Anti-Stalking Projekt

Beratung für Betroffene von Stalking/Cyberstalking

Politische Forderungen des Anti-Stalking-Projektes

Wir haben politische Forderungen, da wir in unserer Beratungspraxis vorhandene Leerstellen und Bedarfe, die gesellschaftlich relevant sind, identifizieren können. Diese haben keinen Anspruch auf Vollständigkeit und sind auch durch unsere gesetzten Themenschwerpunkte bedingt. Diese Forderungen können und sollen gerne unter Angabe des Ursprungs weitergeleitet und veröffentlicht werden. Für Rückfragen kontaktieren Sie gerne projektleitung@anti-stalking-projekt.de

Hilfe für Betroffene von Digitaler Gewalt

Anlässlich des 1-jährigen Jubiläums des Fachbereichs Cyberstalking im Anti-Stalking-Projekt haben wir politische Forderungen im digitalen Bereich formuliert. Diese sind im Mai 2019 erschienen und wurden im Januar 2022 aktualisiert:

Keine Staatstrojaner

Mit dem sogenannten Staatstrojaner möchte die Regierung, die Bevölkerung ausspionieren dürfen und genau das tun, was Stalker*innen nicht dürfen. Hierfür ist es notwendig, sogenannte „Exploits“ zu kaufen. Das sind Informationen über Sicherheitslücken, die sich ausnutzen lassen, um heimlich Spy-Software zu installieren. Diese „Exploits“ sind enorm teuer und verlieren ihren Wert sofort, wenn die Sicherheitslücke bekannt und behoben wird. Damit Staatstrojaner funktionieren, hat der Staat kein Interesse mehr daran, diese entsprechenden Sicherheitslücken zu beheben, sondern möchte sie so lange wie möglich offen halten. Dadurch werden die Geräte aller Menschen unsicherer. Ein Fernzugriff wird dann auch Kriminellen erleichtert. Darüber hinaus werden viele Menschen verunsichert, da sie eine ungefähre Ahnung haben, welche Fähigkeiten der Staat digital hat und annehmen, ihr*e Bedroher*in hätte auch diese Fähigkeiten. Im Falle des Staatstrojaners ist das sogar richtig. Wenn Sicherheitslücken absichtlich nicht geschlossen werden, bleiben sie für alle offen.
Gerade in Situationen, wo seitens des*r Bedrohenden hohe IT-Kenntnisse vorhanden sind, führen Staatstrojaner dazu, dass den Betroffenen kaum noch geholfen werden kann.

Anti-Stalking Projekt

Beratung für Betroffene von Stalking/Cyberstalking

Beharren auf Vorratsdatenspeicherung verhindert alternative Vorschläge

Es gibt mehrere Vorschläge, wie polizeiliche Ermittlungsarbeit im Digitalen verbessert werden kann, ohne dabei die Grundrechte zu gefährden. Digitale Polizeistreifen, „Quick-Freeze“ und auch die „Login-Falle“ sind vielversprechende Maßnahmen, die auch wirklich helfen würden.

Diese Vorschläge gibt es teilweise schon seit 2009, sie werden jedoch nicht umgesetzt, weil die Regierung sich auf die viel weitergehende und grundrechtswidrige Vorratsdatenspeicherung versteift hat. Diese wurde bereits zwei Mal vom Bundestag beschlossen und von den Gerichten wieder „kassiert“, weil sie die Grundrechte unverhältnismäßig angreift. Die aktuelle Vorratsdatenspeicherung liegt brach und liegt derzeit vor dem Bundesverfassungsgericht und wird seitens der EU stark kritisiert.

„Quick-Freeze“ bedeutet, dass ab Bekanntwerden der Straftat alle anfallenden Daten sofort aufgezeichnet werden. Richterliche Anordnungen o.ä. müssen für den Start der Aufzeichnung noch nicht, sondern erst zur Herausgabe der Informationen vorliegen. Damit wird verhindert, dass wertvolle Informationen verloren gehen, während bürokratische Hürden überwunden werden müssen. In den meisten Fällen würde diese Form der „Aufzeichnung ab Verdacht“ völlig ausreichen und Ermittlungen möglich machen, die derzeit nicht möglich sind. Dazu müsste es allerdings auch entsprechende Stellen bei der Polizei geben, an die man sich direkt wenden kann und die das „Quick-Freeze“ sofort in die Wege leiten können.

