorkehrungen gegen Wieder-Upload

19. Gibt es Regelungen guter Praxis in anderen Staaten, auch zu Teilbereichen der digitalen Gewalt, und wie sind die Erfahrungen damit aus Ihrer Sicht?

Diese Frage kann der bff aufgrund der kurzen Bearbeitungsfrist nicht beantworten.

20. Bewerten Sie die anstehenden Novellierungen im Jugendmedienschutz insbesondere die Einführung der Deskriptorenliste - als geeignet mit Blick auf den Schutz von Mädchen und Frauen vor Cybergrooming?

Diese Frage kann der bff aufgrund der kurzen Bearbeitungsfrist nicht beantworten.

21. Reichen die vorhandenen rechtlichen Möglichkeiten zum Löschen von Doxing-Inhalten in den sozialen Medien aus? Wenn nein, welche zusätzlichen Maßnahmen schlagen Sie vor?

Viele Betroffene von Doxing gehen davon aus, dass im Laufe eines Strafverfahrens die betreffenden Inhalte automatisch gelöscht werden, wenn eine Strafbarkeit festgestellt wird, teils ist dies die Hauptmotivation zur Anzeigeerstattung. Dies ist jedoch nicht der Fall.

Um das Löschen von Doxing-Inhalten müssen sich die Betroffenen derzeit selbst kümmern.

Eine Möglichkeit besteht darin, sich direkt an die betreffenden Plattformen zu wenden und um Löschung zu bitten. Teils klappt dies gut, teils machen Betroffene auch sehr negative Erfahrungen, eine Systematik ist nicht erkennbar. Problematisch und überfordernd ist es für Betroffene, wenn Inhalte auf vielen unterschiedlichen Plattformen veröffentlicht sind. Die Kommunikation mit vielen verschiedenen Unternehmen, sehr unterschiedliche und teils nicht selbsterklärende Meldewege sowie gegebenenfalls die Auseinandersetzung mit einzelnen Plattformen über das Löschbegehren sind für Betroffene in der ohnehin schwierigen Situation nur schwer zu bewältigen. Hier gilt es dringend einheitliche, einfache und verlässliche Meldewege zu schaffen.

Eine weitere Möglichkeit besteht in dem Versuch, auf zivilrechtlichem Wege eine Unterlassungserklärung zu erwirken und so dem Täter die Löschverantwortung zu

übertragen. Gelingt das Erwirken, klappt die Löschung erfahrungsgemäß meist schnell und gut. Viele Betroffene scheuen verständlicherweise jedoch diesen Weg, da sie wie bei allen zivilrechtlichen Verfahren das Kostenrisiko tragen. Gewinnen sie das Verfahren, müssen die Kosten zwar von der Gegenseite getragen werden. Hat diese jedoch kein Geld, müssen Betroffene mindestens ihre eigenen Anwält*innenkosten übernehmen, was für viele ein zu großes Risiko darstellt.

Auch die Möglichkeit, ein Unternehmen mit der Löschung dieser Inhalte zu beauftragen, kommt für viele Betroffene nicht infrage, weil die Kosten hoch sind.

Der bff würde es begrüßen, wenn Melderegister-Auskunftssperren leichter zu erreichen wären, besonders für Frauen und Mädchen, die bereits von Cyberstalking, bildbasierter Gewalt oder anderen Formen der Belästigung, Beleidigung und Bedrohung im digitalen Raum betroffen waren. Den Betroffenen würde eine solche Sperre dahingehend Sicherheit verschaffen, dass zusätzliches Doxing erschwert wird.

Das erneute Veröffentlichen von persönlichen Daten ebenso wie von missbräuchlichem Bildmaterial bedeutet für Betroffene eine zeitlich unbegrenzte Ausdehnung der Gewalterfahrung und wird von vielen Betroffenen als besonders belastend erlebt, da sie für die erfahrene Gewalt keinen Abschluss finden. Der bff sieht Bedarf nach Regulierungen, die Plattformen in die Pflicht nehmen, um einen Wiederupload von Doxxing-Inhalten und bildbasierter Gewalt zu verhindern oder zu erschweren. Diese Regulierungen dürfen andere Grundrechte nicht unverhältnismäßig beeinträchtigen.

