# Formen digitaler geschlechtsspezifischer Gewalt

*Jenny-Kerstin Bauer und Ans Hartmann*

Durch den steten Fortschritt im Bereich der Informations- und Kommunikationstechnologien (IKT) entstehen nicht nur neue Möglichkeiten der Nutzung dieser Medien. Vielmehr eröffnen sich hier auch immer neue Möglichkeiten und Wege Menschen zu verfolgen, zu bedrohen, zu belästigen und ihnen massiven Schaden zuzufügen. Dabei spielt das Internet eine besondere Rolle, da es kaum etwas vergisst und damit besondere Belastungen für die Betroffenen mit sich bringt. Fast jede Form geschlechtsspezifischer Gewalt ist von den Auswirkungen der Digitalisierung betroffen; manche Formen der Gewalt sind nur durch Nutzung von IKT möglich. Für die zahlreichen Phänomene, die mit diesem Prozess einhergehen, wurde in den vergangenen Jahren der Oberbegriff »digitale Gewalt« geprägt. Im Folgenden werden vier spezifische Kategorien digitaler Gewalt (Stalking; Belästigung, Diffamierung, Beleidigung, Bedrohung; Bildbasierte sexualisierte Gewalt und Hate Speech) beleuchtet und konkrete Methoden und Strategien erläutert, die in diesen Bereichen angewendet werden.

## Stalking

Als Stalking wird beharrliches, andauerndes und hartnäckiges Verhalten bezeichnet, welches im *direkten*[1] und *nicht direkten* Stalking-Kontakt mittels IKT ausgeübt wird, um eine Person zu belästigen, ihr zu schaden, sie zu verfolgen und/oder zu terrorisieren (vgl. Ogilvie 2000). Die Stalkingmethoden können sich auf vielfältige Weise äußern, wobei mehrere Methoden gleichzeitig auftreten können (vgl. Belik 2007: 30; Port 2012: 40; Bauer 2016: 16). Frauenbera-

1 Im weiteren Verlauf wird hier der Begriff nicht-wissentlicher Stalking-Kontakt verwendet, weil er die Unwissenheit der betroffenen Person besser in den Vordergrund stellt.

tungsstellen und Frauennotrufe weisen darauf hin, dass Stalking eine Gewaltform darstellt, die in Gewaltbeziehungen seit der Verbreitung des Internets und »smarter Geräte« fast nicht mehr ohne digitale Komponente vorkommt. Bei allen Formen von Stalking ist die Beendigung einer Beziehung oder das nicht Eingehen auf ein Beziehungsbegehren ein häufig auftretender Auslöser für die Stalkinghandlungen. Ziel der stalkenden Person ist es, Macht und Kontrolle über die betroffene Person auszuüben, um die Vormachtstellung in der Beziehung aufrecht zu erhalten oder die Beziehung wiederherzustellen (vgl. Ogilvie 2000; Reno 2006).

## Direkter Stalking-Kontakt

Unter direktem Stalking-Kontakt wird beständiges Anrufen oder das Schreiben von Textnachrichten (SMS, Messenger) mit und ohne Bildaufnahmen, Sprachnachrichten, E-Mails oder Kommentaren in sozialen Netzwerken verstanden, um allgegenwärtige Anwesenheit zu demonstrieren, in Kontakt zu bleiben, zu beleidigen oder zu bedrohen. Hierbei hat die betroffene Person Kenntnis darüber, dass sie gestalkt wird und in der Regel weiß sie auch von wem. Je nach stalkender Person und Motivlage kann der Inhalt der Nachrichten sehr unterschiedlich sein und aus Gefühlsäußerungen über Beleidigungen bis hin zu Drohungen reichen und aus Text, Bildern, Sprachnachrichten und Videos bestehen. Die betroffene Person wird nicht zwangsläufig direkt adressiert.

Folgende Stalking-Methoden können unter direktem Stalking zusammengefasst werden:

### Nachrichtenbomben

Es können so viele Nachrichten verschickt werden, dass dies einer ›Bombardierung‹ ähnelt und der Messenger und E-Mail-Verkehr zum Erliegen kommt (vgl. Fiedler 2006: 26). Eine normale Nutzung dieser Dienste ist nicht mehr möglich. Andere Nachrichten gehen in der Flut der Stalkingbotschaften unter.

### Visuelle Überwachung

Permanentes Anrufen kann auch mit visueller Überwachung per Videoanruf erfolgen. Dabei wird die betroffene Person aufgefordert oder genötigt ihre Umgebung zu zeigen, um so Rückschlüsse über ihren Aufenthaltsort ziehen zu können. Diese Methode wird eher in Beziehungen angewendet, um Part-

ner*innen zu kontrollieren und wird oft mit ›Sorge‹ oder ›begründeter‹ Eifersucht oder als vermeintlicher ›Liebesbeweis‹ legitimiert.

#### Installation von Apps

Ähnlich wie bei visueller Überwachung wird die Zustimmung zur Installation von Smartphone-Apps mit möglicher Ortungsfunktion als Vertrauens- oder Liebesbeweis eingefordert oder die betroffene Person unter Druck gesetzt, entsprechende Apps zu installieren. Diese Spionage-Apps (Spyware) haben häufig euphemistische Namen wie »Finde meine Freunde« oder »Anti-Diebstahl-App«. In manchen Fällen werden diese Apps ohne Wissen der betroffenen Person auf dem Handy installiert, um die gestalkte Person ausfindig zu machen und die verarbeiteten Informationen ihres Smartphones oder des Computers jederzeit ohne ihr Wissen einzusehen.[2]

#### Teilen von Passwörtern

Auch das Teilen von Passwörtern kann als ›Vertrauensbeweis‹ eingefordert oder aber erzwungen werden. In manchen Fällen werden die Passwörter bewusst entwendet oder erraten. So erhält die stalkende Person die Möglichkeit auf Online-Profile zuzugreifen, die Kommunikation über die Messengerdienste zu überwachen und Nachrichten im Namen der betroffenen Person zu verschicken. Durch die Änderung des Passwortes kann sich die stalkende Person darüber hinaus den alleinigen Zugang sichern.

### Nicht-wissentlicher Stalking-Kontakt

Unter nicht-wissentlichen Stalking-Kontakt fällt die Nutzung aller IKT, um Personen zu stalken (z.B. Überwachen), ohne dass die betroffenen Personen es aktiv registrieren. Betroffene berichten in diesem Zusammenhang oft von einem ›komischen‹ oder ›unguten‹ Gefühl bzw. dem Eindruck, dass sie überwacht würden, aber nicht genau wissen, wer die stalkende Person ist und welcher Methoden sie sich bedient. Ziel der stalkenden Person ist es auch hier, zu verunsichern, Macht und Kontrolle über die betroffene Person auszuüben.

#### Überwachung und Kontrolle

In Paarbeziehungen ist es nicht ungewöhnlich technische Geräte und Passwörter zu teilen. Oftmals hat oder hatte die gewaltausübende Person, z.B.

2 Siehe Beitrag: Der Feind in der eigenen Tasche: Stalkerware und digitale Überwachung im Kontext von Partnerschaftsgewalt.

der (Ex-)Partner, Zugang zum Gerät der betroffenen Person, kennt ihre Passwörter oder hat gar ihre Benutzer*innenkonten eingerichtet. Wenn er technisch versiert ist, können Informationen über die Online-Aktivität der betroffenen Person oder über mögliche Aufenthaltsorte u.a. durch Hacken von Benutzer*innenkonten in sozialen Netzwerken eingeholt werden. Wenn Kontrolle über einen Messenger-Dienst besteht, kann in Echtzeit geschriebene Kommunikation mitgelesen sowie verschickte Fotos eingesehen werden. Bei nicht-wissentlichem Stalking-Kontakt geschieht all dies ohne Wissen der betroffenen Person, was erklärt, warum Betroffene manchmal das Gefühl haben ›verrückt‹ zu werden. Dies wird verstärkt, wenn diese Überwachung psychologisiert wird, indem beispielsweise Unterstützer*innen annehmen, die Person leide an psychischen Störungen anstatt zu überprüfen, ob nicht eigentlich eine faktische Überwachung stattfindet.

**Mitgliedskarten und Partner-Handyverträge**

Online-Konten mit Mitgliedskarten wie Payback oder die Deutschlandcard verraten der stalkenden Person, wo die Betroffene eingekauft hat. So können wiederum Rückschlüsse auf den Aufenthaltsort und ggf. das Konsumverhalten der betroffenen Person gemacht werden. Bei Partner-Handyverträgen können die genauen Verbindungen, Telefonummern etc. eingesehen und nachvollzogen werden.

**Datenleak über Dritte**

Ein Datenleak wird oftmals unabsichtlich oder unbedacht von Mitgliedern der Online-Community verursacht, indem die betroffene Person ohne eigene Kenntnis in einem Bild oder Event markiert wird. Die stalkende Person kommt so über Dritte an weitere Informationen.

**Internet of Things (IoT)**

Die IoT-Technologie[3] erweitert die Internetverbindung auf physische Geräte und Alltagsgegenstände. Dies können etwa Sicherungssysteme für Türen sein, aber auch Jalousien, Heizungen, Baby-Phones, Lampen, Smartwatches oder Fitnesstracker. Auch medizinische Produkte wie Insulinmessgeräte oder Hörgeräte fallen in diese Kategorie, da diese Geräte über Fernzugriff wie beispielsweise eine App kontrolliert, gesteuert aber auch manipuliert werden

3 Siehe Beitrag: Das Internet der Dinge: Die Auswirkung »smarter« Geräte auf häusliche Gewalt.

können. Betroffene schildern das Gefühl, das eigene Zuhause würde sich gegen sie wenden bzw. sich verselbstständigen, weil z.B. plötzlich Musik angeht oder Stimmen zu hören sind. Der Trend zum smarten Alltagsgegenstand ist weiter steigend und eröffnet gewaltausübenden Menschen zusätzliche Kontroll- und Überwachungsstrategien.

**Ortungsfunktionen**

Über GPS und die Standortübermittlung können die Bewegungen von Personen überwacht und kontrolliert werden. Auch Mikrofone und Kameras können über entsprechende Apps zum Spionieren genutzt werden.[4] Über spezielle Ortungsfunktionen lassen sich Smartphones und andere elektronische Geräte auf den Meter genau lokalisieren. Bei Android-Smartphones geht dies über die Funktion »Mein Gerät finden« und bei dem iPhone über »Mein iPhone suchen«. Diese Funktion sollte ausgeschaltet bzw. durch sichere Passwörter und eine Zwei-Faktor-Authentifizierung geschützt sein. Diese Funktion stellt eine besondere Gefährdung von Frauen in Zufluchtsorten dar, deren Adressen anonym bleiben sollen. Von der gewaltausübenden Person können auch GPS-Sender erworben werden und z.B. in Autos, Taschen oder Kinderspielzeug versteckt werden.

**Spionage-Software**

Spionage-Software[5] für Smartphone, Tablet oder Computer ermöglicht in Echtzeit Zugriff auf Dateninformationen und Kommunikation des infiltrierten Geräts; die Installation dieser Apps kann mit oder ohne Wissen der betroffenen Person geschehen. Spionage-Software ist ein »Remote Access Tool« (Fernwartungssoftware) und wird häufig missbraucht, um die Privatsphäre von aktuellen oder ehemaligen Partner*innen auszuspähen. Die Software kann sehr einfach und kostengünstig online erworben werden und verborgen auf dem Gerät fungieren (vgl. CAS 2019: 5ff.). Zu der Fernsteuerung kommt die Möglichkeit hinzu, die App als Systemanwendung zu tarnen und

4 Siehe Beitrag: Digitale Erste Hilfe und Sicherheitsprinzipien für Berater*innen bei digitaler Gewalt.

5 Diese Software ist auch unter folgenden Begrifflichkeiten zu finden: Spy App, Stalkerware, Spy Software, ›legale‹ Spyware-Apps (Stalkerware oder Spouseware) (vgl. CAS 2019; Köver 2019). Bei dieser Art von Software geht es nicht um »Kindersicherungssoftware«, die darauf abzielt, gewisse Inhalte und Zugriffe auf Seiten einzuschränken und die Nutzer*innen auch darüber zu informieren, sondern um heimliches Überwachen.

verborgen im Hintergrund auszuführen. Diese erscheint weder im »System Tray« (Benachrichtigungsfeld) noch auf dem Desktop oder unter »Software« in der Systemsteuerung. Die Apps tarnen sich in der Liste installierter Apps hinter Namen, die Systemprozesse imitieren (vgl. ebd.: 8). Nur die gewaltausübende Person, die auch die Lizenz gekauft hat, kann die Software öffnen, die Aufzeichnungen ansehen bzw. löschen, Änderungen tätigen oder die Software deinstallieren. Wie bei vielen ähnlichen Apps werden hier zur Ausführung bestimmter Funktionen »Superuser-Rechte« (Administrator*innenrechte) benötigt. Durch eine vorab festgelegte Tastenkombination kann die Spysoftware wieder aufgerufen werden.

