



Beratungs- und Unterstützungsstruktur zur Prävention und Intervention bei geschlechtsspezifischer Digitaler Gewalt



München.
Digital. Erleben.

Management Summary

Geschlechtsspezifische Digitale Gewalt ist ein ernstzunehmendes gesellschaftliches Problem. Da unser Alltag zunehmend von digitalen Hilfsmitteln geprägt ist, verlagert sich auch Gewalt zunehmend in den digitalen Raum. Täter*innen setzen psychische und physische Gewalt mit digitalen Mitteln fort, mit fatalen Folgen für die Betroffenen. Zudem dient Digitale Gewalt vermehrt auch dazu, physischen Zugriff auf Opfer zu erlangen, um physische Gewalt auszuüben. Ebenso kann Digitale Gewalt dieselben psychischen Schäden wie analoge Gewalt verursachen.

Beratungsangebote für Opfer Digitaler Gewalt sind rar und Wartezeiten insbesondere bei spezifischen technischen Fragestellungen dementsprechend lang. Zwar gibt es zivilgesellschaftliche Organisationen, die online Informationen und Hilfe für unterschiedliche Gewaltformen anbieten, diese digital zu kontaktieren, stellt jedoch bereits eine Hürde für Betroffene dar. Bereits das Anzeichen, Hilfe zu suchen, kann Täter*innen alarmieren. Sich persönlich an Beratungsstellen vor Ort zu wenden, ist im Zweifelsfall die einzige sichere Lösung. Weil Anlaufstellen für Gewaltopfer, wie etwa Frauenhäuser, häufig nicht über die erforderliche technische Expertise verfügen, können diese Betroffenen jedoch nicht immer bei technischen Fragen helfen.

An dieser Stelle soll das Konzept für eine „Beratungs- und Unterstützungsstruktur zur Prävention und Intervention bei geschlechtsspezifischer und antifeministischer Digitaler Gewalt“ kurz IT-Fachberatung ansetzen. Es soll Beratungsstellen und Frauenhäuser befähigen, geschlechtsspezifischer Digitaler Gewalt vorzubeugen sowie auch nach einem digitalen Angriff effektiv zu helfen. Die IT-Fachberatung ist neben psycho-sozialer und juristischer Unterstützung ein wichtiger Baustein in der Hilfeleistung. IT-Fachberatung hat, je nach Gewaltform, verschiedene inhaltliche Schwerpunkte. Bei bildbasierter Gewalt wie zum Beispiel DickPics (unaufgeforderte Penisbilder), brauchen Betroffene Informationen dazu, wie sie Betreibende sozialer Medien zum Löschen der gefährdenden Inhalte auffordern können. Bei Cyberstalking, also dem Nachstellen durch z.B. AirTags oder Spyware, benötigen sie Unterstützung, die gefährdende Technologie zu finden und nachhaltig zu entfernen. Während es im ersten Beispiel also eine Informationsleistung ist, geht es beim zweiten Fall um technische Hilfe im eigentlichen Sinne.

Betroffene brauchen zeitnah und unkompliziert qualifizierte und bezahlbare Hilfe. Anlaufstellen für Gewaltopfer bzw. die Betroffenen selbst sollen mit einer Selbsthilfeplattform dabei unterstützt werden, Risiken für Digitale Gewalt (wie etwa Tracker) zu erkennen und nach Möglichkeit auszuschalten, sowie auch einfache Fälle Digitaler Gewalt selbst zu lösen. Die Plattform entlastet den menschlichen Support und befähigt mit Antworten zu häufig gestellten Fragen (FAQs) und Checklisten sich selbst zu helfen. Neben einem öffentlich zugänglichen Bereich soll es einen Login-Bereich mit detaillierteren Informationen geben, die Täter*innen nicht zugänglich sind.

Reichen die Informationen zur Selbsthilfe nicht aus, nimmt die betreuende Anlaufstelle, die IT-Fachberatung in Anspruch. Die aktive Unterstützung der IT-Fachberatung teilt sich in 1st Level und 2nd Level Support auf. Der 1st Level Support kann die Lage der Betroffenen einschätzen. Gemeinsam mit der betreuenden Anlaufstelle und der betroffenen Person kann der 1st Level Support dann grundlegende technische Hilfe leisten und Beweise sichern helfen. Das reicht nach den Erfahrungen aus vergleichbaren Praxisbeispielen in den meisten Fällen Digitaler Gewalt bereits aus. Bei schweren Fällen Digitaler Gewalt braucht der 1st Level Support spezialisierte Unterstützung mit vertiefter Expertise im Bereich IT-Security oder einer IT-Forensik, dem 2nd Level Support.

Kommunikation und Verbreitung des Konzeptes zur IT-Fachberatung, sowie der Aufbau und die Erprobung der beschriebenen Dienstleistungen sind weitere essenzielle Bausteine.

Das hier vorliegende Konzept zur IT-Fachberatung baut auf einer Recherche und Bedarfsanalyse auf. Dennoch müssen Erfahrungswerte gesammelt werden, bis das Konzept in einem Echtbetrieb ausgerollt werden kann. Deshalb schlagen wir eine etwa 2-jährige Testphase vor. Dieser soll offene Fragen, wie etwa zum tatsächlichen Umfang des Bedarfs, sowie zur Eignung verschiedener Bereitstellungsvarianten beantworten und die Praxistauglichkeit des Konzepts sicherstellen.

Inhaltsverzeichnis

1	Einleitung.....	4
1.1	Hintergrund und begriffliche Grundlagen zu Digitaler Gewalt.....	4
1.2	Genaue Daten zum Umfang Digitaler Gewalt unbekannt	5
2	Vorgehen zur Ermittlung von Bedarfs- und Angebotssituation.....	7
3	Bedarfssituation	8
4	Angebotssituation	11
4.1	Zielgruppe der Initiativen.....	11
4.2	Relevante Aspekte während der Beratung.....	12
4.3	Relevante Faktoren beim Einsatz von IT-Fachkräften.....	12
4.4	Weitere Herausforderungen.....	12
4.5	Bedarf nach IT-Fachberatung kann aktuell nicht gedeckt werden	13
4.6	Hilfreiche Ansätze für zukünftige Konzepte für ein Unterstützungsangebot (Good Practices): 14	
5	Konzept für IT-Fachberatung in Fällen geschlechtsspezifischer Digitaler Gewalt.....	15
5.1	Präventionsangebot.....	15
5.1.1	Minimalversion.....	15
5.1.2	Ausbaustufe.....	16
5.2	Selbsthilfeplattform	16
5.2.1	Minimalversion.....	16
5.2.2	Ausbaustufe.....	16
5.3	Technische Hilfe.....	16
5.3.1	1st Level-Support.....	16
5.3.2	2nd Level-Support	16
5.4	Kommunikation	16
5.4.1	Minimalversion.....	16
5.4.2	Aufbaustufe	17
5.5	Bereitstellen & Weiterentwickeln.....	17
6	Ausblick.....	18
7	Literaturverzeichnis	19
8	Anhang.....	19

1 Einleitung

Die Stadt München fördert verschiedene Anlaufstellen für Menschen, die von geschlechtsspezifischer und antifeministischer Gewalt bedroht oder betroffen sind. Unter den Gewaltformen, die hier auftreten, nimmt Digitale Gewalt kontinuierlich zu (BKA, 2024). Täter*innen nutzen immer häufiger digitale Technologien, um analoge Gewalt im digitalen Raum fortzusetzen oder setzen Digitale Gewalt ein, um physischen Zugriff auf ihre Opfer zu erhalten. Gleichzeitig wird Digitale Gewalt im Vergleich zu physischer Gewalt verharmlost. Für Außenstehende ist sie schwer wahrnehmbar, obwohl sie Betroffene selbst im Schutzraum der eigenen Wohnung jederzeit erreichen kann und zu denselben psychischen Beschwerden wie physische Gewalt führt. Betroffene können unter Depressionen leiden bis hin zu Suizidgefahr bei schweren Fällen. Aber auch leichtere Fälle Digitaler Gewalt fallen gesamtgesellschaftlich ins Gewicht.

Der Gender Gap im Bereich der Digitalkompetenz (Initiative D21, o.J.) hat zur Folge, dass weiblich gelesene Personen aller Altersgruppen sich im Schnitt weniger für digitaltechnische Themen interessieren und weniger Wissen und Nutzungsroutine aneignen als männlich gelesene Personen derselben Altersgruppe. Dies führt auch in Gewaltsituationen zu Abhängigkeiten und erhöhten Risiken für Digitale Gewaltformen.

Viele Anlaufstellen für Betroffene geschlechtsspezifischer Gewalt haben nicht genügend Personal- und Wissensressourcen, um in Fällen von Digitaler Gewalt zu helfen. Das bedeutet, dass in diesen Fällen Risiken, die sich aus Digitaler Gewalt ergeben, eventuell nicht erkannt werden oder nicht bearbeitet werden können. Damit sind erhebliche Gefahren für die seelische und physische Gesundheit der Betroffenen verbunden.

