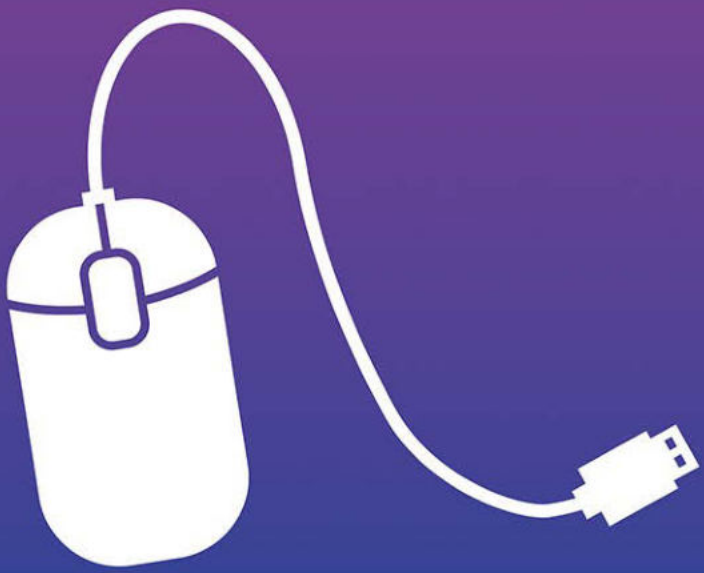
bff: Bundesverband Frauenberatungsstellen
und Frauennotrufe, Nivedita Prasad (Hg.)

GESCHLECHTS-SPEZIFISCHE GEWALT IN ZEITEN DER DIGITALISIERUNG

Formen und Interventionsstrategien



[transcript] GenderStudies

bff: Bundesverband Frauenberatungsstellen und Frauennotrufe,
Nivedita Prasad (Hg.)
Geschlechtsspezifische Gewalt in Zeiten der Digitalisierung

Gender Studies

Der **bff: Bundesverband Frauenberatungsstellen und Frauennotrufe** ist der Dachverband von bundesweit rund 200 Fachberatungsstellen, die schwerpunktmäßig Beratungsarbeit bei geschlechtsspezifischer Gewalt gegen Frauen und Mädchen leisten. Seit 2017 gibt es im bff mit »Aktiv gegen digitale Gewalt: Konzepte gegen digitale Gewalt im sozialen Umfeld und im öffentlichen Raum« das bundesweit erste Projekt, das sich mit geschlechtsspezifischer digitaler Gewalt beschäftigt.

Nivedita Prasad (Dr. phil.) ist Professorin für Handlungsmethoden und genderspezifische Soziale Arbeit an der Alice Salomon Hochschule in Berlin und leitet dort den Studiengang »Soziale Arbeit als Menschenrechtsprofession«. Für ihr Engagement gegen Menschenrechtsverletzungen an Migrantinnen wurde sie 2012 mit dem ersten Anne-Klein-Frauenpreis der Heinrich-Böll-Stiftung geehrt.

bff: Bundesverband Frauenberatungsstellen und Frauennotrufe,
Nivedita Prasad (Hg.)

Geschlechtsspezifische Gewalt in Zeiten der Digitalisierung

Formen und Interventionsstrategien

[transcript]

bff:
FRAUEN GEGEN GEWALT E.V.

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Erschienen 2021 im transcript Verlag, Bielefeld

Umschlaggestaltung: Maria Arndt, Bielefeld
Innenlayout: Emily Jones, Lena Fischer und Antea Mandić
Lektorat: Silvia Zenzen und Laura Busse-Klingler
Korrektorat: Emily Jones, Lena Fischer und Antea Mandić
Druck: Majuskel Medienproduktion GmbH, Wetzlar
Print-ISBN 978-3-8376-5281-9
PDF-ISBN 978-3-8394-5281-3
EPUB-ISBN 978-3-7328-5281-9
https://doi.org/10.14361/9783839452813

Gedruckt auf alterungsbeständigem Papier mit chlorfrei gebleichtem Zellstoff.
Besuchen Sie uns im Internet: *https://www.transcript-verlag.de*
Unsere aktuelle Vorschau finden Sie unter *www.transcript-verlag.de/vorschau-download*

Inhalt

Rechtliche Handlungsoptionen bei digitaler Gewalt

Erfahrungen und Strategien im Umgang mit digitaler geschlechtsspezifischer Gewalt

Digitale Erste Hilfe: Prävention und Intervention

Ausblick

Einleitung

Jenny-Kerstin Bauer, Ans Hartmann und Nivedita Prasad

Digitale Gewalt gerät immer mehr ins Bewusstsein der Öffentlichkeit. Dies hat sicher zum einen mit der zunehmenden Digitalisierung des Alltags, zum anderen aber auch mit dem damit einhergehenden Anstieg von digitalen Angriffen zu tun. Häufig ist Hate Speech gemeint, wenn von digitaler Gewalt die Rede ist; digitale geschlechtsbezogene Gewalt im sozialen Nahraum oder die Digitalisierung geschlechtsspezifischer Gewalt hingegen sind Themenkomplexe, die bislang kaum beachtet werden. Diese Lücke möchte dieses Buch beginnen zu schließen.

Unterscheidung Hate Speech und digitale Gewalt im sozialen Nahraum

In der öffentlichen Debatte wird oft nicht unterschieden zwischen Hate Speech und digitaler Gewalt im sozialen Nahraum; dies ist aber für ein umfassendes Verständnis digitaler Gewalt von fundamentaler Bedeutung. Hate Speech zielt darauf ab, bestimmte Meinungen, Bewegungen, Personen und/oder Personengruppen abzuwerten. Sie ist eine Form der gruppenbezogenen Menschenfeindlichkeit und wird vielfach von rechtsextremen und rechtspopulistischen Akteur*innen koordiniert eingesetzt, um Menschen einzuschüchtern bzw. bestimmte Meinungen zu manipulieren und scheinbar alternative Narrative zu entwickeln (vgl. Bundeszentrale für politische Bildung 2017; Amadeu Antonio Stiftung 2018). In vielen Fällen kennen sich angreifende und betroffene Personen im analogen Leben nicht. All dies macht u.a. juristische Interventionen sehr hürdenreich. Hate Speech richtet sich vorwiegend gegen Personen, die entweder selbst einer strukturell benachteiligten Gruppe angehören oder sich gegen die Diskriminierung dieser Gruppen einsetzen. Hate Speech bedient sich daher häufig rassistischer, se-

xistischer, homo-, transfeindlicher und/oder ableistischer Denkmuster und Beleidigungen, häufig in intersektionaler Kombination.[1] Ein prominentes Beispiel sind die Erfahrungen der Journalistin Dunja Hayali, die regelmäßig aufgrund ihrer politischen Meinung angegriffen, aber gleichzeitig auch wegen ihres Geschlechts, ihrer sexuellen Orientierung und der irakischen Herkunft ihrer Eltern beleidigt und bedroht wird. Dass Frauen und trans Personen auch im Kontext von Hate Speech regelmäßig sexualisierte Gewalt angedroht wird, zeigt, dass auch Hate Speech vielfältige geschlechtsspezifische Komponenten hat.

Eine deutliche geschlechtsspezifische Komponente zeigt sich auch bei digitaler Gewalt im sozialen Nahraum, wo es – wie bei anderen Formen geschlechtsspezifischer Gewalt auch – häufig darum geht, Macht zu demonstrieren, zu kontrollieren, einzuschüchtern und einen Beziehungsabbruch zu vermeiden. Digitale Gewalt im sozialen Nahraum richtet sich gegen Personen mit denen es in der Vergangenheit eine intime Beziehung gab oder aber eine Person, die auf ein Beziehungsbegehren nicht positiv reagierte. Hierbei kann es sowohl darum gehen sich für eine Trennung oder Ablehnung aus Tätersicht zu ›rächen‹ oder aber darum (Ex-)Partnerinnen zu kontrollieren und zu überwachen. Die Möglichkeiten einer solchen Gewaltanwendung sind inzwischen sehr vielfältig und es ist zu befürchten, dass diese Vielfältigkeit sich noch erweitern wird.[2] In der Regel handelt es sich um Einzeltäter[3], mit denen es eine Beziehung gab; ihre Namen, Adressen, soziales Umfeld etc. sind häufig bekannt, was zumindest die Erreichbarkeit von Seiten der Behörden erleichtert. Daher können auch eher niedrigschwellige Interventionsoptionen in Betracht gezogen werden, die sich im Umgang mit geschlechtsspezifischer Gewalt bewährt haben, wie z.B. die sogenannte Gefährderansprache, die von Seiten der Polizei erfolgen kann, wenn Täter wiederholt gewalttätig auffallen. Digitale Gewalt im sozialen Nahraum ist meist keine einzelne losgelöste Gewalthandlung, sie »funktioniert nicht getrennt von ›analoger Gewalt‹, [sondern] sie stellt meist eine Ergänzung oder Verstärkung von Gewaltverhältnissen und -dynamiken dar« (bff 2019: o.S.), weshalb wir hier von der Digitalisierung geschlechtsspezifischer Gewalt sprechen. Vielfach wird die Unschärfe

1 Siehe Beitrag: Intersektionale Machtverhältnisse im Internet.

2 Siehe Beitrag: Formen digitaler geschlechtsspezifischer Gewalt.

3 Auch Frauen oder trans und nicht-binäre Personen können Täter*innen von Gewalt sein; da geschlechtsspezifische Gewalt in oder nach Partner*innenschaften aber weiterhin vorwiegend durch cis-Männer ausgeübt wird, ist hier von »Tätern« die Rede.

dieses Begriffs kritisiert, nicht zuletzt, weil der Oberbegriff keine strafrechtliche Entsprechung findet. Der ganze Themenkomplex ist ein sich im Wandel befindlicher Diskurs. Häufig wird noch mit Vermutungen und Arbeitsdefinitionen gearbeitet, die sich in naher Zukunft verändern können. Derzeit ist der Begriff dafür geeignet, eine Vielzahl an vorhandenen Erfahrungen und Lebensrealitäten einen Namen zu geben und das Thema damit sprech- und schreibbar zu machen.

Inzwischen gibt es zu digitaler Gewalt im internationalen Kontext diverse Studien, Policy Papiere etc. häufig jedoch ohne die notwendige Unterscheidung zwischen Hate Speech und digitaler Gewalt im sozialen Nahraum. Die Ergebnisse der Studien machen deutlich, dass digitale Gewalt ein Phänomen ist, was zunimmt und eine Wirkmächtigkeit aufweist, die mit anderen analogen Formen von geschlechtsspezifischer Gewalt vergleichbar ist.[4] Da auch digitale Gewalt eine Menschenrechtsverletzung[5] darstellt, wird deutlich, dass hier ein (inter)nationaler Handlungsbedarf besteht. Bei aller Ähnlichkeit zu analoger Gewalt gibt es Besonderheiten der Gewalt im digitalen Raum, die es im Umgang mit einzelnen Formen digitaler Gewalt zu beachten gilt.[6]

Erfahrungen mit digitaler Gewalt im sozialen Nahraum

Es ist u.a. den Fachberatungsstellen und Frauenhäusern, die Betroffene geschlechtsspezifischer Gewalt unterstützen, zu verdanken, dass es inzwischen eine gut vernetzte interdisziplinäre Struktur zur Unterstützung von Frauen gibt, die geschlechtsspezifische Gewalt erleben. Die Analyse von Gewalt gegen Frauen als Menschenrechtsverletzung hat dazu beigetragen, dass sich auch auf der Ebene der juristisch möglichen Interventionen in der Vergangenheit viel getan hat. Bitter ist daher die Erfahrung, dass viele strafrechtliche Handlungsoptionen[7] bislang bei digitaler Gewalt erfolglos waren, weshalb es hilfreich sein kann, neben strafrechtlichen Interventionen hier über zivil-

4 Siehe Beitrag: Forschungsstand: Digitalisierung geschlechtsspezifischer Gewalt.

5 Siehe Beitrag: Menschenrechtlicher Schutzrahmen für Betroffene von digitaler Gewalt.

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

7 Siehe Beitrag: Möglichkeiten und Grenzen einer strafrechtlichen Intervention bei digitaler Gewalt.

rechtliche[8] und/oder ordnungsrechtliche[9] Möglichkeiten der Begegnung mit digitaler Gewalt nachzudenken. Die verschiedenen juristischen Analysen zeigen, dass deutlich mehr möglich sein müsste, als derzeit umgesetzt wird. Es bleibt zu hoffen, dass diese – noch theoretisch erscheinenden – Handlungsoptionen dazu beitragen werden, dass Betroffene weiterhin den juristischen Weg suchen, um Gerechtigkeit für sich, aber auch strukturelle Änderungen für ähnlich gelagerte Fälle zu erwirken.

Einige Fachberatungsstellen berichten seit bald 15 Jahren davon, dass – vor allen Dingen jüngere – Klient*innen[10] immer häufiger erleben, dass sie entweder in der Beziehung durch Informations- und Kommunikationstechnik (IKT) kontrolliert wurden oder, dass sie nach einer Trennung durch die Hilfe von IKT beleidigt, verfolgt und/oder diffamiert werden.[11] Erst 2017 startete das erste Projekt in Deutschland zu digitaler Gewalt in Deutschland, welches im bff – dem Bundesverband Frauenberatungsstellen und Frauennotrufe – angesiedelt ist. Bis dahin gab es im deutschsprachigen Raum wenige bis keine fachspezifischen Publikationen und zivilgesellschaftliche Initiativen, die sich mit der Rolle von IKT im Zusammenhang geschlechtsspezifischer Gewalt (gegen Erwachsene) auseinandersetzten. Angebote zur Sensibilisierung und Unterstützung bei digitalen Gewaltformen bezogen sich vornehmlich auf Jugendliche und junge Erwachsene. Größere Bündnisse, wie das 2011 gegründete »Bündnis gegen Cybermobbing« oder das 2013 initiierte »No Hate Speech Movement Deutschland« bezogen sich singulär auf bestimmte Gewaltformen und vernachlässigten häufig noch deren geschlechtsspezifische Dimension. Inzwischen gibt es vereinzelt weitere Projekte, so z.B. ein Projekt zu Cyberstalking beim FRIEDA-Frauenzentrum e.V. in Berlin, ein Projekt bei der Frauenhauskoordinierung zum Schutz vor digitaler Gewalt unter

8 Siehe Beitrag: Zivilrechtliche Interventionen bei digitaler Gewalt.

9 Siehe Beitrag: Rechtliche Handlungsoptionen: Öffentliches Recht.

10 Es könnte der Eindruck entstehen, als würde in diesem Band nicht einheitlich gegendert werden. Die Entscheidung beispielsweise von »Tätern« oder »Täter*innen« zu sprechen entspricht der inhaltlichen Analyse der jeweiligen Autor*in, deren Aussage wir durch ein einheitliches Gendern nicht verändern wollen.

11 Die Beratungsstelle Frauennotruf Frankfurt war Vorreiterin diesbezüglich in Deutschland und veranstaltete bereits 2010 einen Fachtag zum Thema digitale Gewalt, siehe hierzu: https://frauennotruf-frankfurt.de/fachwissen/tagungen/archiv/ [Zugriff: 8.9.2020]. Siehe Beitrag: Erfahrungen mit der Beratung von betroffenen Mädchen und Frauen im Kontext digitaler Gewalt.

Einbeziehung der Datensicherheit im Frauenhaus und eine geplante Ausstellung des PETZE-Institut für Gewaltprävention gGmbH in Trägerschaft des Frauennotruf Kiel e.V. Wissenschaftliche Forschungsarbeiten zum Thema in Deutschland sind weiterhin nicht vorhanden.

Neben den Erfahrungen in der Beratung mit von digitaler Gewalt betroffenen Frauen, gibt es inzwischen auch interdisziplinäre Expertisen, die verdeutlichen, dass schon sehr kleine technische Veränderungen präventiv wirken könnten, wenn sich die Industrie hierauf einließe bzw. die Politik darauf bestünde.[12] Auch hat die Erfahrung gezeigt, dass bei aller möglichen Erleichterung, die technische Errungenschaften mit sich bringen, diese mit Vorsicht zu genießen sind, weil sie ein neues Medium der Gewaltausübung darstellen können.[13]

Da es bislang wenig technische und juristische effektive Maßnahmen gibt, sind Betroffene darauf angewiesen, eigene, zum Teil sehr phantasievolle Bewältigungsstrategien im Kontext von digitaler Gewalt im sozialen Nahraum[14] und Hate Speech[15] zu finden. Diese sehr unterschiedlichen Strategien im Umgang mit digitaler Gewalt zeigen die Handlungsmacht der Betroffenen auf und regen an, einen eigenen Umgang mit digitaler Gewalt zu finden bzw. als Zeug*innen Betroffene öffentlich zu unterstützen.

(Präventiver) Umgang mit geschlechtsspezifischer Gewalt

Neben möglichen juristischen Interventionen, sind technische Interventionen für Einzelpersonen[16] und Organisationen[17] von Bedeutung. Gerade die technischen Interventionen können zum einen nach einem erfolgten Angriff hilfreich sein, vor allen Dingen aber können sie präventiv wirken.

---

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

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

14 Siehe Beitrag: Individuelle Strategien im Umgang mit geschlechtsspezifischer digitaler Gewalt.

15 Siehe Beitrag: Strategien im Umgang mit Online Hate Speech.

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

17 Siehe Beitrag: Digitale Sicherheit für frauenspezifische Einrichtungen.

In anderen Ländern gibt es inzwischen mehrere gute Beispiele im Umgang mit geschlechtsspezifischer digitaler Gewalt, die verdeutlichen, wie eine feministische diskriminierungssensible Antwort auf geschlechtsspezifische digitale Gewalt aussehen könnte.[18] Die Erfahrungen in der Vergangenheit haben gezeigt, dass – wie bei allen Formen von geschlechtsspezifischer Gewalt – auch bei digitaler Gewalt ein effektiver Umgang ein vernetztes interdisziplinäres Vorgehen erfordert, indem sowohl Präventionsmaßnahmen als auch realistische Interventionsmöglichkeiten erarbeitet werden. Anders als bei analoger Gewalt braucht es hier allerdings auch die Expertise von Techniker*innen und Personen, die sich mit IKT auskennen. Hierdurch können nicht nur Präventions- und Interventionsoptionen erarbeitet werden, vielmehr könnten hier auch IKT gestützte Interventionen für Betroffene erarbeitet werden.

Digitale geschlechtsspezifische Gewalt ist kein neues Phänomen, aber teilweise von schnelllebigen technologischen Entwicklungen abhängig. Die in diesem Band zusammengestellten Beiträge zeigen auf, in welcher Vielschichtigkeit die Errungenschaften der Digitalisierung zur Ausübung geschlechtsspezifischer Gewalt genutzt werden. Sie fassen eine Auswahl relevanter Debatten und Praxiserfahrungen zusammen, welche sich täglich weiterentwickeln und fortlaufend diskutiert werden.

Literatur

Amadeu Antonio Stiftung (2018): »Hate Speech und Fake News«. https://amadeu-antonio-stiftung.de/w/files/pdfs/hate_speech_fake_news.pdf [Zugriff: 20.2.2020].

bff: Bundesverband Frauenberatungsstellen und Frauennotrufe (2019): »bff: aktiv gegen digitale Gewalt«. https://frauen-gegen-gewalt.de/de/bff-aktiv-gegen-digitale-gewalt.html [Zugriff: 20.2.2020].

Bundeszentrale für politische Bildung (2017): »Was ist Hate Speech?«. https://bpb.de/252396/was-ist-hate-speech [Zugriff: 12.8.2020].

18 Siehe Beitrag: Ausblick: Effektiver Schutz vor digitaler geschlechtsspezifischer Gewalt.

Digitalisierung geschlechtsspezifischer Gewalt als Diskussionsgegenstand

Digitalisierung geschlechtsspezifischer Gewalt
Zum aktuellen Forschungsstand

Nivedita Prasad

Von geschlechtsspezifischer Gewalt wird ausgegangen, wenn Frauen aufgrund ihres Geschlechts Gewalt ausgesetzt sind, oder aber wenn es sich um eine Form von Gewalt handelt, von der Frauen überproportional betroffen sind (vgl. CEDAW 1992: Abs. 6). Auch digitale Gewalt hat eine geschlechtsspezifische Komponente (vgl. z.B. EIGE 2017), daher ist es nur folgerichtig, dass sie zunehmend auch Beachtung in entsprechenden Dokumenten und Berichten zu geschlechtsspezifischer Gewalt findet. So findet sich bereits 2006 in einem Bericht der UN zu Gewalt gegen Frauen ein expliziter Hinweis auf Informations- und Kommunikationstechnik (IKT) gestützte Gewalt (vgl. UN General Assembly 2006: Abs. 105). Seither finden sich immer wieder implizite und explizite Hinweise auf digitale Gewalt in vielen internationalen Dokumenten, Studien, Berichten oder Studienarbeiten zu Gewalt gegen Frauen, allerdings unter sehr unterschiedlichen Terminologien, wie z.B. IKT Violence, Cyberstalking, Cyberharassment, Digital Violence, Online Violence, Internet based Violence oder Technology-related Violence against Women und Technology-based Abuse. Hierbei kann es sich um Online Hate Speech handeln oder aber um digitale Gewalt im sozialen Nahfeld. Der Fokus dieses Artikels liegt auf der Digitalisierung geschlechtsspezifischer Gewalt im sozialen Nahfeld – häufig im Kontext von (Ex-)Partnerschaften.

Im Rahmen einer Studie des Pew Research Center zu Online Harassment (kurz: Pew-Studie) wurden sowohl Frauen als auch Männer zu ihren Erfahrungen mit digitaler Gewalt befragt; so konnten ihre Erfahrungsberichte direkt gegenübergestellt werden. Dieser Vergleich hat ergeben, dass Frauen überproportional von sexueller Belästigung betroffen sind (vgl. Pew Research Center 2017: 10). Auffällig ist, dass Frauen und trans Personen auch häufig im Kontext ihrer Geschlechtszugehörigkeit oder Geschlechtsidentität diskreditiert wurden (vgl. ebd.: 14f.). Die UN-Sonderberichterstatterin gegen Gewalt

gegen Frauen weist zudem darauf hin, dass der Schaden von Online Gewalt gegen Frauen verstärkt durch gesellschaftliche Stigmen wird, denen Frauen besonders ausgesetzt sind (vgl. UN Special Rapporteur on violence against women 2018: Abs. 25). Auch können Auswirkungen desselben Missbrauchs auf Frauen und Mädchen aufgrund intersektionaler Machtverhältnisse durchaus unterschiedlich sein (vgl. Henry/Powell 2018: 30; European Women's Lobby 2017: 7). So werden Women of Color rassistisch/sexistisch beleidigt, behinderte Frauen ableistisch/sexistisch und/oder lesbische Frauen sexistisch/homophob (vgl. auch Amnesty International 2017).

Annäherung an den Begriff digitalisierte geschlechtsspezifische Gewalt

Die Verwendung dieser sehr unterschiedlichen Begriffe hindert die Annäherung an den Begriff »digitalisierte geschlechtsspezifische Gewalt«; erschwerend kommt hinzu, dass häufig Phänomene – wie psychische Gewalt – beschrieben werden, die auch auf digitale Gewalt zutreffen können, ohne dass dies explizit benannt wird. Digitale Gewalt auf psychische Gewalt zu reduzieren birgt die Gefahr, dass der Eindruck entsteht, hierbei handele es sich durchgängig um eine Form von Gewalt ohne körperliche Bedrohung/Handlung. Es wird ignoriert, dass digitale Gewalt auch zu körperlicher und sexualisierter Gewalt führen kann, z.B. wenn öffentlichen Gewaltaufforderungen gefolgt wird, Personen durch digitale Mittel aufgespürt werden oder Täter[1] häuslicher Gewalt digitale Technik nutzen, um die Wirkmächtigkeit ihrer Gewalt zu verstärken. Hier verschränken sich physische Gewalt und psychische Gewalt mittels digitaler Technik. Gewalthandlungen können so immer weiter über die Sphäre des »Hauses« hinausreichen (vgl. Frey 2020: 46).

1 Natürlich können auch Frauen oder trans Personen Täter*innen von (digitaler) Gewalt sein; da geschlechtsspezifische Gewalt in oder nach Partnerschaften aber weiterhin vorwiegend Gewalt durch cis-Männer gegen Frauen ist, ist hier der Einfachheit halber von Tätern die Rede. Im Hinblick auf die geschlechtsspezifische Verteilung bei Hate Speech und digitaler Gewalt im sozialen Nahfeld kommt das Forschungszentrum Menschenrechte der Universität Wien/Weißer Ring zu dem Ergebnis, dass auch hier Männer einen Großteil (65,3 %) der Gewalthandlungen ausüben, gegenüber 28,2 % Frauen (vgl. 2018: 54). Es ist davon auszugehen, dass dieser Unterschied noch eklatanter wäre, wenn hier ausschließlich nach Gewalt im sozialen Nahraum und/oder Gewalt im Kontext von Partnerschaften gefragt worden wäre.

Es finden sich im Übereinkommen des Europarats zur Verhütung und Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt (Istanbul-Konvention) verschiedene Artikel, die implizit oder explizit Anwendung auf digitale Formen von Gewalt finden können, so z.B. psychische Gewalt (Art. 33), Stalking (Art. 34) oder sexuelle Belästigung (Art. 40). Im Kontext von Stalking geht der Kommentar der Istanbul-Konvention explizit auf »Verfolgung in der virtuellen Welt« (Europarat 2011: Abs. 182) und »unerwünschte Kommunikation […] insbesondere über moderne Kommunikationswege und die IKT« (ebd.) ein. Auch in der Beschreibung von bedrohendem Verhalten wird »die Schaffung falscher Identitäten oder die Verbreitung falscher Informationen im Internet« (ebd. Abs. 183) erfasst.

Der UN-Frauenrechtsausschuss bezieht sich 2017 in einer Allgemeinen Empfehlung auf digitale Gewalt, indem er digitale Umgebung als einen Ort nennt, wo Gewalt gegen Frauen stattfinden kann (vgl. CEDAW 2017: Abs. 20). In Anlehnung an die Definition des CEDAW Ausschusses ergänzt die UN-Sonderberichterstatterin gegen Gewalt gegen Frauen die Definition von Gewalt gegen Frauen als:

> »jede Handlung einer geschlechtsspezifischen Gewalt gegen Frauen, welche teilweise oder vollständig durch die Nutzung von IKT wie Handys und Smartphones, das Internet, soziale Medien, Plattformen oder Email begangen, unterstützt oder verstärkt wird, gegen eine Frau, weil sie eine Frau ist oder Frauen überproportional betrifft.« (UN-Special Rapporteur on violence against women 2018: Abs. 23, Übersetzung N.P.)

Geschlechtsspezifische digitale Gewalt – wie von der UN-Sonderberichterstatterin definiert – kann zum einen in Form von Online Hate Speech auftreten, welches sich vorwiegend gegen politisch agierende Frauen oder trans Personen im öffentlichen Raum richtet, häufig durch fremde Täter*innen. Zum anderen tritt sie als Erweiterung/Verstärkung von Formen analoger Gewalt auf – vorwiegend durch (Ex-)Beziehungspartner, oder solche, deren partnerschaftliches Interesse nicht auf Gegenseitigkeit beruhte. In einer Expertise für den Dritten Gleichstellungsbericht der Bundesregierung ergänzt Frey das Feld der Erwerbsarbeit und Öffentlichkeit (Frey 2020: 12) als eines, in dem digitale geschlechtsspezifische Gewalt stattfinden kann[2]. Während On-

2 Frey weist gleichzeitig darauf hin, dass diese Unterscheidung eine analytische ist, da die verschiedenen Formen der Gewalt ineinandergreifen und sich ggf. gegenseitig verstärken können. Diese Unterscheidung unternimmt sie u.a., um die unterschiedlichen

line Hate Speech nicht zuletzt durch rechtliche Auseinandersetzungen, die durch öffentliche Personen geführt wurden, immer häufiger auch öffentlich diskutiert wird und dadurch ins Bewusstsein rückt, ist die Digitalisierung von Gewalt im sozialen Nahfeld hingegen ein Themenkomplex, der nur langsam in den Fokus der Öffentlichkeit gerät. Dies zeigt sich nicht zuletzt auch darin, dass die meisten Beschreibungen und Definitionen von digitaler Gewalt sich vorwiegend auf Online Hate Speech fokussieren und Digitalisierung geschlechtsspezifischer Gewalt im persönlichen Umfeld eher vernachlässigen (siehe z.B. Human Rights Council 2013: Abs. 66, Amnesty International 2017, Lembke 2018). Allgemeine Definitionen zu Gewalt gegen Frauen im sozialen Nahfeld hingegen berücksichtigen häufig die Besonderheiten der Nutzung von IKT nicht.

Eine aktuelle und ziemlich umfassende Studie ist die des Forschungszentrums Menschenrechte der Universität Wien/Weißer Ring (kurz: Wiener Studie) aus dem Jahr 2018. Hier wurden 61 Berater*innen, 42 Personen im Rahmen von Fokusgruppen und über 1.000 Internetnutzerinnen in einer repräsentativen Stichprobe im Alter von 25 bis über 64 Jahren zu »Gewalt im Netz gegen Frauen und Mädchen in Österreich« befragt. Diese Untersuchung verwendet eine Definition, die sowohl Online Hate Speech als auch digitale Gewalt im sozialen Nahfeld abdeckt und definiert Gewalt im Netz als:

> »*jede sprachliche* (durch Schrift oder aufgezeichnete Sprache) *oder darstellende* (durch Bild oder Video) *Äußerung*, verbreitet oder zugestellt *durch das Medium Internet, die von unmittelbaren und/oder mittelbaren EmpfängerInnen* als *bedrohlich, herabwürdigend oder verunglimpfend empfunden* wird oder durch die die EmpfängerInnen sich in ihrer *Lebensgestaltung auf unzumutbare Weise beeinträchtigt fühlen*. Bezugspunkt ist nicht ausschließlich das individuelle *Empfinden, sondern das Empfinden eines wahrnehmbaren Teiles der rechtsverbundenen Sprachgemeinschaft*. Besonders zu berücksichtigen ist dabei jeder *Ausdruck der Diskriminierung* auf Grund der ethnischen Zugehörigkeit, der Religion oder Weltanschauung, des Alters, der sexuellen Orientierung, einer körperlichen oder intellektuellen Beeinträchtigung oder des Geschlechts.« (Forschungszentrum Menschenrechte der Universität Wien/Weißer Ring 2018: 28 [Herv. i.O.])

Rollen von Akteur*innen, Betroffenen und Verursachenden zu verdeutlichen (vgl. Frey 2020: 13).

Im Rahmen der Pew-Studie wurden 4.248 erwachsene US-Amerikaner*innen[3] zu Online Belästigung befragt. Online Belästigung wurde hier durch die Darstellung möglicher Handlungen wie Beschimpfungen, absichtliches öffentliches Beschämen, physische Bedrohungen und Stalking beschrieben (vgl. Pew Research Center 2017: 3f.). Auch hier wird deutlich, dass sowohl Hate Speech als auch Online Gewalt im sozialen Nahfeld abgefragt wurden.

Eine der wenigen Definitionen, die sich ausschließlich auf digitale Gewalt im sozialen Nahraum fokussiert, ist die seit 2017 regelmäßig aktualisierte Definition des Bundesverbands der Frauenberatungsstellen und Frauennotrufe (bff), da dort die Spezifizität von digitaler Gewalt im sozialen Nahfeld im Fokus steht. Der bff definiert digitale Gewalt als:

> »alle Formen von geschlechtsspezifischer Gewalt, die sich technischer Hilfsmittel und digitaler Medien (Handy, Apps, Internetanwendungen, Mails etc.) bedienen und/oder geschlechtsspezifische Gewalt, die im digitalen Raum, z.B. auf Online-Portalen oder sozialen Plattformen stattfindet. Digitale Gewalt funktioniert nicht getrennt von ›analoger Gewalt‹, sie stellt meist eine Ergänzung oder Verstärkung von Gewaltverhältnissen und -dynamiken dar.« (bff 2019: o.S.)

Neben expliziten Definitionen können auch Beschreibungen psychischer Gewalt auf einzelne Formen digitaler Gewalt Anwendung finden, so z.B. in einem Bericht der Grundrechteagentur der Europäischen Union (FRA), in dem unter psychischer Gewalt neben ökonomischer Gewalt und Erpressung, auch kontrollierendes Verhalten, »Herabsetzen oder Demütigen in der Öffentlichkeit oder Privatsphäre, Verbieten, die Wohnung zu verlassen, bzw. Einschließen, Zwingen, gegen ihren Willen pornografisches Material anzusehen, absichtliches Verängstigen oder Einschüchtern sowie mit Gewalt drohen oder damit drohen, jemand anderen zu verletzen« (FRA 2014: 25) aufgeführt wird.

In der Erfassung von psychischer Gewalt wurden im Rahmen der letzten Prävalenzstudie zu Gewalt gegen Frauen in Deutschland u.a. regelmäßige Erfahrungen der Abwertungen, Schikanierungen, Drohungen, Erpressungen, Verleumdungen abgefragt, die so belastend waren, dass sie als Psychoterror oder seelische Grausamkeit empfunden wurden (vgl. BMFSJ 2004: 104f.). Viele dieser Handlungen finden im Kontext digitaler Gewalt statt. Es ist davon

3 Es ist nicht eindeutig zu erkennen, ob hier tatsächlich nur US-Amerikaner*innen befragt wurden. Da einige Interviews auf Spanisch geführt wurden, liegt es nahe anzunehmen, dass hier Personen befragt wurden, die in den USA leben.

auszugehen, dass künftige Prävalenzstudien digitale Gewalt explizit und ausreichend differenziert abfragen müssten.

Zusammenfassend wird deutlich, dass der Themenkomplex digitale Gewalt im sozialen Nahfeld immer mehr und expliziter Verwendung in Berichten/Studien zu Gewalt gegen Frauen findet. Hier gibt es weiterhin zahlreiche Definitionen und Begrifflichkeiten, die aber verdeutlichen, dass diese Form der geschlechtsspezifischen Gewalt zunehmend in den Fokus rückt. Wünschenswert wäre eine deutlichere Differenzierung zwischen Online Hate Speech und digitaler Gewalt im sozialen Nahraum.

Formen digitalisierter geschlechtsspezifischer Gewalt[4]

Formen digitaler Gewalt, die analoge Gewalt verstärken oder auch alleine wirken, sind vielfältig. Einige dieser Handlungen sind nur mit Hilfe von IKT umsetzbar, während andere ihre Wirkmächtigkeit durch IKT erhöhen können. Bei Gewaltformen, bei denen das Internet eine Rolle spielt, kommt erschwerend hinzu, dass im Internet hinterlassene Informationen sehr schwer endgültig löschbar sind. Hinzu kommt die sehr schnelle Verbreitung, die auch künftig dafür sorgen wird, dass Menschen auf diese Informationen zugreifen können.[5]

Bisher in Studien (vgl. FRA 2014, National Network to end domestic violence 2015, bff 2017, European Women's Lobby 2017, Pew Research Center 2017, UN Special Rapporteur on violence against women 2018 und Forschungszentrum Menschenrechte der Universität Wien/Weißer Ring 2018) und in der Praxis bekannte Formen sind die Durchführung oder Androhung folgender Handlungen:

- »Doxing«: Veröffentlichung von privaten Adressen/Telefonnummern und/oder Herstellung von Profilen von Frauen im Netz, um sie zu diskreditieren, zu beschämen oder ihrem Ruf zu schaden; z.B. mit dem Hinweis sie würden vermeintlich sexuelle Dienstleistungen anbieten.

---

4 Für eine detaillierte Darstellung und Umgang mit Formen digitalisierter Gewalt siehe Beitrag: Individuelle Strategien im Umgang mit geschlechtsspezifischer digitaler Gewalt.

5 Zu Besonderheiten der Gewalt im Netz siehe Beitrag: Funktionsprinzipien des Internets und ihre Risiken im Kontext geschlechtsspezifischer digitaler Gewalt.

- Das bewusste Verbreiten von Gerüchten oder Zwangsoutings, beispielsweise bezüglich der sexuellen Aktivität, des Gesundheitsstands, sexueller Orientierung einer Person.
- Erstellen von Fake Profilen im Netz und Versenden von Infos mit dieser falschen Identität; hierzu gehört auch das sogenannte Deepfaking. Hier werden Gesichter von Personen z.B. in Pornos hineinmontiert; hierfür reichen öffentlich verfügbare Bilder wie z.B. von Facebook oder professionellen Websites (vgl. Forschungszentrum Menschenrechte der Universität Wien/Weißer Ring 2018: 30).
- Hacken von Konten, z.B. um Passwörter zu verändern, die eine Kontaktaufnahme nach außen oder das Abheben von Geld erschweren.
- Andere ermutigen oder auffordern, Frauen zu schaden (z.B. Vergewaltigungsaufrufe).
- Verbreitung von einvernehmlich hergestellten Nacktfotos/pornographischem Material im Bekanntenkreis und/oder dem Internet, auch bekannt als ›Revenge porn‹ oder besser »bildbasierte sexuelle Ausbeutung« (vgl. European Parliament's Committee on Women's Rights and Gender Equality 2018: 17).
- Herstellen und/oder Verbreiten von heimlich hergestellten Nacktfotos/pornographischem Material/Aufnahmen sexualisierter Gewalt im Bekanntenkreis und/oder dem Internet, hierzu gehören auch »Sextortion«[6] oder »Upskirting«[7].
- Cyberharassment[8]: Das ungewollte Empfangen von Nacktfotos/pornographischem Material/Nachrichten, sexuelle Avancen oder Nachrichten mit explizit sexuellem Inhalt und/oder nichteinvernehmliches »Sexting«[9].
- Kontrolle über Aufenthaltsorte, Gespräche etc. durch das (versteckte) Installieren einer entsprechenden App – sogenannte Spy-Apps[10]. Dies kann

6 Hierbei werden Frauen zunächst freiwillig dazu gebracht in Videochats nackt zu posieren oder sexuelle Handlungen an sich vorzunehmen, die heimlich gefilmt werden. Anschließend werden sie mit der Veröffentlichung dieser Aufnahmen erpresst.

7 Das heimliche Fotografieren unter einen Rock. Ein entsprechendes Gesetz ist am 3.7.2020 im Bundestag beschlossen worden.

8 Stelkens kritisiert diesen Begriff als beschönigend, da er lediglich Belästigung meint (vgl. Stelkens 2016: 148).

9 Nachrichten mit sexuellem Kontext.

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

über die Geräte der Frauen oder aber über die Geräte gemeinsamer Kinder erfolgen (vgl. National Network to end domestic violence 2015: 5).
- Online- oder Cyberstalking: hierzu gehören z.B. Nachrichtenterror, ungewollte absurde und kostenintensive Onlinebestellungen und/oder Überwachung der betroffenen Person.
- Kontrolle über das Internet of Things (IoT)[11], also einem »Netzwerk, das alle denkbaren Geräte drahtlos direkt miteinander kommunizieren lässt, ohne dass zwingend ein Mensch dazwischengeschaltet ist« (Stelkens 2019: 3).
- Zerstören von emotional wertvollen Daten, wie z.B. Tagebüchern, E-Mails oder Fotos auf einem Computer/Datenträger.
- Kontrolle über Personen und ihre Social Media Accounts.
- Identitätsdiebstahl im Netz, mit dem Vorhaben unter der gestohlenen Identität ruf- oder finanziell schädigende Handlungen zu tätigen.
- »Swatting«: Notrufe bei der Polizei in Verbindung mit falschen Beschuldigungen.
- Gewalt auf Selbstmordforen oder Foren für Personen mit Magersucht oder Bulimie, wenn vorher vereinbarte ›Ziele‹ nicht erreicht werden (vgl. Forschungszentrum Menschenrechte der Universität Wien/Weißer Ring 2018: 30).
- Beleidigungen und Verletzung (z.B. Vergewaltigungen) von Online Identitäten von Personen im Rahmen von Onlinespielen.

Eine solche Auflistung wird angesichts der zahlreichen und sich ständig (weiter-)entwickelnden technischen Möglichkeiten und Kommunikationswege nie abschließend sein können. Theoretisch ist Onlinegewalt in allen Foren, Plattformen etc. denkbar. Allerdings wird immer wieder Facebook als die Plattform genannt, auf der am häufigsten Gewalt erlebt wurde. Dies hängt vermutlich mit der Häufigkeit der Nutzung von Facebook, dem Nutzungsverhalten der befragten Gruppe und den zum Befragungszeitraum vorherrschenden Trends zusammen. An zweiter Stelle werden textbasierte Kommunikationsdienste wie Messenger, WhatsApp, Emails oder SMS genannt. Gewalt wird zudem auf Datingplattformen ausgeübt, aber auch auf Snapchat oder Instagram. Am wenigsten wurde von Gewalt auf Twitter, YouTube und eigenen Blogs oder Webseiten berichtet (vgl. ebd.: 35f.).

11 Siehe Beitrag: Das Internet der Dinge: Die Auswirkungen smarter Geräte auf häusliche Gewalt.

Vereinzelt sind Berichte von Frauen zu hören, die bei Plattformen wie Ebay Kleinanzeigen oder Kleiderkreisel bei dem Versuch Gebrauchsgegenstände zu verkaufen oder der Suche nach Nebentätigkeiten wie Babysitting sexuell belästigt wurden.

Digitalisierung geschlechtsspezifischer Gewalt als ein Kontinuum von Gewalt

Bei der Digitalisierung geschlechtsspezifischer Gewalt nutzen Täter IKT, um die Wirkmächtigkeit ihrer Gewaltausübung zu verstärken, oder nutzen Gewaltformen, die nur durch IKT möglich sind, häufig jedoch auch in Kombination. »Besonders bei Stalking wird deutlich, dass mittlerweile in nahezu allen Fällen das Internet oder digitale Medien dazu genutzt werden, Stalking-Handlungen auszuüben.« (bff 2017: 8) Ortiz-Müller weist zudem auf die Schwierigkeit der Trennschärfe zwischen Cyberstalking und anderen Formen von Stalking hin, indem er sagt, dass »Cyberstalking […] im weitest gefassten Sinn jede Form der Kontaktaufnahme über elektronische Medien, also bereits das Versenden von E-Mails und SMS [darstellt]« (Ortiz-Müller 2017: 29).

Dass eine Trennung zwischen digitaler und analoger Gewalt vielen Gewaltdynamiken nicht gerecht wird, wird auch in einer Untersuchung von Women's Aid in Großbritannien deutlich, im Rahmen derer 307 Betroffene von häuslicher Gewalt befragt wurden. Fast die Hälfte (45 %) von ihnen gab an, auch Formen digitaler Gewalt im Rahmen ihrer Partnerschaft erlebt zu haben; ebenso berichtete knapp die Hälfte (48 %) über Belästigung oder Online Abuse nach der Trennung und 38 % berichteten von Online Stalking nach der Trennung (vgl. Women's Aid 2014: 8, vgl. auch EIGE 2017: 2). Auch das kanadische Citizens Lab weist auf verschiedene Untersuchungen hin, die die gleichzeitige Betroffenheit von analoger und digitaler Gewalt belegen. So z.B. eine Umfrage des National Public Radio, im Rahmen derer Mitarbeitende von 72 Zufluchtsorten für Betroffene häuslicher Gewalt befragt wurden. Die dort Befragten Berater*innen gaben an, dass 85 % von ihnen Betroffene unterstützt haben, die durch GPS von Gewalttätern verfolgt wurden. Dies deckt sich in etwa mit den Ergebnissen des in den USA ansässigen National Network to End Domestic Violence, wonach 71 % der Täter von häuslicher Gewalt die Computeraktivitäten der Betroffenen überwachten und 54 % dies mit Stalkerware auf dem Smartphone taten (vgl. Parsons u.a. 2019: 1). Es wird dadurch deut-

lich, dass Gewalt gegen Frauen in einem Kontinuum und/oder in Interaktion innerhalb eines digitalen Raums verübt wird.

Wie sich die Wirkmächtigkeit von Gewalt durch die Nutzung von IKT verstärkt, wird an einzelnen Beispielen anschaulich: So hat Eifersucht in Beziehungen immer auch dazu geführt, dass Partner*innen kontrolliert wurden; die ›Effektivität‹ dieser Kontrolle erhöht sich jedoch deutlich mit dem Einsatz von IKT. Auch ist es kein neues Phänomen, dass Paare sich einvernehmlich nackt oder bei sexuellen Handlungen filmen oder fotografieren und dieses Material nach einer Trennung gegen den Willen verbreitet wird. Neu hingegen ist die Reichweite, Geschwindigkeit und Langlebigkeit der Verbreitung solcher Bilder. Auch die Häufigkeit der Belästigungen im Netz ist eine deutlich höhere, da das Internet es ermöglicht, eine Flut von Nachrichten kostenlos in sehr kurzer Zeit immer wieder auch anonym zu verschicken. Hinzu kommt, dass online Gewalt »ohne räumlichen Bezug von jedem Ort der Welt zu jeder Tages- und Nachtzeit ausgeübt werden [kann]. Viele Täter*innen fühlen sich in der scheinbaren Anonymität des Netzes sicher und unangreifbar.« (Ortiz-Müller 2017: 29)

Auch sind Konflikte in einem gemeinsamen Haushalt z.B. über die Wärmeregulierung kein neues Phänomen, ebenso wenig wie – im Kontext von gewaltvollen Beziehungen – Partner*innen verwehrt wird, das Haus zu verlassen. Durch die Einrichtung eines Smarthomes diese Angelegenheiten zentral durch eine Person geregelt werden; es spricht einiges dafür, dass dies den Geschlechterstereotypen entsprechend eher die Männer sind (vgl. Stelkens 2019: 3), was letztendlich dazu führt, dass alle anderen Personen im Haushalt immer weniger Kontrolle über ihr Leben haben. Hier wird nicht nur eine ungleiche Machtverteilung zementiert. Während in einer analogen Auseinandersetzung einzelne Familienmitglieder sich diesen Vorgaben zumindest zeitweise widersetzen können, indem sie z.B. in Abwesenheit die Wärme ihren Wünschen nach regulieren oder das Haus verlassen, indem sie die Tür verkeilen oder heimlich Besuch empfangen, kann auch hier die digitale Kontrolle ganz andere Dimensionen erreichen. In einem Smarthome ist eine Heizung anders gar nicht zu regulieren und jede Bewegung der Wohnungstür kann der Person gemeldet werden, die das Smarthome verwaltet.

Da sich die Gewaltdynamiken zwischen analoger und digitaler Gewalt ähneln und Phänomene wie ungleiche Machtverteilung in Partnerschaften, Kontrolle von Partner*innen, Grenzüberschreitungen oder die Einschränkung der Bewegungsfreiheit Kernelemente von geschlechtsspezifischer Gewalt sind, spricht einiges dafür, digitale Gewalt im sozialen Nahfeld nicht

als ein gesondertes Thema zu betrachten. Vielmehr erscheint es notwendig, diese als eine Erweiterung von analoger Gewalt zu verstehen, nicht zuletzt auch, um die über Jahrzehnte erarbeitete Expertise in diesem Bereich zu nutzen, um Betroffene zu unterstützen und effektive strukturelle Veränderungen zu forcieren. Allerdings geht dies einher mit der Erweiterung der eigenen Expertise und Wissen um digitale Gewalt.