Das Angebot an Funktionen ist für solche Programme je nach Modell und Anbieter*in unterschiedlich und kann folgende Komponenten beinhalten:

- E-Mails, SMS und Messenger-Apps (WhatsApp, Hangouts, Skype, Facebook Messenger, Viber, Telegram usw.) können abgefangen oder sogar umgeleitet werden.
- Durch Audio-Überwachung können Telefongespräche abgehört und Gesprächsverläufe gespeichert werden. Einige Programme sind sogar in der Lage, unbemerkt Video- und Sprachaufnahmen von außen zu machen (vgl. ebd.: 7).
- Im Zuge visueller Überwachung, die den Zugang zur Kamera beinhaltet, können Bilder gemacht bzw. auf die Galerie der abgespeicherten Bilder zugegriffen werden. Zusätzlich können einige Programme in regelmäßigen Abständen unbemerkt Bildschirmfotos vom Gerät der Betroffenen machen.
- Der Browserverlauf kann eingesehen werden. Über diese Funktion kann die gewaltausübende Person genaue Informationen über Zeitpunkt und Dauer von Besuchen einzelner Webseiten erhalten. Darüber hinaus können Dateien und Funktionen auf dem Gerät, etwa Kalender und Kontaktliste, abgerufen und verändert werden. Auch das Aufrufen bestimmter Webseiten wie Social Media oder Informationsportale über Unterstützungsangebote und Frauenberatungsstellen kann blockiert werden.
- Die stalkende Person kann regelmäßig mit Hilfe der GPS-Funktion oder WIFI-Verbindungen über den Aufenthaltsort informiert werden.
- Mit einem »Keylogger« (Tasten-Protokollierer) können Aufnahmen von allen Tastenanschlägen gemacht und chronologisch gespeichert werden. Beim Abruf der Aufnahmen ist ersichtlich, welche Benutzer*in zu welchem Zeitpunkt und in welchem Programm (Word, E-Mail-Programm

etc.) welche Tasten gedrückt hat. Es gibt auch eine Alarmfunktion, wenn beispielsweise ein bestimmtes Wort eingegeben wird. In diesem Fall wird die gewaltausübende Person umgehend per E-Mail informiert.

- Mit Spionage-Software können Programmaufnahmen und Systemvorgänge des Computers oder des Smart-Gerätes präzise mit Bildschirmfotos aufgezeichnet werden. Dadurch können beispielsweise alle Daten, die erstellt, gelöscht, verändert oder umbenannt wurden, erfasst werden. Auch Änderungen von Laufwerk- und Netzwerkverbindungen sowie der Anschluss eines USB-Sticks und die Aufzeichnung von Druckaufträgen können genau erfasst werden. Kopiert eine betroffene Frau etwa Dateien oder Beweismittel auf einen USB-Stick, kann mit Hilfe der Software genau aufgezeichnet und nachverfolgt werden, welche Inhalte zu welchem Zeitpunkt von welchem Gerät kopiert wurden.
- Spyware-Programme verfügen über eine umfassende Exportfunktion, mit der alle Aufzeichnungen im Text- oder Excel-Format exportiert werden können. Bildschirmaufnahmen sind als Bilderserien oder AVI-Videodateien speicherbar. Das Drucken aller oder einzelner Aufzeichnungen ist ebenfalls möglich.
- Sämtliche Informationen können in Echtzeit verfolgt oder abgespeichert und zu einem späteren Zeitpunkt gelesen werden. Mit der Zeitauswertung informiert die Spionage-Software darüber, wie lange jede Computersitzung aktiv und inaktiv ist. Protokolle zeigen an, wann die einzelnen Sitzungen beginnen und enden.

Alle Überwachungsfunktionen sind frei konfigurierbar, das heißt die gewaltausübende Person entscheidet, wie häufig und detailliert die Software das Gerät überwachen soll. Nicht alle Programme verfügen im gleichen Maß über die aufgeführten Funktionen, Konfigurationen unterscheiden sich hier durch Preis und die Art der Software. Einige Anbieter*innen werben damit, dass die Installation der Spionage-Software auf dem Smartphone ganz einfach sei und es keinen »Jailbreak« bei IOS-Geräten oder »Rooting« bei Android-Geräten benötige. Diese zwei englischen Begriffe bezeichnen das nicht-autorisierte Entfernen von Nutzungsbeschränkungen bei elektronischen Geräten, deren Hersteller*innen bestimmte Funktionen serienmäßig gesperrt haben und mit voller Systemkontrolle über die höchstmöglichen Zugriffsrechte am Betriebssystem verfügen (vgl. Eckert 2014: 27ff.).

Grundsätzlich lässt sich Spionage-Software in »Dual-Use-Software« und offen erkenntliche Spionage-Software unterteilen. Dual-Use Software kann

auf zwei Arten genutzt werden. Zum einen etwa als Anti-Diebstahl-App, wobei Anbieter*innen damit werben, dass ›der Dieb‹ so schneller ausfindig gemacht werden und das Smartphone gefunden werden kann. Gleichzeitig können die Funktionen dieser Software als Spyware missbraucht werden. Es können Bewegungen und Aufenthalte registriert und aufgezeichnet, Bildschirmfotos von geöffneten Anwendungen gemacht und Anrufe abgehört werden. Die Software kann problemlos und legal in App-Stores gekauft werden.

Offen erkennbare Spyware richtet sich als Zielgruppe an gewaltausübende Personen und wirbt öffentlich damit, (auch) den Zweck einer Spionage-Software zu erfüllen. Laut Marketing der Anbieter*innen kann sie etwa genutzt werden, wenn der Verdacht besteht, dass die*der Partner*in möglicherweise fremdgeht. Die Funktionen für diese Software können je nach Modell und Anbieter*in alle oben angeführten Komponenten beinhalten. Sie sind allerdings größtenteils nicht in offiziellen App-Stores wie bei Google Play oder im Apple App Store erhältlich und ihre Installation erfordert eine Anmeldung auf der Website der Anbieter*innen sowie den Zugang zum Gerät der betroffenen Person.

Dennoch kann Spionage-Software sehr schnell und einfach installiert werden und benötigt kein spezifisches technisches Verständnis. Es gibt unterschiedliche Möglichkeiten entsprechende Programme auf dem Smartphone oder Computer der betroffenen Person zu installieren:

- Es wird behauptet, das Handy soll über die App bei Verlust schneller gefunden werden. Über die weiteren Möglichkeiten der App wird nicht informiert.
- Die betroffene Person wird überredet und/oder unter Druck gesetzt, der Installation zuzustimmen.
- Die stalkende Person kennt die Passwörter, hat das Gerät geschenkt, ausgeliehen und/oder eingerichtet und hat so sehr unkompliziert die Möglichkeit, Spyware heimlich zu installieren.
- Die gewaltausübende Person hatte einmal kurzen und direkten Zugriff auf das elektronische Gerät, als es noch entsperrt war und hat in dieser Zeit Spionage-Software installiert.
- Spionage-Software kann durch E-Mail- oder Nachrichten-Anhänge unabsichtlich heruntergeladen werden, weil die Software beispielsweise als Foto oder vermeintliches wichtiges Dokument (z.B. als Gerichtstermin) getarnt war.

- Die gewaltausübende Person hat zu Cloud-Diensten der Betroffenen Zugang und die Spionage-Software funktioniert über die Verbindung mit diesen Diensten.

Ein Hinweis auf die Existenz von Spionage-Software auf einem Smartphone kann sein, wenn die stalkende Person viele Informationen und Aufenthaltsorte der Betroffenen kennt und sie sich dies nicht anders erklären kann, so zum Beispiel wenn der Gewalttäter bei Terminen auftaucht oder ihr Nachrichten mit Bezug auf Bilder schickt, die sie auf ihrem Gerät gespeichert hat, aber nicht an den Stalker geschickt wurden. Durch das ständige Abfangen und Auslesen der Daten werden die Geräte außerdem langsamer, der Akku ist schneller leer und das Datenvolumen schneller verbraucht. Ein weiteres Anzeichen kann sein, wenn das Gerät gerootet oder gejailbreakt ist und somit auch nicht-autorisierte Software installiert werden kann. Wenn das der Fall ist, könnte Spionage-Software installiert worden sein.

Der Umgang mit Spionage-Software ist unterschiedlich. Das manuelle Erkennen hat grundlegende Grenzen, auch Anti-Virus-Software identifiziert Spyware nicht immer. Aktuell wird an dieser Stelle von einigen Anbieter*innen nachgebessert. Besonders engagiert in diesem Bereich sind IT-Sicherheitsfirmen, die sich an der internationalen Coalition Against Stalkerware (CAS) beteiligen, z.B. Kaspersky, G Data oder NortonLifeLock. Einige Programme können gelöscht werden. Es kann auch helfen, den Computer neu aufzusetzen oder das Smartphone auf Werkseinstellungen zurückzusetzen. Bei dieser Variante werden jedoch alle Daten gelöscht und somit auch alle Beweise, die als Dateien vorhanden sind. Manche Spionage-Softwares sind so versteckt, dass sie nur für IT-Spezialist*innen auffindbar sind. Hersteller*innen und Softwareentwickler*innen von Spionage-Software weisen die Verantwortung häufig von sich, obwohl die Software Täter unterstützt und Betroffenen schadet. Eine gewaltunterstützende Wirkung dieser Software wird von Hersteller*innen oftmals erkannt, jedoch nicht als problematisch betrachtet.

Aus diesem Grund wurde 2019 die oben erwähnte CAS ins Leben gerufen. Die Zusammenarbeit von Organisationen gegen geschlechtsspezifische und häusliche Gewalt mit IT-Sicherheitsfirmen sollte verbessert und eine größere Aufmerksamkeit auf das Thema Spionage-Software gelenkt werden. Im Zuge dessen wurde der »Stalkerware Report 2019« von der Firma Kaspersky, Anbieter*in einer Sicherheitssoftware und Mitglied der CAS, veröffentlicht. Kaspersky hat den Einsatz von Stalkerware analysiert und die Ergebnisse in

einem Bericht zusammengefasst. Dieser zeigt, wie schwer Spyware für Anti-Virus-Programme zu erkennen ist. Es konnte festgestellt werden, wie viele Nutzer*innen im Zeitraum von Januar bis August 2019 im Vergleich zum Vorjahr von Stalkerware bedroht waren und mit welcher Häufigkeit die Bedrohungen auftraten. 2019 gab es im genannten Zeitraum weltweit mehr als 518.223 Fälle, in denen die Antivirenprogramme entweder Stalkerware auf einem Benutzer*innengerät feststellten oder den Versuch der Installation einer solchen Stalkerware registrierten. Hier ist ein Anstieg von 373 % im Vergleich zum selben Zeitraum in 2018 zu beobachten (vgl. CAS 2019: 6).

In Europa belegen Deutschland, Italien und Großbritannien die drei obersten Plätze beim Verkauf von Stalkerware. Im April 2019 hat Kaspersky einen speziellen Alarm entwickelt, der Nutzer*innen vor kommerzieller Spionage-Software warnt, wenn diese auf dem Handy installiert wird oder wurde. So können Betroffene selbst entscheiden, ob sie die Software entfernen (lassen) oder weiterhin die Verbindung zur gewalttätigen Person aufrechterhalten wollen. Letzteres kann aus strategischen Gründen entschieden werden und eine Wiederaneignung von Kontrolle für die Betroffenen ermöglichen.