22. Wie bewerten Sie die Stärkung des Bundesverbandes Frauenberatungsstellen und Frauennotrufe in der Umsetzungsstrategie Digitalisierung der Bundesregierung? Welche Weiterentwicklungen wären angesichts des auslaufenden Projektes zum Ende 2021 notwendig?

Der bff ist erfreut, dass sein durch das BMFSFJ gefördertes Projekt "aktiv gegen digitale Gewalt" in der Umsetzungsstrategie Digitalisierung der Bundesregierung Erwähnung gefunden hat. Die laufende Projektphase seit 2019 hat angesichts der dynamischen Entwicklung des Projektthemas den Bedarf eines Folgeprojektes aufgezeigt, an dessen Konzeption der bff aktuell arbeitet und für das er auf erneute Förderung hofft.

23.a) Welchen Handlungsbedarf sehen Sie jenseits des Straf- und Zivilrechts?

Siehe Frage 18

23.b) Inwiefern bezieht sich die Istanbul-Konvention auf Digitale Gewalt? Wo besteht für die Bundesregierung Handlungsbedarf?

Die Istanbul-Konvention bezieht sich auf "alle Handlungen geschlechtsspezifischer Gewalt, die zu körperlichen, sexuellen, psychischen oder wirtschaftlichen Schäden oder Leiden bei Frauen führen oder führen können, einschließlich der Androhung solcher Handlungen" (Artikel 3). Weiterhin ist in der Konvention festgeschrieben, dass unter "Frauen" auch Minderjährige (Mädchen) gefasst werden. Diese Definition lässt den Schluss zu, dass digitale geschlechtsspezifische Gewalt in den Geltungsbereich der Istanbul-Konvention fällt.

Dass der Begriff digitale Gewalt im Konventionstext nicht enthalten ist, ist unseres Erachtens der Tatsache geschuldet, dass der Konventionstext bereits vor über 10 Jahren verfasst wurde und zu diesem Zeitpunkt weder Ausmaß noch Bedeutung der Digitalisierung dieser Gewalt erkennbar waren.

Der Handlungsbedarf wird in Frage 26 beantwortet (s.u.).

24. a) Erachten Sie ein Verbot von Video-, Foto- und Audioaufnahmegeräten in haushaltsüblichen Geräten, als notwendig?

b) Sehen Sie darüber hinaus Verbote, z.B. von entsprechenden Apps oder Software („Stalkerware"), als notwendig an?

zu 24 a) Hier kommt es darauf an, welche haushaltsüblichen Geräte gemeint sind. Der bff hält ein solches Verbot für nicht praktikabel und auch nicht für wünschenswert in Bezug auf Computer, Laptops, Smartphones und Tablets, da diese Geräte der Gesellschaft nicht per se Schaden, sondern im Gegenteil das Privatleben ebenso wie das berufliche Leben bereichern.
Anders verhält es sich bei Kameras und Mikrofonen die, z.B. durch besonders kleine Größe, erkennbar auf einen missbräuchlichen, geheimen Einsatz ausgelegt sind. Hier hält der bff eine Regulierung für denkbar.

Kritisch sehen wir das Verbauen von Kameras und Mikrofonen in vernetzten Alltagsgegenständen (Internet of Things, IoT). Mit jeder weiteren Kamera und jedem weiteren Mikrofon in einem Haushalt erhöht sich die Möglichkeit des Missbrauchs zur Überwachung und Kontrolle z.B. der Partnerin.

zu 24 b) Ein Verbot dedizierter Stalkerware würde der bff begrüßen. Die Hersteller von Stalkerware ziehen sich darauf zurück, eine legale Anwendung ihres Produkts - also mit freiwilliger Zustimmung der überwachten Person - liege in der Verantwortung des Kunden. Zunächst ist festzustellen, dass diese freiwillige Zustimmung ein höchst unrealistisches Szenario ist. Darüber hinaus ist dem bff kein legaler Anwendungsfall von Spionagesoftware vorstellbar, bei dem es sinnvoll, notwendig und legitim wäre, dass die Software auf dem Gerät versteckt wird, auf dem sie installiert ist. Genau dafür wäre ein Verbot sinnvoll, damit nicht nur die Täter i.S.v. überwachende Partner / Ex-Partner, sondern auch die Hersteller der auf Stalking ausgelegten Software in Verantwortung genommen werden können.