Im Rahmen der Umsetzung des Aktionsplans der Stadt München gegen geschlechtsspezifische Gewalt hat die Gleichstellungsstelle für Frauen einen vierteiligen Fachaustausch zu kommunalen Präventions-, Interventions- und Unterstützungsmöglichkeiten auf kommunaler Ebene für den Bereich geschlechtsspezifische Digitale Gewalt organisiert. Gemeinsam mit Expert*innen aus unterschiedlichen Bereichen und mit verschiedenen Zugängen zum Themenfeld (Fraueneinrichtungen, Beratungsstellen, Fachberatungen, feministische Communities und Fachstellen aus der Verwaltung RIT, Sozialreferat, Personal- und Organisationsreferat, FgR (Fachstelle für Demokratie), Polizei, Runder Tisch gegen Männergewalt u.a.) wurden rechtliche Fragen und technische Herausforderungen vor dem Hintergrund der Erfahrungen und Bedarfe aus der Praxis besprochen. Die in diesem Prozess herausgearbeiteten Handlungsbedarfe und Maßnahmen wurden der Stadtratskommission zur Gleichstellung von Frauen vorgestellt und in der Empfehlung 189 „Einrichtung einer Beratungs- und Unterstützungsstruktur zur Prävention und Intervention bei geschlechtsspezifischer und antifeministischer digitaler Gewalt“ zusammengefasst.

1.1 Hintergrund und begriffliche Grundlagen zu Digitaler Gewalt

Unter geschlechtsspezifischer Digitaler Gewalt wird in diesem Dokument Folgendes verstanden:

Da sich das Konzept zur IT-Fachberatung an Anlaufstellen für Betroffene geschlechtsspezifischer und antifeministischer Gewalt richtet, wird in diesem Zusammenhang alle Digitale Gewalt, die sich gegen diese Personen richtet, als geschlechtsspezifische Digitale Gewalt verstanden. Dabei spielt keine Rolle, ob die Form bzw. der Inhalt der Digitalen Gewalt Bezug auf das Geschlecht des Opfers nimmt.

In diesem Verständnis kann geschlechtsspezifische Digitale Gewalt in verschiedenen Formen auftreten (Bundesverband Frauenberatungsstellen und Frauennotrufe (bff)) (Frauen gegen Gewalt e.V.) (HateAid):

1. Cyberstalking: Nachstellung mit digitalen Mitteln. Täter*innen verfolgen den Standort, Gespräche oder Chats Betroffener über Router, soziale Medien, SmartTags oder Stalker Ware. Sie üben Kontrolle aus und geben den Betroffenen ein Gefühl der Ohnmacht.
2. Cybergrooming: Sexuelle Annäherung Erwachsener gegenüber Kindern und Jugendlichen in Chats und auf sozialen Plattformen.
3. Doxing: Sammeln und Veröffentlichen personenbezogener Daten, oft im Zusammenhang mit Androhung von Gewalt oder dem Aufruf Dritter zur Vergewaltigung.
4. Sextortion: Nötigung oder Erpressung mit (teilweise Deepfake-) oder einst einvernehmlich aufgenommenen Nacktfotos o.ä.
5. Sexuelle Belästigung & Cybermobbing: sexistische Hatespeech, Beleidigungen, üble Nachrede, Verleumdung und Falschbehauptungen in Social Media und Privatchats.
6. Fakeaccounts: Diffamieren und Beschämen der Betroffenen durch das Verbreiten von sexualisierten Falschinformationen über Fakeaccounts.
7. Cyberflashing: Verbreiten pornografischer Inhalte wie DickPics.
8. Hacken von Konten, z.B. um Passwörter zu verändern, die eine Kontaktaufnahme nach außen oder das Abheben von Geld erschweren.
9. Missbrauch von IoT/Smart Home: Täter*innen schließen von einem externen Standort bspw. Fensterläden oder spielen laute Musik ab. Damit lassen sie Betroffene an ihrer eigenen Urteilskraft zweifeln.
10. Täuschung Dritter mittels generativer KI, wenn z.B. Täter*innen KI-generierte Bilder dem Jugendamt oder anderen relevanten Stellen als Beweis vorlegen.

1.2 Genaue Daten zum Umfang Digitaler Gewalt unbekannt

Bei vielen Gewaltform ist es unklar, wie häufig sie vorkommen. Statistiken erfassen vermehrt physische Gewalt statt Digitaler Gewalt. Das Bundeskriminalamt (BKA) veröffentlichte im Juni 2024 eine Statistik (BKA, 2024), wonach es deutschlandweit im Jahr 2023 119 angezeigte Fälle von Stalking nach §238 StGB und 188 angezeigte Fälle von sexuellem Missbrauch von Kindern und Jugendlichen im familiären Umfeld durch das Tatmittel Internet nach §176 StGB bzw. §182 StGB gab, die Dunkelziffer dürfte um einiges höher liegen. Bei häufig vorkommenden Formen Digitaler Gewalt wie DickPics realisieren viele Betroffene nicht, dass ihnen Gewalt widerfährt. Oder sie trauen sich aufgrund der finanziellen Abhängigkeit von Täter*innen nicht, die Tat anzuzeigen, wie in Fällen Digitaler häuslicher Gewalt. So berichtet eine Studie des Pew Research Centers (Pew Research Center, 2017), dass zwei Drittel aller Betroffenen Taten ignorieren und nichts unternehmen. Lediglich 5 Prozent der Betroffenen melden geschlechtsspezifische Digitale Gewalt den Strafverfolgungsbehörden. Gründe dafür sind die Erfahrung, dass Opfern die Schuld an der Tat gegeben wird, oder die teils auch berechnete Annahme, dass die Strafverfolgung eingestellt wird. Das deckt sich mit den Erkenntnissen unserer Interviews. Beratungsstellen raten Betroffenen nur selten, sich direkt an die Polizei zu wenden. Auch unser Interview mit der Polizei ergab ein ähnliches Bild. Die Zuständigkeit der Polizei beschränkt sich auf den strafbaren Teil Digitaler Gewalt, der in prädigitalen Gesetzen beschrieben ist. Nur ein kleiner Teil der Polizei ist mit Digitaler Gewalt vertraut und kann sich dementsprechend mit diesen Fällen befassen.

Umso mehr sind die Betroffenen auf Anlaufstellen und zivilgesellschaftliche Akteure angewiesen, diese allerdings können meist dem Umfang, der an sie gerichteten Anfragen, aufgrund von Ressourcenknappheit nicht gerecht werden. Es gibt deutschlandweit eine Auswahl von Organisationen, die sich auf bestimmte Formen Digitaler Gewalt spezialisiert haben. Eine Übersicht befindet sich im Abschnitt 4 Angebotssituation.

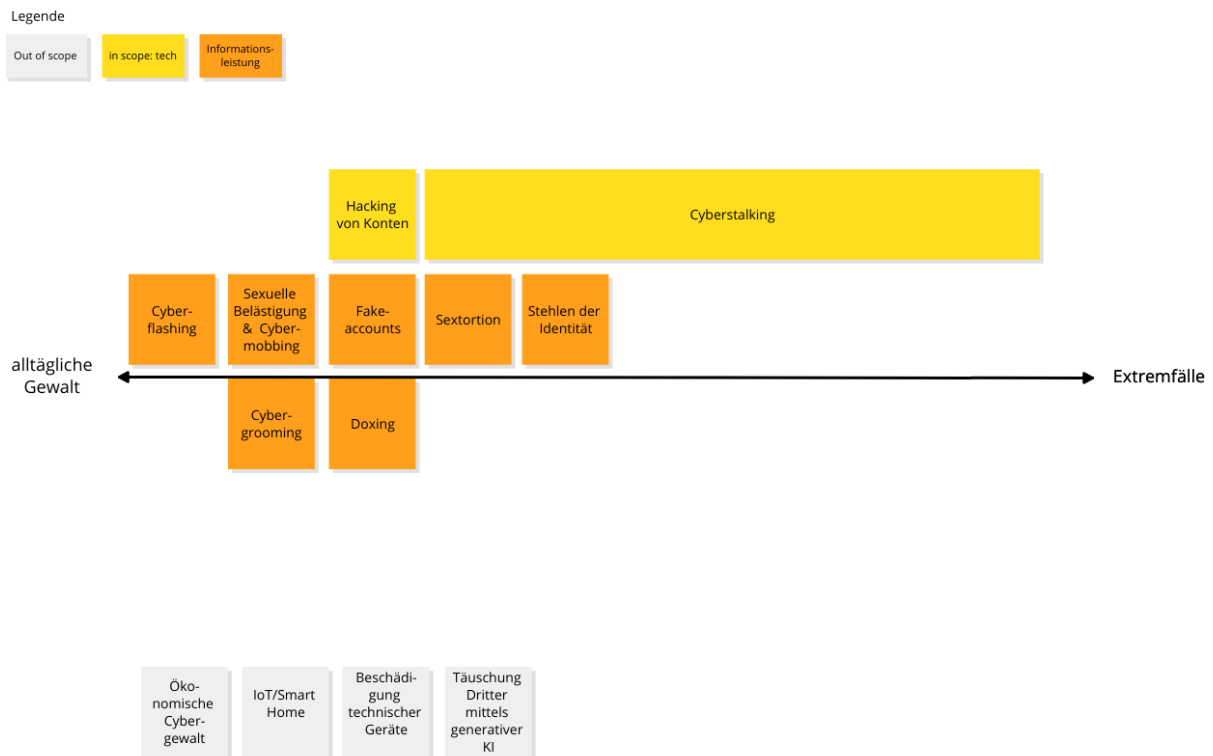


Abbildung 1: Formen Digitaler Gewalt sortiert nach wahrgenommener Häufigkeit & Schwere