Ausmaß und Prävalenzen digitalisierter geschlechtsspezifischer Gewalt

Bislang ist wenig bekannt über die Prävalenz von bzw. Betroffenheit durch IKT unterstützte Gewalt in oder nach partnerschaftlichen Beziehungen. Einzelne Studien und Berichte vermitteln einen ersten Eindruck darüber, wer in welchem Ausmaß betroffen sein könnte. Erschwert werden Aussagen zu digitaler Gewalt im sozialen Nahfeld auch dadurch, dass die meisten Studien auch Online Hate Speech gleichzeitig abfragen. Erst bei der Beschreibung der Handlungen wird deutlich, was sich auf digitale Gewalt im sozialen Nahraum und was sich eher auf Online Hate Speech bezieht. So auch im Rahmen der Wiener Studie, die feststellte, dass

> »[j]ede dritte Befragte (32,4 %, n= 1.005) angab, mindesten [sic!] einmal in den letzten 12 Monaten eine Online-Gewalterfahrung erlebt zu haben. Am häufigsten waren Frauen und Mädchen von Online-Beschimpfungen und Beleidigungen aufgrund ihrer politischen Weltanschauung (12,8 %) und von persönlichen Beschimpfungen (11,6 %) betroffen. Des Weiteren erhielten 10,9 % der Befragten ohne ihre Zustimmung sexuell anzügliche Mitteilungen (in Textformaten, Fotos und Videos). Überdurchschnittlich waren jüngere Frauen und Mädchen (15- bis 18-Jährige) von allen Gewalt-Dimensionen betroffen […].« (Forschungszentrum Menschenrechte der Universität Wien/Weißer Ring 2018: 69)

Im Rahmen der Pew-Studie gaben 41 % (im Unterschied zu 35 % im Jahre 2014) der Befragten an, mindestens eine Art von Online-Belästigung erlebt und 66 % diese beobachtet zu haben (vgl. ebd.: 3). Unter den Betroffenen sind 18 %, die angeben, sie hätten schwere Formen von Belästigung erlebt; hierzu gehören Stalking, physische Bedrohungen, sexuelle Belästigung oder Belästigung über einen längeren Zeitraum (vgl. Pew Research Center 2017: 3f.).

Der Bericht der FRA, der sich explizit auf Gewalt im sozialen Nahfeld fokussiert, hat die Prävalenz von psychischer Gewalt erfasst und kommt zu dem Ergebnis, dass

> »[j]ede dritte Frau (32 %) […] psychische Mißhandlung in der Partnerschaft entweder von ihrem derzeitigen oder früheren Partner/einer derzeitigen oder früheren Partnerin erlebt [hat]. Dazu gehören Verhalten wie Herabsetzen oder Demütigen in der Öffentlichkeit oder Privatsphäre, Verbieten, die Wohnung zu verlassen, bzw. Einschließen, Zwingen, gegen ihren Willen pornografisches Material anzusehen, absichtliches Verängstigen oder Einschüchtern sowie mit Gewalt drohen oder damit drohen, jemand anderen zu verletzen, der der Befragten wichtig ist.« (FRA 2014: 25)

Einigkeit in nahezu allen Studien gibt es darüber, dass Alter »das stärkste Differenzmerkmal« (Forschungszentrum Menschenrechte der Universität Wien/Weißer Ring 2018: 63) bei digitaler Gewalt darstellt, was vermutlich mit der altersdifferenten Nutzung neuer Medien/Technologien einhergeht. Dies bestätigt auch der Bericht der Europäischen Grundrechteagentur FRA zu Gewalt gegen Frauen, der darauf hinweist, dass

> »[d]ie Gefahr, zum Ziel von drohenden und beleidigenden Annäherungsversuchen im Internet zu werden, […] für junge Frauen im Alter zwischen 18 und 29 Jahren zweimal so hoch [ist] wie für Frauen im Alter zwischen 40 und 49 Jahren und mehr als dreimal so hoch wie für Frauen im Alter zwischen 50 und 59 Jahren.« (FRA 2014: 32)

Dieses wird spezifiziert mit dem Ergebnis, wonach »in den 12 Monaten vor der Befragung […] in den 28 EU-Mitgliedstaaten 4 % aller 18 bis 29 Jahre alten Frauen oder 15 Millionen Online-Stalking erlebt [haben], während im Vergleich dazu 0,3 % der Frauen, die 60 Jahre oder älter sind, dies erlebt haben« (FRA 2014: 30). Im Rahmen der Prävalenzstudie zu Gewalt gegen Frauen in Deutschland wurde zwar nicht zwischen analoger und digitaler psychischer Gewalt differenziert, dennoch ist der Befund, dass »junge Frauen […] am häufigsten psychische Gewalt erlebt haben und dass der Anteil der von psychischer Gewalt […] Betroffenen kontinuierlich abnimmt, je älter die Befragten waren« (vgl. BMFSJ 2004: 110) auffällig.

Sowohl die Wiener Studie, als auch die Pew-Studie fanden zunächst heraus, dass ein Großteil der gewaltausübenden Personen nicht bekannt oder gar anonym war. Lediglich rund ein Drittel der Frauen kannten die gewaltausübenden Personen. Diese waren Freund*innen, Bekannte,

Familienmitglieder, (Ex-)Partner*innen. Interessant ist der Befund der Wiener Studie, wonach nur 9,3 % der Befragten (Ex-)Partner*innen sowie 4,1 % derzeitige Partner*innen als Täter*innen nannten (Forschungszentrum Menschenrechte der Universität Wien/Weißer Ring 2018: 53). »Diese Darstellung ändert sich jedoch bei näherer Betrachtung von einzelnen Online-Gewalterfahrungen. Beim Weiterleiten von sexualisierten Fotos oder Videos in intimen Situationen von den befragten Frauen und Mädchen waren es insbesondere der/die Ex-(Ehe)PartnerIn (37,5 %) bzw. Verwandte (26,5 %) […].« (Forschungszentrum Menschenrechte der Universität Wien/Weißer Ring 2018: 54) Aufschlussreich ist die Ausdifferenzierung der Betroffenheiten nach intersektionalen Kategorien sowohl in der Pew-Studie, als auch in der Wiener Studie. Die Pew-Studie stellt fest, dass 32 % der Befragten aufgrund ihrer Geschlechtsidentität angegriffen wurden, 34 % wegen ihres Aussehens, 23 % wegen ihrer ethnischen Zugehörigkeit, 13 % wegen ihrer sexuellen Orientierung, 45 % sprachen von intersektionaler Diskriminierung im digitalen Raum (vgl. Pew Research Center 2017: 21). Die Wiener Studie fand heraus, dass 3,9 % der befragten Frauen und Mädchen auch wegen ihrer Herkunft oder Kultur[12] (3,9 %) bzw. ihrer Religion (3,1 %) einer Beeinträchtigung (2,4 %) und/oder aufgrund ihrer sexuellen Orientierung (1,8 %) beschimpft wurden (vgl. ebd.: 50). Dies führt näher betrachtet zu dem Ergebnis, dass Frauen und Mädchen, die lesbisch, bi, trans oder queer sind, überdurchschnittlich oft persönlich beschimpft wurden und ungefragt sexuell anzügliches Material erhielten (vgl. ebd.: 58). Beschimpfungen aufgrund rassistischer Vorurteile wurden in dieser Studie unter der Kategorie ›Deutsch als Erstsprache‹ erfasst, welche sich auch als eine einflussreiche Differenzkategorie herausstellte. Mädchen und Frauen mit Migrationsgeschichte waren demnach fast doppelt so häufig von persönlichen Beschimpfungen betroffen als Frauen ohne Migrationsgeschichte (vgl. ebd.).

In nahezu allen Studien wird Stalking als die Form von Gewalt dargestellt, bei der Täter sich am häufigsten sowohl analoger als auch digitaler Kontrollmöglichkeiten bedienen. Besorgniserregend ist der Befund, dass in den 28 EU-Mitgliedstaaten 18 % der Frauen seit dem 15. Lebensjahr Stalking erlebt haben; 5 % von ihnen sogar in den letzten zwölf Monaten vor der Befragung (vgl. FRA 2014: 28). »Dies entspricht etwa 9 Millionen Frauen in den 28

12 Diese deutlichen Unterschiede bezüglich rassistischer Diskriminierung haben möglicherweise mit der sehr unterschiedlichen Zusammensetzung der Bevölkerung in den USA und Österreich zu tun.

EU-Mitgliedstaaten, die im Zeitraum von 12 Monaten Stalking erlebt haben.« (Ebd.) Während hier nicht zwischen analogem und Cyberstalking unterschieden wird, zeigen weitere Ergebnisse derselben Untersuchung,

> »dass Frauen durch eine Reihe von verschiedenen TäterInnen sexuell belästigt werden und dies auch durch die sogenannten neuen Medien erfolgen kann. Jede zehnte Frau (11 %) hat unangemessene Annäherungen auf Websites sozialer Medien erlebt oder sexuell explizite E-Mails oder Textnachrichten (SMS) erhalten.« (ebd.: 13)

Explizite Zahlen zu Deutschland gibt es noch keine; Beratungsstellen, Frauenhäuser und andere Zufluchtseinrichtungen für von Gewalt betroffene Frauen berichten aber davon, dass ihre Klient*innen immer häufiger auch digitale Gewalt erleben.[13] Laut einer Sprecherin des Bundeskriminalamts habe es in Deutschland im Jahr 2016 fast 6.000 Fälle gegeben, bei denen Bildmaterial aus intimen Situationen geleakt – also ohne Erlaubnis gepostet – wurde (vgl. Baden 2018: o.S.); über die vermutete Dunkelziffer oder das in der Praxis bekannte Hellfeld gibt es bislang keine belastbaren Schätzungen/Zahlen.

Nutzung von IKT im Kontext von Menschenhandel

Noch weniger ist über das Ausmaß des Einsatzes von IKT im Kontext von Menschenhandel bekannt. Es fällt auf, dass bei der Erwähnung von Menschenhandel nicht explizit darauf hingewiesen wird, um welche Form des Menschenhandels es sich handelt; implizit wird sich aber fast ausschließlich auf Menschenhandel zum Zwecke der sexuellen Ausbeutung bezogen. Einige Berichte nehmen an, dass auch im Kontext Menschenhandel digitale Gewalt stattfindet, ohne jedoch genauere Nachweise hierfür zu liefern oder die zugrunde liegende Definition transparent zu machen (vgl. z.B. UN Special Rapporteur on violence against women 2018: Abs. 32 und European Parliament's Committee on Women's Rights and Gender Equality 2018: 48). Erschwerend kommt hinzu, dass die Quelle mancher Behauptung nicht nachvollziehbar ist, so z.B.:

---

13 Siehe Beitrag: Erfahrungen mit der Beratung betroffener Mädchen und Frauen im Kontext digitaler Gewalt.

> »Social media is used by traffickers to sell people whose photographs they share without their consent, often including photographs of their abuse of women as an example to others. Seventy-six percent of trafficked persons are girls and women and the Internet is now a major sales platform.« (Women's Media Center, zit. nach: European Women's Lobby 2017: 8f.)

Da die European Women's Lobby nicht nur Menschenhandel, sondern auch jede Form der Prostitution und damit auch die selbstbestimmte Prostitution erwachsener Personen als Gewalt gegen Frauen bezeichnet und bekämpft, ist anzunehmen, dass hier möglicherweise nicht deutlich zwischen Prostitution und Menschenhandel differenziert wurde. So ist es durchaus vorstellbar, dass hier z.B. bereits Online-Werbung für sexuelle Dienstleistungen als eine Form digitaler Gewalt dargestellt wird. Daher ist bei solchen Behauptungen Vorsicht geboten. Auch über die Rolle des sogenannten Darknets im Kontext von Menschenhandel ist wenig bekannt (vgl. Cox 2015). Zwar wird vermutet, dass dort auch Menschenhandel stattfindet, Belege hierfür sind bislang nicht bekannt.

Die UN-Sonderberichterstatterin zu Gewalt gegen Frauen weist darauf hin, dass Menschenhändler*innen damit drohen können, private Informationen online zu veröffentlichen, um Macht und Kontrolle über ihre Opfer beizubehalten und sie davon abzuhalten, sich zu trennen oder juristische Schritte gegen sie zu unternehmen (vgl. UN Special Rapporteur on violence against women 2018: Abs. 32). Dies ist eine Praxis, von der auch Berater*innen von Fachberatungsstellen gegen Menschenhandel zum Zwecke der sexuellen Ausbeutung berichten. Auch die (Drohung der) Nennung der Klarnamen von Betroffenen von Menschenhandel zum Zweck der sexuellen Ausbeutung oder (Online-)Veröffentlichung von Fotos in Arbeitskleidung dürfte ein ›effektives‹ Mittel sein, um Betroffene von Menschenhandel zum Zwecke der sexuellen Ausbeutung zu erpressen. Denkbar ist auch, dass IKT genutzt wird, um Betroffene von Menschenhandel zu überwachen. Aber all dies ist bislang wenig grundlegend beforscht.

Auswirkungen digitalisierter geschlechtsspezifischer Gewalt

Die Ähnlichkeiten der Auswirkungen zwischen analoger und digitaler Gewalt sind nicht überraschend, zumal häufig beide Formen von Gewalt gleichzeitig angewandt werden. Die Wiener Studie stellte zunächst fest, dass Betroffene

und Berater*innen die Auswirkungen digitaler Gewalt unterschiedlich einschätzen, kommen aber zu einer Gesamteinschätzung wonach

> »*Betroffene von Gewalt im Netz ähnliche Symptome zu zeigen [scheinen] wie andere Gewaltopfer*, insbesondere bezüglich erhöhter Schreckhaftigkeit und Nervosität, in Bezug auf Ein- und Durchschlafstörungen sowie ein Gefühl der Entfremdung. Als die häufigsten *psychosomatischen Folgen* von Gewalt im Netz wurden *Angespanntheit bzw. Nervosität* (21,5 %), *Schlafstörungen* (9,0 %) und *Konzentrationsschwäche* (8,2 %) genannt. Zu den *sozialen Folgen* gehören *Rückzugsverhalten und eine Beeinträchtigung des Sicherheitsgefühls:* Fast jede fünfte von Gewalt im Netz betroffene Internetnutzerin beteiligte sich nach dem Übergriff weniger oder gar nicht mehr in den sozialen Netzwerken (19,7 %) und fühlt sich nach der Gewalterfahrung bedroht (17,5 %).« (Forschungszentrum Menschenrechte der Universität Wien/Weißer Ring 2018: 70, [Herv.i.O.])

Im Rahmen der Pew-Studie werden psychischer Stress, Probleme mit Familie oder Freund*innen als Auswirkungen digitaler Gewalt genannt. Einige der Befragten nannten zudem Rufschädigung und Schaden an der Liebesbeziehung, einige wenige nannten Probleme in der Schule/Arbeit, finanzielle Einbußen und die Schwierigkeit einen Job oder eine Wohnung zu finden (vgl. Pew Research Center 2017: 20).

Auch in der Darstellung möglicher Auswirkungen digitaler Gewalt differenziert die UN-Sonderberichterstatterin zu Gewalt gegen Frauen nicht zwischen Hate Speech und die Digitalisierung geschlechtsspezifischer Gewalt. Sie nennt aber Rückzug aus dem Internet, soziale Isolation und »limitierte Mobilität, wenn Frauen ihre Freiheit verlieren sich sicher zu bewegen« (UN Special Rapporteur on violence against women 2018: Abs. 26; Übersetzung N.P.) als mögliche Auswirkungen. Darüber hinaus betont sie, dass digitale Gewalt auch zu physischem Schaden führen kann, wenn z.B. durch gefälschte Anzeigen private Adressen von Frauen mit der Behauptung veröffentlicht werden, sie würden dort (vermeintlich) sexuelle Dienstleistungen anbieten. Zu wirtschaftlichem Schaden kann es kommen, wenn im Internet hinterlassene Behauptungen die Arbeitssuche von Betroffenen erschweren oder einschränken (vgl. ebd.: Abs. 27).

Betroffene von Überwachung durch IKT können zudem finanzielle Einbußen erleiden, die je nach Einkommen von erheblichem Ausmaß sein können; diese entstehen z.B. durch die Beschaffung neuer Geräte, E-Mailkonten und Bankkonten. Ein Bericht des European Parliament's Committee on Women's

Rights and Gender Equality schätzt die Kosten von digitaler Gewalt innerhalb von Partnerschaften auf 1.200 US-Dollar ein (vgl. European Parliament's Committee on Women's Rights and Gender Equality 2018: 34). Von digitaler Gewalt Betroffene, die beruflich auf das Internet bzw. auf eine Internetpräsenz angewiesen sind, erleiden einen Schaden, der nicht nur finanzieller Art ist, sondern deren Auswirkungen sich auch ökonomisch bemerkbar machen können. Denn eine (vorübergehende) Abwesenheit im Netz hat berufliche und damit auch ökonomische Folgen. Eine weitere ökonomische Folge von digitaler Gewalt entsteht, wenn Arbeitgeber*innen Personen kündigen, weil sie rufschädigende Informationen über sie im Netz finden.

Ungeklärt ist vielfach die Situation von Betroffenen von (Cyber-)Stalking und der Umgang im beruflichen Kontext mit der verpflichtenden Veröffentlichung von E-Mailadressen, auf die einige Arbeitgeber*innen bestehen. Die Sorge auf diese Weise für Stalker erreichbar zu sein, kann Betroffene davon abhalten beruflich aufzusteigen und hätte dadurch indirekte ökonomische Auswirkungen.

Die Association for Progressive Communication (APC) nennt zu den bereits genannten möglichen Auswirkungen auch die Verletzung des Rechts auf Leben durch den Einsatz von IKT und bezieht sich zum einen auf den Fall Fatma Yildirim gegen Österreich beim UN-CEDAW Ausschuss (vgl. CEDAW 2007). Frau Yildirim wurde, bevor sie von ihrem Mann umgebracht wurde, mehrfach telefonisch bedroht und belästigt (vgl. APC Women's Rights Programme 2015: 2). Zum anderen beziehen sie sich auf Fälle, bei denen Betroffene als Folge von IKT gestützter Gewalt Suizid begangen haben[14] (siehe auch UN-Special Rapporteur on violence against women 2018: Abs. 78). Zu diskutieren wäre daher, inwiefern solche Todesfälle nicht auch als Femizide zu werten wären.

Umgangsstrategien von Betroffenen

Die differenziertesten Aussagen zum Umgang von Betroffenen digitaler Gewalt finden sich ebenfalls in der Wiener Studie, die feststellte, dass die Betroffenen am häufigsten (53,7 %) Nutzer*innen sperren, 38,7 % versuchen, eine sachliche Auseinandersetzung mit den Verursacher*innen der Gewalt zu

14 Zu nennen sind hier Frauen wie Tiziana Cantone aus Italien oder aber die 15-jährige Amanda Todd aus Kanada und die 17-jährige Julia Rebecca aus Brasilien.

suchen, 23,1 % melden das Verhalten den Providern, während nur 21,4 % eine Beweissicherung vornehmen (vgl. Forschungszentrum Menschenrechte der Universität Wien/Weißer Ring 2018: 71f.). Unterstützung durch eine Vertrauensperson oder eine externe Stelle nahmen lediglich 7,5 % der Betroffenen an, manche wechselten ihre Telefonnummer und nur 6,9 % gab an, online Unterstützung durch Freund*innen erhalten zu haben. Erschreckend ist auch das Ergebnis, dass 9,6 % gar nichts unternahmen (vgl. ebd.: 73). Auch berichten Berater*innen mehrheitlich davon, dass »Betroffene nach einer Erfahrung mit Gewalt im Netz soziale Medien mieden oder dort weniger aktiv waren« (ebd.: 66). Diese Ergebnisse decken sich nur zum Teil mit denen der Pew-Studie. Denn diese stellt zunächst fest, dass die Mehrheit der Betroffenen (61 %) die Vorfälle ignorierte. Von den verbleibenden 39 % entschieden sich die Betroffenen zum Teil für mehrfache Reaktionen: die Hälfte konfrontierte die Tatverantwortlichen online und blockierte die Personen, 22 % meldeten die Vorfälle den Providern, 14 % diskutierten das Problem online und jeweils ca. 10 % wechselten ihre Onlineidentität bzw. entfernten Profile und mieden Onlineplattformen. Lediglich 5 % meldeten das Erlebte den Strafverfolgungsbehörden (vgl. Pew Research Center 2017: 26). Auch hier wurde festgestellt, dass sich Personen aus Sorge aus dem Netz zurückzogen.

Neben der Frage des Umgangs durch Betroffene stellt sich auch die Frage, ob und wie Zeug*innen digitaler Gewalt tätig werden oder ob sie durch ihr Schweigen eher eine Zustimmung signalisieren und damit eher gewaltverstärkend wirken. Da ein Großteil der digitalen Gewalthandlungen darauf abzielen, Personen öffentlich zu diskreditieren, ist dies, anders als bei analoger Gewalt, fast immer mit einer Großzahl von Zeug*innen verbunden, die mit ihrer Reaktion als korrektive Instanz auftreten könnten – wie sie dies im Kontext von Hate Speech bereits tun (siehe z.B. Amadeu Antonio Stiftung 2019). Auch sind viele Handlungen durch die öffentliche Verbreitung theoretisch nachweisbar und dem sozialen Umfeld des Täters bekannt. Vorstellbar wäre, das soziale Umfeld des Täters vermehrt zu animieren und hier unterstützend für die Betroffenen tätig zu werden bzw. auf eine Verantwortungsübernahme auf Seiten der Täter hinzuwirken.

Prävention

Selbstschutz bzw. Awareness

Auch im Kontext IKT gestützter Gewalt im sozialen Nahfeld zeigt sich, dass eine genderstereotype Verteilung von Aufgaben im Haushalt die Vulnerabilität von Frauen erhöht. So

> »interessieren sich Frauen durchaus für ein SmartHome, sind jedoch geschlechterrollen- und alltagszeitbedingt nicht bereit, zusätzliche Zeit sozusagen spielerisch für die Auseinandersetzung mit den technischen Hintergründen aufzuwenden. Es ist also wahrscheinlich, dass Frauen nicht hinter die technischen Kulissen ihres Smartphones schauen werden. […]« (Stelkens 2019: 4)

Nicht nur im Sinne einer effektiven Prävention gegen IKT gestützte Gewalt kann es sinnvoll sein, die eigenen digitalen Fähigkeiten zu pflegen, bzw. ständig zu aktualisieren und die Medienkompetenzen zu erweitern. Denkbar wäre zumindest für die kommende Generation, dies zum verpflichtenden Teil des Schulunterrichts zu machen. Realistischerweise wird es nicht von heute auf morgen möglich sein, diesen technologischen Gendergap zu überwinden, daher wäre es wichtig, sich selbst in diesem Bereich fortzubilden, bzw. diesen Bereich nicht ›automatisch‹ männlichen Personen zu überlassen. Im Falle einer (gewaltvollen) Trennung ist es mindestens wichtig, sich zumindest daran zu erinnern, welche Geräte der Ex-Partner eingerichtet hat und wer sich mit wem Passwörter/Clouds etc. teilt. Im Idealfall kennen alle Beteiligten die Passwörter für die Einrichtung von gemeinsam genutzten Geräten, Clouds, Netzwerken, Plattformen etc.

Für Berater*innen im Bereich der Anti-Gewalt-Arbeit heißt es in allen Fällen von Gewalt, mögliche digitale Bedrohungen regelmäßig abzufragen, um die digitale Sicherheit der Frauen, aber auch die Anonymität von Schutzeinrichtungen zu bewahren. Nicht nur in der Vergangenheit geteilte Geräte/Informationen sind hier relevant, sondern auch neue Geräte, die z.B. gemeinsame Kinder von dem getrennt lebenden Partner erhalten. Eine solche Abfrage könnte auch zur Bewusstwerdung der Gefahren digitaler Gewalt beitragen.[15]

Alle ›Warnungen‹, die Frauen davon abhalten sich ungehindert im Internet zu bewegen, können nicht als zielführend im Sinne einer feministi-

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

schen Antwort auf Digitalisierung geschlechtsspezifischer Gewalt sein; vielmehr gleichen diese eher einer Kapitulation. Amnesty International spricht von einem »silencing effect«, wenn Frauen und trans Personen aufgrund ihrer Gewalterfahrung sich aus dem Netz zurückziehen und/oder zensieren (vgl. Amnesty International 2017: Chapter 5) und bewertet diesen Einfluss auf ihre freie Meinungsäußerung als besorgniserregend, nicht nur für Twitter, sondern für die gesamte Gesellschaft (vgl. ebd.). Die Pew-Studie spricht in diesem Zusammenhang von einem »chilling effect«[16], wenn selbst ›nur‹ Zeug*innen von Online-Belästigung sich aus dem Netz aus Sorge zurückziehen (vgl. Pew Research Center 2017: 35).

Strukturelle Ebene: Prävention als menschenrechtliche Verpflichtung

Staaten, die ihren menschenrechtlichen Verpflichtungen nachkommen, alle geeigneten Maßnahmen gegen Gewalt gegen Frauen zu ergreifen, sind auch in der Pflicht präventiv tätig zu werden. So haben Staaten (wie Deutschland), die die Istanbul-Konvention ratifiziert haben, sich verpflichtet

> »die erforderlichen gesetzgeberischen oder sonstigen Maßnahmen [zu treffen], um sicherzustellen, dass vorsätzliches Verhalten, durch das die psychische Unversehrtheit einer Person durch Nötigung oder Drohung ernsthaft beeinträchtigt wird, unter Strafe gestellt wird.« (Europarat 2011: 15)

Eine ähnliche Verpflichtung ergibt sich auch aus der Ratifizierung von CEDAW, der UN-Frauenrechtskonvention[17]. In nahezu allen Studien und Berichten wird deutlich, dass die bestehenden gesetzlichen Möglichkeiten und deren Umsetzung als sehr defizitär bzw. ineffektiv wahrgenommen werden und damit keineswegs den Mindeststandards einer wirksamen Beschwerde[18] erfüllen dürften. Nicht zuletzt deshalb müssen Betroffene eigene – zum Teil sehr phantasievolle und mutige[19] – Wege des Umgangs mit digitaler Gewalt finden. So kommt beispielsweise der Bericht der FRA zu dem Ergebnis, dass

16 Entmutigender Effekt mit der Folge, dass Personen sich zurückziehen.

17 Siehe Beitrag: Menschenrechtlicher Schutzrahmen für Betroffene von digitaler Gewalt.

18 Wie definiert in Art. 2(3) des Zivilpaktes oder Art. 2 CEDAW.

19 So z.B. Emma Holten, deren Nacktfotos ohne ihre Zustimmung 2014 im Internet verbreitet wurden. Holten engagierte eine Photographin und bat sie Nacktfotos von ihr zu machen, die sie dann unter dem Titel »Zustimmung« selbst ins Internet stellte, um so zumindest das Gefühl zu haben, dass sie entscheiden kann, welche Nacktfotos von ihr im Netz kursieren. Zu alternativen Bewältigungsstrategien siehe Beiträge von Klant und Bauer in dieser Publikation.

> »im Internet und in sozialen Medienplattformen Maßnahmen ergriffen werden sollten, um Stalking-Opfer proaktiv bei der Meldung von Missbrauch zu unterstützen. Es sollte auch dazu aufgefordert werden, aktiv auf das Verhalten von TäterInnen zu reagieren. Parallel dazu kann die Polizei bestärkt werden, routinemäßig Fälle aufzugreifen und zu untersuchen, in denen Stalking über Internet oder Mobiltelefon eine Rolle spielt.« (FRA 2014: 13)

Im Kontext von digitaler Gewalt gilt die staatliche Verantwortung auch für technische Erneuerungen. So wäre zu diskutieren, ob Staaten (oder die EU) ihren menschenrechtlichen Verpflichtungen nachkommen, wenn sie weiterhin Hersteller*innen von Apps, bzw. Betreiber*innen von Plattformen den Freiraum gestatten, den sie derzeit genießen. Köver weist darauf hin, dass einige Hersteller*innen ihre Apps ungeniert als »Hilfsmittel für Partnergewalt« (Köver 2019: o.S.)[20] bewerben. Sie erinnert daran, dass Hersteller*innen von Apps beispielsweise gezwungen werden könnten, den

> »›Tarn-Modus‹ zu entfernen, also die Möglichkeit, eine App unsichtbar im Hintergrund auf einem Telefon laufen zu lassen, ohne dass die überwachte Person dies mitbekommt. Schließlich gibt es keinen legalen Anwendungsfall, bei dem so ein Feature nötig wäre. Wenn eine Person der Überwachung zugestimmt hat, muss man die Software nicht vor ihr verstecken. Wenn es um das eigene Kind geht, kann auch dieses über die Kontroll-App informiert werden.« (Köver 2019: o.S.)

Auch im Kontext des IoT gäbe es technische Möglichkeiten, die einen faireren Umgang mit den Geräten ermöglichen. Denkbar wäre auch eine gesetzliche Regelung, nach der eine »manuelle Notsteuerung als Sicherheitsauflage in Smarthome Geräten« (Stelkens 2019: 8) vorgeschrieben wäre.

Um die Ineffektivät bisheriger staatlicher Reaktionen im Kontext digitaler Gewalt zu veranschaulichen, erinnert Stelkens an die lange ignorierten Risiken der atomaren Strahlung und der damaligen Aufforderung staatlicher Stellen sich mit Aktentaschen gegen atomare Strahlen zu schützen! In einer weiteren Analogie argumentiert sie, dass gemäß Straßenverkehrsrecht nur diejenigen ein gefährliches Werkzeug (Auto) bewegen dürfen, die zwangsversichert sind und über eine entsprechende Ausbildung verfügen (vgl. Stelkens 2016: 157). Das, so Stelkens weiter, »erscheint auf digitalen Autobahnen noch

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

undenkbar« (ebd.). So wäre zu diskutieren, wie die Verkehrsregeln für einen fairen gleichberechtigten Zugang im Netz[21] aussehen könnten, die intersektionalen Vulnerabilitäten Rechnung tragen. Hier bräuchte es sowohl Maßnahmen auf präventiver Ebene, als auch Interventionsmöglichkeiten bei Regelbruch, die zum einen die Betroffenen adäquat schützen, aber auch die Regelbrecher*innen effektiv und verhältnismäßig in die Verantwortung nehmen.

Intervention

Da digitale Gewalt ähnliche Auswirkungen hat wie analoge Gewalt gegen Frauen, dürften die Bedarfe von Betroffenen digitaler und analoger Gewalt ebenfalls ähnlich sein. Hierzu gehören z.B. eine sichere Umgebung, ein Umfeld, das ihnen ohne Schuldzuweisungen glaubt und sie stärkt, die Möglichkeit einer Trennung ohne zu große Einbußen und einen diskriminierungsfreien und faktischen Zugang zum Recht (wenn erwünscht). Bei digitaler Gewalt müsste zudem geprüft werden, ob die Hilfsangebote für die vorwiegend jüngeren Betroffenen angepasst werden müssten oder in der jetzigen Form angemessen sind. Erschwerend kommt bei digitaler Gewalt hinzu, dass Betroffene häufig selbst, aber auch ihr Umfeld, die Wirkmächtigkeit der Gewalt in Frage stellen; dies müsste verstärkt in entsprechenden Beratungsangeboten berücksichtigt werden. Auch zeigt sich in vielen Fällen eine technische Überforderung im Umgang mit Gewalt. Daher ist auf der Ebene der Intervention wichtig, neben der individuellen Unterstützung, auch über eine strategische Begleitung von Einzelfällen eine Erweiterung des Schutzrahmens für Betroffene von digitaler Gewalt zu erreichen. Ebenso wäre es wichtig, hier perspektivisch mehr technische Interventionsmöglichkeiten zu entwickeln. Da das Menschenrecht an den Errungenschaften des wissenschaftlichen Fortschritts und seiner Anwendung teilzuhaben (Art. 15 (1) Sozialpakt) natürlich auch für Betroffene von digitaler Gewalt gilt, könnte eine Übersetzung hiervon auch bedeuten, IKT zu nutzen, um gegen Gewalt gegen Frauen vorzugehen. Schmidt weist z.B. darauf hin, »dass IoT-Systeme bald einschreiten können, wenn sie häusliche Gewalt registrieren« (Schmidt 2018: o.S.).

Für gestalkte Personen gibt es die ersten Apps, wie z.B. No Stalk oder Skytsengel (vgl. Institut für Sozialarbeit und Sozialpädagogik e.V. Beobachtungsstelle für gesellschaftspolitische Entwicklungen in Europa 2019: 7f.).

21 So werden einige dieser Ideen diskutiert unter der Utopie eines feministischen Internets; siehe hierfür z.B. https://feministinternet.org/en/principles [Zugriff: 13.2.2020].

Diese Apps können Vorfälle von (Cyber-)Stalking dokumentieren, im Notfall Unterstützer*innen informieren, Betroffenen die Möglichkeit geben in eine aktivere Rolle zu wechseln, aber auch Beweise für eine polizeiliche Anzeige zu verwenden, damit die Polizei eine sogenannte Gefährderansprache halten kann. Interessant ist hierbei der Befund, dass »in 80 % aller polizeilich erfassten Fälle das Stalking bereits nach dieser Ansprache aufhört« (ebd.: 7). Solche Mittel gilt es auszubauen bzw. zu bewerben, damit Betroffene von ihrer Existenz erfahren und Strafverfolgungsbehörden die dort gesicherten Nachweise anerkennen.

Vielfach werden neue gesetzliche Regelungen gefordert; sicherlich gibt es hier Lücken, die es zu schließen gilt.[22] Zu überprüfen wäre aber auch, ob es tatsächlich in allen Fällen neuer Regelungen bedarf, oder ob es in manchen Fällen ›lediglich‹ reichen würde, eine Erweiterung von Interpretationen bestehender Regelungen zu bewirken. So könnte eine Überlegung sein, regelmäßig bei Wegweisungen nach dem Gewaltschutzgesetz auch den digitalen Raum als einen zu definieren, der nicht zu betreten ist. Auch könnte es denkbar sein, z.B. Drohungen, die digitalen Grenzen einer Person zu verletzen, als »Drohung mit einem empfindlichen Übel« zu werten, welches ein Kernelement mancher strafrechtlichen Bestimmung ist. Ähnlich wäre es eine Möglichkeit, bei Schadensersatzklagen die finanziellen Verluste durch die Beschaffung neuer Geräte, aber auch die Offlinezeit, die finanzielle Einbußen mit sich brachten zu berücksichtigen. Auch wäre zu prüfen, ob Geräte, mit deren Hilfe digitale Gewalt ausgeübt wird, im Rahmen einer strafrechtlichen Verfolgung nicht zumindest vorübergehend zu beschlagnahmen wären; dies könnte zum einen die Beweissicherung erleichtern und zum anderen dafür sorgen, dass weitere Handlungen nicht unmittelbar folgen können. Auch dürfte dieser (vorübergehende) Verlust schmerzlich spürbar werden und könnte dadurch präventive Wirkung entfalten.

Ausblick

Sowohl »Rape Culture« als auch »Victim Blaming« bzw. Verantwortungsverschiebung, erleben im Kontext von digitaler Gewalt eine erstaunliche Renaissance. Stelkens weist treffend darauf hin, dass

22 Siehe Beitrag: Möglichkeiten und Grenzen strafrechtlicher Interventionen bei digitaler Gewalt.

> »im virtuellen Raum eine Frau immer gefährdet und verschärft auf ihre Geschlechterrolle zurückverwiesen [ist] und es bleibt ihr nur, sich männlich zu tarnen oder ganz zu tarnen oder technisch abgeschottete Räume zu nutzen, um sich selbst zu schützen. Eine Situation, die wir im öffentlichen Raum eigentlich glaubten überwunden zu haben.« (Stelkens 2016: 148)

Diese Haltung zeigt sich auch in manchen ›Ratschlägen‹. So wird betroffenen Frauen geraten, nicht den »Troll zu füttern« (European Parliament's Committee on Women's Rights and Gender Equality 2018: 21), ihre Sicherheitseinstellungen zu verändern oder gar für eine Weile offline zu gehen (vgl. z.B. ebd.). Die Absurdität des letzten ›Ratschlags‹ wird deutlich, weil auch Frauen, die gar nicht im Netz sind, Opfer von digitaler Gewalt werden können (vgl. Stelkens 2016: 148). Der ›Hinweis‹ sich aus dem Netz zurückzuziehen erinnert daran, wie Frauen in den fünfziger und sechziger Jahren geraten wurde Zuhause zu bleiben, um sich nicht zu gefährden! Bei aller berechtigter Sorge um eine mögliche Viktimisierung, kann das Ergebnis nicht sein, dass Frauen sich aus einem öffentlichen Raum zurückziehen, zumal dies den digitalen Raum noch toxischer machen dürfte.

Gegner*innen von Beschränkungen/Regelungen im Netz befürchten einen Eingriff in ihr Recht auf Meinungsfreiheit oder instrumentalisieren dieses Menschenrecht für eine eigene Agenda. Offenbar wird hierbei das Recht auf Meinungsfreiheit mit dem Recht auf freie Meinungsäußerung verwechselt. So werden beide Rechte im Zivilpakt garantiert (Art. 19); es wird aber auch gleichzeitig darauf hingewiesen, dass die Ausübung der freien Meinungsäußerung mit besonderen Pflichten und einer besonderen Verantwortung verbunden ist und damit bestimmten gesetzlichen Einschränkungen unterworfen werden kann, die z.B. erforderlich sind für die Achtung der Rechte oder des Rufs anderer (Art. 19.3). Dies wird in einem sogenannten General Comment des Menschenrechtsausschusses weiter expliziert, der darauf hinweist, dass mögliche Einschränkungen u.a. das Prinzip der Verhältnismäßigkeit erfüllen und angemessen sein müssen (vgl. ICCPR 2011: Abs. 34). Auch verweist der Ausschuss auf die notwendige Differenzierung zwischen öffentlichen und nichtöffentlichen Personen (vgl. ebd.: Abs. 47). Dieser Zusatz ist von Bedeutung, weil er daran erinnert, dass die Meinungsfreiheit vor allen Dingen dazu da ist, Menschen vor politischen Machthaber*innen zu schützen und daher

auch möglichst nicht einzuschränken ist.[23] Geforderte Einschränkungen der freien Meinungsäußerung gegenüber nicht öffentlichen Personen, um ihren Ruf zu schützen, bzw. um sie zu schützen, dürften damit nicht das Recht auf Meinungsfreiheit einschränken und legitim im menschenrechtlichen Sinne sein.

Zunehmend wird »das Recht auf Vergessen« im Internet diskutiert; zum einen durch Rechtsprechungen[24], aber auch durch Sorge von Pädagog*innen darüber, dass Jugendliche Spuren im Netz hinterlassen, die ihnen im Erwachsenenleben möglicherweise schaden. Dieses »Recht auf Vergessen« könnte künftig auch im Umgang mit der Digitalisierung von Gewalt gegen Frauen erweitert werden, um das »Recht auf Löschen«. Die Wiener Studie weist darauf hin, dass

> »[m]ithilfe einer 2009 von Microsoft vorwiegend zur Bekämpfung von Kinderpornographie entwickelten Technologie es möglich [ist], *Fotos und Videos so etwas wie einem ›digitalen Fingerabdruck‹ – einen sogenannten ›Hash‹ – zuzuordnen und diesen in einer Datenbank abzuspeichern*. Wird danach dasselbe Foto oder Video wieder hochgeladen, kann der Hash dieser neuen Datei mit den Hashes in der Datenbank abgeglichen und bei einer Übereinstimmung die Veröffentlichung des neu hochgeladenen Inhalts verhindert werden. Dieses Verfahren funktioniert selbst dann, wenn die Dateien durch eine Änderung der Größe oder durch das Hinzufügen von Markierungen leicht verändert wurden. Seit Dezember 2016 setzen die IT-Unternehmen Facebook, Microsoft, Twitter und YouTube diese Technik bspw. zur gemeinsamen Bekämpfung von terroristischen Inhalten ein.« (Forschungszentrum Menschenrechte der Universität Wien/Weißer Ring 2018: 41 [Herv. i.O.])

Die Wiener Studie weist ferner darauf hin, dass Facebook in den USA begonnen hat diese Methode auch im Umgang von ›Rachepornos‹ einzusetzen. Facebook Australien geht – nach eigenen Angaben – noch ein Stück weiter und »bietet seinen NutzerInnen die Möglichkeit, die unerwünschte Verbreitung von Nacktfotos bereits präventiv zu unterbinden« (ebd.: 42). Die Ergebnisse dieser Ankündigungen gilt es abzuwarten. Es wird aber deutlich, dass

---

23 Beispielhaft hierfür ist die juristische Auseinandersetzung um Jan Böhmermann und seinen Äußerungen zu dem türkischen Präsidenten Erdoğan.

24 Wie z.B. das Verfahren von Mario Costeja González, der von Google erfolgreich verlangte Links zu entfernen, die eine veraltete Pfändung sichtbar machten (vgl. Härting 2014: o.P.).

technisch sehr viel mehr möglich wäre als gegenwärtig umgesetzt wird, so auch der Wunsch nach Löschung von (ruf-)schädigendem Material im Netz oder die Verfolgung von Material auf ausländischen Servern. Beides ist technisch machbar und wird in anderen Bereichen bereits praktiziert. Es bleibt die Frage, warum Betroffene digitaler Gewalt (in Deutschland) nicht auch hiervon Gebrauch machen können und ob sie hierfür auf die Gunst der Provider angewiesen bleiben sollten oder ob hier der Gesetzgeber in der Verpflichtung wäre präventiv vorzusorgen.

Die Erkenntnis, dass »nur ein relativ kleiner Anteil der Betroffenen (21,1 %) Unterstützung bei Familie oder FreundInnen, der Polizei, Beratungsstellen, PsychotherapeutInnen bzw. PsychologInnen oder bei Providern suchte« (ebd.: 81) gibt Anlass darüber nachzudenken, woran dies liegt. Möglicherweise hat dies auch damit zu tun, dass die Betroffenen das Erlebte – anders als bei körperlichen/sexuellen Angriffen – zunächst nicht als Gewalt klassifizieren. So weisen NGOs darauf hin, dass eine häufige Reaktion auf Kampagnen/Öffentlichkeitsarbeit zu digitaler Gewalt ist, dass sich Betroffene an sie wenden und darüber berichten, dass sie durch die Information erst das Erlebte als eine Gewalterfahrung erkannten.[25] Eine Überlegung wäre, ob nicht Beratungsstellen hierauf im Rahmen ihrer Öffentlichkeitsarbeit vermehrt reagieren sollten. Auch wäre zu überlegen, ob die überproportionale Betroffenheit von Mädchen/jungen Frauen ebenso Konsequenzen für die Öffentlichkeitsarbeit und die Zusammensetzung der Teams von Fachberatungsstellen haben müsste.

Die COVID-19-Pandemie hat, was die Digitalisierung angeht, für große Teile der Gesellschaft einen Quantensprung erzeugt, der sonst vermutlich nicht so schnell vorangegangen wäre. Viele Menschen haben (erstmals) gelernt online zu arbeiten, zu lehren, sich zu treffen oder vielleicht sogar Sport zu machen. Auch wenn diese Zeit offenbar teilweise genderstereotype Arbeitsteilung im Kontext von Care-Arbeit zementiert, bleibt zu hoffen, dass diese unfreiwillige Digitalisierung den Gendertechnologiegap zumindest ein wenig verringert haben könnte. Auch dies gilt es abzuwarten. Sollte dieser Gap allerdings bestehen bleiben, bleibt es zu hoffen, dass sowohl der Staat als auch Einzelne daran arbeiten werden, diesen zu verringern, nicht zuletzt um die Vulnerabilität gegenüber digitaler Gewalt zu senken.

---

25 Siehe Beitrag: Individuelle Strategien im Umgang mit geschlechtsspezifischer digitaler Gewalt.

Literatur

Amadeu Antonio Stiftung (Hg.) (2019): »Menschenwürde online verteidigen. 33 Social Media-Tipps für die Zivilgesellschaft«. https://amadeu-antonio-stiftung.de/wp-content/uploads/2020/03/Broschu%CC%88re-CIVIC-Internet.pdf [Zugriff: 12.5.2020].

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

APC Women's Rights Programme (Hg.) (2015): »Technology-related violence against Women«. https://apc.org/sites/default/files/HRC%2029%20VAW%202-pager_FINAL_June%202015_0.pdf [Zugriff: 8.5.2020].

Baden, Rebecca (2018): »Was es mit mir gemacht hat, als meine Nacktfotos geleakt wurden«. https://vice.com/de/article/xw4kdd/was-es-mit-mir-gemacht-hat-als-meine-nacktfotos-geleakt-wurden [Zugriff: 8.2.2020].

bff: Bundesverband Frauenberatungsstellen und Frauennotrufe (Hg.) (2017): »Ergebnisse einer Umfrage unter Frauenberatungsstellen und Frauennotrufen im bff«. https://frauen-gegen-gewalt.de/de/aktuelle-studien-und-veroeffentlichungen.html?file=files/userdata/downloads/studien/bff_Digitalisierung_geschlechtsspezifischer_Gewalt_Expertise_hartmann.pdf [Zugriff: 3.1.2020].

bff: Bundesverband Frauenberatungsstellen und Frauennotrufe (Hg.) (2019): »bff: aktiv gegen digitale Gewalt«. https://frauen-gegen-gewalt.de/de/bff-aktiv-gegen-digitale-gewalt.html [Zugriff: 20.2.2020].

BMFSJ: Bundesministerium für Familien, Senioren, Frauen, und Jugend (2004): »Lebenssituation, Sicherheit und Gesundheit von Frauen in Deutschland«. https://bmfsfj.de/blob/84328/0c83aab6e685eeddc01712109bcb02b0/langfassung-studie-frauen-teil-eins-data.pdf [Zugriff: 3.1.2020].

CEDAW: Committee on the Elimination of Discrimination against Women (Hg.) (1992): CEDAW General Recommendation No. 19: Violence against women. CEDAW/C/GC19.

CEDAW: Committee on the Elimination of Discrimination against Women (Hg.) (2007): Fatma Yildirim vs. Austria, Communication No. 6/2005. CEDAW/C/39/D/6/2005.

CEDAW: Committee on the Elimination of Discrimination against Women (Hg.) (2017): General recommendation No. 35 on gender-based violence

against women, updating general recommendation No. 19. CEDAW/C/GC/35.

Cox, Joseph (2015): »My Brief Encounter with a Dark Web ›Human Trafficking‹ Site. Nice try Europol«. https://vice.com/en_us/article/vvbazy/my-brief-encounter-with-a-dark-web-human-trafficking-siteb [Zugriff: 15.6.2020].

EIGE: Europäisches Institut für Gleichstellungsfragen (Hg.) (2017): »Gewalt im Internet gegen Frauen und Mädchen«. https://doi:10.2839/81725.

Europarat (Hg.) (2011): »Übereinkommen des Europarats zur Verhütung und Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt und erläuternder Bericht«. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680462535 [Zugriff: 3.1.2020].

European Parliament's Committee on Women's Rights and Gender Equality (Hg.) (2018): »Cyber violence and hate speech online against women«. Brussels: European Parliament. https://europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf [Zugriff: 8.1.2020].

European Women's Lobby (Hg.) (2017): »#HerNetHerRights. Mapping the state of online violence against women & girls in Europe«. https://womenlobby.org/IMG/pdf/hernetherrights_report_2017_for_web.pdf [Zugriff: 8.1.2020].

Forschungszentrum Menschenrechte der Universität Wien/Weißer Ring (Hg.) (2018): »Gewalt im Netz gegen Frauen & Mädchen in Österreich«. https://weisser-ring.at/wp-content/uploads/2019/10/Studie_Bestandsaufnahme_Gewalt_im_Netz_gegen_Frauen_und_Mädchen_in_Österreich.pdf [Zugriff: 10.2.2020].

FRA: European Union Agency for Fundamental Rights (Hg.) (2014): »Gewalt gegen Frauen: eine EU-weite Erhebung. Ergebnisse auf einen Blick«. Wien. https://fra.europa.eu/sites/default/files/fra-2014-vaw-survey-at-a-glance-oct14_de.pdf [Zugriff: 13.1.2020].