Wir wollen jedoch ausdrücklich darauf hinweisen, dass Cyberstalking auch mit Software und Geräten möglich ist, die eigentlich auf andere Zwecke ausgelegt sind, in solchen Fällen ist von Dual-Use-Software die Rede.

25. Welche Maßnahmen zur Prävention digitaler Gewalt gegen Mädchen und Frauen schlagen Sie vor?

Um Gewaltsituationen zu erkennen, zu beenden und ein Gefühl von Kontrolle und Handlungsfähigkeit für die Betroffenen wiederherzustellen oder auch zur Beweissicherung bei digitaler Gewalterfahrung empfiehlt der bff die Stärkung der Medienkompetenz der Betroffenen, ihrer Berater*innen und aller in Frage kommenden Unterstützer*innen.

Wir empfehlen, dass es zu digitaler geschlechtsspezifischer Gewalt Aufklärungsarbeit in Form von Fortbildungen für alle helfenden Berufsgruppen und Curricula in Schulen gibt. Das Wissen über stetig sich wandelnde technische Möglichkeiten und mündiger Umgang mit Medien müssen regelmäßig neu erarbeitet, in die bestehende Expertise zum Umgang mit geschlechtsspezifischer Gewalt integriert oder bei verlässlichen externen Expert*innen abgerufen werden können. Zusätzlich sollten Fachgespräche, Tagungen und Kampagnen regelmäßig zu geschlechtsspezifischer digitaler Gewalt informieren, die neue technische Entwicklungen und dadurch hervorgehende Bedrohungen für Frauen thematisieren.

Zivilgesellschaftliche Organisationen verfügen über das praktische Wissen, mit welchen Technologien digitale Übergriffe ausgeübt werden und wie die Situation der Betroffenen ist. Staaten sollten Technologie- und Softwareunternehmen ermutigen, mit diesen NGOs zusammenzuarbeiten, damit dieses Wissen in die Unternehmen hineingetragen werden kann. Als best practice für einen Zusammenschluss von Unternehmen und NGOs kann die Coalition Against Stalkerware (CAS) angesehen werden (https://stopstalkerware.org). Damit zivilgesellschaftliche Organisationen sich an solchen Bündnissen beteiligen können, benötigen sie dafür ausreichend finanzielle und personelle Ressourcen. Wir empfehlen deswegen, solche Bündnisse zu unterstützen und finanziell auszustatten.

Aktuell werden in Deutschland Digitalisierungsprozesse politisch gestaltet. Im Rahmen dieser Gestaltung und der Vergabe von damit zusammenhängenden Geldern, sollte die potenzielle Nutzbarkeit neuer Technologien für digitale Übergriffe systematisch berücksichtigt und präventiv bearbeitet werden. Auch sollten Entwickler*innen neuer Technologien und IT-Anwendungen verpflichtet werden, in den Entwicklungsprozessen die mögliche Nutzung ihrer Produkte zum Zwecke von Übergriffen und Gewalt abzuschätzen sowie präventiv Gegenmaßnahmen nachzuweisen. Technikfolgenabschätzungen für neue Geräte und Software müssen die missbräuchliche Anwendung für Gewalt berücksichtigen.

26. Sind Sie der Meinung, dass Deutschland seinen Verpflichtungen aus der Istanbul-Konvention im Hinblick auf digitale Gewalt nachkommt und wenn nicht, wo besteht Handlungsbedarf?

Die Istanbul-Konvention (Übereinkommen des Europarates zur Verhütung und Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt) erfordert umfangreiche Maßnahmen der Vertragsstaaten in den Bereichen Prävention, Schutz vor Gewalt, Unterstützung bei Gewalt und Bedrohung, rechtlicher Sanktionierung und Wiedergutmachung.

In Artikel 7 ist vorgeschrieben, dass alle Maßnahmen getroffen werden müssen, "um landesweit wirksame, umfassende und koordinierte politische Maßnahmen zu beschließen und umzusetzen, die alle einschlägigen Maßnahmen zur Verhütung und Bekämpfung aller in den Geltungsbereich dieses Übereinkommens fallenden Formen von Gewalt umfasst, und um eine ganzheitliche Antwort auf Gewalt gegen Frauen zu geben". Weiterhin wird verlangt, dass sämtliche Maßnahmen die Rechte des Opfers in den Mittelpunkt stellen. Die Entwicklung und Umsetzung einer koordinierten politischen Gesamtstrategie mit ganzheitlicher Antwort zur Bekämpfung von

geschlechtsspezifischer Gewalt steht bisher im förderalen Deutschland aus. Bestandteil einer solchen Gesamtstrategie müsste auch die konsequente Berücksichtigung digitaler Begehensweisen dieser Gewalt sein.