**Heimweg-Apps**

Diese Apps bieten virtuelle Begleitung auf Heimwegen an und sollen das subjektive Sicherheitsgefühl der Nutzer*innen steigern; hierfür werden allerdings persönliche Daten von Internetfirmen gesammelt und weiterverwendet (vgl. Pöting 2019: o.S.). Durch diese Apps kann ein*e Nutzer*in entweder professionell oder durch Freund*innen/Verwandte, der*die zuvor angefragt worden ist, begleitet werden. Diese ›Begleiter*innen‹ werden über GPS-Daten in Echtzeit darüber informiert, wo sich die Person mit der App befindet. Zusätzlich ist es möglich einen Notruf über die App abzugeben. Die Verbreitung und Normalisierung dieser Heimweg-Apps wird als problematisch angesehen, weil sie potenziellen Betroffenen die Verantwortung für mögliche gewalttätige Übergriffe im öffentlichen Raum zuschreibt, wenn sie sich diese scheinbare Hilfe nicht einholen (vgl. ebd.). Ein weiterer Kritikpunkt ist, dass die Apps massiv für Stalking missbraucht werden, weil durch sie der Aufenthaltsort der gestalkten Person immer einsehbar ist.

Auch diese Software funktioniert als Dual-Use Anwendung. Zum einen hat sie die Funktion als Heimweg-App, zum anderen können dieselben Funktionen aber auch als Ortungssoftware zur Überwachung verwendet werden.

Im Kontext von Stalking spielen solche Apps daher eine bedeutende Rolle, weil durch sie der Aufenthaltsort der gestalkten Person immer nachverfolgt werden kann.

**Zugang zu Internetseiten oder »Wo bist du gerade angemeldet?«**

»Wo bist du gerade angemeldet?« – unter dieser Funktion lässt sich einsehen, wo und mit welchem Gerät Profile und Konten (z.B. Facebook oder Netflix) angemeldet sind. Auch E-Mail-Services bieten diese Funktion immer öfter an. Sie soll anzeigen, ob sich eine unbefugte Person Zugang zu dem entsprechenden Profil verschafft hat. Im Kontext gewaltvoller Beziehungen erhält die gewaltausübende Person auf diesem Weg Informationen über den Aufenthaltsort der gestalkten Person. Hat die Betroffene nicht den alleinigen Zugriff, sollten so schnell wie möglich die Passwörter geändert und eine Zwei-Faktor-Authentifizierung aktiviert werden. Wird das Profil überwiegend von der gewaltausübenden Person genutzt, sollte es auf keinen Fall weiter von der Betroffenen genutzt werden.

**Heimliche visuelle Überwachung**

Durch Hacken der Webcam, Spyware oder versteckte Kameras in Wohn- oder Waschräumen kann eine Person ohne ihr Wissen visuell überwacht und gefilmt werden. Im Falle von Webcams ist dies am Statuslicht zu erkennen. Sollte das Licht unerwartet angehen, kann dies ein Hinweis darauf sein, dass die am Computer arbeitende Person und ihre Umgebung von außen betrachtet und gehört wird. Kleine Kameras können mit einem Lichtdetektor gefunden werden. Von versteckten Filmaufnahmen oder Fotos erfahren Betroffene in der Regel erst, wenn diese irgendwo – z.B. auf Pornoseiten – veröffentlicht werden und sie Kenntnis davon erlangen.[6] Für potenziell Betroffene bedeutet dies, sich eine große Menge dieser Aufnahmen anschauen zu müssen, um eine eigene mögliche Viktimisierung festzustellen.

**Identitäts- und Datendiebstahl**

Es gibt weder eine gültige Definition noch eine Unterscheidung zwischen den Begriffen »Online-Kriminalität«, »Cyber-Kriminalität« und »Internet-Kriminalität«. Grundsätzlich können unter Cybercrime zunächst alle Straftaten verstanden werden, die unter Ausnutzung der Informations- und Kom-

6 Wie z.B. bei den Aufnahmen auf einer Toilette des Musikfestivals »Monis Rache« und Aufnahmen aus der Dusche des »Fusion Festivals«.

munikationstechnik oder gegen diese begangen werden (vgl. Huber 2019: 14f.). Der Begriff »Cybercrime« ist in Deutschland besonders stark durch den Straftatbestand des Computerbetrugs (§ 263a StGB) bzw. die Polizei[7] und die Strafverfolgungsbehörden geprägt. Darunter fällt Internet-Kriminalität (vgl. Kirwan/Power 2013) wie etwa: Datendiebstahl durch Hacken, Datendiebstahl mittels Social Engineering[8], Identitätsdiebstahl, Online-Betrug, Kreditkartenbetrug, Hack- und Virenangriffe auf Geräte mit und ohne IoT-Funktionen, Angriffe von Schadprogrammen auf Computer und Server mit Botnetzwerken[9] sowie Installation von Schadsoftware (englisch malware) mittels Viren, Würmern und Trojanern.

Die Lageberichte zur IT-Sicherheit in Deutschland des Bundesamts für Sicherheit in der Informationstechnik bestätigen den Trend zur Kommerzialisierung und Professionalisierung der Internetkriminalität. Betroffene sind vor allem Behörden, Unternehmen, Banken und auch Privatanwender*innen (vgl. BSI 2019: 7ff.). Staatliche Bemühungen zur Prävention von Cybercrime beziehen sich jedoch aktuell vornehmlich auf betroffene Unternehmen und staatliche Infrastruktur.

Aus der Beratungspraxis mit betroffenen Frauen ist bekannt, dass Strafverfolgungsbehörden bei Vergehen, die unter Cybercrime fallen und einen finanziellen Schaden für die Betroffenen mit sich bringen, eher ermitteln, als bei anderen Formen geschlechtsspezifischer digitaler Gewalt, für die es keine spezialisierten Abteilungen gibt. In privaten Beziehungen werden Daten und Passwörter häufig entweder bereitwillig oder durch Ausüben von Druck geteilt. So kann dieser Zugang verwendet werden, um die betroffene Person

7 Die statistische Grundlage für das »Bundeslagebild Cybercrime« sind die Daten der Polizeilichen Kriminalstatistik (PKS). Diese umfasst das polizeiliche Hellfeld der Straftaten, einschließlich der mit Strafe bewehrten Versuche, die polizeilich bearbeitet und an eine Staatsanwaltschaft abgegeben wurden (vgl. BSI 2019: 2ff.).

8 Bei Social Engineering oder Social Hacking versucht eine angreifende Person eine andere Person dazu zu bringen, dass sie unabsichtlich oder absichtlich im guten Glauben sensible Informationen an die angreifende Person weitergibt. Ein sehr beliebter Ansatz ist es beispielsweise, sich gegenüber Mitarbeitenden über einen Telefonanruf als vermeintliche*r Systemadministrator*in auszugeben und die Angaben eines Benutzer*innen-Passworts zu erbitten, um angeblich wichtige administrative Aufgaben durchzuführen (vgl: Eckert 2014: 27).

9 Als Botnetz wird ein Verbund von Rechnern (Systemen) bezeichnet, die von einem ferngesteuerten Schadprogramm (Bot) befallen sind. Mit einem solchen Netzwerk können z.B. SPAM-Angriffe durchgeführt werden, die sehr rentabel für die Betreiber*innen des Botnetz sind (vgl. BSI 2019: 77).

zu diffamieren oder finanziell stark zu schädigen. Aus Fachberatungsstellen ist zudem die Täterstrategie bekannt, dass auch nach einer vollzogenen Trennung mit Identitätsdiebstahl online teure Produkte auf Rechnung oder Kreditkarte bestellt, an beliebige Adressen geliefert und in der Regel nicht bezahlt werden. Durch die nicht gezahlten Rechnungen oder das überzogene Kreditkartenlimit gerät die betroffene Person in ernste finanzielle Schwierigkeiten. Inkassobüros schalten sich ein und der SCHUFA-Score verschlechtert sich, was wiederum Einfluss auf die Anmietung von Wohnungen oder Abschlüsse von Verträgen haben kann. Das Motiv des Täters kann auch die Verschuldung der Betroffenen sein, beispielsweise um im Zuge eines Sorgerechtsstreites vor Gericht anzuzweifeln, dass die finanzielle Versorgung der gemeinsamen Kinder ausreichend gewährleistet ist.

Während bei Cyberkriminalität gegenüber Unternehmen vorwiegend ein finanzielles Interesse im Vordergrund steht, ist dies bei Cyberkriminalität im Kontext Gewalt aus dem sozialen Nahraum und Stalking nicht immer der Fall. Hier geht es oftmals um die missbräuchliche Nutzung personenbezogener Daten, um Macht oder Kontrolle gegenüber der Person zu erlangen bzw. diese auszubauen. Dies ist z.B. der Fall, wenn Täter etwa unter dem Namen der Betroffenen E-Mails an Familie, Freund*innen oder Kolleg*innen verschicken. Es kommt ebenfalls vor, dass betroffene Personen – ohne ihr Wissen – auf Datingseiten oder pornografischen Plattformen mit ihrer öffentlich einsehbaren Telefonnummer angemeldet werden. Der Betroffenen soll sozialer, emotionaler und finanzieller Schaden zugefügt werden. Es kann durch die Tat aber auch zu körperlichen oder sexuellen Angriffen kommen.

Eine negative Online-Reputation kann sich für die Betroffene schnell und gleichzeitig langfristig negativ auswirken und ist nur schwer zu entkräften. Eine für den Täter dabei sehr effektive Methode ist die Eingabe des Namens der betroffenen Person in die sogenannten META-Tags von Webseiten. META-Tags werden sehr aufmerksam von Suchmaschinen gelesen, was als Konsequenz – etwa bei einer Google-Suche – den eingetragenen Namen in Verbindung mit einer fragwürdigen Seite erscheinen lässt (vgl. Port 2012: 36).

Eine besondere Form des Identitätsdiebstahls ist das sogenannte Nicknapping, ein englischer Neologismus aus den Wörtern »nickname« und »kidnapping«. Der Täter tritt hierbei online unter dem Namen oder Pseudonym einer anderen Person auf, um das Vertrauen der Betroffenen zu gewinnen. So lassen sich Betroffene unter Umständen auf ein intensives Gespräch ein, bei dem Informationen über Pläne und Aufenthaltsorte preisgegeben werden.

**Doxing**

Eine weitere Erscheinungsform digitaler Gewalt ist das Sammeln und Verbreiten von privaten Informationen über die betroffene Person. In Chaträumen, Massen-E-Mails, auf Social Media-Portalen, Blogs und Homepages kann der Täter persönliche (Kontakt-)Daten der Betroffenen an andere Internetnutzer*innen weitergeben. Hierfür werden z.B. Newsletterabos oder Eintragungen in diversen Kleinanzeigen gemacht. Zudem können vertrauliche Details etwa über die (vermeintliche) Sexualität, den gesundheitlichen oder finanziellen Status der betroffenen Person verbreitet werden. Intime und/oder manipulierte Bilder werden hierbei an sämtliche Kontakte verschickt, in den meisten Fällen in Verbindung mit diffamierenden Lügen und Gerüchten. Die Folgen solcher Informationen im Netz ist nicht nur die Gefährdung der Person, die Verletzung ihres Rufes und soziale Isolation, sondern können auch unmittelbar ökonomischer oder sozialer Art sein, wenn beispielsweise Betroffene deshalb keine Wohnung/Arbeitsstelle bekommen.

## Belästigung, Diffamierung, Beleidigung, Bedrohung im Netz

Bei Belästigung im Netz (Cyberharassment) handelt es sich um die unaufgeforderte Zusendung von belästigendem Material oder Nachrichten. Oft werden dabei sexualisierte, sexistische, misogyne Beleidigungen, Diffamierungen, Beschimpfungen oder Drohungen ausgesprochen. Dies geschieht durch das Verfassen und Versenden von zahlreichen unerwünschten, belästigenden und bedrohenden Nachrichten, SMS und E-Mails sowie Kommentaren in sozialen Netzwerken. Der Inhalt kann auch bildbasierte digitale Gewalt enthalten. Hierbei werden falsche oder vertrauliche Informationen oder diffamierende Behauptungen unter sämtlichen Kontakten der Betroffenen verbreitet. Hierfür werden gezielt falsche Einträge oder Fake Profile in Chats, Blogs, sozialen Netzwerken oder pornografischen Seiten über die Betroffene gestreut bzw. in ihrem Namen verfasst.