Frey, Regina (2020): »Geschlecht und Gewalt im digitalen Raum. Eine qualitative Analyse der Erscheinungsformen, Betroffenheiten und Handlungsmöglichkeiten unter Berücksichtigung intersektionaler Aspekte. Expertise für den Gleichstellungsbericht der Bundesregierung«. https://dritter-gleichstellungsbericht.de/de/article/239.geschlecht-und-gewalt-im-digitalen-raum-eine-qualitative-analyse-der-erscheinungsformen-betroffenheiten-und-handlungsm%C3%B6glichkeiten-unter-ber%C3%BCcksichtigung-intersektionaler-aspekte.html [Zugriff: 14.9.2020].

Härting. Niko (2014): »Einfach löschen ist auch bequem«. https://lto.de/recht/hintergruende/h/eugh-urteil-c-131-12-google-suchergebnisse-loeschen-recht-auf-vergessenwerden/ [Zugriff: 15.2.2020].

Henry, Nicola/Powell, Anastasia (2018): »Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research«, in: Trauma, Violence, & Abuse, vol. 19, No. 2, S. 195-208.

Human Rights Council (Hg.) (2013): Report of the Working Group on the issue of discrimination against women in law and in practice, 19. April 2013, A/HRC/23/50.

ICCPR: International Covenant on Civil and Political Rights (Hg.) (2011): General comment No. 34. Article 19: Freedoms of opinion and expression. CCPR/C/GC/34.

Institut für Sozialarbeit und Sozialpädagogik e. V./Beobachtungsstelle für gesellschaftspolitische Entwicklungen in Europa (Hg.) (2019): »Digitale Gewalt gegen Frauen: Neue Gewaltformen und Ansätze zu ihrer Bekämpfung in Europa«, in: Newsletter 2/2019.

Köver, Chris (2019): »Spionage-Apps sind in erster Linie ein Werkzeug für Partnergewalt«. https://netzpolitik.org/2019/spionage-apps-sind-in-erster-linie-ein-werkzeug-fuer-partnergewalt/ [Zugriff: 17.1.2020].

Lembke, Ulrike (2018): »Kollektive Rechtsmobilisierung gegen digitale Gewalt«. Berlin: Heinrich Böll Stiftung. https://gwi-boell.de/de/2018/01/09/kollektive-rechtsmobilisierung-gegen-digitale-gewalt [Zugriff: 17.1.2020].

National Network to end domestic violence (Hg.) (2015): »A Glimpse From the Field: How Abusers Are Misusing Technology«. https://static1.squarespace.com/static/51dc541ce4b03ebab8c5c88c/t/54e3d1b6e4b08500fcb455a0/1424216502058/NNEDV_Glimpse+From+the+Field+-+2014.pdf [Zugriff: 17.1.2020].

Ortiz-Müller, Wolf (Hg.) (2017): Stalking – das Praxishandbuch. Stuttgart: W. Kohlhammer Verlag.

Parsons, Christopher/Molnar, Adam/Dalek, Jakub/Knockel, Jeffrey/Kenyon, Miles/Haselton, Bennett/Khoo, Cynthia/Deibert, Ronald (2019): »The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry«. Citizen Lab Research (Hg.), Report No. 119, Toronto. https://citizenlab.ca/docs/stalkerware-holistic.pdf [Zugriff: 29.6.2020].

Pew Research Center (Hg.) (2017): »Online Harassment 2017«. https://pewresearch.org/internet/wp-content/uploads/sites/9/2017/07/PI_2017.07.11_Online-Harassment_FINAL.pdf [Zugriff: 26.6.2020].

Schmidt, Francesca (2018): »Das ›Internet der Dinge‹: Digitale Gewalt wird ›smart‹«, in: an.schläge VIII/2018. https://anschlaege.at/das-internet-der-dinge-digitale-gewalt-wird-smart/ [Zugriff: 17.1.2020].

Stelkens, Anke (2016): »Digitale Gewalt und Persönlichkeitsrechte«, in: STREIT 4/2016, S. 147-157.

Stelkens, Anke (2019): »Smarte Gewalt – Zur Digitalisierung häuslicher Gewalt im Internet of Things«, in: STREIT 1/2019, S. 3-9.

UN General Assembly (Hg.) (2006): Advancement of women: advancement of women In-depth study on all forms of violence against women Report of the Secretary-General; A/61/122/Add.1.

UN Special Rapporteur on violence against women (Hg.) (2018): Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective, 18.6.2018, A/HRC/38/47.

University of Bedfordshire/National Centre for Cyberstalking Research (Hg.) (2011): Cyberstalking in the United Kingdom. An Analysis of the ECHO Pilot Survey.

Women's Aid (Hg.) (2014): »Virtual World, real fear. Women's Aid report into online abuse, harassment and stalking«. https://1q7dqy2unor827bqjls0c4rn-wpengine.netdna-ssl.com/wp-content/uploads/2015/11/Women_s_Aid_Virtual_World_Real_Fear_Feb_2014-3.pdf [Zugriff: 8.2.2020].

Menschenrechtlicher Schutzrahmen für Betroffene von digitaler Gewalt

Ulrike Lembke

Gewalt ist eine Grund- und Menschenrechtsverletzung[1], welche der Staat mit allen geeigneten Mitteln unverzüglich zu bekämpfen und zu unterbinden hat. Die Istanbul-Konvention des Europarates konkretisiert die entsprechenden Staatenpflichten für den Bereich geschlechtsbezogener Gewalt. Deutschland hat die Istanbul-Konvention ratifiziert und ist damit zur Umsetzung verpflichtet. Allerdings folgen auch aus der UN-Frauenrechtskonvention (CEDAW), aus der Europäischen Menschenrechtskonvention (EMRK) und aus den Grundrechten des Grundgesetzes (GG) staatliche Schutzpflichten zur Unterbindung von geschlechtsspezifischer Gewalt. Diese Schutzpflichten gewinnen besonderes Gewicht, weil die Freiheit von (auch digitaler) Gewalt eine unverzichtbare Voraussetzung für die politische Teilhabe von Frauen und anderen Betroffenen von struktureller Diskriminierung und damit eine Funktionsbedingung von Demokratie ist.

Geschlechtsbezogene Gewalt als Menschenrechtsverletzung

Dass geschlechtsspezifische Gewalt eine Menschenrechtsverletzung darstellt (vgl. Elsuni 2011), ist im internationalen Rechtsdiskurs inzwischen allgemein anerkannt (vgl. CEDAW-Ausschuss 2017: 1f.). In den Texten der frühen Menschenrechtsverträge hatte sich dies zunächst nicht niedergeschlagen. Der Ausschuss für die UN-Frauenrechtskonvention bezeichnete 1992 erstmals in seiner Allgemeinen Erklärung Nr. 19 geschlechtsspezifische Gewalt explizit als eine Form von Geschlechtsdiskriminierung und Menschenrechtsverletzung (vgl. CEDAW-Ausschuss 1992). Der Ausschuss definierte geschlechtsbezogene

1 Die Ausführungen in diesem Text beziehen sich auf die Rechtslage mit Stand Juli 2020.

Gewalt als Gewalt, die sich »gegen eine Frau richtet, weil sie eine Frau ist, oder die Frauen unverhältnismäßig stark betrifft« (ebd.: § 6). Er betonte ferner, dass solche Gewalt gegen Menschenrechtsverträge verstößt und die Gleichstellung der Geschlechter verhindert (vgl. CEDAW-Ausschuss 1992). Der Staat muss danach nicht nur selbst solch schädigende Handlungen unterlassen. Er muss im Rahmen seiner Sorgfaltspflichten auch die erforderlichen Maßnahmen treffen, um geschlechtsbezogene Gewalt durch Privatpersonen, Organisationen oder Unternehmen zu verhindern, verfolgen und ggf. zu entschädigen (vgl. ebd.). Damit waren wesentliche Eckpunkte des menschenrechtlichen Schutzes vor geschlechtsspezifischer Gewalt benannt.

1993 verabschiedete die UN-Generalversammlung eine Erklärung gegen geschlechtsspezifische Gewalt, 1994 wurde erstmals eine UN-Sonderberichterstatterin für Gewalt gegen Frauen eingesetzt und die Convention of Belém do Pará angenommen, 1995 machte die 4. Weltfrauenkonferenz geschlechtsspezifische Gewalt zu einem wesentlichen Thema und auch in den Folgejahren war dies Gegenstand verschiedenster Aktivitäten.[2] Die UN-Ausschüsse entwickelten jeweils in Bezug auf die von ihnen überwachten Menschenrechtsverträge vergleichbare Konzeptionen von geschlechtsbezogener Gewalt als Menschenrechtsverletzung (vgl. Prasad 2011). Der Europäische Gerichtshof für Menschenrechte (EGMR) erläuterte in mehreren Entscheidungen, dass mangelhafter oder fehlender staatlicher Schutz gegen geschlechtsbezogene Gewalt unter das Verbot der Folter und unmenschlichen oder erniedrigenden Behandlung im Sinne des Artikel 3 EMRK fallen (vgl. EGMR vom 09.07.2019: § 70ff.; vom 09.09.2009: § 154ff.) oder gegen das Recht auf Leben nach Artikel 2 EMRK (vgl. EGMR vom 28.06.2016; vom 09.09.2009: § 128ff.) oder das Recht auf Achtung des Privat- und Familienlebens gemäß Artikel 8 EMRK (vgl. EGMR vom 11.02.2020: § 73ff.;

2 Grundlegend Elsuni (2011). Siehe ferner UNGA, Declaration on the Elimination of Violence against Women, 20. Dezember 1993, UN Doc. A/Res/48/104, Rn. 6; Special Rapporteur on violence against women, its causes and consequences, siehe https://ohchr.org/en/issues/women/srwomen/pages/srwomenindex.aspx [Zugriff: 20.8.2020]; und Inter-American Convention on the Prevention, Punishment and Eradication of Violence against Women (Convention of Belém do Pará) 1994; Fourth World Conference on Women, Beijing Declaration and Platform for Action 1995; UNGA, In-Depth-Study on All Forms of Violence Against Women: Report of the Secretary-General 2006, UN Doc. A/61/122/Add.1; UN Women, Commission on the Status of Women, Agreed Conclusions on the prevention and elimination of violence against women and girls, 15. März 2013, E/CN/6/2013/11.

vom 28.08.2013: § 70ff.), auch jeweils in Verbindung mit dem Diskriminierungsverbot aus Artikel 14 EMRK (vgl. EGMR vom 09.07.2019: § 108ff.; vom 09.09.2009: § 177ff.), verstoßen kann. Mit dem Übereinkommen des Europarates zur Verhütung und Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt (Istanbul-Konvention)[3] aus dem Jahr 2011 wurden solche Überlegungen in einem umfassenden Menschenrechtsdokument verbindlich kodifiziert (vgl. Nousiainen/Chinkin 2015: 37ff.), auf das gewaltbetroffene Frauen und Mädchen sich nun auch berufen können.

Digitale geschlechtsbezogene Gewalt und Menschenrechte

Die menschenrechtliche Konzeption geschlechtsbezogener Gewalt beruht auf mehreren wesentlichen Festlegungen. Gewalt wird als Effekt wie Grundlage hierarchischer Geschlechterverhältnisse verstanden (vgl. CEDAW-Ausschuss 2017). Ihre Bekämpfung erfordert daher Maßnahmen in verschiedenen Bereichen, betreffend insbesondere Geschlechterrollenstereotype, sozioökonomische Machtverhältnisse zwischen den Geschlechtern und intersektionale Diskriminierung (vgl. ebd.). Geschlechtsbezogene Gewalt kann durch staatliche Akteur*innen ausgeübt werden, aber auch durch Privatpersonen oder Unternehmen, sie kann Grenzen überschreiten und sie findet in öffentlichen wie in privaten Räumen statt (vgl. ebd.). Einige Formen geschlechtsbezogener Gewalt wie Gewalt in sozialen Nahbeziehungen (sogenannte häusliche Gewalt), sexualisierte Gewalt oder Gewalt im Bereich reproduktiver Gesundheit sind schon länger identifiziert (vgl. exemplarisch Lembke 2017), doch geschlechtsbezogene Gewalt kann unterschiedliche Formen annehmen, die alle zu bekämpfen sind (vgl. ebd.).

Ein notwendig entwicklungsfähiger Begriff von geschlechtsbezogener Gewalt umfasst auch ihre digitalen Erscheinungsformen. Die Einbeziehung erfolgt unterschiedlich: Teils werden zu den öffentlichen und privaten Räumen, in denen geschlechtsbezogene Gewalt ausgeübt wird, auch digitale Räume

3 Übereinkommen des Europarates zur Verhütung und Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt (Istanbul-Konvention) vom 11. Mai 2011, siehe https://rm.coe.int/1680462535 [Zugriff: 20.8.2020]. Der Europarat ist kein Organ der Europäischen Union, sondern ein regionaler völkerrechtlicher Zusammenschluss, dem beispielsweise auch Russland und die Türkei angehören.

oder »technology-mediated settings« (vgl. ebd.: § 6) gezählt. Teils wird darauf abgestellt, dass Informations- und Kommunikationstechnologien (IKT) oder soziale Medien als Mittel zur Ausübung geschlechtsbezogener Gewalt missbraucht werden (vgl. Commission on the Status of Women 2013: 13). Teils wird darauf verwiesen, dass menschenrechtlicher Schutz offline wie online effektiv sein muss (vgl. Human Rights Council 2012: 2), ob dies nun beispielsweise die Fortführung sogenannter häuslicher Gewalt mit digitalen Mitteln (vgl. Human Rights Council 2015: § 4) oder die strategische Nutzung digitaler Gewalt gegen Menschenrechtsaktivistinnen (vgl. UN General Assembly 2013: 2; Working Group on the issue of discrimination against women in law and in practice 2013: § 66) betrifft. Im Jahr 2018 hat die Sonderberichterstatterin zu Gewalt gegen Frauen einen Bericht zu digitaler geschlechtsbezogener Gewalt vorgelegt, in dem sie neben Ausmaß, Erscheinungsformen und Folgen auch die Entwicklungen im Internationalen Recht und den menschenrechtlichen Schutzrahmen nachzeichnet (vgl. UN Special Rapporteur 2018). Wichtige Menschenrechte, auf die Betroffene von geschlechtsspezifischer digitaler Gewalt sich berufen können, sind die Rechte auf Gleichheit und Nichtdiskriminierung, auf ein Leben frei von Gewalt, auf Meinungsfreiheit und Informationszugang sowie auf Datenschutz und Privatsphäre (vgl. ebd.: 11ff.).

Als Konventionen, die sich ausdrücklich mit digitaler Gewalt befassen, werden häufig noch die Lanzarote-Konvention[4], welche dem Schutz von Kindern vor sexualisierter Gewalt und Übergriffen im Internet dient sowie die Budapest-Konvention[5] angeführt, welche die Bekämpfung von Cyberkriminalität zum Gegenstand hat (vgl. Cybercrime Convention Committee 2018: 21ff., 36ff.). Die Lanzarote-Konvention kann für den Schutz von Kindern eine wichtige Rolle spielen und die Budapest-Konvention aufgrund ihres spezifischen Zuschnitts wesentliche Unterstützung bei der technischen Erfassung und effektiven Verfolgung von Cyberkriminalität bieten. Beide legen ihren Fokus jedoch nicht auf geschlechtsspezifische digitale Gewalt und rezipieren entsprechende Konzepte auch nur begrenzt. Sie können daher nur im Zusammenspiel mit den einschlägigen menschenrechtlichen Instrumenten erfolgreich sein. Rechtliche Diskurse zu digitaler Gewalt werden in Deutschland

4 Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention), 25. Oktober 2007.

5 Council of Europe Convention on Cybercrime, 23. November 2001, siehe https://coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 [Zugriff: 20.8.2020].

wenig geführt und fokussieren entweder auf den Kinder- und Jugendschutz[6] oder auf (häufig überdies eng verstandene) rassistische Hate Speech (vgl. exemplarisch Wissenschaftliche Dienste des Deutschen Bundestages 2016; siehe auch European Court of Human Rights 2020), ohne die Analogien und Intersektionen von rassistischer und geschlechtsspezifischer digitaler Gewalt zu berücksichtigen (vgl. hierzu Lembke 2016: 387ff.).

Digitale geschlechtsbezogene Gewalt und die Istanbul-Konvention

Es bietet sich daher an von den spezifischen Menschenrechtsinstrumenten auszugehen. Im europäischen Raum und in Deutschland ist neben CEDAW, die weltweit gilt, und der EMRK, der wichtigste Menschenrechtsvertrag, auf den sich gewaltbetroffene Frauen und Mädchen berufen können, die Istanbul-Konvention des Europarates (vgl. hierzu ausführlich Nousiainen/Chinkin 2015: 39ff.). Sie trat auf völkerrechtlicher Ebene am 1. August 2014 und für Deutschland nach Ratifikation am 1. Februar 2018 in Kraft. In der Istanbul-Konvention wird (in Artikel 3[d]) erstmals der Begriff geschlechtsbezogener Gewalt explizit in einem Menschenrechtsvertrag kodifiziert als Gewalt, die gegen eine Frau gerichtet ist, weil sie eine Frau ist, oder die Frauen unverhältnismäßig stark betrifft. Erfasst sind nach Artikel 3(a) alle Handlungen, die zu körperlichen, sexuellen, psychischen oder wirtschaftlichen Schäden oder Leiden bei Frauen führen oder führen können. Die Istanbul-Konvention verpflichtet die Vertragsstaaten detailliert und mit konkreten Handlungsaufträgen zur Verhütung, Verfolgung und Beseitigung geschlechtsspezifischer und häuslicher Gewalt, zur umfassenden Unterstützung der Betroffenen, zur grundlegenden Änderung der sozialen und kulturellen Rechtfertigungsstrukturen geschlechtsbezogener Gewalt und zur Förderung substantieller Gleichheit zwischen den Geschlechtern.

Auch wenn der Begriff der digitalen geschlechtsspezifischen Gewalt nicht explizit in der Istanbul-Konvention verwendet wird, erscheint sie besonders geeignet, auch gegen diese Formen geschlechtsspezifischer Gewalt zu wirken (vgl. Lange 2019: 3f.; ferner European Parliament 2017). Der Gewaltbegriff der Konvention, wie er insbesondere aus Artikel 3, Artikel 33 (Psychische Gewalt), Artikel 34 (Stalking) und Artikel 40 (Sexuelle Belästigung) folgt, ist nicht auf physische Erscheinungsformen beschränkt. Er umfasst auch nicht-physische

6 Siehe Beitrag: Rechtliche Handlungsoptionen: Öffentliches Recht.

Gewaltformen und damit auch Formen digitaler Gewalt (vgl. Lembke/Steinl 2018: 204) – ob diese im Einzelfall nun körperliche Auswirkungen haben (vgl. Henry/Powell 2015: 767ff.) oder nicht. Im Erläuternden Bericht zur Istanbul-Konvention wird in Bezug auf Stalking explizit festgestellt, dass dieses auch Verfolgung in der virtuellen Welt, unerwünschte Kontaktaufnahmen über IKTs und die Verbreitung von Falschinformationen im Internet umfasst (§ 182f.; vgl. Cybercrime Convention Committee 2018: 24). In seinem Plädoyer für einen Beitritt der EU zur Istanbul-Konvention hat das Europäische Parlament ausdrücklich auch geschlechtsbezogene digitale Gewalt, Cyber-Harassment und sexistische Hassrede als weit verbreitete und auf Grundlage der Istanbul-Konvention zu bekämpfende Gewaltformen benannt (European Parliament 2017: G, I, W). Und in einer aktuellen Entscheidung führte der EGMR (vom 11.02.2020: Rn. 74) – dessen Rechtsprechung für die Entstehung und Auslegung der Istanbul-Konvention von besonderer Bedeutung war und ist – aus, dass anerkannt sei, dass Cybergewalt eine wesentliche Dimension von geschlechtsbezogener Gewalt darstellt.

Die Expert*innengruppe GREVIO, welche die Umsetzung der Istanbul-Konvention in den Vertragsstaaten überwacht,[7] hat sich in ersten Evaluierungsberichten ebenfalls zu geschlechtsspezifischer digitaler Gewalt geäußert. Zum einen hat GREVIO nationale Maßnahmen zur Bekämpfung von digitaler geschlechtsspezifischer Gewalt (»cyberharassment«, »cybersexism«, »cyberbullying«, »digital raids«, »sexist insults« etc.) begrüßt und zu deren Vertiefung ermutigt (vgl. GREVIO 2017a: § 46f.; 2017b: § 16; 2019a: § 187, 203). Zum anderen wurden Vertragsstaaten ausdrücklich aufgefordert, digitale geschlechtsbezogene Gewalt insgesamt (vgl. GREVIO 2019a: § 91), sexistische Hassrede (vgl. GREVIO 2019b: § 87) oder die digitale Dimension von Gewaltformen wie Stalking (vgl. GREVIO 2018: § 221) oder sexueller Belästigung (vgl. GREVIO 2019c: § 235f.) zu fokussieren und entsprechende Maßnahmen zu ergreifen. Es ist davon auszugehen, dass der Fokus auf geschlechtsspezifischer digitaler Gewalt sich künftig eher noch erweitern wird.

7 Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO), gegründet 2015, siehe https://coe.int/en/web/istanbul-convention/grevio [Zugriff: 20.8.2020].

Die Geltung von Menschenrechten in Deutschland

Wenn die Bundesrepublik einen menschenrechtlichen Vertrag wie CEDAW oder die Istanbul-Konvention ratifiziert hat, kommt dieser quasi doppelt zur Geltung. Er gilt zum einen auf der Ebene internationalen Rechts und verpflichtet die Bundesrepublik zur Umsetzung der menschenrechtlichen Verpflichtungen. Gegenüber den jeweiligen UN-Ausschüssen (treaty bodies) muss vom Staat regelmäßig über die Umsetzung Bericht erstattet werden und, wenn dies vertraglich vorgesehen ist, können auch Betroffene Individualbeschwerde erheben oder der Ausschuss kann ein Untersuchungsverfahren einleiten (vgl. Rabe 2018: 152f.). Aufgrund der Völkerrechtsfreundlichkeit des Grundgesetzes sind die Grundrechte menschenrechtskonform auszulegen, solange dies methodisch vertretbar ist (vgl. BVerfG vom 29.1.2019 und vom 30.1.2020) und nach Ratifikation sind alle staatlichen Organe verpflichtet, alle nationalen Rechtsnormen im Lichte der Menschenrechte auszulegen und anzuwenden und auch ihr Ermessen menschenrechtskonform auszuüben (vgl. Rudolf/Chen 2014: 42ff.; Rabe 2018: 148f.; Uerpmann-Wittzack 2017: 1813f.).

Nach Artikel 59 Absatz 1 Satz 2 Grundgesetz setzt die Ratifikation ein Zustimmungsgesetz des Bundestages voraus, um wirksam durchgeführt zu werden. Dieses Zustimmungsgesetz führt zugleich dazu, dass der Menschenrechtsvertrag nun auch als innerdeutsches Recht im Rang eines Bundesgesetzes gilt (vgl. Uerpmann-Wittzack 2017: 1812). Durch den sogenannten innerstaatlichen Rechtsanwendungsbefehl verpflichtet der ratifizierte Menschenrechtsvertrag wie die UN-Frauenrechtskonvention (vgl. Rudolf/Chen 2014: 42ff.) oder die Istanbul-Konvention (vgl. Rabe 2018: 147ff.; Lembke/Steinl 2018: 204) alle staatlichen Ebenen in Deutschland, also Bund und Länder (und Kommunen) und ist von allen staatlichen Organen wie insbesondere Gesetzgeber, Gerichten und Behörden anzuwenden. Die Verpflichtung der Bundesländer (und damit Landesgesetzgeber) folgt aus ihrer Einbeziehung vor der Ratifikation im Rahmen des sogenannten Lindauer Abkommens sowie aus dem Grundsatz der Bundestreue. Die Verpflichtung für Gerichte und Behörden folgt aus ihrer Bindung an Recht und Gesetz (vgl. Deiseroth 2013: 26; Rudolf 2012: 600).

Die beschriebene Doppelgeltung hat verschiedene Folgen. Da der Menschenrechtsvertrag die Bundesrepublik auf internationaler Ebene verpflichtet, kann das inhaltsgleiche innerstaatliche Bundesrecht nicht einfach durch spätere widersprechende Gesetze ausgehebelt werden (vgl. Rudolf/Chen 2014:

42f.). Auch kann sich die Auslegung der Konventionen im Interesse internationaler Einheitlichkeit nicht an nationalen Maßstäben orientieren, sondern an der Spruchpraxis der jeweiligen UN-Ausschüsse (vgl. Rabe 2018: 148). Unterschiede ergeben sich in der innerstaatlichen Anwendung dadurch, dass einige Regelungen in Menschenrechtsverträgen Rechte und Pflichten so weit konkretisieren, dass sie unmittelbar durch Gerichte und Behörden anwendbar sind,[8] während andere Regelungen zunächst noch Konkretisierungen des Gesetzgebers fordern oder staatlichen Organen einen weiten Ermessensspielraum lassen[9] (vgl. Rudolf/Chen 2014: 45ff.; Uerpmann-Wittzack 2017: 1813).

Dies führt im deutschen Rechtsdiskurs immer wieder zu dem verblüffenden Missverständnis, Menschenrechtsverträge müssten trotz des innerstaatlichen Rechtsanwendungsbefehls eigentlich nicht angewendet werden, sondern »die Politik« könne frei entscheiden, ob sie die menschenrechtlichen Verpflichtungen umsetze oder nicht. Die Reduktion von Menschenrechten auf Politik ignoriert schon, dass es sich um verbindliches internationales *und* innerstaatliches Recht handelt. Vor allem aber bedeuten Umsetzungsspielräume nicht, dass die verpflichteten staatlichen Ebenen und Organe nicht tätig werden müssten. Ganz im Gegenteil: das Anforderungsprofil von Menschenrechtsverträgen geht teils deutlich weiter als verfassungsrechtliche Anforderungen an staatliches Handeln. Substantielle oder gar inklusive Gleichheit

8 Die UN-Frauenrechtskonvention ist weitgehend unmittelbar anwendbar und kann spezifische Schutzlücken füllen, so beispielsweise bezüglich des Schutzes vor sexueller Belästigung an Hochschulen (vgl. Rudolf/Chen 2014: 45ff.), aber auch grundsätzlich subjektive Ansprüche auf staatliches Handeln vermitteln wie den Verzicht auf schädigende Stereotype in Sexualstrafverfahren, die effektive Durchsetzung des Gewaltschutzgesetzes, die Aufhebung genereller Kopftuchverbote oder die Einschätzung der Bedarfsgemeinschaft als verfassungswidrig (vgl. Rudolf 2012: 601). Der subsidiäre staatliche Opferentschädigungsanspruch aus Art. 30 Abs. 2, 3 der Istanbul-Konvention könnte unmittelbar anwendbar sein, wobei es bereits die gesetzlichen Regelungen des OEG gibt (vgl. Uerpmann-Wittzack 2017: 1813).

9 Artikel 33 bis 40 der Istanbul-Konvention sind insoweit nicht anwendbar, als Straftatbestände durch den deutschen Gesetzgeber eindeutig statuiert werden müssen (vgl. Rabe 2018: 148; Uerpmann-Wittzack 2017: 1813). In Bezug auf das Strafprozessrecht kommt aber eine konventionskonforme Auslegung in Betracht (vgl. OLG Hamburg vom 8.3.2018); ebenso bei prozessualen Fragen im Familienrecht nach Artikel 31 der Istanbul-Konvention (Uerpmann-Wittzack 2017: 1813). Auch auf eine ermessensfehlerfreie Entscheidung über die Finanzierung von Frauenhäusern kann ein Anspruch geltend gemacht werden (vgl. Rudolf 2012: 601).

ist das Ziel. Fördermaßnahmen sind nicht nur erlaubt, sondern oftmals geboten. Und die staatlichen Pflichten umfassen nicht nur das Unterlassen von Benachteiligungen durch den Staat selbst, sondern effektive Maßnahmen gegen Ausgrenzung und Abwertung, gegen Gewalt und Stereotype sowie gegen Diskriminierung durch Hoheitsträger oder durch Private (Privatpersonen wie Unternehmen).

Staatliche Schutzpflichten gegen Gewalt durch Private

Aus den ratifizierten Menschenrechtsverträgen folgen verschiedene staatliche Pflichten. So ist die Bundesrepublik Deutschland (auf allen Ebenen und durch alle Organe) unter anderem aus der UN-Frauenrechtskonvention (vgl. UN Special Rapporteur 2018: 13ff.) und der Istanbul-Konvention verpflichtet, unverzüglich alle geeigneten Maßnahmen zur Verhütung und Verfolgung von geschlechtsbezogener digitaler Gewalt zu ergreifen, Betroffene zu unterstützen und ggf. zu entschädigen (vgl. Deutscher Juristinnenbund 2020) sowie soziale und kulturelle gewaltlegitimierende Muster radikal zu verändern. Dabei ist nicht ausreichend, dass der Staat irgendwie tätig wird, sondern die Maßnahmen müssen effektiv, also beispielsweise mögliche Sanktionen wirksam, verhältnismäßig und abschreckend sein (vgl. Erläuternder Bericht IK; Grans 2018: 145). Überdies besteht die Pflicht zur Verhütung und Verfolgung von geschlechtsbezogener digitaler Gewalt im Rahmen staatlicher Sorgfaltspflichten (due diligence) auch gegenüber Privaten, also Personen, die solche Gewalt ausüben, oder Betreiber*innen von Plattformen, Social Media und IKTs, welche diese ermöglichen oder von ihr profitieren (vgl. UN Special Rapporteur 2018: 13ff.; UN General Assembly 2013: § 9).

Ursprünglich bestand in internationalen wie deutschen Rechtsdiskursen die Vorstellung, dass Grund- und Menschenrechte nur gegen Maßnahmen und Verletzungen durch den Staat und staatliche Akteur*innen schützen sollten. Allerdings wird gerade im Bereich der geschlechtsbezogenen Gewalt deutlich, dass erhebliche Gefährdungen und Übergriffe auch von Privatpersonen, Organisationen und Unternehmen ausgehen; dies gilt auch für digitale Formen der Gewalt. Während Menschenrechtsverträge wie in Artikel 2(e) CEDAW und in Artikel 5 Absatz 2 der Istanbul-Konvention explizit staatliche Schutzpflichten gegen Menschenrechtsverletzungen durch Private vorsehen,

musste das Bundesverfassungsgericht[10] eine grundrechtliche Schutzpflicht erst aus der Wertordnung des Grundgesetzes eher aufwändig herleiten. Auch im menschenrechtlichen Diskurs war und ist allerdings umstritten, wie weit solche Schutzpflichten von Vertragsstaaten reichen (vgl. hierzu EGMR vom 9.9.2009: § 72ff.). Zunächst wurde der menschenrechtliche Sorgfaltsmaßstab (due diligence) für staatliches Handeln so verstanden, dass geschlechtsbezogene Gewalt bekämpft wurde, wenn sie auftrat. Inzwischen liegt weitaus mehr Augenmerk auf der Pflicht zur Vorbeugung und Verhinderung geschlechtsbezogener Gewalt, welche auch grundlegende Veränderungen patriarchaler Strukturen verlangt (vgl. grundlegend UN Special Rapporteur 2006: 6ff.; Grans 2018). Die Bundesrepublik begeht wie alle anderen Vertragsstaaten daher eine Menschenrechtsverletzung, wenn sie es versäumt, *alle* geeigneten Maßnahmen (vgl. hierzu CEDAW 2005: § 9.1ff.; 2007: § 12.1.1ff.; EGMR vom 9.9.2009: § 128ff.; UN Special Rapporteur 2006: § 38ff.; Beispiele auch bei Prasad 2011) zur Verhinderung oder zur Aufklärung, Verfolgung und Bestrafung geschlechtsbezogener Gewalt durch nicht-staatliche Akteur*innen zu ergreifen sowie die Betroffenen hierfür zu entschädigen (vgl. CEDAW 2017: § 24).

Digitale Gewalt als Demokratiegefährdung

Freiheit von geschlechtsbezogener Gewalt ist eine zentrale Bedingung dafür, dass Frauen und Mädchen ihre Rechte und Freiheiten gleichberechtigt genießen und aktiv wahrnehmen können. In politischen und rechtlichen Diskursen um digitale geschlechtsbezogene Gewalt wird nicht selten reflexhaft auf Meinungsfreiheit und Zensurverbot verwiesen und behauptet, rechtliche Interventionen würden das Internet als demokratiefunktionalen, digitalen öf-

10 Eine grundrechtliche Schutzpflicht wurde vom BVerfG (vom 25.2.1975) erstmals in seiner ersten Entscheidung zur Strafbarkeit des Schwangerschaftsabbruchs hergeleitet. Grundsätzlich sind Grundrechte Abwehrrechte der*des Einzelnen gegen den Staat und beschreiben ein bilaterales Verhältnis. Eine staatliche Schutzpflicht setzt ein trilaterales Verhältnis voraus, wonach Grundrechtsverletzungen von einer Person gegen eine andere Person drohen und der Staat sich zwischen beide stellt (beispielsweise bei sogenannter häuslicher Gewalt). Beim Schwangerschaftsabbruch fehlt es aber gerade an diesem konstituierenden Dreiecksverhältnis, weil Schwangere und Fötus nicht trennbar sind und der Staat kann auch nicht für die Schwangere eintreten, da er keine Gebärmutter hat (vgl. Rupp-v. Brünneck/Simon 1975; Lembke 2018: 34).

fentlichen Raum zerstören (sehr kritisch Citron 2014: 190ff.). Diese Reaktion ist bekannt in Bezug auf alle Anstrengungen, bislang diskriminierten Gruppen rechtliche Mittel und effektiven Rechtszugang zu verschaffen. Zudem übersieht ein solcher Ansatz, dass die Meinungsfreiheit nicht unbeschränkt gilt (vgl. European Court of Human Rights 2020) und sich überdies gerade auch (potentiell) gewaltbetroffene Frauen und Mädchen auf dieses Grund- und Menschenrecht berufen können (vgl. UN Special Rapporteur 2018: 11f.). Frauen und Mädchen dürfen nicht durch digitale geschlechtsbezogene Gewalt an der Teilhabe an Information und Kommunikation gehindert oder gezielt aus digitalen öffentlichen Räumen verdrängt und gemobbt werden.

Effektiver Zugang zu digitalen Räumen und IKT-Diensten ist eine wesentliche Voraussetzung für die politische Partizipation von Frauen und ihre aktive Mitwirkung am Gemeinwesen (vgl. Gurumurthy 2013). Die menschenrechtlich geforderte gleiche Teilhabe von Frauen am politischen und öffentlichen Leben meint nicht nur formale Gleichheit oder technische Mittel und Kompetenzen (obwohl dies auch sehr wichtige Voraussetzungen sind), sondern ebenso einen diskriminierungsfreien Zugang zu digitalen Öffentlichkeiten und Diskursen in der gelebten Rechtswirklichkeit (vgl. Lembke 2016: 403f.). Effektiver Gewaltschutz im digitalen wie analogen Raum ist nicht nur eine aus Grund- und Menschenrechten folgende, zwingende staatliche Verpflichtung, sondern eine Funktionsbedingung für Demokratien im 21. Jahrhundert.

Literatur

CEDAW-Ausschuss (Committee on the Elimination of Discrimination Against Women) (1992): »General recommendation No. 19: Violence against women«. https://ohchr.org/EN/HRBodies/CEDAW/Pages/Recommendations.aspx [Zugriff: 28.6.2020].

CEDAW-Ausschuss (Committee on the Elimination of Discrimination Against Women) (2005): »Communication No. 2/2003 of 26 January 2005 – Ms. A.T. v. Hungary. https://un.org/womenwatch/daw/cedaw/protocol/decisions-views/CEDAW%20Decision%20on%20AT%20vs%20Hungary%20English.pdf [Zugriff: 28.6.2020].

CEDAW-Ausschuss (Committee on the Elimination of Discrimination Against Women) (2007): »Communication No. 6/2005 of 1 October 2007 – Fatma

Yildirim v. Austria«. https://coe.int/t/dg2/equality/domesticviolencecampaign/resources/FatmaYildirimVsAustria_en.pdf [Zugriff: 28.6.2020].

CEDAW-Ausschuss (Committee on the Elimination of Discrimination Against Women) (2017): »General recommendation No. 35 on gender-based violence against women, updating general recommendation No. 19«. https://ohchr.org/EN/HRBodies/CEDAW/Pages/Recommendations.aspx [Zugriff: 28.6.2020].

Citron, Danielle Keats (2014): Hate Crimes in Cyberspace. Cambridge: Harvard University Press.

Commission on the Status of Women (2013): »Report on the fifty-seventh session (4-15. March 2013)«. https://refworld.org/docid/51f0f2344.html [Zugriff: 28.6.2020].

Cybercrime Convention Committee (2018): »Mapping study on cyber violence. T-CY(2017)10«. Council of Europe. 9 July 2018. https://rm.coe.int/t-cy-2017-10-cbg-study-provisional/16808c4914 [Zugriff: 28.6.2020].

Deiseroth, Dieter (2013): »Innerstaatliche Gerichte und Völkerrecht«, in: Roggan, Fredrik/Busch, Dörte (Hg.), Das Recht in guter Verfassung? Festschrift für Martin Kutscha, Baden-Baden: Nomos, S. 23-38.

Deutscher Juristinnenbund (djb) (2020): »Themenpapier 11 vom 7.2.2020 zur Umsetzung der Istanbul-Konvention in Deutschland: Entschädigung Betroffener bei psychischer Gewalt mit schweren Folgen«. https://djb.de/themen/thema/ik/st20-09/ [Zugriff: 28.6.2020].

Elsuni, Sarah (2011): Geschlechtsbezogene Gewalt und Menschenrechte. Eine geschlechtertheoretische Untersuchung der Konzepte Geschlecht, Gleichheit und Diskriminierung im Menschenrechtssystem der Vereinten Nationen. Baden-Baden: Nomos.

European Court of Human Rights (2020): »Fact Sheet – Hate Speech«. https://echr.coe.int/Documents/FS_Hate_speech_ENG.pdf [Zugriff: 28.6.2020].

European Parliament (2017): »Resolution of 12 September 2017 on the proposal for a Council decision on the conclusion, by the European Union, of the Council of Europe Convention on preventing and combating violence against women and domestic violence (COM(2016)0109 – 2016/0062[NLE])«. https://europarl.europa.eu/doceo/document/TA-8-2017-0329_EN.html [Zugriff: 28.6.2020].

Grans, Lisa (2018): »The Istanbul Convention and the Positive Obligation to Prevent Violence«, in: Human Rights Law Review, Vol. 18 Nr. 1, S. 133-155.

Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO) (2017a): »Baseline Evaluation Report Monaco«. https:/

/coe.int/en/web/istanbul-convention/country-monitoring-work [Zugriff: 28.6.2020].

Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO) (2017b): »Baseline Evaluation Report Denmark«. https://coe.int/en/web/istanbul-convention/country-monitoring-work [Zugriff: 28.6.2020].

Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO) (2018): »Baseline Evaluation Report Turkey«. https://coe.int/en/web/istanbul-convention/country-monitoring-work [Zugriff: 28.6.2020].

Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO) (2019a): »Baseline Evaluation Report France«. https://coe.int/en/web/istanbul-convention/country-monitoring-work [Zugriff: 28.6.2020].

Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO) (2019b): »Baseline Evaluation Report Italy«. https://coe.int/en/web/istanbul-convention/country-monitoring-work [Zugriff: 28.6.2020].

Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO) (2019c): »Baseline Evaluation Report Netherlands«. https://coe.int/en/web/istanbul-convention/country-monitoring-work [Zugriff: 28.6.2020].

Gurumurthy, Anita (2013): »Participatory citizenship: Tracing the impact of ICTs on the social and political participation of women«, in: Association for Progressive Communications (APC) & Humanist Institute for Cooperation with Developing Countries (Hivos) (Hg.), Women's rights, gender and ICTs, Global Information Society Watch, S. 25-30.

Henry, Nicola/Powell, Anastasia (2015): »Embodied Harms: Gender, Shame, and Technology-Facilitated Sexual Violence«, in: Violence Against Women, Vol. 21 Nr. 6, S. 758-779.

Human Rights Council (HRC) (2012): »The promotion, protection and enjoyment of human rights on the Internet«. A/HRC/RES/20/8. https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/G12/153/25/PDF/G1215325.pdf [Zugriff: 28.6.2020].

Human Rights Council (HRC) (2015): »Accelerating efforts to eliminate all forms of violence against women: eliminating domestic violence«. A/HRC/RES/29/14. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/161/82/PDF/G1516182.pdf [Zugriff: 28.6.2020].

Lange, Katrin (2019): »Digital violence against women at European level«, in: Newsletter of the Observatory for Sociopolitical Developments in Europe, Nr. 2, S. 2-4. https://sociopolitical-observatory.eu/ [Zugriff: 28.6.2020].

Lembke, Ulrike (2016): »Ein antidiskriminierungsrechtlicher Ansatz für Maßnahmen gegen Cyber Harassment«, in: Kritische Justiz, Vol. 49 Nr. 3, S. 385-406.

Lembke, Ulrike (2017): »Staatliche Handlungspflichten gegen geschlechtsspezifische Gewalt«, in: Zeitschrift des Deutschen Juristinnenbundes (djbZ), Nr. 2, S. 63-66.

Lembke, Ulrike (2018): »Staatsbürgerinnenschaft unter Vorbehalt: reproduktive Politiken und Geschlechterdemokratie«, in: Journal Netzwerk Frauen- und Geschlechterforschung NRW, Nr. 43, S. 28-36.

Lembke, Ulrike/Steinl, Leonie (2018): »Die Istanbul-Konvention – ein Meilenstein für den Schutz vor geschlechtsbezogener Gewalt«, in: Zeitschrift des Deutschen Juristinnenbundes (djbZ), Nr. 4, S. 203-206.

Nousiainen, Kevät/Chinkin, Christine (2015): »Legal implications of EU accession to the Istanbul Convention«. European Equality Law Network. https ://equalitylaw.eu/publications/thematic-reports [Zugriff: 28.6.2020].

Prasad, Nivedita (2011): Mit Recht gegen Gewalt. Die UN-Menschenrechte und ihre Bedeutung für die soziale Arbeit. Opladen, Farmington Hills: Barbara Budrich.

Rabe, Heike (2018): »Die Istanbul-Konvention – innerstaatliche Anwendung«, in: Feministische Rechtszeitschrift STREIT, Nr. 4, S. 147-153.

Rudolf, Beate (2012): »Diskriminierung wegen des Geschlechts ist mehr als Ungleichbehandlung. Potentiale der UN-Frauenrechtskonvention in der anwaltlichen Praxis«, in: Anwaltsblatt (AnwBl), Nr. 7, S. 599-601.

Rudolf, Beate/Chen, Felicitas (2014): »Die Bedeutung von CEDAW in Deutschland«, in: Hanna Beate Schöpp-Schilling/Rudolf, Beate/Gothe, Antje (Hg.), Mit Recht zur Gleichheit. Die Bedeutung des CEDAW-Ausschusses für die Verwirklichung der Menschenrechte von Frauen weltweit, Baden-Baden: Nomos, S. 25-70.

Rupp-von Brünneck, Wiltraut/Simon, Helmut (1975): Abweichende Meinung zum Urteil des Ersten Senats des Bundesverfassungsgerichts vom 25. Februar 1975 – 1 BvF 1, 2, 3, 4, 5, 6/74, BVerfGE 39, S. 68-95.

Uerpmann-Wittzack, Robert (2017): »Innerstaatliche Wirkung des Europaratsübereinkommens gegen Gewalt gegen Frauen«, in: Zeitschrift für das gesamte Familienrecht (FamRZ), Vol 63. Nr. 22, S. 1812-1814.

UN General Assembly (2013): »Promotion of the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms: protecting women human rights defenders«. A/RES/68/181. https://un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/181 [Zugriff: 28.6.2020].

UN Special Rapporteur on violence against women, its causes and consequences, Yakin Ertürk Special Rapporteur (2006): »The Due Diligence Standard as a Tool for the Elimination of Violence against Women«. E/CN.4/2006/61. https://ohchr.org/en/issues/women/srwomen/pages/srwomenindex.aspx [Zugriff: 28.6.2020].

UN Special Rapporteur on violence against women, its causes and consequences, Dubravka Šimonović (Special Rapporteur (2018): »Report on online violence against women and girls from a human rights perspective«. E/CN.4/2006/61. https://ohchr.org/en/issues/women/srwomen/pages/srwomenindex.aspx [Zugriff: 28.6.2020].

Wissenschaftliche Dienste des Deutschen Bundestages (2016): Hassrede (hate speech) und Holocaustleugnung in der menschenrechtlichen Spruchpraxis. WD 2 – 3000 – 055/15. Deutscher Bundestag. https://bundestag.de/resource/blob/485798/13870af2cbd422605e56121a9821a7f0/WD-2-055-15-pdf-data.pdf [Zugriff: 30.8.2020].

Working Group on the issue of discrimination against women in law and in practice (2013): Report of 19 April 2013. A/HRC/23/50. https://ohchr.org/Documents/Issues/Women/WG/A.HRC.23.50_English.pdf [Zugriff: 28.6.2020].

Rechtsprechungsverzeichnis

Bundesverfassungsgericht (BVerfG), Beschluss vom 30.01.2020, Az. 2 BvR 1005/18, https://bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2020/01/rk20200130_2bvr100518.html [Zugriff: 28.6.2020].

Bundesverfassungsgericht (BVerfG), Beschluss vom 29.01.2019, Az. 2 BvC 62/14, https://bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2019/01/cs20190129_2bvc006214.html [Zugriff: 28.6.2020].

Bundesverfassungsgericht (BVerfG), Urteil vom 25.02.1975, Az. 1 BvF 1, 2, 3, 4, 5, 6/74, Sammlung der Entscheidungen des Bundesverfassungsgerichts

(BVerfGE) 39, S. 1-68 (95), https://servat.unibe.ch/dfr/bv039001.html [Zugriff: 28.6.2020].

Europäischer Gerichtshof für Menschenrechte (EGMR), Urteil vom 09.09.2009, Nr. 33401/02 –Opuz v.Turkey. https://hudoc.echr.coe.int/ [Zugriff: 28.6.2020].

Europäischer Gerichtshof für Menschenrechte (EGMR), Urteil vom 28. 08.2013, Nr. 3564/11 – Eremia v. The Republic of Moldova. https://hudoc.echr.coe.int/ [Zugriff: 28.6.2020].

Europäischer Gerichtshof für Menschenrechte (EGMR), Urteil vom 28.06.2016, Nr. 63034/11 – Halime Kiliç v. Turkey. https://hudoc.echr.coe.int/ [Zugriff: 28.6.2020].

Europäischer Gerichtshof für Menschenrechte (EGMR), Urteil vom 04.11.2019, Nr. 41261/17 – Volodina v. Russia. https://hudoc.echr.coe.int/ [Zugriff: 28.6.2020].

Europäischer Gerichtshof für Menschenrechte (EGMR), Urteil vom 11. 02.2020, Nr. 56867/15 – Buturugă v. Rumänien. https://hudoc.echr.coe.int/ [Zugriff: 28.6.2020].

Oberlandesgericht (OLG) Hamburg, Beschluss vom 08.03.2018, 1 Ws 114-115/17. https://iww.de/quellenmaterial/id/201039 [Zugriff: 28.6.2020].

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].