Abbildung 1 liegen Expert*innen-Interviews zu Grunde. Sie ordnet Formen geschlechtsspezifischer Digitaler Gewalt in ein Spektrum zwischen alltäglicher Gewalt und vergleichsweise seltenen Extremfällen ein. Außerdem zeigt die Farbmarkierung, ob eher eine Informationsleistung oder technische Hilfe bei dieser Gewaltform anzuwenden ist.

Bei den meisten Formen von Gewalt reicht es aus, Betroffenen Lösungswege aufzuzeigen. Sei es, dass die Betroffenen Passwörter neu vergeben, sich eine zusätzliche E-Mail-Adresse zulegen oder sexistische Inhalte an die zuständige Plattform melden. Hier genügt es, dass Betroffene gemeinsam mit Berater*innen Schritt-für-Schritt-Anleitungen befolgen.

Bei einigen Fällen von Gewalt wie schweren Stalking sind komplexere Schritte erforderlich. Hier muss analysiert werden, mit welchen technischen Mitteln Betroffenen Gewalt angetan wird, um diese zu entfernen. In diesem Fall sprechen wir von technischem Support.

Das weitere Dokument ist wie folgt aufgebaut: Als Grundlage für die Entwicklung eines Konzepts zur IT-Fachberatung zu Fällen Digitaler Gewalt haben wir uns mit der Bedarfs- und Angebotssituation für diese Beratung auseinandergesetzt. Das Vorgehen dazu wird im nachfolgenden Abschnitt erläutert. Die Erkenntnisse zu Bedarf und Angebot werden daran anschließend vorgestellt. Aus der Auswertung dieser Erkenntnisse haben wir das Konzept für die IT-Fachberatung für Anlaufstellen geschlechtsspezifischer Gewalt entwickelt. Die Elemente dieses Konzepts werden im Abschnitt Konzept für IT-Fachberatung in Fällen geschlechtsspezifischer Digitaler Gewalt beschrieben. Daran anschließend folgt ein Ausblick der bisherigen Überlegungen zu möglichen Bereitstellungsvarianten für die IT-Fachberatung und schließlich ein Fazit mit Empfehlungen für das weitere Vorgehen.

2 Vorgehen zur Ermittlung von Bedarfs- und Angebotssituation

Zur Ermittlung der Bedarfs- und Angebotssituation wurden zunächst eine Literaturrecherche und im weiteren Verlauf eine Vielzahl umfangreicher Interviews durchgeführt.

Ziel der Literaturrecherche war es, bestehende Forschungsergebnisse, theoretische und praktische Ansätze zu identifizieren, die für das Verständnis der thematischen Verortung im Bereich Digitaler Gewalt und als Grundlage für die Analyse der Interviews dienten.

Die ausgewählte Literatur wurde systematisch ausgewertet und für das Projekt relevante Informationen wurden in einem Literaturüberblick, in der zentralen Arbeitsplattform eines digitalen Whiteboards, zusammengefasst. Besonders hilfreich zur Kontextualisierung und Vergleichbarkeit der Interviews waren ein Handlungsleitfaden zu Cybergewalt der Stadt Wien, die Kriminalitätsstatistik der bayerischen Polizei und die Studie (K)ein Raum: Cyber-Gewalt gegen Frauen in (Ex-) Beziehungen (Hochschule Wien, 2022). Insgesamt ist der Forschungsstand zu Digitaler Gewalt auf nationaler Ebene noch sehr dünn, im internationalen Vergleich ist die Studienlage in den USA am umfangreichsten.

Das Hauptanliegen der Interviews war es, tiefere Einblicke in die Erfahrungen der Anlaufstellen in München mit Digitaler Gewalt und über ihren Bedarf an entsprechender technischer Beratung zu gewinnen. Dabei wurden qualitative Daten gesammelt, die durch quantitative Erhebungen nicht erfasst werden können. Darüber hinaus sollten Erkenntnisse über die Situation in anderen Städten gesammelt werden, die bereits vergleichbare Angebote für IT-Fachberatung im Zusammenhang mit geschlechtsspezifischer Digitaler Gewalt aufgebaut haben. Dies geschah über Gespräche mit Vertreter*innen von Good Practice Beispielen aus Projekten in Deutschland und Österreich und relevanten Akteur*innen wie dem polizeilichen Kommissariat für Prävention und Opferschutz.

Für die Interviews wurden semi-strukturierte Gesprächsleitfäden erarbeitet. Diese Methodik ermöglicht es, spezifische Themen (hier a.) eigenes Projekt, b.) organisatorische Ausgestaltung und c.) rechtliche Ausgestaltung) gezielt anzusprechen, während gleichzeitig Raum für individuelle Erfahrungen der Teilnehmer*innen bleibt.

Die Stichprobe bestand aus 19 Einrichtungen und Akteur*innen (12 Good Practice Einrichtungen und weitere Akteur*innen, sieben Anlaufstellen aus München), die persönlich angeschrieben wurden. Auswahlkriterien waren u.a. nationale Tragweite/Vorbildfunktion im Themenschwerpunkt, inhaltliche Überschneidung und Bezug zu Digitaler Gewalt, sowie die Bereitschaft, über persönliche Erfahrungen aus dem Arbeitsalltag zu berichten.

Die Interviews wurden zwischen März und Mai 2024 durchgeführt. Jedes Interview dauerte durchschnittlich etwa 50 Minuten und fand bis auf zwei Ausnahmen per Videokonferenz statt. Mit Zustimmung der Teilnehmenden wurden 9 der 19 Gespräche aufgezeichnet, um eine genaue Transkription und Analyse zu ermöglichen. Die wichtigsten Erkenntnisse wurden im projektinternen digitalen Whiteboard dokumentiert, zusammengeführt und geclustert.

3 Bedarfssituation

Die Stadt München fördert Einrichtungen wie Frauenhäuser sowie Beratungsstellen für Jungen, Mädchen, Männer, Frauen und Personen aller anderen Geschlechter. Diese sind in Tabelle 1 aufgelistet:

Bezeichnung der Einrichtung	URL
Frauenhilfe München	https://www.frauenhilfe-muenchen.de
Frauen helfen Frauen	https://www.homeless-online.de/frauen-helfen-frauen-e-v-muenchen/
Haus Hager	https://haus-hager-muenchen.de
IN VIA München e.V.	https://www.invia-muenchen.de
IMMA Zufluchtsstelle für Mädchen und junge Frauen	https://imma.de
Frauennotruf München	https://frauennotruf-muenchen.de
Münchner Informationszentrum für Männer	https://www.maennerzentrum.de
KIBS – Beratungsstelle für Jungen* und junge Männer*	https://www.kinderschutz.de/angebote/kibs-beratung-bei-missbrauch-haesuslicher-gewalt/
Trans*Inter*Beratungsstelle Fachstelle gegen Diskriminierung und Gewalt	https://www.trans-inter-beratungsstelle.de/de/
STRONG – LGBTIQ*	https://strong-community.de
Before	https://www.before-muenchen.de

Tabelle 1: geförderte Anlaufstellen für Opfer geschlechtsspezifischer Gewalt in München

Wir konnten mit sieben Einrichtungen sprechen. Die Erkenntnisse sind im Folgenden zusammengefasst.

Vorab lässt sich sagen, dass das Wissen rund um Digitale Gewalt je nach Einrichtung sehr unterschiedlich ausgeprägt ist. Teilweise gibt es bereits umfangreiche Erfahrung mit Digitaler Gewalt und teils noch wenig. Eine Einrichtung beschäftigt nach eigener Aussage schon Dienstleister*innen, um ihre Klient*innen vor Digitaler Gewalt zu schützen, während andere sich seit Jahren um entsprechende Unterstützung bemühen. Einrichtungen für Kinder und Jugendliche brauchen eine andere Art von Unterstützung als Frauenhäuser oder Beratungsstellen für Trans-Menschen.

