Cyberstalking entgegentreten

- aktuelle Herausforderung in der Beratung für Frauen*.

Möglichkeiten, Handlungsbedarfe und Forderungen

Dokumentation des gleichnamigen Fachtags
vom 24. Mai 2016 in Berlin

AntiStalking PROJEKT
Information • Unterstützung • Beratung

Frieda
frauenzentrum e.V.

Inhaltsverzeichnis

Impressum

Herausgabe:	Anti-Stalking-Projekt, FRIEDA-Frauenzentrum e. V.
Redaktion und Lektorat:	Therese Gerstenlauer, Beate M. Köhler, Friederike Augat
Grafikdesign:	Juliane Brandt
Graphic Recording (S. 15-27, 56):	Julia Both, 123comics
Jahr/Ort:	2016, Berlin

Die vorliegende digitale Dokumentation ist eine leicht ergänzte Version der Printpublikation.

Der Fachtag und die Dokumentation werden gefördert von der Senatsverwaltung Arbeit, Integration und Frauen – Geschäftsstelle Gleichstellung.

Senatsverwaltung für Arbeit, Integration und Frauen

be Berlin

Programm Fachtag Cyberstalking entgegentreten

12.00 Uhr	**Ankommen**
12.30 Uhr	**Begrüßung** Therese Gerstenlauer Geschäftsleitung, FRIEDA-Frauenzentrum e. V. **Grußwort** Anja Kofbinger MdA, Bündnis 90/Die Grünen, Sprecherin für Frauen- und Queerpolitik
12.45 Uhr	**Was tun gegen Cyberstalking? Möglichkeiten und Bedarfe von Fachberatungsstellen** Silvia Zenzen Referentin für Kommunikation und Information, Bundesverband Frauenberatungsstellen und Frauennotrufe (bff)
13.15 Uhr	**Aktuelle Herausforderung in der Anti-Stalking-Beratung – ein Beratungsgespräch bei Cyberstalking** Beate M. Köhler Projektkoordinatorin, Anti-Stalking-Projekt Saskia Benter Schauspielerin
13.45 Uhr	Diskussion in Kleingruppen
14.15 Uhr	Pause
14.45 Uhr	Diskussion im Plenum
15.15 Uhr	**Effektives rechtliches Vorgehen gegen Cyberstalking anhand unterschiedlicher Begehungsformen** Julia Wortmann Rechtsanwältin, u. a. für strafrechtliche und sozialrechtliche Opfervertretung
15.45 Uhr	**Sicher im Web unterwegs: Strategie und Technik kennen und in Beratungssituationen vermitteln** Vera Kätsch EDV- und IT-Beraterin, Durchblick GmbH
16.30 Uhr	Diskussion
17.00 Uhr	Ausklang

Einleitung

Therese Gerstenlauer
Geschäftsleitung, FRIEDA-Frauenzentrum e. V.

Cyberstalking als eine Gewaltform, die mit digitalen Hilfsmitteln ausgeübt wird und von der zu über 80 Prozent Frauen betroffen sind, nimmt seit den letzten Jahren stark zu. Mittlerweile spielt Cyberstalking bei fast jeder Nachstellung eine Rolle. Durch das Hinzukommen des Internets und neuer Kommunikationsmedien wird der Raum, in dem das Stalking wirkt, größer. Die Nachstellung wird permanenter und zugleich oftmals weniger fassbar. Der Täter kann schneller, massenhafter, zu jedem Zeitpunkt, mit einer größeren Reichweite und Beständigkeit, zugleich selbst anonym tätig sein und in den privaten Raum und an private Daten der Betroffenen kommen. Hinzu kommt, dass durch das dabei entstehende Misstrauen oder die Angst im Umgang mit Informations- und Kommunikationsmitteln sowie durch deren Missbrauch, den betroffenen Frauen* eine wichtige Möglichkeit genommen wird, selbstbestimmt an einem gesellschaftlichen Leben teilzuhaben, das mittlerweile stark durch diese Informations- und Kommunikationsmittel geprägt ist. Eine Folge davon ist, dass viele betroffene Frauen* zunehmend isoliert sind.

In der öffentlichen Wahrnehmung aber und auch in fachlichen Handreichungen wird – wenn überhaupt – nur sehr allgemein Cybergewalt behandelt. Um spezielle Formen von Cybergewalt, wie Cyberstalking, geht es selten und wenn, dann kaum mit einer geschlechtssensiblen Perspektive, was jedoch angesichts der hohen Betroffenheit von Frauen* wichtig wäre. Eine gewisse Ausnahme stellt die Auseinandersetzung mit Cybermobbing dar. Dabei wird eine spezielle digitale Gewaltform betrachtet und durch die Ausrichtung auf Jugendliche ein zielgruppenspezifischer Fokus gelegt. Aber auch hierbei fehlt – mit wenigen Ausnahmen – der Blick auf weitere bereits in der Gesellschaft wirkende Diskriminierungsmechanismen, die sich auf digitale Gewaltformen übertragen können. Rassismus, Klassizismus, Ableismus und Trans- und Homophobie spielen auch hier eine wichtige Rolle. Dementsprechend differenzierende und belastbare Erhebungen zu Cybergewalt gibt es nicht.

In der breiten Öffentlichkeit, bei politisch Verantwortlichen, Betroffenen von Cybergewalt und Personen, die privat oder beruflich Betroffene unterstützen und beraten, fehlt oftmals das Wissen um Formen und Auswirkungen von digitaler Gewalt. Um Cybergewalt aber entgegentreten zu können, wird Wissen um Möglichkeiten, sich vor dieser Gewalt zu schützen und dagegen zur Wehr zu setzen, benötigt.

Dieses fehlende öffentliche Bewusstsein und die Unkenntnis von Gegenmaßnahmen führen zu einer Stärkung der Täter bei der Ausübung von Cybergewalt. Bezogen auf Cyberstalking kann es sein, dass Täter mit Einschüchterungen, Herabwürdigungen der Betroffenen sowie

> Mit Frauen* sind alle gemeint, die Diskriminierungsformen ausgesetzt sind, weil sie der Kategorie Frau zugeordnet werden oder sich selbst zuordnen. Dazu gehören Menschen, die eine weibliche Sozialisation erfahren haben, von außen als Frauen wahrgenommen werden und so definiert werden. Auch sprechen wir von Frauen, die sich selbst der Kategorie Frau zuordnen, unabhängig davon, ob das Umfeld diese Zuordnung akzeptiert oder nicht. Women* of color, Lesben, Frauen* mit Behinderung, arme Frauen*, Transfrauen sind zudem mit Mehrfachdiskriminierungen konfrontiert.

einer Infragestellung ihrer Urteilsfähigkeit eine Isolierung der betroffenen Frauen* provozieren. Einerseits, weil Betroffene gegenüber ihrem sozialen Umfeld immer misstrauischer werden, andererseits, weil das soziale Umfeld die Betroffenen als immer weniger sozial empfindet. Unter anderem auch, weil sich diese Frauen* oftmals nicht mehr über moderne Kommunikationsmittel verständigen wollen.

Fehlt im sozialen Umfeld die Sensibilität bezogen auf die Problemlage sowie das Wissen um einen Umgang damit, so werden betroffene Frauen* bald alleine gelassen. Es kann sein, dass eine der wenigen Personen, die dann noch mit der Betroffenen im kontinuierlichen Kontakt steht oder „für" die Betroffene nach außen in Kontakt geht, der Stalker ist. Der Raum, den dieser dann einnimmt, kann enorm sein.

Dem entgegenzutreten, hat sich das Anti-Stalking-Projekt in Trägerschaft des FRIEDA-Frauenzentrum e. V. zur Aufgabe gemacht. Das Anti-Stalking-Projekt ist eine parteiliche Anlaufstelle für von Stalking und/oder Cyberstalking betroffene Frauen* sowie deren soziales Umfeld und Unterstützer*innen. Seit 2014 bietet das Anti-Stalking-Projekt Beratung, stabilisierende Begleitung, eine Selbsthilfegruppe, öffentliche Themenabende, Multiplikator*innenschulungen, Materialien und Öffentlichkeitsarbeit zu dieser Gewaltform an. Dabei wurde klar, dass für die Stärkung der Betroffenen verschiedene Unterstützungsmechanismen und -akteure zusammenwirken und sich koordinieren müssen. Gefragt sind in diesem Prozess Beratungsstellen, Hilfs–angebote für Frauen* gegen Gewalt, Anwält*innen, Prozessbegleiter*innen, Mediziner*innen und entsprechende Abteilungen der Polizei und der Gerichte. Aber auch die Schulung der Betroffenen im Umgang mit neuen Medien und Internetsicherheit sowie weitere Angebote zur Stabilisierung und Selbstermächtigung der Betroffenen – wie feministische Selbstbehauptung, Empowerment gegen diverse Diskriminierungsformen und Selbsthilfezusammenhänge – können auf einem solchen Weg unterstützend wirken.

Dies plastisch zu verdeutlichen und die verschiedenen Akteure in Berlin mit ihren jeweiligen Fachgebieten, Fragen und Anregungen zueinander und in Diskussion zu bringen, war Ziel des vom Anti-Stalking-Projekt des FRIEDA-Frauenzentrum e. V. veranstalteten Fachtags „Cyberstalking entgegentreten – aktuelle Herausforderung in der Beratung für Frauen*" am 24. Mai 2016 im Haus der Demokratie und Menschenrechte in Berlin.

> Selbstverständlich für uns ist dabei ein für die betroffenen Frauen* parteilicher Ansatz. Frauen*, die von Stalking betroffen sind, werden oftmals von ihrer Umgebung und der Gesellschaft nicht ernst genommen oder sie werden einseitig als Opfer gesehen, die dem Täter nichts entgegensetzen können und so in ein Ohnmachtsgefühl gedrängt. Umso wichtiger ist es, dass sie bei einer ersten Anlaufstelle ernst genommen und wertgeschätzt werden. Es ist für die Betroffenen von großer Hilfe, wenn ihre Situation in gesamtgesellschaftliche Verhältnisse eingeordnet wird. Die Berater*in muss deshalb einen gesellschaftspolitischen Standpunkt beziehen können und die vorliegende Situation mitsamt dem darin vorhandenen asymmetrischen Machtverhältnis zwischen dem sogenannten Täter und dem sogenannten Opfer auch in eine von weiblicher Sozialisation durchzogene Biographie und/oder das Großwerden in einer homo- und trans*phoben, einer Behinderungen verstärkenden und rassistischen Gesellschaft einordnen. Mit dieser grundlegenden Verortung der Situation kann zusammen mit den Frauen* nach Lösungsmöglichkeiten geschaut werden.

Über 90 Teilnehmende aus diversen Verantwortungsbereichen waren auf dem Fachtag vertreten. Zahlreiche Beratungsstellen, Anti-Gewalt-Projekte, soziokulturelle Frauenprojekte, Menschen aus der Opferhilfe und Zeugenbetreuung, Gleichstellungs- und Frauenbeauftragte aus den unterschiedlichen Bezirken sowie der Berliner Hochschulen, Mitarbeiter*innen von Wohnungsbaugenossenschaft, Jobcenter, Verantwortliche entsprechender Abteilungen der Polizei, interessierte Privatpersonen

sowie Vertreter*innen der Senatsverwaltung für Arbeit, Integration und Frauen und aus verschiedenen Bereichen der Berliner Justiz waren anwesend und beteiligten sich am Diskussionsprozess.

In einem Grußwort, mit vier Fachreferaten sowie in Kleingruppen und Pausendiskussionen wurden Ist-Zustände und Perspektiven aus diversen Handlungsbereichen gesammelt und diskutiert. Die Dokumentation des Fachtags soll nun eine breitere Öffentlichkeit erreichen und die auf dem Fachtag aufgeworfenen Fragen, vorhandenen Möglichkeiten und genannten Handlungsbedarfe festhalten. Damit wird weiterführenden Auseinandersetzungen eine Grundlage gegeben. Insbesondere eine auf dem Fachtag aufgeworfene Frage, greift die Broschüre auf: Wie schaffen wir es, dass Frauen*, die von Cyberstalking betroffen sind, auf ein gut organisiertes Unterstützungsnetzwerk stoßen, das sie in dem oftmals schwierigen und langen Prozess gegen Cyberstalking professionell und parteilich begleitet?

Aufbau der Broschüre

Wie auf dem Fachtag werden auch in der Broschüre verschiedene Komponenten bei der Bekämpfung von Cyberstalking in den Blick genommen. In einem Grußwort benennt Anja Kofbinger, Mitglied des Abgeordnetenhauses von Berlin (Bündnis 90/die Grünen), die politische Handlungsebene. Anschließend daran gibt Silvia Zenzen vom Bundesverband Frauenberatungsstellen und Frauennotrufe (bff) eine Einführung zu den verschiedenen Formen von Cybergewalt und den Überblick zur bundesweiten Situation der Frauenfachberatungsstellen und Frauennotrufe zum Thema. Beate M. Köhler gibt – auf dem Fachtag zusammen mit Saskia Benter umgesetzt – einen Einblick in die konkrete Beratungsarbeit anhand eines Falls von Cyberstalking. Grafisch wurde dies von Julia Both von 123comics in einem Comic festgehalten. Dieses ist in Ausschnitten im Beitrag von Beate M. Köhler und in Gänze auf Seite 27 abgebildet. Sie zeichnete außerdem das Zusammentragen der Kleingruppendiskussionen mit (siehe Seite 56). Rechtliche Aspekte und Reformempfehlungen werden von der Rechtsanwältin Julia Wortmann benannt. Abschließend benennt Vera Kätsch, EDV- und IT-Beraterin von Durchblick GmbH, wichtige Techniken und Strategien zur Internetsicherheit. Die auf dem Fachtag einleitend gestellten Fragen zur Selbsteinschätzung bezüglich der eigenen Internetsicherheit begleiten den Beitrag.

Alle Beiträge werden an den Rändern ergänzt von den Fragen, Interessen und Diskussionsbeiträgen der Teilnehmenden des Fachtags. Insgesamt entsteht so ein Bild zu Möglichkeiten und Herausforderungen in der Arbeit für von Cyberstalking Betroffene. Am Ende der Broschüre sind die im Fachtag zusammengetragenen Handlungsbedarfe zusammengefasst und sortiert. Sie laden zur weiteren Bearbeitung des Themas ein. Denn wir stehen noch am Anfang einer gesamtgesellschaftlichen und politische Debatte um konkrete Schutzmaßnahmen und rechtliche Möglichkeiten zur Stärkung von durch Cyberstalking betroffenen Menschen.

Grußwort

Anja Kofbinger
MdA Berlin, Bündnis 90/die Grünen

Liebe Frauen,

es ist gut, dass heute der Fachtag “Cyberstalking entgegentreten” veranstaltet vom Anti-Stalking-Projekt des FRIEDA-Frauenzentrum e. V. stattfindet. Endlich möchte man sagen. Es handelt sich um ein Thema, das leider sehr in unsere Zeit passt und das es ohne unsere moderne Kommunikationstechnik gar nicht gäbe. Dahinter verbirgt sich ein Tatbestand, der uns allen leider sehr bekannt ist. Gewalt gegen Frauen. Gewalt gegen Frauen und Mädchen ist weltweit die häufigste Menschenrechtsverletzung. Und schauen wir genauer hin, sehen wir, dass es sich bei Cyberstalking - ebenso wie bei Cybermobbing, Cybergrooming, oder Cybersexism – nur um eine zeitgemäße Variante von frauenspezifischer Gewalt handelt.

Lange wurde das Thema von der Politik kaum beachtet. Ich war daher sehr froh, als sich die Gleichstellungs- und Frauenminister*innenkonferenz (GMFK) vor zwei Jahren endlich damit befasst hat. Es wurden zwar verschiedene Umsetzungsbedarfe auf Bundes- und Landesebene benannt, aber leider stellte sich heraus, dass außer hehrer Worte und Absichtserklärungen nicht mehr viel passierte.

Ich habe deshalb beschlossen, das Thema ins Berliner Parlament zu tragen und das getan, was aus der Opposition heraus möglich ist: Ich habe einen Antrag geschrieben. In diesem Antrag fordern wir den Senat auf, die Beschlüsse der GMFK umzusetzen und sich aktiv gegen Cybergewalt einzusetzen. Zuvor hatte ich zahlreiche schriftliche Anfragen gestellt und auf Veranstaltungen Gespräche mit Expert*innen geführt. Auch eine UN-Studie hatte ich angeführt, die aufzeigt, dass Angriffe im Internet wahrgenommen werden wie physische Gewalt. Die dringende Notwendigkeit, vor allem auch Beratungsstellen für von Gewalt betroffene Frauen besser auszustatten, lag auf der Hand. Dennoch wurde dieser Antrag mit der Begründung, es würde bereits genug auf diesem Gebiet getan, zu Beginn dieses Jahres abgelehnt. Auch wenn ich mich in den anderen Bundesländern umsehe, muss ich leider feststellen, dass von den Forderungen der Frauenminister*innenkonferenz nicht viel umgesetzt wurde. In Nordrhein-Westfalen ist eine Fachstelle geplant, sonst ist außer Prüfaufträgen aber nicht viel dabei herausgekommen. Umso wichtiger ist es, dass wir das Thema weiterhin verfolgen und uns dafür einsetzen, dass es zukünftig weiter ins Zentrum der Aufmerksamkeit rückt.

Deshalb freue ich mich um so mehr, dass die Mitarbeiterinnen des FRIEDA-Frauenzentrum e. V. viel Mühe und Arbeit investiert haben, um heute diesen ersten deutschlandweiten Fachtag zum Thema Cyberstalking auf die Beine zu stellen. Ich wünsche uns allen gutes Gelingen dabei und hoffe, dass wir uns gut austauschen können und voneinander lernen können. Ein weiterer Wunsch von mir wäre, dass von diesem Fachtag und unserer Arbeit auch ein Signal ausgeht. Ein Signal, dass Gewalt im Internet endlich genau so konsequent und unnachsichtig verfolgt werden muss wie ihre anderen Erscheinungsformen.

Cybergewalt ist kein abstraktes Internet-Problem, sondern stellt die Fortsetzung von Gewalt im realen Raum mit digitalen Mitteln dar. Die Ursachen sind im realen Umfeld zu suchen. Gewalt im Netz ist eine Form frauenspezifischer Gewalt. Das ist leider in der öffentlichen Wahrnehmung wie in der Politik noch nicht ausreichend angekommen. Wenn uns das mit gemeinsamen Einsatz gelingt, sind wir schon einen großen Schritt weiter.

Was tun gegen Cyberstalking?

Möglichkeiten und Bedarfe von Fachberatungsstellen für weibliche Betroffene von Gewalt

Silvia Zenzen
Referentin für Kommunikation und Information des Bundesverbands Frauenberatungsstellen und Frauennotrufe (bff), Frauen gegen Gewalt e. V.

Einführung

Laut einer Studie der Grundrechteagentur der Europäischen Union sagen 85% aller Frauen, dass das Internet Ihnen eine größere persönliche Freiheit gibt. Gleichzeitig haben EU-weit aber 18% der über 15-jährigen Frauen schon einmal eine schwere Form digitaler Gewalt erlebt. EU-weit sind das 9 Millionen Frauen.[1]

Im Folgenden werden die unterschiedlichen Ausprägungen des Cyberstalking vorgestellt und ihre Auswirkungen auf die Betroffenen beleuchtet. Im Weiteren wird darauf eingegangen, welche Erfahrungen die Fachberatungsstellen in der Unterstützung der Betroffenen machen und welche Maßnahmen nötig sind, damit die Unterstützung bedarfsgerecht erfolgen kann.

[1] http://fra.europa.eu/de/publication/2014/gewalt-gegen-frauen-eine-eu-weite-erhebung-ergebnisse-auf-einen-blick, letzter Zugriff am 28.06.2016.

[2] An Frauenberatungsstellen und Frauennotrufe wenden sich Frauen und Mädchen, wenn sie sexuelle Nötigung, Vergewaltigung, Gewalt in der Partnerschaft, psychische Gewalt oder Stalking erleben. Seit Anfang Mai ist auch das FRIEDA-Frauenzentrum e. V. mit dem Anti-Stalking-Projekt Mitglied im bff.

[3] Dreßing, H., Gass, P.: Stalking! Verfolgung, Bedrohung, Belästigung. 2005.

Der bff und die Unterstützung Betroffener von Cyberstalking

Im bff sind über 170 Fachberatungsstellen aus dem gesamten Bundesgebiet zusammengeschlossen, die weibliche Betroffene von Gewalt beraten und unterstützen.[2]

In den Beratungsstellen findet sich eine seit Jahrzehnten auf- und ausgebaute Kompetenz im Umgang mit geschlechtsspezifischer Gewalt in ihren unterschiedlichen Ausprägungen (körperliche, sexualisierte und psychische Gewalt innerhalb und außerhalb von intimen Beziehungen, Stalking, Belästigung). Seit einigen Jahren sind die Beratungsstellen zunehmend mit dem Phänomen der Digitalisierung von Angriffen konfrontiert. Frauen und Mädchen wenden sich an die Fachberatungsstellen, wenn sie von „digitaler Gewalt“ oder „Cybergewalt“ betroffen sind. Im bff werden die Erfahrungen der Beratungspraxis gebündelt und weiter entwickelt.

Digitale Angriffe wie Diffamierung, Beleidigung und Rufschädigung werden zwar von Frauen und Männern begangen. Schwere Deliktformen, und insbesondere Stalking, werden unserer Erfahrung nach überwiegend von Männern an Frauen verübt. Auch Studien belegen, dass 80% der Betroffenen Frauen sind und 80% der Täter Männer.[3] Häufig werden unterschiedliche – nicht nur digitale – Angriffsformen kombi-

niert. In sehr vielen Fällen kennen die von Stalking betroffenen Frauen den Täter. Es sind also meistens keine wildfremden Angreifer, sondern ehemalige oder aktuelle Beziehungspartner, aber auch Arbeitskollegen, Bekannte oder Nachbarn.