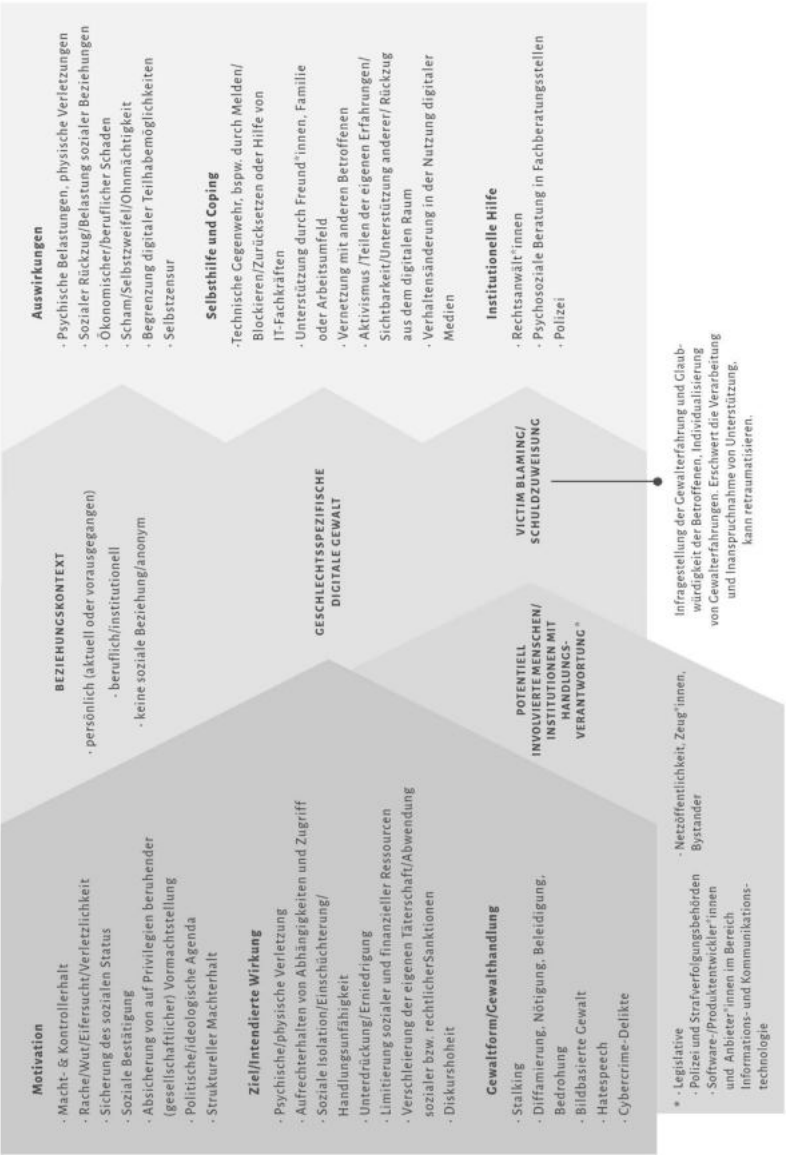
Hate Speech gegen feministische Positionen

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].

Spezifika geschlechtsspezifischer Gewalt im digitalen Raum

Funktionsprinzipien des Internets und ihre Risiken im Kontext digitaler geschlechtsspezifischer Gewalt

Jenny-Kerstin Bauer

Im Zuge der Verbreitung der Informations- und Kommunikationstechnologien in den letzten 20 Jahren sind das Internet sowie alle damit ausgestatteten Geräte wie Computer, Smartphones, Tablets, Spielekonsolen, SmartHome-Anwendungen etc. nicht mehr aus unserem Alltag wegzudenken. Rund 90 % der über 14-Jährigen der deutschen Bevölkerung nutzen das Internet zumindest gelegentlich. Laut einer Onlinestudie der Medienkommission[1] von ARD und ZDF aus dem Jahr 2019 beträgt die tägliche Nutzungsdauer des Internets drei Stunden und bei den unter 30-Jährigen ist die Zeitdauer mit sechs Stunden doppelt so lang. Das Verhältnis zwischen Frauen und Männern ist bezüglich der Internetnutzung für dieses Berichtsjahr ausgeglichen. Die Unterwegsnutzung des Internets ist in weiten Teilen der Bevölkerung auch 2019 auf konstant hohem Niveau mit steigender Tendenz nach oben. Bei den unter 50-Jährigen nutzen etwas über 90 % das Internet zumindest gelegentlich unterwegs, bei über 70-Jährigen ist es nur knapp jede dritte befragte Person. Trotzdem ist eine Steigerung vor allem bei 60- bis 69-Jährigen zu vermerken, während in den übrigen Altersgruppen nur geringfügige Schwankungen zu verzeichnen sind (vgl. ARD/ZDF-Medienkommission 2019). Damit wird deutlich, dass das Internet ein Medium ist, welches maßgeblich zur Kommunikation beiträgt und auch in Zukunft beitragen wird.

Die Entstehungsgeschichte des Internets, immer im Kontext des gesellschaftlichen Hintergrunds der entsprechenden Zeit betrachtet, bildet die Struktur und Besonderheit des Mediums über die Zeit aus. Seit den 1960er-Jahren, als eine zunächst militärische Erfindung mit einer strikten

1 Die Studie ist rein binär angelegt.

dezentralen Netzstruktur (vgl. Hörisch 2004: 386f.), über eine konträre freie universitäre Diskussions- und Austauschplattform ab den 1970er-Jahren (vgl. Castells 2005: 20ff.), bis hin zur internationalen Ausbreitung durch die Erfindung des World Wide Web durch Tim Berners-Lee und der bis heute anhaltenden Kommerzialisierung in den 1990er-Jahren (vgl. Barry u.a. 2012) war das Internet immer eng verbunden mit gesellschaftlichen Entwicklungen und wird aktuell u.a. anhand gesellschaftlich relevanter Themen wie Überwachung, Datenschutz und Privatsphäre diskutiert (vgl. Schütz/Karaboga 2018: 263f.; Ganz 2013: 4f.).

Aus der Entstehungsgeschichte können vier zunächst neutrale, jedoch gleichzeitig zentrale mediale Eigenschaften des Internets charakterisiert und deren jeweiliges Missbrauchspotential für geschlechtsspezifische digitale Gewalt herausgearbeitet werden. Diese sich gegenseitig verstärkenden Funktionsprinzipien sind das Fehlen von Hoheitsinstanzen, die Anonymität der Nutzer*innen, das Fehlen bzw. gering vorhandene Zutrittsbarrieren sowie die Verbreitungsgeschwindigkeit von Informationen. Ziel des folgenden Artikels ist es, ein System an medialen Eigenschaften des Internets darzustellen, um das Verständnis dafür zu erleichtern, wie digitale geschlechtsspezifische Gewaltformen im Internet möglich werden. Daran anschließend soll für jede der medialen Eigenschaften kurz beschrieben werden, warum sie für die Intensivierung von geschlechtsspezifischer digitaler Gewalt relevant ist.

Nach Winker u.a. (2004) waren in feministischen Diskursen große Hoffnungen an das Internet geknüpft. Es versprach einen geschlechtsneutralen Raum zu ermöglichen, in dem alle Personen unabhängig ihrer Genderidentität ungehindert Zugang zum Internet und der Netzkommunikation haben, ohne die Anwender*innen auf ihr soziales bzw. biologisches Geschlecht zu reduzieren oder Geschlecht überhaupt als notwendige Information zu erachten. In der Realität zeichnet sich der Technologiesektor aber durch ein (Macht-)Ungleichgewicht zwischen den Geschlechtern aus. Eine Zugangsneutralität und Gewaltfreiheit im Internet ist daher nur theoretisch gegeben, gesellschaftliche Macht- und Dominanzverhältnisse sind auch im Internet sehr wirksam. So haben auch im Netz cis-Männer eine Vormachtstellung (vgl. Köver 2018; Krempl 2020); andere, eher marginalisierte Perspektiven sind unterrepräsentiert oder finden weniger Gehör (vgl. European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs 2018: 25f.), so dass die geschaffenen Technologien und Online-Plattformen in ihrer Programmierung und Ausführung durchaus Vorurteile und Diskriminierung transportieren können. Wenn spezifische Nutzungsanforderungen und

Bedarfe marginalisierter Perspektiven nicht in die Entwicklung von Technologie einfließen, wird sie für Menschen außerhalb der impliziten Normen der Auftraggeber*innen und Entwickler*innen entweder nicht nutzbar sein, gegen sie verwendet werden oder sie zumindest unsichtbar machen und gegenüber anderen Nutzer*innen benachteiligen. Dies wird z.B. deutlich, wenn Maschinen und künstliche Intelligenz Stereotype reproduzieren, die lebensbedrohliche Auswirkungen haben können. Dies ist z.B. der Fall wenn Gesichtserkennungssysteme, die von der US-amerikanischen Polizei zur Identifizierung von Menschen verwendet werden, eine massive Verwechselungsrate bei den Gesichtern von Schwarzen Menschen aufweisen[2], weil sie auf einer imaginierten weißen Norm basieren.

Fehlen einer Hoheitsinstanz

Die erste zentrale Eigenschaft des Internets ist das Fehlen einer Hoheitsinstanz. Die technische Koordination/Bereitstellung und Entwicklung des Internets ist zwar weitgehend durch Regierungs- und Nicht-Regierungs-Organisationen geregelt, jedoch fehlt bei der Kontrolle der Nutzung fast zur Gänze eine globale Regelung der Zuständigkeiten und Kompetenzen (vgl. DeNardis 2010: 2ff.). Polizeibeamt*innen als Ansprechpartner*innen für Betroffene haben selten Schulungen zur Problematik der digitalen Gewalt. Es mangelt an Wissen über die Schwere der Angriffe und Kenntnisse der Technologien, mit denen sie durchgeführt werden sowie eigene schlechte technische Ausstattungen der Polizeibehörden, um die digitalen Angriffe verfolgen zu können. Dies ist für den Bereich der Gewalt im digitalen Raum besonders fatal.

Obwohl besonders von staatlicher Seite, z.B. durch das Vorantreiben eines Internetrechts intensive Bemühungen unternommen werden, dieses Manko zu beheben, ist die Entwicklung eines Regelwerks sowie insbesondere

2 Eine Studie aus dem Jahr 2018 stellte bei der Prüfung einiger dieser Software-Systeme fest, dass sie Schwarze Frauen in fast 35 % der Fälle falsch klassifizierten, während weiße Männer fast immer richtig identifiziert wurden. Auch in der Medizin können sogenannte racial und gender bias lebensgefährlich sein. Zu Beginn der weltweiten Corona-Pandemie 2020 gingen etwa Videos von elektronischen Desinfektionsspendern in Krankenhäusern viral, deren Sensoren lediglich auf helle Flächen reagierten und es Schwarzen Menschen und People of Color unmöglich machten, sich kontaktfrei die Hände zu desinfizieren.

dessen Umsetzung äußerst schwierig und funktioniert in vielen Bereichen nur langwierig und mangelhaft (vgl. Ludes 2003: 145). Insgesamt sind bisher auch die vorhandenen staatlichen Strafverfolgungsbehörden den Herausforderungen des neuartigen, hochkomplexen Mediums Internet in Verbindung mit geschlechtsspezifischer digitaler Gewalt noch nicht gerecht geworden. Erschwerend kommt hier hinzu, dass geschlechtsspezifische digitale Gewalt oft sehr unterschiedlich in bestehenden Gesetzen eingeordnet ist und Gesetze zur Ahndung geschlechtsspezifischer Gewalt digitale Gewaltformen nur ungenügend berücksichtigen. Die Anwendung gängiger Gesetze auf explizit geschlechtsspezifische digitale Gewalt gestaltet sich zudem in der Praxis schwierig. Selbst wenn die Tatbestände tatsächlich erfüllt sind, ist die Ahndung bei Gewalt im Internet oft äußerst kompliziert (vgl. Mathiesen 2014: 5f., 35). Somit werden durch das Fehlen einer eindeutigen rechtlich bestimmbaren Hoheitsinstanz im Internet Täter*innen oft nicht angemessen juristisch zur Rechenschaft gezogen.[3]

Anonymität der Nutzer*innen

Die zweite mediale Eigenschaft des Internets, die für die Auseinandersetzung mit dem Thema digitaler Gewalt im sozialen Nahraum einen sehr hohen Stellenwert hat, ist die inhärente Anonymität der Nutzer*innen im Internet. Grundsätzlich ist es – mit entsprechendem Know-how technisch möglich, z.B. über die IP-Adresse, Geräte und Netzzugänge zu identifizieren, von denen aus im Internet gesurft wird. Jedoch ist es mit einfachsten Mitteln und auch ohne besonderes technisches Wissen möglich, dieses System zu umgehen und sich anonym im Internet zu bewegen (vgl. Stroud/Cox 2018: 291; Mathiesen 2014: 28f.). Webseiten können besucht, Inhalte geteilt, Kommentare verfasst, sogar ganze Homepages online gestellt werden, ohne dass die dahinterstehende Person über den Zugang des Gerätes im Internet identifiziert werden kann.

Für die Eindämmung geschlechtsspezifischer digitaler Gewalt ist die Anonymität der Nutzer*innen aus zwei Gründen besonders relevant. Einerseits wird eine Identifikation von Täter*innen durch die Anonymität naheliegen-

3 Siehe Beitrag: Möglichkeiten und Grenzen strafrechtlicher Interventionen bei digitaler Gewalt.

derweise erschwert bis verunmöglicht,[4] was wiederum die oben erwähnte Anwendung von Gesetzen und Strafverfolgung zusätzlich erschwert. Darüber hinaus kann die Anonymität durch den »Online Disinhibition Effect« auch direkt geschlechtsspezifische digitale Gewalt im Internet begünstigen. Dieses von Suler (2004) beschriebene Prinzip sagt aus, dass die Anonymität gekoppelt mit der distanzierten Kommunikationssituation zu einem Vernachlässigen oder vollständigen Aufgeben sozialer Regeln und Einschränkungen im Internet bis hin zu Enthemmung führen kann. Dadurch wird sozial unerwünschtes, unmoralisches, unethisches oder illegales Verhalten begünstigt. In Bezug auf geschlechtsspezifische digitale Gewalt bedeutet dies, dass das Anonymitätsprinzip im Internet die Hemmschwelle für das Ausüben von Gewalt senken kann, während es gleichzeitig die Verfolgung der Täter*innen deutlich erschweren kann.

Bezüglich der Anonymität von Nutzer*innen im Internet und Verschlüsselung von Informationen, bestehen insbesondere staatliche Bestrebungen zur Änderung und Überwachung (vgl. Gieseler 2013: 62f., 71; Krempl 2015). Diese stoßen aber regelmäßig auf großen Widerstand, etwa bei Vertreter*innen von (digitalen) Menschenrechten, netzpolitischen Initiativen und Expert*innen oder in Form von politischem Online-Aktivismus mit Thematisierung von Diskriminierungserfahrungen (vgl. Feminist In Internet 2020). Die Bewegungsfreiheit und potentielle Anonymität im Internet[5] wird als massiv bedroht angesehen, weil einzelne Staaten u.a. Gesetze einführen wollen oder bereits anwenden, die staatliche Überwachung und Eingriffe in die Privatsphäre ermöglichen. Dies geschieht häufig mit der Begründung, die Sicherheit der Bevölkerung zu erhöhen, Strafverfolgung zu erleichtern oder

4 Ob das Internet tatsächlich anonym genutzt werden kann, wird von vielen Seiten angezweifelt (vgl. Lobo 2015). Gleichzeitig ist jedoch das Ermitteln einer Person, welche anonymisierende Hilfsmittel nutzt, um sich im Internet zu bewegen, mit großem Aufwand verbunden und wird nur in Ausnahmefällen wie z.B. bei schwerwiegenden Straftaten vorgenommen. Für die Ermittlung von geschlechtsspezifischer digitaler Gewalt ist dies in den seltensten Fällen gegeben, weshalb auch die Anonymität der Täter*innen gewahrt werden kann. Für den vorliegenden Artikel wird darum davon ausgegangen, dass ein*e Internetnutzer*in anonym agieren kann.

5 Auf der Plattform für digitale Freiheitsrechte »netzpolitik.org« erscheinen fast täglich Meldungen und Recherchen darüber, wie staatliche Institutionen weltweit die Rechte von Internetnutzer*innen einschränken und gesetzliche Maßnahmen zur Überwachung diskutieren. Auch die Entwicklung der Diskussionen in Deutschland lässt sich unter dem Schlagwort »Überwachung« sehr gut nachvollziehen.

gegen Hate Speech und Fake News vorzugehen, so z.B. aktuell in Brasilien (vgl. Reuter 2020) oder in Deutschland, wo die Regierung immer wieder versucht die Vorratsdatenspeicherung einzuführen, zuletzt als Teil der Reform des Telekommunikationsgesetzes. Für viele Aktivist*innen, Forscher*innen und Journalist*innen, die sich für Menschenrechte einsetzen, kann ein Mangel an Anonymität und Verschlüsselung zur Enthüllung von privaten Informationen und Gewalt führen, manchmal zu direkten Bedrohungen – nicht nur für sich selbst, sondern auch für die schutzbedürftigen Gruppen, für die sie sich einsetzen (vgl. European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs 2018: 26f.).

Fehlen bzw. die deutliche Senkung von Zutrittsbarrieren

Die dritte mediale Eigenschaft des Internets ist das Fehlen bzw. die deutliche Senkung von Zutrittsbarrieren. Dies gilt sowohl für die Sender- sowie die Empfängerperspektive. So ist einerseits der Zugang zum Internet mittlerweile in vielen Teilen der Welt für einen Großteil der Menschen selbstverständlich und erschwinglich geworden, da sich die Kosten stark reduziert haben. So sind heute 9 von 10 Haushalten in Deutschland online (vgl. Eurostat 2020). Der dadurch ermöglichte Zugriff auf Informationen ist grundsätzlich unbegrenzt und der Zugriff darauf kann auch nicht gesteuert werden (vgl. Meurer 2003: 24; Münker 2009: 83; Liebsch 2011: 88). Darüber hinaus ermöglichen die Strukturen des Web 2.0 (Social Media) auch auf einfachste Weise das Bereitstellen von Inhalten. Jeder Mensch kann als Medienproduzent*in auftreten und Informationen öffentlich zugänglich machen (vgl. Meurer 2004: 24f.). Parallel zur wachsenden Verfügbarkeit, z.B. von Smartphones und der Zugänglichkeit zum Internet, steigen auch die Missbrauchsmuster dieser Systeme (vgl. Gámez-Guardix/Borrajo/Calvete 2018).

Wird dieser sehr niederschwellige Medienzugang gerade in Nutzer*innenkreisen häufig als »Demokratisierung von Information« zelebriert (vgl. OnlineAktivisten 2011), birgt er auch spezifische Risiken, da die Kontrolle der veröffentlichten Inhalte massiv erschwert wird – die klassische Gatekeeperfunktion (Filter- und Kontrollfunktion) der Medienschaffenden entfällt. Dadurch ist die Gefahr der Publikation unrechtmäßiger Inhalte auch deutlich erhöht; beispielsweise wenn diese die Persönlichkeitsrechte von Anderen verletzen, diskriminierend und/oder schlichtweg illegal sind (z.B. gewaltverherrlichend, rassistisch oder dokumentierte Missbrauchsdarstellungen von Min-

derjährigen beinhalten). Diese können durch den einfachen Zugang zum Internet eine enorme öffentliche Aufmerksamkeit erreichen. Dies birgt auch großes Potential, um geschlechtsspezifische digitale Gewalt im Internet zu begünstigen, da beispielsweise private oder schädliche Informationen öffentlich zugänglich gemacht werden können.

Verbreitungsgeschwindigkeit von Informationen

Die vierte mediale Eigenschaft des Internets ist die Verbreitungsgeschwindigkeit von Informationen. Wie bei keinem anderen Medium ist es durch das Internet möglich Texte, Bilder, Audio- oder Videoinhalte in Echtzeit von einem beliebigen Punkt im Netz zu potentiell jedem anderen Punkt im Netz zu übermitteln. Dies ist einerseits begründet in der Übertragungsgeschwindigkeit des Mediums: Wie bei allen elektronischen Medien entsteht (im Gegensatz zu gedruckten Medien) keine Verzögerung durch die Übermittlung des Inhalts (vgl. Hörisch 2004: 331ff.). Zusätzlich kommt hier auch die dichte Vernetzung der Internetnutzer*innen zum Tragen; insbesondere durch Social Media steht heute ein Großteil der Nutzer*innen mit zahlreichen Freund*innen, Kolleg*innen, Bekannten und Unbekannten in Verbindung, mit denen Informationen per Klick international geteilt werden können. Dadurch erfahren Informationen innerhalb kürzester Zeit eine so starke Verbreitung wie noch nie zuvor in unserer Geschichte (vgl. Keller 2013; vgl. Parliament's Policy Department for Citizens' Rights and Constitutional Affairs 2018: 27f.).

Das Missbrauchsrisiko dieses Faktors in Bezug auf geschlechtsspezifische digitale Gewalt ist enorm. Ähnlich des niedrigschwelligen Zugangs zum Internet wird die Verbreitungsgeschwindigkeit von digitalen Informationen häufig gelobt, kann jedoch im gleichen Zuge auch negative Konsequenzen haben, wenn z.B. gewalttätige Inhalte im Internet geteilt werden. Denn die Reaktion auf die Veröffentlichung kann in aller Regel erst zu einem Zeitpunkt erfolgen, zu dem diese Inhalte bereits unüberschaubar weit verbreitet sind. Eine Verbreitung zu unterbinden ist dann kaum noch möglich. Lädt etwa ein Gewalttäter Nacktfotos seiner/ihrer Ex-Freundin in einem sozialen Netzwerk hoch und teilt sie mit seinen Freund*innen, so werden diese Bilder bereits hundertfach gesehen, gespeichert und weiterverbreitet worden sein, bis die betroffene Frau überhaupt darauf aufmerksam wird. Bis zur rechtskräftigen Verpflichtung des Täters diese Information zu löschen, vergeht nochmal mehr Zeit, die für Betroffene sehr belastend ist.

Neben dem Verbreiten von Bildern etc. im Netz stellen Live-Streams ein großes Problem dar; es ist davon auszugehen, dass diese Nachfrage nach Echtzeitinhalten im Internet steigen wird (vgl. Katsh/Rabinovich-Einy 2017). So können Live-Streaming-Inhalte wie z.B. voyeuristische, heimliche Filmaufnahmen oder gefilmte Vergewaltigungen durch das Hochladen auf pornografische Plattformen in Realzeit übermittelt werden und einer noch breiteren Masse zugänglich gemacht werden.

Abb. 3: Gewaltbegünstigende Funktionsprinzipien des Internets bei geschlechtsspezifischer digitaler Gewalt, Bauer 2020.

Diese Grafik verdeutlicht, wie die vier Funktionsprinzipien des Internets bei digitaler geschlechtsspezifischer Gewalt zusammenwirken. In ihrer Gesamtheit und in diesem Zusammenwirken bilden sie einen Faktor, der geschlechtsspezifische digitale Gewalt begünstigen kann. Das Medium Internet ist an sich nicht genuin gewalttätig, es bietet aber gewaltbereiten Personen Möglichkeiten diese Funktionsprinzipien auszunutzen, um z.B. anderen Personen zu schaden oder Macht über sie auszuüben. Das Internet kann so Teil einer Täterstrategie werden, wenn es zu einem bevorzugten Medium der Macht- und Gewaltausübung wird. Durch das Fehlen einer Hoheitsinstanz agieren Täter*innen im vermeintlich rechtsfreien Raum, in dem die Zuständigkeit bei Rechtsverletzungen zusätzlich oft uneindeutig ist. Die fehlende Sensibilisierung der Strafverfolgungsbehörden und fehlende bzw. nicht ausreichende Gesetze zur Ahndung führen demnach nicht zwingend zu rechtlichen Konsequenzen für Täter*innen. Im Gegenteil fühlen sich diese oft sicher in der Anonymität des Internets. Die Anonymität erschwert die Strafverfolgung zusätzlich.

Gleichzeitig sind Zutrittsbarrieren für das Agieren im Internet gering. Die Nutzung des Internets ist sehr niederschwellig. Jede teilnehmende Person kann Informationen publizieren und diese einer großen Netzöffentlichkeit zugänglich machen. Zudem erhöht sich die Gefahr, dass Dritte die schädlichen oder gewaltvollen Inhalte unbedacht rezipieren und zu einer Weiterverbreitung beitragen. Für Gewalttäter*innen bietet das Internet so einen leicht zugänglichen Raum, in dem Informationen zum Schaden von Betroffenen publiziert werden können, während Täter*innen in der Anonymität verbleiben. Private Daten können in einer enormen Geschwindigkeit geteilt oder abfotografiert werden, so dass die Streuung einer Information im Internet kaum beeinflusst werden kann. Hier kommt das vierte Funktionsprinzip zum Tragen. Die enorme Verbreitungsgeschwindigkeit von Informationen zusammen mit nicht vorhandenen schnellen Löschoptionen auf Online-Plattformen und in Messengerdiensten verstärken und begünstigen geschlechtsspezifische digitale Gewalt.

Bei jeder Betrachtung der Potentiale des Internets, die die geschlechtsspezifische digitale Gewalt begünstigen, ist jedoch unabdingbar zu beachten, dass die Funktionsprinzipien sich nicht ausschließlich negativ auswirken müssen. Sie können ebenfalls Bedingung für Gegenwehr, Hilfe und Solidarität bei geschlechtsspezifischer digitaler Gewalt ermöglichen. Für Frauen und andere diskriminierte Personengruppen ist das Internet ein wichtiger Ort, um sich auszutauschen, sich zu organisieren und sich zu unterstützen. Die

angeführten medialen Funktionsprinzipien des Internets sind daher nicht einseitig abzulehnen, denn gleichzeitig sind sie in anderen Zusammenhängen für den Schutz von Freiheits- und Menschenrechten relevant. Sie können auch Menschen schützen, die Diskriminierung erfahren und ermöglichen ihnen die Teilhabe im Internet und damit an der Gesellschaft.

Das Internet und die Entwicklung von Informations- und Kommunikationstechnologien sind nicht losgelöst von gesellschaftlichen Verhältnissen zu bewerten. Handlungsbedarf besteht dabei auf verschiedenen Ebenen. Zum Beispiel können auf der individuellen Ebene Kompetenzen von Betroffenen im Umgang mit dem Internet, Informations- und Kommunikationstechnologien gestärkt werden. Um dies zu ermöglichen, bedarf es dann auch der Strukturen und finanziellen Ressourcen in Beratungs- und Präventionseinrichtungen. Als Gegenwehr gegen Täter*innen sollten auch rechtliche Interventionsmöglichkeiten in Gesetzen in Bezug auf digitale Gewalt und die Sensibilisierung für diese Gewaltform in den staatlichen Strafverfolgungsbehörden stark verbessert werden.

Die Verantwortung für den Umgang mit dem Internet, das in seiner Funktionsbreite sowohl Gefahren als auch Chancen bietet, liegt letztlich auf gesellschaftlicher Ebene. Für einen gleichberechtigten und diskriminierungsarmen Umgang mit dem Medium Internet bräuchte es einen queer-feministischen und intersektionalen Diskurs. Unterschiedliche Perspektiven mit einem Fokus auf dem Schutz von Betroffenen sind notwendig, um Konflikte zu benennen und zu intervenieren (vgl. Ganz 2013: 5; Köver 2018). Dies ist eine gesamtgesellschaftliche Aufgabe.

Literatur

ARD/ZDF-Medienkommission (Hg.) (2019): »ARD und ZDF Onlinestudie«. https://ard-zdf-onlinestudie.de [Zugriff: 14.1.2019].

Castells, Manuel (2002): »Frauen in der Netzwerkgesellschaft: Fragen an den Feminismus«, in: Heinrich-Böll-Stiftung und Feminist_spaces (Hg.), Frauen im Netz. Diskurse. Communities. Visionen. Berlin: Ulrike Helmer Verlag, S. 147-160.

DeNardis, Laura (2010): The Emerging Field of Internet Governance. Yale: Yale Information Society Project Working Paper Series.

European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs (2018): Cyber Violence and Hate Speech Online Against

Women. Women's Rights @ Gender Equality. Brüssel: Europäische Union.

Eurostat (2020): »Haushalte – Internet-Zugangsdichte«. https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_ci_in_h&lang=de [Zugriff: 15.4.2020].

Feminist Principle of the Internet (2020): »https://feministinternet.org«. https://feministinternet.org/en/principle/anonymity [Zugriff:13.5.2020].

Gámez-Guadix, Manuel/Borrajo, Erika/Calvete, Esther (2018): »Partner Abuse, Control and Violence Through Internet and Smartphones: Characteristics, Evaluation and Prevention«, in: Papeles Del Psicólogo – Psychologist Papers, Vol. 38 Nr. 3, S. 218-227.

Ganz, Kathrin (2013): »Feministische Netzpolitik: Perspektiven und Handlungsfelder«. Heinrich-Böll-Stiftung und Gunda-Werner-Institut (Hg.). https://nbn-resolving.org/urn:nbn:de:0168-ssoar-59852-5 [Zugriff: 19.5.2020].

Gieseler, Christoph (2013): »Klarnamenpflicht vs. Anonymität im Internet: Das Grundrecht auf Nichtidentifizierung«, in: Emmer, Martin/Filipović, Alexander/Schmidt, Jan-Hinrik/Stapf, Ingrid (Hg.), Echtheit, Wahrheit, Ehrlichkeit. Authentizität in der Online-Kommunikation. Weinheim und Basel: Beltz Juventa, S. 67-73.

Hörisch, Jochen (2004): Eine Geschichte der Medien. Vom Urknall zum Internet. Frankfurt am Main: Suhrkamp.

Katsh, Ethan/Rabinovich-Einy, Orna (2017): Digital Justice: Technology and the Internet of Disputes. New York: Oxford University Press.

Keller, Maura (2013): »Social Media and Interpersonal Communication«, in: Social Work Today, Vol. 13 Nr. 3, S. 10.

Köver, Chris. (2018): »Weltwirtschaftsforum: Künstliche Intelligenz ist zu männlich«. https://netzpolitik.org/2018/weltwirtschaftsforum-kuenstliche-intelligenz-ist-zu-maennlich/ [Zugriff: 15.7.2020].

Krempl, Stefan (2015): »Urheberkonferenz: »Heilige Kuh der Anonymität gehört geschlachtet«. https://heise.de/newsticker/meldung/Urheberkonferenz-Heilige-Kuh-der-Anonymitaet-gehoert-geschlachtet-3029833.html [Zugriff: 1.6.2020].

Krempl, Stefan (2020): »Digital Gender Gap: Frauen schneiden bei Digitalisierung schlechter ab als Männer«. https://heise.de/newsticker/meldung/Digital-Gender-Gap-Frauen-schneiden-bei-Digitalisierung-schlechter-ab-als-Maenner-4628228.html [Zugriff: 25.5.2020].

Liebsch, Burkhard (2011): »Medien – Ethik – Gewalt, Neue Perspektiven«, in: Grimm, Petra/Badura, Heinrich (Hg.) Medien – Ethik – Gewalt, Neue Perspektiven. Stuttgart: Franz Steiner Verlag, S. 77-92.

Lobo, Sascha (2015): »Keine Anonymität ist auch keine Lösung«. https://faz.net/aktuell/feuilleton/medien/klarnamen-im-netz-keine-anonymitaet-ist-auch-keine-loesung-13381486.html [Zugriff 8.4.2020].

Ludes, Peter (2003): Einführung in die Medienwissenschaft. Entwicklungen und Theorien. 2. überarbeitete Auflage. Berlin: Erich Schmidt Verlag GmbH & Co.

Mathiesen, Asbjørn (2014): »Cybermobbing und Cybergrooming. Neue Kriminalitätsphänomene im Zeitalter moderner Medien«. Jahrbuch des Kriminalwissenschaftlichen Instituts der Leibniz. Universität Hannover.

Meurer, Dirk (2004): Politische Öffentlichkeit im Internet. Eine Analyse der Verlinkungsstrukturen politischer Angebote im World Wide Web. Institut für Publizistik- und Kommunikationswissenschaft. Berlin: Freie Universität Berlin.

Münker, Stefan (2009): Emergenz digitaler Öffentlichkeit. Die Sozialen Medien des Web 2.0. Frankfurt am Main: Suhrkamp.

OnlineAktivisten (2011): »BundestagTV, Peter Kruse – Revolutionäre Netze durch kollektive Bewegungen«. https://youtube.com/watch?v=e_94-CH6h-0 [Zugriff: 6.2.2020].

Reuter, Markus (2020): »Brasilien. Das »schlechteste Internetgesetz der Welt« steht zur Abstimmung (Update)«. https://netzpolitik.org/2020/das-schlechteste-internetgesetz-der-welt-steht-zur-abstimmung/ [Zugriff: 1.7.2020].

Schütz, Philip/Karaboga, Murat (2018): »Datenschutz im Internet: Akteure, Regulierungspraktiken und Interessenlagen«, in: Busch, A./Breindl, Y./Jakobi, T. (Hg.), Netzpolitik. Ein einführender Überblick. Wiesbaden: Springer VS, S. 263-301.

Stroud, Scott R./Cox, William (2018): »The Varieties of Feminist Counterspeech in the Misogynistic Online World«, in: Vickery, Ryan Jacqueline/Everbach, Tracy (Hg.), Mediating Misogyny. Gender, Technology and Harassment. New York: Palgrave Macmillan, S. 293-332.

Suler, John (2004): »The Online Disinhibition Effect«, in: CyberPsychology & Behavior, Vol. 7 Nr 3, S. 321-326.

Winker, Gabriele/Drüeke, Ricarda/Sude, Kerstin (2004): »Neue Öffentlichkeit durch frauenpolitsche Netze im Internet?«, in: Kahlert, Heike/Kajatin, Claudia (Hg.), Arbeit und Vernetzung im Informationszeitalter.

Wie neue Technologien die Geschlächterverhältnisse verändern. Frankfurt/New York: Campus Verlag, S. 239-258.

Intersektionale Machtverhältnisse im Internet

Jasna Strick und Anne Wizorek

»Ain't I a Woman?« (dt. Bin ich denn keine Frau?) – mit dieser provokanten Frage wies die afroamerikanische Frauenrechtlerin Sojourner Truth 1851 darauf hin, wie Sexismus und Rassismus miteinander verknüpft sind. Sie war als ehemalige Sklavin nicht nur rassistischer Diskriminierung, sondern als Frau genauso Sexismus ausgesetzt. Diese Form der verwobenen Diskriminierung wurde von der Frauenbewegung wenig beachtet, da diese sich vorwiegend um die Probleme weißer mittelständischer Frauen kümmerte. Sojourner Truth war eine der Personen, die wie viele andere Schwarze Frauen und/oder Frauen mit Behinderungen und/oder klassistisch benachteiligte Frauen das benannten, was später unter dem Begriff »Intersektionalität« festgehalten wurde. Das Intersektionalitätskonzept wurde schließlich 1989 von der Schwarzen amerikanischen Juristin Kimberlé Crenshaw eingeführt, um vielfache Ungleichheits- und Unterdrückungsverhältnisse zu analysieren. Statt sie nur einzeln zu betrachten, sind Strukturkategorien wie Geschlecht, Ethnie, Klasse, Sexualität oder Behinderung aus intersektionaler Perspektive miteinander verwoben und stehen in Wechselwirkung zueinander (vgl. Crenshaw 1989). Intersektionale Realitäten erhielten hierdurch eine Terminologie, die Eingang in akademische Diskurse fand.

Vision des Internets vs. Realitäten heute[1]

Nur vier Jahre nachdem die Bedeutung und das Zusammenwirken von Identitätskategorien mit dem Intersektionalitätsbegriff bezeichnet wurden, scheinen sie auch schon wieder vor ihrer Auflösung zu stehen, denn: »On the in-

1 Die Ausführungen in diesem Text beziehen sich auf die Diskussionslage mit Stand Frühjahr 2020.

ternet, nobody knows you're a dog« (dt. Im Internet weiß niemand, ob du ein Hund bist). Dieser heute geradezu ikonische Satz steht 1993 auf einer Zeichnung des Karikaturisten Peter Steiner. Das Bild ist im Magazin New Yorker (vgl. Holland 2018) abgedruckt und zeigt einen Hund, der am Schreibtisch vor einem Computer sitzt. Mit einer Pfote auf der Tastatur schaut er zu einem zweiten Hund herunter und spricht seine mittlerweile berühmte Behauptung aus. Dahinter steckt natürlich die Vorstellung, im Internet jemand ganz anderes sein zu können als im Alltag. Es ist eine Vorstellung, die Freiheit verspricht, eine Utopie, laut der wir im Netz jederzeit frei wählen, ob und wie unser Geschlecht, unsere Sexualität oder unsere Herkunft überhaupt thematisiert werden und auch unser Aussehen spielt keinerlei Rolle mehr.

So sah die Vision vom Internet zu Beginn des Web 2.0 aus. Inzwischen sind die Grenzen zwischen online und real life längst verschwommen. Beide Sphären lassen sich nicht mehr voneinander trennen. Ganz im Gegenteil: Für viele ist das Internet inzwischen gleichbedeutend mit sozialen Medien geworden. Wir teilen Ereignisse aus unserem Privatleben auf Instagram, Facebook oder Twitter, inszenieren unsere berufliche Persönlichkeit bei LinkedIn und versuchen uns auf Tinder für mögliche Partner*innen möglichst attraktiv darzustellen. Wir sind keine geschlechts- und gesichtslosen Cyborgs (mehr). Selbst wenn wir davon ausgehen, dass einige Inhalte geschönt sind und nicht eins-zu-eins das Leben einer Person wiedergeben, ist heute die Person hinter dem Account in den Fokus gerückt. Und mit ihr die gesellschaftliche Positionierung der Person. Im Internet ist eben keineswegs egal, wer du bist.

Aber war es überhaupt jemals egal, wer sich hinter einer Netzpersona verbirgt? In Zeiten, in denen vor allem weiße Jungs und junge Männer aus der Mittelschicht mit dem nötigen Kleingeld für einen eigenen Computer ausgestattet und mit dem Internet groß wurden, mochte das vielleicht stimmen. Heute sind weltweit aber so viele Menschen online wie nie und auch im Internet gilt, was wir bereits von der zweiten europäischen Frauenbewegung wissen: Das Private ist politisch. Als Social Media-Nutzer*innen bringen wir unsere eigenen Geschichten mit und für viele von uns ist das Internet zu einem Ort geworden, an dem wir überhaupt zum ersten Mal erfahren, dass unsere Erfahrungen Gewicht haben. Als Menschen mit Diskriminierungserfahrungen wird uns oft abgesprochen, dass die Gewalt, die uns tagtäglich widerfährt, real ist und Bedeutung hat. Aus dem Teilen unserer Erlebnisse und dem Vernetzen mit anderen Gleichgesinnten ziehen wir jedoch Kraft, um für ein selbstbestimmtes Leben einzustehen (Empowerment). Was von Internetkritiker*innen gerne abfällig als bloße Selbstdarstellung abgewertet

wird, kann also für viele Menschen heilsam wie bestärkend sein und gehört heutzutage ganz selbstverständlich zum politischen Aktivismus dazu.

Hashtag-Kampagnen: Geeignetes Mittel gegen intersektionale Diskriminierungen?

Online haben sich vor allem Hashtag-Kampagnen innerhalb des letzten Jahrzehnts als aktivistisches Werkzeug bewiesen, das große Aufmerksamkeit und Wirkung erzielen kann. Unter dem mit einer Raute versehenen Schlagwort werden so Diskriminierungs- und Gewalterfahrungen unterschiedlicher Social Media-Nutzer*innen gesammelt und sichtbar gemacht. Diese sprichwörtliche Verlinkung miteinander zeigt, dass es sich um kollektive Erfahrungen statt um singuläre Ereignisse handelt. Äußern sich Diskriminierungsbetroffene sonst, wird ihnen das Narrativ vom bloßen Einzelfall entgegengehalten. Das Erlebte klein- und wegreden zu wollen, wird wiederum Teil ihrer Diskriminierungserfahrung. Im Netz wird dieses Narrativ aufgebrochen und die Vielzahl der Beiträge unter einem Hashtag verdeutlicht die strukturelle Komponente einer Ungerechtigkeit. Das legt den Grundstein für vertiefende gesellschaftliche Verhandlungen und Veränderungen (vgl. Drüeke/Klaus 2014: 64).

Im deutschsprachigen Raum wurden Hashtag-Kampagnen und die Verwendung von Hashtags für aktivistische Zwecke vor allem durch die #Aufschrei-Debatte ab Januar 2013 bekannter. Die Beiträge auf Twitter handelten von Sexismus und sexualisierter Gewalt aus Sicht der Betroffenen. Erstmals wurde damit in Deutschland anlässlich eines Hashtags über gesamtgesellschaftliche Probleme diskutiert. Diese neu gewonnene Aufmerksamkeit inspirierte auch andere Hashtags wie #QueerAufschrei zu Queerfeindlichkeit oder #Schauhin, um Alltagsrassismus sichtbar zu machen. Eine Dynamik, die sich fast genauso wieder beobachten ließ, als 2017 der Hashtag #MeToo aufkam und sexualisierte Gewalt weltweit in bisher unbekanntem Ausmaß thematisieren konnte. In Deutschland entstanden kurz darauf #MeTwo (Alltagsrassismus) und #MeQueer (Queerfeindlichkeit) und wurden insgesamt schon viel breiter rezipiert als die Hashtags aus dem Jahr 2013, woran deutlich wird, dass hierzu bereits ein größeres Problembewusstsein geschaffen werden konnte.

Diese Sensibilisierung ist ein wichtiger Effekt von Hashtag-Kampagnen. Nicht-Betroffene können – im Idealfall – mit Hilfe der Erfahrungsberichte

Betroffener aufgeklärt werden, ihr diskriminierendes oder übergriffiges Verhalten ändern und sich für strukturelle Veränderungen einsetzen. Die Berichte machen greifbar, was als Zahl in einer Statistik oft zu unfassbar und abstrakt bleibt. Betroffene werden dagegen empowert, offen über ihre Erfahrungen zu sprechen, die damit verbundene Scham abzulegen und finden Halt in der (Online-)Gemeinschaft. Besonders deutlich zeigt sich das Zusammenwirken von Online- und Offline-Räumen darin, dass Beratungsstellen immer wieder berichten, im Rahmen der breiten öffentlichen Debatten um Hashtags vermehrt Anfragen von Betroffenen zu erhalten (vgl. Salzburger 2014: o.S.).

Social Media kann also die Initialzündung bringen. Doch die klassischen Medien haben, zumindest im deutschsprachigen Raum, immer noch eine wichtige Multiplikationsfunktion, wenn es darum geht, Hashtag-Kampagnen aufzugreifen. Neben der medialen Reichweite zeigen sich hier ebenso die Grenzen der Berichterstattung, denn darin bleibt nur selten Platz für kollektive Entstehungsgeschichten oder mehrdimensionale Inhalte, wie es einer intersektionalen Analyse entsprechen würde.

Klassische Medien verkürzen und vereinfachen in der Regel die Komplexität unserer gesellschaftlichen Verhältnisse (vgl. Drüeke/Klaus 2014: 65). Einerseits, weil sie müssen, da das Vorwissen beim Publikum nicht zwingend gegeben ist und die Sendezeit zu knapp ist. Andererseits liegt die Vermutung nahe, dass der Wille zur Komplexität nicht vorhanden ist und vielen Journalist*innen selbst das nötige Wissen um strukturelle Diskriminierungen fehlt, sodass häufig Stereotype reproduziert werden. In der Berichterstattung über digitale Gewalt schlägt sich das zum Beispiel darin nieder, eher über bereits bekanntere bis prominente Betroffene zu sprechen, statt die Erfahrungen marginalisierter Menschen in den Fokus zu rücken. Das Bild davon, wer als ›gutes Opfer‹ gilt und in solch einer Debatte beteiligt sein darf, wem geglaubt wird und wem wiederum die Expertise abgesprochen wird, ist immer noch von Stereotypen rund um den Opferbegriff geprägt. Das Verständnis von einem ›idealen Opfer‹, das schutzbedürftig, hilflos und dem Täter unterlegen ist, ist grundlegend für die Identifizierungsfähigkeit mit diesem (vgl. Christie 1986: 17ff.). Menschen, die beispielsweise arm, behindert, of Color und/oder nicht cis-/hetero sind, also marginalisiert werden, entsprechen diesem Verständnis nicht.

Der tatsächlichen Vielfalt der Beiträge innerhalb einer Hashtag-Kampagne wird somit kaum Rechnung getragen. Darüber hinaus sind Hinweise zur sensiblen Berichterstattung, zum Beispiel über Betroffene sexualisierter Gewalt, bisher kaum Bestandteil der journalistischen Ausbildung. An anderer

Stelle gehören bestimmte Medien bzw. Medienbeiträge zu genau der Unterdrückung, die unter einem Hashtag kritisiert wird – zum Beispiel, wenn im Zusammenhang antisexistischer Hashtags vorwiegend antifeministische Journalist*innen zu Wort kommen.

Aber auch Hashtags selbst sind bei allen positiven Auswirkungen kritisch zu betrachten. Gerade aus feministischer Perspektive müssen wir uns fragen, inwieweit eine Hashtag-Kampagne intersektionale Machtverhältnisse überhaupt abbilden kann. Wenn es für jede Diskriminierung einen eigenen Hashtag gibt, besteht durchaus das Risiko, am Ende wieder eine Eindimensionalität zu zementieren. Hashtags können der tatsächlichen Komplexität von Diskriminierungserfahrungen also auch nur bis zu einem gewissen Punkt Raum geben.[2]

Erschwerend kommt hinzu, dass möglicherweise viele Erinnerungen an vergangene Traumata mitunter durch das Lesen der Erfahrungen der anderen Nutzer*innen unter einem Hashtag wieder hochkommen, was schließlich zu einer Retraumatisierung führen kann. Wer heutzutage einen Hashtag initiiert, der Verletzungserfahrungen thematisiert, hat insofern ebenfalls eine

2 Ergänzend sei hierzu angemerkt, dass sich diese Kritik auf Hashtag-Kampagnen im Sinne von Awareness-Kampagnen bezieht. Kampagnen also, bei denen Betroffene den Hashtag als Ventil für ihre Diskriminierungserfahrungen nutzen, während sie gleichzeitig das Bewusstsein Nicht-Betroffener für ein bestimmtes Problem schärfen oder überhaupt erst herstellen können. Es gibt allerdings auch andere Formen von Hashtag-Kampagnen, die mitunter besser geeignet sind, um intersektionale Machtverhältnisse abzubilden. Hierzu sei als Beispiel die Kampagne #Ausnahmslos genannt, die im Januar 2016 als feministische Intervention entstand, nachdem der öffentliche Diskurs um sexualisierte Übergriffe in der Kölner Silvesternacht 2015/2016 extrem rassistisch verlief. Unter ausnahmslos.org wurde ein von 22 Feminist*innen (zu denen auch die Autorinnen dieses Artikels gehören) verfasster Aufruf veröffentlicht, der Kritik am aktuellen Diskurs enthielt sowie 14 konkrete Forderungen, um gegen sexualisierte Gewalt vorzugehen und dabei gleichzeitig antirassistisch zu handeln. Die Abbildung intersektionaler Machtverhältnisse ergab sich durch eine vielfältige Zusammensetzung der Initiator*innengruppe und ihrer jeweiligen Perspektiven, die auch in den Aufruf einflossen. Diese Vielfalt spiegelte sich schließlich auch in den Mitzeichnungen des Aufrufs wider, da er in zahlreichen persönlichen Netzwerken geteilt wurde und unterschiedliche Communitys erreichte. Der Hashtag #Ausnahmslos fungierte insofern im Vergleich zu Awareness-Kampagnen viel stärker als Label für den Aufruf und die politische Haltung dahinter, statt eine Ventilfunktion für einzelne Diskriminierungserfahrungen zu erfüllen.

Verantwortung zur Fürsorge. Hierzu kann es unterstützend wirken, hilfreiche Online-Quellen und Hinweise zu Anlaufstellen für Betroffene unter dem Hashtag zu verbreiten.