Aktuell wird die Digitalisierung aller gesellschaftlichen Bereiche politisch gestaltet, durch Zuständige innerhalb von Regierungen, wissenschaftliche Beiräte sowie den Einsatz massiver finanzieller Ressourcen (z.B. für die Entwicklung künstlicher Intelligenz). Eine systematische Integration des Themas digitale geschlechtsspezifische Gewalt in Digitalisierungsprozessen und -strategien ist bislang nicht gegeben, gleiches gilt für eine systematische Gleichstellungsperspektive in Digitalisierungsprozessen.

Weiterer Handlungsbedarf im Zusammenhang mit digitaler geschlechtsbezogener Gewalt aus der Istanbul-Konvention ergibt sich u.a. für folgende Bereiche:

- Artikel 11 (Datensammlung und Forschung), siehe dazu Fragen 8 und 9
- Artikel 22 (Spezialisierte Hilfsdienste), siehe dazu Fragen 14 und 15
- Artikel 49 (Ermittlungen, Strafverfolgung, Verfahrensrecht und Schutzmaßnahmen, Allgemeine Verpflichtungen), siehe dazu Frage 12

27. Welche erfolgreichen Maßnahmen, Projekte oder Gesetze zur Bekämpfung digitaler Gewalt sind Ihnen aus anderen Staaten bekannt?

Diese Frage kann der bff aufgrund der kurzen Bearbeitungsfrist nicht beantworten.

Literatur

Amnesty International (Hg.) (2017): »Toxic Twitter«. https://amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/#topanchor [Zugriff: 17.1.2020].

BSI: Bundesamt für Sicherheit in der Informationstechnik (2019): »Lagebericht zur IT-Sicherheit 2019«. https://bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html [Zugriff: 17.3.2021].

Delanie Woodlock (2014): Technology-facilitated stalking: findings and resources from the SmartSafe project. University of New England (Australia) https://www.researchgate.net/publication/267928015_Technology-facilitated_stalking_findings_and_resources_from_the_SmartSafe_project [Zugriff: 18.3.2021].

FRA: European Union Agency for Fundamental Rights (Hg.) (2014): »Gewalt gegen Frauen: eine EU-weite Erhebung. Ergebnisse auf einen Blick«. Wien. https://fra.europa.eu/sites/default/files/fra-2014-vaw-survey-at-a-glance-oct14_de.pdf [Zugriff: 18.3.2021].

JIM-Studie, Jugend, Information, Medien (2017) http://www.mpfs.de/studien/?tab=tab-18-1 [Zugriff: 18.3.2021].

Monckton-Smith (2019) Intimate Partner Femicide: using Foucauldian analysis to track an eight stage relationship progression to homicide. Violence Against Women, 26 (11). pp. 1267-1285 http://eprints.glos.ac.uk/6896/1/6896%20Monckton-Smith%20(2019)%20Intimate%20Partner%20Femicide%20using%20Foucauldian…… pdf [Zugriff: 18.3.2021].

Plan International: Welt-Mädchenbericht (2020): „Free to be online? Erfahrungen von Mädchen und jungen Frauen mit digitaler Gewalt", Studie von Plan International zu den Erfahrungen von Mädchen und jungen Frauen auf Online-Plattformen, https://www.plan.de/presse/pressemitteilungen/detail/welt-maedchenbericht-2020-digitale-gewalt-vertreibt-maedchen-und-junge-frauen-aus-den-sozialen-medien.html [Zugriff: 18.3.2021].

UN Special Rapporteur on violence against women (Hg.) (2018): Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective, 18.3.2021, **A/HRC/38/47.**

Weitere Informationen/ Ansprechpartnerin: Katja Grieger
Petersburger Straße 94 | 10247 Berlin
t: +49(0)30 32299500 | f: +49(0)30 32299501
info@bv-bff.de | www.frauen-gegen-gewalt.de