Einzeltäter sind in der Regel den Betroffenen bekannt; bei Tätergruppen können nicht alle Täter bekannt sein. Das Internet ermöglicht es dem Täter problemlos einen neuen Namen, andere Identitätsmerkmale und einen Foto-Avatar[10] zu erfinden, um das Online-Selbst zu formen (vgl. Stroud/Cox 2018:

10 Avatare sind Bilder mit Icons oder einer 3D-Figur und zeigen Menschen, Tiere oder Fantasiewesen.

295) und somit anonym im Internet zu agieren[11]. Diese Möglichkeiten können auch die Betroffenen als Gegenstrategie nutzen, wenn sie trotz erfahrener digitaler Gewalt online agieren wollen.

Wie die folgenden Beispiele verdeutlichen, beginnt diese Form der Gewalt häufig nach einem Streit oder Kontaktabbruch seitens der Betroffenen oder wenn diese auf eine Annäherung nicht positiv reagiert:

- Nach Beendigung der Beziehung hinterlässt z.B. der Ex-Freund diffamierende und rufschädigende Kommentare und Bewertungen in einem Online-Bewertungstool und stachelt den Freundeskreis an, es ihm gleich zu tun. Die Betroffene ist eine Woman of Color, als selbstständige Arbeiternehmerin tätig und von Online-Bewertungen und ihrer Online-Präsenz abhängig. Die betroffene Person erlebt massive rassistische und/oder sexistische Kommentare in diesem Forum. Sie erleidet daraufhin schwerwiegende finanzielle Einbußen, weil Kund*innen wegen der schlechten Bewertungen nicht mehr mit ihr zusammen arbeiten wollen.
- Nach schwerer körperlicher Gewalt gegenüber einer Frau und ihren Kindern, flüchten diese in den anonymen Schutzraum eines Frauenhauses. Der Gewalttäter ist außer sich und verfasst Nachrichten mit Beleidigungen und intimen Bildern, die in der Zeit der Beziehung entstanden sind. Diese verschickt er an ihre Freund*innen, Bekannte und Verwandte. Zum einen verliert die Betroffene ihr soziales Ansehen, zum anderen sorgt die eigene Scham dafür, dass sie und ihre Kinder sozial isoliert werden.
- Eine Person lehnt die Annäherung eines Arbeitskollegen bei einer Firmenfeier ab. Tage später wird in einem WhatsApp-Gruppenchat des Arbeitsteams eine sexualisierte Fotomontage von der Person ohne Zustimmung geteilt. Die abgebildete Person befindet sich auch in diesem Chat, fühlt sich belästigt und stark beschämt.

### Beleidigungen im Netz

Beleidigungen im Netz gegen eine Person auszusprechen, ist wohl das am einfachsten anwendbare digitale Gewaltmittel. Der Täter benötigt dazu nur einen Internetzugang. Auch hier agiert der Täter nicht immer kenntlich und öffentlich für die Betroffenen. Beleidigungen können ohne Wissen der Betroffenen ausgesprochen werden.

11 Siehe Beitrag: Funktionsprinzipien des Internets und ihre Risiken im Kontext digitaler geschlechtsspezifischer digitaler Gewalt.

**Fake Profile in sozialen Netzwerken**

Hier werden Fake Profile mit Bildern und Informationen aus realen Profilen erstellt. Zusätzlich wird die Sprache und Emojis der Betroffenen kopiert. Bei manchen Betroffenen sind die Fake Profile teilweise so gut kopiert, dass sie selbst unschlüssig sind, ob es nicht doch ihr echtes Profil ist. Auf diesen Fake Profilen streut die gewaltausübende Person Gerüchte, es werden Fotomontagen geteilt oder es wird zu Gewalt aufgerufen.

**Gerüchte im Netz/›Mobbingseiten‹ erstellen**

Aus Beleidigungen und Diffamierungen können Gerüchte werden, die sich im Internet verbreiten. Diese Gerüchte kann der Täter gestreut haben, sie können aber auch von Unterstützer*innen verbreitet werden. Aus diesen Zusammenschlüssen können wiederum Mobbingseiten erstellt werden. Dort werden Informationen und Bilder der Betroffenen digital abgebildet und verbreitet. Diese Bilder der Betroffenen können mittels einer Gamification, also in einer spielerisch anmutenden Art und Weise von Dritten verändert werden. Ein Beispiel dazu kann sein, dass ein Foto von der Betroffenen angeklickt werden kann und danach werden Verletzungen auf dem Körper derselben sichtbar.

**Ständiges Hinzufügen in Nachrichtengruppen**

Personen können gegen ihren Willen immer wieder in Nachrichtengruppen hinzugefügt werden. So hat es Fälle gegeben, in denen Frauen aus diesen Gruppen rausgegangen sind, weil dort pornografische Inhalte und/oder Beleidigungen geteilt und sie wiederholt in dieselbe Gruppe hinzugefügt wurden. So waren sie der Belästigung immer wieder ausgesetzt und ihre Telefonnummer war für die Gruppenmitglieder sichtbar. Einige Messengerdienste haben inzwischen diese Sicherheitslücke nachgebessert.

**Täuschungs-Software für Belästigung**

Diese Software kann so eingestellt werden, dass sie mit unbekannter Telefonnummer in regelmäßigen Abständen Anrufe tätigt bzw. Nachrichten schreibt (vgl. Safety Net Canada 2013: 6). Mit einer stimmeverstellenden Software können Stimmen so manipuliert werden, dass sie tiefer oder langsamer klingen, so kann in vielen Fällen die Stimme der gewaltausübenden Person nicht erkannt werden. Auf diese Weise ist es auch möglich, dass sich z.B. ein Gewalttäter als eine andere Person am Telefon ausgibt, beispielsweise als Mitarbei-

terin des Jugendamtes, und die (Ehe-)Partner dazu bringt, an bestimmtem Ort und Zeit zu erscheinen.

**›Slut Shaming‹ Foren**
In Foren wird eine Person öffentlich oder privat beleidigt, weil sie ihre Sexualität tatsächlich oder vermeintlich nicht auf eine Weise ausdrückt, die mit den patriachalen und heteronormativen Erwartungen übereinstimmt. Hierzu gehören beispielsweise homosexuelles Begehren, ein als promiskuös wahrgenommenes Sexualleben und/oder das Anbieten sexueller Dienstleistungen.

**Sexanzeigen**
Sexanzeigen werden von den Tätern auf pornografische Internetseiten gestellt. Die Betroffenen wissen in den meisten Fällen nichts davon. Erst durch die Reaktionen potenzieller Freier erfahren sie davon. Da in diesem Zusammenhang häufig Adresse und Telefonnummer oder E-Mail-Adresse veröffentlicht werden, entsteht eine reale Gefahr, wenn potentielle Kunden vor der Tür stehen und verärgert über die nichterhaltene Leistung sind bzw. diese erhalten wollen. Es sind Fälle bekannt, in denen Täter Bilder und Daten ihrer (Ex-)Partner*innen unter der Angabe veröffentlichen, dass sie sexuelle Dienstleistungen anböten oder an spontanem Sex und speziellen Praktiken interessiert seien. Die Betroffenen sind daraufhin häufig unzähligen digitalen oder auch direkten Kontaktaufnahmen und Übergriffen ausgesetzt. Bildbasierte Gewalt in Verbindung mit Informationen zum Wohnort der Betroffenen kann in diesem Kontext zu massiver sexualisierter Gewalt und Vergewaltigungen durch unbekannte Täter führen.

**Sexuelle Belästigung auf Dating Plattformen**
Frauen und trans Personen, die auf Datingplattformen angemeldet sind, erleben immer wieder, dass sie unaufgefordert und unerwünschte Bilder und Texte mit sexuellem Inhalt erhalten; hierzu gehören auch Bilder von Genitalien, sogenannte Dickpics.

## Bildbasierte sexualisierte Gewalt

Im deutschsprachigen Raum hat sich bisher kein einheitlicher Oberbegriff für bildbasierte Gewalthandlungen durchgesetzt. Im Medien- und Alltagsdiskurs haben sich für einige Formen eher umgangssprachliche Bezeichnungen, wie

z.B. ›Revenge Porn‹, ›Nonconsensual porn‹ und ›Kinderpornografie‹ etabliert. Die Verwendung solcher Terminologien ist jedoch hochproblematisch, weil diese die Gewalterfahrung unsichtbar machen und Gewaltdynamiken nicht berücksichtigen. Auch der Begriff der Pornografie eignet sich in diesem Zusammenhang nicht als adäquate Bezeichnung. Inhalte, die in pornografische Zusammenhänge gestellt werden, aber ohne Zustimmung erstellt und verbreitet wurden, stellen sexualisierte Gewalt dar und keineswegs Pornografie.

Viele der verwendeten Begriffe entstammen dem Bereich der Kinder- und Jugendschutzarbeit im digitalen Raum. Digitales Bildmaterial spielt aber ebenso eine Rolle bei (Ex-)Partnerschaftsgewalt und sexualisierter Gewalt gegen Erwachsene. Die systematische Auseinandersetzung mit bildbasierter Gewalt macht es daher notwendig sehr spezifisch zu betrachten, unter welchen Voraussetzungen das Bildmaterial erstellt und verbreitet wird. Um möglichst viele Gewalthandlungen im Zusammenhang mit digitalem Bildmaterial erfassen zu können, wird hier in Anlehnung an die englische Terminologie »image-based sexual abuse« der Begriff »bildbasierte sexualisierte Gewalt« verwendet, der erstmals 2015 von den Rechtswissenschaftlerinnen Clare McGlynn and Erika Rackley eingeführt wurde (vgl. McGlynn/Rackley 2017: 534).

Die Vielzahl technischer Möglichkeiten mit denen Bilder und Videos – auch ohne Wissen der Abgebildeten – erstellt, manipuliert und zielgruppenspezifisch verbreitet werden können, bringen grundlegende digitalisierungsspezifische Effekte auf geschlechtsspezifische Gewalt mit sich. Bildbasierte (sexualisierte) digitale Gewalt umfasst eine Vielzahl von Gewalthandlungen, die durch die Erstellung, Verbreitung und anderweitige Verwendung digitaler – meist intimer – Bilder gekennzeichnet sind. Charakteristisch sind häufig der sexualisierte diffamierende Kontext, die Anfertigung und/oder Veröffentlichung gegen den Willen der (vermeintlich) abgebildeten Person und eine schwer zu kontrollierende Verbreitung, die sich äußerst belastend und potentiell (re-)traumatisierend auf die Betroffenen auswirken kann. Zudem kann auch sexualisierte Belästigung durch das unerwünschte Zusenden von pornografischem Bildmaterial, welches nicht die Betroffenen zeigt, als bildbasierte Gewalt verstanden werden.

Von intimem Bildmaterial wird ausgegangen, wenn die Genitalien oder der Analbereich einer Person – unbedeckt oder in Unterwäsche, die Brüste einer Person (vornehmlich von Frauen, trans und inter* Personen) und/oder bestimmte Posen oder Aktivitäten (z.B. sexuelle Aktivitäten, Toilettennutzung, Duschen, An- oder Ausziehen von Kleidung) zu sehen sind. Auch der Kon-

text in dem Bilder erstellt und verbreitet werden, kann relevant für die Einordnung als grenzverletzendes, gewaltvolles Verhalten sein, so z.B. bei der Darstellung einer Person ohne spezifische religiöse Kleidung oder ohne eine Perücke, die sie sonst in der Öffentlichkeit tragen würde.