Unabhängig von den Münchner Einrichtungen gibt es auch überregionale Anlaufstellen für Betroffene Digitaler Gewalt. Sich in der Vielfalt der Angebote zu orientieren und das Richtige zu finden, ist allerdings alles andere als einfach. Daher ist es verständlich, dass nicht alle Betroffenen in einer für sie schwer belastenden Situation zu den benötigten Angeboten finden.

Grundsätzlich braucht es im Kontext Digitaler Gewalt immer beides: präventive Hilfe, um Gewalt vorzubeugen, und kurative Hilfe (Intervention), nachdem eine Gewalttat geschehen ist. Daneben wird bei Digitaler Gewalt immer auch psychosoziale und rechtliche Beratung seitens der Anlaufstellen geleistet. Mit technischen Fragen sind die Anlaufstellen in Fällen Digitaler Gewalt mangels entsprechender Expertise i.d.R. überfordert.

Unter IT-Fachberatung verstehen wir das Analysieren und Entfernen der Gefahrenquelle (Stalking-Software, Social Engineering, etc.). Ergänzend zur aktiven Analyse und Entfernung von digitalen Bedrohungen werden auch Informationen benötigt, damit die Betroffenen selbst aktiv werden können. Davon abweichend geht es bei der Informationsleistung um klare Handlungsschritte, etwa das Kontaktieren von Plattformbetreibern, um z.B. Fake-Profilen oder Hasskommentare löschen zu lassen.

Leider gibt es kaum Statistiken zur Häufigkeit der verschiedenen Formen Digitaler Gewalt. Auch die Münchner Einrichtungen konnten auf Anfrage nicht mitteilen, wie oft eine Informationsleistung und wie oft technischer Support gebraucht wird. Der Frauennotruf Wien lieferte zumindest erste Anhaltspunkte. So waren 2023 bezogen auf die insgesamt dort registrierten Fälle geschlechtsspezifischer Digitaler Gewalt ca. 20% Stalking, 17% Erpressung mit Fotos, 13% Belästigung und 9% Androhung von Gewalt. Insgesamt gab es ca. 160 Fälle mit erwachsenen Betroffenen; Kinder und Jugendliche werden dort nicht betreut.

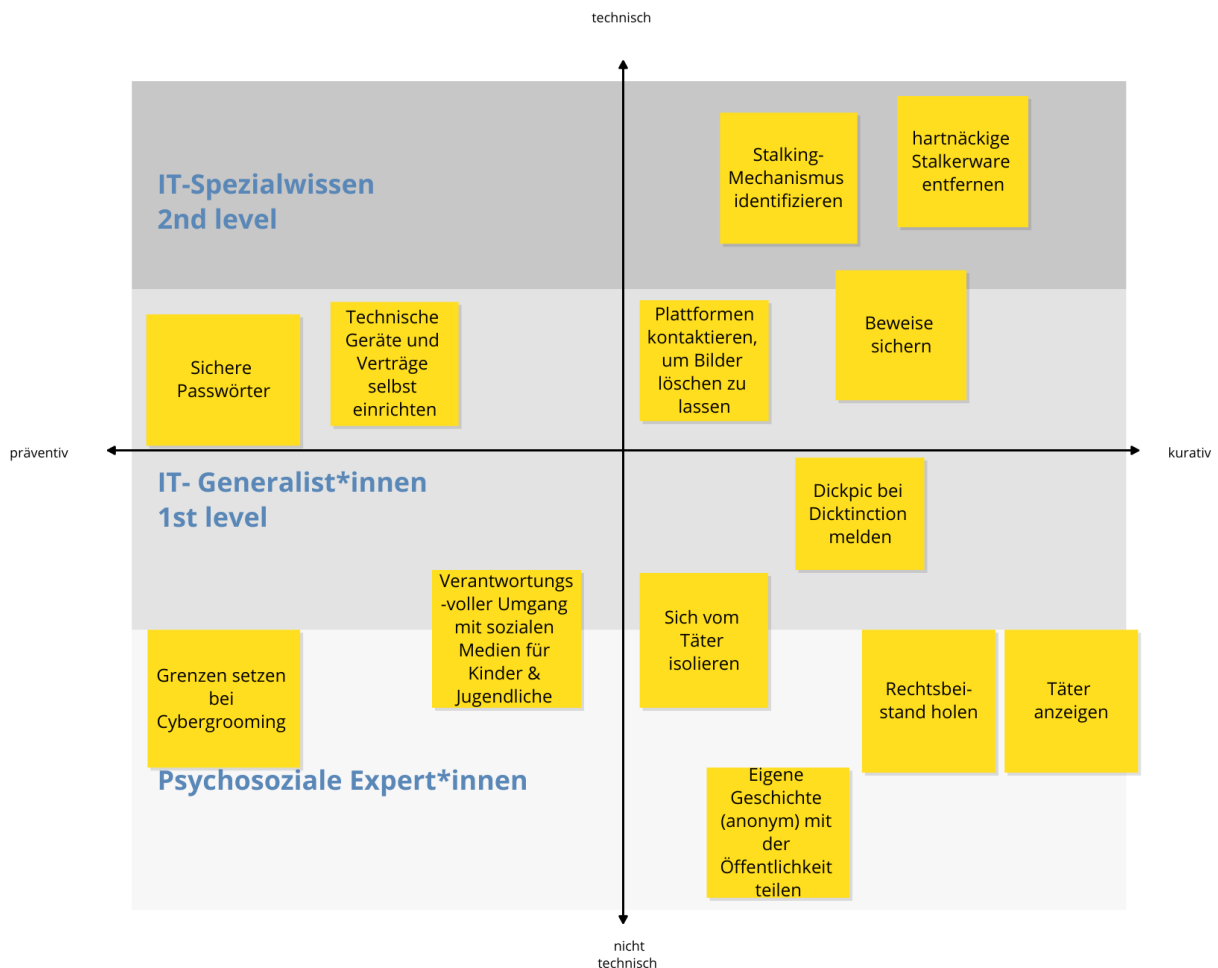


Abbildung 2: Maßnahmen und Zuständigkeiten bei Hilfestellung beim Umgang mit Digitaler Gewalt

Abbildung 2 beschreibt das Zusammenspiel der Akteur*innen für Gegenmaßnahmen gegen geschlechtsspezifische Digitale Gewalt. Auf der waagerechten Achse bewegt sich das Spektrum zwischen präventiven und kurativen Maßnahmen, während die senkrechte Achse die Maßnahmen nach technisch bzw. nicht technisch gliedert. Bei allen nicht-technischen Aspekten können laut Auskunft unserer Interviewpartner*innen die Anlaufstellen/Beratungsfachkräfte im Umfeld der Betroffenen mit geeigneter Unterstützung selbst helfen. Technischere Fragen und Probleme sollten an IT-Generalist*innen bzw. -Spezialist*innen gerichtet werden.

Jugendlichen den verantwortungsvollen Umgang mit sozialen Medien zu vermitteln, könnte nach unseren Erkenntnissen in beiderlei Zuständigkeit, in die von Beratungsstellen und auch von IT-Generalist*innen fallen. IT-Generalist*innen sollten Frauen zeigen, wie sie technische Geräte selbst einrichten, um Digitaler Gewalt vorzubeugen. Oder wie sie soziale Plattformen kontaktieren, um gegen ihren Willen veröffentlichte Nacktaufnahmen löschen zu lassen. Bei schweren Stalking-Fällen müssen IT-Spezialist*innen herangezogen werden.

Fast alle Anlaufstellen nannten den Bedarf an Selbstbefähigung der Betroffenen. Die wesentlichen Inhalte, zu denen Betroffene befähigt werden sollten und sich selbst zu helfen, werden nachfolgend geordnet nach Priorität aufgelistet:

1. Gerätechecklisten bereitstellen und aufzeigen, dass das **Einhalten gängiger Sicherheitsstandards** (Passwörter wechseln etc.) gegen geschlechtsspezifische Digitale Gewalt hilft.
2. Anleitungen zur **rechtskräftigen Beweissicherung und Dokumentation** Digitaler Gewalt
3. **Erwartungshaltung der Betroffenen** hinsichtlich der **Polizei** formen: bewusst machen, wo die Polizei helfen kann und wo nicht, um weitere Enttäuschung zu vermeiden.
4. **Interesse an technischen Themen** wecken: Mädchen* und Frauen* motivieren, sich Wissen anzueignen, und Verantwortung für ihre technischen Geräte zu übernehmen.
5. **Bewusstsein für Risiken** schaffen: Anschauliche Szenarien bieten, womit sich Betroffene identifizieren und die ihnen widerfahrene Gewaltform einordnen können, ohne dabei Täter zu inspirieren.
6. Eine **'Safe Space'-Plattform** bieten, wo Betroffene sich untereinander austauschen können.
7. Niedrigschwellige und leicht verständliche **Informationen über die eigenen Rechte**, juristischen Möglichkeiten und nachfolgenden Prozessschritte bereitstellen.
8. **Kinder & Jugendliche sensibilisieren**, wo Digitale Gewalt anfängt, und Handlungsoptionen aufzeigen; Kindern, Erziehungsberechtigten und Lehrkräften eine sichere Nutzung von Social Media beibringen.