Die Login-Falle ist ebenfalls eine anlassbezogene Ermittlungsmethode, bei der nach dem ersten Übergriff durch einen anonymen Account, dieser beim Plattformbetreiber markiert und beim nächsten Login mit seinen Einwahldaten „gefangen“ wird.

Digitale Polizeistreifen zielen darauf ab, dass viele Vergehen in offenen Foren und unter Klarnamen stattfinden. Ebenso wie Polizeipräsenz auf der Straße wäre es notwendig, dass die Polizei z.B. auch in öffentlichen Telegram-Gruppen patrouilliert.

Es ist nicht einzusehen, weshalb wirkungsvolle Maßnahmen seit über 10 Jahren nicht umgesetzt werden. Das endlose Festhalten an der grundrechtsproblematischen Vorratsdatenspeicherung lenkt von den echten Problemen ab und verhindert die Einführung notwendiger grundrechtskonformer Maßnahmen.

Anti-Stalking Projekt

Beratung für Betroffene von Stalking/Cyberstalking

Tor muss legal bleiben

Viele Betroffene von Cyberstalking sind so verunsichert, dass sie auf Computernutzung völlig verzichten und dadurch gesellschaftlich ausgegrenzt werden, oder gar berufsunfähig werden. Das Betriebssystem „Tails“, das auf Tor basiert, bietet unsere bisher stärkste technikbasierte Antwort auf dieses Problem. Hier können sich Betroffene erstmals wieder sicher fühlen und haben die Möglichkeit, Internet und Computer ohne Furcht zu nutzen. Da Tails auf Tor basiert, würde eine Einschränkung von Tor unseren Klientinnen* direkt schaden. Selbst wenn Tor nicht komplett verboten wird, aber Provider durch Rechtsunsicherheit Tor-Dienste lieber vorsorglich sperren, bedeutet das für unsere Klientinnen*: Diese Seiten können sie nicht mehr aufrufen.
Die Kriminalisierung von Tor würde uns um unsere bisher beste technische Hilfe für betroffene Frauen berauben.

Keine Klarnamens- und Impressumspflicht

Während sich Bedroher*innen von einer Klarnamenspflicht kaum abschrecken lassen, würde eine Klarnamenspflicht für die Betroffenen katastrophale Folgen haben. Oft ist Anonymität der einzige Weg für Betroffene, ihre Lebenssituation wieder in den Griff zu bekommen. Eine Klarnamenspflicht würde sie dem*r Bedroher*in völlig ausliefern und letztlich dazu führen, dass sie sich aus dem digitalen öffentlichen Leben komplett rausziehen müssen.
Das gleiche Problem gilt in Bezug auf die Impressumspflicht, die nicht dazu führen darf, dass besonders bedrohte Gruppen sich aus dem öffentlichen Diskurs zurückziehen. Im Übrigen haben feministische Blogs grundsätzlich das Problem, dass sie viel Hass auf sich ziehen und nicht gezwungen werden wollen, private Daten zu veröffentlichen. Für solche Fälle braucht es Lösungen, wie z.B. eine Chiffre-Nummer/Postfach beim Bürgeramt, die man im Impressum statt einer ladungsfähigen Anschrift angeben kann.

Personal bei Polizei und Justiz sensibilisieren, schulen und verstärken

Häufig berichten Betroffene, dass sie bei der Polizei auf überforderte oder unverständige Beamte stießen, die gar nicht wussten, wie man mit Digitaler Gewalt umgeht oder diese einordnen soll. Deshalb braucht die Polizei aber nicht mehr Befugnisse, sondern es braucht Verfahren, Schulungen und v.a. mehr Personal bei Polizei und Justiz, die sich mit dem Thema der digitalen Gewalt befassen.