Die Zunahme bildbasierter Gewalt im Rahmen von Mobbing, sexualisierter Gewalt oder Gewalt nach Trennungen wird von den Frauenberatungsstellen und Frauennotrufen in Deutschland seit der Einführung von Handys mit Kamerafunktion und integrierten Schnittstellen zur Datenübertragung beobachtet. Neben Formen von Online-Belästigungen und Bedrohungen konnte bildbasierte sexualisierte Gewalt bereits seit Mitte der 2000er-Jahre als wesentliche digitalisierungsbedingte Entwicklung von geschlechtsspezifischer Gewalt im sozialen Nahraum festgestellt werden. Bislang gibt es hierzu keine Studien in Deutschland. Die weltweit erste Untersuchung zu bildbasierter sexualisierter Gewalt wurde 2019 in Australien, Neuseeland und Großbritannien durchgeführt (Powell u.a. 2020). Für alle drei Länder konnten sehr ähnliche Verteilungsraten – zwischen 35 % und 39 % – festgestellt werden. Es wurde deutlich, dass ungefähr jede dritte befragte Person bereits mindestens eine Form bildbasierter Gewalt erlebt hat. Abgefragt wurden hier Erfahrungen, die das Anfertigen und das Teilen von intimen Bildern gegen den Willen oder die Androhung der Verbreitung von Bildern beinhalteten (vgl. ebd.).

Die geschlechtsbezogene Auswertung der australischen Daten stellt wesentliche Unterschiede zwischen Männern und Frauen im Erleben bildbasierter Gewalt fest. Männer und Frauen erfahren zwar in einem ähnlichen Umfang bildbasierte sexualisierte Gewalt, die damit verbundenen Belastungen und negativen Folgen fallen für Frauen jedoch deutlich massiver aus (vgl. ebd.: 8). Generell berichten fast alle betroffenen Frauen (92,1 %) von negativen Reaktionen auf die erlebte Gewalt (gegenüber 75,9 % der betroffenen Männer) (vgl. ebd.). Vor allem nicht-heterosexuelle Frauen erfahren signifikant häufiger Belästigung im Rahmen bildbasierter Gewalt und sind im Besonderen mit negativen Folgen für Gesundheit und soziale Beziehungen konfrontiert. Die Ergebnisse bestätigen die Relevanz bildbasierter Gewalt für geschlechtsspezifische Gewaltdynamiken im sozialen Nahraum. Wichtig für Intervention und Prävention ist insbesondere der Befund, dass fast 90 % der Betroffenen die Person kannten, von der die Gewalt ausging. 60,9 % der Täter*innen waren (Ex-)Partner*innen (vgl. ebd.).

Auch eine Zunahme bildbasierter Gewalt innerhalb der letzten Jahre kann anhand der australischen Daten festgestellt werden. Vor der länderübergreifenden Studie wurde im Jahr 2016 bereits eine ähnliche Erhebung in Austra-

lien durchgeführt. Zu diesem Zeitpunkt gab noch jede fünfte befragte Person an, mindestens eine Form bildbasierter digitaler Gewalt erfahren zu haben. 2019 traf dies bereits auf jede dritte Person in Australien zu (vgl. RMIT University Australia 2020: o.S.). Die Ergebnisse deuten zudem darauf hin, dass vor allem Täterverhalten und neue Tatmuster den Anstieg begründen. So stellte die Follow-Up Studie eine größere Anzahl von Fällen fest, bei denen Bildaufnahmen heimlich erstellt wurden, während Fälle mit Bildern, die einst konsensuell erstellt und verschickt wurden, nicht anstiegen (vgl. Powell u.a. 2020: 11f.).

Für eine Systematisierung verschiedener Formen und Methoden bildbasierter sexualisierter Gewalt ist es hilfreich zu unterscheiden, ob die betreffenden Aufnahmen ursprünglich mit Einverständnis der abgebildeten Person oder heimlich bzw. unter Zwang erstellten wurden. Wie sich Täter das Bildmaterial nach deren Entstehung aneignen und in welcher Form daraufhin eine Verbreitung stattfindet, sind weitere grundlegende Unterscheidungsmerkmale.

*Abb. 1: Bildbasierte Gewalt, Hartmann 2020.*

### Verwendung einvernehmlich erstellter intimer Bilder

Intime Aufnahmen, die von den Betroffenen selbst oder mit deren Einverständnis aufgenommen wurden, finden in zahlreichen Gewaltzusammenhängen Anwendung. In der Regel teilen Betroffene das betreffende Bildmaterial zuvor mit Einzelpersonen oder veröffentlichen dieses ohne bestimmte Adressat*innen auf ihren eigenen Internetpräsenzen.

Intime Bilder anzufertigen und mit anderen digital zu teilen, ist für viele ein selbstverständlicher Bestandteil von romantischen/sexuellen Beziehungen, Online-Dating oder in manchen Fällen der Erwerbsarbeit. Der Gewalterfahrung geht in diesem Kontext meist ein Vertrauensverhältnis und ein geteiltes implizites oder explizites Einverständnis zum ausschließlich privaten Verfügen über die Bilder voraus. Häufig werden diese im Vertrauen geteilten Bilder allerdings Bestandteil von Gewaltdynamiken, wenn sich z.B. das Verhältnis zwischen den beteiligten Personen ändert. Szenarien, in denen der Ex-Partner nach einer Trennung intime Aufnahmen der Ex-Partnerin an ihre Familie schickt und/oder im Internet veröffentlicht bzw. Fälle, in denen ›Sex-Videos‹ als Druck- und Nötigungsmittel verwendet werden, können als bildbasierte sexualisierte Gewalt im engeren Sinn verstanden werden. Bildbasierte Gewalt kann dabei heißen, dass Täter durch die Androhung der Veröffentlichung an einen bestimmten Adressat*innenkreis (Eltern, Freund*innen, Arbeitgebende) die Zurücknahme einer Trennung oder den Verzicht auf eine Anzeige erwirken wollen. Auch die Personen, die diese Aufnahmen unaufgefordert erhalten, erleben zumindest sexuelle Belästigung, indem sie mit diesen Bildern konfrontiert werden.

Auch intime Bilder, die etwa beim Sexting[12] ausgetauscht wurden, ohne dass längerer Kontakt bestand, landen nicht selten ohne Wissen der Betroffenen auf einschlägigen Plattformen und in Foren. Auch in diesem Kontext nutzen Täter die betreffenden Aufnahmen, um ein Bedrohungsszenario zu kreieren, die Betroffenen öffentlich bloßzustellen, zu beleidigen oder weiteren Kontakt zu erzwingen.

#### Aneignung von Bildmaterial

Zu diesem Bereich bildbasierter Gewalt gehören Fälle, bei denen die selbstbestimmte Veröffentlichung (intimer) Bilder auf Social Media Accounts und

12 Der Begriff Sexting (engl. sex und texting) wird verwendet, um das einvernehmliche digitale Versenden oder Austauschen intimer Fotos oder Texte mit sexuellem Inhalt zu beschreiben.

anderen digitalen Räumen ›außer Kontrolle gerät‹, indem fremde Accounts die Aufnahmen in spezifischen digitalen Räumen verbreiten, um die abgebildete Person zu beleidigen und bloßzustellen. Dies ist z.B. der Fall, wenn Sexarbeiter*innen intime Bilder und Videos als Dienstleistungen anbieten und Kund*innen diese Bilder unbefugt weiterverbreiten. Solche Übergriffe sind nicht nur aus ökonomischer Perspektive relevant und existenzgefährend für die Betroffenen, sie können zudem Anlass weiterer Gewalt sowie eine massive Bedrohung ihrer digitalen und körperlichen Sicherheit darstellen.

Nicht immer besteht dabei eine Beziehung zwischen den abgebildeten Personen und denjenigen, die die Bilder nutzen. Viele feministische Aktivist*innen und im Netz sichtbare Frauen machen die Erfahrung, dass Bilder, die sie für ihren Netzauftritt und in beruflichen Zusammenhängen veröffentlichen, für solche Manipulationen verwendet und mit dem Ziel ihnen zu schaden, veröffentlicht werden. An solchen Angriffen können sich unzählige User*innen beteiligen und bestärkt fühlen. Häufig kommt es dadurch zur Ausweitung der Gewalt wie dem *Doxing* (s.u.) von Informationen über die Betroffenen und darauffolgendem Stalking und Belästigungen.

### Deepfakes

Eine spezifische Form der gewaltvollen Aneignung von online verfügbarem Bildmaterial ist die Erstellung sogenannter Deepfakes. Hierbei können mit Hilfe entsprechender Programme etwa die Mimik von live übertragenen Gesichtern in Echtzeit gefälscht und vermittelte Botschaften manipuliert werden. Die zugrundeliegende Technologie ermöglicht es, allein auf Basis weniger online verfügbarer Bilder, das Gesicht einer Person täuschend echt in Videos einzufügen (vgl. Qin 2019: o.S.). Die gesellschaftlichen Auswirkungen und Gefahren dieser neuen, sich rasant entwickelnden Technologie werden vor allem anhand der Gefahr von Fake News diskutiert. Laut einer 2019 veröffentlichten Analyse des niederländischen Cybersecurity-Unternehmens Deeptrace, hatten jedoch 96 % aller zu diesem Zeitpunkt im Internet identifizierten Deepfake Videos pornografische Inhalte (vgl. Ajder u.a. 2019: 1ff.). Die Auswertung der pornografischen Deepfakes ergab laut Deeptrace, dass ausschließlich Frauen[13] betroffen waren (vgl. Cox 2019: o.S.). Die Expert*innen von Deeptrace gehen außerdem davon aus, dass die Anzahl solcher Videos

13 Es ist zu vermuten, dass die Zuordnung anhand von weiblich gelesenen Körpern vorgenommen wurde.

in den nächsten Jahren immens wachsen und die dahinter stehende Technologie innerhalb kurzer Zeit besser, billiger und einfacher anzuwenden sein wird (vgl. Ajder u.a. 2019: 3ff.). Bereits jetzt werden Deepfakes als eine der größten, aus KI-Anwendung resultierenden Gefahren der nächsten Jahre diskutiert (vgl. o.A. 2020). Selbst das Potential des Gebrauchs autonomer Fahrzeuge als Waffe oder der Nutzung von KI im Rahmen von Fake News schätzen Forscher*innen des University College London (UCL) in einer Studie als geringer ein (vgl. Bastian 2020: o.S.). Es ist davon auszugehen, dass diese Form der digitalen Gewalt künftig zunehmen und an Relevanz gewinnen wird.

Hacken/Diebstahl/Leaks

Täter*innen können auch durch Diebstahl an selbstbestimmt erstelle intime Aufnahmen gelangen – zum Beispiel aus der Cloud der Betroffenen, die mit dem Smartphone verknüpft ist und automatisch alle Bildaufnahmen abspeichert. Hierfür kann es notwendig sein, Sicherheitsmaßnahmen wie Passwörter zu überwinden. Aber auch unbeaufsichtigte und ungesicherte Datenträger oder der Zugriff auf Online-Accounts, aus denen sich nicht ausgeloggt wurde, können Unbefugten den Zugriff ermöglichen. Zudem kann es Teil der Täterstrategie sein, intime Aufnahmen nicht selbst zu veröffentlichen, sondern an Dritte, wie z.B. Pressevertreter*innen, weiterzuleiten, um eine Veröffentlichung vor größerer Öffentlichkeit mit maximaler medialer Aufmerksamkeit zu erwirken.

**Art der Verbreitung/Ort der Veröffentlichung**

Die Vielfältigkeit digitaler Medien und Kommunikationswege eröffnet diverse Möglichkeiten intime Bilder zu verbreiten und gezielt an bestimmte Personen zu übermitteln. Für die Wahl der Verbreitungsmethode kann es u.a. von Bedeutung sein, über welchen Kommunikationsweg die Bilder ursprünglich übermittelt wurden und welche Wirkung sich die gewaltausübende Person davon verspricht. Die Übermittlung an das direkte soziale Umfeld der Betroffenen kann es erschweren, dass diese Unterstützung und Rückhalt erhalten und basierend auf Schamgefühlen oder Verurteilung von Außen letztlich zu sozialer Isolation führen. Eine Veröffentlichung in sozialen Netzwerken, die die Bilder in direkte Verbindung mit dem Account der Betroffenen bringt, kann von zahlreichen Menschen bemerkt werden und konfrontiert die Betroffenen nicht nur mit deren Reaktionen, sondern zwangsläufig auch mit der Ungewissheit darüber, wie oft die Bilder bereits anderweitig kopiert und

verbreitet wurden. Eine Veröffentlichung in anonymen Foren, beispielsweise sogenannten ›Slut Shaming Foren‹, ohne dass Betroffene davon erfahren, kann Tätern zur Bestätigung des eigenen Narrativs oder dem Einholen von Zuspruch und sozialer Bestätigung dienen.