Unsere Recherche ergab, dass sich Formen geschlechtsspezifischer Gewalt je nach Zielgruppe unterscheiden:

Kinder und Jugendliche werden Opfer von Cybergrooming. Dabei geht es per Definition um die sexuelle Annäherung Erwachsener an Kinder mit digitalen Mitteln. Auch im schulischen Kontext gibt es Digitale Gewalt seitens Gleichaltriger wie DickPics oder sexistische Kommentare in Klassenchats oder sozialen Plattformen. Stalking oder Doxing wurden von den befragten Einrichtungen nicht ausdrücklich benannt, können jedoch ebenso vorkommen. Ebenso selten sind Kinder und Jugendliche nach Aussage der befragten Anlaufstellen durch Gewalt im Kontext Smart Home betroffen (im Zweifelsfall eher ihre Eltern). Technische Hilfe ist in diesem Fall eher eine Informationsleistung. Um weitere Gewalt zu verhindern, müssen Konten auf sozialen Medien privat gestellt, Täter*innen gesperrt, Passwörter geändert oder Kommentare gemeldet werden. Das alles sind klar definierte, vom zeitlichen Aufwand überschaubare Abläufe.

Bei Frauenhäusern, in denen nur erwachsene Frauen aufgenommen werden, sieht die Situation nach unseren Erkenntnissen anders aus. Täter*innen sind in vielen Fällen Ex-Partner*innen in dem entsprechenden Alter der Betroffenen und haben anders als Jugendliche und ältere Menschen eher die Möglichkeit, sich technisches Tiefenwissen anzueignen. Entsprechend geht von ihnen technischanspruchsvollere Gewalt aus. Deswegen ist gerade bei Frauenhäusern technische Hilfestellung im Sinne von Cyberforensik besonders wichtig. Während sich Betroffene bei vielen Arten der Digitalen Gewalt Informationen selbst beschaffen können, ist praktische Hilfe nur schwer zu bekommen. Die Auftragsbücher von Cyberforensik-Unternehmen sind voll und Aufträge können mehrere Tausend Euro kosten. Zumal es für forensische Dienstleistungen keine Kund*innenbewertungen oder andere Evidenzen gibt, auf deren Basis Betroffene auswählen könnten. Auch neue Geräte zu kaufen, kann sich längst nicht jede Betroffene leisten. Und selbst bei der Münchner Polizei müssen Betroffene bis zu einem Jahr warten, um ihre Geräte prüfen zu lassen. Daher ist es wichtig, dass eine IT-Fachberatung zeitnah verfügbar, verlässlich und bezahlbar ist.

4 Angebotssituation

Aus den elf erfolgten Gesprächen konnten umfangreiche Erkenntnisse über die aktuelle Angebotssituation (Stand April 2024) für IT-Fachberatung im Kontext geschlechtsspezifische Digitale Gewalt erhoben werden. Es wurde mit folgenden Anbieter*innen gesprochen:

Angebot	Stadt	Webseite
Frauenberatung Nürnberg	Nürnberg	https://www.frauenberatung-nuernberg.de/ueber_uns.html
Dornrose Weiden, Pilotprojekt InterAktion	Weiden	https://dornrose.de/infoecke/digitale-sexualisierte-gewalt/
bff, Bundesverband Frauenberatungsstellen und Frauennotrufe	Berlin	https://www.frauen-gegen-gewalt.de/de/ueber-uns/der-bundesverband/geschaeftsstelle/team.html
ETUJ /Ein Team	Berlin	https://ein-team.org
FHK, Frauenhauskoordinierung	Berlin	https://www.frauenhauskoordinierung.de/ueber-uns/geschaeftsstelle
BLKA, Bayrisches Landeskriminalamt	München	https://www.polizei.bayern.de/wir-ueber-uns/organisation/dienststellen/0901100000000.html
Koordinierungsstelle Digitale Gewalt, Frauen helfen Frauen	Heidelberg	https://www.fhf-heidelberg.de/de/digitale-gewalt/koordinierungsstelle-digitale-gewalt/
Frauennotruf Wien	Wien	https://www.wien.gv.at/menschen/frauen/beratung/frauennotruf/
HateAid	Berlin	https://hateaid.org
K105, Kommissariat für Verhaltensorientierte – & Technische Prävention & Opferschutz	München	https://www.polizei.bayern.de/schuetzen-und-vorbeugen/beratung/beauftragte-der-polizei-fuer-kriminalitaetsopfer/005006/index.html

Tabella 2: Angebotssituation Überblick

Die Erkenntnisse können in mehreren thematischen Clustern zur Beratung zusammengefasst werden, um die Ansätze zur Digitalen Gewalt zu beschreiben. Diese Cluster sind: (1) Welche Zielgruppen werden von den Initiativen adressiert, (2) welche Aspekte spielen im Kontext der Beratung eine Rolle, (3) was ist beim Einsatz von IT-Fachkräften zu beachten und (4) welche weiteren Herausforderungen gibt es.

Im Anschluss daran wird die bisherige Angebotssituation für IT-Fachberatung geschildert und Good Practice Beispiele vorgestellt.

4.1 Zielgruppe der Initiativen.

Die betrachteten Angebote richten sich zum einen direkt an Betroffene als Teil eines umfassenden Beratungsangebots und zum anderen an Berater*innen in Anlaufstellen für Opfer geschlechtsspezifischer Gewalt, um deren psycho-soziale Betreuung durch technische Beratung zu ergänzen.

Direkte und niedrigschwellige Beratung für Betroffene als Teil eines Beratungsangebots bieten beispielsweise die Frauenberatung Nürnberg, der Frauennotruf Wien oder das Bayerische Landeskriminalamt. Eine Unterstützung für Berater*innen in Frauenhäusern, Beratungsstellen und Frauennotrufen stellen beispielsweise FHK, bff oder Ein Team bereit.

Angebote wie HateAid wenden sich sowohl direkt an Betroffene, bieten aber auch Angebote für Berater*innen an.

4.2 Relevante Aspekte während der Beratung.

Bei den betrachteten Angeboten steht im Fokus, eine besonders niedrigschwellige Beratung für die Betroffenen anzubieten, da diese meist wenig IT-Kenntnisse mitbringen. Viele Betroffene sind laut Aussagen der Interviewpartner*innen über das Ausmaß an Digitaler Gewalt überwältigt, wenn sie z.B. AirTags in Haarbürsten finden, die Kinder mit Spyware-ausgestattete Geräte von Ex-Partner*innen als Geschenk erhalten haben oder Chat-Verläufe veröffentlicht worden sind. In dieser Situation ist es besonders wichtig, die Betroffenen über die Maßnahmen zu einer juristisch verwertbaren Beweissicherung aufzuklären, sowie Haftungsthemen für die Berater*innen zu klären. Sobald ein Gerät durch eine dritte Person z.B. von Spyware gereinigt worden ist, können die vorab gesicherten Daten als Beweismittel vor Gericht nicht mehr zulässig sein. Viele Anbieter*innen haben daher begleitend juristische Beratung mit Zivil- und Strafrechtexpertise engagiert. Alle Anbieter*innen haben allerdings darauf hingewiesen, dass es weder für die Betroffenen noch für die Berater*innen bislang ausreichend klare juristische Absicherung gibt.

Es gibt eine Dunkelziffer bezüglich der Betroffenen, die zwar Digitale Gewalt erfahren, diese aber weder den Eltern, den Beratungsstellen noch der Polizei melden. Für die Polizei ist es überdies sehr schwierig, Digitale Gewalt-Fälle zu erfassen, da sie laut Aussagen der Interviewpartner*innen kaum über Kapazitäten oder Fachkräfte für eine Beratung zum Thema Digitale Gewalt verfügen. Beratungsstellen verweisen nach unseren Erkenntnissen die Betroffenen nach einem Gespräch daher nicht an die Polizei, sondern an Anwalt*innen für juristische Unterstützung.

4.3 Relevante Faktoren beim Einsatz von IT-Fachkräften.

Der Einsatz von zusätzlichen IT-Fachkräften in der Beratung war bei allen Anbieter*innen erfolgreich. Sie waren entweder Teil der Beratung gemeinsam mit erfahrenen psycho-sozial Berater*innen oder im Hintergrund aktiv, d.h. ihnen wurden die kontaminierten Geräte vorgelegt.