Anti-Stalking Projekt

Beratung für Betroffene von Stalking/Cyberstalking

Forensische Untersuchung von Geräten

Eine forensische Untersuchung der betroffenen Geräte ist meist der einzige Weg für Beweissicherung und Gewissheit bei digitaler Nachstellung. Dennoch findet diese fast nie statt. Es braucht sowohl bei der Polizei als auch bei Beratungsstellen Möglichkeiten, ein Gerät forensisch analysieren zu lassen. Dafür braucht es klare und verlässliche Kriterien, wann z.B. die Polizei ein Gerät annimmt, was als „Anfangsverdacht" gilt und welche Beweise gerichtsfest sind. Für forensische Untersuchungen bei der Polizei darf nicht vorausgesetzt werden, dass die Betroffenen erste Beweise selbst liefern. Damit auch Beratungsstellen solche Dienste anbieten können, brauchen diese finanzielle Mittel, um Fachkräfte finanzieren zu können.

Sichere Arbeitsbedingungen für Berater*innen

Berater*innen, die von Gewalt betroffene Frauen* unterstützen und entsprechend auch Berater*innen, die zu Stalking und Cyberstalking beratend tätig sind und in der Öffentlichkeit stehen, sind einem erhöhten Bedrohungsrisiko ausgesetzt. Diesem Umstand muss vorausschauend Rechnung getragen werden. Das Erlangen einer Auskunftssperre der Melderegisterauskunft muss für Menschen (und deren direktes Wohnumfeld), die in so einer Risikogruppe arbeiten, stark vereinfacht werden und darf nicht erst nach einem Straftatbestand erfolgen. Dann ist es oftmals zu spät.
Beratungseinrichtungen müssen technisch und finanziell besser ausgestattet sein. Fortbildungen und Supervisionsprogramme müssen ausgebaut werden. Ganz besonders für den konkreten Fall eines „Shitstorms" braucht es psychosoziale, juristische und mediale Unterstützung. Außerdem müssen genügend Mittel zur Betreuung der technischen Infrastruktur (Administration der Geräte) zur Verfügung gestellt werden. Kaum eine Beratungsstelle hat eine extra dafür geschulte Administrator*in. Dadurch sind die Berater*innen und die Klient*innen einem großen Risiko ausgesetzt.

Staatliche Meldestellen

Der Staat darf die Verantwortung zur Meldung von Rechtsverstößen nicht auf digitale Plattformen abwälzen. Deren Meldemöglichkeiten sind oft abschreckend, unübersichtlich oder gar nur mit einem Account auf derselben Plattform erreichbar. Schmähaccounts oder veröffentlichte Nacktbilder müssen auch ohne Account oder besondere Kenntnisse gemeldet werden können. Hier muss der Staat Hilfe leisten. Insbesondere das Recht am eigenen Bild oder die Veröffentlichung von privaten Daten

(Doxxing) sind derzeit kaum ohne großen rechtlichen Aufwand durchsetzbar. Es ist Aufgabe des Staates, hier Abhilfe zu leisten und die Schnittstelle zwischen Betroffenen und Plattformen zu stellen. Letztlich darf auch die Entscheidung darüber, ob ein Inhalt rechtswidrig ist, in einem Rechtstaat nicht an die Plattformbetreiber abgeschoben werden.

Anonyme Legitimation

Häufig ist es notwendig, sich gegenüber einem Dienst als Person zu legitimieren. Beispielsweise wenn man die Löschung eines Schmähaccounts beantragt, muss der Dienst ja wissen, dass man auch wirklich die betroffene Person ist. Auch für Anfragen nach DSGVO oder Informationsfreiheitsgesetz (IFG) muss sichergestellt sein, dass die privaten Daten nicht an jemanden geschickt werden, der diese gar nicht einsehen darf. Zur Legitimation verlangen diese Dienste eine Kopie des Personalausweises. Dies ist in vielerlei Hinsicht problematisch:

1) Es ist nicht 100%ig gesichert, ob damit die Richtigkeit der Identität gewährleistet werden kann, denn eine Ausweiskopie könnte man sich auch irgendwie beschaffen.
2) Es ist fraglich, ob dies laut Personalausweisgesetz überhaupt legitim ist.
3) Man übermittelt damit viele sensible Informationen, die den Dienst nichts angehen.