Der Preis für die Sichtbarkeit unter einem Hashtag bedeutet für Betroffene meistens erneut verletzlich zu sein und birgt das Risiko, Opfer digitaler Gewalt zu werden. Der Ort, der uns eben noch empowert hat, kann dann zum Ort werden, an dem wir uns wieder fragen müssen, ob wir uns überhaupt weiter als Betroffene struktureller Diskriminierung und Gewalt äußern können. Um dem entgegen zu wirken, sollten zusätzlich geschlossene Räume existieren, online wie offline, in denen Betroffene sich nicht verteidigen müssen und Unterstützung finden.

Intersektionale Vulnerabilitäten

Unabhängig von der Teilnahme an einer Hashtag-Kampagne lassen Untersuchungen aus Ländern wie Großbritannien, Spanien oder Schweden darauf schließen, dass vor allem Frauen von den extremsten Formen von Hasskommentaren auf Social Media betroffen sind (Amnesty International 2017: o.S.). Diese verschärfen sich umso mehr, wenn sie von intersektionaler Diskriminierung betroffen sind und ebenso Rassismus, Transfeindlichkeit, Homo- oder Behindertenfeindlichkeit erfahren. Für Deutschland fehlen bisher leider konkrete Zahlen, sollten aber dringend ergänzt werden, um auf dieser Basis entsprechende Maßnahmen zu entwickeln und das Hilfsangebot für Betroffene auszubauen und einen intersektionalen Blick auf das Problem digitaler Gewalt zu stärken.

Auch das in Deutschland eigens erlassene Netzwerkdurchsetzungsgesetz (NetzDG) schafft bisher keine Abhilfe. Vielmehr wird es sogar benutzt, um politisch aktive Menschen nachhaltig mundtot zu machen. Gerade rechte bis rechtsextreme Gruppen melden hierzu massenweise angebliche Verstöße gegen das NetzDG und führen schließlich eine Sperrung, insbesondere aktivistischer Accounts, herbei (vgl. @apolitAsh/@zugezogenovic 2018: o.S.). Vor allem Frauen of Color, trans Personen und Menschen mit Behinderung sind hiervon betroffen – umso stärker, wenn sich diese Identitätskategorien überschneiden. Neben Hate Speech und gesperrten Accounts kommt es dabei auch

oft zu Stalking, »Deadnaming«[3] (bei trans Personen), »Doxing«[4] und Morddrohungen (sogar gegen Familie und Freund*innen). Immer häufiger wird davon berichtet, dass die Wohn- oder Arbeitsadressen der betreffenden Personen aufgesucht werden, um dort ebenfalls ein Gefühl der Bedrohung zu erzeugen.

Trotz des erhöhten Risikos sich angreifbar zu machen, zeigen Beispiele zu Aktivismus in sozialen Medien, dass sehr viele politische Inhalte von Menschen mit intersektionalen Zugehörigkeiten publiziert werden. Das nutzt den Netzwerken wie Twitter, Facebook oder Instagram gleich zweifach: Erstes gehört es zu ihrem Geschäftsmodell, über »Traffic«[5] Geld zu verdienen. Mehr publizierte Inhalte bedeuten auch immer mehr Einnahmen für die Plattformen. Zweitens profitieren die Netzwerke von der positiven Aufmerksamkeit, die sie durch die medialen Diskussionen dieser aktivistischen Inhalte bekommen. Gleichzeitig haben die Netzwerke progressiven Aktivist*innen bisher wenig ernsthafte Unterstützung gegen digitale Gewalt angeboten. Meist wird auf die vorhandenen Systeme zum Stummstellen und Blockieren von Nutzer*innen verwiesen, diese sind jedoch nicht ausreichend. Aktuell ist das Videoportal »TikTok« sogar dadurch aufgefallen, die Inhalte von Menschen mit Behinderungen, aber auch queere und dicke Menschen in ihrer Reichweite einzuschränken, d.h. ihre Videos wurden anderen Nutzer*innen wesentlich seltener angezeigt. Dies geschehe angeblich, um diese Personengruppen vor Angriffen zu schützen (vgl. Köver/Reuter 2019: o.S.). Dem Unternehmen ist also offensichtlich klar, dass es Menschen gibt, die besonders häufig Opfer von Gewalt im Netz werden. Statt aber hier eine halbwegs sichere Umgebung für alle durchzusetzen und Sanktionen gegen diejenigen zu verhängen, die sich diskriminierend verhalten, werden die Betroffenen selbst zum Risikofaktor und bestraft. Aufgrund der weltweiten Kritik wurden die Richtlinien bei TikTok diesbezüglich angepasst.

---

3 Deadnaming ist das Ansprechen einer trans Person mit ihrem alten Namen (vgl. Giese 2018: o.S.).

4 Doxing ist das Sammeln und Veröffentlichen persönlicher Daten im Internet (z.B. E-Mail-Adresse, Telefonnummer, Wohnort, Arbeitsstelle, Geburtsdatum, Adresse der Eltern usw.)

5 Der Begriff Traffic beschreibt den Datenverkehr auf einer Internetpräsenz. Vorrangig geht es dabei um das Besuchsaufkommen – je höher dieses ist, umso mehr Geld kann beispielsweise mit Werbeeinnahmen verdient werden.

Ausblick

Den sozialen Netzwerken fehlt es oftmals an Diversity-Kompetenz – möglicherweise nicht zuletzt, weil viele Positionen in den Unternehmen zum großen Teil von weißen Männern besetzt sind (vgl. Coles 2016: o.S.). Die Anliegen von (intersektional) diskriminierten Menschen finden dadurch deutlich seltener Einzug in die Entwicklungsprozesse. Welche neuen Eigenschaften eines Netzwerks sich besonders gut zum Missbrauch eignen und wo die Gefahren für diskriminierte Personen liegen, zeigt sich deswegen meistens zu spät. Verbesserungen, die soziale Netzwerke für alle sicherer machen, die sie benutzen, müssen eben jene diskriminierten Personen oft im Nachhinein durchsetzen. Zum Aktivismus mithilfe eines Netzwerks kommt dann oft zusätzlich noch der Aktivismus gegen ein Netzwerk. Empowerment und Probleme stehen für marginalisierte Menschen, die sich in sozialen Netzwerken bewegen, folglich Seite an Seite.

Social Media-Dienstanbieter müssen gegen digitale Gewalt noch stärker in die Pflicht genommen werden. Die Positionen in den Unternehmen müssen diverser besetzt sein, damit die Anliegen von diskriminierten Personen von vornherein mitgedacht werden. Die Unternehmen müssen sich außerdem an den Kosten für ein umfassendes Beratungsangebot beteiligen und gleichzeitig die Unabhängigkeit der Informations- und Beratungsstellen respektieren.

Die Vision, im Internet einen Raum zu finden, der frei von Diskriminierung ist, ist nicht aufgegangen. Online wie offline wirken die gleichen Machtverhältnisse: Menschen werden aufgrund ihres Geschlechts, ihrer Sprache, ihrer Religionszugehörigkeit, ihrer ethnischen oder sozialen Herkunft, ihrer Sexualität, einer Behinderung oder Ähnlichem benachteiligt und beleidigt. Wer sich gegen Diskriminierung einsetzen möchte, muss sich demzufolge auch anschauen, was im Internet passiert und kann nicht davon ausgehen, hier nur auf besonders progressive Menschen zu treffen. Gleichzeitig darf in der Debatte um Gewalt im Netz eins nicht vergessen werden: Gewalt gegen marginalisierte Menschen wurde nicht im Internet erfunden. Nicht Onlinekommunikation an sich ist das Problem. Im Internet spiegeln sich aber natürlich Entwicklungen und Probleme, die offline entstanden sind.

Literatur

@apolitAsh und @zugezogenovic (2018): »›Sind Almans Abfall?‹ Das NetzDG richtet sich gegen Hassinhalte, führt aber oft zu Sperrungen von antirassistischen Accounts«, in: ak – analyse & kritik – zeitung für linke Debatte und Praxis Nr. 63. https://akweb.de/ak_s/ak639/43.html [Zugriff: 5.3.2020].

Amnesty International (Hg.) (2017): »Amnesty reveals alarming impact of online abuse against women«. https://amnesty.org/en/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/ [Zugriff: 5.3.2020].

Christie, Nils (1986): »The ideal victim«, in: Fattah, Ezzat (Hg.), From Crime Policy to Victim Policy, New York, S. 17-30.

Coles, Donyae (2016): »How Reporting and Moderation On Social Media is Failing Marginalized Groups«. https://modelviewculture.com/pieces/how-reporting-and-moderation-on-social-media-is-failing-marginalized-groups [Zugriff: 5.3.2020].

Crenshaw, Kimberlé (1989): »Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics«. https://philpapers.org/archive/CREDTI.pdf [Zugriff 15.6.2020].

Drüeke, Ricarda/Klaus, Elisabeth (2014): »Öffentlichkeiten im Internet: Zwischen Feminismus und Antifeminismus«, in: femina politica, Vol. 23 Nr. 2, S. 59-71.

Giese, Linus (2018): »Was ist eigentlich ein Deadname?«. https://ichbinslinus.de/2018/04/24/was-ist-eigentlich-ein-deadname/ [Zugriff: 5.3.2020].

Holland, Martin (2018): »25 Jahre Hunde im Internet – ein Cartoon erklärt das Netz«. https://heise.de/newsticker/meldung/25-Jahre-Hunde-im-Internet-Ein-Cartoon-erklaert-das-Netz-4100562.html [Zugriff 15.6.2020].

Köver, Chris/Reuter, Markus (2019): »Diskriminierende Moderationsregeln. TikToks Obergrenze für Behinderungen«. https://netzpolitik.org/2019/tiktoks-obergrenze-fuer-behinderungen/ [Zugriff: 5.3.2020].

Salzburger, Sonja (2014): »Ein Jahr #Aufschrei. Christine Lüders, Antidiskriminierungsstelle des Bundes«. https://sueddeutsche.de/leben/ein-jahr-aufschrei-noch-viel-zu-tun-1.1868630-5 [Zugriff: 5.2.2020].

Rechtliche Handlungsoptionen bei digitaler Gewalt

Möglichkeiten und Grenzen strafrechtlicher Intervention bei digitaler Gewalt

Christina Clemm

Die strafrechtliche Erfassung von digitaler Gewalt

Die meisten Regelungen im deutschen Strafgesetzbuch[1] (StGB) stammen aus einer Zeit, lange bevor die Digitalisierung und damit strafwürdiges Verhalten im digitalen Raum entstanden sind. Insofern gibt es bislang viele kleine mühsame Schritte, dem Phänomen strafrechtlich zu begegnen. Dabei wird zum einen durch Gesetzesänderungen reagiert, zum anderen aber muss sich die Rechtsprechung auf die Spezifika von Gewalt im digitalen Raum einstellen. Neben den konkreten Straftatbeständen ist problematisch, dass bereits das Wissen über und der Umgang mit sozialen Medien auch im Jahr 2020 noch bei vielen Richter*innen und Ermittlungspersonen fehlen und die Folgen digitaler Gewalt nicht ernst genommen werden.

Im Folgenden sollen die für diesen Bereich bestehenden strafrechtlichen Tatbestände aufgezeigt werden. Dabei ist festzustellen, dass es neben und zusätzlich zu digitaler Gewalt im und aus dem öffentlichen Raum heraus (Hate Speech) noch strafrechtlich relevante digitale Taten gibt, die ihren Ursprung im sozialen Nahraum haben. Delikte also, die nur aufgrund besonderer Kenntnisse über die betroffene Person begangen werden können. In den letzten Jahren ist festzustellen, dass im sozialen Nahraum neben der physischen Gewalt immer häufiger auch digitale Gewalt ausgeübt wird, häufig als Fortsetzung analoger Gewalt. Dabei nutzen die Täter*innen persönliche Kenntnisse wie Zugangsmöglichkeiten zu Accounts, Passwörter, gemeinsam oder mit Einwilligung erlangte Fotos und Videos, Kenntnisse über Freund*innen oder Kolleg*innen oder Details aus dem beruflichen Alltag.

1 Die Ausführungen in diesem Text beziehen sich auf die Rechtslage mit Stand Juli 2020.

Die rechtspolitisch virulente Frage, ob die Straftatbestände, die bereits im geltenden Strafgesetzbuch vorhanden sind, ausreichen oder ob eigene Tatbestände, die dem besonderen Unrecht der digitalen Gewalt gerecht werden, geschaffen werden müssen, wird hier nicht weiter behandelt. Tatsache ist jedenfalls derzeit, dass digitale Gewalt massenhaft verübt wird und in Deutschland mehr oder weniger straflos hingenommen wird.

Durch die für alle zugängliche öffentliche Verbreitungsmöglichkeit über das Internet, hat sich ein erhebliches Ausmaß an Möglichkeiten eröffnet, digitale Gewalt auszuüben und Betroffene intensiv und fast nicht endend zu schädigen. Hierbei können verschiedenste Wirkmechanismen angewandt werden, wie etwa das Posten, also Veröffentlichen von Blogeinträgen und Kommentieren unter Berichten, Artikeln oder in sozialen Medien, aber auch Liken, Retweeten, Fake-Accounts nutzen, persönliche Daten veröffentlichen und Ähnliches. Zum Teil wird hierzu auch Künstliche Intelligenz, insbesondere z.B. sogenannte Social Bots[2] angewandt.

In der Regel werden Ehrdelikte erfüllt (§§ 185ff. StGB). Darüber hinaus kommen jedoch auch Bedrohung (gem. § 241 StGB), Volksverhetzung (gem. § 130 StGB) oder auch das öffentliche Aufrufen zu Straftaten (gem. § 111 StGB) in Betracht.

Ehrdelikte gemäß §§ 185 ff StGB

Das zu schützende Rechtsgut (Schutzgut) ist die Ehre einer Person oder Personengruppe, wobei sowohl die faktische Ehre, welche das subjektive Ehrgefühl und den objektiven guten Ruf einer Person umfasst, als auch die normative Ehre mit dem Anspruch auf Achtung der Persönlichkeit geschützt sind. Eine Ehrverletzung kann sowohl durch eine Tatsachenbehauptung[3] als auch durch die Abgabe eines ehrenrührigen Werturteils[4] erfolgen.

Bei digitaler Gewalt geht es um Äußerungen, die durch die Täter*innen im Internet verbreitet werden und dadurch, anders als analog, häufig eine

2 Social Bots sind Programme, die automatisiert Inhalte veröffentlichen, aber auch andere Inhalte teilen und liken oder mit Nutzer*innen interagieren können. In der Regel verbieten die AGBs der meisten sozialen Netzwerke die Verwendung solcher Programme.

3 Eine Tatsachenbehauptung ist eine Äußerung, die eine objektive Klärung des Sachverhaltes zulässt.

4 Ein Werturteil ist eine subjektive Einschätzung, die die persönliche Überzeugung der äußernden Person wiedergibt.

sehr große Verbreitung erfahren. Beispielsweise wenn in den sozialen Medien Aussagen über eine Person verbreitet werden, wie etwa, sie habe ihren Arbeitgeber bestohlen, ihre Kinder misshandelt oder ihren Ex-Partner fälschlicherweise wegen einer Vergewaltigung angezeigt. Ebenso erfasst ist, wenn die betroffene Person beispielsweise als »dumme Kuh«, »Schlampe« oder als minderwertig beschimpft wird. Dabei können nicht nur einzelne Personen, sondern auch Personengruppen zu Opfern von Ehrdelikten werden, wenn sie »eine anerkannte soziale Funktion erfüllen« und »einen einheitlichen Willen bilden können« (vgl. BVerfG vom 17.05.2016).[5] Bei sämtlichen Ehrverletzungsdelikten ist eine Abwägung zwischen Ehrverletzung und dem Grundrecht der Meinungsfreiheit aus Artikel 5 Abs. 1 GG zu beachten. Eine besondere Ausprägung der Meinungsfreiheit ist dabei die Wahrnehmung berechtigter Interessen (vgl. § 193 StGB). So kann etwa die identifizierende Verdachtsberichterstattung über eine Vergewaltigung zulässig sein, obwohl der Beschuldigte noch nicht erstinstanzlich verurteilt worden ist (vgl. Saarländisches Oberlandesgericht Saarbrücken vom 5.10.2016) oder die Bezichtigung eines nahen Verwandten des sexuellen Missbrauchs, wobei die Veröffentlichung nur innerhalb des engsten Verwandtenkreis zulässig ist (vgl. AG Brandenburg, Streit 2017: 43-44). Bei der Bewertung einer Äußerung bzw. Veröffentlichung ist deren objektiver Sinngehalt zugrunde zu legen, wie ihn »ein unbefangener, verständiger Dritter« auffasst. Konkret ist zu hinterfragen, ob noch ein Sachbezug besteht oder eine Schmähkritik vorliegt. Eine Schmähkritik liegt immer dann vor, wenn die Diffamierung der Person im Vordergrund steht – selbst, wenn ein sachlicher Anlass vorgegeben wird. Wie kontrovers und häufig auch unverständlich die juristische Auseinandersetzung um die Ehrverletzungsdelikte geführt wird, zeigt sich an Verfahren wie etwa das der Bundestagsabgeordneten Renate Künast[6] oder der Staatssekretärin Sawsan Chebli.[7] Beachtlich ist insofern auch der in § 188 StGB zum Ausdruck kommende besondere Schutz für Personen des politischen Lebens.

---

5 Interessant hierzu grundlegende Entscheidungen des BVerfG zu »ACAB« BVerfG, Stattgebender Kammerbeschluss vom 17. Mai 2016 – 1 BvR 2150/14.

6 Nach erstinstanzlicher Einschätzung, dass »Schlampe«, »Drecks Fotze«, »Diese hohle Nuß gehört entsorgt, auf eine Mülldeponie, aber man darf ja dort keinen Sondermüll entsorgen«, »Schlamper« und »Ferck du Drecksau« keine Formalbeleidigungen seien, folgte eine lesenswerte Umentscheidung des Landgerichts (vgl. Sehl 2020: o.S.).

7 Erstinstanzlicher Freispruch nach Bezeichnung als »Quotenmigrantin« und »islamische Sprechpuppe« (vgl. o.A. 2020: o.S.).

Wichtig ist, dass die meisten Ehrdelikte Antragsdelikte sind und insofern die Stellung von Strafanträgen erforderlich ist (s.u.).

Öffentlicher Aufruf zu Straftaten gemäß § 111 StGB

Hiernach macht sich eine Person strafbar, wenn sie öffentlich zu Straftaten aufruft, wie etwa der Aufruf jemanden zu töten, wie zum Beispiel mehrfach verbreitet wurde, die Bundeskanzlerin Angela Merkel zu töten oder Sozialarbeitende oder Flüchtlingsunterstützer*innen damit eingeschüchtert werden sollen, indem Täter*innen auffordern, die Unterstützerin zu vergewaltigen oder anderweitig zu misshandeln. Wichtig ist, dass zur Erfüllung der Straftat die Tat hinreichend konkret sein muss, reine »Unmutsäußerungen« reichen für eine Strafbarkeit nicht aus.

Störung des öffentlichen Friedens durch Androhung von Straftaten gemäß § 126 StGB

Strafbar ist zudem das ausdrückliche oder konkludente Ankündigen oder In-Aussicht-Stellen von bestimmten in § 126 StGB genannten Taten. Dabei müssen Straftaten wie etwa Mord, Totschlag, Völkermord, Verbrechen gegen die Menschlichkeit, Verbrechen des schweren Menschenhandels, Erpressung angekündigt werden. Es reicht auch die Ankündigung einer gefährlichen Körperverletzung oder eine Straftat gegen die sexuelle Selbstbestimmung in den Fällen des § 177 Absatz 4 bis 8 (schwere sexuelle Nötigung u.a.) oder des § 178. (sexuelle Nötigung mit Todesfolge)[8].

§ 126 StGB schützt den öffentlichen Frieden, sodass die Androhung geeignet sein muss, den öffentlichen Frieden zu stören. Das ist dann der Fall, wenn die Tat die konkrete Besorgnis begründet, dass der Friedenszustand oder das Vertrauen in seinen Fortbestand in Teilen der Bevölkerung erschüttert oder deren Neigung zu Rechtsbrüchen angereizt wird. Dies kann etwa die Androhung eines Amoklaufs, eines Femizides (vgl. OLG Frankfurt vom 16.04.2019[9]) oder eine Bombendrohung sein. Der*die Täter*in muss die Verwirklichung der Androhung nicht ernstlich wollen, es reicht aus, wenn der Anschein der Ernstlichkeit des Vorhabens erweckt wird.

---

8 Eingeführt mit dem »Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität« vom 18.6.2020.

9 Eine Person hat mit einer täuschend echt aussehenden Scheinwaffe in der Hand einer anderen Person mitgeteilt, dass er nun seine Frau töten werde.

Volksverhetzung gemäß § 130 StGB

Als Volksverhetzung gelten laut StGB verschiedene Handlungen, die sich gegen bestimmte »nationale, rassische [sic!][10], religiöse oder ethnische Gruppen« (§130 StGB) bzw. Bevölkerungsteile richten. Eine solche Handlung ist z.B. das Aufstacheln zu Hass oder die Aufforderung zu Gewalt gegen diese Personen. Voraussetzung einer Strafbarkeit wegen Volksverhetzung ist dabei, dass die Tat geeignet ist, den öffentlichen Frieden zu stören. So kann etwa die Bezeichnung von Frauen als »Menschen zweiter Klasse«, »minderwertige Menschen« und »den Tieren näherstehend« eine Volksverhetzung darstellen (vgl. Legal Tribune Online 2020: o.S.). Dabei sind die Äußerungen stets »freiheitsfreundlich« hinsichtlich der Meinungsfreiheit auszulegen. Dies bedeutet, dass stets sowohl der Kontext der Äußerungen betrachtet werden muss, wie auch das hohe Gut der Meinungsfreiheit berücksichtigt werden muss, die auch drastische, zugespitzte und polemische Äußerungen schützt. Art. 5 Abs. 1 und 2 GG erlaubt nicht den staatlichen Zugriff auf die Gesinnung, sondern ermächtigt erst dann zum Eingriff, wenn Meinungsäußerungen die rein geistige Sphäre des Für-richtig-Haltens verlassen und in Rechtsgutverletzungen oder erkennbar in Gefährdungslagen umschlagen (vgl. BVerfGE 2009).

Belohnung und Billigung von Straftaten gemäß § 140 StGB

Ähnlich wie bei § 126 StGB, bei dem die Tathandlung die Androhung bestimmter schwerer Straftaten strafbar ist, ist auch die Billigung und Belohnung entsprechender Straftaten nach § 140 StGB strafbar. Wer etwa öffentlich Morde, Völkermorde, schweren Menschenhandel, Landesverrat und andere schwere Straftaten wie die sexuelle Nötigung in einem schweren Fall lobt oder sogar belohnt, wird bestraft. Bei der Beurteilung, ob eine solche Straftat vorliegt, wird von der Rechtsprechung sehr genau unterschieden, ob es sich »lediglich um eine Beschreibung einer Tat« handelt, oder ausdrücklich eine positive Bewertung der Ursprungstat erfolgt. Außerdem muss diese Billigung abstrakt den öffentlichen Frieden stören und soll – da sie das Grundrecht auf freie Meinungsäußerung einschränkt – nur sehr restriktiv angewandt werden (vgl. KG Berlin vom 18.12.2017: Rn. 47).

Das ausdrückliche Gutheißen etwa eines Femizides erfüllt nur dann den Tatbestand, wenn begründet werden kann, wie dieses Gutheißen abstrakt den

10 Es gibt eine kontrovers geführte Debatte, ob der Begriff ›Rasse‹ aus deutschen Gesetzen gestrichen werden sollte (vgl. u.a. Cremer 2010: o.S.).

öffentlichen Frieden stören kann, weil etwa andere dies gutheißen und nachahmen könnten. Möglich wäre dies beispielsweise bei lobenden Äußerungen zu einem aus Frauenhass begangenen Terroranschlag durch Anhänger der Incel-Ideologie (vgl. Mertins 2020: o.S.).

Nötigung gemäß § 240 StGB

Strafbar ist es auch, eine andere Person mit Gewalt oder durch Drohung mit einem empfindlichen Übel zu einer Handlung, Duldung oder Unterlassung zu nötigen. Typisch sind insofern Fälle, in denen etwa damit gedroht wird, Details aus dem Privatleben einer Person, Adressen, Bankverbindungen etc. zu veröffentlichen, wenn die Betroffene nicht etwas Bestimmtes unternimmt oder unterlässt (etwa unterlässt, weiter über Neonazis zu schreiben, unterlässt weiter öffentlich aufzutreten, unterlässt ihre digitale Reichweite zu nutzen, um bestimmte feministische Meinungen zu verbreiten, nicht aufhört über ihre Transition zu berichten etc.) Wenn die betroffene Person weiblich oder als queere Person gelesen wird, kommen häufig Drohungen mit sexualisierter Gewalt hinzu. Im sozialen Nahraum gibt es häufig Nötigungen, etwa in der Form, dass gedroht wird, einverständlich aufgenommene intime Fotos zu veröffentlichen oder einem weiteren Bekanntenkreis zugänglich zu machen, wenn die Betroffene die Beziehung beendet oder sie beabsichtigen könnte, in der Beziehung erlebte Gewalt anzuzeigen. Auch die Drohung, Kolleg*innen Wissen mitzuteilen, dass dem*r Täter*in im Vertrauen mitgeteilt wurde, kommt häufig vor.

Bedrohung gemäß § 241 StGB

Ebenso ist es strafbar, eine Person mit der Begehung einer gegen sie oder eine ihr nahestehenden Person gerichteten rechtswidrigen Tat gegen die sexuelle Selbstbestimmung, die körperliche Unversehrtheit, die persönliche Freiheit oder gegen eine Sache von bedeutendem Wert zu bedrohen. Voraussetzung ist in diesen Fällen, dass die Bedrohung objektiv ernst zu nehmen ist. Es kommt nicht allein darauf an, ob die Betroffene sich hierdurch hat beeindrucken lassen. Strafschärfend ist eine Bedrohung zu bewerten, die im öffentlichen Raum, durch Schriften, aber auch digital, geschehen ist.

Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen gemäß § 201a StGB

Es gibt immer wieder Fälle, bei denen heimlich in einer geschlossenen Wohnung Aufnahmen von einer Person erstellt, oder Aufnahmen, die mit Zustimmung der betroffenen Person hergestellt wurden und unbefugt an Dritte weitergegeben werden. Dies ist als Verletzung des höchstpersönlichen Lebensbereichs gem. § 201a StGB strafbar.

Diese Fälle kommen in der Praxis häufig vor. Insbesondere in Form sogenannter ›Rachepornos‹ (›Revenge Porn‹), also dass zunächst einverständlich aufgenommene intime Bilder oder Videos gegen den Willen der Betroffenen veröffentlicht werden. In diesen Fällen kann tateinheitlich eine Strafbarkeit gem. § 184 StGB, dem Verbreiten pornografischer Schriften, vorliegen. Wichtig für die Strafverfolgung ist, dass bewiesen werden kann, dass die Aufnahmen tatsächlich verschickt wurden, weshalb der Erhalt unbedingt zu sichern und zu dokumentieren ist. Bei dem Tatbestand des Herstellens heimlicher Bildaufnahmen ist zu beweisen, dass die Aufnahmen tatsächlich ohne Einwilligung erfolgten.

Es handelt sich auch hier um ein sogenanntes relatives Antragsdelikt, d.h. es ist sinnvoll, dass ein Strafantrag gestellt wird.

Ausspähen von Daten gemäß § 202a StGB

Strafbar macht sich auch, wer sich oder einem Dritten zu Daten, die nicht für ihn*sie bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung Zugang verschafft. Wer also beispielsweise das Passwort der Ex-Freundin ermittelt und sich damit in ihre Accounts begibt und dort deren Nachrichten liest. Dies gilt für soziale Netzwerke, Clouds, Apps und Streaming-Dienste.

Durch den Tatbestand wird nicht nur das Verschaffen dieser Daten unter Strafe gestellt, sondern auch bereits das Verschaffen des Zugangs zu diesen, im Sinne von sogenanntem Hacking. Wobei sich die Frage stellt, ob grundsätzlich ein Eindringen ohne Kenntnisnahme bzw. Abrufen der Daten möglich ist. Ein Verschaffen des Zugangs liegt auch bei der Infizierung fremder Systeme mit sogenannten Trojanern (z.B. KeyLogging-Trojaner, Sniffer oder Backdoorprogramme) oder der heimlichen Installation von Spionage-Apps vor. Insbesondere die Verwendung von sogenannter Spyware kommt im sozialen Nahraum häufig zur Überwachung der (Ex-)Partner*in vor und ist ein massiver Eingriff in die Persönlichkeitsrechte der betroffenen Person. Immer

wieder kommt es vor, dass sogenannte Stalkerware bzw. Spy Apps auf dem Smartphone oder dem Rechner der Betroffenen installiert werden.[11] Diese Programme befinden sich dann versteckt auf den Systemen und schneiden unter anderem Chatverläufe, Telefonate sowie Browserverläufe und Passwörter mit und verfolgen auch anhand der Geo-Daten des Smartphones, wo sich jemand gerade aufhält.

Häufig berichten Betroffene, dass sie scheinbar zufällig auf ihre*n (Ex-)Partner*in treffen und sie sich nicht erklären können, wie dies geschehen kann. Wenn die betroffene Person diese Software unwissentlich selbst installiert, etwa durch das Klicken auf einen E-Mail-Anhang, liegt mittelbare Täterschaft vor, d.h. da die betroffene Person selbst die Daten öffentlich macht, benutzt der*die Täter*in die handelnde Person nur als Werkzeug und bleibt damit Täter*in. Die Strafbarkeit entfällt aber beispielsweise, wenn etwa ein*e Ex-Partner*in noch auf dem fremden Handy oder Computer eingeloggt ist und auf diesem Weg Nachrichten mitgelesen werden, da die betroffene Person selbst das Passwort eingegeben und gespeichert hat bzw. es versäumt hat sich auszuloggen.

Häufig greift der § 202a StGB nicht, weil Betroffene ihrer Partner*in die Zugangsdaten während der Partnerschaft übergeben haben, sei es zur Einrichtung der Accounts oder als ›Vertrauensbeweis‹.

Das Überwinden der Zugangssicherung muss unbefugt, also ohne Einwilligung erfolgen, wobei auch die durch Täuschung erlangte Einwilligung nicht ausreicht. Etwa wenn die betroffene Person denkt, sie gäbe ihr Passwort nur für eine bestimmte App, tatsächlich kann der*die Täter*in aber damit zahlreiche Anwendungen nutzen. Deshalb sind sogenannte Password-Fishing Handlungen, die insbesondere zur Vorbereitung von Computerbetrug durchgeführt werden, ebenfalls unbefugt, wenn die betroffene Person davon ausgeht, es handele sich um Abfragen von Berechtigten, wie dem Anbieter selbst. Es sei denn, die betroffene Person gibt hierbei Daten preis, bei denen bekannt ist, dass sie auch gegenüber der vermeintlichen Stelle geheim sind – wie z.B. Passwörter. Zur Verfolgung ist ein Strafantrag der betroffenen Person erforderlich.

---

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

Abfangen von Daten gemäß § 202b StGB

Wer unbefugt mit technischen Mitteln Daten abfängt, die nicht für ihn*sie bestimmt sind (§ 202b Abs. 2 StGB), macht sich ebenfalls strafbar. Dies gilt für nichtöffentliche Datenübermittlungen oder Daten aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage. Besonders relevant ist das Abfangen von Daten im Rahmen der Verwendung von Telefon, Fax und E-Mail oder analoger Post. Erfasst werden z.B. das Mithören von Skype-Gesprächen oder die Kenntnisnahme von E-Mails. Es ist dabei gleichgültig, ob die Daten über eine Leitung laufen oder drahtlos übermittelt werden. Schlichtes Hacking, also das Eindringen in das fremde System an sich, ist dagegen von § 202b StGB nicht erfasst, sondern fällt unter § 202a StGB, da bei § 202b StGB eine Kenntnisnahme der Daten vorliegen muss. Auch das Abfangen von Standortdaten durch sogenannte Spyware fällt unter die Strafvorschrift des § 202b StGB. Auch für diese Begehungsform ist ein Strafantrag zur Verfolgung Voraussetzung.

Vorbereiten des Ausspähens und Abfangen von Daten gemäß § 202c StGB

Hier geht es etwa um das sogenannte Passwort-Phishing und das spätere Verkaufen dieser oder darum, Systeme zur Verfügung stellen, deren objektiver Zweck es ist, Passwörter bzw. Zugangsschranken zu entschlüsseln – also diejenigen Handlungen, die ein späteres Ausspähen oder Abfangen der Daten ermöglichen. Häufig begeht diese Straftat nicht der*die ehemalige Partner*in selbst, sondern eine Person, die ihn*sie dabei technisch unterstützt, die Passwörter herauszufinden. Wenn er*sie jedoch selbst die technischen Fähigkeiten dazu besitzt und ausführt und später tatsächlich die Daten ausspäht oder abfängt, wird er*sie nicht wegen des Vorbereitens, sondern nur wegen der Tat selbst bestraft.

Datenhehlerei gemäß § 202d StGB

Strafbar ist auch, wenn ein*e Täter*in private Daten, die eine dritte Person zuvor rechtswidrig erlangt hat, verbreitet oder einem anderen überlässt, um sich selbst zu bereichern oder einen anderen, z.B. die betroffene Person, zu schädigen. Dies sind beispielsweise Handlungen, wie die Veröffentlichung rechtswidrig, also ohne Einwilligung erlangter Zugangsdaten, Kontonummern etc. Ausgenommen sind Handlungen von Amtsträgern und Ermittlungsbehörden. Die Tathandlungen werden nur auf Strafantrag verfolgt, § 205 StGB.

Nachstellung gemäß § 238 StGB (Stalking)

Werden von einer Person zahlreiche und mehrfach wiederkehrend E-Mails, WhatsApp-Nachrichten etc. verschickt, kann dies als Nachstellung gem. § 238 StGB strafbar sein. Ausgenommen sind solche Nachrichten, mit denen berechtigte Interessen vertreten werden, dies ist z.B. der Fall, wenn nach einer gemeinsamen Feier sehr viele Fotos verschickt werden. Als Stalking zu werten wäre, wenn über einen längeren Zeitraum hinweg die betroffene Person immer wieder per E-Mail, WhatsApp oder auf den sozialen Medien angeschrieben, kommentiert oder in sonstiger Form kontaktiert würde, obwohl diese bereits mitgeteilt hat, dass sie einen Kontakt nicht wünscht. Dabei kommt es immer wieder vor, dass Täter*innen Accounts der betroffenen Personen geradezu überschwemmen. Sehr oft geht digitales Stalken mit analogen Handlungen einher. Wichtig ist eine gute Dokumentation der einzelnen Kontaktaufnahmen, denn der Straftatbestand setzt eine Vielzahl hiervon voraus, bevor es unter Stalking fällt.[12] Die Strafverfolgung erfolgt nur auf Antrag oder wenn die Staatsanwaltschaft dies von Amts wegen für geboten hält und das besondere öffentliche Interesse annimmt.

Computerbetrug gemäß § 263a StGB

Neben den Angriffen auf das Ansehen und die höchstpersönlichen Informationen über die Betroffenen, kommt es auch immer wieder vor, dass Täter*innen das Vermögen einer Person angreifen. Ein Computerbetrug kann durch vier Handlungsweisen begangen werden: Durch unrichtige Gestaltung eines Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Einwirkung auf den Datenverarbeitungsvorgang in sonstiger Weise und durch die unbefugte Verwendung von Daten. So beispielsweise, wenn Waren mit der digitalen Identität der betroffenen Person bestellt werden.[13]

Stellt der*die Täter*in selbst Programme (wie Phishing-Programme) her, die nur dazu dienen, Daten zu erlangen, um sie später unbefugt zu verwenden, sind auch diese Vorbereitungshandlungen von § 263a Abs. 3 StGB erfasst.

Die Tat wird grundsätzlich als Offizialdelikt von Amts wegen verfolgt. Ausnahmsweise erfordert die strafrechtliche Verfolgung der Tat einen Straf-

12 Siehe Beitrag: Individuelle Strategien im Umgang mit geschlechtsspezifischer digitaler Gewalt.

13 Zu Formen digitaler Gewalt im Bereich Computerbetrug siehe ebd./Anm. 11.

antrag, wenn Opfer des Computerbetrugs eine angehörige Person, Vormund oder Betreuer*in ist oder wenn der durch die Tat entstandene Schaden gering ist.

Datenveränderung gemäß § 303a StGB

Strafbar ist es auch, wenn ein*e Täter*in rechtswidrig, also ohne Einwilligung, (fremde) Daten löscht, unterdrückt, unbrauchbar macht oder verändert. Dies kann auch durch den Einsatz von Viren erfolgen oder indem Zugangshindernisse wie Passwörter eingerichtet werden und somit der berechtigten Person der Zugriff auf die Daten entzogen wird. Auch das Löschen oder Unterdrücken von E-Mails fällt hierunter. Das bloße Hinzufügen von Daten fällt ebenfalls unter den Tatbestand, wenn hierdurch der Bedeutungsgehalt bereits gespeicherter Daten verändert wird. Vor allem während Partnerschaften sind die Hürden auf Daten und Geräte der anderen Person zuzugreifen meist gering. Das Verändern und Löschen von Daten, die emotionalen Wert besitzen oder relevant für Berufsausübung und Einkommen sind, kann Betroffenen wesentlichen Schaden zufügen.

Strafvorschriften des Bundesdatenschutzgesetzes in Bezug auf Stalkerware gemäß § 42 BDSG

Das Bundesdatenschutzgesetz (BDSG) sieht eine Strafandrohung von Geldstrafe oder bis zu zwei Jahren Freiheitsstrafe vor, wenn der*die Täter*in diese Daten verarbeitet ohne hierzu berechtigt zu sein oder durch unrichtige Angaben erschleicht und entweder gegen Entgelt oder in der Absicht handelt, jemand anderen zu bereichern oder zu schaden (vgl. § 42 Abs. 2 BDSG). Die Strafverfolgung erfolgt nur auf Antrag (vgl. § 43 Abs. 2, Nr. 3 BDSG).

Normen des Urheber- und Kunsturheberrechts

Werden Bilder der betroffenen Person öffentlich im Internet verbreitet, sei es im Original oder durch manipulierte Versionen, können auch die Normen des Urheberrechts (unerlaubte Verwertung urheberrechtlich geschützter Werke gemäß § 106 UrhG und unerlaubte Eingriffe in verwandte Schutzrechte gemäß § 108 UrhG) und des Kunsturheberrechts (unbefugtes Verbreiten oder öffentliches zur Schau stellen von Bildnissen gemäß §§ 33 i.V. 22, 23 KUG) greifen. Auch hier sind eigene Straftatbestände geschaffen worden, die entweder nur auf Antrag oder bei der Annahme des öffentlichen Interesses verfolgt werden.

Möglichkeiten und Grenzen der Strafverfolgung

Erfolgen Handlungen, die unter den genannten Straftatbeständen zu subsumieren sind, können diese angezeigt und müssen sodann von den Ermittlungsbehörden ermittelt werden. Sofern sich eine beschuldigte Person finden lässt, es sich um eine strafbare Handlung handelt und keine Verfahrenshindernisse, wie etwa Verjährung im Weg stehen, wird die Person bei hinreichendem Tatverdacht angeklagt oder es ergeht ein Strafbefehl. Der Erlass eines Strafbefehls gem. § 407 StGB ist dann zulässig, wenn die Staatsanwaltschaft die Durchführung einer Hauptverhandlung nicht für erforderlich erachtet und durch den Strafbefehl keine höhere Strafe als ein Jahr Freiheitsstrafe ausgesprochen wird. Sofern die beschuldigte Person hiergegen Einspruch einlegt, wird eine Hauptverhandlung durchgeführt. Wenn die beschuldigte Person nicht widerspricht, wird der Strafbefehl wie ein Urteil rechtskräftig. Erhebt die Staats- oder Amtsanwaltschaft Anklage, kommt es nach Eröffnung durch ein Gericht zu einer Gerichtsverhandlung. Unter den Bedingungen von §§ 395, 396 StPO kann sich die verletzte Person als Nebenkläger*in dem Verfahren anschließen und durch eine Rechtsanwältin oder einen Rechtsanwalt vertreten werden (vgl. § 397ff. StPO).

Darüber hinaus bestehen aufgrund von Persönlichkeitsrechtsverletzungen durch digitale Gewalt zivilrechtliche Unterlassungs- und Entschädigungsansprüche.[14] Handelt es sich um digitale Nachstellungen, kann ein Kontakt- und Näherungsverbot nach dem Gewaltschutzgesetz (GewSchG) beantragt werden.

Namhaftmachung

Größtes Problem bei der Durchsetzung der Ansprüche ist in vielen Fällen, dass die relevanten Veröffentlichungen anonym erfolgen, sodass die Täter*innen zunächst namhaft gemacht werden müssen. Dies betrifft die Strafverfolgung von Hate Speech wie auch digitaler Gewalt im Nahbereich, da selbst bei starken Indizien, dass die für die Tat erforderlichen Informationen nur einem*einer bestimmten Täter*in aus dem Nahbereich vorliegen, dies allein oftmals nicht ausreicht, um die konkrete Täterschaft zu belegen. Insofern werden immer wieder Forderungen nach Einführung einer Klarnamenspflicht im Netz laut (Amann/Deleja-Hotko/Rosenbach 2019: o.S.).

14 Siehe Beitrag: Zivilrechtliche Interventionen bei digitaler Gewalt.

Gleichzeitig ist Meinungs- und Zensurfreiheit ein hohes Gut und gerade im Internet, in dem jedes Thema besprochen wird, man sich über jedes Thema informieren und grenzüberschreitend auf Missstände aufmerksam machen kann, essentiell für eine demokratische Teilhabe. Hierbei ist auch die Wahrung von Anonymität ein wichtiger Faktor, insbesondere wenn man etwa an besonders diskriminierte und gefährdete Gruppen, wie etwa trans Personen, Oppositionelle, Sexarbeiter*innen u.v.a. denkt. Im Hinblick auf die Durchsetzung der Strafverfolgung bildet sich daher ein Spannungsfeld zwischen dem Erfordernis der Wahrung von Anonymität und der Verfolgungsmöglichkeit von Täter*innen digitaler Gewalt, welches bisher nicht aufgelöst werden kann.

Im Juni 2020 wurde das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität vom Bundestag beschlossen[15], welches besagt, dass in sozialen Netzwerken künftig Inhalte mit Neonazi-Propaganda, Mord- und Vergewaltigungsdrohungen oder kinderpornographischem Material gemeldet werden müssen und laut § 3a NetzDG nicht nur entfernt, sondern auch der Zugang zu ihnen gesperrt werden muss. Vielmehr soll das soziale Netzwerk auch das Bundeskriminalamt (BKA) einschalten, damit es die nötigen Ermittlungen einleitet. Hierfür wird das BKA extra eine neue Zentralstelle einrichten. Die sozialen Netzwerke müssen dem BKA nicht nur den verdächtigen Inhalt, sondern auch die IP-Adresse des verdächtigen Nutzers mitteilen. Die Betroffenen selbst können zur Namhaftmachung der Täter*innen gemäß § 14 Abs. 3 TMG Auskunft über Bestandsdaten von Nutzer*innen beantragen, wenn dies zur Durchsetzung zivilrechtlicher Ansprüche erforderlich ist. Voraussetzung ist die Verletzung absolut geschützter Rechte durch diese Nutzer*innen durch strafbare Handlungen nach den in § 1 Abs. 3 NetzDG aufgezählten Tatbeständen. Genannt werden hier beispielsweise Beleidigungsdelikte (§§ 185 ff StGB), Volksverhetzung (§ 130 StGB) oder auch die Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen (§ 201a StGB). Der Auskunftsanspruch des NetzDG greift jedoch nur, wenn es sich um Dienstanbieter handelt, die soziale Netzwerke im Sinne des § 1 Abs. 1 NetzDG betreiben.

Auch § 101 Abs.2 UrhG gibt Betroffenen einen Auskunftsanspruch bezüglich Tatsachen, die zur Verfolgung der eigenen Rechtsansprüche notwendig sind. Voraussetzung ist, dass die Rechtsverletzung offensichtlich ist. Die be-

15 Dieser Artikel berücksichtigt die Gesetzeslage im April 2021.

troffenen Personen können diesen Anspruch nicht nur gegenüber dem Täter geltend machen, sondern z.B. auch gegenüber Internetprovider.

Für Betroffene ist häufig der einfachste Weg eine Namhaftmachung über die Ermittlungsbehörden, nachdem die Tat strafrechtlich angezeigt wurde. Problematisch wird dies jedoch, wenn die Ermittlungsbehörden weder fachlich noch personell hinreichend zur Bekämpfung und Verfolgung von digitaler Gewalt ausgestattet sind. Problematisch ist auch, dass sich Server in anderen Ländern befinden und Rechtshilfeersuchen an die Standorte der Anbieter wegen der dortigen Rechtsvorschriften nicht bearbeitet werden.

Durchsetzung der Löschung/Recherche

Eine strafrechtliche Anzeige führt überwiegend nicht dazu, dass die Ermittlungsbehörden die Löschung etwaiger Veröffentlichungen veranlassen. Zum einen liegt das an fehlenden Zugangsmöglichkeiten der Beamt*innen etwa zu Pornoseiten oder fehlender Kenntnisse für das Aufspüren weiterer Verbreitungen im Internet sowie Kompetenzen im Bereich digitaler Gewalt. Zum anderen scheitert dies insbesondere an den fehlenden Kapazitäten der Ermittlungsbehörden. Die strafrechtlichen Ermittlungsbehörden sind stark überlastet und verfügen häufig über keine ausreichende Ausstattung, um die Taten effektiv zu verfolgen. Erledigungsdruck der vielen offenen Verfahren und personelle Engpässe machen es unmöglich, Beweise schnell zu sichern oder ambitioniert aktiv weitere strafbare Inhalte nachzuverfolgen.

Daher werden die Betroffenen in der Regel angehalten, selbstständig Beweise zu sichern oder zu recherchieren, wo und welche Veröffentlichungen im Internet auffindbar sind, ebenso die Veröffentlichungen zu melden oder sich an die Verantwortlichen zu wenden und diese zur Löschung aufzufordern. Dies scheitert wiederum häufig an der Namhaftmachung (s.o.). In der Praxis passiert es häufig, dass sich die Identität des*der Verantwortlichen nicht mehr nachvollziehen lässt.

Besteht ein Löschanspruch eines Kommentars oder Postings, hat der EuGH in einer Entscheidung im Oktober 2019 entschieden, dass der Verantwortliche auch nach wort- und sinngleichen Kommentaren suchen und die Löschung weiterverbreiteter Kommentare sicherstellen muss – zumindest bei im wesentlichen unverändertem Inhalt, soweit sich dieser durch technische Maßnahmen ermitteln lässt.

Probleme im Rahmen der Strafverfolgung der einzelnen Tatbestände

Antragserfordernis als Voraussetzung für die Strafverfolgung

Eine Vielzahl der einschlägigen Straftatbestände im Rahmen von digitaler Gewalt sind Antragsdelikte. Das heißt, sie bedürfen eines expliziten Strafantrags der betroffenen Person, damit die Tat durch die Ermittlungsbehörden verfolgt wird. Hierzu besteht eine Frist von drei Monaten. Die Frist beginnt bereits mit Kenntnis der Tat zu laufen, nicht erst wenn beispielsweise Täter*innen namhaft gemacht wurden. Unterbleibt der Strafantrag, ist zu unterscheiden, ob es sich um absolute oder relative Antragsdelikte handelt.