In der Wahrnehmung der Betroffenen sind IT-Fachkräfte zwar eine willkommene fachliche Autorität, allerdings gibt es auch Betroffene, die keine Beratung von einem Mann wünschen. Das Skillprofil dieser IT-Fachkräfte sollte nach unseren Erkenntnissen Empathie für die Betroffenen, Grundwissen zu geschlechtsspezifischer Gewalt und Kenntnisse zur Auswertung von Metadaten aus öffentlichen Bildern enthalten. Zusätzlich sind Kenntnisse aus der IT-Forensik und IT-Sicherheit von Vorteil. Diese Personen werden oft als Ehrenamtliche über eine Aufwandsentschädigung oder auf Honorarbasis engagiert. Dabei sind Haftungsfragen nach wie vor ungeklärt. Zudem ist eine nachhaltige Finanzierung und Verfügbarkeit einer IT-Fachkraft zwar nach Aussage der Anbieter*innen wünschenswert, aber oft aufgrund von Fachkräftemangel nicht realisierbar.

4.4 Weitere Herausforderungen

Zusammenfassend sehen sich die Angebote zu Digitaler Gewalt sowohl bundesweit als auch regional vor einer Vielzahl von Herausforderungen, während der Bedarf an Beratung zu Fragen Digitaler Gewalt steigt. Wie bereits in den vorausgehenden Abschnitten beschrieben, sind fehlende IT-Fachkräfte und Expertise für die Unterstützung von Berater*innen eine große Herausforderung. Die Finanzierung eines Angebots zur IT-Fachberatung sowie die rechtlichen Rahmenbedingungen bei der Bearbeitung von Fällen Digitaler Gewalt sind bis heute nicht abschließend gelöst. Darüber hinaus formulieren die Interviewpartner*innen den Wunsch nach Enttabuisierung des Themas in der Gesellschaft, d.h. die Opfer werden oft mit dem Vorwurf konfrontiert, selbst an der Digitalen Gewalt „schuld zu sein“ und Eltern sowie Fachkräfte können nicht nachvollziehen, warum Betroffene immer wieder Bilder schicken. Oft sind sich laut Aussagen der Interviewpartner*innen die Betroffenen gar nicht der Digitalen Gewalt bewusst, weil es Teil ihrer Lebensrealität geworden ist.

4.5 Bedarf nach IT-Fachberatung kann aktuell nicht gedeckt werden

Die vorgestellten Anbieter*innen und die Vorabanalysen der Gleichstellungsstelle für Frauen der LHM (GST) haben mehrfach bestätigt, dass es einen zunehmenden Bedarf an Unterstützung für die Beratungsstellen zu geschlechtsspezifischer Gewalt zum Thema Digitaler Gewalt gibt. Pilotprojekte und erste Initiativen haben sich als sehr erfolgreich herausgestellt, stehen aber auch vor Problemen, geeignete IT-Fachkräfte zu finden, den rechtlichen Rahmen für die Beratung abzusichern sowie eine Finanzierung des Angebots sicherzustellen. Aus diesem Grund mussten bereits Pilotprojekte wie beispielsweise Interaktion in Weiden, eingestellt werden.

Ein weiteres Problem ist, dass es in Deutschland zwar Statistiken zur Nutzung von Beratung von Frauennotrufen gibt, aber noch keine durchgängige Statistik über die Häufigkeit von Digitaler Gewalt existiert, auch wenn die Fälle kontinuierlich deutschlandweit zunehmen. Viele Beratungsstellen schildern insbesondere, dass der Übergang von physischer Gewalt zu Digitaler Gewalt fließend ist und dies die Erstellung einer Statistik zu Digitaler Gewalt zusätzlich erschwert.

Der schnelle technologische Fortschritt ist eine weitere Herausforderung, mit dem Anbieter*innen technischer Hilfestellung mithalten müssen, um eine adäquate Beratung für die Betroffenen gewährleisten zu können. Parallel zum technischen Fortschritt entwickeln sich Formen und Methoden Digitaler Gewalt weiter. Dies bedeutet erheblichen Aufwand für Beratende, um die eigenen Kenntnisse jederzeit aktuell zu halten – zeitlicher Aufwand, der in Konkurrenz mit dem Zeitbudget für die eigentliche Beratung steht. Anlaufstellen, an die sich Betroffene geschlechtsspezifischer Digitaler Gewalt mit ihren Geräten wenden können, gibt es bisher nicht flächendeckend. Die betrachteten Modellprojekte in Weiden und Nürnberg waren nur für eine begrenzte Zeit vollumfänglich lokal zugänglich.

Demgegenüber steht der Bedarf nach einer sehr schnellen und kurzfristigen Unterstützung für die Betroffenen, wenn der Verdacht auf Cyberstalking entstanden ist. Betroffene können nach Aussagen der Interviewpartner*innen nicht wochenlang auf einen Termin warten, um Unterstützung zu erfahren, da die Auswirkung von Digitaler Gewalt meist eine akute Bedrohungslage bedeutet.

Neben konkreter technischer Beratung setzen die interviewten Anbieter*innen auf Multiplikator*innen, d.h. Aufklärung zu Möglichkeiten der Prävention gegenüber Digitaler Gewalt und regelmäßiger Ausbildung der (psycho-sozial) Beratenden. Für die technische Qualifizierung zur Prävention und Maßnahmen gegen Digitale Gewalt wird in den Interviews immer wieder auf das Angebot von Ein Team, verwiesen – offenbar gibt es keine oder kaum weitere vergleichbare Angebote. Für eine Kooperation mit Ein Team ist aktuell eine Vorlaufzeit von sechs Monaten einzuplanen.

Alle Angebote haben im Rahmen eines Unterstützungssystems oder als gemeinnützige Einrichtung, den Fokus auf geringe Kosten. So werden IT-Fachkräfte ehrenamtlich engagiert und neben der finanziellen Unterstützung aus der Stadt, werden zusätzliche Einnahmequellen wie bspw. Stiftungen genutzt. Diese sind allerdings oft nicht verlässlich einzuplanen oder decken nur einen Teil der entstandenen Kosten ab, da IT-Fachkräfte bei nicht ehrenamtlicher Arbeit z.B. auf Stundenbasis, ein marktübliches Honorar anfragen.

4.6 Hilfreiche Ansätze für zukünftige Konzepte für ein Unterstützungsangebot (Good Practices)

Die Gespräche mit den Anbieter*innen haben nicht nur die Herausforderungen aufgezeigt, sondern auch hilfreiche Ansätze, die Teil zukünftiger Konzepte für das Unterstützungsangebot sein sollten.

(1) Beratung UND Prävention

Es empfiehlt sich, ein Angebot anzubieten, dass nicht nur im Fall Digitaler Gewalt unmittelbar unterstützt, sondern auch in Bildungseinrichtungen, bei Lehrer*innen, in Frauenhäusern und Beratungsstellen für dieses Thema sensibilisiert. Eine Grundausbildung für Beratende zum Thema Digitaler Gewalt, um in der Erstberatung direkt unterstützen zu können, erwies sich ebenfalls als hilfreich. Multiplikator*innen zu qualifizieren, ist ein Prinzip, dass das Angebot von Ein Team verfolgt und v.a. in der Koordinierungsstelle für Digitale Gewalt in Heidelberg sowie vom Frauennotruf in Wien und bff erfolgreich eingesetzt worden ist.

(2) Selbsthilfe-Angebote

Um die Reichweite ihrer technischen Beratung zu vergrößern, haben viele Angebote und Initiativen aufbereitete Selbsthilfe-Angebote, d.h. öffentlich zugängliche Informationen, die sich an Betroffene, aber auch an Berater*innen richten. Die Stadt Wien hat auf ihrer Webseite eine öffentliche Checkliste, um auf Formen und Risiken Digitaler Gewalt aufmerksam zu machen und über mögliche erste präventive Schritte aufzuklären. Sie hat aber auch eine interne Checkliste entwickelt, die im Erstgespräch bei der Fallanalyse unterstützt, d.h. im 1st Level Support, und erste Maßnahmen aufzeigt. Einen ähnlichen Ansatz verfolgt auch die Koordinierungsstelle für Digitale Gewalt in der Stadt Heidelberg, die eine Webseite mit Tipps veröffentlicht hat, aber auch einen geschlossenen Zugang für alle Frauenhäuser und Beratungsstellen in Baden-Württemberg anbietet. Es ist wichtig zu betonen, dass gezielte Tipps zur Behebung von Digitaler Gewalt nicht veröffentlicht werden sollten, da diese von potenziellen Täter*innen genutzt werden könnten.

Das bundesweit erreichbare Angebot von HateAid sendet auf Anfrage eine automatische E-Mail mit Tipps zur Beweissicherung von Bildern und Chat-Verläufen sowie juristischer Unterstützung durch den Weißen Ring.

(3) Kaskadieren der Anfragen und ein nachgeschalteter Level 2-Support

Die Erfahrungen der Stadt Wien legen nahe, die technische Beratung in zwei Leveln zu strukturieren. Zunächst werden alle Anfragen mit technischem Bezug gesammelt und sortiert. Der Frauennotruf Wien unterstützt die Betroffenen dabei, einzuordnen, welche Unterstützungsangebote als nächstes für ihren Fall kontaktiert werden sollten oder ergreift erste Maßnahmen (1st Level), den Betroffenen direkt auf dem Gerät zu helfen. So kann einem Großteil der Betroffenen bereits schnell und niedrigschwellig geholfen werden.