Formen von Cyberstalking

Mit dem Begriff Cyberstalking werden unterschiedliche Angriffsformen im digitalen Raum zusammengefasst. Die am häufigsten vorkommenden Formen von Cyberstalking sind folgende:

> Mich beschäftigen die vielfältigen Möglichkeiten der Ausübung von Cyberstalking.

Ausspionieren und Abfangen von Daten
Von dieser Angriffsform berichten in der Beratung häufig Betroffene, die in einer von Gewalt, Kontrolle oder übermäßigen Eifersucht geprägten Beziehung leben.

Der stalkende Ehemann oder Lebensgefährte nimmt mittels Passwortdiebstahl Einsicht in private oder auch geschäftliche Mails, lädt unerlaubt private Daten auf seinen eigenen PC herunter und knackt dafür Passwörter oder er verfolgt mittels Spionageprogrammen die telefonischen Aktivitäten der Betroffenen und kontrolliert, wer wann angerufen wird, lässt sich SMS-Berichte schicken, usw.

Mit all diesen Dingen macht sich der Angreifer strafbar. Das Ausspähen von Daten unter Überwindung eines besonderen Schutzsystems – in diesem Fall von Passwörtern – ist nach §202a Strafgesetzbuch (StGB) strafbar.

Identitätsdiebstahl und Identitätsmissbrauch
Unter Identitätsdiebstahl und -missbrauch versteht man die Aneignung einer fremden, bereits bestehenden Identität, indem man bspw. einen Account knackt und dann unter dieser falschen Identität Einträge in Chats, Blogs oder soziale Netzwerke macht. Das sind dann oft beleidigende oder für das Opfer peinliche Einträge. Ziel des Täters ist es, den Ruf der betroffenen Person zu schädigen. Wenn von ihrem Account aus plötzlich Freund_innen auf Facebook beschimpft werden oder auf ihrem Profil peinliche Posts auftauchen, dann hat das für die Betroffene nicht nur zur Folge, dass ihr Ruf vielleicht beschädigt ist, sondern sie bekommt auch das Gefühl, dass jemand anderes die Kontrolle über ihre persönlichen Daten und ihr soziales Leben übernommen hat.

Von Identitätsmissbrauch wird auch gesprochen, wenn jemand beispielsweise Waren und Dienstleistungen unter dem Namen der Betroffenen bestellt.

Überwachen und Verfolgen
Von einer Überwachung oder Verfolgung kann dann die Rede sein, wenn ein Täter die Betroffene online verfolgt, z. B. wenn er auf dem Computer überwacht, welche Seiten dort besucht wurden oder wenn er durch GPS-Ortung auf dem Handy nachverfolgt, wo die Betroffene sich aufhält. Die Software dafür ist relativ leicht zu bekommen und kann auf dem Smartphone installiert werden, ohne dass die Betroffene etwas bemerkt. Strafbar ist das Orten einer Person durch GPS nicht.

Cyberharassment (Belästigung)
Eine weitere Form von Online-Stalking ist das Cyberharassment. Davon sind oft Frauen betroffen, die im Netz aktiv sind und sich dort öffentlich zu politischen Themen äußern, bspw. auf Blogs oder Twitter. Ein zuletzt sehr bekanntes Beispiel ist

der Hashtag #aufschrei. Es kam zu einer Flut von Beschimpfungen und Bedrohungen in den Kommentarspalten. Diese reichten bis hin zu Vergewaltigungs- und Morddrohungen.

> Stimmt es, dass gegen Cyberharassment die Konfrontation gesucht werden soll? Also, dass Gegenargumente gepostet und Richtigstellungen publiziert werden sollen?

Das Besondere an dieser Form der Cybergewalt ist, dass es sich in der Regel um anonyme Täter handelt, die der Betroffenen nicht persönlich bekannt sein müssen. Die Täter nutzen ihre Anonymität, um diese heftigen Beschimpfungen und Bedrohungen zu äußern.

Es gibt auch eine Form des Cyberharassments, bei der die Angriffe von Menschen aus dem engen sozialen Umfeld kommen. Ein Beispiel hierfür ist das permanente Schicken von SMS. Auch andauernde Anrufe und das Hinterlassen von Nachrichten auf dem Anrufbeantworter, damit niemand anderes mehr Nachrichten hinterlassen kann, zählt zu dieser Form der Cybergewalt. In solchen Fällen ist der Täter der Betroffenen in den meisten Fällen bekannt oder sie hat zumindest eine Ahnung, wer Urheber der Belästigung ist. Auch das nennt man Cyberharassment, es ist im Prinzip aber eine klassische Form von Stalking.

Funktion und Wirkungsweise von Cyberstalking

Fachberatungsstellen unterstützen sehr häufig Frauen, die sich in Trennungssituationen von Partnern befinden. Aus der Forschung ist bekannt, dass diese Situationen für Frauen sehr gefährlich werden können, wenn die Beziehung schon vorher gewaltbelastet war und der Partner die Trennung nicht akzeptiert und weiterhin Kontrolle ausüben möchte. Es kommt dann zum so genannten Trennungs-Stalking, also der gezielten Nachstellung durch den Ex-Partner. Dabei kommt es häufig vor, dass sich Stalker auch digitaler Medien bedienen. In der Beratung berichten Betroffene von Trennungs-Stalking häufig von einer Kombination aus den unterschiedlichen o.g. Formen von Cyberstalking.

Grundsätzlich zielen die Angreifer bei Cybergewalt mit ihren Aktionen auf Herabsetzung, Rufschädigung und soziale Isolation der Betroffenen ab und verfolgen die Nötigung bzw. Erpressung eines bestimmten Verhaltens – im Falle von Trennungs-Stalking die Wiederaufnahme der Beziehung und die fortdauernde Kontrolle über das Leben der Betroffenen. Dass Männer über Frauen Macht und Kontrolle erlangen oder erhalten wollen, ist nicht neu; das ist quasi der Kern von geschlechtsspezifischer Gewalt gegen Frauen. Das besondere an der Digitalisierung dieser Angriffe ist aber, dass der Täter sich während des Angriffs in „körperlicher Sicherheit“ befindet. Bei Angriffen im Netz findet keine physische Konfrontation zwischen Täter und Betroffener statt und das scheint die Hemmschwelle sinken zu lassen.

Die Position des Täters wird dadurch noch mächtiger, weil seine Angriffe quasi kontinuierlich und ohne Ortsbindung stattfinden können. Täter können auf diese Weise Macht über ihre Opfer ausüben, ganz egal, wo sich beide gerade befinden.

Die Situation der Betroffenen von Cyberstalking

Das Erleben von Gewalt und insbesondere von Stalking ist für die Betroffenen in den allermeisten Fällen geprägt von einem starken Gefühl der Ohnmacht und von großer

Scham. Sehr oft fühlen sich Betroffene selbst Schuld an dem, was passiert. Dies ist charakteristisch für das Erleben von (geschlechtsspezifischer) Gewalt, z. B. auch bei Sexualdelikten oder Partnerschaftsgewalt. Frauen fragen sich oft: „Habe ich das provoziert?“ oder „Was habe ich falsch gemacht?“ und bekommen solche Haltungen auch von ihrem sozialen Umfeld gespiegelt. Diese Gefühle bei den Betroffenen sind völlig unabhängig davon, ob die Angriffe im digitalen Raum oder analog in der nicht-digitalen Welt stattfinden.

Was genau ist das Spezielle beim Cyberstalking?

Betroffene von Cyberstalking haben aber unserer Erfahrung nach ein noch größeres Gefühl der eigenen Ohnmacht und Hilflosigkeit. Und zwar deswegen, weil sie nicht nur mit einem gewaltausübenden Täter konfrontiert sind, sondern zusätzlich noch mit der Macht und den Möglichkeiten des digitalen Raums. Das Internet erscheint den Betroffenen dabei noch mächtiger als der Täter selbst, unüberschaubar und unkontrollierbar.

Viele Betroffene hatten sich bis zum Zeitpunkt der ersten Angriffe noch keine Gedanken über Möglichkeiten der „digitalen Selbstverteidigung“ gemacht. Sie bewegen sich zwar selbstverständlich im Internet und nutzen vielfältige digitale Medien, aber das Wissen um Schutzmöglichkeiten ist gering.

Immer wieder schildern uns Betroffene, dass sie lange Zeit gehofft haben, die Angriffe würden von selbst aufhören. Uns ist kein Fall bekannt, in dem das eingetreten ist. Die Zeit, die Betroffene verstreichen lassen, in der Hoffnung, der Täter würde ein Einsehen haben, wird von diesem meist für die Planung weiterer Angriffe genutzt.

Betroffene unternehmen häufig zunächst keine Schritte, weil sie das Gefühl haben, nichts ausrichten zu können. Sie fühlen sich ohnmächtig und schämen sich. Auch bei einem einmaligen sexuellen Angriff ist die Scham der Betroffenen in der Regel groß und verhindert, dass z. B. Hilfe gesucht wird und sie sich jemandem anvertrauen.

Möglichkeiten des Schutzes und der Gegenwehr

Welche Ratschläge kann man Betroffenen geben, Cyberstalking zu beenden?

Betroffene von Cyberstalking können Beweise für die Taten sammeln. Empfehlenswert ist das Führen eines Stalking-Tagebuchs, in dem Ort, Datum, Uhrzeit und die Stalking-Handlung notiert werden. Damit kann später der Stalking-Verlauf rekonstruiert werden, was bei möglichen rechtlichen Schritten sehr hilfreich sein kann. Konkret bedeutet dies, die diffamierenden Nachrichten zu speichern, auszudrucken und zu notieren, wann sie abgeschickt wurden. Von diffamierenden Bildern in sozialen Netzwerken können Screenshots angefertigt werden und notiert werden, wann diese online gestellt wurden.

Welche technischen Möglichkeiten gibt es, sich dagegen zu wehren?

Gegen das Ausspähen und Ausspionieren können Betroffene Accounts wechseln und präventiv öfter Passwörter von Mail-Accounts, Computern oder Smartphones erneuern. Bei Verdacht auf Spyware können die entsprechenden Geräte offline geschaltet werden und von Expert_innen auf Spyware untersucht werden.
Insbesondere nach einer Trennung empfiehlt es sich, Partner-Verträge für Handy und Internet zu kündigen und neue Passwörter zu verwenden.

Wie können Betroffene empowert werden?

Dies sind nur ein paar wenige Tipps, wie Betroffene sich selbst schützen können.[4] Wichtig ist bei jeder Form von Gewalt, egal ob online oder nicht, mit dem Erlebten nicht alleine zu bleiben und sich Menschen anzuvertrauen, die einen unterstützen können. Damit ist schon ein erster wichtiger Schritt getan, dem Täter etwas entgegenzusetzen. Denn der intendiert genau das: sein Opfer zu isolieren und so Macht über die andere Person ausüben zu können. Ein Anruf bei einer Freundin, einem Familienmitglied oder auch einer Frauenberatungsstelle ist häufig der erste Schritt, aus der Hilflosigkeit auszubrechen und der Gewalt etwas entgegenzusetzen.

Was kann Beratung in Fällen von Cyberstalking leisten?

Wie gehen Beratungsstellen an die Beratung heran?

Eine zentrale und erste Aufgabe der Beratungsstellen ist häufig, Informationen zu geben und aufzuklären. Betroffene erhalten Information darüber, welche Schutzmöglichkeiten es gibt und welche Schritte eingeleitet werden können, um der Cybergewalt etwas entgegenzusetzen. Die meisten Beratungsstellen arbeiten mit Rechtsanwältinnen zusammen und können den Betroffenen Auskunft geben, welche rechtlichen Handlungsmöglichkeiten es gibt und wie diese eingeleitet werden können. Auch die Entscheidung darüber, ob rechtliche Schritte gegangen werden, mit welchen Risiken und Chancen dies verbunden ist, kann in einem Beratungsprozess gemeinsam mit einer Beraterin getroffen werden.

[4] Einen ausführlicheren Überblick über technische Schutzmaßnahmen und eine Strategie gegen digitale Gewalt bietet Vera Kätsch in ihrem Beitrag in dieser Broschüre.

Wie wird man diese Schuldgefühle los?

Ganz zentral bieten Frauenberatungsstellen den Betroffenen psychosoziale Unterstützung im Umgang mit der Gewalt und ihren Folgen. Konkret bedeutet das, gemeinsam mit den Betroffenen einen Ausweg aus den Gefühlen der eigenen Schuld und Scham zu finden und zu ergründen, welche Ressourcen die Betroffenen haben, um mit der Situation anders umzugehen.

Wie kann ich Betroffenen die Scham nehmen und sie wieder handlungsfähig machen, wenn z. B. Nacktbilder oder Videomaterial veröffentlicht wurden oder dieses angedroht wird?

Durch das Erfahren von Handlungsmöglichkeiten kann es gelingen, mit den Betroffenen wieder eine Handlungsmächtigkeit zu erarbeiten und aus dem Gefühl der Ohnmacht herauszukommen.

Herausforderungen

Es ist davon auszugehen, dass die Phänomene der Cybergewalt und des Cyberstalking in Zukunft nicht abnehmen werden, sondern sich weiter verbreiten werden. Unserer Erfahrung nach birgt dieses Thema einige spezifische Herausforderungen, auf die es bisher noch keine befriedigenden Antworten gibt.

Was ist politisch hinsichtlich Cyberstalking nötig?

Es ist bislang nicht gelungen, Cybergewalt (gegen Frauen) als gesamtgesellschaftliches Problem zu thematisieren, auf das auch gesamtgesellschaftlich reagiert werden muss.

Dies gilt insgesamt auch noch für viele Angriffsformen im Bereich Gewalt gegen Frauen. So lange ein Problem aber nicht als gesellschaftlich verursacht betrachtet wird, verbleiben die Betroffenen mit ihren Erfahrungen alleine und es findet eine Individualisierung des Problems statt.

Auf Seiten der Betroffenen und ihres sozialen Umfeldes kann die Individualisierung der Gewaltbetroffenheit im Falle von Cyberstalking fatale Folgen haben. Über einen längeren Zeitraum Opfer von Cyberattacken zu sein, kann dazu verleiten, sich aus dem digitalen Raum zurückzuziehen. Wer kein Smartphone besitzt, kann nicht geortet werden, wer sich nicht digital fotografieren lässt, von dem können keine Fotos im Netz verbreitet werden, wer nicht bei Facebook ist, kann dort nicht belästigt werden, usw. Der vermeintlich einfachste und naheliegende Umgang mit Cyberstalking ist die Vermeidung des digitalen Raumes, um keine Angriffsfläche zu bieten.

Die Herausforderung besteht für uns alle, die wir an der Bekämpfung von Cyberstalking gegen Frauen interessiert sind, darin, das Problem als ein Thema der öffentlichen und inneren Sicherheit zu benennen und einzufordern, dass ihm auf diese Weise begegnet wird, z. B. durch gesetzliche Maßnahmen und die Inverantwortungnahme auch von Online-Dienstleistern für die Sicherheit ihrer Nutzer_innen.

> Ich möchte uni-intern eine Öffentlichkeit zum Thema schaffen.

Gewalt, die digital ausgeübt wird, wird aber zu oft noch nicht richtig ernst genommen und nicht selten bekommen Frauen den Rat: „Dann lies den Mist doch nicht."

Digitale Gewalt wird bagatellisiert und viel zu oft als individuelles Problem abgetan.

> Es müssen den Beratungsstellen mehr Ressourcen für Vernetzung und Öffentlichkeitsarbeit an die Hand gegeben werden.

Der in den letzten 20 Jahren im Bereich Partnerschaftsgewalt gelungene veränderte gesellschaftliche Umgang, nämlich, häusliche Gewalt aus dem Privaten ans Licht zu holen und gesellschaftlich zu ächten, muss auch mit Cybergewalt gelingen.

Für die Beratungsstellen ist aber gerade das eine große Herausforderung: neben dem großen Wissen und der Erfahrung über Gewaltdynamiken (vorhanden) und der Kompetenz in psychosozialer Unterstützung (vorhanden) muss auch eine immer größere Kompetenz und Wissen über die Möglichkeiten und Funktionsweise der unterschiedlichsten digitalen Medien hinzukommen.

> Es gibt einen hohen Bedarf der Berater*innen an Informationen zu neuen Gewalt- und Angriffsformen

Diese Aneignung findet im Moment statt. Sie ist aber bei weitem nicht abgeschlossen und sie muss stetig weiter entwickelt werden, weil sich die digitalen Möglichkeiten ständig verändern und sich immer neue technische Möglichkeiten auftun.

> Es fehlt Medienkompetenz in Bezug auf soziale Netzwerke und Internetsicherheit.

Wir als Bundesverband sehen es auch als unsere Aufgabe an, die Beratungsstellen dabei zu unterstützen, diese Kompetenzen stetig weiter zu entwickeln. Dringend notwendig sind Fortbildungen für die Mitarbeiterinnen der Beratungsstellen, damit sie zum einen auf dem aktuellen Stand neuer Angriffsformen sind und gleichzeitig gut vernetzt sind, um Betroffenen auch ganz praktische, technische Hilfestellung bieten zu können.

> Ich wünsche mir mehr Informationen, Vernetzung und Austausch zum Thema.

> Cybergewalt ist in den meisten Beratungen von Frauen*, die von Gewalt betroffen sind, ein Thema. Das wird weiterhin zunehmen und wir müssen darauf vorbereitet sein. Aber nicht alle Berater*innen können Fachfrauen* werden. Es braucht Fachberatungsstellen zu Cybergewalt, die geschlechtsspezifisch arbeiten.

Nicht jede Beraterin ist ein Computerfreak und kennt alle Social Media-Kanäle, geschweige denn deren Sicherheitseinstellungen. Umso wichtiger ist es, sich mit Expert*innen zu vernetzen und Wissen weiterzutragen.

Ein großes Hindernis stellt die desolate finanzielle Situation der meisten Beratungsstellen dar. Zum Beispiel haben viele Beratungsstellen zu wenige und viel zu alte Computer. Um in einem Beratungsprozess mit einer von Cybergewalt betroffenen Klientin die Möglichkeiten des Schutzes zu besprechen, sollte aber die Möglichkeit bestehen, sich gemeinsam im Internet die nötigen Schritte anzuschauen.

Zudem verfügen die allerwenigsten Beratungsstellen über die personellen Ressourcen, um mit ihren Beratungsangeboten im digitalen Raum anwesend zu sein. Denn die Präsenz in sozialen Netzwerken, dort wo die Gewalt stattfindet und wo die Betroffenen sich aufhalten, kostet Arbeitszeit und diese muss finanziert sein.

An dieser Stelle sind die Geldgeberinnen gefragt, die Ausstattung der Beratungsstellen derart aufzustocken, dass dem Bedarf entsprechende Angebote gemacht werden können.

In den Frauenberatungsstellen und Frauennotrufen arbeiten hochmotivierte und hochqualifizierte Fachkräfte, die Expertinnen sind auf dem Gebiet Gewalt gegen Frauen, einige seit mehr als 30 Jahren. Sie wissen, was gewaltbetroffenen Frauen hilft und was die Dynamiken geschlechtsspezifischer Gewalt sind. Wir müssen erreichen, dass diese wichtige Arbeit auf stabile finanzielle Füße gestellt wird und wir auch Phänomenen wie Cyberstalking jederzeit stark entgegentreten können.

Weiterführende Literatur:

bff: Fact sheet stalking: Zahlen und Fakten, 2013 (https://www.frauen-gegen-gewalt.de/weitere-informationen.html, letzter Zugriff am 28.06.2016).

bff: Digitale Welten, digitale Medien, digitale Gewalt: https://www.frauen-gegen-gewalt.de/weitere-informationen-226.html, letzter Zugriff am 28.06.2016.

Bündnis gegen Cybermobbing (Hg.): Mobbing und Cybermobbing bei Erwachsenen. Eine empirische Bestandsaufnahme in Deutschland. 2014.

Europäische Grundrechteagentur: Gewalt gegen Frauen. Eine EU-weite Erhebung, 2014 (http://fra.europa.eu/de/publication/2014/gewalt-gegen-frauen-eine-eu-weite-erhebung-ergebnisse-auf-einen-blick, letzter Zugriff am 28.06.2016)
Jens Hoffmann, Hans-Georg Voß: Psychologie des Stalking. Grundlagen – Forschung – Anwendung. 2006.

Julia Hurrelmann, Irmgard Nauck, Dagmar Freudenberg: Stalking - Grenzenlose Belästigung. Eine Handreichung für die Beratung. Bundesministerium für Familie, Senioren, Frauen und Jugend. 2009.

Andrea Weiss: Stalking und häusliche Gewalt. 2005.

Ein Beratungsgespräch bei Cyberstalking:

Aktuelle Herausforderung in der Anti-Stalking-Beratung

Beate M. Köhler
Projektkoordinatorin und Beraterin des Anti-Stalking-Projekts des FRIEDA-Frauenzentrum e. V.

Das digitale Zeitalter bietet heute jede Menge ungeahnter und faszinierender Chancen und Möglichkeiten. Vor ein paar Jahren hätten wir vieles davon nicht für möglich gehalten. Dieser Fortschritt beinhaltet aber auch Gefahren und eine Vielzahl an Möglichkeiten des Missbrauches.

Neben Cybermobbing, Cybergrooming, Cybersexism, Sexting und vielen anderen digitalen Gewaltformen mehr, ist Cyberstalking eines jener besorgniserregender Phänomene, das Tag für Tag zunimmt.

Ich bin hier, weil Cyberstalking in meiner Tätigkeit als Beraterin* bei häuslicher Gewalt eine zunehmende Rolle spielt.