Außerdem kann davon ausgegangen werden, dass Videos von sexuellen Aktivitäten, deren Anfertigung zum Zeitpunkt der Aufnahme zugestimmt wurde, ohne Wissen und Zustimmung der Betroffenen, auf Porno-Portalen verbreitet werden können. In diesem Zusammenhang sind Fälle dokumentiert, bei denen außerdem der Name, persönliche Informationen und sogar das Facebook-Profil der Betroffenen mit dem Video verlinkt wurden (vgl. Cole/Maiberg 2020: o.S.).

### Verwendung heimlich erstellter Aufnahmen

Das Anfertigen und Verbreiten heimlicher Aufnahmen ist ein Phänomen bildbasierter sexualisierter Gewalt, welches erst seit kürzerer Zeit Beachtung findet. Häufig geht es um Aufnahmen, die mit Hilfe versteckter Kameras oder Smartphones in geschützten Räumen wie öffentlichen Toiletten oder Umkleidekabinen gemacht werden und daraufhin unter einschlägigen Kategorien auf Pornoportalen oder in privaten/halböffentlichen Netzwerken ausgetauscht werden (vgl. Beer 2018: o.S.). Ebenfalls wird auf diese Art Bildmaterial verbreitet, das Personen ohne ihr Wissen bei sexuellen Handlungen zeigt. Übergriffe im öffentlichen Raum, bei denen Aufnahmen unter den Rock einer Person gemacht werden, werden auch als »Upskirting« bezeichnet. Journalistische Recherchen zeigen zudem, dass Aufnahmen aus Privaträumen ins Internet gestellt werden (vgl. hierzu Schlosser 2020), was vermuten lässt, dass Täter zudem im eigenen sozialen Umfeld agieren. Auch von Partnerschaftsgewalt betroffene Frauen, berichten, dass sie vermutlich jahrelang in der eigenen Wohnung gefilmt worden sind, ohne zu wissen, was mit den Aufnahmen geschehen ist.

Über das Ausmaß und die Verbreitung von heimlichen sexualisierten Aufnahmen in Deutschland gibt es keine Erkenntnisse. Internationale Untersuchungen weisen darauf hin, dass diese Methode bildbasierter Gewalt immer häufiger angewendet wird und in den letzten Jahren zugenommen hat (vgl. Powell u.a. 2020: 11f.). In Südkorea beispielsweise weisen Feminist*innen schon seit längerer Zeit auf die Alltäglichkeit derartiger Eingriffe in die Privatsphäre und die fatalen Konsequenzen für Betroffene und die öffentli-

che Sicherheit hin (vgl. Tai 2018: o.S.)[14]. Immer wieder werden in Südkorea Fälle großen Ausmaßes bekannt (vgl. Peters 2019: o.S.), Medien sprechen bisweilen von einer regelrechten ›Epidemie‹ (vgl. Bešić 2019: o.S.). Eine Studie der Vereinigung koreanischer Anwältinnen stellte fest, dass im Jahr 2015 bereits ein Viertel (24,9 %) aller erfassten Sexualdelikte im Zusammenhang mit versteckten Kameras standen (vgl. Kang 2018: o.S.).

In Deutschland findet erst seit Kurzem eine wahrnehmbare öffentliche Diskussion und Einordnung dieses Problems als geschlechtsspezifische Gewalt statt. Ausschlaggebend waren die Kritik der zu diesem Zeitpunkt noch vorliegenden Straffreiheit bei Upskirting-Delikten und das Bekanntwerden konkreter nachweisbarer Fälle von heimlichen Aufnahmen in Festival-Toiletten (siehe z.B. Wiedemann 2020). Nicht nur öffentliche Toiletten, sondern auch Solarien, Fitnessstudios, Schwimmbädern, Saunen, öffentlichen Verkehrsmitteln, Hotels oder Airbnb-Wohnungen können Orte heimlicher Aufnahmen sein.

### Verbreitung und Anfertigung von Aufnahmen (sexualisierter) Gewalt

Intimes Bildmaterial in den Händen von Tätern zeigt sich als wirkmächtiges Gewalt- und Druckmittel. In der Regel verfügen die Täter über weitere Informationen über die Betroffenen, sei es aus (vorangegangenen) sozialen Beziehungen oder durch das Zusammentragen öffentlich verfügbarer Daten. In Verbindung mit diesen Informationen können intime Bilder zielgenau zur Nötigung, Bedrohung und Kontrolle Betroffener eingesetzt werden und den Täterkreis immens erweitern. Auch Betroffene wissen sehr genau um die Funktionsweise digitaler Medien und der zusätzlichen Gefährdung durch eine unkontrollierbare Verbreitung. Täter können somit allein durch die Androhung einer Veröffentlichung immense Macht über Verhalten und Verfassung der Betroffenen erlangen.

Die Verbreitung intimer Bilder erfolgt nicht selten in einem bewusst gewählten frauenfeindlichen, gewaltvollen Milieu. Es gibt unzählige Seiten und Plattformen, auf denen vor allem bzw. ausschließlich intime Bilder und private Informationen von Frauen und queeren Menschen veröffentlicht und mit

14 Bereits seit den 1990er-Jahren hat sich dafür ein eigener Begriff etabliert. »Molka« ist die Kombination aus dem koreanischen Wort »mollae« (Geheimnis) und dem englischen »camera« (vgl. Tai 2018: o.S.). An anti-molka Protesten beteiligen sich in Südkorea regelmäßig mehrere zehntausend Menschen (ebd.).

einer Art Community[15] von Tätern geschlechtsspezifischer Gewalt geteilt werden[16] (siehe z.B. Hoppenstedt 2018: o.S.). Potentiell kann sich jede mitlesende Person an weiteren – nicht nur digitialen – Angriffen beteiligen oder motiviert fühlen und ebenfalls Aufnahmen veröffentlichen.

**Gefilmte Vergewaltigungen**

Fachberatungsstellen berichten in den letzten Jahren von einem signifikanten Anstieg an gefilmten Vergewaltigungen, die meist der Einschüchterung der Betroffenen dienen und u.a. eine Strafanzeige verhindern sollen. Täter erwirken durch die Androhung der Veröffentlichung an einen gezielten Adressat*innenkreis (Eltern, Freund*innen, Arbeitgebende) zudem die Aufgabe von Widerstand, etwa gegen weitere sexualisierte Übergriffe und Körperverletzungen. Häufig sehen Betroffene keinen Ausweg und beugen sich der Nötigung. Sie befürchten eine fortdauernde und weitreichendere Gefährdung durch die Verbreitung des Bildmaterials und halten deshalb (zunächst) körperliche und sexualisierte Gewalt aus.

Die Drohung Bilder oder Filmmaterial der Vergewaltigung zu verbreiten, kann für die meisten Betroffenen eine Verlängerung der traumatischen Situation darstellen. Allein die Existenz einer manifesten Dokumentation der erlebten Gewalt stellt eine immense psychische Belastung dar. Die Vergewaltigung/der sexualisierte Übergriff hört metaphorisch gesprochen nie auf und kann im Fall einer Verbreitung jederzeit auf unzähligen Endgeräten erneut ablaufen.

**Sexualisierte Belästigung mit Bildern**

Übergriffe, bei denen Betroffene ungewollt mit digitalen intimen, pornografischen Bildmaterialien konfrontiert werden, können ebenso als bildbasierte sexualisierte Gewalt bezeichnet werden. Hierzu gehören Bilder, die meist

15 In der sogenannten ›Slut-Exposer‹-Community werden Bilder mit der expliziten Aufforderung ausgetauscht, die abgebildete Person öffentlich bloßzustellen. Diese Community ist an die BDSM-Szene angebunden, die Bilder tragen häufig den Zusatz, dass die betreffende Person um die Veröffentlichung gebeten hat. Es ist schwer zu bewerten, welche Bilder tatsächlich mit Einwilligung der Abgebildeten veröffentlicht werden, journalistische Recherchen weisen aber daraufhin, dass auch Täter bildbasierter Gewalt diesen Kontext nutzen (vgl. Alfering 2019: o.S.).

16 Eine Analyse geleakter Daten der Seite »Anon IB« zeigt, dass die meisten Täter dabei nicht einmal ihre IP-Adresse verschleiern (vgl. Hoppenstedt 2018: o.S.).

Männer von ihren Penissen anfertigen (sogenannte Dickpics) und im Rahmen sexualisierter Belästigung an Online-Kontakte versenden. Die Betroffenen stehen dabei nicht selbst im Zusammenhang mit den Bildern, sodass selten eine Gefährdung durch Weiterverbreitung o.ä. besteht. Eine inzwischen auch weitverbreitete Form der sexuellen Belästigung mit Bildern – vor allen Dingen unter Jugendlichen – ist, die Verschickung von neutral anmutenden Bildern, die aber in der Jugendszene als Codes für Genitalien stehen, so z.B. ein Auberginen-Emoji, welches für einen Penis steht oder ein Pfirsich-Emoji für ein Gesäß. Diese Belästigung ist ohne das Wissen um die Codierung nicht erkennbar. Immer öfter wird auch der englische Begriff »Cyberflashing« verwendet, um das Versenden belästigender obszöner Bilder an Fremde zu beschreiben.

## Hate Speech

Hate Speech (dt. Hassrede) wird im Allgemeinen verwendet, um menschenverachtende Aussagen und Botschaften zu beschreiben, die Einzelne und bestimmte Gruppen abwerten. Aktuell verwendete Definitionen können sich in Punkten unterscheiden und sind auch Ausdruck der Vielzahl an Organisationen, Initiativen und Forschungsprojekten, die zum Thema Hate Speech arbeiten. Dieses Kapitel soll vorrangig einer kurzen Einordnung des Phänomens als Form geschlechtsspezifischer digitaler Gewalt dienen.

Die Vereinten Nationen definieren Hate Speech wie folgt:

> »[t]he term hate speech is understood as any kind of communication in speech, writing or behaviour, that attacks or uses pejorative or discriminatory language with reference to a person or a group on the basis of who they are, in other words, based on their religion, ethnicity, nationality, race, colour, descent, gender or other identity factor.« (United Nations 2019: 2).

Vielen Konzepten von Hate Speech liegt die Annahme zugrunde, dass Ausübende und Betroffene sich nicht persönlich kennen, sondern in (halb-)öffentlichen Bereichen des Internets aufeinandertreffen oder Betroffene bewusst ausgesucht und angegriffen werden. Hate Speech ist Ausdruck von gesellschaftlichen Macht- und Diskriminierungsverhältnissen, deren Wirkmächtigkeit im digitalen Raum keineswegs ausgesetzt ist (vgl. Ganz 2013: 4ff.). Hate Speech richtet sich vorrangig gegen marginalisierte Gruppen und wird dementsprechend auch als gruppenbezogene Menschenfeindlichkeit

verstanden (vgl. Amadeu Antonio Stiftung 2015). Hierin liegt ebenfalls die politische Dimension des Begriffs. Verbale Angriffe und Belästigung im Netz sind als Hate Speech zu fassen, wenn die Adressierten aufgrund bestimmter (zugeschriebener) Merkmale angegriffen werden und diese Merkmale tatsächlich mit einer marginalisierten, mit Diskriminierung verbundenen, gesellschaftlichen Positionierung einhergehen.[17] Hate Speech als Form geschlechtsspezifischer Gewalt, von der Frauen signifikant häufiger betroffen sind (vgl. Pew Research Center 2014: o.S.), äußert sich etwa in sexualisierten Beleidigungen, Belästigung und Vergewaltigungsandrohungen. Vor allem auch Transmisogynie und LGBTIQA+-Feindlichkeit sind mit dieser geschlechtsbezogenen Komponente verknüpft.