Zu dieser Praxis braucht es dringend eine Alternative. Beispielsweise eine Stelle beim Bürgeramt, bei der man sich legitimieren kann und eine Legitimationsnummer erhält. Diese kann dann dem Betreiber gegenüber, zusammen mit dem Namen, genannt werden. Dieser kann sodann bei der Behörde elektronisch erfragen, ob sich unter dieser Nummer mit diesem Namen jemand legitimiert hat. (Postident und die Funktionen über den elektronischen Personalausweis kommen dafür aus vielen Gründen nicht in Frage.)

Thema Digitale Gewalt ernst nehmen und Forschung betreiben, Bewusstsein stärken

Das Thema digitale Gewalt wird im öffentlichen Diskurs viel zu wenig ernst genommen. Allein „Hate Speech“, ein Problem, von dem ja auch viele Politiker*innen und Journalist*innen betroffen sind, wird öffentlich diskutiert. Das fehlende gesellschaftliche Bewusstsein führt dazu, dass viel zu wenig Vorsorge betrieben wird und Betroffene oft große Schwierigkeiten haben, in ihrem Umfeld Verständnis und Unterstützung zu erfahren. Es ist dringend erforderlich, dass zum Thema digitale Gewalt geforscht wird und Betroffenenzahlen spezifisch erfasst werden. Neben Hate Speech müssen auch andere

Anti-Stalking Projekt

Beratung für Betroffene von Stalking/Cyberstalking

Formen von digitaler Gewalt (Identitätsbetrug, Cyberstalking, Belästigung, Verleumdung, Revenge-Porn usw.) öffentlich diskutiert werden.

Mehr Fachberatungsstellen zu digitaler Gewalt und Angebote zur Stärkung der allgemeinen Medienkompetenz für Frauen*

Derzeit berät das Anti-Stalking-Projekt mit Fachbereich Cyberstalking faktisch nicht nur zu Cyberstalking, sondern auch zu anderen Formen digitaler Gewalt. Das derzeit sehr überschaubare Beratungsangebot in Deutschland muss aufgestockt werden.
Neben allgemeiner Computerberatung für ganz normale Alltagsprobleme braucht es Programme zur Stärkung der Medienkompetenz. Nur so kann sinnvoll Prävention betrieben werden, z.B. indem Frauen* frühzeitig lernen, dass sie die Kontrolle über ihre Geräte nicht ihrem*r Partner*in überlassen sollten. Nach einer Trennung hat diese*r oftmals die komplette Kontrolle über die Accounts und Geräte, was häufig zu Problemen führt. Damit sie die Kontrolle über ihre Geräte selbst tragen können, müssen insbesondere Frauen* ermutigt und unterstützt werden, bevor sie in eine solche Situation geraten.

Offline Lösungen erhalten

Immer mehr Betroffene geraten in Probleme z.B. bei der Jobsuche. Entweder weil der*die Bedroher*in ihre Bewerbungsversuche aktiv sabotiert, oder weil sie das Vertrauen in ihre Geräte und Internetverbindungen verloren haben und diese Kanäle nicht zur Übertragung solch sensibler Informationen nutzen wollen.
Da die meisten Bewerbungen mittlerweile nur noch online eingereicht werden können, geraten Betroffene auf Arbeitssuche in große Schwierigkeiten. Eine Regelung, dass Bewerbungen auf Papier angenommen werden müssen und nicht benachteiligt behandelt werden dürfen, wäre ebenso wichtig, wie ein Recht auf verschlüsselte E-Mail-Bewerbung. Wer eine Bewerbung nur über E-Mail und spezielle Bewerbungsportale anbietet, muss gewährleisten, dass man diese auch per verschlüsselter E-Mail verschicken kann. Bewerbungsportale dürfen niemals alternativlos genutzt werden, da diese voraussetzen, dass die Betroffene höchst sensible Daten an eine ihnen unbekannte dritte Firma überträgt.
Auch in anderen Lebensbereichen, wie beim Jobcenter oder beim Kauf von Bahntickets, dürfen analoge Prozesse nicht alternativlos von digitalen Prozessen ersetzt werden.