Auch wenn es hierzu noch keine genauen Zahlen gibt, können wir davon ausgehen, dass mit einer weiteren Digitalisierung der Gesellschaft und zukünftigen Techniken auch die Häufigkeit der Nutzung der digitalen Medien sowie der damit zusammenhängenden Problematiken der Cyberkriminalität und des Cyberstalking zunehmen werden.

Gibt es valide Statistiken zur Problematik Cyberstalking?

Aus der Arbeit des Anti-Stalking-Projektes, für das ich heute spreche, und aus anderen Anti-Gewalt-Projekten, wissen wir, dass Frauen* häufiger als Männer die Betroffenen von Gewalt, von Stalking und vor allem von sexualisierter Gewalt sind.

Existieren auch Statistiken zum Alter der Betroffenen und der Aggressoren?

Das Anti-Stalking-Projekt des FRIEDA-Frauenzentrum e. V. berät seit Januar 2014 Frauen*, die von Stalking betroffen sind. Dabei ist Cyberstalking eine der Thematiken, die in den letzten Jahren immer mehr Raum einnimmt. In unserer parteiischen Beratung und Begleitung stehen die Frauen* und ihre Bedürfnisse im Mittelpunkt der Unterstützungsbemühungen.
Wir orientieren uns an den verschiedenen Bedürfnissen der betroffenen Frauen*, unterstützen sie individuell und versuchen, gemeinsam mit den Betroffenen, einen Weg zu finden, das Cyberstalking/Stalking zu beenden und die Zeit bis dahin möglichst unbeschadet zu überstehen.

Wir beraten zu sexualisierter Diskriminierung und Gewalt und nehmen in der Beratung zunehmende Tendenzen von Cyberstalking war.

An wen kann ich Opfer weiterleiten?

Jede Frau, die sich, wenn sie von Cyberstalking/Stalking betroffen ist, auf den Weg macht, sich ihren Raum wieder zu nehmen und dem Stalking etwas entgegenzusetzen, tut gut daran, sich bei diesem Vorhaben unterstützen und begleiten zu lassen. Hierfür sind wir mit dem Anti-Stalking-Projekt da.

Welche Beratungsstellen gibt es speziell für diesen Bereich?

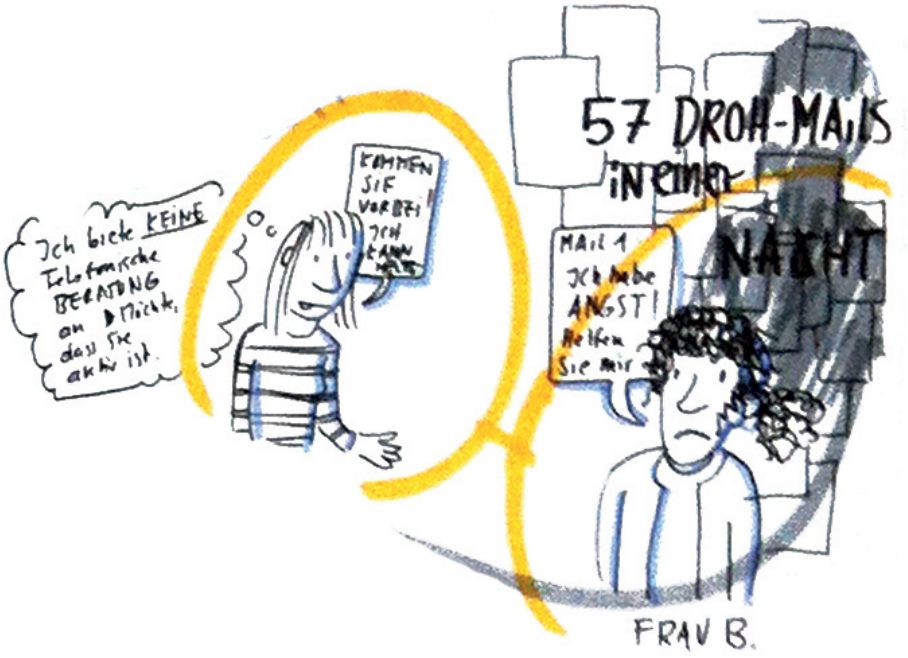
Im Folgenden beschreiben Saskia Benter und ich einen Cyberstalking-Fall aus unserer Praxis. Saskia Benter wird der Betroffenen eine Stimme geben, da wir nicht losgelöst über die betroffenen Frauen* reden wollen.[1]

Mail 1 1

Sehr geehrte Frau Köhler,

eine Freundin gab mir Ihre Adresse mit dem Rat, dass ich mich mal mit Ihnen in Verbindung setzten solle. Diese Mail schreibe ich auch von ihrem PC aus. Ich weiß einfach nicht mehr weiter. Ich werde verfolgt beschimpft und bedroht und ich weiß nicht, was ich machen soll. Ich hab´ heute Nacht 57 Mails bekommen. Alle ganz böse. Er weiß alles, er sieht alles und ich weiß nicht, was er als nächstes macht. Ich habe Angst.

Bitte, bitte helfen Sie mir.



Hier nimmt eine Frau Kontakt mit uns auf, die ihrer Beschreibung nach von Cyberstalking betroffen ist. Typische Handlungen des Cyberstalking sind der hohe Eingang an E-Mails. Später wird sich herausstellen, dass auch Telefonterror, SMS-bombing sowie weitere Taten über die elektronischen Medien begangen wurden.

[1] Die hier wiedergegebene Stalkingdynamik und der Verlauf der E-Mail Kommunikation wurden uns von Frau B. freundlicherweise für die anonymisierte Verwendung auf dem Fachtag und in dieser Dokumentation zur Verfügung gestellt.

Mail 2

Sehr geehrte Frau Köhler,

Ich bin total verzweifelt. Ich glaube, ich werde verrückt.

Ich gehe nicht mehr an mein Telefon und meinen PC hab´ ich seit Wochen nicht mehr geöffnet. Er steht auf meinem Schreibtisch, glotzt mich an und macht mir richtig Angst. Ich habe das Gefühl, dass er mich beobachtet. Ich fühle mich total alleine und trau´ mich nicht mehr, mich bei meinen Freunden zu melden.

Das Gefühl, ständig beobachtet und verfolgt zu werden, wie es die Frau hier beschreibt, kann eine ganze Reihe von körperlichen und psychischen Symptomen auslösen. Schreckhaftigkeit, Gereiztheit, Albträume, Panikattacken, aber auch Depressionen, Schlaf- und Essstörungen sowie das Gefühl, aufgrund von Kontrollverlust verrückt zu werden, können auftreten. Wer sich ständig, 24 Stunden am Tag, beobachtet fühlt, steht unter Dauerstress. Dies schwächt das Immunsystem der Betroffenen enorm und kann Auslöser für eine Vielzahl von Folgeerkrankungen sein, die oft nicht mit dem Stalking in Verbindung gebracht werden.

Welche psychischen und körperlichen Folgen kann Cyberstalking haben?

Mail 3

Sehr geehrte Frau Köhler,

denken Sie denn, dass Sie mir wirklich helfen können? Ich hab´ total Angst und weiß nicht mehr, was ich tun soll.

Ich bin von der Welt abgeschnitten, kann nicht mehr schlafen und er macht immer mehr Stress.

Kann er nicht einfach aufhören??????
Ich hab´ Angst, dass er mir folgt, wenn ich zu ihnen komme.

Was soll ich bloß tun?

Aus Erfahrungen wissen wir, dass das Stalking in den wenigsten Fällen von alleine aufhört bzw. der Verursacher es einfach bleiben lässt. Daraus folgt, dass die Betroffenen selbst etwas dagegen unternehmen müssen und in die Handlung kommen sollten. Es ist wichtig, das eigene Leben nicht einem Anderen zu überlassen.

> Wie kann ich Frauen* dabei unterstützen, sich Hilfe zu holen?

Je eher Betroffene reagieren, umso einfacher ist es oftmals, das Gleichgewicht in ihrem Leben wieder herzustellen. Das aber ist ein Kraftakt und hier bedarf es zu Recht oftmals der Unterstützung von außen.

Mail 4

Hallo Frau Köhler,

gestern habe ich bei Ihren Kolleginnen einen Termin ausgemacht. Ich werde nächste Woche zu Ihnen kommen. Wenn sie mir nicht helfen, weiß ich auch nicht, was ich noch tun soll. Ich weiß nicht, ob das gut ist.

Es ist wichtig, sich Beratung und Hilfe zu holen. Damit sollte möglichst nicht zu lange gewartet werden. Denn wie man hier gut sehen kann, nehmen die Hilflosigkeit und Gefühle wie Kontrollverlust und die des Ausgeliefertseins immer weiter zu.

Der erste Schritt ist gemacht. Für viele Frauen* bedeutet dieser einen großen Kraftaufwand. Oftmals haben sie all ihren Mut zusammengenommen, um einen Termin zu vereinbaren. Leider verlässt aber manche vor dem Beratungstermin wieder der Mut und so kann es vorkommen, dass zum Termin niemand kommt.

Das war auch bei Frau* B. der Fall, worauf ich vorsichtig nachhakte und ihr anbot, doch eine Vertrauensperson mitzubringen. Frau* B. machte daraufhin einen weiteren Anlauf und kam eine Woche später in Begleitung einer Freund*in ins Beratungszentrum.

Frau* B.s Geschichte – Warum der erste Schritt schwierig ist

Welche Verlaufsformen von Cyberstalking gibt es?

Begonnen hatte alles damit, dass Frau* B. eine E-Mail erhielt, die mit Tim unterschrieben war. Frau* B. kennt zu diesem Zeitpunkt niemanden mit diesem Namen, will aber wissen, wer oder was dahinter steckt und antwortet auf diese Mail. Es entwickelt sich eine Art Smalltalk, den Frau* B. anfangs noch für unverfänglich hält und sich gerne darauf einlässt. Tim ist unterhaltsam und ihr zugewandt und baut den Kontakt zu ihr schnell aus.

Dazu benutzt er nicht nur die Mailadresse von Frau* B., sondern kontaktiert sie auch über WhatsApp und Facebook. Mit der Zeit wächst bei Frau* B. das Gefühl, dass Tim überall ist. Dann werden die Inhalte der Mails beleidigend und enthalten zudem immer mehr Wissen über aktuelle Geschehnisse aus dem Leben von Frau* B.. An manchen Stellen ist sie sich sicher, dass sie Tim nichts über diese Dinge geschrieben hatte. Das lässt Frau* B. innehalten, verärgert und verunsichert sie. Es zeigt sich, dass Tim über viele Informationen verfügt, die er nicht von ihr bekommen hat. Beispielsweise nimmt er abwertend Bezug auf ihren Körper in einem neuen Kleid: „In dem neuen Kleid von H&M hast du einen fetten A…“ oder „Bei deiner Figur hilft auch kein neues Fitnessstudio.“

Auf die Fragen, wer er sei und was er von ihr wolle, reagiert Tim nicht und sie bleibt weiterhin im Ungewissen bezüglich dieser für sie wichtigen Fragen. Dies erschreckt und ängstigt sie sehr. Gleichzeitig nimmt ihre Wut auf den Unbekannten zu und sie beginnt, genervt auf ihn zu reagieren. Auf der Arbeit ist sie zunehmend verunsichert und unkonzentriert und beginnt Fehler zu machen. Daraus folgen zusätzlicher Ärger mit Kolleg*innen und ihrer Chef*in.

Alle Versuche ihrerseits, den Kontakt zu Tim abzubrechen, bleiben ohne Erfolg. Vielmehr wird der Ton in den von ihm verfassten Mails immer schärfer, gemeiner und beleidigender: „Du wirst schon sehen, was Du davon hast!“, „Bald will niemand mehr mit dir was zu tun haben.“, „Was sollen bloß deine Eltern von so einer wie dir denken?“

In Frau* B. steigt das Gefühl, beobachtet und verfolgt zu werden immer weiter an. Ihre Angst nimmt zu und Gefühle wie Hilf- und Machtlosigkeit verstärken sich. Sie wird misstrauisch, beginnt, sich von Familie und Freund*innen zurückzuziehen und isoliert sich zunehmend. Diese Einsamkeit verstärkt ihre Hoffnungslosigkeit und Frau* B. fragt sich, ob das alles noch einen Sinn macht. Sie beginnt über Suizid nachzudenken. Hinzu kommen zunehmende Schlaf-, Ess- und Konzentrationsstörungen. Sie hat Angst und Panikattacken und das permanente Gefühl, verfolgt zu werden.

Dieser Dauerstress, dem Frau* B. ausgesetzt ist, kann Auslöser für viele Krankheiten sein, die sich, wenn die Stresssituationen über einen längeren Zeitraum andauern, chronifizieren können. Frau* B. nennt sich in dieser Situation später selbst: „ein Nervenbündel“.

Neben den physischen und psychischen Auswirkungen entsteht für Frau* B. mit der Zeit auch ein erheblicher finanzieller Schaden. Sie bezahlt bis zum Zeitpunkt der ersten Beratung Waren im Wert von 1200,- €, die sie selbst nie bestellt hat, aber aus Scham nicht retour sendet. Bei den Warensendungen handelt es sich vorwiegend um Sexspielzeug und Pornohefte, die sie selbst abstoßend findet.

Zu diesem Zeitpunkt ist der Postbote eine der angsteinflößendsten Personen in ihrem Umfeld.

Zur gleichen Zeit erhält Frau* B. verstärkt von fremden Männern Kontaktanfragen, die sie auf Sexdienste ansprechen, die sie angeblich auf einer einschlägigen Plattform anbieten würde. Ihre Mutter erhält ein Foto, auf dem sie in einer erotischen Pose abgebildet ist, zugeschickt. Ihr Bruder bekommt per Mail einen Link zu einer Sex-Seite, auf der eine Fotomontage von ihr zu sehen ist. In ihr steigt der Leidensdruck.

Sie leidet vor allem unter der sexualisierten Gewalt und unter den weiteren Androhungen durch Tim. Frau* B. hat Angst, schämt sich und zieht sich immer weiter von ihren Freund*innen und ihrer Familie zurück. Dies macht es für ihren Bedroher noch einfacher, sie weiter in die Enge zu drängen. Aber die Familie und speziell eine ihrer Freund*innen lassen nicht locker und ermutigen sie, etwas zu tun.

Bei Frau* B. wächst der Verdacht, dass hinter all dem ihr Ex-Freund, von dem sie sich vor ca. vier Jahren trennte, stecken könnte. Vor allem ist das Foto, das ihre Mutter erhalten hatte, in ihren Augen ein Indiz dafür. Frau* B. konfrontiert Tim mit ihrer Vermutung. Er aber geht darauf nicht ein. Er verneint es nicht und versucht nicht, sich aus der Sache raus zu reden. Ihre Fragen, warum er das alles mache, was er von ihr wolle und warum er sich nach so langer Zeit wieder meldet, bleiben unbeantwortet.

Da bittet Frau B. ihre Freund*in um Hilfe und sie schreiben gemeinsam die erste Mail an das Anti-Stalking-Projekt.

Die Erstberatung – konkrete Schritte

Welche Aspekte sollten in der Beratung beachtet werden?

Für die Erstberatung nehmen wir uns im Anti-Stalking-Projekt bis zu zwei Stunden für die Klientin* und ihre Fragen Zeit. Die Betroffene soll genügend Raum haben, ihre Geschichte erzählen zu können. Denn wir wissen, dass viele von Stalking Betroffene nur selten die Möglichkeit haben, dem Bedürfnis, alles Erlebte einmal von der Seele zu reden, zu folgen.

Alle weiteren Schritte sind an den Bedürfnissen und Möglichkeiten der jeweiligen Frau* ausgerichtet. In erster Linie geht es darum, was sie möchte und was sie dabei unterstützt, ihr Leben wieder ins Gleichgewicht zu bekommen.

Mich interessiert das Thema der Ohnmacht der Betroffenen und wie sie wieder Handlungsfähigkeit erlangen können.

Schritt 1: Zuhören
Wir hören erst mal nur zu.

Schritt 2: Überblick verschaffen, nachfragen, sortieren
Wir versuchen uns einen Überblick über die momentane Situation und den Stand der Dinge zu verschaffen. Fragen entsprechend nach und sortieren gemeinsam mit der Klientin*.

Schritt 3: Erwartungen klären
Es werden die Erwartungen, mit der die Betroffene ins Anti-Stalking-Projekt kommt abgefragt und es werden die Möglichkeiten, die eine Beratung und eine Begleitung durch das Anti-Stalking-Projekt abdecken können, geklärt. An dieser Stelle ist es wichtig, zu erfragen, was genau die Betroffene sucht und welche Art der Unterstützung sie für sich benötigt. Daran orientiert sich der weitere Verlauf des Gespräches. Denn es geht um den individuellen Bedarf und die spezifischen Möglichkeiten jeder einzelnen Frau und nicht darum, was Andere denken und für richtig halten.

Schritt 4: Klärung: Ist es Stalking/Nachstellung?
Der nächste Schritt ist das Abklären, ob es sich um Stalking bzw. Cyberstalking handelt und/oder ob die andere Person eventuell ein „berechtigtes Interesse“ am Kontakt hat. Dies ist wichtig, um eine künftige Strafverfolgung unter dem richtigen Straftatbestand führen zu können. Beispiele könnten ungeklärte Sorgerechtsfälle oder Nachbarschaftsstreitigkeiten sein. An dieser Stelle wird auch erfragt, ob es sich bei dem Stalking um “so ein Gefühl!“ handelt oder ob es klare Hinweise oder sogar Beweise gibt.

> Wie bereite ich eine beweiskräftige Anzeige vor?

Schritt 5: Information und Aufklärung.
Schließlich werden die unterschiedlichen Möglichkeiten des Handelns auf verschiedenen Ebenen aufgezeigt. Folgende Aufzählung benennt zentrale Themen einer Erstberatung, kann aber um individuelle, für die Klientin* bzw. den Fall relevante Fragen ergänzt werden.

- Welche rechtlichen Maßnahmen gibt es, sowohl strafrechtlich wie auch zivilrechtlich?
- Welcher rechtliche Beistand ist vorhanden oder sollte hinzugezogen werden?
- Wie gefährlich ist die Situation einzuschätzen?
- Was ist über den Bedroher/die Bedroherin* bekannt? Wie gefährlich ist er/sie einzuschätzen?
- Welche Schritte zur persönlichen Sicherheit der Klientin* sind anzuraten? Wie definiert sie persönlich Sicherheit?
- Welche Unterstützung wünscht sie sich?
- Will die Frau* eine Anzeige machen? Was spricht aus ihrer Sicht dafür, was dagegen? Was spricht aus der Sicht der Beraterin* dafür, was dagegen?
- Welche sind die einzelnen Schritte, wenn eine Anzeige gemacht wird?
- Was ist wichtig dabei und was sollte schon im Voraus bedacht werden?
- Welche Vorbereitungen müssen noch getroffen werden?
- Welche Unterlagen sollte die Klientin* zur Anzeigenerstellung mitnehmen?
- Gibt es eine Dokumentation der Vorfälle? Wenn ja, in welcher Form? Reicht diese aus? Oder an welchen Punkten sollte diese ergänzt oder erweitert werden? Benötigt die Klientin* hier Unterstützung?
- Gibt es Beweismaterial, das hinzugefügt werden sollte? Sind Zeug*innen benannt?
- Wie sieht es mit einer Begleitperson aus?
- Welche Haltung hat die Klientin* gegenüber dem Internet? Welche Sicherheitsmaßnahmen/Vorkehrungen hat sie bereits getroffen? Wie sieht es generell mit der Sicherheit bei PC, Handy usw. aus?

- Weiß sie über sichere Passworte Bescheid? Was sollte unbedingt überdacht, verändert und neu hinzugefügt werden?
- Was sind die nächsten Schritte in Bezug auf Internetsicherheit?
- Welche Fachfrauen* sollten unterstützend hinzugezogen werden?
- Welche Ressourcen, stabilisierenden Faktoren und unterstützenden Personen gibt es im Umfeld der Klientin*?
- Welche Entspannungstechniken sind bekannt und welche können darüber hinaus hilfreich sein?
- Welche Methoden zur Unterbrechung des Gedanken-Karussells können eingesetzt werden?
- Wie sieht es mit den Fähigkeiten zur Grenzsetzung aus?
- Welche Unterstützung kann hier gegeben werden?
- Wie sieht es mit geschlechtsspezifischer Selbstbehauptung und Selbstverteidigung aus? Sollten hier weitere Fachfrauen* hinzugezogen werden?
- Wünscht sich die Klientin* therapeutische Unterstützung?
- Welche Art der kontinuierlichen Begleitung empfindet die Klientin* als entlastend und unterstützend?
- Welche weiteren unterstützenden und entlastenden Möglichkeiten gibt es noch?

Konsequentes Handeln

Ein wichtiger Punkt in der Beratung für Frauen*, die von Cyberstalking oder Stalking betroffen sind, ist konsequentes Handeln. In der Beratung gehe ich darauf gesondert ein. Denn ob Stalking beendet wird oder sich noch lange hinzieht, kann vom konsequenten Handeln der Betroffenen abhängen. Je klarere Signale sie setzt, umso klarer kommt die Botschaft an. Das bedeutet aber nicht, dass sie die Verantwortung dafür trägt, dass der Stalker aufhört. Dass sie das Stalking nicht möchte, hat sie bereits mehrfach deutlich gemacht. Frauen* haben also keine Schuld an dem Stalking. Ein Gefühl, das viele der Betroffenen haben und vermittelt bekommen. Gleichzeitig aber sind sie dem Stalker auch nicht hilflos ausgeliefert, sondern können etwas an der Situation verändern. Hierbei ist eine Begleitung äußerst wichtig.

> Wie kann Cyberstalking durchbrochen werden?

> Welchen menschlichen Rat kann ich als Polizist*in einem „Opfer“ mitgeben? Mich interessiert dazu die Meinung der Beratungsstellen.