Detaillierte IT-Expertise wird dann in einem zweiten Schritt, d.h. wenn die Berater*innen vom Frauennotruf nicht mehr weiterkommen, auf Einzelfallbasis, angefragt. Diese wird in der Stadt Wien durch IT-Sicherheitsexpert*innen angeboten (Level 2-Support). Das hat den Vorteil, dass die Belastung der Anfragen an die IT-Fachkräfte nicht so hoch ist und dadurch die Aufwände geringer ausfallen.

Weitere Initiativen zum Thema Digitale Gewalt finden sich im Anhang.

5 Konzept für IT-Fachberatung in Fällen geschlechtsspezifischer Digitaler Gewalt

Um geschlechtsspezifischer Digitaler Gewalt zu begegnen, braucht es ein umfassendes und niedrigschwelliges Lösungskonzept.

Das vorgeschlagene Lösungskonzept besteht aus den in Abbildung 3 dargestellten Bausteinen. Grundsätzlich ist das gesamte Angebot für Anlaufstellen, also Berater*innen, gedacht. Es unterstützt die Einrichtungen Münchens dabei, Prävention gegen Digitale Gewalt gegenüber Betroffenen anzubieten und selbst 'technische' erste Hilfe zu leisten. Reichen die Informationen zur Selbsthilfe nicht aus, wenden sich die Anlaufstellen an die technische Hilfe der IT-Fachberatung.

IT-Fachberatung

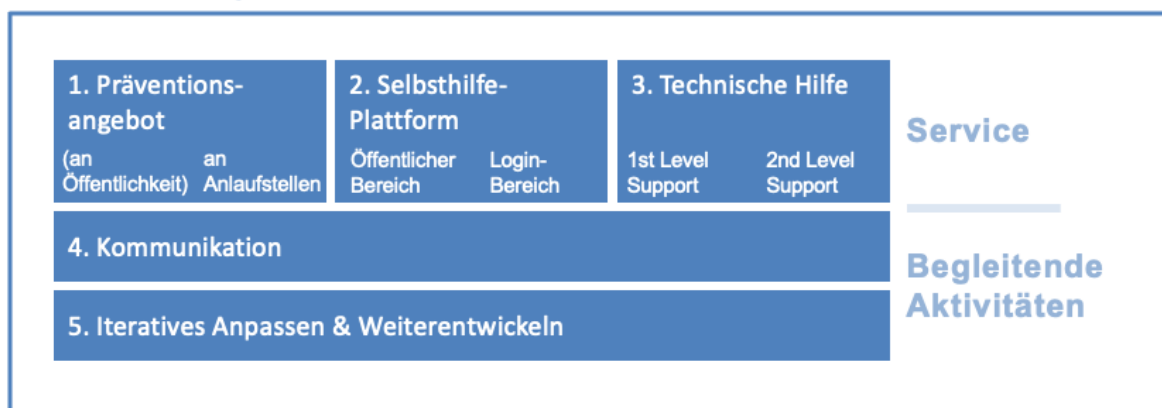


Abbildung 3: Bausteine des Konzepts zur IT-Fachberatung

Im Folgenden werden die Bausteine im Einzelnen vorgestellt. Für jeden Baustein ist eine Minimal-Version vorgesehen, die unbedingt erforderliche Servicebestandteile realisiert und in den ersten Jahren erprobt wird. Weitere wünschenswerte Komponenten werden in Ausbaustufen beschrieben und sollen umgesetzt werden, wenn der Bedarf in der Praxis bestätigt wird und das Konzept sich bewährt hat.

5.1 Präventionsangebot

5.1.1 Minimalversion

Anlaufstellen für Opfer geschlechtsspezifischer Gewalt in München sowie entsprechende interne Stellen (Zentrale Beschwerdestelle nach dem AGG, für sexuelle Belästigung, häusliche Gewalt und Mobbing (ZAGG), FgR = Fachstelle für Demokratie, GsT = Gleichstellungsstelle, Koordinierungsstelle für LGBTIQ*; ZSPD = zentraler schulspsychologischer Dienst) sollen dabei unterstützt werden, Digitaler Gewalt vorzubeugen. Zur Sensibilisierung für Risiken und zur Vermittlung von Basiswissen zu Maßnahmen gegen Digitale Gewalt werden Vorträge konzipiert, die entweder online oder vor Ort in regelmäßigen Abständen stattfinden sollen. Inhaltlich sollen die Vorträge sich um lebensnahe Szenarien wie digitale Trennung und grundlegende Sicherheitsmaßnahmen wie das Geheimhalten von Passwörtern, sicheres Browsen und bewusste Smartphone-Einstellungen gehen. Anschauliche Fallbeispiele Betroffener sollen den Beratenden in den Anlaufstellen die Bedeutung dieser Sicherheitsmaßnahmen verdeutlichen. Sinnvoll ist es auch, ihnen die Rechte der Betroffenen vor Augen zu führen und aufzuzeigen, was diese tun können, sollte ihnen Digitale Gewalt widerfahren.

5.1.2 Ausbaustufe

Hat sich das Kernkonzept bewährt, kann die Sensibilisierung für Digitale Gewalt und Handlungsmöglichkeiten auch gegenüber Multiplikator*innen wie Erziehungsberechtigten, Lehrer*innen, Schulpsycholog*innen etc. erfolgen. Vorstellbar ist außerdem, dass bestehende Angebote wie bspw. die [Digitale Hilfe](#) des Medienzentrums München oder die [Frauencomputerschule](#) um Module gegen Digitale Gewalt ausgebaut werden.

Teilnehmer*innen sollen nicht nur Informationen erhalten, sondern auch praxisnah an Geräten üben können. Wichtig ist auch, über aktuelle technologische Entwicklungen informiert zu bleiben und sie in die Schutzkonzepte einzubeziehen.

5.2 Selbsthilfeplattform

5.2.1 Minimalversion

Die Ausprägungen Digitaler Gewalt sind vielfältig und ebenso zahlreich sind Anleitungen, was man vorbeugend oder bei einem konkreten Vorfall tun kann bzw. sollte. Gleichzeitig sollen allzu detaillierte Informationen vermieden werden, um Täter*innen von der Nachahmung abzuhalten.

Die Selbsthilfeplattform soll daher neben einem öffentlichen Bereich mit allgemeinen Informationen auch einen Login-Bereich mit weiterführenden Inhalten haben. So haben Anlaufstellen und künftig potenziell auch weitere Gruppen die Möglichkeit, nach einer initialen Einführung, sich in einer umfassenden, gut sortierten Informationssammlung weiter zu informieren. Die Plattform soll neben Abklärungsfragen für den Einstieg in Beratungsgespräche eine allgemeine Herangehensweise zur Risikoabschätzung und für Erstmaßnahmen bieten, aber auch detaillierte Anleitungen bereithalten. So sollen sowohl Neulinge als auch Expert*innen an ihrem Wissensstand abgeholt werden. Ebenso soll die Plattform auf spezialisierte Anlaufstellen wie HateAid oder den Weißen Ring verweisen.

5.2.2 Ausbaustufe

Perspektivisch ist es vorstellbar, die Plattform weiteren Multiplikator*innen wie Sozialarbeiter*innen und Schulpsycholog*innen oder auch Betroffenen zugänglich zu machen. Ein smartes Beratungstool würde die Einarbeitungszeit verkürzen und mehr Berater*innen befähigen, Betroffenen zu helfen. Auch digitale Austauschräume, über die Betroffene sich gegenseitig unterstützen können, würden allen Beteiligten langfristig viel Arbeit abnehmen und mehr Menschen helfen können.

5.3 Technische Hilfe

5.3.1 1st Level-Support

Unter einem 1st Level Support stellen wir uns eine Gruppe von IT-Generalist*innen vor. Anlaufstellen können sich bei grundlegenden Fragen dort hinwenden. Der 1st Level Support bietet alle Informationsleistungen, hilft bei der Beweissicherung und kann gemeinsam mit den Betroffenen Standard-Sicherheitseinstellungen an Geräten vornehmen.

5.3.2 2nd Level-Support

Der 2nd Level Support wird vom 1st Level Support bei Bedarf hinzugezogen. Bei dem 2nd Level Support handelt es sich um IT-Spezialist*innen aus dem Fachbereich Cybersecurity und IT-Forensik. Sie sind in der Lage, komplexe Analysen durchzuführen. Allerdings sind diese Expert*innen auf dem Arbeitsmarkt nur schwer zu finden, weshalb der 1st Level Support möglichst viel abdecken sollte.