Absolute Antragsdelikte können nur strafrechtlich verfolgt werden, wenn ein Antrag gestellt wurde. Andernfalls besteht ein Verfolgungshindernis, das zwingend zur Einstellung des Verfahrens führt. Absolute Antragsdelikte sind z.B. die §§ 185ff StGB und 42 BDSG, wobei hier neben der betroffenen Person auch der Dienstvorgesetzte, die oder der Bundesbeauftragte und die Aufsichtsbehörde antragsberechtigt sind.

Bei relativen Antragsdelikten besteht die Möglichkeit, dass die Staatsanwaltschaft – unabhängig von der Stellung des Strafantrags durch die Betroffene – das besondere öffentliche Interesse annimmt. Dies kann sogar auch noch in der Hauptverhandlung erfolgen. Zwar bestimmt die sogenannte RistBV (Richtlinien für das Straf- und Bußgeldverfahren) in Nr. 86 zu häuslicher Gewalt, dass die Strafverfolgung ein gegenwärtiges Anliegen der Allgemeinheit ist, weshalb ein öffentliches Interesse an der Verfolgung einer Tat im Kontext von Partnerschaftsgewalt in der Regel anzunehmen ist. Faktisch erfolgt dies jedoch häufig nicht. Oder die Taten werden aus prozessökonomischen Gründen gemäß §§ 153/153a StGB, also mit oder ohne Auflage und ohne Feststellung einer Schuld eingestellt, da es sich um vermeintliche Bagatellen handelt. Die umfassenden Auswirkungen der digitalen Gewalt werden dabei häufig übersehen. Relative Antragsdelikte sind z.B. §§ 201a, 202a, 202b, 202d, 238 und 303a StGB.

In jedem Fall ist es wichtig, gerichtsfest zu dokumentieren, wann und in welcher Weise die betroffene Person von der Tat erfahren hat. Dafür ist es sinnvoll sämtliche Postings, Meinungsäußerungen, Kontaktaufnahmen etc. zu sichern. Gut ist es, so viele Screenshots wie möglich anzufertigen und möglichst alle Informationen, die Aufschluss auf die Verantwortlichen geben können zu dokumentieren.

Verfolgung sexualisierter digitaler Gewalt

Eine weit verbreitete Form der Bedrohung im Kontext von Hate Speech und in manchen Fällen von digitaler Gewalt im sozialen Nahraum ist die Androhung sexualisierter Gewalt. Erst seit der Neuregelung durch das Gesetz zur Bekämpfung von Rechtsextremismus und Hasskriminalität ist diese als Bedrohung im Sinne von § 241 StGB mit Strafe erfasst.

Uneinheitliche Auslegung Ehrdelikte

Letztlich kommt es grundsätzlich auf die Auslegung der Normen an. Gerade im Hinblick auf Hate Speech werden die Tatbestände dabei, sobald Personen des öffentlichen Lebens involviert sind, sehr restriktiv ausgelegt. Aufmerksamkeit hat in diesem Zusammenhang beispielsweise der Beschluss des Landgerichts Berlin (vgl. LG Berlin 2019) in Sachen der Beleidigungen gegen die Bundestagsabgeordnete Renate Künast erhalten. Dabei muss festgestellt werden, dass je mehr sich in der Gesellschaft der Eindruck verstärkt, es handele sich im Internet um einen rechtsfreien Raum, desto drastischer sich die Äußerungen zuspitzen, wodurch weiterhin die Gefahr besteht, dass auch juristisch die Grenze etwa der Schmähkritik weiter angehoben wird.

Grundsätzlich wäre es begrüßenswert, wenn die strafrechtlichen Regelungen zur digitalen Gewalt den Besonderheiten des Netzes angepasst würden. Im Hinblick auf Beleidigungsdelikte muss dabei berücksichtigt werden, dass diese aufgrund der Veröffentlichung dauerhaft für weitere Personen sichtbar sind und aufgrund der vielschichtigen Weiterverbreitungsmöglichkeiten sich oftmals einer Kontrolle durch die betroffenen Personen entziehen. Dabei muss bezüglich der Schwere der Verletzung berücksichtigt werden, dass Personen häufig durch die Taten in ihrem privaten aber auch beruflichen Umfeld diskreditiert werden, was zu ganz erheblichen persönlichen, beruflichen wie auch finanziellen Schäden führen kann. Auch sind Kinder von Betroffenen häufig indirekt verletzt, da sie etwa im Schulkontext mit beleidigenden oder verleumderischen Veröffentlichungen über ihre Mütter/Eltern konfrontiert werden.

Bagatelldelikte und Ermessenseinstellung

In der bisherigen Praxis (Stand 2020) werden die Verfahren wegen digitaler Gewalt meist eingestellt. Dabei wäre Voraussetzung für einen effektiven Schutz insbesondere, dass digitale Gewalt als Gewaltform anerkannt wird und nicht weiter unbeachtet oder bagatellisiert bleibt. Bisher werden Verfahren

häufig eingestellt, weil die Ermittlungsbehörden und Strafjustiz die Dimension der Verletzung nicht verstehen. Oft verkannt wird auch die reale Gefahr, die etwa von frauenverachtenden Hasskommentaren oder Bedrohungen ausgeht und die massiven Konsequenzen, denen Betroffene ausgesetzt sind wie etwa Arbeitsplatzverlust, posttraumatische Belastungsstörungen, Angst- und Panikattacken u.v.m. Häufig wird den Betroffenen bei Anzeigenerstattung der Ratschlag erteilt, sie sollten ihren Account einfach löschen oder die Passwörter ändern – dann sei das Thema beendet. Der gesamtpolitische Hintergrund wird meist ebenfalls nur in Ausnahmefällen erkannt und ermittelt. Dabei ist bei digitaler Gewalt im Vergleich zu physischer Gewalt nicht nur der Wirkkreis erheblich erhöht und praktisch grenzenlos, auch ist die Weiterverbreitung nicht kontrollierbar. Durch Hashtags werden einzelne Beiträge verknüpft und erweitern ihre Reichweite somit gegenseitig. Eine vergleichbare Wirkung hat das Liken oder Retweeten. Die Abgabe und Wahrnehmung von Äußerungen erfolgt binnen kürzester Zeit gegenüber eine unbestimmten Anzahl von Personen. Mit dem Ausspähen eines Telefons oder Computers können intimste Details über das Leben einzelner Personen herausgefunden werden, häufig mehr, als dies bei einem physischen Eindringen in die Wohnung betroffener Personen in so kurzer Zeit der Fall wäre.

Die falsche Einschätzung der Auswirkungen und Folgen digitaler Gewalt sowie die massiven Kapazitätsprobleme und Wissenslücken bei den Ermittlungsbehörden führen leider dazu, dass häufig mangelhaft ermittelt wird und Verfahren bereits deshalb mangels Tatverdacht eingestellt werden müssen. Unzählige Verfahren werden auch nach §153ff StPO eingestellt, sprich aus rein verfahrensökonomischen Gründen. Insofern gehen die Staatsanwaltschaft und/oder Gericht davon aus, dass eine Hauptverhandlung zur Wiederherstellung des Rechtsfriedens nicht notwendig sei oder die Erfüllung einer bestimmten Auflage ausreiche. Es ist grundsätzlich möglich, solche Auflagen auch in Form einer Teilnahme an bestimmten Kursen, Anti-Aggressionstherapien oder auch Schmerzensgeldzahlungen zu erteilen, oftmals werden jedoch nur geringe Geldauflagen an die Justizkasse verhängt. Da eine solche Einstellung nicht mit einer Verurteilung gleichzusetzen ist, führt dies bei der Geltendmachung von Schmerzensgeld und Schadensersatzansprüchen für die Betroffenen zu erheblichen Schwierigkeiten. Für viele Betroffene wäre eine Schuldfeststellung von erheblicher Bedeutung, auch in Bezug auf Gewaltschutzverfahren etc. Sie selbst können aber gegen eine solche Verfahrenseinstellung nichts unternehmen, sie erfolgt ausschließlich mit Zustimmung der angeklagten Person und der Staatsanwaltschaft.

Flankierende Maßnahmen

Neben der strafrechtlichen Verfolgung besteht die Möglichkeit, zivilrechtlich wegen Unterlassung und Löschung gegen den Täter vorzugehen. Aber auch ein Näherungs- und Kontaktverbot nach dem Gewaltschutzgesetz (GewSchG) ist denkbar. Ein Verstoß gegen eine erlassene Gewaltschutzverfügung führt sodann zu der Möglichkeit der strafrechtlichen Verfolgung oder Geltendmachung von sogenannten Ordnungsgeldern.

Das GewSchG erfasst in § 1 Abs. 1 GewSchG vorsätzliche Verletzungen des Körpers, der Gesundheit oder der Freiheit einer anderen Person. Digitale Gewalt wird nicht explizit aufgezählt. Zwar umfasst die »Gesundheit« im Sinne des § 1 GewSchG auch die psychische Gesundheit, so dass medizinisch feststellbare psychische Gesundheitsschäden jedenfalls bei einer erheblichen Beeinträchtigung Unterlassungsansprüche auslösen können. Problematisch wird aber so gut wie immer der Vorsatz, also Wissen und Wollen der Verletzung des geschützten Rechtsgutes, sein. Zwar genügt der bedingte Vorsatz, also das Wissen um einen möglichen Erfolg, der nicht erwünscht sein muss, aber billigend in Kauf genommen wurde aus (dolus eventualis), aber es muss bewiesen werden, dass der*die Täter*in die konkrete psychische Folge zumindest billigend in Kauf genommen hat und nicht nur fahrlässig verursacht hat. Bei Formen digitaler Gewalt, die körperliche Auswirkungen haben, ist der Bezug zum Gewaltschutzgesetz unproblematisch.

Erfasst ist digitale Gewalt jedoch im Rahmen von § 1 Abs. 2 GewSchG, der auf die Androhung der Verletzungen nach Abs. 1 abstellt sowie Nachstellung. Beides erfolgt häufig unter Verwendung digitaler Hilfsmittel. Größtes Problem ist hier, dass von den Gerichten der Erlass einer Anordnung abgelehnt wird, wenn die (digitalen) Kontaktaufnahmen über Dritte erfolgen. Fast immer versucht der*die Täter*in auch über das persönliche Umfeld der betroffenen Person Kontakt herzustellen, fordert etwa Familienmitglieder auf, Nachrichten zu übermitteln oder auf die Betroffene einzuwirken. Hintergrund ist, dass die Betroffene den*die Täter*in häufig bereits in allen Netzwerken und Accounts blockiert hat. Anders als § 238 StGB, der explizit auch Kontaktaufnahmen über Dritte erfasst, ist dieser Zusatz in § 1 Abs. 2 GewSchG nicht enthalten und wird von den Familiengerichten daher auch weit überwiegend nicht berücksichtigt.

Letztlich werden aber viele Formen der digitalen Gewalt nicht im GewaltSchG erfasst. Zum Beispiel Beleidigungsdelikte i.S.d. §§ 185ff StGB, wenn sie nicht unter Nachstellung fallen, genauso die Verbreitung intimer Auf-

nahmen (i.S.v. § 201a StGB oder auch §§106, 108 UrhG; §§ 33 i.V. 22, 23 KUG). Auch die Abnötigung eines bestimmten Verhaltens durch Androhung der Veröffentlichung intimer Fotos (gem. § 240 StGB) wird nicht erfasst. Ebenfalls nicht erfasst sind heimliche digitale »Nachstellungen«, wie das Ausspähen von Daten gem. § 202a StGB, Abfangen von Daten gem. § 202 b StGB bzw. Handlungen, die Strafvorschriften des Bundesdatenschutzgesetz erfüllen (vgl. § 42 BDSG) z.B., indem sogenannte Stalkerware bzw. Spy Apps auf dem Smartphone oder dem Rechner der betroffenen Personen installiert werden. Es wäre Aufgabe künftiger Lobbyarbeit, diese Ergänzungen zu erwirken.

Ausblick

Auch wenn die bisherigen Erfahrungen nicht sehr ermutigend erscheinen, so ist im Weiteren zu beobachten, inwiefern das Gesetz gegen Hasskriminalität und Rechtsextremismus Fortschritte bringt und die Betroffenen besser schützt. Wichtig wird aber vor allem, die Ermittlungspersonen zwingend darauf zu sensibilisieren, welche massiven Auswirkungen digitale Gewalt haben kann. Insbesondere im Licht der sogenannten Istanbul-Konvention (Übereinkommen des Europarats zur Verhütung und Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt) sind die besonderen Formen geschlechtsspezifischer digitaler Gewalt besonders zu bewerten und ggf. strikter zu verfolgen.[16] Auch muss die Rechtsprechung darauf sensibilisiert werden, dass gerade bei Zusammentreffen von analoger und digitaler Gewalt im persönlichen Nahraum für die Betroffenen weitere Auswirkungen und Diffamierungen in einem unübersichtlichen Wirkungskreis zu befürchten sind und damit die Betroffenen massiv unter Druck gesetzt werden können. Da sich gerade der Frauenhass, der Hass auf politische Gegner*innen und die Diffamierungen vielfältiger Lebensweisen vehement ausbreiten und häufig das Internet als propagandistischer Raum genutzt wird, ist es wichtig, diesem Phänomen möglichst zeitnah und effektiv entgegenzuwirken.

16 Siehe Beitrag: Menschenrechtlicher Schutzrahmen für Betroffene von digitaler Gewalt.

Literatur

Amann, Melanie/Deleja-Hotko, Vera/Rosenbach, Marcel (2019): »Digitales Vermummungsverbot. Schäuble drängt auf Klarnamen im Netz«. https://spiegel.de/netzwelt/netzpolitik/wolfgang-schaeuble-will-klarnamen-pflicht-im-internet-a-1267993.html [Zugriff: 3.9.2020].

Cremer, Hendrik (2010): »Ein Grundgesetz ohne »Rasse« – Vorschlag für eine Änderung von Artikel 3 Grundgesetz«, in: Deutsches Institut für Menschenrechte (Hg.). https://institut-fuer-menschenrechte.de/fileadmin/user_upload/Publikationen/Policy_Paper/policy_paper_10_und_welcher_rasse_gehoeren_sie_an.pdf [Zugriff: 14.9.2020].

Legal Tribune Online (2020): »OLG Köln: Verunglimpfung von Frauen kann Volksverhetzung sein«, in: Legal Tribune Online (LTO). https://lto.de/recht/nachrichten/n/olg-koeln-iii1rvs7720-volksverhetzung-minderheit-frauen-verunglimpfung-menschenwuerde-gleichheitssatz-diskriminierung-auslegung-tatbestand-130-stgb/ [Zugriff: 3.9.2020].

Mertins, Silke (2020): »Terroranklage wegen Frauenhass. Wenn Männer morden«. https://taz.de/Terroranklage-wegen-Frauenhass/!5684070/ [Zugriff: 3.9.2020].

o.A. (2020): »Prozess wegen Beleidigung von Sawsan Chebli. Gericht spricht Angeklagten frei«, in: Tagesspiegel https://tagesspiegel.de/berlin/prozess-wegen-beleidigung-von-sawsan-chebli-gericht-spricht-angeklagten-frei/25588164.html [Zugriff: 3.9.2020].

Sehl, Markus (2020): »Künast mit Teilerfolg gegen Hasspostings im Netz«, in: Legal Tribune Online. https://lto.de/recht/hintergruende/h/lg-berlin-27ar17-19-aendert-beschluss-kuenast-beleidigung-hass-posting-facebook-schmaehkritik/ [Zugriff: 3.9.2020].

Rechtsprechungsverzeichnis

AG: Amtsgericht Brandenburg (2016): Urteil vom 24.06.2016, Az. 34 C 39/16, in: Streit – Feministische Rechtszeitschrift, 01/2017, o.S.

BVerfG: Bundesverfassungsgericht (2009): Beschluss vom 04.11.2009, Az. 1 BvR 2150/08, Sammlung der Entscheidungen des Bundesverfassungsgerichts (BVerfGE) 124, S. 300-347 (330).

BVerfG: Bundesverfassungsgericht (2016): Stattgegebener Kammerbeschluss vom 17.05.2016, Az. 1 BvR 2150/14. https://bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/05/rk20160517_1bvr215014.html [Zugriff: 17.9.2020].

LG: Landgericht Berlin (2019): Beschluss vom 09.09.2019, 27 AR 17/19.

KG: Kammergericht Berlin (2017): Beschluss vom 18. Dezember 2017, (2) 161 Ss 104/17 (6/17), juris.

OLG: Oberlandesgericht Frankfurt (2019): Urteil vom 16.04.2019, 2 Ss 336/18, juris.

Saarländisches Oberlandesgericht Saarbrücken (2016): Urteil vom 05.10.2016, 5 U 3/16, juris.

Zivilrechtliche Interventionen bei digitaler Gewalt

Nadine Dinig

Einleitung

Der vorliegende Beitrag will verdeutlichen, dass neben den oftmals eher bekannten und genutzten strafrechtlichen Interventionen auch eine zivilrechtliche Möglichkeit[1] besteht, gegen digitale Gewalt vorzugehen. In den Monaten vor Redaktionsschluss des Buches ist die zivilrechtliche Vorgehensweise durch erste prominente Vorstöße und vor allem durch eine breite Medienresonanz vermehrt in der juristischen wie auch öffentlichen Diskussion angekommen (vgl. u.a. LG Berlin vom 02.09.2019; KG vom 11.03.2020). Wie dies im zivilrechtlichen Äußerungs- und Medienrecht regelmäßig der Fall ist, bedarf es jedoch bei neuen Fallgestaltungen und Problemfeldern einige Zeit, bis sich ein tragfähiges Fallrecht gebildet hat. Bis dafür notwendige höchstrichterliche Entscheidungen vorliegen, zeigen zuvor erlassene Gerichtsurteile oft unerwartete und auch sich widersprechende Auslegungen. Da zu erwarten ist, dass die derzeit vorliegenden Entscheidungen bis zur Veröffentlichung des Buches überholt sein werden, wird der vorliegende Beitrag nicht im Einzelnen auf diese eingehen, sondern vielmehr einen grundsätzlichen Überblick über das zivilrechtliche Vorgehen gegen digitale Gewalt anstreben.

Formen des zivilrechtlichen Vorgehens

Die Geltendmachung zivilrechtlicher Ansprüche lässt sich in außergerichtliches und gerichtliches Vorgehen unterteilen, wobei natürlich das außergerichtliche Vorgehen oftmals in das gerichtliche übergeht.

1 Die Ausführungen in diesem Text beziehen sich auf die Rechtslage mit Stand Juli 2020.

Abmahnung

Außergerichtlich können zivilrechtliche Ansprüche zunächst über eine Abmahnung geltend gemacht werden. Der Zweck einer Abmahnung ist es, gegenüber Verletzer*innen die Rechtswidrigkeit ihres Handelns anzuzeigen und sie aufzufordern, dieses zukünftig zu unterlassen. Ferner wird durch eine Abmahnung regelmäßig verdeutlicht, dass eine Person nicht gewillt ist, die Rechtsverletzung hinzunehmen, sondern vielmehr bereit, gegen diese rechtlich, unter Umständen auch gerichtlich, vorzugehen[2].

Mit einer Abmahnung werden regelmäßig Ansprüche auf Unterlassung, also die Aufforderung, die konkrete Äußerung oder Handlung zu unterlassen, geltend gemacht.[3] Hat bereits eine Verbreitung der betreffenden Äußerung oder des Bildmaterials stattgefunden, können Verletzer*innen ferner zur Folgenbeseitigung verpflichtet werden. Demnach müssen sie beispielsweise selbst dafür Sorge tragen, dass die entsprechenden Inhalte nicht mehr im Internet aufzufinden sind und entfernt werden.

Strafbewehrte Unterlassungserklärung

Zudem werden Verletzer*innen aufgefordert, eine sogenannte strafbewehrte Unterlassungserklärung abzugeben. In dieser verpflichten sich Verletzer*innen, die Äußerung oder Handlung zu unterlassen sowie für den Fall der Zuwiderhandlung eine Vertragsstrafe zu zahlen. Die Vertragsstrafe dient der Abschreckung und damit der Sicherung des Unterlassungsversprechens. In jedem Fall der schuldhaften Zuwiderhandlung gegen die Unterlassungsverpflichtung, also etwa bei einer erneuten Verbreitung der konkreten Äußerung bzw. Wiederholung der Handlung, wird eine Vertragsstrafe verwirkt. Daneben umfasst das Unterlassungsgebot auch sogenannte kerngleiche Verstöße, also etwa leicht abgewandelte Äußerungen. Betroffene haben es mithin in der Hand, bei Zuwiderhandlungen gegen die Unterlassungserklärung unverzüglich selbst gegen Verletzer*innen vorzugehen und die Zahlung der Vertragsstrafe zu fordern.

---

2 Die für dieses Vorgehen festzusetzenden Kosten schwanken erheblich und können nicht pauschal beziffert werden – sie hängen vom Gegenstandswert der Sache ab und werden anhand verschiedener Aspekte, z.B. bezüglich des Ausmaßes und Verbreitungsgrades, bemessen.

3 Auch wenn ein gerichtliches Verfahren angestrebt wird, ist eine vorherige Abmahnung in der Regel aus Kostengründen ratsam, da ansonsten bei einem sofortigen Anerkenntnis der Verletzer*innen den Antragsteller*innen die Kosten des Verfahrens auferlegt werden können.

Zur Unterlassung und Beseitigung der Handlung sowie der Abgabe einer strafbewehrten Unterlassungserklärung wird Verletzer*innen regelmäßig eine Frist gesetzt, gerade bei Taten oder Äußerungen im Internet kann diese Frist sehr kurz bemessen werden. Regelmäßig wird dabei eine Woche als ausreichend angesehen. Je nach Art des Mediums und der Schwere der Rechtsverletzung lassen sich jedoch auch deutlich kürzere Fristen, etwa von 24 bis 48 Stunden, gut argumentieren.

Ferner können Abgemahnte zugleich aufgefordert werden, die durch die Beauftragung einer Anwält*in entstandenen Kosten zu tragen.[4] Daneben können bereits im Abmahnschreiben Ansprüche auf Schadensersatz oder Geldentschädigung geltend gemacht werden. Regelmäßig ist hier eine Entscheidung im Einzelfall angezeigt, ob zunächst nur auf den Unterlassungsanspruch und dessen Durchsetzung abgestellt wird oder von Anbeginn sämtliche Ansprüche geltend gemacht werden.

Grundsätzlich ist es für Betroffene zwar möglich, eine Abmahnung selbst auszusprechen. Aufgrund der rechtlichen Vielschichtigkeit des zivilrechtlichen Vorgehens gegen Rechtsverletzungen im Bereich der digitalen Gewalt ist dies in der Regel jedoch nicht zu empfehlen. Zu beachten ist dabei insbesondere, dass eine Abmahnung den Grundstein für das weitere zivilrechtliche Vorgehen bildet und Fehler auf dieser Ebene in einem späteren gerichtlichen Verfahren fortwirken können. Erheblich ist dies vor allem im Hinblick auf die Beweissicherung, die regelmäßig nur im Vorfeld einer Abmahnung umfassend erfolgen kann. Also bevor Verletzer*innen Kenntnis von dem rechtlichen Vorgehen der Betroffenen erlangen.

Über anfallende Kosten und potentielle Unterstützungsleistungen informieren Anwält*innen in der Regel ausführlich beim Erstkontakt. Auch die Kosten der anwaltlichen Vertretung richten sich nach dem Gegenstandswert der Sache, sodass nur anhand des konkreten Falls Aussagen darüber getroffenen werden können, mit welchen Kosten Betroffene zu rechnen haben.

---

4 Eine Erstattung der Kosten eines Abmahnschreibens können von den Abgemahnten unter dem Gesichtspunkt der Geschäftsführung ohne Auftrag (§§ 670, 683 S. 1, 677 BGB) verlangt werden. Hierzu wird dem Abmahnschreiben üblicherweise eine Kostennote beigefügt. Wird die Erstattung verweigert, können die Kosten in einem gerichtlichen Verfahren eingeklagt werden.

Einstweilige Verfügung

Verweigern Verletzer*innen die Abgabe einer strafbewehrten Unterlassungserklärung, können Betroffene bei dem zuständigen Zivilgericht eine einstweilige Verfügung beantragen. Bei dem einstweiligen Verfügungsverfahren handelt es sich um ein Verfahren des einstweiligen Rechtsschutzes, das Rechtsverletzung schnell unterbinden kann und soll. Eine einstweilige Verfügung stellt einen vollstreckbaren Titel dar, gegen den im Fall der Zuwiderhandlung Ordnungsmittel, also Sanktionsmaßnahmen wie Ordnungsgeld, beantragt werden können. Aufgrund der Eilbedürftigkeit einer Angelegenheit kann ein einstweiliges Verfügungsverfahren, gerade eine aktive betriebene Antragstellung, relativ schnell durchgeführt werden.

Zu beachten ist dabei, dass der Antrag auf eine solche Verfügung nur innerhalb einer engen Frist gestellt werden kann. Diese Frist variiert teilweise bei den Gerichten, in der Regel ist jedoch von einem Monat seit Kenntnis der Rechtsverletzung auszugehen. Ferner unterliegt das einstweilige Verfügungsverfahren dem Grundsatz, dass es keine endgültige Regelung schaffen soll, also ein etwaiges Hauptsacheverfahren nicht vorwegnehmen darf. Deshalb können nur Unterlassungsansprüche, nicht aber Ansprüche auf Beseitigung, Schadensersatz oder Geldentschädigung in diesem Verfahren geltend gemacht werden.

Ein Gericht kann in einem einstweiligen Verfügungsverfahren eine Unterlassungsverfügung zwar ohne mündliche Verhandlung erlassen, in der Regel ist jedoch kurzfristig ein entsprechender Termin einzuräumen, aufgrund dessen das Gericht entweder die Unterlassungsverfügung erlässt oder den Antrag auf diese zurückweist.

Hauptsacheverfahren

Da die Ansprüche auf Beseitigung, Schadensersatz und Geldentschädigung nur in einem Hauptsacheverfahren geltend gemacht werden können, kann es sich auch empfehlen, ohne vorheriges Verfügungsverfahren Klage gegen die Rechtsverletzung zu erheben. Sinnvoll kann dies auch sein, wenn davon ausgegangen wird, dass Verletzer*innen eine einstweilige Verfügung nicht anerkennen und daher jedenfalls das Hauptsacheverfahren betreiben werden. Der Nachteil des Hauptsacheverfahrens liegt offensichtlich in der Verfahrensdauer. Für eine rasche Unterbindung einer Rechtsverletzung ist dieses Verfahren ungeeignet, da bereits für die erste Instanz in der Regel von einer Verfahrensdauer von mindestens einem Jahr zu rechnen ist.

Vor- und Nachteile des zivilrechtlichen Vorgehens

Betroffene entscheiden über das Verfahren

Ein entscheidender Vorteil des zivilrechtlichen Verfahrens ist, dass Betroffene sowohl außergerichtlich als auch gerichtlich die Kontrolle über das Verfahren haben. Entgegen dem strafrechtlichen Vorgehen entscheiden Betroffene selbst, ob und wie sie das Verfahren betreiben. Mithin kann das Verfahren nicht wie im Strafrecht von staatlicher Seite eingestellt oder gegen den Willen der Betroffenen betrieben werden. Dementsprechend haben Betroffene auch die Wahl, das Verfahren (nur) außergerichtlich oder auch bzw. ausschließlich vor Gericht zu führen.[5]

Geringere Hürden in der Durchsetzung von Unterlassungs- und Beseitigungsansprüchen

Ferner können in einem zivilrechtlichen Verfahren Handlungen verfolgt werden, die kein strafrechtlich relevantes Verhalten darstellen, beispielsweise nicht die Schwelle zur Beleidigung oder Verleumdung im strafrechtlichen Sinn überschreiten. Dabei sind die zur Beendigung einer Rechtsverletzung notwendigen Unterlassungs- und Beseitigungsansprüche verschuldensunabhängig. Das heißt für die Durchsetzung zivilrechtlicher Ansprüche ist es nicht relevant, ob etwa bestimmte Äußerungen mit der Absicht getätigt worden sind, einer Person Schaden zuzufügen oder ob die äußernde Person wusste, welche Auswirkungen diese Äußerungen haben. Somit sind Unterlassungs- und Beseitigungsansprüche meist leichter durchsetzbar als Strafanzeigen, die auch den subjektiven Tatbestand, also den Vorsatz, eines Delikts erfüllen müssen.

Schnelle Durchsetzung

Gerade bei Rechtsverletzungen im Internet kann die Durchsetzung zivilrechtlicher Unterlassungs- und Beseitigungsansprüche zudem sehr schnell erfol-

5 Vorsorglich ist auch darauf hinzuweisen, dass eine Person, die sich mit einem aus ihrer Sicht ungerechtfertigten Anspruch konfrontiert sieht, auch ihrerseits eine zivilrechtliche Klärung anstreben kann. Im Fall einer Abmahnung kann beispielsweise eine Klage erhoben werden, um festzustellen, dass der mit der Abmahnung geltend gemachte Anspruch nicht besteht. In einem gerichtlichen Verfahren besteht nach einem Obsiegen in einer Instanz immer die Möglichkeit, dass die andere Partei nicht gewillt ist, die Entscheidung gegen sich gelten zu lassen und das Verfahren von sich aus weiter betreibt.

gen und damit die Verbreitung einer Rechtsverletzung frühzeitig und effektiv unterbinden. Wie beschrieben, gibt das Verfahren Betroffenen zudem die Möglichkeit, die Einhaltung der Unterlassungs- und Beseitigungspflicht aufgrund einer strafbewehrten Unterlassungserklärung oder eines gerichtlichen Titels selbst zu überwachen und im Zweifelsfall entsprechende Sanktionen einzuleiten.

Schwer abzuschätzende Kostenfolge

Offensichtlicher Nachteil des zivilrechtlichen Verfahrens ist die Kostenfolge. Hier müssen Betroffene die Kosten des Verfahrens, jedenfalls zunächst, selbst tragen. Auch besteht das Kostenrisiko bei einem Unterliegen. In diesem Fall wären auch die Kosten der Gegenseite zu erstatten. Zwar kann in einem zivilgerichtlichen Verfahren zudem Schadensersatz bzw. eine Geldentschädigung gefordert werden, die Höhe der hier einklagbaren Beträge sollte jedoch nicht überschätzt werden.

Sachverhalt wird nicht durch das Gericht ermittelt

Auch ist darauf hinzuweisen, dass ein zivilrechtliches Verfahren in der Regel nur dann betrieben werden kann, wenn die handelnden Personen namentlich bekannt sind. Die Möglichkeit einer Anzeige gegen unbekannt, wie das Strafrecht sie kennt, besteht also nicht. Da das Zivilrecht zudem nicht dem Amtsermittlungsgrundsatz unterliegt, erfolgt auch keine Ermittlung der Person oder des Sachverhalts des Falls von staatlicher Seite, d.h. die betroffene Person muss beispielsweise Realnamen von Internetuser*innen und Adresse selbst ermitteln.

Da das Zivilverfahren von den Parteien betrieben wird, ist es zudem auch für Betroffene weder außergerichtlich noch gerichtlich möglich, anonym zu bleiben.

Rechtliche Grundlagen der zivilrechtlichen Intervention

Ein zivilrechtliches Vorgehen gegen digitale Gewalt ist vor allem nach den Regelungen des Deliktsrechts möglich. Das Deliktsrecht ermöglicht Personen, sich gegen sogenannte unerlaubte Handlungen zu wehren, die Schutzgüter

im Sinne der §§ 823ff. BGB verletzen.[6] Zunächst ist über § 823 Abs. 2 BGB möglich, insbesondere gegen solche Handlungen und Äußerungen, die auch strafrechtliche Tatbestände erfüllen, zivilrechtliche Ansprüche geltend zu machen. Insbesondere betrifft dies die strafrechtlichen Normen der §§ 185ff. (Beleidigungs- und Ehrdelikte), § 201a (Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen), § 238 (Nachstellung), §§ 240 f. StGB (Nötigung und Bedrohung) sowie Verletzungen des Rechts am eigenen Bild (§§ 22 S. 1, 23 II KUG). Dabei ist im Gegensatz zum Strafrecht regelmäßig die objektive Rechtswidrigkeit eines Verhaltens ausreichend, um einen Unterlassungsanspruch zu begründen. Es kommt somit nicht auf die strafrechtlichen Verschuldensvoraussetzungen an, wodurch die Rechtsdurchsetzung erleichtert wird.

Dagegen kann nach § 823 Abs. 1 BGB zivilrechtlich auch gegen solche Handlungen und Äußerungen vorgegangen werden, die keinen Straftatbestand erfüllen, aber ein Schutzgut der Norm verletzen. Als wichtigstes Schutzgut für das Feld der digitalen Gewalt ist dabei das Allgemeine Persönlichkeitsrecht zu nennen, auf das aus diesem Grund im Folgenden kurz einzugehen ist.

Allgemeines Persönlichkeitsrecht

Als Ausprägung der verfassungsrechtlichen Prinzipien der Unantastbarkeit der Menschenwürde und des Rechts auf freie Entfaltung der Persönlichkeit (Art. 1 und 2 GG) stellt das Allgemeine Persönlichkeitsrecht bestimmte Aspekte der Persönlichkeitsentfaltung einer Person und ihrer Selbstbestimmtheit unter einen speziellen grundrechtlichen Schutz.

Als sonstiges Recht im Sinne des § 823 Abs. 1 BGB handelt es sich bei dem Allgemeinen Persönlichkeitsrecht um einen offenen Tatbestand, der keinen abschließenden Inhalt hat. Seine Ausprägung ist vielmehr jeweils anhand des konkreten Falls zu ermitteln und bei seiner Auslegung und Anwendung im Rahmen einer Güterabwägung mit widerstreitenden Grundrechten, bei Äußerungen etwa regelmäßig der Meinungsfreiheit, in Einklang zu bringen (vgl. Soehring/Hoene 2019: § 19, Rn. 2a). In der Rechtsprechung sind derzeit u.a. folgende Ausprägungen des Allgemeinen Persönlichkeitsrechts als Fallgruppen anerkannt, die für das Vorgehen gegen digitale Gewalt den Schwerpunkt

6 Vorliegend wird nur auf § 823 BGB eingegangen, da dieser den Schwerpunkt des zivilrechtlichen Vorgehens gegen digitale Gewalt bildet.

bilden: das Recht am eigenen Bild, das Recht auf informationelle Selbstbestimmung, das Recht auf Privatheit, der Schutz vor Unwahrheit, der Schutz von Ehre und Ruf und der Schutz vor Gefährdung von Leben und Freiheit.

Diese Fallgruppen sind jedoch nicht abschließend, sondern in der Rechtsprechung gerade im Hinblick auf die technischen und medialen Entwicklungen der letzten beiden Jahrzehnte in ständigem Wandel.[7] In der Praxis überschneiden sich die von der Rechtsprechung gebildeten Fallgruppen oftmals. Sämtliche Fallgruppen erfahren zudem seit kurzem zusätzlichen Schutz über die datenschutzrechtlichen Regelungen des Zivilrechts.

Folgende Ausprägungen sind im Bereich der digitalen Gewalt regelmäßig einschlägig:

Schutz des Rufs und der Ehre

Eine der wichtigsten Ausprägungen des Allgemeinen Persönlichkeitsrechts ist das Recht auf soziale Anerkennung und Wertschätzung einer Person. In der Rechtsprechung wird dabei vom Schutz der Ehre und des Rufs einer Person gesprochen, wobei Ehre im Sinne der durch Art. 1 GG jedem Menschen garantierten Menschenwürde, die den unabänderlicher Statuts jeder Person auch Strukturen und Einrichtungen, die bei geschlechtsspezifischer darstellt, zu verstehen ist.

Verletzt wird dieses besondere Persönlichkeitsrecht durch Äußerungen oder Bildmaterial, die darauf abzielen, eine Person zu diffamieren, verächtlich oder lächerlich zu machen, ohne dass die Aussage in einem sachlichen Zusammenhang steht (sogenannte Schmähkritik) (vgl. BVerfG, NJW 1993: 1462). Dabei ist die Form einer Äußerung unerheblich und kann auch beispielsweise über eine Textnachricht, in einem geschlossenen Forum oder einem Chat erfolgen (vgl. BGH, MMR 2016: 849; OLG Dresden MMR 2017: 704).

7 In den letzten Jahren wurde etwa das Recht auf informationelle Selbstbestimmung um den Schutz der Persönlichkeit vor Kommerzialisierung erweitert. Bisher noch wenig durch die Rechtsprechung konkretisiert ist die Fallgruppe des Rechts von Kindern auf ungehinderte Entfaltung ihrer Persönlichkeit und ungestörte kindgemäße Entwicklung, also das Recht jedes Kindes auf ungehinderte Entwicklung zu einer Persönlichkeit, also darauf, eine »Person zu werden« (vgl. Wenzel u.a. 2018: Kap. 5, Rn. 175f.).

Recht auf Privatheit

Das Recht auf Privatheit wurde im Lauf der Rechtsprechung in verschiedene Bereiche unterteilt, die jeweils ein unterschiedliches Schutzniveau genießen.[8]

Gerade im Bereich der Beziehungsgewalt wird oftmals der am stärksten gegen Eingriffe Dritter geschützte Bereich, die Intimsphäre, betroffen sein (vgl. Wenzel u.a. 2018: Kap. 5, Rn. 47; Soehring/Hoene 2019: § 19, Rn. 4). Informationen über eine Person, die der Intimsphäre zuzurechnen sind, sind absolut geschützt. Die Person kann also verlangen, dass andere diese nicht ohne ihre Zustimmung an Dritte weitergeben oder veröffentlicht werden. Hierzu zählen u.a. die sexuelle Orientierung einer Person, Einzelheiten über sexuelle Beziehungen (vgl. EGMR, NJW 2012: 747; BGH AfP 1988: 34; BGH, NJW 1974: 1947), Erkrankungen, die für die Öffentlichkeit nicht erkennbar sind (vgl. KG, AfP 2009: 418), Details medizinischer Untersuchungen (vgl. OLG Hamburg, UFITA 1978: 278), nicht öffentlich gelebte Beziehungen (vgl. Soehring/Hoene 2019: § 19, Rn. 5), Gründe für das Scheitern einer Beziehung (vgl. BGH, AfP 1999: 350), Nacktaufnahmen oder Filmaufnahmen schlafender oder bewusstloser Personen (vgl. OLG Karlsruhe, AfP 1999: 489). Eine Einschränkung des absoluten Schutzes kann sich in der Regel nur dann ergeben, wenn die Person selbst die öffentliche Diskussion über einen bestimmten Aspekt ihrer Intimsphäre eröffnet hat.

Die zweite Schutzstufe, die Privatsphäre, beschreibt den Bereich im Leben einer Person, zu dem andere nur Zugang haben, wenn ihnen dieser gewährt wird. Dabei wird der Schutzbereich räumlich und thematisch bestimmt (vgl. BGH, AfP 1996: 140; Wenzel u.a. 2018: Kap. 5, Rn. 54). Dies betrifft insbesondere alle Vorgänge und Lebensäußerungen innerhalb des häuslichen und familiären Bereichs einer Person, aber auch andere Orte und Thematiken, bei denen das berechtigte Interesse auf Privatheit besteht (vgl. Wenzel u.a. 2018: Kap. 5, Rn. 56). Zur Privatsphäre gehören u.a. die Adresse, Telefonnummer, Fotos des Wohnhauses (vgl. KG, AfP 2008: 396), Beziehungsstatus,

8 Im allgemeinen Presse- und Medienrecht ist diese Abgrenzung oftmals von erheblicher Bedeutung, wenn es um die Zulässigkeit der Berichterstattung über prominente Personen, insbesondere in der Boulevardpresse geht. Je nach Sphäre, in welche die Berichterstattung der Medien eingreift, kann eine Rechtfertigung etwa aufgrund des öffentlichen Interesses an bestimmten Lebensereignissen oder Verhaltensweisen in der Öffentlichkeit stehender Personen begründet werden. Bei Privatpersonen wird eine solche Rechtfertigung regelmäßig misslingen, insbesondere, wenn die Veröffentlichung einer Information oder eines Fotos ebenfalls durch eine Privatperson erfolgt ist.

soweit eine Beziehung öffentlich gelebt wird, gesundheitliche Probleme, Erkrankungen, Aufenthalte in Krankenhäusern etc. (vgl. BGH, AfP 1996: 137), Elternschaft eines Kindes, Einkommens- und Vermögensverhältnisse, private Gespräche (vgl. BGH, NJW 1981: 1366), familiäre Auseinandersetzungen, religiöse und weltanschauliche Überzeugungen, (Nicht-)Zugehörigkeit zu religiösen Gemeinschaften (vgl. Soehring/Hoene 2019: § 19, Rn. 18), oder die passive Zugehörigkeit zu einer Partei (vgl. BGH, NJW 2012: 771). Eine Verletzung der Privatsphäre kann beispielsweise bei einer Videoüberwachung eines Hauseingangs oder sonstiger Bereiche eines Privatgrundstücks, ohne dass die betroffene Person hiervon Kenntnis hat, vorliegen (vgl. BGH, AfP 2010: 257).[9]

Noch weiter eingeengt ist der Schutz der Sozialsphäre. Diese betrifft den Lebensbereich einer Person, der nach außen in Erscheinung tritt und dabei von anderen Menschen wahrgenommen werden kann, selbst wenn zu diesen keine persönliche Beziehung besteht (vgl. Wenzel u.a. 2019: Kap. 5, Rn. 65). Geschützt ist also die Person als Teil einer sozialen Gemeinschaft und zwar auch davor, mit einer größeren Öffentlichkeit als der von ihr gewählten Öffentlichkeit konfrontiert zu werden (vgl. BGH, NJW 1981: 1366). Dementsprechend ist das Schutzniveau in dieser Sphäre relativ und oftmals davon abhängig, wie öffentlich eine Information bereits aufgrund des Verhaltens einer Person ist. Geschützt sind jedoch insbesondere Aussagen Dritter gegenüber Personen, denen die Person selbst diese Informationen nicht zukommen lassen wollte wie etwa gegenüber Lehrer*innen, Arbeitgeber*innen oder Vermieter*innen. Gerade solche Mitteilungen, deren (gezielte) Verbreitung bezweckt, einer Person zu schaden oder sie bloß zu stellen, können eine Verletzung der Sozialsphäre darstellen, obgleich die Informationen eigentlich nicht geheim sind. Hierzu zählen u.a. berufliche oder gewerbliche Tätigkeit (vgl. BGH, NJW 2012: 767), politische Betätigung, Anwesenheit bei öffentlichen Veranstaltungen oder strafrechtliche Ermittlungsverfahren, Mitteilung etwa an Arbeitgeber in der Regel unzulässig (vgl. OLG Düsseldorf, AfP 1992: 369).

Kein Schutz auf Privatheit im Rahmen des Allgemeinen Persönlichkeitsrechts ergibt sich für Aspekte, die der Öffentlichkeitsphäre zugerechnet werden. Diese umfasst den Bereich des menschlichen Lebens, der grundsätzlich allen anderen Menschen zugänglich ist, in dem die Person also bewusst in

9 Unter Umständen kann ein Anspruch auf Unterlassung solcher Aufnahmen bereits bestehen, wenn eine solche Videoüberwachung ernsthaft zu befürchten steht.

die Öffentlichkeit tritt (vgl. Wenzel u.a. 2018: Kap. 5, Rn. 65). Zur Öffentlichkeitsphäre zählen regelmäßig öffentlich zugängliche Internetseiten, öffentliche Profile in sozialen Netzwerken oder Kommentare in sozialen Netzwerken, wenn der kommentierte Beitrag öffentlich ist.

Zu beachten ist mithin, dass eine Person sich durch ihr Verhalten den Schutz auf Privatheit vergeben kann. Entscheidet sich eine Person etwa, ihr Profil in sozialen Medien oder ihre Internetseite ohne Einschränkung öffentlich zugänglich zu machen, kann argumentiert werden, dass sie ihr Recht auf Privatheit im Hinblick auf die dort veröffentlichten Inhalte nicht geltend machen möchte (vgl. EGMR, AfP 2004: 348; OLG München, GRUR-RR 2016: 304); andere dort nicht veröffentlichte Informationen wären aber weiterhin geschützt. In der Rechtsprechung zeichnet sich diesbezüglich ein strenges Verständnis gegenüber Nutzer*innen sozialer Medien ab. Die Gerichte gehen wohl überwiegend davon aus, dass eine Person zumindest im Hinblick auf die von ihr selbst zu kontrollierenden Bereiche wie eigene Profilseiten über ihr Recht auf Privatheit entscheiden kann und dies mit den von ihr vorgenommen Einstellungen auch tut. Die von den sozialen Netzwerken angebotenen Einstellungen zur Privatsphäre sowie ihre Umsetzung werden dabei als bekannt vorausgesetzt. Es kann deshalb für Ansprüche, die auf das Recht auf Privatheit gestützt werden entscheidend sein, dass nachgewiesen werden kann, dass eine Person entsprechende Einstellungen zum Schutz ihrer Privatsphäre vorgenommen hat.

Unabhängig von den oben genannten Sphären kann ein Recht auf Privatheit bei der Vertraulichkeitssphäre anerkannt werden, also bei dem Bereich der Persönlichkeit, der aufgrund des erkennbaren Willens der Person geschützt ist. Teilweise kann sich dies aus dem erkennbar vertraulichen Charakter einer Information ergeben, jedenfalls aber bei einem klar zutage tretenden Willen der Person, wie etwa dem Hinweis auf Vertraulichkeit oder durch entsprechende Sicherung von Daten. Insbesondere in letzterem Fall können Aspekte aus sämtlichen oben genannten Sphären unter die Vertraulichkeitssphäre fallen. Hierunter fallen beispielsweise aus dem Charakter der Information insbesondere Inhalt von persönlichen Briefen, E-Mails, SMS-Nachrichten, private Facebook- oder WhatsApp-Chatverläufe (vgl. BGH 1954, BGHZ 15: 249; BGH, AfP 2016: 149; EGMR, AfP 2004: 348; OLG Köln, NJOZ 2016: 245; LG Köln, CR 2016: 48; KG, ZUM 2011: 145), Aufzeichnungen oder Mithören vertraulicher Telefonate, Tagebuch oder sonstige private Aufzeichnungen, von der Person angefertigte Bild- und Tonaufnahmen, auch wenn diese mit ihrer Kenntnis gefertigt, jedoch ohne ihre Zustimmung verbreitet

wurden (vgl. BGH, AfP 1987: 508) oder auf technischen Geräten gespeicherte Informationen, die entwendet wurden.

Recht auf informationelle Selbstbestimmung

Das Recht auf informationelle Selbstbestimmung umfasst das Recht einer Person grundsätzlich selbst zu entscheiden, ob und innerhalb welcher Grenzen ihr Lebensbild, persönliche Lebenssachverhalte oder Meinungen durch andere öffentlich dargestellt oder offenbart werden dürfen (vgl. BVerfG, NJW 1973: 1226; BVerfG 1983, BVerfGE 65: 42f.; BGH, AfP 2014: 534, 536). Im Kern schützt das Recht auf informationelle Selbstbestimmung damit die Individualität einer Person, insbesondere im Hinblick auf die wahrheitsgemäße Darstellung der eigenen Person (vgl. BGH, AfP 2014: 534, Rz. 15) sowie das Recht einer Person auf Achtung ihrer Privatsphäre (vgl. Wenzel u.a. 2018: Kap. 5, Rn. 17).