Frau* B. erzählte mir in der Beratung ihre Geschichte. Gemeinsam haben wir die Dynamik des Stalking analysiert und abgesprochen, was sie zukünftig für sich möchte und welche Unterstützung sie dafür benötigt, um den Weg gehen zu können, den sie gehen möchte. Vor Frau* B. lag ein langer Weg, auf dem sie sich von verschiedenen Fachfrauen* aus diversen Bereichen unterstützen ließ.

Mail 7

Hallo Frau Köhler,

sie hatten Recht. Die meisten Menschen sind nett und ich erfahre einiges an Hilfe.

Ich hab´ ganz viele Termine, aber ich bekomme langsam das Gefühl, dass ich etwas erreichen kann. Danke für Ihre unterstützenden Worte.

Ich melde mich wieder.

Frau* B. ging mit einer Strategie aus der Beratung. Sie wusste, wie sie vorgehen könnte und welches die nächsten Schritte sein sollten, die sie tun wollte. Diese abgesprochenen nächsten Schritte sind für die Frauen*, wenn sie dann wieder alleine sind, nicht immer wirklich umsetzbar. Aus diesem Grund hatten wir vereinbart, dass Frau* B. sich bei mir nach einiger Zeit nochmals meldet. Zeigt sich dann, dass die besprochenen Strategien nicht aufgehen, ist es wichtig, sich diese nochmals gemeinsam anzusehen, neu zu überdenken und weitere Absprachen zu treffen.

Mail 8

Liebe Frau Köhler,

es ist einige Zeit vergangen, seit ich Sie getroffen habe.

Er stand tatsächlich nie bei mir vor der Tür, was ja meine große Sorge war. Auch haben sich für den ganzen Mist tatsächlich Lösungen finden lassen. Auch wenn das Ganze dann doch viel Zeit und Nerven gekostet hat.

Und ich möchte Ihnen sagen, dass Sie an vielen Stellen Recht hatten.

Es war gut, Sie an meiner Seite zu wissen. Und wissen Sie, was mir am meisten geholfen hat? Das war zum einen, dass Sie mir von Anfang an immer wieder gesagt haben, dass es Lösungen für meine Probleme gibt, auch wenn ich die zuerst nicht sehen konnte. Zum anderen, dass Sie nie locker gelassen haben, egal, ob ich reagiert habe. Ich hatte immer das Gefühl, sie verstehen meine Angst und wollen diese nicht klein reden, wie ich es oftmals erfahre habe. Ich hatte das Gefühl, da ist eine Person, die sich wirklich interessiert und die da ist.

Ein ganz herzliches Dankeschön dafür.

Die Begleitung, die das Anti-Stalking-Projekt anbietet, ist daran orientiert, was die jeweiligen Betroffenen benötigen, um wieder in eine Stabilität zu kommen. Das braucht vor allem Zeit. Es zeigt sich immer wieder, wie wichtig es für die Frauen ist, dass sie jemanden im Hintergrund wissen, der über ihre Situation informiert ist, und ihnen zur Seite steht.

Ziele der Beratung und der Begleitung durch das Anti-Stalking-Projekt

Mich beschäftigt die Hilfslosigkeit und Ratlosigkeit von Betroffenen, die trotz umfassenden Dokumentationen und Anzeigen den Täter nicht stoppen können.

Wie bereits oben beschrieben, liegt es oftmals nicht in den Händen der Betroffenen oder der Unterstützer*innen das Stalking zu beenden. Aber jede einzelne Frau kann für sich festlegen, wieviel Platz oder welchen Stellenwert sie dem Stalking in ihrem Leben geben möchte und kann einzelne Schritte dagegen angehen. Dabei begleitet und unterstützt zu werden, ist eine große Hilfe und unabdingbar, damit sich die Frauen nicht wieder in Schuld- und Ohnmachtsgefühlen verlieren. Denn bei genauerem Hinsehen, und das gelingt den Betroffenen oftmals leichter in Begleitung des Anti-Stalking-Projekts, sehen wir und vor allem die Frauen selbst, dass es immer verschiedene Handlungsmöglichkeiten und jede Menge Ressourcen auf den verschiedensten Ebenen gibt.

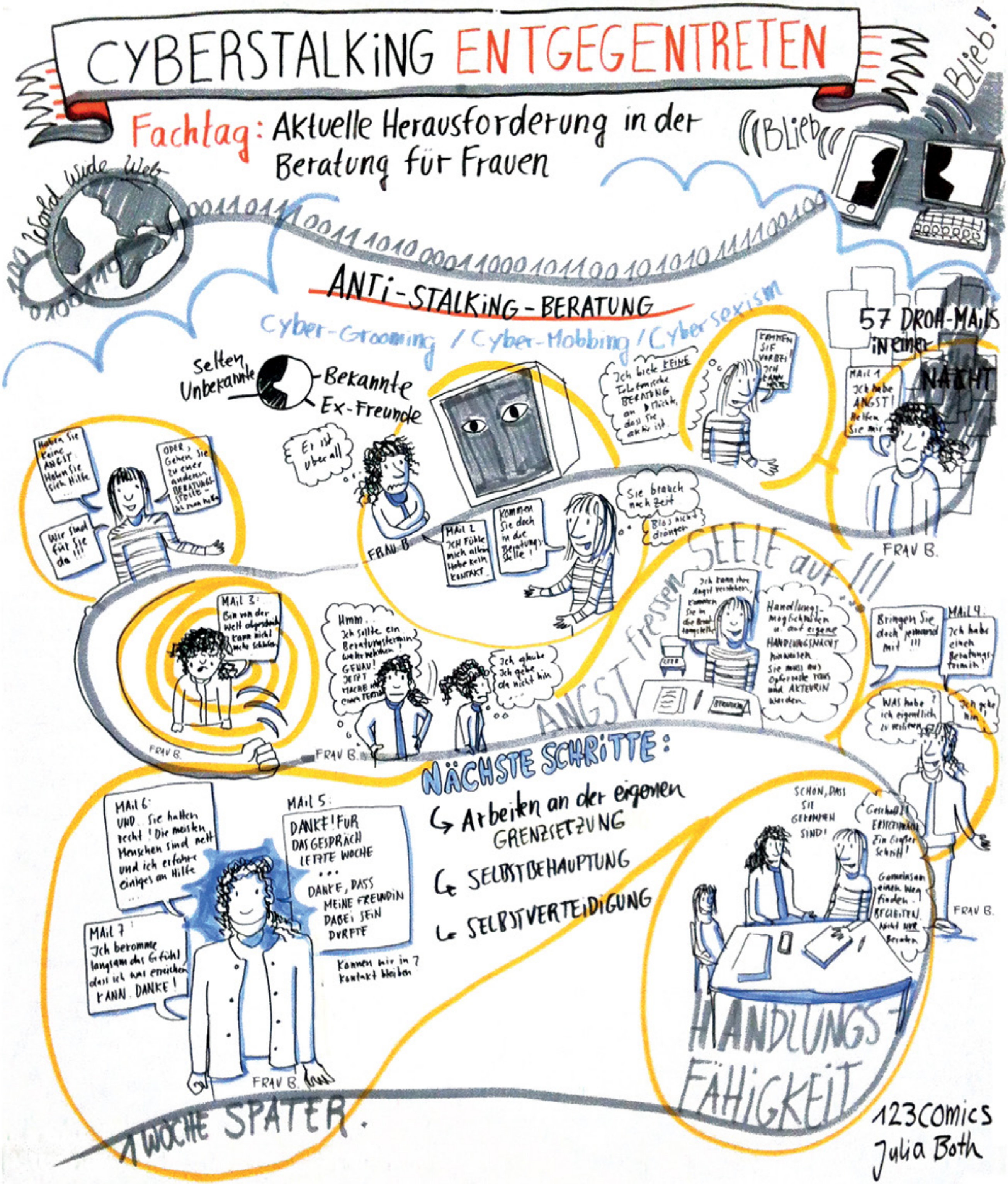
Oftmals verlieren die Betroffenen in den Stresssituationen, in denen sie sich aufgrund des Stalking befinden, den Zugang zu und den Glauben an sich selbst und an ihre Möglichkeiten. Hier unterstützend zu sein, sehen wir, neben der Information über die bestehenden Handlungsmöglichkeiten, als die zentrale Aufgabe in der Beratung und Begleitung. Die Frauen* sollen wieder einen Zustand erreichen, der sich gut für sie anfühlt, auch wenn das Stalking noch kein endgültiges Ende genommen hat. Das Anti-Stalking-Projekt des FRIEDA-Frauenzentrum e. V. berät und begleitet betroffene Frauen also bis zu dem Punkt, an dem sie wieder so stabil sind, dass sie ihr Leben selbst in der Hand haben.

Bei Cyberstalking ist ein weiteres wichtiges Ziel der Beratung, auch die positiven Seiten des Internets darzustellen.

Wir zeigen auf, wie ein souveräner, selbstbestimmter und angstfreier Umgang und eine solche Nutzung der zur Verfügung stehenden Medien aussehen kann. Dazu ziehen wir oftmals andere Fachfrauen hinzu.*

Wir kann ich andere dazu motivieren, aufmerksam im Umgang mit Daten zu sein?

Denn wer einmal Cyberstalking erfahren hat, verliert zeitweise das Vertrauen in das Internet und den Umgang damit. Aber heute gehören diese Medien zu unserem Alltag und halten viele Möglichkeiten der Teilhabe für uns bereit. Diese Möglichkeiten sollten allen Menschen zur Verfügung stehen und von uns allen nutzbar sein.


CYBERSTALKiNG ENTGEGENTRETEN
Fachtag: Aktuelle Herausforderung in der Beratung für Frauen
World Wide Web
Blieb
Blieb!
ANTi-STALKiNG-BERATUNG
Cyber-Grooming / Cyber-Mobbing / Cybersexism
Selten Unbekannte
Bekannte
Ex-Freunde
57 DROH-MAiLS in einer NACHT
MAiL 1 Jch habe ANGST! Helfen Sie mir
Haben Sie keine ANGST! Holen Sie sich Hilfe ...
ODER, Gehen Sie zu einer anderen BERATUNGSSTELLE
Wir sind für Sie da!!!
Er ist überall
FRAU B.
MAiL 2 JCH Fühle mich allein Habe kein KONTAKT.
Kommen Sie doch in die Beratungsstelle!
Sie braucht noch Zeit
Bloß nicht drängen
KOMMEN SIE VORBEI!
FRAU B.
MAiL 3: Bin von der Welt abgeschnitten kann nicht mehr schlafen
Hmm... Jch sollte ein Beratungstermin wahrnehmen! GENAU! JETZT
Jch glaube Jch gehe da nicht hin ...
FRAU B.
FRAU B.
ANGST fressen SEELE auf!!!
Jch kann ihre Angst verstehen, kommen Sie in die Beratungsstelle
Handlungsmöglichkeiten u. auf eigene HANDLUNGSMACHT hinweisen. Sie muss aus Opferrolle raus und AKTEURIN werden.
Bringen Sie doch jemand mit!!!
MAiL 4: Jch habe einen Beratungstermin!
WAS habe ich eigentlich zu verlieren?
FRAU B.
NÄCHSTE SCHRiTTE:
Arbeiten an der eigenen GRENZSETZUNG
SELBSTBEHAUPTUNG
SELBSTVERTEiDiGUNG
MAiL 5: DANKE! FÜR DAS GESPRÄCH LETZTE WOCHE ... DANKE, DASS MEINE FREUNDIN DABEi SEIN DURFTE
Können wir in Kontakt bleiben?
MAiL 6: UND.. Sie hatten recht! Die meisten Menschen sind nett und ich erfahre einiges an Hilfe ...
MAiL 7: Jch bekomme langsam das Gefühl dass ich was erreichen KANN. DANKE!
FRAU B.
SCHÖN, DASS SIE GEKOMMEN SIND!
Geschafft! Ein großer Schritt!
Gemeinsam einen Weg finden. BEGLEITEN, nicht nur Beraten
HANDLUNGS-FÄHiGKEiT
1 WOCHE SPÄTER.
123COMiCS Julia Both

Rechtliches Vorgehen

Effektives rechtliches Vorgehen gegen Cyberstalking anhand unterschiedlicher Begehungsformen[1]

Julia Wortmann, Rechtsanwältin

I. Einleitung

Dieser Beitrag erfolgt aus der Perspektive einer Rechtsanwältin, deren Fokus im Familienrecht und Teilbereichen des Sozialrechts sowie der Geschädigtenvertretung im Strafrecht liegt. Die Vertretung von Geschädigten im Bereich des Gewaltschutzes fokussiert sich zunehmend auch auf das Vorgehen gegen im weitesten Sinne digitale Gewalt. Hier ist festzustellen, dass speziell bei der sogenannten häuslichen Gewalt gegen Frauen*[2] digitale Gewalt eine immer größere Rolle spielt und immer neue Formen von Cyberstalking auftauchen. Die immer weiter fortschreitende Digitalisierung der menschlichen Kommunikation und Beziehungen bietet ein nahezu unerschöpfliches Feld für potentielle Täter*innen, die Betroffenen zu belästigen.

> Es kommen immer mehr Betroffene mit dem Thema Cybergewalt in die Beratung.

Für die erfolgreiche rechtliche Vertretung von Geschädigten von Cyberstalking ist die Arbeit der Fachberatungsstellen unverzichtbar, vor allem als erste Anlaufstelle und auch als Begleitung durch zum Teil sehr langwierige Verfahren.

Mandant*innen, die von Fachberatungsstellen kommen oder begleitet werden, sind in der Regel besser in der Lage mit den erheblichen Anforderungen, die ein rechtliches Vorgehen gegen Cyberstalking mit sich bringt, umzugehen. Sei es, dass die notwendige psychosoziale Begleitung geleistet wird, sei es, dass mit realistischen Erwartungen in das Verfahren gegangen wird oder sei es schlicht die Hilfestellung beim Ordnen und Katalogisieren der Tathandlungen. Diese Arbeit können wir als Rechtsanwält*innen oftmals schon aus zeitlichen Erwägungen nicht leisten.

Von Cyberstalking Betroffene müssen sich derzeit wegen der vielfältigen Begehungsmöglichkeiten durch einen Dschungel unterschiedlicher Rechtsbereiche kämpfen, um effektiven Rechtschutz zu erlangen. Dieser Beitrag soll einen Überblick über die Rechtsschutzmöglichkeiten verschaffen. Daher wird zunächst definiert, was Cyberstalking eigentlich rechtlich gesehen ist. Da bei Cyberstalking immer die Intimsphäre der Betroffenen verletzt wird, wird kurz erklärt, wie Persönlichkeitsrechte durch das Grundgesetz geschützt werden. Dann wird auf konkrete Handlungsmöglichkeiten eingegangen, die das Cyberstalking unterbinden können. Zunächst wird als schnellstes Mittel gegen Cyberstalking das Gewaltschutzgesetz (GewSchG)

> Welche rechtlichen Handlungs- und Schutzmöglichkeiten haben Betroffene aktuell?

[1] Begehungsformen von Cyberstalking sind zum Beispiel das Ausspionieren von Daten, Identitätsmissbrauch im Internet, das Überwachen einer anderen Person mittels GPS.

[2] Betroffen von Stalking sind in erster Linie Frauen* (vgl. www.globalviolence.org/2014/03/10/european-union-publishes-comprehensive-survey-ofviolence-against-women/). Dies spiegelt sich in meiner Mandantschaft.

vorgestellt und dessen Anwendung speziell bei Cyberstalking erläutert. Neben dem familiengerichtlichen Schutz über das Gewaltschutzgesetz ist immer zu prüfen, ob zur besseren Rechtsdurchsetzung auch zusätzlich weitere zivilrechtliche Abwehransprüche geltend gemacht werden können, diese werden im Anschluss daran kurz dargestellt. Auf der strafrechtlichen Ebene spielt der strafbewehrte Schutz von Persönlichkeitsrechten eine wichtige Rolle, da der eigentliche Stalking-Paragraph, § 238 Strafgesetzbuch (StGB), in vielen Fällen bei Cyberstalking nicht greift. Die relevanten Normen werden dargestellt.

Eine hohe Hürde bei wirksamen Schutz vor Cyberstalking besteht auch darin, dass es spezifisch für Cyberstalking sein kann, dass die Identität der stalkenden Person zunächst unbekannt ist oder diese ihre Identität verschleiert. Es werden im Abschnitt über das Ermittlungsverfahren Möglichkeiten aber auch Grenzen aufgezeigt, die Identität von Täter*innen zu ermitteln.

Als Fazit wird am Ende stehen, dass es in der sowieso schon belastenden Situation von den Betroffenen ein erhebliches und zu hohes Maß an eigenständigem Handeln und äußerst schnellen Reaktionen gefordert wird. Rechtlicher Schutz ist derzeit über das Gewaltschutzgesetz schneller und daher effektiver zu erlangen als durch ein Strafverfahren.

Es besteht jedoch gesetzgeberischer Handlungsbedarf, um Betroffenen umfassenden und einfach zu erlangenden Schutz vor weiteren Nachstellungen zu gewähren.

II. Was ist Cyberstalking?

In der rechtlichen Beratungspraxis bedeutet Cyberstalking: Das Bedrohen und/oder Nachstellen mittels sogenannter moderner Kommunikationsmittel. Dies ist die weitest mögliche Definition. Die unterschiedlichen Handlungsformen werden verschiedentlich in Unterbegriffe wie Cybermobbing, Cyberstalking, Depersonalisation etc. aufgeteilt. Dies ist für die rechtliche Betrachtung zunächst irrelevant. Unter die hier gewählte Definition des Cyberstalkings fallen sämtliche Handlungen wie Mobbing im Internet, das Erstellen von Fake-Profilen in sozialen Netzwerken, das Überschwemmen mit E-Mails, WhatsApp-Nachrichten oder SMS, die Ausspähung des Aufenthaltsortes, das Veröffentlichen von rufschädigenden Bildern im Internet, die betrügerische Verwendung von missbräuchlich erlangten Zugangsdaten und so weiter. Allen Varianten gemein ist, dass die Tatbegehung mit dem Ziel geschieht, der betroffenen Person nachzustellen bzw. diese einzuschüchtern.

> Wo beginnt strafrechtlich Cyberstalking?

Das in die digitale Welt verlagerte Stalking im Rahmen sogenannter häuslicher Gewalt oder nach Beendigung der Beziehung findet sich in nahezu jedem meiner spezifischen Beratungsfälle. Am Ende einer, oft auch sehr kurzen, Beziehung haben sich oft ganze Berge an persönlichen Daten angesammelt, die geeignet sind, erheblichen Schaden bei ehemaligen Partner*innen anzurichten. Hierbei kommen in nahezu jedem Fall Tatmittel wie E-Mail oder WhatsApp und Facebook zum Einsatz. Dies ist nur dann nicht der Fall, wenn im Einzelfall auf Seiten des Täters keinerlei Zugang zur digitalen Welt besteht. (Den Täter, der vor der Tür steht und Postkarten verschickt, gibt es durchaus auch noch.)

Der genderspezifische Aspekt bei Cyberstalking zum Nachteil von Frauen* besteht unter anderem in der oftmals sexistisch unterlegten Tathandlung. Hierunter fallen sexualisierte Drohungen, das Bloßstellen durch das Versenden von sexualisierten Bildern an Dritte, Profilerstellung und/oder Profilfälschung im Rahmen sozialer Netzwerke, auch mit sexualisiertem oder bedrohlichem Inhalt oder das Verfolgen der Geschädigten durch Tracking-Apps. Es verlagern sich also allgemeine Muster der analogen Gewaltanwendung gegenüber Frauen* in den virtuellen Raum. Ziel von Cyberstalking ist es, die Betroffene zu kontrollieren, sie bloßzustellen und zu bedrohen. Dies gelingt auch durch das massive Unsicherheitsgefühl, welches durch Stalking/Cyberstalking bei den Geschädigten hervorgerufen wird.

Der erhebliche Unterschied zu Tathandlungen in der analogen Welt ist die immer weiter fortwirkende Rechtsgutverletzung bei Cyberstalking. Eine von Angesicht zu Angesicht ausgesprochene Beleidigung ist mit dem Aussprechen beendet. Aber einmal im sozialen Netzwerk vorhandene Posts verschwinden nicht einfach. E-Mails an ein ganzes Adressbuch erreichen einen weiten Personenkreis. Die hier betroffenen Rechtsgüter, zum Beispiel das Recht auf sexuelle Selbstbestimmung oder der Schutz des höchstpersönlichen Lebensbereiches sind Rechtsgüter, die besonders sensibel sind und deren Verletzung gravierende Folgen bei den Geschädigten hinterlässt.

Daher ist seitens sämtlicher Akteure dafür Sorge zu tragen, das Cyberstalking vor allem schnell zu beenden.

Die Beendigung des Cyberstalkings ist auch der Wunsch der Mandant*innen. Nur selten steht an erster Linie der Wunsch nach Bestrafung oder Entschädigung.

III. Rechtsschutz bei Cyberstalking

Welche Handlungsstrategien und Interventionsmöglichkeiten gibt es im Umgang mit dem Tatbestand des Cyberstalkings?

Zunächst wird in diesem Beitrag die Grundlage jeglichen rechtlichen Schutzes bei Cyberstalking aufgezeigt. Im Folgenden werden dann zivilrechtliche und strafrechtliche Schutzmöglichkeiten herausgearbeitet, wobei jeweils gekennzeichnet ist, inwieweit im Hinblick auf unterschiedliche Formen von Cyberstalking nach der derzeitigen Rechtslage Schutzmöglichkeiten bestehen oder Defizite gegeben sind.