Öffentliche Äußerungen im Netz können von einer Vielzahl von Menschen wahrgenommen und wiederum verbreitet werden. Teilweise werden sie über das Medium Internet hinaus rezipiert, beispielsweise wenn Zeitungen oder Fernseh-Formate über bestimmte Äußerungen von Prominenten oder Politiker*innen berichten. Hate Speech kann in seinen komplexen Verbreitungs- und Rezeptionsmechanismen zu einer massiven Bedrohung und Gefährdung der adressierten Personen führen. Täter*innen können anonym und unter Verwendung von Pseudonymen agieren, tun dies aber nicht zwangsläufig. Für das massenweise, zeitlich gebündelte Auftreten von Hate Speech und anderen damit verbundenen Formen digitaler Gewalt, etablierte sich schnell der Begriff »Shitstorm«. Mittlerweile versuchen Betroffene und betroffenenorientierte Organisationen den Begriff »Hatestorm« zu etablieren – als eine Bezeichnung, die weniger die Perspektive der Täter*innen, sondern mehr die Benennung der Gewalt transportiert. Debatten um die Diskussionskultur im Netz oder die vielbemühte Angst um die Verrohung der Sprache sind seit jeher mit der Frage verknüpft, inwiefern Online-Debatten gesellschaftliche Diskurse und politische Entscheidungen beeinflussen und wie damit umgegangen werden kann, dass ganze Debatten von verhältnismäßig wenigen Personen mittels Hate Speech vereinnahmt werden können (vgl. Kreißel u.a. 2018: 1ff).

17 Auch cis-Männer sind von digitalen Beleidigungen und Bedrohungen betroffen. Auch sie können Gewalt im digitalen Raum erfahren. Dennoch ist diese Gewalt nicht in geschlechtsspezifischen Machtverhältnissen begründet, die cis-Männer strukturell benachteiligen und so die Bewältigung von Gewalterfahrungen erschweren. Somit sind erlebte digitale Angriffe auf cis-Männer nicht spezifisch mit deren Geschlechtsidentiät verknüpft – also keine Form geschlechtsspezifischer Gewalt. Unabhängig davon können cis-Männer z.B. auch queerfeindliche, rassistische oder behindertenfeindliche Hassrede erfahren.

Diese gesamtgesellschaftliche Relevanz und die für alle bezeugbare Sichtbarkeit der Gewalt scheint einer der Gründe zu sein, warum Online-Hate Speech relativ schnell problematisiert und in politische Debatten eingebunden wurde. Besonders sichtbar und von medialem Interesse sind Angriffe auf Menschen, die in der Öffentlichkeit stehen. Bekanntheitsgrad und ein breites Identifizierungspotential mit den betroffenen Person entscheiden allerdings vorrangig darüber, ob Gewalterfahrungen im Internet als solche ernstgenommen und öffentlich diskutiert werden – jedoch nicht allein darüber, wer besonders von Hate Speech betroffen ist.

## Hate Speech im Zusammenhang mit Stalking, Doxing und bildbasierter Gewalt

Angriffe im Rahmen von Online-Hate Speech oder Hatestorms beschränken sich häufig nicht nur auf sprachliche Gewalt in Form von Beleidigungen oder Vergewaltigungsandrohungen. Die Übergänge zu Stalking, Doxing und bildbasierter sexualisierter Gewalt sind fließend und Teil der Täterstrategien. Je größer die Aufmerksamkeit und Reichweite der Angriffe sind, die sich auf die Betroffenen richten, umso mehr User*innen beteiligen sich an der Ausweitung der Gewalt.[18]

Das Zusammentragen und Veröffentlichen persönlicher Informationen (Doxing, s.o.), kann dazu führen, dass die Familie der Betroffenen ebenfalls bedroht oder berufliche Kontakte involviert werden, mit dem Ziel, das soziale Gefüge und die Existenzgrundlage zu zerstören. Die Veröffentlichung von Wohn- oder anderen Aufenthaltsadressen führt zu einer realen Gefährdung, zusätzlich körperliche oder sexualisierte Übergriffe zu erfahren. Häufig werden auch online verfügbare Bilder der Betroffenen für Bildmontagen in einem sexualisierten Kontext verwendet und verbreitet.

Einschlägige Internetforen, Image-Boards und Memes[19] können Hate Speech kultivieren und spielen ebenso eine wesentliche Rolle bei der Ver-

18 Zu beobachten ist dies z.B. regelmäßig, wenn bekannte Accounts mit großer Reichweite und Follower*innenschaft im konservativen, rechten, antifeministischen Spektrum explizit auf einzelne feministische Accounts hinweisen, wohl in dem Wissen, dass die Personen hinter den Accounts dadurch in den Fokus vieler Hate Speech erfahrener Angreifer geraten. Beispielhaft hierzu die Hasskampagne gegen Natascha Strobl im Sommer 2020 (vgl. HateAid 2020: o.S.).

19 Memes transportieren humoristisch digitale Botschaften, meist in Form von Bildern oder Videos, die auf popkulturellen Ereignissen oder Inhalten beruhen, deren Kenntnis häufig Voraussetzung ist, um sie zu verstehen (vgl. Das NETTZ o.J).

mittlung und Bestätigung misogyner antifeministischer Positionen in Verbindung mit rechten, faschistischen Ideologien und Verschwörungsmythen. Hate Speech-Dynamiken können sich ebenso vor dem Hintergrund persönlicher Beziehungen entwickeln und bewusst initiiert sein.

Die Verbreitungsmechanismen sozialer Medien und die Unterstützung anderer Internetnutzer*innen werden genutzt, um Diffamierungen und Bedrohungen zu verstärken. Fachberatungsstellen berichten, dass Online-Accounts ihrer Klient*innen nach Trennungen häufig nicht nur durch den Ex-Partner selbst, sondern auch durch dessen Familie und Bekanntenkreis attackiert werden. Nicht selten werden personenbezogene Daten wie die Adresse oder Bildaufnahmen auch in spezifischen Foren geteilt, mit der expliziten oder impliziten Aufforderung zu weiterer Gewalt[20].

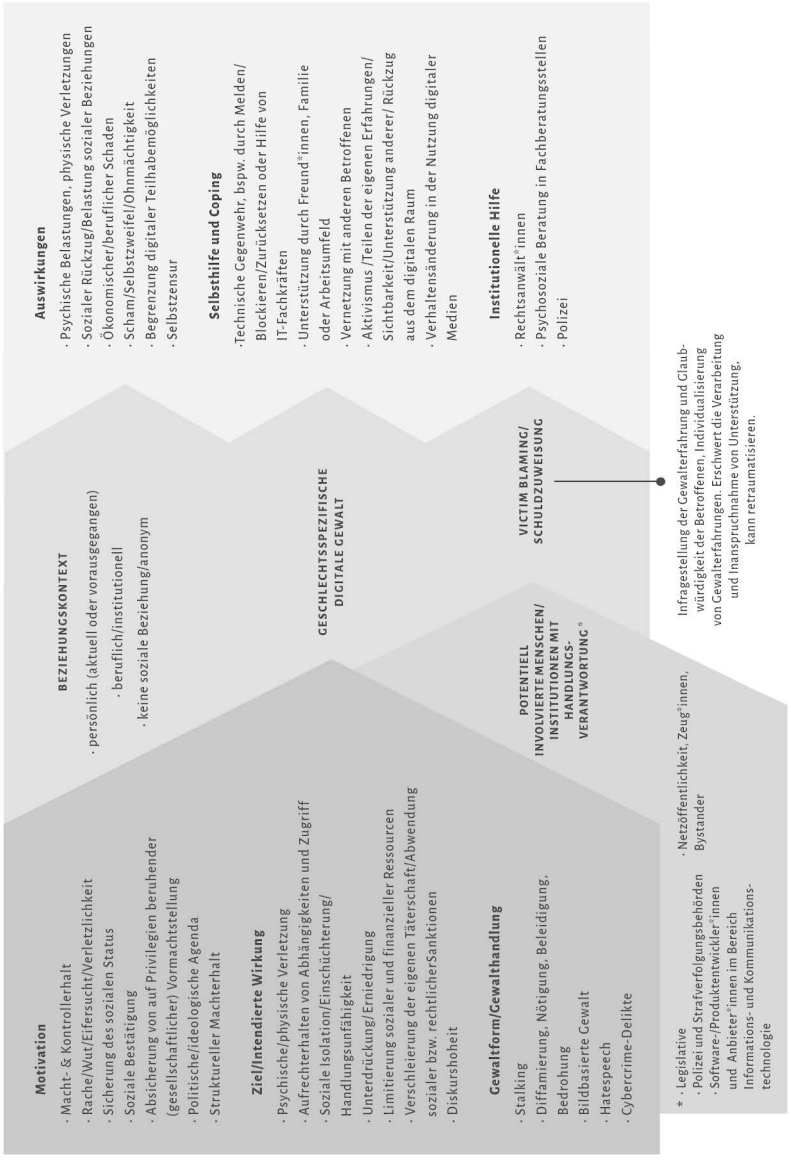
## Hate Speech gegen feministische Positionen

Auch Strukturen und Einrichtungen, die bei geschlechtsspezifischer Gewalt helfen oder auch einzelne Berater*innen, sind antifeministisch motivierten Angriffen im digitalen Raum ausgesetzt. Dies ist insbesondere der Fall, wenn sich Projekte mit sexuellen und reproduktiven Rechten, sexualpädagogischen und queeren Aspekten beschäftigen oder Zusammenhänge von geschlechtsspezifischer Gewalt und Rassismus thematisieren. Diese berichten von digitalen Angriffen in Form von Bedrohungen und Belästigungen via E-Mail und Versuchen von Datendiebstahl. Die öffentliche organisierte Diffamierung solcher Projekte erfolgt u.a. auch mit dem Ziel deren Finanzierung durch öffentliche Gelder in Frage zu stellen.

20 Viele Organisationen bieten Beratung, Unterstützung, Trainings etc. für Betroffene und Berater*innen an. Zu nennen sind insbesondere die Amadeu Antonio Stiftung, HateAid, #ichbinhier, Lovestorm, Das NETTZ, No Hatespeech Movement und ZARA (Zivilcourage und Anti-Rassismus-Arbeit).

## Formen digitaler Gewalt in Verschränkung mit Machtverhältnissen

*Abb. 2: Geschlechtsspezifische digitale Gewalt und die Auswirkungen auf Betroffene, Bauer/Hartmann 2020.*



Betroffene erfahren geschlechtsspezifische digitale Gewalt durch Personen, mit denen sie in unterschiedlichen aktuellen oder vergangenen, persönlichen oder beruflichen Beziehungen stehen können. Auch können bei geschlechtsspezifischer digitaler Gewalt gewaltausübende Personen den Betroffenen unbekannt sein, da sie im Internet anonym agieren können. Einzelne Fälle von geschlechtsspezifischer Gewalt können sich in Häufigkeit, Intensität und Form unterscheiden. Auch tritt geschlechtsspezifische Gewalt meist nicht als einzige Form von Gewalt auf, sondern verschränkt sich häufig mit anderen Diskriminierungsformen.

Die Motivation des Täters ist geprägt von Macht- und Kontrollverhalten gegenüber der betroffenen Person, verbunden mit dem Ziel, sie psychisch und/oder physisch zu verletzen, Abhängigkeiten aufrechtzuerhalten sowie die betroffene Person sozial zu isolieren oder zu unterdrücken. Auch kann eine politische oder ideologische Agenda die Person, die digitale geschlechtsspezifische Gewalt ausübt, bestimmen. Diese Ideologien sorgen wiederum für die Aufrechterhaltung der ungerechten und diskriminierenden Gesellschaft und die Sicherung des sozialen Status der gewaltausübenden Person.

Das Verhalten der Täter zeigt sich in der aktiven Umsetzung von geschlechtsspezifischer Gewalt. Diese kann Formen von Stalking, Diffamierung, Beleidigung, Bedrohung, bildbasierter digitaler Gewalt und/oder Hate Speech annehmen. Diese Gewaltformen können auch verschränkt miteinander auftreten und wirken mit ihren bedrohlichen und stark belastenden Faktoren auf die betroffene Person ein. Zum einen erlebt die betroffene Person die Gewalt mit unterschiedlichen Auswirkungen auf ihre psychische und körperliche Verfassung. Zusätzlich kann digitale Gewalt Einfluss auf den sozialen Status oder auch ökonomische Einbußen der betroffenen Person haben (z.B. das Kursieren eines Nacktbildes mit zerstörender Wirkung auf die Reputation der betroffenen Person). Zum anderen erfährt die betroffene Person häufig in der Form des Victim Blaming von unterschiedlichen Menschen und Institutionen mit möglicher (Handlungs-)Verantwortung zusätzlichen Schaden. Von ihnen erfahren die Betroffenen dann zwar keine direkte digitale Gewalt, aber es wird ihnen Hilfe und Unterstützung verwehrt und sie erfahren Stigmatisierung. Beim Victim Blaming wird die Verantwortung für die erlebte Gewalt auf die Betroffenen übertragen. Die Gewalterfahrung wird individualisiert, ohne Einbezug des gesellschaftlichen und strukturellen Kontexts in dem die Gewalt stattfindet. Oftmals wird der betroffenen Person die Glaubwürdigkeit aberkannt, was wiederum retraumatisierend wirken kann.