5.4 Kommunikation

5.4.1 Minimalversion

Um für unterschiedliche Aspekte geschlechtsspezifischer Digitaler Gewalt zu sensibilisieren, wird von der Gleichstellungsstelle für Frauen in Kooperation mit dem Sozialreferat und dem Referat für Bildung

und Sport die Kampagne „Gleichberechtigung schützt vor Gewalt“ um Aspekte Digitaler Gewalt erweitert und zielgruppenorientiert über die soziale Infrastruktur der Stadt (Sozialbürgerhäuser, Jugendeinrichtungen, Schulen) angeboten.

5.4.2 Aufbaustufe

Zusätzlich zur zielgruppenorientierten Ansprache werden die entwickelten Maßnahmen mit einer breit angelegten Öffentlichkeitskampagne im öffentlichen Raum beworben, die für die unterschiedlichen Aspekte geschlechtsspezifischer Digitaler Gewalt sensibilisiert, niedrigschwelligen Zugang zu präventiven Maßnahmen und Selbsthilfemöglichkeiten eröffnet und die bestehenden Fachberatungen und Anlaufstellen bekannt macht.

5.5 Bereitstellen & Weiterentwickeln

Auch wenn einige Good Practice Beispiele aus anderen Städten ähnliche Konzepte wie das oben beschriebene umgesetzt haben, ist die Situation in den verschiedenen Städten nur bedingt mit München vergleichbar. Daher soll eine Testphase die Praxistauglichkeit des Konzeptes als Hilfestellung für die Anlaufstellen geschlechtsspezifischer Gewalt in München sicherstellen.

Die Testphase soll u.a. folgende Fragen beantworten:

- Wie viele Fälle geschlechtsspezifischer Digitaler Gewalt sind durch die IT-Fachberatung zu bearbeiten (1st und 2nd Level) und welche Gewaltformen sind besonders relevant?
- Wie viel Zeit braucht der Support, um einen Fall zu bearbeiten?
- In welchen Fällen reicht der 1st Level Support aus und ab wann braucht man einen 2nd Level Support?

Während der Testphase werden Statistiken und Feedback seitens einer User Group ausgewählter Beratungsstellen gesammelt. Ziel ist es zu verstehen, wie gut die Maßnahmen den Bedarf treffen und wo nachjustiert werden muss.

Zeitgleich informiert sich der 1st Level Support kontinuierlich zu aktuellen Gewaltformen und technischen Möglichkeiten weiter. Dadurch versetzt er sich in die Lage, die Beratungsstellen proaktiv fortzubilden. So soll die Landeshauptstadt München auch neuen Entwicklungen begegnen können.

Bei der späteren Umsetzung des Konzeptes zur IT-Fachbereitschaft nach der Testphase stellt sich die Frage, in welchem Umfang die vorgesehenen Aufgaben und Services durch die LHM selbst oder durch Dritte erledigt und bereitgestellt werden sollen. Grundsätzlich kann diese Entscheidung bei jedem der in vorangehenden Abschnitt vorgestellten Elemente gesondert getroffen werden. Zwischen den beiden Extremvarianten,

1. die LHM stellt alle Elemente der IT-Fachberatung selbst bereit und
2. die LHM beauftragt Dritte für die Bereitstellung aller Elemente der IT-Fachberatung

sind zahlreiche Varianten denkbar.

Bei der Bewertung der Vor- und Nachteile einer Eigenerstellung eines Teilbereichs oder des gesamten Hilfeframeworks sind verschiedene Faktoren zu berücksichtigen:

- In welchem Umfang können Vorarbeiten und Erfahrungen, die in der LHM vorhanden sind, genutzt werden?
- Welche Aufwände (Sachmittel, Personalmittel) sind initial und dauerhaft mit den möglichen Varianten verbunden?
- In welchem Umfang können die Varianten an sich verändernde Bedarfe angepasst werden?

- In welchem Umfang werden die verschiedenen Varianten den Anforderungen der Anlaufstellen nach verlässlicher technischer Unterstützung gerecht?

Zum aktuellen Zeitpunkt können diese Fragen noch nicht belastbar beantwortet werden. Im Rahmen eines Testlaufs müssen die praktischen Anforderungen der Anlaufstellen noch konkreter ermittelt werden. Diese konkretisieren sich erst in der Zusammenarbeit bei der Nutzung des 1st und 2nd Level Supports sowie der weiteren Teile des Konzepts. Zudem ist aktuell der quantitative Umfang des Bedarfs nach technischer Unterstützung bei den Anlaufstellen nicht genau bezifferbar.

Aus den ersten Erfahrungen mit der Bereitstellung des technischen Hilfekonzepts können Ableitungen für die Bewertung verschiedener Optionen für die Bereitstellung getroffen werden. Außerdem kann während des Probetriebs ermittelt werden, welche Akteur*innen für Kooperationen, als Dienstleister*innen sowie als Fördernehmer*innen in Betracht gezogen werden können. Auch eine potenzielle organisatorische Verankerung in der LHM kann während dieser Zeit genauer eruiert werden.

6 Ausblick

Nach den bisherigen Recherchen und Gesprächen mit Expert*innen kann der Bedarf nach einer IT-Fachberatung für Fälle geschlechtsspezifischer und antifeministischer Digitaler Gewalt qualitativ umrissen werden. Basierend auf diesen Erkenntnissen haben wir das dargestellte Konzept für eine solche Dienstleistung erarbeitet.

Aktuell kann allerdings nicht genau beziffert werden, in welchem Umfang diese Dienstleistung erforderlich sein wird und wie gut das beschriebene Konzept den realen Bedarf decken kann. Außerdem kann ohne praktische Erfahrungen auch nicht beurteilt werden, in welcher organisatorischen Konstellation die dargestellte Dienstleistung idealerweise erbracht wird bzw. welche Kooperationen möglich und sinnvoll sind.

Um diese Fragen zu beantworten ist eine Testphase von etwa 2 Jahren vorgesehen. Zunächst ist geplant, das skizzierte Konzept in einer Minimalversion zu testen und später nach Möglichkeit bedarfsorientiert auszubauen.

7 Literaturverzeichnis

BKA. (2024). Von

https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/240607_BLB_Haesliche_Gewalt.html abgerufen

Bundesverband Frauenberatungsstellen und Frauennotrufe (bff). (o.J.).

Frauen gegen Gewalt e.V. (o.J.). Was tun gegen geschlechtsspezifische Gewalt? Kooperation zwischen Fachberatung und IT als Lösungsansatz.

HateAid. (o.J.). Von <https://hateaid.org/digitale-gewalt/> abgerufen

Hochschule Wien. (2022). *(K)ein Raum. Cyber-Gewalt gegen Frauen in* . https://www.fh-campuswien.ac.at/fileadmin/redakteure/Forschung/Projekte/Dolumente/Forschungsbericht_K_ein_Raum_final.pdf.

Initiative D21. (o.J.). *Gender Gap Studie*. Von <https://initiated21.de/publikationen/digital-gender-gap> abgerufen

Pew Research Center. (2017).

8 Anhang

Weitere Initiativen zum Thema Digitale Gewalt:

- Organisationen die digital Hilfe und/oder rechtliche Unterstützung anbieten:
 - Hateaid: <https://hateaid.org/>
 - Juuuport: www.juuuport.de: [Online-Beratung bei Cybermobbing und anderen Problemen](#)
 - hatefree: <https://hatefree.de/>
 - NummergegenKummer: <https://www.nummergegenkummer.de/>
 - Weißer Ring <https://weisser-ring.de>
 - Dickstinction: Meldestelle für DickPics <https://dickstinction.com/>
- Organisationen, die die Digitalkompetenz der Menschen fördern wollen:
 - Die EU-Initiative klicksafe: <https://www.klicksafe.de/die-initiative>
- Vermittlungsstellen von Beratungen zu Hass im Netz:
 - Zivile Helden: [Beratungsstellen helfen auch bei Hassrede im Internet \(zivile-helden.de\)](#)
 - Informations- und Beratungsstelle zu bildbasierter sexualisierter Gewalt, ehrenamtlich arbeitende Betroffenenelbsthilfe-Organisation Anna Nackt: <https://annanackt.com/>
- Auch regional gibt es einige Anlaufstellen, z.B.:

- Anti-Stalking-Projekt in Berlin mit fester IT-Beraterin im Team:
<https://www.anti-stalking-projekt.de/>
- Solinet: Beratungsstelle in Koblenz gegen Hass und Gewalt im Netz, mit Schwerpunkt auf rassistischer und antisemitischer Gewalt: <https://www.solinet-rlp.de/>
- Kompetenzstelle gegen Cyber-Gewalt an Frauen in Wien:
IT-Sicherheitsexpert*innen des WienCERT von Wien Digital arbeiten mit dem 24-Stunden Frauennotruf und dem Verein Wiener Frauenhäuser in konkreten Fällen von Cyber-Gewalt eng zusammen: <https://wien.gv.at>