1. Der Schutz des Persönlichkeitsrechts

Bei dem Phänomen des Cyberstalkings ist aus rechtlicher Sicht nahezu ausnahmslos das sogenannte Allgemeine Persönlichkeitsrecht betroffen. Das Allgemeine Persönlichkeitsrecht ist ein absolutes umfassendes Recht gegenüber Jedermann auf Achtung der Menschenwürde und Entfaltung der individuellen Persönlichkeit. Es wird auf Art. 2 Abs. 1 Grundgesetz (GG), der die freie Entfaltung der Persönlichkeit schützt, in Verbindung mit Art. 1 Abs. 1 GG, dem Schutz der Menschenwürde, gestützt.[3] Es handelt sich bei den Tathandlungen also in der Regel um grundrechtsrelevante Eingriffe. Dabei entfaltet das Allgemeine Persönlichkeitsrecht nicht etwa seine Funktion als Abwehrrecht gegenüber Eingriffen des Staates gegenüber dem Bürger, sondern seine Schutzgebotsfunktion, wonach der Staat sich schützend vor es stellen und es vor Eingriffen Privater abschirmen muss.[4]

---

[3] vgl. Sodan in: Sodan, Grundgesetz, Becksche Kompakt Kommentare 2009, Art. 2, Rn. 5.

[4] J. Lange/Schmidbauer in: Herberger/Martinek/Rüßmann u.a., jurisPK-BGB, 7. Aufl. 2014, § 823, Rn. 28.

Das Allgemeine Persönlichkeitsrecht beinhaltet das Recht, selbst über Angelegenheiten zu bestimmen, die der Persönlichkeitssphäre zuzuordnen sind und im privaten Bereich in Ruhe gelassen zu werden, das heißt seine Privatsphäre freizuhalten von Einflüssen Dritter, und selbst zu bestimmen, mit welchen Personen und in welchem Umfang ein Kontakt gewünscht ist.[5]

Digitale Nachstellungen berühren also das Recht der Betroffenen, in Ruhe gelassen zu werden, und ihre Persönlichkeit im privaten und beruflichen Umfeld, in der Privat- und der Intimsphäre frei zu entfalten. Hierunter fallen zweifelsohne sämtliche denkbare Tathandlungen des Phänomens Cyberstalking.

2. Zivilrechtliche Maßnahmen

a. Einstweilige Anordnung nach dem Gewaltschutzgesetz

Das Gewaltschutzgesetz (GewSchG) ist 2002 in Kraft getreten. Zuständig für den Erlass von Anordnungen nach dem Gewaltschutzgesetz ist seit 2009 ausschließlich das Familiengericht. Es gelten die Verfahrensvorschriften des Zivil- und Familienrechtes. Bei Verstößen gegen eine einstweilige Anordnung kann das Familiengericht auf Antrag Ordnungsgeld oder sogar Ordnungshaft verhängen. Zudem sind Verstöße strafbar.

[5] Sprau in Palandt, BGB, 71. Aufl., § 823, Rn. 112 u.117.

Gewaltschutzgesetz (GewSchG) - Auszug

§ 1 Gerichtliche Maßnahmen zum Schutz vor Gewalt und Nachstellungen

(1) Hat eine Person vorsätzlich den Körper, die Gesundheit oder die Freiheit einer anderen Person widerrechtlich verletzt, hat das Gericht auf Antrag der verletzten Person die zur Abwendung weiterer Verletzungen erforderlichen Maßnahmen zu treffen. Die Anordnungen sollen befristet werden; die Frist kann verlängert werden. Das Gericht kann insbesondere anordnen, dass der Täter es unterlässt,

1. *die Wohnung der verletzten Person zu betreten,*
2. *sich in einem bestimmten Umkreis der Wohnung der verletzten Person aufzuhalten,*
3. *zu bestimmende andere Orte aufzusuchen, an denen sich die verletzte Person regelmäßig aufhält,*
4. ***Verbindung zur verletzten Person, auch unter Verwendung von Fernkommunikationsmitteln, aufzunehmen,***
5. *Zusammentreffen mit der verletzten Person herbeizuführen, soweit dies nicht zur Wahrnehmung berechtigter Interessen erforderlich ist.*

(2) Absatz 1 gilt entsprechend, wenn

1. *eine Person einer anderen mit einer Verletzung des Lebens, des Körpers, der Gesundheit oder der Freiheit widerrechtlich gedroht hat oder*
2. *eine Person widerrechtlich und vorsätzlich*

a) in die Wohnung einer anderen Person oder deren befriedetes Besitztum eindringt oder

b) eine andere Person dadurch unzumutbar belästigt, dass sie ihr gegen den ausdrücklich erklärten Willen wiederholt nachstellt oder sie unter Verwendung von Fernkommunikationsmitteln verfolgt.

Im Falle des Satzes 1 Nr. 2 Buchstabe b liegt eine unzumutbare Belästigung nicht vor, wenn die Handlung der Wahrnehmung berechtigter Interessen dient.

(3) In den Fällen des Absatzes 1 Satz 1 oder des Absatzes 2 kann das Gericht die Maßnahmen nach Absatz 1 auch dann anordnen, wenn eine Person die Tat in einem die freie Willensbestimmung ausschließenden Zustand krankhafter Störung der Geistestätigkeit begangen hat, in den sie sich durch geistige Getränke oder ähnliche Mittel vorübergehend versetzt hat.

Relevant für Cyberstalking ist vor allem § 1 Abs. 2 Nr. 2b GewSchG. Also die unzumutbare Belästigung durch Nachstellung oder der Verfolgung unter Verwendung von Fernkommunikationsmitteln. Nur in diesem Teilbereich des Gewaltschutzgesetzes ist ausnahmsweise das Allgemeine Persönlichkeitsrecht geschützt.[6] Auf die übrigen Varianten des Absatzes 1 wird hier nicht näher eingegangen. Sie ergeben sich aus dem Wortlaut des Gesetzes und sind typisch bei Gewaltanwendung im Beziehungskontext.

Eine nach dem Gesetzestext des § 2 Abs. 1 Nr. 2 b GewSchG unzumutbare Belästigung durch wiederholte Nachstellungen kann durch eine Vielzahl von Verhaltensweisen begangen werden (sog. „Stalking"). Außer der körperlichen Verfolgung, einer ständigen demonstrativen Anwesenheit des Täters in der Nähe des Opfers oder einer Beobachtung bzw. Überwachung fällt darunter auch die unerwünschte wiederholte Kontaktaufnahme durch Anrufe (Telefonterror), Briefe, Fax, E-Mail oder SMS.[7]

Inhalt der einstweiligen Anordnung sind Unterlassungsanordnungen wie sie in § 1 Abs. 1 Nr. 1-5 GewSchG beschrieben sind. Die Aufzählung des Gesetzes ist dabei nur beispielhaft. Es ist also immer schon bei der Antragstellung darauf zu achten, dass die tatsächliche Begehungsform, beispielsweise die Belästigung per Chatnachrichten, in den Antrag mit aufgenommen wird und als zu unterlassende Handlung beantragt wird.

Ist das GewSchG anwendbar bei Cyberstalking?

Bei dem Versenden von SMS, WhatsApp-Nachrichten und E-Mails direkt an Geschädigte ist das GewSchG unproblematisch anwendbar.

Hinsichtlich der Tatbegehung mittels sozialer Medien muss aber differenziert werden:

a) Bei Kontaktaufnahme von Täter*innen mittels Facebook oder anderer sozialer Netzwerke direkt an Geschädigte ist ebenfalls § 1 Nr. 2 b GewSchG anwendbar.

b) Das Erstellen von (Fake-)Accounts bei Facebook oder auch bei E-Mailanbietern und die anschließende Verbreitung diffamierender Inhalte über Geschädigte oder das sich als Geschädigte selbst Ausgeben, ohne sich direkt an die Geschädigte*n zu wenden, fällt derzeit nicht ohne weiteres unter das GewSchG, denn in aller Regel ergehen keine Gewaltschutzanordnungen, die die Begehungsvariante in

[6] Brudermüller in: Palandt, 73. Aufl., § 1 GewSchG Rn.4.
[7] Breidenstein in: Herberger/Martinek/Rüßmann u.a., jurisPK-BGB, 7. Aufl. 2014, § 1 GewSchG, Rn. 21.

Bezug auf Fake-Accounts gezielt beschreiben. Manchmal ist nebulös davon die Rede, der Antragsgegner habe auch die Kontaktaufnahme durch „das Internet“ zu unterlassen. Dies greift dann aber nicht, weil Täter*innen dann oft ja gerade keinen Kontakt mit Geschädigten aufnehmen, sondern mit Dritten. Geschädigte* sollten ausdrücklich beantragen, dass der/die Antragsgegner*in es zu unterlassen hat,Tatsachen oder Bildaufnahmen des höchstpersönlichen Lebensbereiches der/des Antragsteller*in für eine größere Zahl von Menschen wahrnehmbar zu machen. Eine ähnliche Formulierung befindet sich in dem neuen österreichischen Straftatbestand zu Cybermobbing, siehe § 107 c Strafgesetzbuch Österreich (StGB Ö).

Das Erstellen von Fake-Accounts kann aber auch strafrechtlich relevant sein und löst jedenfalls einen allgemeinen Unterlassungsanspruch nach §§ 1004 Abs. 1 S. 2 analog, 823 Abs. 1 Bürgerliches Gesetzbuch (BGB) bzw. Schadensersatzanspruch nach § 823 Abs. 2 BGB aus. Dieser ist allerdings als Verletzung des Allgemeinen Persönlichkeitsrechtes als Unterlassungs- bzw. Schadensersatzklage beim Zivilgericht anhängig zu machen.

Bei der Antragstellung bei dem Familiengericht, sei es durch Geschädigte selbst bei der Rechtsantragstelle des Familiengerichts oder durch die anwaltliche Vertretung, sind sämtliche Mittel zur Glaubhaftmachung mit dem Antrag einzureichen, also Screenshots, Ausdrucke, Fotos, Zeugenaussagen in Form einer eidesstattlichen Versicherung, eigene eidesstattliche Versicherung.

*Es ist unbedingt anzuraten, sich bei einer Fachberatungsstelle oder spezialisierten Rechtsanwält*innen dahingehend beraten zu lassen.*

b. Erlass und Zustellung der Anordnung

Liegen die eben genannten Voraussetzungen vor, erlässt das Familiengericht eine einstweilige Anordnung nach § 1 GewSchG, sofern die Handlung nicht der Wahrnehmung berechtigter Interessen dient. (Dies ist vor allem dann problematisch, wenn gemeinsame Kinder vorhanden sind und es um den Umgang geht; eine ausführliche Darlegung würde den Rahmen hier sprengen.)

Die einstweiligen Anordnungen ergehen in der Regel im Rahmen eines Eilverfahrens und werden, da im Eilverfahren nur ein vorläufiger Zustand geregelt werden soll, befristet. Der/die Antragsgegner*in kann nach Zustellung der einstweiligen Anordnung mündliche Verhandlung beim Familiengericht beantragen. Zu dieser Verhandlung haben zur Sachverhaltsaufklärung die Beteiligten zu erscheinen. Spätestens hier ist bei bedrohlichen Gegner*innen die anwaltliche oder psychosoziale Unterstützung erforderlich. Ebenso ist für den/die Antragsgegner*in die Möglichkeit der Beschwerde zum nächsthöheren Gericht (Oberlandesgericht bzw. Kammergericht in Berlin) gegeben.

Voraussetzung für den Erlass einer einstweiligen Anordnung ist immer, dass die Geschädigten den/die Täter*in eindeutig und nachweisbar aufgefordert hat, in Ruhe gelassen zu werden. Die Aufforderung ist entbehrlich, wenn sich aus den Vorfällen ergibt, dass die Handlungen unerwünscht sind. Dies ist insbesondere bei beleidigenden, bedrohenden und verleumderischen Inhalten gegeben.

Von immenser Bedeutung ist die ordnungsgemäße Zustellung der Anordnung.

Gesetzestext:

§ 214 Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit (FamFG): Einstweilige Anordnung

(1) Auf Antrag kann das Gericht durch einstweilige Anordnung eine vorläufige Regelung nach § 1 oder § 2 des Gewaltschutzgesetzes treffen. Ein dringendes Bedürfnis für ein sofortiges Tätigwerden liegt in der Regel vor, wenn eine Tat nach § 1 des Gewaltschutzgesetzes begangen wurde oder auf Grund konkreter Umstände mit einer Begehung zu rechnen ist.

(2) Der Antrag auf Erlass der einstweiligen Anordnung gilt im Fall des Erlasses ohne mündliche Erörterung ***zugleich als Auftrag zur Zustellung durch den Gerichtsvollzieher unter Vermittlung der Geschäftsstelle und als Auftrag zur Vollstreckung****; auf Verlangen des Antragstellers darf die Zustellung nicht vor der Vollstreckung erfolgen.*

Sollte die einstweilige Anordnung ohne anwaltliche Hilfe beantragt werden, ist unbedingt auf die Zustellung bei dem/der Antragsgegner*in zu achten. Das Familiengericht veranlasst die Zustellung von Amts wegen bei Erlass der Anordnung ohne mündliche Verhandlung. Dies wird aber leider manchmal nicht richtig gemacht, deshalb ist die einstweilige Anordnung notfalls selbst innerhalb eines Monats durch Gerichtsvollzieher*innen zustellen zu lassen.

Das Gericht teilt Anordnungen sowie deren Änderung oder Aufhebung der zuständigen Polizeibehörde und anderen öffentlichen Stellen, die von der Durchführung der Anordnung betroffen sind, unverzüglich mit. Die Mitteilung erfolgt vorsorglich, damit die Polizei bei Verstößen direkt tätig werden kann. Verstöße gegen die Anordnung teilt das Gericht jedoch nicht selbständig an die Polizei weiter, so dass hier jeweils unverzüglich Strafanzeige erstattet werden muss.

Fazit:

Sobald eine Gewaltschutz-Anordnung erwirkt werden kann, in der die im Einzelfall relevanten Begehungsformen beschrieben sind und die Anordnung wirksam zugestellt wurde, ist diese ein durchaus taugliches Mittel, um sich effektiv gegen Cyberstalking zu wehren. Die Möglichkeit bei Verstößen, Ordnungsgeld zu beantragen und die Möglichkeit, Strafanzeige zu stellen, machen die (einstweilige) Anordnung wegen der schnellen Durchsetzbarkeit zum derzeit effizientesten Mittel beim rechtlichen Vorgehen gegen Cyberstalking. Allerdings nur, wenn die Täter*innen durch diese Sanktionsformen derart „erreicht“ werden, dass sie das Cyberstalking beenden.

Wie wird der rechtliche Schutz vor Cyberstalking merkbar durchgesetzt?

Welche Nachhaltigkeit haben rechtliche und präventive Maßnahmen?

c. Weitere Unterlassungsansprüche

Aus einer Verletzung des Allgemeinen Persönlichkeitsrechts kann sich ein Anspruch auf Schadensersatz (§ 823 Abs. 1 BGB) oder ein Unterlassungsanspruch beziehungsweise Berichtigungsanspruch (§ 823 Abs. 1 i.V.m. § 1004 BGB) ergeben.[8] Zudem kann ein Anspruch auf Schmerzensgeld,

[8] vgl. Sodan in: Sodan, Grundgesetz, Becksche Kompakt Kommentare 2009, Art. 2, Rn. 5.

der aus § 823 I BGB i.V.m. Art. 1 I, 2 I GG abgeleitet wird, bestehen.

Einzelne Bereiche des Persönlichkeitsrechts sind gesetzlich besonders geschützt, beispielsweise die persönliche Ehre in den §§ 185 ff. StGB, das Recht am eigenen Bild (§§ 22 ff. Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie, KunstUrhG) oder das Urheberrecht (UrhG). Hierbei handelt es sich um besondere Persönlichkeitsrechte, deren Verletzung zu einem Anspruch auf Schadensersatz aus § 823 Abs. 2 BGB i.V.m. dem jeweils verletzten Schutzgesetz führen kann.

Cyberstalking und zivilrechtliche Unterlassungs- bzw. Schadensersatzansprüche

Hierzu zählen:

- das Verbreiten von unwahren oder sexualisierten Nachrichten oder sensiblen Daten der Geschädigten (auch an Dritte) über öffentliche Kommunikationsmedien,
- das Versenden von Nachrichten mit erschreckendem oder drohenden Inhalt an Geschädigte,
- das Annehmen einer falschen Identität bzw. der Identität der Geschädigten,
- der heimliche Einsatz von privaten Ortungsdiensten zum Ermitteln des aktuellen Aufenthaltsortes des/der Betroffenen*

Auch die Betreiber von Internetseiten sind haftbar zu machen. Sie können ebenfalls auf Unterlassung verklagt werden. Jedoch trifft Betreiber eine Prüfungspflicht erst dann, wenn sie Kenntnis von der Rechtsverletzung erlangen. Hierzu erklärt der Bundesgerichtshof: „Weist ein Betroffener den Betreiber (Host-Provider) auf eine Rechtsverletzung hin, ist dieser verpflichtet, zukünftig derartige Verletzungen zu verhindern, wenn der Hinweis hinreichend konkret ist. Er wird mithin erst dann zum Störer, wenn er trotz Kenntniserlangung den rechtsverletzenden Inhalt nicht löscht bzw. sperrt.[9]

Wie können Betreiber von sozialen Netzwerken und anderen Internetseiten auch in die Verantwortung gezogen werden?

Gibt es Präventionsmöglichkeiten seitens des Providers gegen Cyberstalking?

Für die derartige Rechtsverfolgung ist es ratsam, spezialisierte anwaltliche Hilfe in Anspruch zu nehmen, auch da sich die Niederlassungen der Betreiberfirmen oft im Ausland befinden und daher schon bei der Ermittlung des zuständigen Gerichtes Schwierigkeiten auftauchen können.

3. Strafrechtliche Maßnahmen

Es werden nun die relevanten Normen in Bezug auf Cyberstalking kurz erörtert. Im Allgemeinen lässt sich feststellen, dass der strafrechtliche Schutz hinsichtlich der Phänomene des Cyberstalkings sich recht umfassend tatbestandlich im Strafgesetzbuch abbilden lässt, wenn auch nicht gebündelt in einer Norm. Probleme zeigen sich eher im Hinblick auf die geringe Strafdrohung vieler einzelner Delikte. Dies wiederum zieht nach derzeitiger Rechtslage nach sich, dass wirksame Ermittlungsansätze zur Feststellung der Identität unbekannter Täter*innen nicht ergriffen werden können. Bei wegen Cyberstalking infrage kom-

Welche strafrechtlichen Folgen kann Cyberstalking haben?

Wie kann mit anonymen Angriffen, Hassmails etc. in sozialen Medien umgegangen werden?

[9] OLG Stuttgart, Beschluss vom 22. Oktober 2013 – 4 W 78/13 –, Rn. 23, juris; vgl. BGH GRUR 2012, 751 Tz. 20, juris

menden Delikten muss oft binnen drei Monaten zusätzlich zur Strafanzeige ein sogenannter Strafantrag gestellt werden. Wenn der Strafantrag fehlt, kann keine Strafverfolgung stattfinden, es sei denn, die Staatsanwaltschaft nimmt im Einzelfall ein besonderes öffentliches Interesse an der Strafverfolgung an. Dies geschieht meist nicht.

> Es ärgert mich, dass hier wieder ein Phänomen der Gewalt gegenüber Frauen* auftaucht, das die Geschädigten strafrechtlich gesehen im Regen stehen lässt.

a. § 4 Gewaltschutzgesetz (GewSchG)

§ 4 GewSchG
§ 4 Strafvorschriften

Wer einer bestimmten vollstreckbaren Anordnung nach § 1 Abs. 1 Satz 1 oder 3, jeweils auch in Verbindung mit Abs. 2 Satz 1, zuwiderhandelt, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft. Die Strafbarkeit nach anderen Vorschriften bleibt unberührt.

Für vorsätzliche und rechtswidrige Verstöße gegen eine gerichtliche Schutzanordnung nach § 1 GewSchG schafft § 4 GewSchG einen eigenständigen Straftatbestand. Strafbar ist aber genau genommen nicht das Stalking, sondern der Verstoß gegen die einstweilige Anordnung.

Wegen der Strafbewehrung ist insbesondere bei den Belästigungsverboten gemäß § 1 Abs. 2 Satz 1 Nr. 2 b GewSchG darauf zu achten, dass sie ausreichend bestimmt formuliert sind und die einstweilige Anordnung zugestellt wurde. Denn im Strafverfahren prüfen Amtsanwaltschaft und Gericht jeweils diese Voraussetzungen eigenständig.