Eine Person kann sich daher unter Berufung auf das Recht auf informationelle Selbstbestimmung dagegen wehren, dass ihre Persönlichkeit verzerrt, unterkomplex oder in wesentlicher Hinsicht falsch dargestellt wird. Für eine Verletzung ist es dabei nicht notwendig, dass eine solche Fremddarstellung rufschädlich ist. Zu beachten ist jedoch, dass das Recht der informationellen Selbstbestimmung nicht als allgemeines Verfügungsrecht über die Darstellung der Person durch andere zu verstehen ist, insbesondere lässt sich daraus kein Anspruch herleiten, in der Öffentlichkeit nur so dargestellt zu werden, wie eine Person sich selbst sieht oder von anderen gesehen werden möchte (vgl. BVerfG, NJW 1999: 1322; BVerfG, AfP 2000: 76). Auch das Recht auf informationelle Selbstbestimmung schützt ferner das Interesse daran, dass der Inhalt schriftlicher privater Nachrichten nicht an die Öffentlichkeit gelangt (vgl. BVerfG 2006, BVerfGE 115: 83f., 187ff.; EGMR, EuGRZ 2007: 415). Derzeit noch nicht abschließend geklärt ist dabei, welcher Schutz persönlichen Nachrichten in sozialen Netzwerken zukommt (vgl. BGH, GRUR 2015: 92; OLG Köln, NJOZ 2016: 245).[10]

10 Teilweise wird vertreten, dass bei Nachrichten in sozialen Netzwerken bewusst ein Kommunikationsweg gewählt werde, der weniger vertrauenswürdig sei als etwa ein Brief, da die Nachricht etwa nicht in gleichem Maße gegen den Zugriff von dritter Seite geschützt sei bzw. Dritten leichter zugänglich gemacht werden könne. Mithin könne solchen Nachrichten nicht der gleiche Schutz zukommen. Da jedoch nach Auffassung des Bundesgerichtshofs jedenfalls E-Mails Briefen gleichzusetzen sind, ist richtigerweise davon auszugehen, dass der Schutz der Kommunikation unabhängig vom

Insbesondere durch den technischen und medialen Wandel wurde das Recht auf informationelle Selbstbestimmung in den vergangenen Jahren durch die Rechtsprechung weiter ausgebaut. Spezialgesetzliche Regelungen sind zudem mittlerweile in den datenschutzrechtlichen Regelungen des Zivilrechts kodifiziert. Verletzungen des Rechts auf informationelle Selbstbestimmung können insbesondere sein: permanente Beobachtung sowie Erstellung von Bildaufnahmen, etwa um ein Bewegungsbild der Person zu erstellen (vgl. BGH, AfP 1995: 597), Veröffentlichung des Wohnsitzes, der Telefonnummer etc. (vgl. BGH, AfP 2004: 119), Weitergabe personenbezogener gespeicherter Daten (vgl. BGH, NJW 1984: 1886) oder Veröffentlichung von Daten zuvor entwendeter technischer Geräten wie Laptops, Telefone, Tablets etc.

Auch das »Recht am gesprochenen Wort« ist ein Unterfall des Rechts auf informationelle Selbstbestimmung. Geschützt ist dabei laut dem Bundesverfassungsgericht die Selbstbestimmung über die eigene Darstellung der Person in der Kommunikation sowie das Kommunikationsverhalten, insbesondere im Hinblick darauf, mit wem die Kommunikation geführt wird, also nur mit einer Person, mit einer Gruppe oder mit der Öffentlichkeit (vgl. BVerfG, AfP 1980: 149; BVerfG, NJW 2002: 3619). Da Gegenstand des Schutzes die Selbstbestimmung der sprechenden Person über das Gesagte ist, ist unerheblich, über was gesprochen wird, ob es sich also um vertrauliche oder belanglose Gesprächsinhalte handelt. Entscheidend ist vielmehr, ob eine Person nach den Umständen des Gesprächs darauf vertrauen durfte, dass ihr die Zuhörenden bekannt sind.

Verletzungen des Rechts am gesprochenen Wort stellen daher insbesondere das Mithören oder Aufzeichnen von Gesprächen ohne Kenntnis der Person oder technische Manipulationen von Gesprächsmitschnitten dar, etwa wenn Aufzeichnungen der Stimme einer Person neu kontextualisiert werden, um ihnen einen anderen Inhalt zu geben sowie Kürzungen, Veränderungen etc. Strittig ist derzeit noch, ob Telefonate ebenso wie persönliche Gespräche

---

gewählten Kommunikationsmittel gewährt wird, insbesondere wenn der vertrauliche Charakter der Kommunikation offensichtlich ist.

geschützt sind.[11] Auch Handlungen nach § 201 StGB (Verletzung der Vertraulichkeit des Wortes) fallen unter dieses Schutzgut.

Schutz vor Unwahrheit

Das Allgemeine Persönlichkeitsrecht schützt eine Person auch davor, dass beeinträchtigende unwahre Aussagen über sie aufgestellt werden. Eine Verletzung liegt dann vor, wenn die unwahre Tatsachenbehauptung dem sozialen Geltungsanspruch widersprechen oder das Lebensbild einer Person in der Öffentlichkeit beeinträchtigt (vgl. BVerfG, NJW 1980: 2070; BVerfG, NJW 1999: 1322).

Dies ist regelmäßig der Fall bei verfälschenden und/oder entstellenden Darstellungen einer Person, Unterstellung einer nicht getätigten Äußerung, falschen Verdächtigungen, technischer Manipulation von Bildmaterial, das nicht als Manipulation zu erkennen ist oder verfälschte Wiedergabe des gesprochenen oder geschriebenen Wortes (vgl. BVerfG 1980: 2070; BGH, NJW 1965: 685). Strafrechtlich ähnelt diese Ausprägung des Allgemeinen Persönlichkeitsrechts weitgehend dem Tatbestand der üblen Nachrede, § 186 StGB.

Recht am eigenen Wort

Das Recht am eigenen Wort schützt eine Person davor, dass ihr Äußerungen zugeschrieben werden, die sie nicht getätigt hat und die geeignet sind, ihre Privatsphäre und den von ihr selbst definierten sozialen Geltungsanspruch zu beeinträchtigen. Dies betrifft insbesondere Fehlzitate, aber auch die unrichtige, verfälschte oder entstellte Wiedergabe einer Äußerung (vgl. BVerfG, NJW 1993: 2925; BVerfG AfP 2013: 49).

Ansprüche gegen Veröffentlichungen und Verbreitungen von Bildmaterial

Als besondere Ausprägung des Allgemeinen Persönlichkeitsrechts gewährt das »Recht am eigenen Bild« allen natürlichen Personen das ausschließliche Recht, über die Verbreitung und öffentliche Zurschaustellung ihres Bildnisses

11 Teilweise wird im Hinblick auf Telefonate argumentiert, dass die Person bewusst einen Kommunikationsweg gewählt habe, der ihr die Kontrolle über die Zuhörenden nicht bieten könne. Auch die mit dieser Argumentation verbundene Einschränkung des Persönlichkeitsrechts ist abzulehnen. Auch bei einem Telefongespräch darf eine Person darauf vertrauen, nur von Personen gehört zu werden, die ihrer Kenntnis nach an dem Gespräch teilnehmen. Kann sich eine Person im Hinblick auf den Inhalt des Gesprächs auf ihr oben dargestelltes Recht auf Privatheit berufen, ist das Gespräch zudem bereits unter diesem Aspekt des Allgemeinen Persönlichkeitsrechts geschützt.

zu entscheiden (vgl. BVerfG, AfP 1998: 192ff.; BGH, BGHZ 20: 347; BGH, NJW 1979: 2205; BGH, AfP 1996: 137; EGMR, AfP 2015: 137).[12] Einfachgesetzlich geregelt ist das Recht am eigenen Bild zudem in den §§ 22, 23 des Gesetzes betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (KUG).[13]

Der Schutzzweck des § 22 KUG besteht mithin nach allgemeinem Verständnis darin, die Persönlichkeit der Einzelnen davor zu bewahren, gegen ihren Willen in Gestalt einer Abbildung für andere verfügbar zu werden. Personen sollen über ihre Privatsphäre entscheiden und dabei auch den Schutz der Anonymität in Anspruch nehmen können. Bildnisse einer Person dürfen deshalb gem. § 22 Satz 1 KUG grundsätzlich nur mit Einwilligung der Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Zudem können solche Handlungen die Verletzungen anderer Ausprägungen des Allgemeinen Persönlichkeitsrechts darstellen.

An die Wiedergabe des Erscheinungsbilds der Person stellt die Rechtsprechung dabei keine allzu hohen Anforderungen. So können auch teilweise Darstellungen einer Person, eine Rückenaufnahme oder auch nur die Abbildung einer Silhouette ausreichend sein.[14] Dabei muss die Person zwar erkennbar sein, wobei es aber auf ein tatsächliches Erkanntwerden nicht ankommt. Ausreichend ist vielmehr, dass eine begründete Sorge besteht, dass die abgebildete Person von ihrem Freundes- und Bekanntenkreis erkannt werden könnte, eine Identifizierung durch die Allgemeinheit ist hingegen nicht notwendig (vgl. BGH, GRUR 1962: 211; BGH vom 26.06.1979). Unerheblich ist auch, aufgrund welcher Umstände einer Identifizierbarkeit der Person vorliegt (z.B. durch Gesichtszüge oder besondere körperliche Merkmale wie Tätowierungen), aber auch aus den Umständen oder einem Begleittext zu dem Bildnis ergeben. Die identifizierenden Umstände können also auch außerhalb des Bildnisses liegen oder sich lediglich in Zusammenhang mit diesem ergeben.

12 Der EGMR hat festgestellt, dass das Bild einer Person eines der wichtigsten Elemente ihrer Persönlichkeit darstellt, da es ihre besonderen Eigenschaften zeigt und sie von anderen unterscheidet.

13 Daneben ergibt sich aus § 33 KUG auch die Strafbarkeit für die Verbreitung und öffentliche Zurschaustellung von Bildnissen ohne wirksame Einwilligung der abgebildeten Person. Die Straftat wird jedoch nur auf Antrag der betroffenen Person verfolgt. Strafrechtlich kann zudem eine Verletzung des höchstpersönlichen Lebensbereichs, § 201a StGB, vorliegen.

14 Diskussionswürdig ist hingegen, ob die Abbildung einzelner Körperteile als ausreichend anzusehen ist.

Bei Beiträgen in sozialen Netzwerken kann eine Identifizierbarkeit auch aufgrund einer entsprechenden Markierung oder Zuordnung zu einem anderen Beitrag entstehen.

Tathandlungen

Als Tathandlungen nennt § 22 KUG die Verbreitung und die öffentliche Zurschaustellung von Bildnissen. Ein Verbreiten liegt nach Auffassung der Rechtsprechung jedenfalls bei jeder Art der Weitergabe körperlicher Exemplare des Bildnisses vor. Derzeit noch nicht höchstrichterlich entschieden ist, ob auch die Weitergabe eines Bildnisses in digitaler Form als tatbestandsmäßig im Sinne des § 22 KUG anzusehen ist. Nach Sinn und Zweck des § 22 KUG ist hiervon jedoch auszugehen (vgl. OLG Frankfurt vom 23.12.2008: Rz. 23; Höning 2012: 133). Entscheidend ist dabei, dass das Bildnis in digitaler Form den Herrschaftsbereich der Person verlässt, die es hochlädt oder verschickt, sie also keinen Einfluss mehr darauf nehmen kann, wer das Bildnis zur Kenntnis nimmt (vgl. Höning 2012: 133). Dies wird regelmäßig der Fall sein, wenn eine Person eine Bilddatei auf einer Profilseite eines sozialen Netzwerks postet oder per WhatsApp versendet (vgl. OLG Oldenburg, AfP 2018: 466).

Als zweite Tathandlung kommt die öffentliche Zurschaustellung eines Bildnisses in Frage. Darunter wird jede Art der Sichtbarmachung eines Bildnisses verstanden, die einer Mehrzahl von Personen das Bildnis zur Kenntnis bringt, ohne dass diese Verfügungsgewalt über das Bildnis erhalten. Um das Merkmal der Öffentlichkeit zu erfüllen ist es dabei notwendig, dass der Personenkreis nicht abgegrenzt oder durch Beziehungen untereinander persönlich verbunden ist. Auch hier ist noch nicht höchstrichterlich geklärt, ob die Zurschaustellung in sozialen Medien, entweder auf einer eigenen oder fremden Profilseite, als Tathandlung ausreichend ist. Da grundsätzlich jede Art der Sichtbarmachung als tatbestandsmäßig im Sinne des § 22 KUG anzusehen ist, ist dies allerdings zu bejahen, zumindest wenn keine Account-Einstellungen vorgenommen wurden, die den Kreis der Personen, die das Bildnis wahrnehmen können, erheblich einschränkt.

Einwilligung der betroffenen Person in die Verbreitung

Grundsätzlich ist gem. § 22 Satz 1 KUG die Einwilligung der betroffenen Person in die Veröffentlichung und Verbreitung ihres Bildnisses erforderlich, die

ausdrücklich oder konkludent[15] erfolgen kann.[16] Als Einwilligung ist dabei die vorherige Zustimmung[17] anzusehen.

Liegt die Einwilligung einer Person vor, ist diese nur dann und soweit wirksam, wie der abgebildeten Person die Art, der Zweck und der Umfang der geplanten Verwendung des Bildmaterials bekannt sind und sie gerade diesen zustimmt. Sendet eine Person beispielsweise einer anderen Person in einer privaten Nachricht per WhatsApp Fotos, kann hieraus nicht geschlossen werden, dass die Person damit der öffentlichen Verbreitung dieser Fotos zugestimmt hat (vgl. OLG Oldenburg, AfP 2018: 466). Der Umstand, dass eine Einwilligung in Kenntnis sämtlicher tatsächlichen und konkreten Umstände vorlag, ist im Fall eines Verfahrens von den Verbreiter*innen des Bildmaterials zu beweisen.

Eine Einwilligung kann im Zivilrecht grundsätzlich nur dann wirksam sein, wenn die einwilligende Person unbeschränkt geschäftsfähig ist. Dies ist insbesondere bei minderjährigen Personen nicht der Fall. In diesen Fällen entscheidet sich Wirksamkeit der Einwilligung nach dem allgemeinen Zivilrecht und hängt von dem Alter der abgebildeten Person ab.[18]

---

15 Bei der Rechtsfigur der konkludenten Einwilligung lässt eine Person durch nonverbales Verhalten ihren Willen durch schlüssiges Verhalten erkennen.

16 Zur vorliegend weniger relevanten Ausnahme vom Einwilligungserfordernis vgl. die Regelung des § 23 Abs. 1 KUG sowie BGH, NJW 1965: 2148; BGH, NJW 2000: 2201. m.w.N. Eine andere, im allgemeinen Presse- und Medienrecht oftmals streitgegenständliche Frage ist die Zulässigkeit einer nicht von der Einwilligung der abgebildeten Person gedeckte Verbreitung ihres Bildes, wenn dieses Bild dem Bereich der Zeitgeschichte positiv zuzuordnen sein könnte (§ 23 Abs. 1 Nr. 1 KunstUrhG) und berechtigte Interessen des Abgebildeten nicht verletzt werden (§ 23 Abs. 2 KunstUrhG). Auch dies wird bei privaten, nicht prominenten Personen nur in seltenen Ausnahmen der Fall sein.

17 Im Sinne des § 183 BGB.

18 Gemäß § 104 BGB sind Personen, die das siebte Lebensjahr noch nicht vollendet haben, geschäftsunfähig und damit nicht in der Lage, eine wirksame Einwilligung zu erteilen. Diese kann nur von den gesetzlichen Vertreter*innen der Person erteilt werden (§§ 1626, 1629 BGB oder § 1793 BGB). Bis zur Vollendung des 16. Lebensjahres sind Personen gemäß § 106 BGB beschränkt geschäftsfähig. Grundsätzlich ist auch bei diesen Personen eine rechtmäßige Verbreitung oder öffentliche Zurschaustellung von Bildnissen von der Einwilligung der gesetzlichen Vertreter*innen der Person abhängig. Anerkannt ist jedoch, dass eine Einwilligung generell erfolgen kann, etwa indem Eltern grundsätzlich zustimmen, dass ihre Kinder über die Verbreitung ihrer Fotos in sozialen Netzwerken selbst entscheiden. Ferner sieht die Rechtsprechung aufgrund der höchstpersönlichen Natur des Rechts am eigenen Bild von der ausschließlichen Einwilligungsfähigkeit der gesetzlichen Vertreter*innen der Person ab, wenn eine ausrei-

Das Zivilrecht kennt ferner die Rechtsfigur der konkludenten Einwilligung, bei der eine Person durch nonverbales Verhalten ihren Willen durch schlüssiges Verhalten erkennen lässt. Diese Rechtsfigur wird gerade im Hinblick auf soziale Medien oftmals zur Rechtfertigung der Verbreitung von Bildmaterial genutzt. Von einer solchen konkludenten Einwilligung ist im Rahmen des § 23 KUG etwa grundsätzlich dann auszugehen, wenn eine Person Bildnisse von sich selbst öffentlich zugänglich in sozialen Medien hochlädt. Da die Person in diesem Fall keine der von den Medien angebotenen Einschränkungen in Anspruch nimmt, um die Verbreitung bzw. öffentliche Zurschaustellung ihres Bildnisses zu kontrollieren, darf angenommen werden, dass sie diesen uneingeschränkt zustimmt.

Dementgegen liegt bisher keine gefestigte Rechtsprechung zu der Frage vor, ob es für Nutzer*innen sozialer Netzwerke grundsätzlich eine berechtigte Erwartung geben kann, dass Beiträge, die in einer als privat wahrgenommenen Sphäre des Internets geteilt werden, etwa einem privaten Profil, tatsächlich als privat angesehen werden dürfen. Hier sollte deutlich vertreten werden, dass eine Person, die entsprechenden, ihre Privatsphäre schützenden Einstellungen in Übereinstimmung mit den Funktionen des sozialen Netzwerks vorgenommen hat, auch auf die Wirksamkeit dieser Einstellungen vertrauen darf. Sollte es einem solchen Fall dennoch zu einer Verbreitung durch Dritte kommen, etwa weil diese Sicherungen eines sozialen Netzwerks umgangen haben, kann dies nicht zu Lasten der betroffenen Person gehen.

Jedenfalls zeichnet sich auch im Hinblick auf das Recht am eigenen Bild sowohl in der Diskussion in der Rechtswissenschaft als auch der Rechtsprechung zu dieser Frage die Auffassung ab, dass von Nutzer*innen sozialer Netzwerke erwartet wird, zumindest entsprechende Einstellungen in ihren Accounts vorzunehmen, um ihre Privatsphäre zu schützen, sollten sie dies wünschen. Dabei wird vorausgesetzt, dass Nutzer*innen sich mit den entsprechenden Möglichkeiten auseinandergesetzt haben und diese umsetzen können. Dies gilt in sozialen Medien insbesondere auch für das eigene Profilfoto.

Zu beachten ist auch, dass eine Kontrolle der Nutzer*innen von sozialen Netzwerken regelmäßig nur im Hinblick auf eigene Profilseiten und Beiträge

---

chende Einsichts- und Urteilsfähigkeit der Person vorliegt. Regelmäßig soll dies mit der Vollendung des 14. Lebensjahres der Fall sein. Zwischen dem 14. und der Vollendung des 18. Lebensjahres muss also eine Einwilligung der abgebildeten Person selbst sowie ihrer gesetzlichen Vertreter*innen vorliegen.

erfolgen kann. Da für Beiträge Dritter die von diesen vorgenommenen Einstellungen gelten, kann etwa bei einem Kommentieren öffentlicher Beiträge von einer konkludenten Einwilligung zur öffentlichen Verbreitung ausgegangen werden. Nutzer*innen treten dann durch einen solchen Beitrag mit ihren (Profil-)Bildern und ihren Aussagen bewusst in die Öffentlichkeit und können sich im Hinblick auf diese (aber nur auf diese) nicht mehr auf ihre Privatsphäre berufen.[19]

Einzelfälle der Verletzung des Rechts am eigenen Bild und des Allgemeinen Persönlichkeitsrechts

Im Fall von digitaler Gewalt wird eine Verletzung des Rechts am eigenen Bild oftmals zugleich auch unter anderen Aspekten schwerwiegende Verletzungen des Allgemeinen Persönlichkeitsrechts darstellen und daher unter mehreren Begründungen verfolgt werden können. Dies betrifft insbesondere folgende Fälle:

- Nacktfotos: Die Verbreitung von Nacktaufnahmen einer Person ohne ihre Zustimmung stellt regelmäßig eine schwerwiegende Persönlichkeitsrechtsverletzung dar, die sowohl in die Intim- und Privatsphäre der Person als auch in ihr Selbstbestimmungsrecht eingreift (vgl. BGH, NJW 1974: 1947-1950). Erst recht gilt dies für Bildmaterial, das sexuelle Handlungen darstellt (vgl. VG Münster, BeckRS 2014: 47310).
- Überwachung: Bereits die Erstellung verdeckter Bild- oder Tonaufnahmen einer Person stellt einen schwerwiegenden Eingriff in das Persönlichkeitsrecht der betroffenen Person dar. Dies gilt insbesondere, wenn die Aufnahmen getätigt werden, um die Person zu überwachen, also ihre

19 Eine diesbezüglich weitergehende Diskussion, nämlich ob eine Person sich auch insgesamt nicht mehr auf ihr Recht auf Privatsphäre berufen kann, wenn sie diese »selbst aufgegeben hat«, betrifft vor allem die Verbreitung von Fotos prominenter Personen. Bei diesen wird der Umstand, dass sie oftmals über ihr eigenes Privatleben in sozialen Netzwerken berichten und hierzu Fotos von sich veröffentlichen, von den Medien zur Begründung der Auffassung genutzt, dass sie ihr Recht auf Privatheit praktisch aufgegeben hätten. In der Folge wird dies als Rechtfertigung genutzt, Fotos prominenter Personen etwa in deren Freizeit auch ohne deren Zustimmung anzufertigen und zu verbreiten. Obgleich diese Argumentationslinie schon bei prominenten Personen fraglich und mit dem Schutzzweck des Rechts am eigenen Bild sowie dem Allgemeinen Persönlichkeitsrecht schwer vereinbar erscheint, kann dies bei Privatpersonen jedenfalls nur in Ausnahmefällen gelten.

Lebensgewohnheiten systematisch zu erfassen (vgl. BVerfG, BVerfGE 101: 361). Zusätzlich liegt eine Verletzung des Rechts am eigenen Bild vor, wenn das so gewonnene Überwachungsmaterial später veröffentlicht wird oder mit einer Veröffentlichung gedroht wird (vgl. ebd.).

- Technisch manipuliertes Bildmaterial: Erfolgt eine technische Manipulation des Bildmaterials derart, dass Fotos oder Videos einer dritten Person mit dem Bild einer Person versehen werden, ohne dass dies für das durchschnittliche Publikum als Fotomontage zu erkennen ist (z.B. Deepfakes), wird mit dem Bildmaterial zugleich eine unwahre Tatsachenbehauptung aufgestellt. Dem Bildmaterial ist in diesen Fällen nämlich die Aussage zu entnehmen, das Dargestellte habe sich in dieser Form tatsächlich so zugetragen bzw. erweckt es den Anschein, ein authentisches Abbild einer Person zu liefern. Neben der Verletzung des Rechts am eigenen Bild liegt somit auch eine Verletzung des Rechts auf Schutz vor Unwahrheit vor (vgl. BVerfG, AfP 2005: 171; LG München I vom 30.10.2015).
- Mit Zustimmung entstandenes Bildmaterial: Sind während einer Beziehung intime Foto- oder Videoaufnahmen mit Zustimmung der aufgezeichneten Person entstanden, ist regelmäßig davon auszugehen, dass die Einwilligung zeitlich beschränkt für die Dauer der Beziehung gelten sollte (BGH, AfP 2016: 243). Werden solche Aufnahmen nach dem Ende einer Beziehung nicht gelöscht oder herausgegeben, kann dies eine Verletzung des Allgemeinen Persönlichkeitsrechts darstellen.

Hinweise für die Beratungspraxis

Erfahrungen aus der Praxis zeigen, dass die Durchsetzbarkeit zivilrechtlicher Ansprüche bei digitaler Gewalt oftmals an deren Nachweisbarkeit scheitern kann. Es ist mithin in einer Beratungssituation unbedingt darauf hinzuwirken, dass Betroffene eine gute und ausführliche Beweissicherung betreiben. Hierzu eigenen sich insbesondere Screenshots oder die Speicherung von Posts, Nachrichten etc., aus denen sich die Rechtsverletzung, die Verletzer*innen, das Datum und das Medium ergeben.[20] Da gerade in sozialen Medien der Kontext eines Beitrags von Bedeutung sein kann, sollte eine

20 Hat die Rechtsverletzung durch eine persönliche Nachricht stattgefunden, sollten eventuell vor- oder nachgehende Nachrichten ebenfalls gesichert werden. Wenn möglich sollte dabei ein Chatverlauf auch archiviert werden. Bei E-Mails sollte ebenfalls ein Screenshot angefertigt werden, aus dem sich die Informationen zur Absender*in der E-Mail ergeben (sogenannte Header).

möglichst umfassende Dokumentation und Sicherung erfolgen.[21] Finden die Rechtsverletzungen durch Telefonanrufe statt, sollte ein Screenshot des Telefons angefertigt werden, aus dem sich die anrufende Telefonnummer, der Zeitpunkt und die Dauer des Gesprächs ergibt. Werden Sprachnachrichten gesendet, sollten diese umgehend abgespeichert werden sowie deren Eingang ebenfalls wie oben beschrieben dokumentiert werden.

Für die spätere Beweisführung vor Gericht kann es zudem eine erhebliche Erleichterung darstellen, wenn die Beweise zusätzlich von anderen Personen als den Betroffenen gesichert werden, beispielsweise durch Berater*innen. Findet eine Rechtsverletzung etwa für andere sichtbar in sozialen Medien statt, können andere Personen diese auch über ihren Account dokumentieren. Nachrichten sollten weitergeleitet und von der empfangenden Person entsprechend gesichert werden.

Damit liegt zum einen eine von den Parteien des Verfahrens unabhängige Dokumentation vor, zum anderen können die Dritten in einem späteren Verfahren als Zeug*innen benannt werden. Sinnvoll ist ferner, gerade auch bei mündlichen Verstößen, ein Gedächtnisprotokoll anzufertigen, insbesondere wenn es sich um anhaltende Rechtsverletzungen handelt. Ein solches Protokoll kann hilfreich sein, um die zeitlichen Abläufe später nicht aufwendig rekonstruieren zu müssen. Hierbei sollte auch notiert werden, ob andere Personen, etwa gemeinsame Bekannte, mit denen über die Rechtsverletzung gesprochen wird, in einem späteren Verfahren als Zeug*innen in Frage kommen.

Literatur

Höning, Nina (2012): Das Recht am eigenen Bild und der Schutz prominenter Persönlichkeiten im deutschen und US-amerikanischen Recht. Schriftenreihe zum internationalen Einheitsrecht und zur Rechtsvergleichung. Band 25. Hamburg: Verlag Dr. Kovač.

21 Regelmäßig sollte dies den Beitrag selbst, Reaktionen auf diesen wie Kommentare und Likes etc. umfassen. Dabei sollten sämtliche reagierenden Nutzer*innen erkennbar sein. Handelt es sich bei dem Beitrag um einen Kommentar, sollte neben diesem auch der ursprüngliche Beitrag sowie etwaige andere Kommentare und Reaktionen gesichert werden.

Soehring, Jörg/Hoene, Verena (2019): Presserecht. Recherche, Darstellung, Haftung im Recht der Presse, des Rundfunks und der neuen Medien. Köln: Dr. Otto Schmidt.

Wenzel, Karl Egbert/Burkhardt, Emanuel/Gamer, Waldemar/Pfeifer, Karl-Nikolaus/von Strobl-Albeg, Joachim (2018): Das Recht der Wort- und Bildberichterstattung. Handbuch des Äußerungsrechts, 6. neu bearbeitete Auflage. Köln: Dr. Otto Schmidt.

Rechtsprechungsverzeichnis[22]

BGH: Bundesgerichtshof, Urteil vom 26.11.1954, Az. I ZR 266/52 – Cosima Wagner, Sammlung der Entscheidungen des Bundesgerichtshofes in Zivilsachen (BGHZ), Nr. 15, o.S.

BGH: Bundesgerichtshof, Urteil vom 08.05.1956, Az. I ZR 62/54, Sammlung der Entscheidungen des Bundesgerichtshofes in Zivilsachen (BGHZ), Nr. 20, o.S.

BGH: Bundesgerichtshof, Urteil vom 10.11.1961, Az. I ZR 78/60 – Hochzeitsbild, in: Gewerblicher Rechtsschutz und Urheberrecht (GRUR), Nr. 04/1962, S. 169-215.

BGH: Bundesgerichtshof, Urteil vom 08.12.1964, Az. VI ZR 201/63, in: Neue Juristische Wochenschrift (NJW), Nr. 15/1965, S. 683-712.

BGH: Bundesgerichtshof, Urteil vom 09.06.1965, Az. Ib ZR 126/63 – Spielgefährtin, in: Neue Juristische Wochenschrift (NJW), Nr. 46/1965, S. 2147-2176.

BGH: Bundesgerichtshof, Urteil vom 02.07.1974, Az. VI ZR 121/73 – Nacktaufnahmen, in: Neue Juristische Wochenschrift (NJW), Nr. 43/1974, S. 1939-1968.

BGH: Bundesgerichtshof, Urteil vom 26.06.1979, Az. VI ZR 108/78 – Fußballtor, in: Neue Juristische Wochenschrift (NJW), Nr. 43/1979, S. 2193-2224.

BGH: Bundesgerichtshof, Urteil vom 20.01.1981, Az. VI ZR 163/79 – Wallraff II, in: Neue Juristische Wochenschrift (NJW), Nr. 25/1981, S. 1337-1400.

BGH: Bundesgerichtshof, Urteil vom 22.05.1984, Az. VI ZR 105/82 – AEG-Aktionär, in: Neue Juristische Wochenschrift (NJW), Nr. 34/1984, S. 1841-1920.

22 Ein besonderer Dank gilt Antea Mandić für die Erstellung dieses Rechtsprechungsverzeichnisses.

BGH: Bundesgerichtshof, Urteil vom 10.03.1987, Az. VI ZR 244/85, in: Zeitschrift für Medien- und Kommunikationsrecht (AfP), 0. Nr./1987, 0.S.

BGH: Bundesgerichtshof, Urteil vom 15.12.1987, Az. VI ZR 35/87 – Intime Beziehungen, in: Zeitschrift für Medien- und Kommunikationsrecht (AfP), 0. Nr./1988, 0.S.

BGH: Bundesgerichtshof, Urteil vom 25.04.1995, Az. VI ZR 272/94, in: Zeitschrift für Medien- und Kommunikationsrecht (AfP), 0. Nr./1995, 0.S.

BGH: Bundesgerichtshof, Urteil vom 05.12.1995, Az. VI ZR 332/94, in: Zeitschrift für Medien- und Kommunikationsrecht (AfP), 0. Nr./1996, 0.S.

BGH: Bundesgerichtshof, Urteil vom 19.12.1995, Az. VI ZR 15/95 – Caroline von Monaco III, in: Zeitschrift für Medien- und Kommunikationsrecht (AfP), 0. Nr./1996, 0.S.

BGH: Bundesgerichtshof (BGH), Urteil vom 29.06.1999, Az. VI ZR 264/98, in: Zeitschrift für Medien- und Kommunikationsrecht (AfP), 0. Nr./1999, 0.S.

BGH: Bundesgerichtshof, Urteil vom 01.12.1999, Az. I ZR 226/97 – Der blaue Engel, in: Neue Juristische Wochenschrift (NJW), Nr. 30/2000, S. 2129-2224.

BGH: Bundesgerichtshof, Urteil vom 09.12.2003, Az. VI ZR 373/02 – Feriendomizil II, in: Zeitschrift für Medien- und Kommunikationsrecht (AfP), 0. Nr./2004, 0.S.

BGH: Bundesgerichtshof, Urteil vom 16.03.2010, Az. VI ZR 176/09, in: Zeitschrift für Medien- und Kommunikationsrecht (AfP), Nr. 03/2010, 0.S.

BGH: Bundesgerichtshof, Urteil vom 25.10.2011, Az. VI ZR 332/09, in: Neue Juristische Wochenschrift (NJW), Nr. 11/2012, S. 705-800.

BGH: Bundesgerichtshof, Urteil vom 20.12.2011, Az. VI ZR 261/10, in: Neue Juristische Wochenschrift (NJW), Nr. 11/2012, S. 705-800.

BGH: Bundesgerichtshof, Urteil vom 30.09.2014, Az. VI ZR 490/12, in: Gewerblicher Rechtsschutz und Urheberrecht (GRUR), Nr. 01/2015, S. 1-104.

BGH: Bundesgerichtshof, Urteil vom 30.09.2014, Az. VI ZR 490/12, in: Zeitschrift für Medien- und Kommunikationsrecht (AfP), Nr. 06/2014, 0.S.

BGH: Bundesgerichtshof, Urteil vom 13.10.2015, Az. VI ZR 271/14 – Löschung intimer Filmaufnahmen nach Ende einer Beziehung, in: Zeitschrift für Medien- und Kommunikationsrecht (AfP), Nr. 03/2016, 0.S.

BGH: Bundesgerichtshof, Urteil vom 15.12.2015, Az. VI ZR 134/15, in: Zeitschrift für Medien- und Kommunikationsrecht (AfP), Nr. 02/2016, 0.S.

BGH: Bundesgerichtshof, Urteil vom 24.05.2016, Az. VI ZR 496/15, in: Zeitschrift für IT-Recht und Recht der Digitalisierung (MMR), Nr. 12/2016, S. 785-852.

BVerfG: Bundesverfassungsgericht, Beschluss vom 03.06.1980, Az. 1 BvR 185/77 – Eppler, in: Neue Juristische Wochenschrift (NJW), Nr. 38/1980, S. 2069-2096.

BVerfG: Bundesverfassungsgericht, Beschluss vom 03.06.1980, Az. 1 BvR 185/77, in: Zeitschrift für Medien- und Kommunikationsrecht (AfP), o. Nr./1980, o.S.

BVerfG: Bundesverfassungsgericht, Beschluss vom 25.02.1993, Az. 1 BvR 151/93 – Böll, in: Neue Juristische Wochenschrift (NJW), Nr. 22/1993, S. 1417-1497.

BVerfG: Bundesverfassungsgericht, Beschluss vom 10.11.1998, Az. 1 BvR 1531/96 – Helnwein, in: Neue Juristische Wochenschrift (NJW), Nr. 18/1999, S. 1281-1352.

BVerfG: Bundesverfassungsgericht, Beschluss vom 09.10.2002, Az. 1 BvR 1611/96, 1 BvR 805/98 – Mitgehörtes Telefonat, in: Neue Juristische Wochenschrift (NJW), Nr. 49/2002, S. 3577-3656.

BVerfG: Bundesverfassungsgericht, Kammerbeschluss vom 31.03.1993, Az. 1 BvR 295/93 – BKA-Präsident, in: Neue Juristische Wochenschrift (NJW), Nr. 45/1993, S. 2897-2961.

BVerfG: Bundesverfassungsgericht, Nichtannahmebeschluss vom 25.10.2012, Az. 1 BvR 2720/11, in: Zeitschrift für Medien- und Kommunikationsrecht (AfP), Nr. 01/2013, o.S.

BVerfG: Bundesverfassungsgericht, Stattgegebener Kammerbeschluss vom 14.02.2005, Az. 1 BvR 240/04, in: Zeitschrift für Medien- und Kommunikationsrecht (AfP), Nr. 02/2005, o.S.

BVerfG: Bundesverfassungsgericht, Urteil vom 05.06.1973, Az. 1 BvR 536/72 – Lebach I, in: Neue Juristische Wochenschrift (NJW), Nr. 28/1973, S. 1221-1248.

BVerfG: Bundesverfassungsgericht, Urteil vom 15.12.1983, Az. 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83 – Volkszählung, Sammlung der Entscheidungen des Bundesverfassungsgerichts (BVerfGE), Nr. 65, S. 1-71.

BVerfG: Bundesverfassungsgericht, Urteil vom 17.02.1998, Az. 1 BvF 1/91, in: Zeitschrift für Medien- und Kommunikationsrecht (AfP), o. Nr./1998, o.S.

BVerfG: Bundesverfassungsgericht, Urteil vom 15.12.1999, Az. 1 BvR 653/96 – Caroline von Monaco, in: Zeitschrift für Medien- und Kommunikationsrecht (AfP), Nr. 01/2000, o.S.

BVerfG: Bundesverfassungsgericht, Urteil vom 15.12.1999, Az. 1 BvR 653/96, Sammlung der Entscheidungen des Bundesverfassungsgerichts, Nr. 101, S. 361-396.

BVerfG: Bundesverfassungsgericht, Urteil vom 02.03.2006, Az. 2 BvR 2099/04, Sammlung der Entscheidungen des Bundesverfassungsgerichts, Nr. 115, S. 166-204.

EGMR: Europäischer Gerichtshof für Menschenrechte, Urteil vom 24.06.2004, Az. 59320/00 – Hannover v. Deutschland, in: Zeitschrift für Medien- und Kommunikationsrecht (AfP), Nr. 04/2004, o.S.

EGMR: Europäischer Gerichtshof für Menschenrechte, Urteil vom 03.04.2007, Az. 62617/00, in: Europäische Grundrechte-Zeitschrift (EuGRZ), o. Nr./2007, o.S.

EGMR: Europäischer Gerichtshof für Menschenrechte (EGMR), Urteil vom 10.05.2011, Az. 48009/08 – Mosley v. The United Kingdom, in: Neue Juristische Wochenschrift (NJW), Nr. 11/2012, S. 705-800.

EGMR: Europäischer Gerichtshof für Menschenrechte, Urteil vom 16.01.2014, Az. 13258/09, in: Zeitschrift für Medien- und Kommunikationsrecht (AfP), Nr. 02/2015, o.S.

KG: Kammergericht Berlin, Beschluss vom 18.06.2009, Az. 9 W 123/09, in: Zeitschrift für Medien- und Kommunikationsrecht (AfP), Nr. 04/2009, o.S.

KG: Kammergericht Berlin, Beschluss vom 11.03.2020, Az. 10 W 13/20 – Künast. https://openjur.de/u/2253932.html [Zugriff: 8.9.2020].

KG: Kammergericht Berlin, Urteil vom 18.12.2007, Az. 9 U 95/07, in: Zeitschrift für Medien- und Kommunikationsrecht (AfP), Nr. 04/2008, o.S.

KG: Kammergericht Berlin, Urteil vom 18.04.2011, Az. 10 U 149/10, in: Zeitschrift für Urheber- und Medienrecht (ZUM), Nr. 07/2011, S. 529-608.

KG: Landgericht Berlin, Beschluss vom 02.09.2019, Az. 27 O 433/19 – Künast. https://openjur.de/u/2186154.html [Zugriff: 8.9.2020].

LG: Landgericht Köln, Urteil vom 10.06.2015, Az. 28 O 547/14, in: Computer und Recht (CR), Nr. 01/2016, o.S.

LG: Landgericht München I, Urteil vom 30.10.2015, Az. 9 O 5780/15. https://gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2016-N-03704?hl=true&AspxAutoDetectCookieSupport=1 [Zugriff: 10.9.2020].

OLG: Oberlandesgericht Dresden, Beschluss vom 14.02.2017, Az. 4 U 195/17, in: Zeitschrift für IT-Recht und Recht der Digitalisierung (MMR), Nr. 10/2017, S. 649-720.

OLG: Oberlandesgericht Düsseldorf, Urteil vom 22.01.1992, Az. 15 U 228/90, in: Zeitschrift für Medien- und Kommunikationsrecht (AfP), o. Nr./1992, o.S.

OLG: Oberlandesgericht Frankfurt, Urteil vom 23.12.2008, Az. 11 U 22/08. ht tps://openjur.de/u/301694.html [Zugriff: 10.9.2020].
OLG: Oberlandesgericht Hamburg, o.A., in: Schriftenreihe des Archivs für Urheber- und Medienrecht (UFITA), o.Nr./1978, o.S.
OLG: Oberlandesgericht Karlsruhe, Urteil vom 14.10.1998, Az. 6 U 120/97, in: Zeitschrift für Medien- und Kommunikationsrecht (AfP), o. Nr./1999, o.S.
OLG: Oberlandesgericht Köln, Urteil vom 03.02.2015, Az. 15 U 133/14, in: Neue Juristische Online-Zeitschrift (NJOZ), Nr. 08/2016, S. 241-280.
OLG: Oberlandesgericht München, Urteil vom 17.03.2016, Az. 29 U 368/16, in: Gewerblicher Rechtsschutz und Urheberrecht – Rechtsprechungs-Report (GRUR-RR), Nr. 07/2016, S. 265-312.
OLG: Oberlandesgericht Oldenburg, Beschluss vom 05.03.2018, Az. 13 U 70/17, in: Zeitschrift für Medien- und Kommunikationsrecht (AfP), Nr. 05/2018, o.S.
VG: Verwaltungsgericht Münster, Urteil vom 22.01.2014, Az. 20 K 1277/13. BDG, Beck'sche Rechtssprechungssammlung (BeckRS) 2014, o.S.

Rechtliche Handlungsoptionen: Öffentliches Recht

Ulrike Lembke

Neben der Möglichkeit, digitale Gewalt als Straftat anzuzeigen oder zivilrechtlich gegen eine solche Rechtsverletzung vorzugehen, gibt es auch im Öffentlichen Recht[1] einige wenige Regelungen, die auf digitale Gewalt bezogen werden können. Strafrecht legt fest, welche Rechtsverletzungen eine Straftat darstellen und wie diese bestraft und verfolgt werden. Zivilrecht regelt Ansprüche und Verpflichtungen zwischen Privaten. Öffentliches Recht umfasst die hoheitlichen staatlichen Aufgaben, Pflichten und Befugnisse und deren konkrete Ausübung. In Bezug auf digitale Gewalt ist zum einen der oben[2] beschriebene grund- und menschenrechtliche Schutzrahmen ein relevanter Teil des Öffentlichen Rechts. Die aus der Verfassung und den Menschenrechtsverträgen resultierende staatliche Pflicht zum effektiven Schutz vor geschlechtsspezifischer Gewalt in all ihren Formen ist die Grundlage für alles staatliche Handeln in diesem Bereich. Sie ist daher auch Richtschnur für Entscheidungen der Zivilgerichte oder Strafverfolgungsorgane.

Zum anderen gibt es konkrete gesetzliche Pflichten staatlicher Behörden, die auch auf digitale Gewalt bezogen werden können bzw. müssen. Der Vorteil möglicher Handlungsoptionen im Öffentlichen Recht liegt vor allem in der Rechtsmobilisierung – die Betroffenen müssen nicht wie im Zivilrecht selbst die gesamte Rechtsverfolgung stemmen und es muss auch nicht gleich die Staatsanwaltschaft eingeschaltet werden, welche überdies zunächst nur Individuen verfolgt, nicht aber Strukturen ändern kann. Präventive öffentlichrechtliche Strukturen wie der Jugendmedienschutz brauchen überdies keine konkret Betroffenen, jede Person kann sich mit Beschwerden an staatliche Stellen wenden. Allerdings sind auch die Behörden, die öffentliches Recht an-

1 Die Ausführungen in diesem Text beziehen sich auf die Rechtslage mit Stand Juli 2020.

2 Siehe Beitrag: Menschenrechtlicher Schutzrahmen für Betroffene von digitaler Gewalt.

wenden sollen, bisher wenig auf den Kampf gegen digitale Gewalt eingestellt und auch das Recht selbst ist verbesserungsfähig.

Jugendmedienschutz

Wer digitale Gewalt ausübt, beruft sich oft auf die Meinungsfreiheit. Doch Artikel 5 Absatz 2 Grundgesetz benennt als eine der Grenzen der Meinungsfreiheit die »gesetzlichen Bestimmungen zum Schutze der Jugend«. Die Kommission für Jugendmedienschutz[3] (KJM) prüft Angebote in Telemedien, also öffentliche Kommunikation im Internet, anhand des Jugendmedienschutz-Staatsvertrages[4] (JMStV) auf ihre Zulässigkeit. Bei Verstößen erfolgen behördliche Sanktionen gegen die Anbieter*innen, welche Beanstandung, Untersagung oder Sperrung sowie die Verhängung erheblicher Bußgelder umfassen können. Zudem nimmt die KJM Stellung zu Indizierungsanträgen für Telemedien oder stellt eigene Indizierungsanträge. Wird festgestellt, dass ein Telemedium gegen den JMStV verstößt, kommt es auf eine nicht-öffentliche Liste (Index) und ist damit indiziert. Indizierte Telemedien dürfen für Kinder und Jugendliche nicht mehr zugänglich sein, auch nicht über Verlinkungen (vgl. BayVGH vom 01.05.2018) oder aufbereitete Ergebnisse in Suchmaschinen (vgl. VG München vom 14.12.2017).

Anbieter*in ist nicht nur, wer in Deutschland ansässig Eigentümer*in oder Administrator*in von Telemedien ist, sondern auch, wer nur die Möglichkeit der Einflussnahme auf die inhaltliche Gestaltung des (ggf. vom Ausland aus bereitgestellten) Angebots hat (vgl. OVG Sachsen-Anhalt vom 18.05.2017; VG Kassel vom 08.06.2017). So soll verhindert werden, dass Anbieter*innen sich ihrer Verantwortung entziehen, indem sie einfach die Domain abgeben oder nicht mehr im Impressum genannt werden (vgl. VG Hamburg vom 21.08.2013). Es ist auch nicht erforderlich, dass Anbieter*innen mit dem

3 Die Kommission für Jugendmedienschutz (KJM) ist ein Organ der Landesmedienanstalten und die zentrale Aufsichtsstelle für den Jugendschutz im privaten Rundfunk und in Telemedien, wenn die Anbieter*innen ihren Sitz in Deutschland haben, siehe https://kjm-online.de/ [Zugriff: 6.8.2020].

4 Staatsvertrag über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telemedien (Jugendmedienschutz-Staatsvertrag – JMStV) in der Fassung des Neunzehnten Staatsvertrages zur Änderung rundfunkrechtlicher Staatsverträge von 2016 (Neunzehnter Rundfunkänderungsstaatsvertrag), abrufbar unter https://kjm-online.de/service/rechtsgrundlagen/ [Zugriff: 6.8.2020].

Telemedium einen Gewinn erzielen oder dies beabsichtigen, das planmäßige Betreiben über einen längeren Zeitraum auch ohne wirtschaftliches Interesse genügt (vgl. OVG Sachsen-Anhalt vom 18.05.2017). Betreiber*innen eines Profils in den sozialen Medien können auch für Inhalte verantwortlich gemacht werden, die von Dritten eingestellt werden, wie insbesondere Kommentare (vgl. AG Tiergarten vom 10.10.2016), oder für Inhalte auf verlinkten Webseiten, wenn sie diese beschreiben und anpreisen (vgl. VG Kassel vom 08.06.2017).

Unzulässig sind Telemedien-Angebote nach § 4 JMStV, welche Aufstachelung zum Hass, Angriffe auf die Menschenwürde, Beschimpfung von Bevölkerungsgruppen, Verharmlosung von grausamen Gewalttätigkeiten, Billigung des Nationalsozialismus, pornografische Darstellungen oder indizierte Inhalte enthalten. Unzulässig sind ferner Telemedien-Angebote, die »offensichtlich geeignet sind, die Entwicklung von Kindern und Jugendlichen oder ihre Erziehung zu einer eigenverantwortlichen und gemeinschaftsfähigen Persönlichkeit unter Berücksichtigung der besonderen Wirkungsform des Verbreitungsmediums schwer zu gefährden«. Ist lediglich eine »Beeinträchtigung« der Entwicklung zu befürchten, muss gemäß § 5 JMStV dafür Sorge getragen werden, dass Kinder oder Jugendliche der gefährdeten Altersgruppen diese nicht wahrnehmen können. Grundsätzlich könnte der Jugendmedienschutz ein wirksames Mittel gegen geschlechtsspezifische digitale Gewalt darstellen, da häufig Aufstachelung zum Hass, Angriffe auf die Menschenwürde, Beschimpfung von Bevölkerungsgruppen oder eine Gefährdung oder Beeinträchtigung der Entwicklung von Kindern und Jugendlichen vorliegen dürfte. Wird einer überzeugenden Entscheidung des Amtsgerichts Bielefeld (vom 09.11.2015) gefolgt, wären ferner etliche Vergewaltigungsandrohungen als verbotene Pornografie erfasst.