Anti-Stalking Projekt

Beratung für Betroffene von Stalking/Cyberstalking

Recht auf Verschlüsselung (v.a. mit Behörden)

Gerade mit Behörden findet häufig wichtige und sensible Kommunikation über E-Mail statt. Betroffene von Cyberstalking haben aber zu diesem Kanal kein sehr großes Vertrauen. Dabei gäbe es mit E-Mail-Verschlüsselung (PGP) eine hervorragende Lösung für dieses Problem. Da aber die wenigsten Behörden verschlüsselte Kommunikation über E-Mail anbieten, ist diese Lösungsoption für Betroffene wertlos. Die Datenschutzgrundverordnung legt Wert darauf, dass verschlüsselte Kommunikation ermöglicht werden muss. Staatliche Einrichtungen und Behörden müssen hier mit gutem Beispiel voran gehen.
Dabei ist zu beachten, dass auf sichere und allgemein zugängliche Verschlüsselungsmethoden, wie PGP zurückgegriffen werden muss.

Auf gar keinen Fall darf Ende-zu-Ende-Verschlüsselung gesetzlich geschwächt oder gar verboten werden. Denn nur damit können wir unseren Klientinnen* helfen, sich endlich wieder sicher zu fühlen. Wir brauchen vielmehr ein Recht auf Verschlüsselung für die Menschen und eine Pflicht zur Verschlüsselung bei Behörden und öffentlichen Einrichtungen. (Bei entsprechender Stärkung der Administrationskapazitäten.)

Bessere psychosoziale Betreuung von wahnhaften bzw. hypervigilanten Personen

Stalking, besonders Cyberstalking greift die Psyche an. Es ist ein Spiel mit der Realität und zielt darauf ab, das Vertrauen in die eigene Wahrnehmung anzugreifen. Gerade im digitalen Zusammenhang wird es beinahe unmöglich, im Alltag zwischen tatsächlichem Angriff und erlebtem Angriff zu differenzieren. Ist man einmal auf die Gefahrenquelle „Computer“ aufmerksam geworden, neigt man unter Umständen dazu, auch harmlose Computerfehler als Angriff zu deuten (Hypervigilanz). Der erlebte Kontrollverlust macht anfällig für falsche Vermutungen.
Im Zuge des allgemeinen Überwachungsdrucks und bei Betroffenen von Cybergewalt im Besonderen, kann mit einer Zunahme an Hypervigilanz gerechnet werden. Viele Menschen, die dies betrifft, werden oft nicht ernst genommen und von Beratungsstelle zu Beratungsstelle verwiesen, was sowohl für die Betroffenen als auch für die Beratungsstellen eine große Belastung darstellt. Hier muss dringend Abhilfe geschaffen werden. Einerseits an den Ursachen (zunehmende Überwachung und Kontrollverlust) und andererseits in Bezug auf die Unterstützung und Betreuung solcher Menschen, die meist sehr unter ihrem Zustand leiden. Es braucht Strukturen, die diese Menschen auffangen, ohne sie dabei für unglaubwürdig zu erklären.

Anti-Stalking Projekt

Beratung für Betroffene von Stalking/Cyberstalking

Stalking-Apps verbieten

Der Markt der Stalking-Apps wächst. Manche bezeichnen sich als “Pärchen-App” oder geben vor nur der Überwachung von Kindern zu dienen. Andere machen gar keinen Hehl daraus, dass es um digitale Übergriffe geht. Egal zu welchem Zweck sie eigentlich gedacht sind, sie werden meist illegal eingesetzt und selbst ihr legaler Einsatz ist höchst bedenklich.

Stalking-Apps übermitteln sensibelste Daten, wie z.B. den Standort, angesurfte Websites, Passwörter oder Kurznachrichten und können sogar in die Kommunikation eingreifen, indem sie z.B. Websites oder Telefonnummern sperren oder Nachrichten mit gefälschtem Absender verschicken. Außerdem haben sie häufig Zugriff auf die Kameras und das Mikrofon und können Videos, Fotos und Tonaufzeichnungen vornehmen. Eine solche Spy-App kann man auf dem Gerät so verstecken, dass sie kaum mehr aufzufinden ist. Der Verkauf dieser Software darf nicht länger legal sein, gängige App-Stores dürfen solche Apps nicht länger führen.