Im Zuge der Reform des Nachstellungstatbestandes soll auch das GewSchG geändert werden. In Zukunft sollen nicht nur gerichtliche Anordnungen sondern auch Vergleiche strafbewehrt sein. Dies ist eine aus Opferschutzgesichtspunkten unbedingt zu begrüßende Änderung, da sehr viele Gewaltschutzverfahren mit einem Vergleich enden. Nach derzeitiger Rechtslage sind Verstöße gegen Vergleiche nicht strafbewehrt und (wenn sie nicht gerichtlich durch Beschluss gebilligt werden) auch nicht mit Ordnungsmitteln zu ahnden.

b. § 238 Strafgesetzbuch (StGB)

§ 238 StGB: Nachstellung

(1) Wer einem Menschen unbefugt nachstellt, indem er beharrlich

1. *seine räumliche Nähe aufsucht,*
2. ***unter Verwendung von Telekommunikationsmitteln oder sonstigen Mitteln der Kommunikation oder über Dritte Kontakt zu ihm herzustellen versucht,***
3. *unter **missbräuchlicher Verwendung von dessen personenbezogenen Daten** Bestellungen von Waren oder Dienstleistungen für ihn aufgibt oder Dritte veranlasst, mit diesem Kontakt aufzunehmen,*
4. *ihn mit der Verletzung von Leben, körperlicher Unversehrtheit, Gesundheit oder Freiheit seiner selbst oder einer ihm nahe stehenden Person bedroht oder*

5. eine andere vergleichbare Handlung vornimmt *und dadurch seine Lebensgestaltung schwerwiegend beeinträchtigt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.*

(2) Auf Freiheitsstrafe von drei Monaten bis zu fünf Jahren ist zu erkennen, wenn der Täter das Opfer, einen Angehörigen des Opfers oder eine andere dem Opfer nahe stehende Person durch die Tat in die Gefahr des Todes oder einer schweren Gesundheitsschädigung bringt.
(3) Verursacht der Täter durch die Tat den Tod des Opfers, eines Angehörigen des Opfers oder einer anderen dem Opfer nahe stehenden Person, so ist die Strafe Freiheitsstrafe von einem Jahr bis zu zehn Jahren.
(4) In den Fällen des Absatzes 1 wird die Tat nur auf Antrag verfolgt, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

Im Grundtatbestand des Absatzes 1 werden vier konkret bezeichnete Handlungsalternativen und ein sog. Auffangtatbestand beschrieben. Tathandlungen, die Cyberstalking betreffen, sind unter § 238 Abs. 1 Nr. 2 StGB, „unter Verwendung von Telekommunikationsmitteln oder sonstigen Mitteln der Kommunikation oder über Dritte Kontakt herzustellen versucht“ zu fassen. Diese Begehungsvariante schildert die unerwünschte Kontaktaufnahme auch über Dritte. Unter den Auffangtatbestand des § 238 Abs. 1 Nr. 5, wer „eine andere vergleichbare Handlung vornimmt“ können wohl Sachverhalte wie gefälschte Webseiten, beleidigende Foreneinträge oder Verleumdungen im Internet fallen. Diese Ansicht ist aber durchaus umstritten. Denn ganz grundsätzlich legen Rechtsprechung und auch strafrechtliche Literatur den Anwendungsbereich des Nachstellungstatbestandes sehr eng aus. Dies sei aufgrund der Vielzahl von unbestimmten Rechtsbegriffen erforderlich.

Zur Erfüllung des Tatbestandes müssen jedoch auch die übrigen Voraussetzungen für den Tatbestand der “Nachstellung” erfüllt sein, die Handlung muss also unbefugt und beharrlich erfolgen und zudem das Opfer in seiner Lebensführung schwerwiegend beeinträchtigen.

Unter „Nachstellen“ im Sinne des § 238 Abs. 1 StGB ist eine Annäherungshandlung zu verstehen, die darauf gerichtet ist, in den persönlichen Lebensbereich des Tatopfers einzugreifen und seine Entschließungs- und Handlungsfreiheit zu beeinträchtigen. Der Straftatbestand dient dem Schutz der eigenen Lebensführung vor gezielten, hartnäckigen und schwerwiegenden Belästigungen der Lebensgestaltung.[10]

“Beharrlichkeit” im Sinne des § 238 StGB liegt vor, wenn eine wiederholte Begehung erfolgt ist, welche subjektiv unter Missachtung des entgegenstehenden Willens des Tatopfers ausgeübt wurde und die Absicht besteht, sich auch in Zukunft entsprechend zu verhalten.[11]

Der Stalking-Straftatbestand ist als sogenanntes Erfolgsdelikt ausgestaltet. Voraussetzung ist eine “schwerwiegende Beeinträchtigung der Lebensgestaltung”. Diese ist dann gegeben, wenn es beim Tatopfer zu erzwungenen gravierenden Veränderungen der Lebensumstände gekommen ist. Entscheidend sind hier die Umstände des Einzelfalls.[12]

---

[10] Mosbacher, NStZ 2007, 665.
[11] vgl. BGH, Beschluss vom 19.11.2009, 3 StR 244/09, juris.
[12] Fischer, StGB, 59. Aufl., § 238 Rn. 21.

Reformbedarf

Hier wird also auf das Verhalten der Geschädigten abgestellt. Dies hat zur Folge, dass für Geschädigte, die besonders „wehrhaft“ sind, also zum Beispiel keine nachweisbaren psychischen Schädigungen davontragen oder diese nicht nach außen darstellen wollen oder aber finanziell gar nicht in der Lage sind, die geforderten einschneidenden Lebensveränderungen wie zum Beispiel einen Umzug vorzunehmen, wegen Nachstellung im Sinne des StGB kein strafrechtlicher Schutz greift.

> Mich beschäftigt die Begrenztheit juristischer Möglichkeiten.

Hier sind Reformbemühungen der Bundesregierung im Gange, es gibt einen Gesetzentwurf der Bundesregierung, der vorsieht, den Tatbestand in ein Gefährdungsdelikt umzuwandeln und die Auffangklausel des Nr. 5 zu streichen.[13]

Zu begrüßen ist sicherlich das Vorhaben, dass es in Zukunft genügen soll, wenn die Tathandlung geeignet ist, die Lebensweise schwerwiegend zu beeinträchtigen. Nicht Realität werden sollte die geplante Abschaffung des § 238 Abs. 1 Nr. 5 StGB.

Schon Sachbeschädigungen fallen dann nicht mehr unter § 238 StGB. Ganz zu schweigen von den Formen digitaler Gewalt, die wir uns jetzt noch gar nicht ausdenken können.

[13] http://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_Stalking.pdf?__blob=publicationFile&v=1, zuletzt abgerufen am 09.09.2016.

c. Weitere strafrechtliche Normen

Cyberstalking ist je nach Konstellation nach § 238 StGB oder folgenden Normen strafbar:

- § 44 Bundesdatenschutzgesetz (BDSG): Strafbarkeit der missbräuchlichen Nutzung personenbezogener Daten
- § 185 StGB: Beleidigung, § 186 StGB: Verleumdung, § 187 StGB: üble Nachrede, Strafantragserfordernis jeweils in § 194 StGB
- § 201a StGB: Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen, Strafantragserfordernis in § 205 StGB,
- § 202 a StGB: Ausspähen von Daten, Strafantragserfordernis in § 205 StGB
- § 263 a StGB: Computerbetrug, Strafantragserfordernis in § 263 Abs. 4 StGB
- § 269 StGB: Fälschung beweiserheblicher Daten
- § 270 StGB: Täuschung im Rechtsverkehr bei Datenverarbeitung

Reformbedarf

Letztlich besteht eine umfassende Strafbarkeit hinsichtlich der angesprochenen Delikte.

Das Problem stellt sich meiner Ansicht nach nicht darin, dass die einzelnen Cyberstalkinghandlungen heute nicht strafbar wären, das Problem ist das teilweises Strafantragserfordernis, auch beim Nachstellungsgrundtatbestand, und eine sehr geringe Strafdrohung der geschilderten Normen.

Die Folge hiervon ist oftmals die Einstellung der Verfahren mangels Strafantrag, mangels Tatnachweis oder wegen Geringfügigkeit. Die erhebliche Rechtsgutverletzung rechtfertigt aber meiner Meinung nach durchaus eine höhere Strafandrohung. In Österreich wurde zum Jahresbeginn 2016 ein eigener Cybermobbingtatbestand (§ 107 c StGB Ö) eingeführt, diese Möglichkeit sollte hier auch diskutiert werden.

Gesetzestext § 107 c StGB Ö: Fortgesetzte Belästigung im Wege einer Telekommunikation oder eines Computersystems

§ 107c. (1) Wer im Wege einer Telekommunikation oder unter Verwendung eines Computersystems in einer Weise, die geeignet ist, eine Person in ihrer Lebensführung unzumutbar zu beeinträchtigen, eine längere Zeit hindurch fortgesetzt

1. eine Person für eine größere Zahl von Menschen wahrnehmbar an der Ehre verletzt oder

2. Tatsachen oder Bildaufnahmen des höchstpersönlichen Lebensbereiches einer Person ohne deren Zustimmung für eine größere Zahl von Menschen wahrnehmbar macht,
ist mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 720 Tagessätzen zu bestrafen.

(2) Hat die Tat den Selbstmord oder einen Selbstmordversuch der im Sinn des Abs. 1 verletzten Person zu Folge, so ist der Täter mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

4. Prozessuale Fallstricke im Ermittlungsverfahren

Durch die Ausgestaltung des § 238 Abs. 1 StGB als Vergehenstatbestand und das in Abs. 4 geregelte Strafantragserfordernis und die geringe Strafdrohung werden die Tatbestände meist nur der leichteren Kriminalität zuzuordnen sein. Ermittlungsmaßnahmen wie Telefonüberwachung oder Erhebung von Verkehrsdaten sind so meist nicht möglich.

Ein weiteres Problem stellt die Dauer der Ermittlungsverfahren dar.

Bis es zu einer Verurteilung kommt, vergeht oft ein Jahr. Teilweise besteht schon bei der Anzeigenaufnahme ein Problem. Leider werden die Geschädigten gerade bei Belästigungen im Internet oft nicht ernst genommen. Zudem ist die Ermittlungsarbeit bei Fällen von Stalking/Cyberstalking sehr mühsam. Oftmals müssen über einen gewissen Zeitraum nahezu täglich Strafanzeigen aufgenommen werden. Hier mangelt es oft an klaren Hinweisen an die Betroffenen, dass zusätzlich zur Stellung von Strafanzeigen jedes Mal ein Strafantrag innerhalb von 3 Monaten zu stellen ist.

Ein weiteres erhebliches Problem liegt darin, die Täter*innen auch zu ermitteln. Dies ist nicht nur in Fällen von unbekann-

ten Täter*innen erforderlich, auch bei den Geschädigten bekannten Täter*innen muss jeder Einzelfall den Täter*innen zuzuordnen sein. Technisch ist dies möglich. Rechtlich und tatsächlich nur teilweise.

Seit der Neuregelung der Vorratsdatenspeicherung Ende 2015 werden die Rufnummern der beteiligten Anschlüsse sowie Zeitpunkt und Dauer des Anrufs gespeichert. Eine Verpflichtung hierzu für Telefonanbieter und Internetprovider findet sich in § 113 b Telekommunikationsgesetz (TKG). Bei Mobilfunk werden auch die Standortdaten gespeichert. Ebenso werden IP-Adressen einschließlich Zeitpunkt und Dauer der Vergabe einer IP-Adresse vorgehalten. Diese Verkehrsdaten werden im Telekommunikationsgesetz genau bezeichnet. E-Mails sind aber von der Speicherung ausgenommen. Kommunikationsinhalte ohnehin. Die Speicherfrist von Daten ist auf zehn Wochen beschränkt: Unmittelbar nach Ablauf der Speicherfrist müssen sie gelöscht werden. Standortdaten dürfen nur vier Wochen gespeichert werden. IP-Adressen nach der Rechtsprechung nur 7 Tage. Auf die Verkehrsdaten darf nur zugegriffen werden, um schwerste Straftaten zu verfolgen, die auch im Einzelfall schwer wiegen müssen. Erfasst werden insbesondere terroristische Straftaten und Straftaten gegen höchstpersönliche Rechtsgüter, insbesondere Leib, Leben, Freiheit und sexuelle Selbstbestimmung. Diese werden in einem eigenen Katalog festgelegt. Zugriffe auf Daten durch Polizei oder Staatsanwaltschaft erfordern immer einen richterlichen Beschluss.

Hier stehen sich Positionen recht unversöhnlich gegenüber. Einerseits bestehen Forderungen von Geschädigten und Strafverfolgungsakteuren – wie zum Beispiel die des Bundes deutscher Kriminalbeamter –, dass zwingend der Straftatenkatalog auf solche Delikte ausgeweitet werden muss, die unter Nutzung von Internet oder Telekommunikationsmitteln begangen werden. Andererseits gibt es berechtigte Befürchtungen von Datenschützer*innen, die Datenspeicherung auf Vorrat als Angriff auf die Freiheit des Einzelnen ablehnen.

*In Fällen, in denen der Täter tatsächlich unbekannt ist, muss das Dilemma zwischen Datenschutz und dem nachvollziehbaren Interesse an Kenntnis über die Erlangung der Identität der Täter*innen in Zukunft aufgelöst werden.*

Ein effektives Mittel, um eventuell das Cyberstalking früh zu stoppen, sind aus strafrechtlicher Sicht (je nach Einzelfall) Gefährder*innenansprachen durch die Polizei. Manche Täter*innen lassen sich durchaus durch eine frühe Ansprache durch die Staatsgewalt von weiteren Taten abhalten. Hierzu ist es weiterhin nötig, Strafanzeigen zu stellen. Auch nach Erlangung einer Gewaltschutzanordnung sollte bei Verstößen unbedingt konsequent Strafanzeige gestellt werden.

> Gibt es Erfahrungen, ob polizeiliche Gefährderansprachen dazu beitragen, Cyberstalking zu beenden?

IV. Fazit

Reformbedarf

Da das Strafrecht erst eingreift, wenn die Tat schon begangen ist, und eine Verurteilung oft erst Monate, wenn nicht Jahre nach der Tat erfolgt und auch zivilrechtliche Klagen oft lange Zeit beanspruchen, ist es aus Gründen des effektiven Opferschutzes erforderlich, die vielgestaltigen Erscheinungsformen des Cyberstalkings sämtliche unter das Gewaltschutzgesetz fallen zu lassen. Hierzu könnte § 1 des Gewaltschutzgesetzes um ein Regelbeispiel Cyberstalking (mit sicherlich noch zu diskutierendem Inhalt) erweitert werden. Weiterhin wäre es sehr sinnvoll, einen Löschungsanspruch oder Beseitigungsanspruch im Gewaltschutzgesetz zu verankern. Dieser könnte gegen die/den Antragsgegner*in gerichtet werden, als Verpflichtung solche öffentlichen Inhalte entfernen zu lassen. Für die Geschädigten* wäre dies eine eindeutige Erleichterung, da sie sich nicht weiter mühsam durch sämtliche weitere zivilrechtliche Unterlassungsansprüche wühlen müssten, sondern einmal in Gestalt der einstweiligen Anordnung ein taugliches Werkzeug zur Hand hätten, die andauernde Rechtsgutverletzung zu beseitigen.

Zudem müssen Betreiber von Blogs, sozialen Medien etc. in die Pflicht genommen werden.

Es muss für Nutzer*innen einfach und schnell möglich sein, Persönlichkeitsrechtverletzungen löschen zu lassen.

Sehr wichtig ist die weitere Sensibilisierung der Ermittlungsbehörden.

Die Einrichtung von Ansprechpersonen bei Polizei und Staatsanwaltschaft, die im Internet auch so benannt werden, wäre ein wichtiger Schritt für Geschädigte und Ermittelnde.

Wer hilft bei Cyberstalking?
Welche Anlaufstellen gibt es?

Es ist in der Beratungspraxis zuvorderst auf tatsächlicher Ebene durch geeignete Maßnahmen für die Sicherheit der Geschädigten zu sorgen.

*Hierbei ist die Stärkung der Medienkompetenz der Geschädigten wie auch der Mitarbeiter*innen der Fachberatungsstellen unerlässlich.*

Dies muss durch entsprechend finanzierte Fortbildungsangebote geschehen. Den Reformbestrebungen im Strafrecht in Bezug auf § 238 StGB im Sinne der Umwandlung in ein Gefährdungsdelikt ist zuzustimmen. Jedoch sollte gerade aus dem Blickwinkel der Cybergewalt § 238 Abs. 1 Nr. 5 StGB nicht gestrichen werden. In Zukunft sollte aber intensiv die Schaffung eines Straftatbestandes des Cybermobbings diskutiert werden.

Es muss aber klar sein, dass eine wirksame Strafverfolgung im Sinne des Zugriffes der Ermittlungsbehörden auf Verkehrs- und Bestandsdaten von Betreibern von Internetseiten auch bei Delikten, die nur eine geringe Strafandrohung haben, mit erheblichen Grundrechtseinschränkungen für uns alle einhergehen.

Sicher im Web unterwegs

Strategie und Technik kennen und in Beratungssituationen vermitteln

Vera Kätsch
EDV- und IT-Beraterin, Durchblick GmbH

Seit 2010 gibt es in Berlin eine kostenlose Computerberatung für Frauen. Das Projekt BER-IT bietet diese Beratung sechsmal im Monat[1] an. Die Empfehlungen und Hinweise im Text sind aus der Computerberatung heraus entstanden. Die dort gesammelten Erfahrungen haben mich dazu gebracht, zwischen Technik und Strategie zu unterscheiden. Eine Kollegin, die nicht nur als IT-Dozentin, sondern auch als Selbstverteidigungstrainerin arbeitet, hat es treffend formuliert:

„Es reicht nicht aus, Kampf- und Abwehrtechniken zu erlernen, ich muss auch trainieren, gefährliche Situationen zu erkennen und mich mental darauf vorbereiten."

In Computerberatungen kann ich klar benennen, welche technischen Schutz-Maßnahmen für einen Computer, ein Notebook, Tablet oder Smartphone notwendig sind. Wesentlich komplexer sind Fragen nach einer Nutzungsstrategie. Dazu muss eben bei jeder einzelnen Nutzerin angesetzt werden: Welche Software, welchen Dienst wählt die Nutzerin? Zu welchem Zweck? Mit welchem Grad an Medienkompetenz? Was sind ihre Vorstellungen von Privatheit und Datenschutz?

> Wie kann man sich schützen?

Ich möchte in diesem Beitrag die wichtigsten Technikpunkte zuerst benennen, Strategiefragen umreißen und Maßnahmen für den Notfall darstellen. Eingebaut habe ich zudem Fragen, die in Beratungssituationen zum Thema Cyberstalking gestellt werden müssen. Einige Quellen zur Vertiefung sind am Ende aufgelistet.

Vorneweg noch eine Bemerkung: Im April 2016 haben fünfzig Vertreterinnen und Vertreter aus Zivilgesellschaft, Wissenschaft, Wirtschaft und Verwaltung auf einer Tagung in Lohmar die Frage diskutiert, wie eine Informationsgesellschaft zugleich smart und sicher sein kann.[2] Es wurden sieben Thesen erarbeitet, zwei davon möchte ich hier zitieren und damit zeigen, dass wir mit dem Fachtag „Cyberstalking entgegentreten – aktuelle Herausforderung in der Beratung für Frauen*" auf dem richtigen Weg sind:

[1] Donnerstags von 14.00 bis 16.00 Uhr am Standort UCW in der Sigmaringer Straße 1 in 10713 Berlin und jeden 2. und 4. Freitag am Standort BER-IT am Kottbusser Damm 79 in 10967 Berlin.

[2] Alle weiteren Thesen am Ende dieses Beitrags und auf www.bsi-fuer-buerger.de

These 1:
Informationssicherheit ist nicht nur eine technische, sondern eine politische und gesellschaftliche Frage, die einer interdisziplinären Betrachtung bedarf.

Wie kann über die Gefahren des Internet aufgeklärt werden, ohne dass den Betroffenen von Cybergewalt eine Schuld zugeschrieben wird? Was kann die Politik tun?

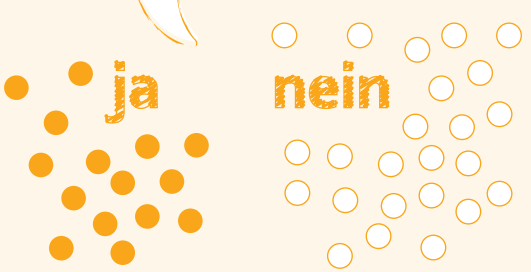
These 4:
Informationssicherheit ist ein aktives, gesamtgesellschaftliches Generationenprojekt mit lebenslangem Lernen.

Hier auf dem Fachtag „Cyberstalking entgegentreten – aktuelle Herausforderung in der Beratung für Frauen*“ sitze ich als IT-Fachfrau zwischen PädagogInnen, SozialarbeiterInnen, RechtsanwältInnen, Gleichstellungsbeauftragen, Angestellten aus dem Polizeidienst und Menschen anderer Profession. Unser gemeinsames Thema ist „Cyberstalking“ und allen Anwesenden scheint deutlich zu sein, dass es mit nur einer Tagung oder einer Fortbildung zu dem Thema nicht getan ist.

Sicherheitsfragen – vor allem im Bereich IT – müssen immer wieder neu gestellt und beleuchtet werden.

Ich bin hier, weil ich mich stärker zum Thema informieren und vernetzen möchte.

Internet Security - gibt es die auch auf Ihrem Tablet und/oder Smartphone?



I. Technik

Mit Technik, genauer Informationstechnik oder kurz IT, meine ich hier Hardware, Software und unsere Zugangswege ins Internet. Über grundlegende Sicherheitsmaßnahmen vor allem für die Software (Programme oder Apps), die wir nutzen, kann nicht diskutiert werden. Im Folgenden liste ich auf, was zum Pflichtprogramm in Sachen Sicherheit gehört. Diese Punkte sind eigentlich nicht verhandelbar. Nun gibt es allerdings ganz unterschiedliche Sicherheitsbedürfnisse. In Firmen sind die Sicherheitsanforderungen anders ausgeprägt als im privaten Bereich und im privaten Bereich treffe ich auf sehr individuelle Vorstellungen von Privatsphäre und Datenschutz. Also kann es sein, dass Sicherheitsmaßnahmen nicht immer gleich streng befolgt oder umgesetzt werden.

Nicht eingehen kann ich hier auf „gesellschaftliche“ Aspekte und Risiken. Schlagzeilen zum Thema Datenschutz, Überwachung und Privatsphäre verunsichern viele NutzerInnen. Irritiert hat mich in vielen Computerberatungen, dass Teilnehmerinnen einen oft angst-starren Blick auf Nachrichten aus diesem Bereich haben, der eigenen Computersicherheit aber nur einen Bruchteil ihrer Aufmerksamkeit widmen. Verweigerung und Nicht-Teilnahme kann nicht unser Ziel sein.

NutzerInnen müssen unterschiedliche Bedrohungen kennen und einschätzen können, Sicherheitsmaßnahmen sinnvoll einsetzen und sich souverän an digitalen Kommunikationsprozessen beteiligen.

Welche technischen Möglichkeiten des Selbstschutzes gibt es?