Menschen und Organisationen mit Handlungsverantwortung sind zuallererst die gewaltausübende Person, dann die Polizei und Strafverfolgungsbehörden, Betreiber*innen von Internetplattformen und Sozialen Netzwerken, Software- und Produktentwickler*innen, Politik und Bundesregierung, Anbieter*innen von Online-Diensten, Trittbrettfahrer*innen im Internet, Journalist*innen und Meinungsbildende. Sie sind angehalten Victim Blaming zu vermeiden bzw. dem aktiv entgegenzuwirken.

Betroffene können die Gewalterfahrung sehr unterschiedlich bewältigen. Das Melden, Blockieren, Löschen oder Zurücksetzen von Geräten führt meist zu schneller Entlastung der Betroffenen. Weitere Selbsthilfe und Bewältigungsmechanismen reichen von Rückzug aus dem Internet und stark verändertem Verhalten bei Technik- und Internetnutzung, bis hin zu Vernetzung mit anderen Betroffenen und Unterstützer*innen sowie politischem Aktivismus. Zusätzlich können Betroffene sich auch professionelle Hilfe holen. Diese finden sie in der psychosozialen Beratung von Fachberatungsstellen, bei Rechtsanwält*innen sowie auch Polizei und IT-Fachkräften, die auf das Thema digitale geschlechtsspezifische Gewalt sensibilisiert sind.

Die Gewaltdynamiken und Machtverhältnisse im Kontext (digitaler) geschlechtsspezifischer Gewalt machen deutlich, dass hier interpersonelle, gesellschaftliche und patriarchale Prozesse und Strukturen ineinandergreifen und auf die unterschiedlichen Positionen und gesellschaftliche Verantwortung gegenüber Betroffenen von digitaler geschlechtsspezifischer Gewalt hinweisen.

## Literatur

Ajder, Henry/Patrini, Giorgio/Cavalli, Francesco/Cullen, Laurence (2019): »The State of Deepfakes: Landscape, Threats, and Impact«. https://regmedia.co.uk/2019/10/08/deepfake_report.pdf [Zugriff: 18.9.2020].

Alfering, Yannah (2019): »Tom fand Nacktfotos seiner Frau im Netz, jetzt jagt das Paar den Uploader. 190 Nacktfotos. Sieben unerlaubt veröffentlichte Sexvideos. Ein mutmaßlicher Täter. Und kaum eine Chance«. Vice (Hg.). https://vice.com/de/article/4agyy3/private-nacktfotos-im-internet-kampf-gegen-revenge-porn [Zugriff: 23.9.2020].

Amadeu Antonio Stiftung (2015): »Diskriminierung, Abwertung und Missachtung«. https://amadeu-antonio-stiftung.de/themenflyer-zu-gruppenbezogener-menschenfeindlichkeit/ [Zugriff: 18.3.2020].

Bastian, Matthias (2020): »Studie: Diese sechs KI-Verbrechen sind besonders gefährlich«. https://mixed.de/die-20-schlimmsten-ki-verbrechen-forscher-veroeffentlichen-liste/ [Zugriff: 3.9.2020].

Bauer, Jenny-Kerstin (2016): Gewalt gegen Frauen ist Gewalt. Auch online! Handlungsempfehlungen für die Soziale Arbeit als Menschenrechtsprofession. Unveröffentliche M.A.-Arbeit im Rahmen des M.A.-Studiengangs: Soziale Arbeit als Menschenrechtsprofession an der Alice Salomon Hochschule, Berlin.

Beer, Isabell (2018): »Voyeurismus: Das unsichtbare Verbrechen«, in: Zeit, Nr. 34 vom 16.8.2017. https://zeit.de/zeit-magazin/2017/34/voyeurismus-pornoseiten-netzwerk-illegales-filmen [Zugriff: 5.9.2020].

Belik, Cornelia (2007): Cyberstalking. Stalking im Internet, Foren, Newsgroups, Chats, per eMail. Ergebnisse einer Online-Befragung von Opfern, TäterInnen und indirekt Betroffenen. Norderstedt: Books on Demand GmbH.

Bešić, Ariana (2019): »Und plötzlich macht es Klick.« Medien Mittweida (Hg.). https://medien-mittweida.de/voyeurismus-in-asien/2019/ [Zugriff: 4.9.2020].

BSI: Bundesamt für Sicherheit in der Informationstechnik (2019): »Lagebericht zur IT-Sicherheit 2019«. https://bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html [Zugriff: 25.6.2020].

CAS: Coalition against Stalkerware (2019): »The State of Stalkerware in 2019«. https://media.kasperskydaily.com/wp-content/uploads/sites/92/2019/11/18053214/Kaspersky_Coalition_The-state-of-stalkerware-in-2019_ENG_fin.pdf [Zugriff: 6.6.2020].

Cole, Samantha/Maiberg, Emanuel (2020): »Pornhub Doesn't Care«. https://vice.com/en_us/article/9393zp/how-pornhub-moderation-works-girls-do-porn [Zugriff: 5.9.2020].

Cox, Joseph (2019): »Most Deepfakes Are Used for Creating Non-Consensual Porn, Not Fake News«. https://vice.com/en_us/article/7x57v9/most-deepfakes-are-porn-harassment-not-fake-news [Zugriff: 29.8.2020].

Das NETTZ (o.J.): »Glossar. Meme«. https://das-nettz.de/glossar/meme [Zugriff: 23.9.2020].

Eckert, Claudia (2014): IT-Sicherheit. Konzepte – Verfahren – Protokolle. 9. Auflage. München/Oldenbourg: De Gruyter.

Fiedler, Peter (2006): Stalking. Opfer, Täter, Prävention, Behandlung. Basel: Beltz.

Ganz, Kathrin (2013): »Feministische Netzpolitik: Perspektiven und Handlungsfelder; Studie im Auftrag des GWI«. Heinrich Böll Stiftung/Gunda-Werner-Institut (Hg.). https://gwi-boell.de/sites/default/files/uploads/2013/04/ganz_feministische_netzpolitik_web.pdf [Zugriff: 18.9.2020].

HateAid (2020): »Kalkulierte Hasskampagne. Natascha Strobl, #Panoramagate und Don Alphonso«. https://hateaid.org/hasskampagne-natascha-strobl-don-alphonso/ [Zugriff: 5.9.2020].

Hoppenstedt, Max (2018): »Leak zeigt: Tausende Deutsche tauschen gehackte Nacktbilder wie Panini-Sticker«. https://vice.com/de/article/9kgw9a/leak-zeigt-tausende-deutsche-tauschen-gehackte-nacktbilder-wie-panini-sticker [Zugriff: 5.9.2020].

Huber, Edith (2019): Cybercrime. Eine Einführung. Wiesbaden: Springer VS.

Kang, Haeryun. (2018): »Unser Leben ist nicht euer Porno«. https://zeit.de/entdecken/2018-10/spycam-porn-suedkorea-proteste-frauen-rechte/seite-2 [Zugriff: 4.9.2020].

Kirwan, Gráinne/Power, Andrew (2013): »Cybercrime: The psychology of online offenders«. Cambridge: Cambridge University Press. https://doi:10.1017/CBO9780511843846 [Zugriff: 18.9.2020].

Köver, Chris (2019): »Warum es so schwer ist, rechtlich gegen Spionage-Apps vorzugehen«. https://netzpolitik.org/2019/warum-es-so-schwer-ist-rechtlich-gegen-spionage-apps-vorzugehen/ [Zugriff: 23.9.2020].

Kreißel, Philip/Ebner, Julia/Urban, Alexandra/Guhl, Jakob (2018): »Hass auf Knopfdruck: Rechtsextreme Trollfabriken und das Ökosystem koordinierter Hasskampagnen im Netz«. https://isdglobal.org/wp-content/uploads/2018/07/ISD_Ich_Bin_Hier_2.pdf [Zugriff: 29.8.2020].

McGlynn, Clare/Rackley, Erika (2017): »Image-Based Sexual Abuse«, in: Oxford Journal of Legal Studies, Vol. 37 No. 3, S. 534-561. https://claremcglynn.files.wordpress.com/2015/06/mcglynnrackley-ojls-offprint-jan-2017-image-based-sexual-abuse.pdf [Zugriff: 3.9.2020].

o.A. (2020): »Press Releases. Wicker, Cantwell Introduce Forensic Legislation«. U.S. Senate Committee on commerce, science & transportation (Hg.). https://commerce.senate.gov/2020/9/wicker-cantwell-introduce-forensic-research-and-standards-legislation [Zugriff: 28.9.2020].

Ogilvie, Emma (2000): »Australian Government – Australian Institute of Criminology«. https://aic.gov.au/publications/tandi/ti166.pdf [Zugriff: 18.3.2020].

Peters, Katharina Graça (2019): »Illegales Filmen in Südkorea ›Mein Leben ist nicht dein Porno‹«. https://spiegel.de/panorama/gesellschaft/suedkorea-

versteckte-kameras-in-hotels-mein-leben-ist-nicht-dein-porno-a-1259219.html [Zugriff: 4.9.2020].

Pew Research Center (2014): »Online harassment«. https://pewinternet.org/2014/10/22/onlineharassment/ [Zugriff: 21.8.2020].

Port, Verena (2012): Cyberstalking. Berlin: Logos.

Pöting, Inga (2019): »Heimweg-Apps: Was bringen die digitalen Begleiter?«. https://mobilsicher.de/aktuelles/heimweg-apps-unser-testsieger [Zugriff: 18.9.2020].

Powell, Anastasia/Scott, Adrian/Flynn, Asher/Henry, Nicola (2020): »Image-based sexual abuse: An international study of victims and perpetrators«. https://doi:10.13140/RG.2.2.35166.59209 [Zugriff: 18.9.2020].

Qin, Liwen (2019): »Deepfake-Technologie – Identität in der Krise«. https://goethe.de/prj/ger/de/wow/21621733.html [Zugriff: 5.9.2020].

Reno, Janet (1999): »Cyberstalking: A New Challenge for Law Enforcement and Industry. A Report from the Attorney General to the Vice President«. The United States Department of Justice (Hg.). https://usdoj.gov/criminal/cybercrime/cyberstalking.html [Zugriff: 16.3.2020].

RMIT University Australia (2020): »Australian-first research investigates perpetration of image-based sexual abuse«. https://rmit.edu.au/news/media-releases-and-expert-comments/2019/feb/research-image-based-sexual-abuse [Zugriff 22.8.2020].

Schlosser, Patrizia (2020): »Spannervideos: Wer filmt Frauen auf Toiletten?«. STRG_F Reportage (Hg.). https://youtube.com/watch?v=nGldiXxljhQ [Zugriff: 10.9.2020].

Stroud, Scott R./Cox, William (2019): »The Varieties of Feminist Counterspeech in the Misogynistic Online World«, in: Vickery Ryan, Jacqueline/Everbach, Tracy (Hg.), Mediating Misogyny. Gender, Technology, and Harassment. Cham: Springer Nature, S. 293-210.

Tai, Crystal (2018): »›My life is not your porn‹: South Korean women fight back against hidden-camera sex crimes«. https://scmp.com/week-asia/long-reads/article/2168028/my-life-not-your-porn-south-korean-women-fight-back-against [Zugriff: 4.9.2020].

United Nations (2019): »United Nations Strategy and Plan of Action on Hate Speech«. https://un.org/en/genocideprevention/hate-speech-strategy.shtml [Zugriff: 19.5.2020].

Wiedemann, Carolin (2020): »Das ist kein Porno, das ist Gewalt«. https://spiegel.de/kultur/musik/fusion-festival-monis-rache-und-spannervideos-d

as-ist-kein-porno-das-ist-gewalt-a-88712a38-9193-4dec-9c2b-29928d37c6d5 [Zugriff: 5.9.2020].