Grundlegende Maßnahmen

Grundlegende Maßnahmen gelten für alle Nutzerinnen, egal welche Hardware (PC, Notebook, Tablet, Smartphone) oder welches Betriebssystem (Windows, Mac OS oder Android) zum Einsatz kommt.

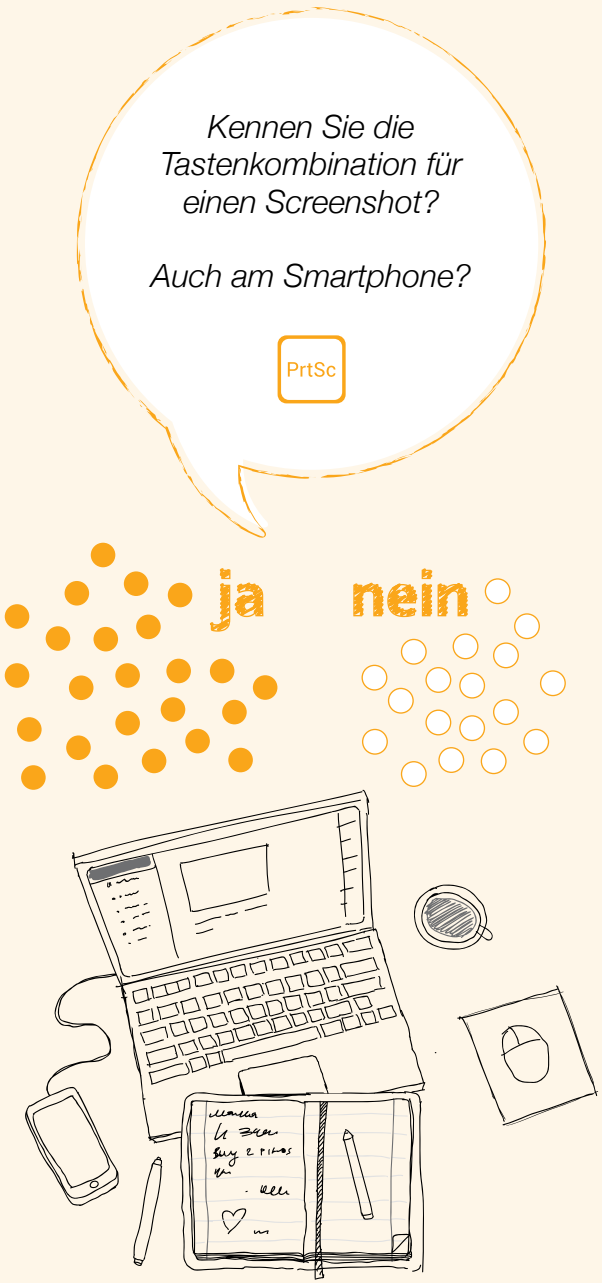
Einen 100%igen Schutz gibt es nicht. Veränderungen, Neuerungen und auch neue Bedrohungen gehören zu unseren IT- und Online-Aktivitäten. Wir können Risiken einschränken und müssen sie im Blick behalten.

Welche konkreten technischen Schutzmaßnahmen kann ich ergreifen, um kein Opfer von Cyberstalking zu werden?

Internet Security / Firewall

Jede Hardware benötigt ein aktuelles Schutzprogramm – Anti-Virus und Internet Security. Es gibt kostenlose Angebote aus dem Web; so ein Programm sollte mindestens installiert werden. Empfehlenswert sind kostenpflichtige Programme, die in der Regel schneller aktualisiert werden und einen breiteren Schutz (z.B. für E-Mail-Programme und Online-Banking) bieten. Aus den Computerberatungen heraus haben sich oft kleine Nutzerinnengemeinschaften gebildet, die recht kostengünstig gemeinsam Pakete mit Mehrfach-Lizenzen nutzen.

Eine Firewall kontrolliert eingehende und ausgehende Verbindungen, prüft Anfragen ins Internet und eingehende Daten. Sie schützt die Hardware und das eigene Netzwerk gegen Angriffe von außen. Eine Firewall ist in vielen Betriebssystemen bereits integriert. Einige Internet Security Programme enthalten eine zusätzliche Firewall.



Aktuelle Software

Für jede Hardware benötigen wir Software. Neben dem Betriebssystem nutzen wir die unterschiedlichsten Programme oder Apps. Haben Sie einen Überblick? Welche Software, welche Apps – und welche Version – sind auf einem Gerät vorhanden? Gibt es Programme oder Apps, die nie oder andere, die regelmäßig genutzt werden? Sind die Programme, die auf einem System benötigt werden, bekannt? Oft finde ich auf Computern Programme, die – vor vielen Jahren und in guter Absicht – installiert wurden, aber nie benutzt werden.

Hier gilt es, aufzuräumen. Nicht benutzte Programme stellen eine Sicherheitslücke dar und sind zudem oft eine ungesunde Grundlage für Mutmaßungen, weil nicht mehr erinnert wird, wann, wieso, zu welchem Zweck und vor allem von wem das Programm installiert wurde. Je weniger „ungenutzte“ Programme und Apps installiert sind, desto kleiner ist die Angriffsfläche des gesamten Systems. Installieren Sie nur Programme aus einer zuverlässigen Quelle und deinstallieren Sie alle Programme, die nicht benötigt werden.

Regelmäßige Updates

Dass ein veraltetes Betriebssystem, z.B. Windows XP, zu einem Sicherheitsrisiko werden kann, war zum aktuellen Umstieg auf Windows 10 sogar in der Tagespresse zu lesen. Betriebssystem, Browser, Anwendungsprogramme und Apps müssen immer auf dem neuesten Stand sein, Updates also automatisch installiert werden. Nur so werden frisch erkannte Sicherheitslücken geschlossen. Updates „wegdrücken“, weil es gerade nicht passt oder ich mich noch nicht mit der Notwendigkeit auseinandergesetzt habe, ist fahrlässig.

PC-Benutzerkonten

Wird ein Computer von mehreren Personen genutzt, dann sollten unterschiedliche Benutzerkonten – auch mit unter-

schiedlichen Berechtigungen – angelegt werden. So kann jede einzelne Nutzerin Programm-Einstellungen einrichten und Daten individuell speichern. Eingeschränkte Berechtigungen erschweren unbemerkte oder ungewollte Installationen. Diese Vorgehensweise kann auch für Einzelnutzerinnen hilfreich sein: ein Benutzerkonto mit eingeschränkten Rechten kann zusätzlichen Schutz beim Surfen im Web bieten. Allerdings sind unterschiedliche Benutzerkonten kein sicherer Schutz für individuelle Daten. Versierte Nutzerinnen/Administratorinnen können auf die Daten anderer Benutzerkonten zugreifen.

Datensicherung und Datenverwaltung
Ein Computer hält nicht ewig. Daten, die dort gespeichert sind, sollten regelmäßig auf einen externen Datenträger oder ein sicheres Cloud-Laufwerk übertragen werden. Hardware und Software können Sie ersetzen. Daten, Texte in die Sie viel Arbeit investiert haben, Fotos, die Sie gesammelt haben, können im Schadensfall unwiederbringlich verschwinden.

Finden Sie Ihre Daten auf Anhieb oder suchen Sie oftmals nach Bildern, Texten oder anderen Dateien? Wenn eine Dateiablage einem Irrgarten gleicht, dann muss nicht nur viel Zeit in die Suche gesteckt werden, sondern es entsteht schnell der Eindruck von Kontrollverlust. Finde ich eine Datei nicht oder hat jemand die Datei gelöscht? Vermeiden Sie „unaufgeräumte“ Ordner, speichern Sie Daten nicht in mehrfachen Versionen und halten Sie sich an einmal festgelegte Ordnerstrukturen.

Im Web unterwegs

Internet-Zugang
In der Regel wird der Internet-Zugang über einen Router hergestellt. Im heimischen Router wird das WLAN eingerichtet und mit einem Verschlüsselungsverfahren und einem Passwort gesichert. Sie legen fest, wer diese Zugangsdaten erhält und Ihren Internetzugang mit benutzen darf.

Mit mobilen Geräten nutzen wir nicht nur das eigene, heimische WLAN, sondern öffentliche Hotspots oder Access Points (so werden WLAN-Zugänge in öffentlichen Netzwerken genannt) in Internetcafés, Hotels oder öffentlichen Einrichtungen. Viele unserer mobilen Geräte speichern diese Zugangsdaten, wenn sie einmal erfolgreich eingerichtet sind. Dann werden diese Verbindungen automatisch hergestellt, wenn ich mit meinem mobilen Gerät in der Nähe des Hotspots bin. Aber wie schalten Sie den automatischen Zugang wieder ab? Wer nutzt noch diesen öffentlichen Internetzugang? Welche Daten sind in diesem öffentlichen Netzwerk sichtbar? Wer kann auf die Daten zugreifen?

Diese Fragen können für öffentliche Netzwerke nicht immer beantwortet werden. Deshalb sollten Sie lernen, die WLAN-Einstellungen an mobilen Geräten zu steuern. Web-Aktivitäten mit privaten oder sensiblen Daten sind bei der Nutzung öffentlicher Netze nicht zu empfehlen.

Browser
Browser sind Programme, die wir nutzen, um Webseiten aufzurufen: Internet Explorer, Edge, Mozilla Firefox oder Google Chrome. Neueste Versionen zu nutzen und regelmäßige Updates tragen erheblich zur Sicherheit bei. Zudem sollte

ich sichere Nutzungsmöglichkeiten und Systemeinstellungen in meinem Browser kennen:

- Wie nutze ich einen Browser, ohne Spuren zu hinterlassen – genannt Private- oder Inkognito-Browsersitzungen?
- Welche Einstellungen zum Datenschutz nehme ich vor?
- Möchte ich ein „No tracking“ aktivieren, damit meine Aktivitäten nicht nachverfolgt werden können?
- Möchte ich eine Chronik der besuchten Webseiten erstellen lassen?
- Sollen meine Anmeldungen und Kennworte gespeichert werden?
- Wie gehe ich mit PopUp-Fenstern um?
- Was mache ich mit Cookies?
- Welche AddOns und PlugIns habe ich installiert?
- Und wie halte ich sie aktuell?

Wie Sie diese ganzen Einstellungen steuern, ist von Ihren sehr persönlichen Vorlieben und Sicherheitsbedürfnissen abhängig. Je höher Ihre Anforderungen an die Sicherheit sind, umso weniger „bequem“ wird sich das Surfen auf unterschiedlichen Webseiten gestalten. Haben Sie beispielsweise die Cookies ausgeschaltet, werden Sie sich bei einigen Online-Händlern gar nicht mehr anmelden können. Haben Sie die PopUps blockiert, können Sie auf einigen Lern-Webseiten keine Übungsaufgaben trainieren. Sie müssen also nicht nur die Browsereinstellungen steuern, sondern ggf. auch vorher über das Ziel bei Ihrem Ausflug ins WorldWideWeb nachdenken.

„Technik-Fragen“ in der Beratungssituation

Nun habe ich die ersten wichtigen Punkte zum Thema Sicherheit benannt. In den Computerberatungen realisieren viele Kundinnen, dass Sicherheit nicht in wenigen Minuten einmal eben abgehandelt werden kann. Einige fassen dann den Plan, diese Punkte durch regelmäßige Besuche der Computersprechstunde zu bearbeiten.

- Aber wie kann das in einer Frauenberatungsstelle, wo die Ratsuchende den Verdacht von Cyberstalking mitbringt, umgesetzt werden?
- Wie kann eine Beraterin dort die Technik der Kundin überprüfen?
- Können Fehlfunktionen bei Hard- oder Software ausgeschlossen werden?
- Können Fehler in der Nutzung und Anwendung ausgeschlossen werden?
- Können Fehlinterpretationen (Meldungen, Mails …) ausgeschlossen werden?
- Wie kann eine Beraterin die Medienkompetenz der Kundin beurteilen?

> Wie berate ich betroffene Frauen*? Woran erkenne ich Cyberstalking? Was sind die ersten Angriffe?

Zur Beantwortung dieser Fragen setzte ich auf die interdisziplinäre Zusammenarbeit, auf die gesammelte Kompetenz und Erfahrung der Teilnehmerinnen und Teilnehmer dieses Fachtags.

II. Strategie

Wie kann man sich als aktive Nutzer*in der Medien effektiv schützen?

Zu einer Strategie gehört, dass Sie sich vorher mit der Technik (Hardware, Software und Internetzugang) und all den Aktionen und Aktivitäten, die Sie dann damit durchführen möchten, beschäftigen. Das bedeutet, die Ziele anzuvisieren, zu bedenken, was dazu notwendig ist (Anmeldungen, Zugänge, Daten) und die Risiken dabei zu beachten. Das hört sich gut an, doch was heißt das konkret in der Umsetzung? Wir gehen das an einem praktischen Beispiel durch: Sie möchten mit Ihrem neuen Smartphone E-Mails empfangen und verschicken. Das Ziel ist damit klar umrissen und mit den Sicherheitsmaßnahmen aus dem vorherigen Kapitel hätten Sie auch schon einige Risiken in den Griff bekommen. Weiter notwendig ist: Um ein Smartphone oder iPhone zu nutzen, müssen Sie für das Gerät einen Internetzugang organisiert haben, einen Account zur Nutzung des Betriebssystems angelegt haben, die Zugangsdaten für Ihren E-Mail-Account parat haben und die Adressen vom Posteingangsserver und Postausgangsserver kennen.

Accounts = Digitale Konten

Bei vielen Aktivitäten im Web benötigen wir digitale Konten, auch Accounts genannt. Egal ob Sie sich bei einem Online-Händler anmelden, um dort einzukaufen, ob Sie Bücher in einer öffentlichen Web-Bibliothek ausleihen möchten oder ob Sie sich an einem sozialen Netzwerk beteiligen möchten – ohne Registrierung ist kein Zugang möglich. Allein die einfache Nutzung von Smartphones oder Tablets setzt immer einen Account voraus. Möchten Sie ein iPhone nutzen, müssen Sie sich in der iCloud von Apple anmelden. Haben Sie ein Smartphone mit Android, wird ein Google-Konto vorausgesetzt.

Konten sind ein zentraler Bereich, wenn es um Sicherheit geht: Konten enthalten sensible Daten, z. B. meine Adresse, Kontaktdaten oder Bankdaten, um Zahlungen zu tätigen. Sie enthalten meist viele private Daten, z. B. die gesamte E-Mail-Korrespondenz, alle Einkäufe bei einem Online-Händler oder meine Profil-Einstellungen für ein soziales Netzwerk.

Wenn die Zugangsdaten zu einem Konto anderen Personen bekannt sind oder in einem öffentlichen Netzwerk „abgegriffen“ oder einfach gestohlen werden, ist das eine folgenschwere Bedrohung. Hier seien nur einige Schäden genannt, die entstehen können: falsche E-Mails werden in meinem Namen verschickt, verleumderische oder rufschädigende Inhalte werden in sozialen Netzwerken verbreitet, falsche Bestellungen werden unter meinem Namen getätigt.

Accounts dokumentieren

Allein die Frage nach unterschiedlichen Konten, nach einer Benutzerkennung – das ist in der Regel eine E-Mail-Adresse - und dem dazugehörigen Kennwort, bringt viele Nutzerinnen ins Schwitzen. Dass es hilfreich sein kann, die unterschiedlichen Anmeldungen zu notieren, fällt oft erst in „Notsituationen“ auf.

Um es vermeintlich leichter zu machen, wählen Nutzerinnen für neue Konten gerne die bereits vorhandene E-Mail-Adresse. Das empfehle ich nicht! Ich finde es sehr übersichtlich, wenn meine Personalausweisnummer nicht identisch ist mit meinem Bankkonto oder meiner Mitgliedsnummer im Sportverein. Wenn eine Anmeldung – womöglich noch mit dem immer gleichen Passwort – für alle möglichen Konten genutzt wird, dann haben Datendiebe ein leichtes Spiel.

Hier noch ein paar Tipps zu digitalen Konten:
Nutzen Sie zu jeder Anmeldung einen anderen Anmeldenamen. Damit haben Sie vielleicht eine größere Sammlung von E-Adressen, können diese aber eindeutiger einem Konto zuordnen. Und zudem bündeln Sie nicht so viele Informationen an einer E-Mail-Adresse und bei einem Anbieter.

Dokumentieren Sie ihre Konten. Die Fortschrittlichen nutzen vielleicht einen Passwortsafe – ein Programm, in dem Sie alle Zugänge und Kennworte speichern. Die Bodenständigeren werden eventuell ein kleines – gut verstecktes – Heft haben und dort alle Infos eintragen.

Sichere Passworte
Zu Accounts und digitalen Konten gehört das leidige Thema „Passwort"… es ist nervig, aber wirklich sicherheitsrelevant.

Ein gutes, sicheres Passwort hat folgende Merkmale:
- es hat mindestens acht Zeichen,
- enthält Groß- und Kleinbuchstaben,
- Ziffern und Sonderzeichen, es lässt sich nicht aus ihrem Namen (oder dem nahestehender Personen) oder dem Geburtsdatum ableiten
- es ist für jedes Konto unterschiedlich – also kein Generalschlüssel für alle Konten
- es wird regelmäßig verändert

Mit jedem Merkmal, das Sie berücksichtigen, wird es für ein „Passwort-Knackprogramm" schwieriger, Ihr Passwort herauszufinden. Im besten Fall benötigt so ein Programm schon einmal paar Wochen, um dann das richtige Passwort zu ermitteln.

Hilfreich kann eine Strategie zum Anlegen von Passworten sein: Denken Sie sich zu einem Account einen „Leitsatz" aus, kombinieren Sie ihn mit Ziffern und Sonderzeichen und schon haben Sie ein recht sicheres Passwort, zum Beispiel:

Ich **e**sse **t**äglich **O**bst **u**nd **G**emüse**!**2016 ergibt=**IetOuG!2016**

In folgenden Situationen ist Ihr Passwort bedroht:

Sie haben die oben genannten Merkmale nicht berücksichtigt.

Sie geben Anmeldedaten in einem öffentlichen Netzwerk ein.

Phishing (Phishing = Passwort + „fischen"):
Sie beantworten eine Mail, in der Sie um Ihre Zugangsdaten gebeten werden oder geben Ihre Zugangsdaten auf einer gefälschten Webseite ein.

Es befindet sich ein Spähprogramm oder ein Key-logger auf dem Computer oder dem Smartphone, Ihre Eingaben werden heimlich protokolliert und weitergegeben.

Besteht der Verdacht, dass ein digitales Konto auch von einer anderen Person genutzt wird, sollten Sie von einem anderen, vertrauenswürdigen Platz aus das Passwort ändern und den eigenen Computer oder das Smartphone überprüfen.

Einstellungen
Die Überschrift „Einstellungen“ hat hier eine doppelte Bedeutung und macht noch einmal deutlich, dass jede Nutzerin eine Strategie benötigt: Zum einen meine ich Systemeinstellungen oder das Profil, das ich in jedem Account bearbeiten kann. Dort können Sie Ihr Kennwort ändern, Datenschutzbestimmungen kontrollieren und – das ist vor allem in sozialen Netzwerken wichtig – Einstellungen zur Privatsphäre vornehmen. Zum anderen meine ich persönliche Einstellungen, die Überlegungen im Vorfeld, die zwingend notwendig sind. Welche Daten will ich veröffentlichen? Mit welchem Ziel? Wer kann die Daten einsehen (Freunde, Bekannte, Arbeitgeber, Vermieter)? Kann ich die Daten löschen? Welche Konsequenzen hat eine Veröffentlichung jetzt oder in zehn Jahren für mich?

Wenn Sie ein digitales Konto anlegen, klären und überprüfen Sie folgende Punkte:

- Legen Sie ein neues Konto nicht auf einem Computer oder Smartphone in einem öffentlichen Netzwerk an. Nutzen Sie ein sicheres Gerät.
- Kennen Sie die allgemeinen Geschäftsbedingungen und die Regelungen zum Datenschutz für den neuen Account? Welche Rechte haben Sie an ihren eigenen Bildern und Daten, nachdem die einmal hochgeladen sind?
- Überdenken Sie grundsätzlich, wann Sie in einem Profil Ihren wirklichen Namen, Adressdaten oder eine Telefonnummer eingeben.
- Gehen Sie sparsam mit privaten Daten um. Wenn Sie sich irgendwo anmelden, schränken Sie einen Zugriff auf Ihre Daten ein, füllen Sie selber nur Pflichtfelder in Formularen aus.
- Legen Sie sich mehrere E-Mail-Adressen zu, die keinen direkten Rückschluss auf persönliche Daten geben. Legen Sie sich – da wo Sie keine rechtsverbindlichen Aktivitäten

betreiben – eine Adresse mit Künstlernamen zu. Benutzen Sie Nicknames!
- Nutzen Sie Privatsphäre-Einstellungen, nicht jeder sollte Ihre Profildaten lesen können.

Für alles, was Sie in sozialen Netzwerken veröffentlichen, gilt: „Think before you post“

Beachten Sie die Sicherheitsregeln zu E-Mails und Anhängen. Laden Sie kein Adressbuch hoch, geben Sie Ihr Adressbuch nicht frei, kontrollieren Sie Kontakte und Kontaktanfragen. Prüfen Sie jede Kontaktaufnahme mit einem gesunden Maß an Skepsis und Vorsicht.

Löschen Sie Ihre Daten, wenn Sie aus einem Netzwerk aussteigen oder einen Account nicht mehr nutzen. Aber bedenken Sie auch, dass Ihre Daten bereits kopiert und auf einem anderen Server – auf den Sie keinen Zugriff haben – liegen können.

„Strategie-Fragen“ in der Beratungssituation

Gerade bei der Nutzung von Smartphones und Tablets musste ich leider in vielen Computerberatungen feststellen, dass Teilnehmerinnen ihre Konten gar nicht selbst eingerichtet hatten und in einigen Fällen noch nicht einmal die Zugangsdaten kannten. Bekannte, Verwandte, nette Verkäufer haben das für sie erledigt. Nach Wochen oder Monaten erinnern sich diese Menschen vielleicht nicht an den Vorgang oder das Verhältnis zu der Person ist angespannt und lässt eine Rückfrage zum digitalen Account nicht zu. Hier sind die technischen Möglichkeiten begrenzt, ein solches Konto darf eigentlich nicht mehr weiterverwendet werden.

In einer Beratungssituation zum Thema Cyberstalking muss die Frage nach digitalen Konten gestellt werden. Zugang, Nutzung und Veröffentlichungen müssen thematisiert werden. Als IT-Beraterin konzentriere ich mich auf die technischen Aspekte. Bei einem Verdacht auf Cyberstalking befindet sich die Ratsuchende oft in einer psychischen Ausnahmesituation. Das kann in der IT-Beratung nicht aufgefangen werden.

Wohin sollen sich Opfer von Cyberstalking als erstes wenden?

In der Zusammenarbeit unterschiedlicher Beraterinnen und Beratungsstellen sehe ich die einzig mögliche, adäquate Herangehensweise.

Zur Klärung müssen folgende Fragen gestellt werden:

Wer hat den Router, den WLAN-Zugang eingerichtet?
Welche Netzzugänge – private und öffentliche – nutzt die Kundin?
In welchen sozialen Netzwerken ist die Kundin aktiv?
Sind die Einstellungen zu Privatheit und Datenschutz bekannt?
Welche Konten nutzt die Kundin? Sind diese dokumentiert?
Wer hat die Konten eingerichtet, wer kennt die Zugangsdaten?
Gibt es einen Plan für Passworte?
Werden sichere Passworte genutzt?
Werden unterschiedliche Passworte genutzt?
Sind Passworte schon einmal geändert worden?

III. Plan für Notfall

Ich wünsche mir für jede betroffene Person, die sich einer Notsituation befindet, von Cyberstalking betroffen ist oder die einfach nur bemerkt, dass ihre Lücken in Sachen Medienkompetenz zu einer Gefährdung werden können, eine angemessene Hilfestellung.

> Welche konkreten Ansprechpartner*innen für mein persönliches Cyberstalking-Problem gibt es in Berlin?

Wünschenswert ist, dass Beratungsstellen Checklisten, Adressen von spezialisierten Anlaufstellen und genügend personelle Ressourcen bereithalten können.

Schaden feststellen & begrenzen
Zuerst gilt es, alle digitalen Konten – vor allem diejenigen, über die ein finanzieller Schaden entstanden ist oder entstehen könnte – zu überprüfen. Die Zugangsdaten sollten geändert werden. Können Sie sich nicht mehr anmelden, hilft eventuell noch die Funktion „Passwort zurücksetzen“. Wenn Sie auch dabei auf Probleme stoßen, weil Sie auf die Referenz-E-Mail-Adresse nicht zugreifen können, sollten Sie umgehend den Kundensupport kontaktieren.

Fälle von Mobbing oder Stalking-Versuche sollten umgehend dem Betreiber des Netzwerkes gemeldet werden.

In gravierenden Fällen sollte eine Anzeige bei einer Polizeidienststelle erfolgen.

Beweissicherung
Screenshots – auch hardcopies genannt – sollten von jeder verdächtigen Bildschirmseite angelegt werden. Googeln Sie die Tastenkombination, die einen Screenshot in Ihrem Betriebssystem auslöst und wie Sie den Screenshot dann speichern können.

Legen Sie sich einen gesonderten USB-Stick zu, auf dem Sie alle Beweise sichern. Führen Sie dort auch Protokoll über alle verdächtigen Aktionen.

Holen Sie – wann immer es möglich ist – eine zweite Person mit an den Bildschirm.

IV. Hier finden Sie weitere Informationen

Welche Leitfäden, Checklisten und Übersichten zu Internetsicherheit gibt es schon?

Webseiten

www.bsi-fuer-buerger.de
BSI für Bürger ist ein kostenloses Informationsangebot des Bundesamtes für Sicherheit in der Informationstechnik. Sie finden dort viele Hinweise und Checklisten.

www.sicher-im-netz.de
DsiN (Deutschland sicher im Netz) veröffentlicht regelmäßig Leitfäden, Studien, Flyer für Unternehmen und Verbraucher sowie Erklärfilme und Pocket-Seminare mit praktischen Anleitungen zum sicheren Umgang mit dem Internet.

www.klicksafe.de
Eine EU-Initiative für mehr Sicherheit im Netz - c/o Landeszentrale für Medien und Kommunikation (LMK) Rheinland-Pfalz. Webseite mit Materialien, Infos, Lerneinheiten für Kinder, Eltern und Lehrende.

Bücher und Broschüren

Mein Recht im Netz: Der Ratgeber für die digitale Selbstbestimmung. Peter Apel/Stiftung Warentest.

Daten schützen und sichern, in: Ratgeber Verbraucherschutz kompakt. Guter Rat in Alltagsfragen. Presse und Informationsamt der Bundesregierung, 11044 Berlin. 2015. S. 168-185. (https://www.bundesregierung.de/Content/Infomaterial/BPA/Bestellservice/Ratgeber_Verbraucherschutz_2015.pdf?__blob=publicationFile&v=5)

7 Thesen des Bundesamts für Sicherheit in der Informationstechnik (BSI)

These 1:	Informationssicherheit ist nicht nur eine technische, sondern eine politische und gesellschaftliche Frage, die einer interdisziplinären Betrachtung bedarf.
These 2:	Es muss eine gesamtgesellschaftliche Debatte zur Sicherheitsverantwortung in der Informationsgesellschaft geführt werden.
These 3:	Die Motivation sich um Informationssicherheit zu kümmern braucht keine moralischen Appelle, sondern positive Anreize.
These 4:	Informationssicherheit ist ein aktives, gesamtgesellschaftliches Generationenprojekt mit lebenslangem Lernen.
These 5:	Fehler sind menschlich; Informationssicherheit braucht technische und organisatorische Resilienz und Fehlermanagement.
These 6:	Informationssicherheit und Benutzerfreundlichkeit müssen Hand in Hand gehen.
These 7:	Informationssicherheit soll ein wichtiger Faktor werden, sodass jeder für die eigenen Daten bestimmen kann, wer was mit diesen Daten macht.

Quelle: https://www.bsi.bund.de/DE/Presse/Kurzmeldungen/Meldungen/news_worldcafe_21042016.html?nn=6722622, letzter Zugriff am 09.09.2016

Ergebnisse des Fachtags:

Forderungen und Handlungsbedarfe zur Stärkung der Betroffenen von Cyberstalking

Cyberstalking ist eine gesamtgesellschaftliche Herausforderung:

Cyberstalking muss als gesamtgesellschaftliches Problem wahrgenommen und es muss entsprechend darauf reagiert werden. Cyberstalking darf nicht als individuelles Problem betrachtet werden und im Privaten verbleiben. Es gibt neben der Schuld des Täters auch eine gesellschaftliche Verantwortung.

Für die weitere Arbeit wären nach Gewaltformen differenzierende und intersektional angelegte Studien zu Cybergewalt wichtig. Gleichzeitig können bereits jetzt die Beobachtungen und statistisch erfassten Daten der im Feld Tätigen – beispielsweise von Frauen*beratungsstellen – als Grundlage genommen werden. Auch die vorliegende Dokumentation belegt, dass Gewalt gegen Frauen* durch Cyberstalking zunimmt und eine zusätzliche Dimension erfährt.

Entsprechend sollte eine Sensibilisierung der breiten Öffentlichkeit zu Cyberstalking erfolgen. Einerseits, um präventiv gegen Cyberstalking vorzugehen, andererseits, damit davon Betroffene auf ein sensibilisiertes Umfeld treffen, das sie unterstützt.

Mehr Medienkompetenz für Frauen*:

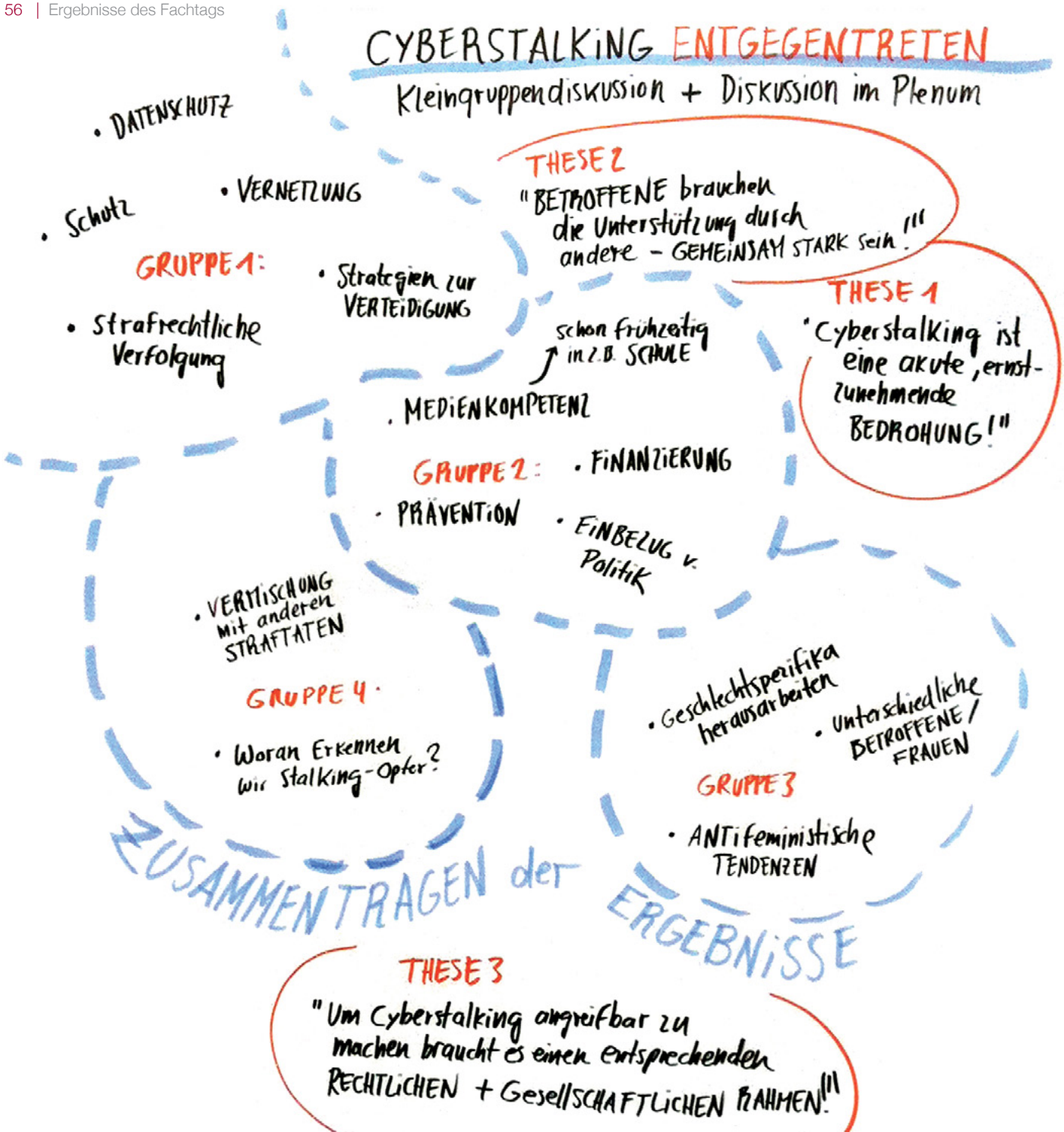
Alle Frauen* müssen die Möglichkeit bekommen, sich mehr Medienkompetenz anzueignen, die auch Internetsicherheit abdecken muss. Weiterbildungsmöglichkeiten müssen zeitnah zu den immer wieder neu entstehenden digitalen Herausforderungen gegeben sein.

Bessere Ausstattung der Beratungs- und Anlaufstellen gegen Gewalt gegen Frauen*:

Um die Vereinzelung der durch Cyberstalking Betroffenen zu durchbrechen, sind dezentral angelegte und niedrigschwellig zu erreichende parteilich arbeitende Anlaufstellen wichtig. Diese gibt es schon jetzt. Die vorhandene Infrastruktur und Fachkompetenz erfüllen eine wichtige gesellschaftliche Aufgabe. Das muss öffentlich bekannt sein und wertgeschätzt werden, nicht zuletzt deshalb, damit auch die noch immer schambehaftete Hürde, eine solche Beratung in Anspruch zu nehmen, möglichst niedrig gestaltet ist.

Die bereits bestehenden Frauen*computerberatungsstellen müssen ausgebaut und finanziell abgesichert werden.

Die vorhandene Infrastruktur gegen Gewalt gegen Frauen* muss gestärkt werden. Eine über einen längeren Zeitraum abgesicherte ausreichende Finanzierung ist zu gewährleisten, damit kontinuierliche Beratungs- und Begleitangebote möglich sind.


CYBERSTALKING ENTGEGENTRETEN
Kleingruppendiskussion + Diskussion im Plenum
THESE 2
"BETROFFENE brauchen die Unterstützung durch andere – GEMEINSAM STARK sein!"
THESE 1
"Cyberstalking ist eine akute, ernstzunehmende BEDROHUNG!"
GRUPPE 1:
• DATENSCHUTZ
• VERNETZUNG
• Schutz
• Strategien zur VERTEIDIGUNG
• Strafrechtliche Verfolgung
schon frühzeitig in z.B. SCHULE
• MEDIENKOMPETENZ
GRUPPE 2:
• FINANZIERUNG
• PRÄVENTION
• EINBEZUG v. Politik
GRUPPE 4:
• VERMISCHUNG mit anderen STRAFTATEN
• Woran Erkennen wir Stalking-Opfer?
GRUPPE 3
• Geschlechtsspezifika herausarbeiten
• unterschiedliche BETROFFENE / FRAUEN
• ANTIfeministische TENDENZEN
ZUSAMMENTRAGEN der ERGEBNISSE
THESE 3
"Um Cyberstalking angreifbar zu machen braucht es einen entsprechenden RECHTLICHEN + GESELLSCHAFTLICHEN RAHMEN!"

Den Berater*innen müssen Weiterbildungsmöglichkeiten gegeben werden, damit sie ein fundiertes Basiswissen zum Thema Internetsicherheit aufbauen können und damit sie auf neu entstehende Herausforderungen adäquat reagieren können.

Darüber hinaus müssen diesen Beratungsstellen genügend finanzielle Mittel für eine technische Ausstattung zur Verfügung gestellt werden, damit vor Ort mit den Klient*innen Nutzer*innenstrategien erarbeitet und Wege der Umsetzung gemeinsam erprobt werden können.

Ergänzt werden sollte diese Struktur durch Fachstellen, die den Themenkomplex Cybergewalt mit einem intersektionalen Blick fokussieren und mit entsprechendem Fachpersonal ansprechbar sind. Diese müssen in jedem Fall auch analog erreichbar sein. Viele Betroffene nutzen digitale Kommunikationsmittel nicht (mehr).

Ausbau von Unterstützungsnetzwerken und von Vernetzung:

Wünschenswert wäre es, dass ein Unterstützungsnetzwerk für von Cyberstalking Betroffene weiter entwickelt wird. Die Beendigung von Cyberstalking kann ein langer Prozess sein, an dem unterschiedliche Fachkräfte und Unterstützer*innen Hand in Hand arbeiten sollten. Gefragt sind dabei die bereits benannten Akteure: Beratungsstellen, Hilfsangebote für Frauen* gegen Gewalt, Anwält*innen, Prozessbegleiter*innen, Mediziner*innen, Therapeut*innen und entsprechende Abteilungen der Polizei und der Gerichte, Fachfrauen* für Internetsicherheit und Medienkompetenz sowie Angebote zur Stabilisierung und Selbstermächtigung der Betroffenen.

Die Vernetzung von Expert*innen der verschiedenen Bereiche ist anzustreben, um das vorhandene Wissen auszutauschen, weiterzutragen und bei Bedarf schnell gemeinsam handeln zu können.

Die bereits begonnene Spezialisierung und Sensibilisierung bei Ermittlungsbehörden muss weitergeführt und ausgebaut werden.

Die unterschiedlichen Ansprechpersonen der verantwortlichen Stellen müssen klar benannt werden. Kontaktmöglichkeiten müssen transparent und leicht zugänglich sein.

Für die Unterstützung der Betroffenen gegen Cyberstalking und gegenüber dem Täter ist es von großer Bedeutung, dass die Frauen* wieder ihren Raum bekommen. Dies wird durch parteiliche Arbeit geleistet.

Handlungsbedarfe auf rechtlicher Ebene:

Geltendes Recht muss an digitale Besonderheiten angepasst werden, damit Recht auch im Cyberspace zeitnah durchsetzbar ist. Eine konsequente Strafverfolgung ist nötig.

Die Ermittlungsarbeiten bei Fällen von Stalking und Cyberstalking sind sehr mühsam, da über einen gewissen Zeitraum fast täglich Strafanzeigen aufgenommen werden müssen.

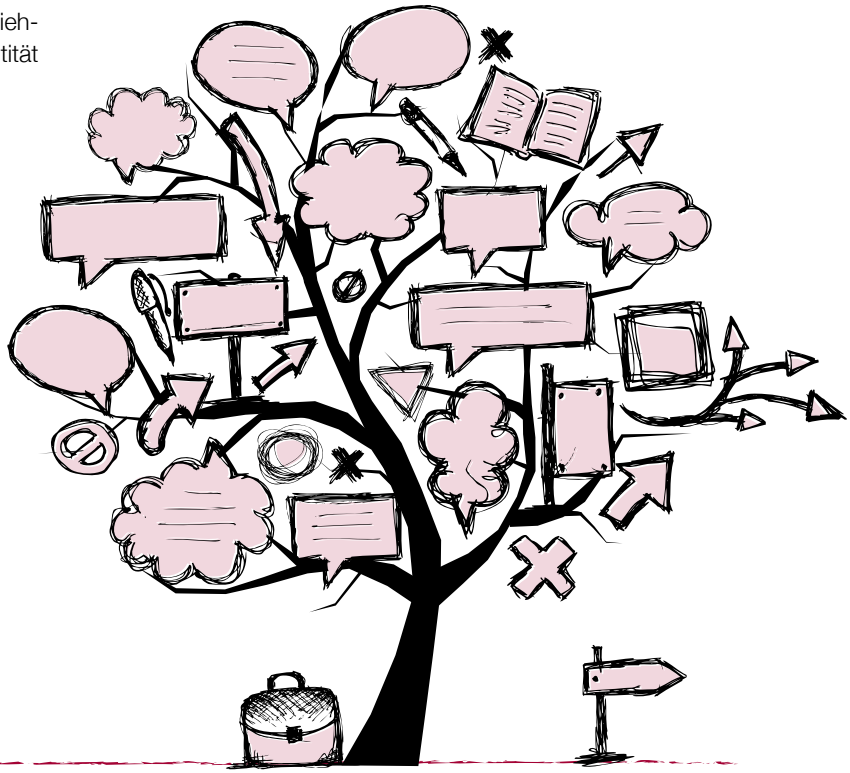
Bei der dabei notwendigen Stellung von Strafanzeigen und Strafanträgen sollten Betroffene unterstützt werden.

Ein Regelbeispiel „Cyberstalking“ soll in das Gewaltschutzgesetz eingefügt werden und es muss einen Anspruch auf Löschung geben.

Die Reformbestrebungen in Bezug auf § 238 StGB (Nachstellung) im Sinne der Umwandlung in ein Eignungsdelikt sind zu begrüßen. Jedoch sollte § 238 Abs. 1 Nr. 5 StGB nicht gestrichen werden.

Die Betreiber von Onlinediensten müssen stärker Verantwortung übernehmen, was die Sicherheit und die Gewaltabwehr im Rahmen der von ihnen angebotenen Dienste betrifft.

In Fällen, in denen der Täter tatsächlich unbekannt ist, muss das Dilemma zwischen Datenschutz und dem nachvollziehbaren Interesse an Kenntnis über die Erlangung der Identität der Täter in Zukunft aufgelöst werden.



Danksagung:

Wir danken der Abteilung Frauen und Gleichstellung der Senatsverwaltung für Arbeit, Integration und Frauen für die Finanzierung des Fachtags sowie der Dokumentation. Anja Kofbinger danken wir für ihr politisches Engagement das Thema betreffend, ihr Grußwort und eine private Spende. Unser Dank richtet sich zudem an die Referentinnen Silvia Zenzen, Beate M. Köhler, Julia Wortmann und Vera Kätsch für die gute Zusammenarbeit und wichtige Beiträge zur Debatte. Wir danken Frau* B. für ihr Vertrauen. Wir danken Saskia Benter, dass sie Frau* B. auf dem Fachtag eine Stimme gegeben hat. Julia Both von 123comics danken wir für das graphic recording des Fachtags. Herzlicher Dank gilt den Moderator*innen und Protokollant*innen der Kleingruppen auf dem Fachtag. Wir danken allen Mitarbeiter*innen und Praktikant*innen des FRIEDA-Frauenzentrum e. V. für ihr überaus großes Engagement in der Organisation und Durchführung ohne das dieser Fachtag so nicht hätte stattfinden können. Unser besonderer Dank gilt überdies allen Teilnehmenden des Fachtags, die sich für das Thema engagieren und die das Zusammentragen von Handlungsbedarfen erst möglich gemacht haben.

Die Dokumentation steht auch als Download zur Verfügung:
http://www.frieda-frauenzentrum.de/anti-stalking-projekt/cyberstalking/dokumentation

Download

AntiStalking
PROJEKT
Information • Unterstützung • Beratung

Frieda
frauenzentrum e.V.

anti-stalking@frieda-frauenzentrum.de
frieda@frieda-frauenzentrum.de
www.frieda-frauenzentrum.de

FriedaFrauenzentrum
@BerlinerFrauen