Tatsächlich geht die KJM kaum jemals gegen geschlechtsspezifische digitale Gewalt vor. Der ganz überwiegende Teil der Prüffälle und Indizierungsanträge bezieht sich auf Pornografie, wobei Vergewaltigungsandrohungen bislang nicht erfasst werden (vgl. KJM 2017: 27ff.; KJM 2019: 20ff.). Mit Prüfungen wegen geschlechtsbezogener Diskriminierung befasst sich die KJM nur ungefähr drei Mal im Jahr (vgl. KJM 2017: 29, 31, 32; KJM 2019: 20, 24, 25). Obwohl Hass und Hetze im Netz als Problemfeld identifiziert sind (vgl. KJM 2017: 28; KJM 2019: 20), wird darunter praktisch nur Rechtsextremismus in einem

sehr engen Sinne verstanden[5] (vgl. Hopf 2019b: 63ff.). In einer größeren Publikation der Landesmedienanstalten zu Hass im Netz wird Diskriminierung immerhin ganz knapp definiert, wobei das verwendete Vokabular ebenso irritiert wie die konkrete Inbezugnahme von Geschlecht und Sexualität: »*Sexuelle Diskriminierung*: Einseitige Charakterisierungen der Geschlechter (Objektcharakter, sexuelle Fremdbestimmung, Rollenklischees) sind geeignet, die Wahrnehmung des anderen Geschlechts negativ zu prägen und können den Prozess der sexuellen Selbstfindung Heranwachsender beeinträchtigen.« (Mosler 2019: 53 [Herv. i.O.])

Die unangebrachte Zurückhaltung der KJM könnte zum einen ihrer Orientierung an den Einschätzungen von Staatsanwaltschaften und Strafgerichten[6] geschuldet sein, obwohl der Jugendmedienschutz gerade keine strafrechtliche Verantwortlichkeit voraussetzt. Auch sind Aufsichtsbehörden durch mangelnde Durchsetzbarkeit gegenüber ausländischen Anbieter*innen entmutigt; hier besteht ein dringender Änderungsbedarf (vgl. Hopf 2019a: 20f.). Zugleich könnte die Zivilgesellschaft aktiver werden und auch geschlechtsspezifische digitale Gewalt bei der KJM rügen. Zwar dient der JMStV dezidiert nur dem Jugendschutz, jede Person kann aber wegen geschlechtsspezifischer Gewalt jugendgefährdende Telemedien bei der KJM anzeigen, ohne dass ein*e konkret betroffene*r Jugendliche*r präsentiert werden muss. Allerdings werden solche Beschwerden nur verarbeitet werden können, wenn KJM und Landesmedienanstalten sich für einen grundlegenden antidiskriminierungsrechtlichen Ansatz öffnen, wie er im europäischen

5 Dies meint bestimmte, NS-nahe Formen von Antisemitismus sowie Hetze gegen ›Ausländer und Flüchtlinge‹, obwohl rassistische Diskriminierung und Gewalt in weitaus mehr und komplexeren Formen auftreten. Trotz Knappheit deutlich differenzierter: LfM und AJS (2016).

6 Siehe Beitrag: Möglichkeiten und Grenzen strafrechtlicher Interventionen bei digitaler Gewalt.

Recht bereits angelegt ist (vgl. Artikel 6 RL 2018/1808[7]) und in der deutschen Rechtswissenschaft nachdrücklich gefordert wird (vgl. Lembke 2016).

Staatliche Opferentschädigung bei nicht-physischer Gewalt mit gesundheitlichen Folgen

Richtig genutzt, könnte das Jugendmedienschutzrecht zur Prävention und Verhinderung der Ausbreitung von geschlechtsspezifischer digitaler Gewalt beitragen. Andere Bereiche des Öffentlichen Rechts wie das im Folgenden vorgestellte Entschädigungsrecht beziehen sich dagegen auf die Unterstützung von Personen, *nachdem* diese von geschlechtsspezifischer digitaler Gewalt betroffen sind. Im Grenzbereich beider Funktionen können staatliche Pflichten zur Garantie einer effektiven Beratungs- und Unterstützungsinfrastruktur oder Schutzpflichten staatlicher Arbeitgeber*innen und Körperschaften des öffentlichen Rechts wie Universitäten diskutiert werden. Im Folgenden soll es jedoch um das soziale Entschädigungsrecht gehen, wonach Personen, die durch eine Gewalttat gesundheitliche Schäden erleiden, eine Entschädigung sowie Unterstützung und Hilfe vom Staat einfordern können. Dies ist insbesondere dann relevant, wenn der Täter nicht ermittelt wird oder nicht zahlen können. Erhebliche gesundheitliche Beeinträchtigungen können auch durch geschlechtsspezifische digitale Gewalt entstehen.

7 Richtlinie (EU) 2018/1808 des Europäischen Parlaments und des Rates vom 14. November 2018, Artikel 6 Absatz 1 lit. a: »Unbeschadet der Verpflichtung der Mitgliedstaaten, die Menschenwürde zu achten und zu schützen, sorgen die Mitgliedstaaten mit angemessenen Mitteln dafür, dass die audiovisuellen Mediendienste, die von den ihrer Rechtshoheit unterworfenen Mediendiensteanbietern bereitgestellt werden, keine Aufstachelung zu Gewalt oder Hass gegen eine Gruppe von Personen oder gegen ein Mitglied einer Gruppe aus einem der in Artikel 21 der Charta genannten Gründe enthalten.« Artikel 21 EU-Grundrechte-Charta: »Diskriminierungen insbesondere wegen des Geschlechts, der Rasse [sic!], der Hautfarbe, der ethnischen oder sozialen Herkunft, der genetischen Merkmale, der Sprache, der Religion oder der Weltanschauung, der politischen oder sonstigen Anschauung, der Zugehörigkeit zu einer nationalen Minderheit, des Vermögens, der Geburt, einer Behinderung, des Alters oder der sexuellen Ausrichtung sind verboten. Unbeschadet besonderer Bestimmungen der Verträge ist in ihrem Anwendungsbereich jede Diskriminierung aus Gründen der Staatsangehörigkeit verboten.«

Mit dem Gesetz zur Regelung des sozialen Entschädigungsrechts vom 12. Dezember 2019[8] wurde das Entschädigungsrecht grundlegend reformiert. Zuvor waren nur die gesundheitlichen Folgen von »tätlichen Angriffen« entschädigungsfähig (vgl. Kirstein 2013: 11ff.). Digitale Gewalt oder Stalking waren nicht erfasst, die Betroffenen erhielten keine Unterstützung. Die Istanbul-Konvention[9] umfasst aber alle Handlungen geschlechtsspezifischer Gewalt, die zu körperlichen, sexuellen, psychischen oder wirtschaftlichen Schäden oder Leiden bei Frauen führen oder führen können, einschließlich der Androhung solcher Handlungen, der Nötigung oder der willkürlichen Freiheitsentziehung, sei es im öffentlichen oder privaten Leben, siehe Artikel 3a der Konvention. In Artikel 33 der Konvention werden nochmals explizit staatliche Maßnahmen gegen psychische Gewalt, also »vorsätzliches Verhalten, durch das die psychische Unversehrtheit einer Person durch Nötigung oder Drohung ernsthaft beeinträchtigt wird«, gefordert. Dies verlangt, dass auch nicht-physische Gewalt mit gesundheitlichen Folgen gleichbehandelt und damit entschädigt wird.

Durch die Gesetzesänderung im Dezember 2019 wurde die Voraussetzung des »tätlichen Angriffs« durch die Voraussetzung eines »schädigenden Ereignisses« abgelöst. In § 13 Absatz 1 SGB XIV sind nun Opfer von körperlichen *und psychischen* Gewalttaten explizit als entschädigungsberechtigt benannt. Das Gesetz definiert eine psychische Gewalttat als ein »vorsätzliches, rechtswidriges, unmittelbar gegen die freie Willensentscheidung einer Person gerichtetes schwerwiegendes Verhalten«. Als Beispiele werden Verbrechen wie sexueller Missbrauch, Vergewaltigung[10], Menschenhandel, lebensbedrohliches Stalking, Geiselnahme und räuberische Erpressung aufgezählt. Die Istanbul-Konvention kennt aber keine Beschränkung auf »schwerwiegendes« Verhalten, womit überdies die Täterperspektive eingenommen wird (vgl. Deutscher Juristinnenbund 2019). Auch geschlechtsspezifische digitale Gewalt und nicht-physische Formen von Gewalt in sozialen Nahbeziehungen

8 Gesetz zur Regelung des sozialen Entschädigungsrechts vom 12. Dezember 2019, BGBl. I, S. 2652. Zur Gesetzgebungsgeschichte siehe https://dipbt.bundestag.de/extrakt/ba/WP19/2517/251749.html [Zugriff: 6.8.2020].

9 Siehe Beitrag: Menschenrechtlicher Schutzrahmen für Betroffene von digitaler Gewalt.

10 Wie eine Vergewaltigung, welche von Gesetzes wegen das Eindringen in den Körper voraussetzt, als psychische Gewalttat ohne physische Beeinträchtigung gedacht werden kann, bleibt das Geheimnis des Gesetzgebers.

(sogenannte häusliche Gewalt) können erhebliche gesundheitliche Beeinträchtigungen und chronische Leiden verursachen. Zwar sind diese Formen von der gesetzlichen Regelung nicht erfasst, so dass es schwierig ist, eine Entschädigung geltend zu machen. Betroffene, Beratungsstellen und Rechtsanwält*innen könnten aber auf eine menschenrechtskonforme Auslegung der Entschädigungsregeln drängen, welche den staatlichen Verpflichtungen aus der Istanbul-Konvention gerecht wird.

Das Bundesministerium erklärte in der Begründung zum Gesetzentwurf, dass der Begriff der »psychischen Gewalttat« eingeschränkt werden müsse, da die Entschädigungsmöglichkeiten sonst uferlos würden (vgl. Bundesministerium für Arbeit und Soziales 2018: 149). Eine solche Einschränkung kann aber nur mit Blick auf die gesundheitlichen Auswirkungen bei den Betroffenen erfolgen. Die Beschränkung auf »schwerwiegende« psychische Gewalt und die Konkretisierung durch einige Verbrechenstatbestände ist unvereinbar mit der Istanbul-Konvention (vgl. Deutscher Juristinnenbund 2020). Die Staatsaufgabe der Bekämpfung geschlechtsspezifischer Gewalt und die rechtliche Verpflichtung zur Implementation der Istanbul-Konvention bedingen die verfassungs- und konventionskonforme Anwendung des sozialen Entschädigungsrechts. Betroffenen von geschlechtsspezifischer digitaler Gewalt stehen damit Ansprüche auf sogenannte schnelle Hilfen, Beratung, Unterstützung und Entschädigung zu.

Literatur

Bundesministerium für Arbeit und Soziales (2018): »Referentenentwurf zur Regelung des sozialen Entschädigungsrechts vom 20.11.2018«. https://bmas.de/DE/Service/Gesetze/gesetz-zur-regelung-des-sozialen-entschaedigungsrechts.html [Zugriff: 6.8.2020].

Deutscher Juristinnenbund (2019): »Stellungnahme vom 09.01.2019 zum Referentenentwurf des Bundesministeriums für Arbeit und Soziales »Entwurf eines Gesetzes zur Regelung des Sozialen Entschädigungsrechts (Bearbeitungsstand 20.11.2018)«. https://djb.de/verein/Kom-u-AS/K3/st19-01/ [Zugriff: 6.8.2020].

Deutscher Juristinnenbund (2020): »Themenpapier 11 vom 07.02.2020 zur Umsetzung der Istanbul-Konvention in Deutschland: Entschädigung Betroffener bei psychischer Gewalt mit schweren Folgen«. https://djb.de/themen/thema/ik/st20-09/ [Zugriff: 6.8.2020].

Hopf, Kristina (2019a): »Die Entwicklung des Jugendmedienschutzes 2017/2018«, in: Zeitschrift für Urheber- und Medienrecht, Nr. 1, S. 8-21.

Hopf, Kristina (2019b): »Mobbing, Hass und Extremismus. Möglichkeiten und Grenzen des Medienrechts«, in: die medienanstalten (Hg.), Der Ton wird härter. Hass, Mobbing und Extremismus, Berlin: Vistas, S. 56-67.

Kirstein, Katrin Inga (2013): Entschädigung nach dem Opferentschädigungsgesetz und der gesetzlichen Unfallversicherung. Betroffenen von Ausbeutung und Gewalt zu ihren Rechten verhelfen. Eine Handreichung für Beratungsstellen. Berlin: Deutsches Institut für Menschenrechte.

Kommission für Jugendmedienschutz (KJM) (2017): 7. Tätigkeitsbericht. März 2015 – Februar 2017. Leipzig: VISTAS Verlag.

Kommission für Jugendmedienschutz (KJM) (2019): 8. Tätigkeitsbericht. März 2017 – Februar 2019. Berlin: die medienanstalten.

Landesanstalt für Medien Nordrhein-Westfalen (LfM) und Arbeitsgemeinschaft Kinder- und Jugendschutz (AJS) (Hg.) (2016) Hate Speech – Hass im Netz. Informationen für Fachkräfte und Eltern. Selbstverlag.

Lembke, Ulrike (2016): »Ein antidiskriminierungsrechtlicher Ansatz für Maßnahmen gegen Cyber Harassment«, in: Kritische Justiz, Vol. 49 Nr. 3, S. 385-406.

Mosler, Sabine (2019): »Beeinträchtigend oder gefährdend? Wirkungsrisiken von Hass, Hetze und Extremismus im Internet aus der Perspektive der Kriterien für die Aufsicht im Rundfunk und in den Telemedien der KJM«, in: die medienanstalten (Hg.), Der Ton wird härter. Hass, Mobbing und Extremismus, Berlin: Vistas, S. 48-55.

Rechtsprechungsverzeichnis

Amtsgericht (AG) Bielefeld, Urteil vom 09.11.2015, Az. 36 Ds-216 Js 160/12-257/15.

Amtsgericht (AG) Tiergarten, Urteil vom 10.10.2016, Az. (327 OWi) 3034 Js-OWi 3211/16 (187/16).

Bayerischer Verwaltungsgerichtshof (BayVGH), Beschluss vom 01.05.2018, Az. 7 ZB 18.31.

Oberverwaltungsgericht OVG Sachsen-Anhalt, Beschluss vom 18.05.2017, Az. 4 L 103/16.

Verwaltungsgericht (VG) Hamburg, Urteil vom 21.08.2013, Az. 9 K 507/11.
Verwaltungsgericht (VG) Kassel, Urteil vom 08.06.2017, Az. 1 K 573/13.KS.
Verwaltungsgericht (VG) München, Urteil vom 14.12.2017, Az. M 17 K 16.4916.

Erfahrungen und Strategien im Umgang mit digitaler geschlechtsspezifischer Gewalt

Erfahrungen mit der Beratung von betroffenen Mädchen und Frauen im Kontext digitaler Gewalt

Andrea Bocian, Jessica Lütgens und Angela Wagner

Als sich Mädchen und Frauen um das Jahr 2006 mit Anliegen wie Verleumdung mittels falscher Behauptungen im Internet, digitaler Überwachung und Kontrolle oder Erpressung durch Bild- und Videoaufnahmen an die Beratungsstelle Frauennotruf Frankfurt wendeten, gab es den Begriff ›digitale‹ Gewalt im deutschsprachigen Raum noch nicht. Dieser wurde von unserer Beratungsstelle zunächst intern diskutiert und dann zeitnah über Beratungs-, Presse- und Öffentlichkeitsarbeit etabliert. Durch die explizite Benennung dieser Form der Gewalt wollten wir zum einen ein neues soziales Phänomen beschreiben und zum anderen die Gewaltdimension dieser Angriffe verdeutlichen. Hierbei unterscheiden wir zwischen ›leichteren‹ Formen digitaler Gewalt wie etwa die Beleidigung oder Diffamierung von Personen und ›schweren‹ Formen digitaler Gewalt wie beispielsweise das Filmen einer Vergewaltigung und die angedrohte oder verwirklichte Veröffentlichung dieser Aufnahmen.

Der Bundesverband Frauenberatungsstellen und Frauennotrufe (bff), definiert digitale Gewalt wie folgt:

> »Mit digitaler Gewalt meinen wir alle Formen von Gewalt, die sich technischer Hilfsmittel und digitaler Medien (Handy, Apps, Internetanwendungen, Mails etc.) bedienen und/oder Gewalt, die im digitalen Raum, z.B. auf Online-Portalen oder sozialen Plattformen stattfindet. Wir gehen davon aus, dass digitale Gewalt nicht getrennt von ›analoger Gewalt‹ funktioniert, sondern meist eine Fortsetzung oder Ergänzung von Gewaltverhältnissen und -dynamiken darstellt.« (bff 2017: 2)

In unserer Arbeit, sowohl in der Beratung als auch der Presse- und Öffentlichkeitsarbeit, verwenden wir trotz der medialen Präsenz englischsprachiger

Begriffe (wie z.B. Cyberstalking oder Cyberharassment)[1] diese nach Möglichkeit nicht. Sie wecken bei vielen Betroffenen eher Unklarheit; manche kennen die englischen Begriffe nicht, andere haben Schwierigkeiten mit der genauen Übertragung dieser in das deutsche Äquivalent.

In den Jahren 2010 bis2019 haben wir 322 Fälle schwerer digitaler Gewalt in unserer Beratungspraxis dokumentiert. Dies sind nicht einmal 40 Fälle im Jahr; diese Zahlen verdeutlichen, dass die Befürchtung, eine Beratungsstelle könnte von Betroffenen digitaler Gewalt ›überrannt‹ werden, eher unbegründet ist. Leichtere Fälle digitaler Gewalt werden in unserer Beratungsstelle insgesamt eher selten thematisiert. Dies liegt auch daran, dass ein Bewusstsein für die Strafbarkeit der Angriffe und ein adäquates Vorgehen dagegen selten vorhanden sind. Deutlich häufiger wird von digitaler Gewalt in Verbindung mit Körperverletzungsdelikten und/oder stark kontrollierenden und belästigende Handlungen des Partners – oft nach einer Trennung, die von der Frau ausging – berichtet.

Das Thema digitale Gewalt spricht auch Frauen an, die Verfolgung durch digitale Medien, Spionagesoftwares und Abhörwanzen gegebenenfalls in Phantasien einbauen und mit einem allgemeinen Gefühl von Bedrohung verknüpfen. Solche Fälle werden bei uns nicht zwangsläufig unter digitalen Gewalterfahrungen erfasst.

Wir sind uns dessen bewusst, dass Mädchen und junge Frauen im digitalen Raum nicht nur Opfer digitaler Gewalt werden können. Als sehr aktive Nutzerinnen der sozialen Netzwerke beteiligen sie sich auch daran, andere öffentlich bloßzustellen und zu diffamieren und tun sich somit ebenfalls als Täterinnen hervor. Insoweit zielt einer unserer Flyer (vgl. Beratungsstelle Frauennotruf Frankfurt 2017a) sowohl auf die Prävention von Straftaten Jugendlicher, als auch auf die Vermittlung von Handlungskompetenzen im Falle eigener Betroffenheit.

Dieser Beitrag legt seinen Fokus jedoch auf die Beratung von Mädchen und Frauen als Betroffene digitaler Gewalt, weil wir hier inzwischen über eine Expertise verfügen, die über den Einzelfall hinaus allgemeine Aussagen zulässt. Beschrieben werden die Fallkonstellationen, ein feministischer Beratungsansatz, Hürden der Kontaktaufnahme und Auswirkungen digitaler Gewalt.

---

1 Einige dieser Begriffe werden in der Broschüre »Digitale Gewalt« (Beratungsstelle Frauennotruf Frankfurt 2017b: 5ff.) definiert.

Erste Fälle in der Beratungspraxis

Im Jahr 2005 kamen kostengünstige Handys mit integrierter Kamera und Bluetooth-Funktion auf den deutschen Markt. Gleichzeitig verbreiteten sich Kenntnisse über digitale Bildbearbeitung ebenso rasant. Für die Aufnahme und Entwicklung von Bildern mussten keine Fotostudios mehr beauftragt werden, weshalb eine Kontrollinstanz über die Art der Aufnahmen (wie z.B. erotische private Fotografien aber auch Aufnahmen von Straftaten), ebenso wie die Kontrolle über deren Besitz oder Verbreitung, weitestgehend verschwand. Kurz darauf, im Jahr 2006, wurden wir mit ersten Fällen konfrontiert:

- Eine 60-jährige Frau befürchtete, dass einverständlich aufgenommene Nacktaufnahmen von Ihrem Ex-Lebensgefährten digital weitergegeben würden.
- Eine Studentin wurde nach einer Vergewaltigung damit bedroht, dass im Falle einer Anzeige intime Aufnahmen an ihre Professor*innen gesendet würden.
- Eine Schülerin, die sich beim Geschlechtsverkehr mit ihrem Freund plötzlich von dessen Freunden – mit gezückten Handykameras – umringt sah.
- Und eine junge Frau, die von mehreren Männern vergewaltigt und dabei gefilmt wurde und nun die Verbreitung der Aufnahmen befürchtete.

Wie diese Fallbeispiele zeigen, sind sowohl Mädchen und junge Frauen als auch ältere Frauen in ganz unterschiedlichen Lebenslagen und von unterschiedlicher Herkunft von digitaler Gewalt betroffen. Dies bestätigt sich fortwährend in unserer alltäglichen Beratungsarbeit. In Gesprächen mit verschiedenen Kooperationspartner*innen wurde schnell deutlich, dass auch öffentliche Institutionen bereits mit gravierenden Einzelfällen konfrontiert waren und Handlungsbedarfe sahen. Berichtet wurde z.B. aus Schulen, dass

- Aufnahmen auf den Schultoiletten, auch unter den Trennwänden hindurch, gemacht wurden.
- peinliche oder intime Situationen gefilmt und verbreitet wurden, mit dem Ziel, die Betroffenen zu diskreditieren und in Folge vom Schulbesuch abzuhalten.

- Unterrichtsstunden auditiv aufgenommen, Äußerungen der Lehrkräfte und deren Unterricht gefilmt, kommentiert und online veröffentlicht wurden.

Erste Publikationen und Präventionsansätze

Aufgrund der medialen Berichterstattung lag die Aufmerksamkeit zunächst auf den eher jugendbezogenen Themen wie »Happy Slapping«[2], Gefahren im Chat und Cybermobbing. Geschlechtsspezifische Aspekte wie sexualisierte Gewalt oder sexistisch motivierte Herabwürdigung von Mädchen und Frauen hingegen wurden nicht thematisiert. Dank der Fördermittel des Frauenreferats der Stadt Frankfurt a.M. konnten wir uns dieser fehlenden Perspektive intensiv widmen. So wurden beispielweise

- in Kooperation mit dem Staatlichen Schulamt Beratungslehrer*innen aller Schulsysteme im Raum Frankfurt a.M. fortgebildet.
- ein inzwischen mehrfach aktualisierter Präventions-Flyer (vgl. Beratungsstelle Frauennotruf Frankfurt 2017a) für die Zielgruppe ab zwölf Jahren entwickelt, der den Bogen von mehr oder weniger alltäglichen digitalen Aktivitäten, bis hin zu strafbaren Handlungen und der Erläuterung des rechtlichen Rahmens schlägt. Behandelt werden nicht nur die Angriffsformen, die sich gegen Mädchen und Frauen richten, sondern auch eine deutliche Warnung an sie formuliert, nicht selbst den digitalen Raum zu nutzen, um andere zu diffamieren, zu bedrohen oder zu beleidigen.
- 2009 der Videospot »Folgenschwer« entwickelt, zugeschnitten auf jugendliche Nutzer*innen des digitalen Raums. Der Spot handelt von einer jungen Frau, die nach einer Party mit einem jungen Mann nach Hause geht. Dieser macht intime Aufnahmen von ihr und veröffentlicht diese nach Ende der Beziehung in ihrem schulischen Umfeld. Der Abspann infor-

2 Bei Happy Slapping werden körperliche Angriffe auf eine oder mehrere Personen gefilmt und die Aufnahmen öffentlich im Internet oder in bestimmten Gruppen geteilt.

miert, dass die Beratungsstelle Frauennotruf Frankfurt in solchen Fällen hilft und zeigt unsere Kontaktdaten.[3]
- die ebenfalls inzwischen mehrfach aktualisierte Broschüre »Digitale Gewalt« (vgl. Beratungsstelle Frauennotruf Frankfurt 2017b) entwickelt. Diese richtet sich an erwachsene Betroffene und Multiplikator*innen, die sich mit digitaler Gewalt auseinandersetzen oder konfrontiert sehen.

Seit den hier genannten ersten Veröffentlichungen wurden unsere Flyer und Broschüren stetig überarbeitet. Auch neue Publikationen gehen auf das Themenfeld ein und erläutern alltägliche und professionelle Umgangsweisen mit digitalen Medien und digitaler Gewalt.

Erfahrungen aus der Beratungspraxis

Im Folgenden werden einige Fallkonstellationen erläutert, die einen feministischen Beratungsansatz im Umgang mit digitaler Gewalt und Erfahrungen aus der Praxis beschreiben. Diese sollen einen Eindruck über die von den Mädchen und Frauen thematisierten Problemstellungen und den Beobachtungen der Beraterinnen vermitteln.

Fallkonstellationen

Neben den oben erwähnten ersten Fällen haben sich in der Zwischenzeit auch Frauen und Mädchen mit anderen digitalen Gewalterfahrungen an uns gewandt. So melden sich beispielsweise Frauen, die durch Täter mittels digitaler Gewalt gezielt in berufliche Schwierigkeiten gebracht werden. Neben Diffamierungen und Verleumdungen, wie z.B. »XYZ treibt es mit jedem!«, kursieren beispielweise E-Mails mit einer gefälschten Mail-Adresse der betroffenen Frau im Intranet, in denen Kolleg*innen beleidigt werden. So werden Konkurrenzen ausagiert, Frauen für die Ablehnung einer Liebesbeziehung ›bestraft‹, am Arbeitsplatz diskreditiert und so existenziell gefährdet. In diesen Fällen ist es oftmals unerlässlich, Vorgesetze oder Arbeitgeber*innen zu informie-

3 Der Spot wurde im Rahmen eines Praxisseminars von Student*innen der Fachhochschule Wiesbaden in Kooperation mit der Werbeagentur Young & Rubicam entwickelt. Er kann gern verwendet werden und ist auf unserer Website zu finden unter: https://frauennotruf-frankfurt.de/infothek/videos/folgenschwer/[Zugriff: 30.6.2020].

ren und immer erforderlich, eine Beratung in einer Kanzlei für Arbeitsrecht wahrzunehmen.

Berichtet wird auch häufig, dass Mädchen und Frauen selbst Aufnahmen gepostet oder verschickt haben und im Anschluss die Kontrolle über dieseverloren haben. Dass mit Aufnahmen, wie etwa Selfies, im sozialen Umfeld nicht immer diskret oder freundlich umgegangen wird, ist eine häufig anzutreffende Realität. Aufnahmen können in Klassen, auf Schulhöfen, in Vereinen, Firmen und Bekanntenkreisen und darüber hinaus kursieren. Manchmal ist das auch gewünscht, aber eben nicht immer, vor allem, wenn die Aufnahmen nicht ›perfekt‹ geworden sind. Auffällig ist, dass nicht die Veröffentlichung einer nur für einen bestimmten Adressaten gedachten Aufnahme von der Öffentlichkeit sanktioniert wird, sondern das Erwischt-Werden beim Posieren, Performen, Sich-Zeigen – alles Handlungen, die viele andere ebenfalls tun. Insbesondere bei intimen Aufnahmen befürchten Mädchen und Frauen ausgelacht oder als ›Schlampe‹ benannt und in Folge sozial geächtet zu werden.

In vielen der uns bekannt gewordenen Fällen kamen zu der Nötigung im Kontext digitaler Gewalt noch weitere Angriffe hinzu oder fanden bereits im Vorfeld statt. Die gravierendsten Fälle sind jedoch Schilderungen von Mädchen und Frauen, die vergewaltigt und dabei gefilmt wurden. Unabhängig davon, ob diese Aufnahmen jemals weitergegeben werden, ist die Bedrohung, dass eine Veröffentlichung jederzeit möglich ist, so stark, dass die Vergewaltigung selbst in den Hintergrund rücken kann. Laut Döll-Hentschker ist »alleine die Existenz von Bildern oder Filmmaterial ihrer Vergewaltigung […] für die betroffenen Frauen eine kaum vorstellbare psychische Belastung. Die Vergewaltigung hört quasi nie auf, kann jederzeit durch die Verbreitung der Bilder von neuem ablaufen.« (Döll-Hentschker 2012: 9) Hierüber potenzieren sich die Folgen der sexualisierten Gewalterfahrungen (vgl. ebd.).

Es kommen auch Mädchen und Frauen in die Beratung, die sich getrennt haben und von der Familie des Ex-Partners oder dessen Freund*innen permanent bei ihren Freizeitaktivitäten verfolgt und aufgenommen werden. Ob die Aufnahmen im Anschluss veröffentlicht werden oder nicht, ist nicht entscheidend. Allein die bestehende Option, dass sie aufgenommen wurden oder werden könnten, führt zu einer massiven Einschränkung der Lebensqualität und Mobilität. Betroffene vermeiden es, in den öffentlichen Raum zu gehen (wie etwa Schwimmbad, Restaurants oder Clubs) und sich frei zu bewegen.

Auch erleben wir Fälle in denen digitale Gewalt angedroht wird, um Betroffene von einer strafrechtlichen Verfolgung abzubringen, wie in dem Fall einer jungen Frau, die von ihrem Freund nach der geäußerten Trennungs-

absicht vergewaltigt wurde. Sie trennte sich dennoch und suchte, vermittelt über eine Lehrerin, unsere Beratungsstelle auf. Ihr wichtigstes Ziel war es, dass ihre Eltern und Geschwister auf keinen Fall von der Tat erfahren. Die junge Frau besuchte mehrfach unsere Beratungsstelle und war bereit eine Anzeige zu erstatten. Der Mann erfuhr jedoch vorab von der geplanten Anzeige und bedrohte die 17-Jährige damit, dass er Aufnahmen der Vergewaltigung bei Facebook verbreiten würde. Trotz guter juristischer Aussichten und dem Hinweis, dass ein gezieltes Vorgehen den Mann rechtzeitig stoppen kann, äußerte die Frau, dass sie jegliches Vorgehen gegen den Aggressor beenden wolle, in der Hoffnung, dass die Aufnahmen nicht ins Netz gelangen. Sie befürchtete, dass ihre Familie von der Vergewaltigung erfahren könnte.

Da so viele Betroffene aus den beschriebenen Gründen eine Anzeige vermeiden, kommen Delikte aus dem Bereich der digitalen Gewalt bei Polizei und Justiz häufig als Einzelfälle oder subsumiert unter den Körperverletzungs- oder Vergewaltigungsdelikten vor. Dies ist auch einer der Gründe dafür, dass es wenig statistisches Material und wenig veröffentlichte Rechtsprechung hierzu gibt.

Hindernisse bei der Kontaktaufnahme

Wie bei anderen Gewaltformen zeigt sich auch bei digitaler Gewalt, dass Betroffene sich häufig zunächst auf die eigene vermeintliche Schuld fokussieren. Sie fragen sich, ob sie ›unvorsichtig‹ waren oder ob sie mit einem anderen Verhalten den Angriff verhindern oder hätten vermeiden können. Dies ist z.B. der Fall, wenn sie ihrem (Ex-)Partner selbst eigene Nacktaufnahmen geschickt haben und dieser nun droht, die Aufnahmen an Eltern, Schulkamerad*innen oder Arbeitgeber*innen weiterzugegeben, um ihrem Ruf und Ansehen zu schaden. Solche Selbstvorwürfe verursachen Scham und verhindern häufig ein aktives und zügiges Vorgehen gegen eine Bedrohung durch digitale Gewalt. Viele Mädchen und Frauen befürchten zudem Vorwürfe ihres sozialen Umfeldes und trauen sich daher nicht über die Angriffe zu sprechen.

Insbesondere bei Jugendlichen besteht die Befürchtung, dass Erwachsene von der Bedrohung erfahren und im Anschluss die digitalen Aktivitäten der Jugendlichen einschränken. Diese berechtigte Angst führt häufig dazu, dass keine Unterstützung gesucht wird. Hinzu kommt, dass die meisten jungen Menschen (wie auch viele Erwachsene) keine Erfahrungen mit Unterstützungssystemen wie etwa Beratungsstellen haben. Vielleicht informieren sie sich im Internet. Wie bei anderer Gewalt ist der Schritt, sich Fachbera-

tungsstellen oder Erwachsenen anzuvertrauen, vielen zu hochschwellig und suspekt. Mädchen und junge Frauen wenden sich oftmals erst an uns, wenn ihnen die Bedrohung buchstäblich über den Kopf gewachsen ist. So meldete sich z.B. eine 17-Jährige, die nach Beendigung einer Liebesbeziehung damit bedroht wurde, dass intime Aufnahmen von ihr an ihre Eltern weitergegeben werden sollten. Der Täter nutzte hierbei gezielt das Wissen, dass die Eltern des Mädchens eine Beziehung vor der Ehe missbilligten. Die Betroffene befürchtete zu Recht massive Auswirkungen auf ihr Leben, wenn die Beziehung bekannt werden würde.

Die Verbreitung von intimen oder ›freizügigen‹ Aufnahmen in der Familie, der Community oder dem sozialen Umfeld wird durch Betroffene als kaum zu bewältigende Bedrohung erlebt, die oft dazu führt, dass sie in Angst regelrecht erstarren und sich isolieren, da sie annehmen, dass es für sie keine Hilfe gibt. In der Konsequenz erfüllen sie die Forderungen der Täter mit der Hoffnung, er würde aufhören oder seine Drohungen nicht wahr machen. Solche Fälle zeigen, dass digitale Gewalt oftmals mehrere Ebenen aufweist, die in der Beratung bedacht werden müssen.

Viele Betroffene scheuen aus Scham eine Kontaktaufnahme mit der Polizei oder einer Beratungsstelle. Scham, so Döll-Hentschker:

> »ist eine Emotion, die im Zusammenhang mit digitaler, körperlicher und/oder sexualisierter Gewalt eine wichtige Rolle spielt. […] Je größer die Scham, desto größer ist der Wunsch zu verschwinden. Scham ist eine Emotion, die einer nach außen gerichteten Handlung entgegen wirkt. Wer sich verbergen will, erstattet keine Anzeige, die erklärt, begründet und belegt werden muss […]. Die Veröffentlichung von Fotos beispielsweise im Internet […] kann eine andauernde und kaum zu bewältigende Scham auslösen. Es ist nicht überschaubar, wer alles die Bilder zu sehen bekommt.« (ebd. 2012: 8f.)

Auch dies können wir aus der Praxis bestätigen. Den Betroffenen ist es peinlich, dass die Aufnahmen im Rahmen einer Strafanzeige auch von den Beamt*innen und anderen Beteiligten angesehen werden könnten. Sie hoffen, dass der Aggressor das Interesse an der Bedrohung verliert. Jedoch: In allen uns bekannten Fällen hat nie ein*e Täter*in ›einfach so‹ aufgehört. Wenn eine betroffene Person allerdings sofort reagiert, besteht eine Chance, Aufnahmen löschen zu lassen, ihre Verbreitung einzudämmen und Täter*innen zur Verantwortung zu ziehen.

Ein feministischer Beratungsansatz gegen digitale Gewalt

Die Beratung von Frauen und Mädchen, die von digitaler Gewalt betroffen sind, ist komplex und erstreckt sich häufig über einen längeren Zeitraum. Sie ist dennoch weniger voraussetzungsvoll als häufig angenommen wird, da bei Bedarf Expertise von außen dazu geholt werden kann. Auch wenn die Berater*innen keine ›digital Natives‹ sind, sind die Täter-Opfer-Beziehungen, Falldynamiken und strafrechtlichen Möglichkeiten im digitalen Raum oftmals dieselben wie im nicht-digitalen Raum.

Die Beratungen können nur dann gelingen, wenn Betroffene dabei unterstützt werden, zügig und mithilfe aller erforderlichen Expertise, gegebenenfalls auch unter Einsatz finanzieller Mittel, gegen Täter*innen vorzugehen. Nur so kann weiterer Schaden abgewendet und bisher entstandener Schaden effektiv eingedämmt werden. Daher sind Kooperationen und die Vernetzung von Beratungsstellen mit Technikexpert*innen und Rechtsanwält*innen in dem Themenfeld digitaler Gewalt dringend notwendig.

Ziel der Beratung ist es, den Betroffenen zu vermitteln, dass digitale Gewalt zeitnah beendet werden kann, wenn frühzeitig und gezielt dagegen vorgegangen wird. Täter-Opfer-Umkehrungen und andere Dynamiken werden besprochen und Mädchen und Frauen aufgezeigt, dass sie sich adäquat zur Wehr setzen können. Grundsätzlich zielt digitale Gewalt auf Herabsetzung, Rufschädigung, soziale Isolation und die Nötigung zu einem bestimmten Verhalten. Ziel ist es auch, Gefühle von Hilflosigkeit und Angst hervorzurufen und die Betroffenen zum Schweigen zu bringen. Die Angriffskonstellationen sind im Kontext der feministischen Antigewaltarbeit hinlänglich bekannt, ebenso das strafrechtliche Vorgehen, nur erfolgen die Angriffe zusätzlich oder ausschließlich mittels digitaler Medien. In der Beratung geht es darum, die verschiedenen Ebenen der Angriffe zu identifizieren, die individuellen Folgen zu benennen und ein mögliches Vorgehen zu skizzieren. Wir ermutigen Betroffene, über die Situation zu sprechen und mit diesem Schritt aus der von den Täter*innen geschaffenen Isolation zu treten. Dabei vermitteln wir, dass Schweigen oder ›Nichts-tun‹ in der Regel zu einer weiteren Bedrohung durch die Täter*innen führen kann.

Wir zeigen in der Beratung auf, dass

- digitale Angriffe nicht in einem rechtsfreien Raum stattfinden.
- Abwarten und Stillhalten eine Strategie darstellt, die vor allem dem*der Angreifer*in zuspielt.

- es auch in den Fällen, in denen ein strafrechtliches oder zivilrechtliches Vorgehen nicht möglich ist oder nicht gewünscht wird, Wege gibt, sich zur Wehr zu setzen.

Neben Fragen von Schutz und wie sich die Situation der Betroffenen verbessern lässt, werden die Möglichkeiten eines individuellen Vorgehens erörtert. Gefragt werden muss, welche Unterstützung es im sozialen Umfeld gibt. Wir prüfen gemeinsam vorhandene Ressourcen und besprechen die Bedürfnisse der Betroffenen. Ganz grundsätzlich geht es in der Beratung auch um einen umsichtigen Umgang mit eigenen Daten und Aufnahmen – auch und besonders in engen sozialen Beziehungen und darum, die eigenen Grenzen in dem nicht-digitalen wie auch digitalen Raum wahrzunehmen und zu schützen. In der Beratung werden die Konsequenzen eines Nichthandelns bei digitaler Gewalt sehr deutlich besprochen. Der Schaden wächst rasant, wenn die Gefahr besteht, dass Aufnahmen veröffentlicht werden oder sich Gerüchte verbreiten. Aus diesem Grund muss konsequent und zügig vorgegangen werden.

Insgesamt sollten Berater*innen sich davor hüten, Aufnahmen von betroffenen Personen anzusehen, auch wenn dies (in Einzelfällen) angeboten wird. Nicht zu unterschätzen ist die »Macht der Bilder« (Döll-Hentschker 2012: 9), denn

> »Dritte, die mit solchen Bildern konfrontiert werden, können diese nicht vergessen, selbst wenn sie solidarisch mit der Frau sind und das Veröffentlichen der Bilder verurteilen. Die Bilder werden von nun an immer ein Teil in der Beziehung mit dieser Frau sein. Das wissen auch die Frauen. Die Schamgefühle werden dadurch immer wieder reaktiviert. Das Sehen der Bilder verändert die Beziehung. Insofern ist es ein berechtigtes und nachvollziehbares Anliegen der Frauen, dass die Menschen, an die sie sich zwecks Unterstützung wenden, diese Bilder nicht zu sehen bekommen.« (ebd.)

Fester Bestandteil der Beratung ist, wie in anderen Fällen auch, die Funktion einer Anzeige und der Ablauf eines möglichen Verfahrens.[4] Das weitere juristische Vorgehen lässt sich an spezialisierte und engagierte Rechtsanwält*innen abgeben. Wichtig ist zudem, dass Betroffene strukturiert zu einer oder einem Rechtsanwält*in gehen: d.h. sie sollten dort eine vorbereitete und kurze Zusammenfassung des Geschehens abgeben. Es gilt anzuregen und abzu-

4 Siehe Beitrag: Möglichkeiten und Grenzen strafrechtlicher Interventionen bei digitaler Gewalt.

klären, wer sie gegebenenfalls bei einer chronologischen Auflistung und der Dokumentation von digitalen Gewalthandlungen unterstützen kann. Umso wichtiger ist es, Expert*innen aus dem digitalen Bereich hinzuzuziehen und z.B. die Wiederherstellung oder das Löschen von Daten im Internet zu forcieren.

Wenn sich in der Beratung Anhaltspunkte für Spionage, Überwachung und Ortung ergeben, sollten die Frauen dringend aufgefordert werden ihre Geräte von Technikexpert*innen überprüfen zu lassen. Zu fragen ist, ob die Beratung in solchen Fällen in der Einrichtung stattfinden kann und ob die Vertraulichkeit der Beratung in solchen Fällen gewährleistet ist. Immer wieder bestätigten die betroffenen Personen, dass die Täter*innen aus dem sozialen Umfeld stammen, z.B. ehemalige Partner*innen, die bei der Einrichtung ihrer Geräte geholfen haben oder einen Moment genutzt haben, in denen Geräte unbeaufsichtigt waren. Da jedoch inzwischen Spionageprogramme über das Internet auf Geräte aufgespielt werden können, ohne diese in den Händen zu halten oder auf Webcams zugegriffen werden kann, hat sich die Problematik vervielfacht. Für technische Fragen und die Überprüfung von Geräten empfiehlt es sich, dass die Beratungsstelle zunächst die Person anspricht, die den technischen Support in der beratenden Einrichtung leistet, da diese bereits das Vertrauen der Einrichtung genießt und befähigt ist, Geräte zu prüfen. Zusätzlich finden sich einige alltagspraktische Tipps und Hinweise für den Schutz von Handy und Privatsphäre in einem Flyer des bff »Sicher mit Smartphone« (bff: Bundesverband Frauenberatungsstellen und Frauennotrufe o.J.). Selbstverständlich müssen für Mädchen und Frauen ohne finanzielle Mittel für anwaltliche Beratung oder Technik-Überprüfung, wie bei allen anderen Angriffsformen auch, Wege gefunden werden.[5]

5 Digitale Gewalt erfordert schnelles Handeln und Expert*innen, die professionell und zügig agieren können. Der Verweis auf die anwaltliche Beratungshilfe ist in solchen Fällen oftmals schwierig, da die Fallkonstellationen häufig sehr komplex und arbeitsaufwendig sind und eine Beratungshilfe bei Weitem nicht kostendeckend ist. Jedoch ist teilweise eine anwaltliche Beratung finanziert über eine Rechtsschutzversicherung möglich. Eine anwaltliche Erstberatung, die selbst finanziert werden muss, kann um die 250 Euro kosten.

Auswirkungen digitaler Gewalt

Folgen von digitaler Gewalt sind gesundheitsgefährdend und schränken z.T. die Lebensqualität massiv ein. Beschrieben werden starke Verunsicherung, Hilflosigkeit, Selbstzweifel, Misstrauen, Angstzustände, sozialer Rückzug, somatische Erkrankungen, Gefühle ständiger Bedrohung, Schlafstörungen und Leistungsblockaden. Dies kann zu sogenannten reaktiven psychischen Erkrankungen wie Depressionen und Ängsten, sozialer Isolation, Ausbildungsabbrüchen, Schul- und Jobwechsel und Umzügen führen.

In den Beratungen stehen für die Betroffenen häufig die Fassungslosigkeit darüber, dass sie sich in einer oder mehreren Personen so getäuscht haben und der Bruch des Vertrauens im Vordergrund. Die eigentlichen Täter*innen, die die Aufnahmen veröffentlicht haben, geraten völlig aus dem Blickfeld. Die Betroffenen stehen als naiv oder ›Selbst-Schuld-Daran‹ da und fühlen sich schlecht und schuldig. Diese Dynamik einer solchen Täter-Opfer-Umkehr ist regelmäßiges Thema in der Beratung.

Eine ebenfalls gravierende Auswirkung, die in der Beratung vorsichtig besprochen wird, ist die Gefahr, dass mittels der breiten Veröffentlichung von Aufnahmen, wie etwa erotische Aufnahmen aus einer romantischen Beziehung oder dem Filmen von sexualisierter Gewalt, auch andere Personen die Betroffene potentiell als wehrloses Objekt wahrnehmen könnten. Somit gerät das Mädchen oder die Frau in Gefahr erneut ›Opfer‹ von Gewalthandlungen zu werden. Wir konnten über die Jahre immer wieder feststellen, dass es Jungen und Männer gibt, die das Wissen um die Gewalterfahrung einer Betroffenen zu animieren scheint, selbst übergriffig oder gewalttätig ihr gegenüber zu werden.

Bei der Androhung, intime Aufnahmen an Eltern oder Arbeitgeber*innen zu senden, handelt es sich zumeist um einverständlich aufgenommene Fotos oder Videos bzw. mit der Webcam übertragene Aufnahmen. Bei der Herstellung solcher Aufnahmen wurde oftmals nicht überlegt, was mit diesen nach dem Abend, in zwei Monaten, nach zwei Jahren oder nach dem Ende einer Affäre oder Beziehung geschehen soll und könnte. Sehr viele Frauen gehen davon aus, dass sie selbstverständlich mitentscheiden, wie mit diesen Bildern und Videos umgegangen wird. Die wenigsten konnten sich zu dem Zeitpunkt der Beziehung die Gefahr einer Veröffentlichung oder Weitergabe vorstellen – der darin enthaltene Vertrauensbruch war ihnen unvorstellbar. In der Beratung fragen sie sich, warum sie sich auf die Aufnahmen eingelassen haben, sie fühlen sich schuldig, verantwortlich und schämen sich. Auffällig ist, dass

zu diesem Zeitpunkt nicht mehr differenziert wird; die Zustimmung zur Aufnahme, deren Weiterleitung oder Speicherung unter der Maßgabe, dass diese vertraulich bleibt, ist eine völlig andere gewesen, als die Zustimmung zur Veröffentlichung. Dass die Mädchen und Frauen letzteres nicht erlaubt haben, hat emotional für sie im Nachhinein wenig Bedeutung und muss erst in der Beratung wieder angeeignet werden.

Sehr oft äußern Betroffene, dass sie vieles dafür tun würden, damit nicht noch weitere Personen, potentielle Unterstützer*innen inbegriffen, von den Aufnahmen erfahren. Dies bleibt den Tätern in der Regel nicht verborgen und so können sie den Druck oder die direkte Gewalt erhöhen. Die Mädchen und Frauen befürchten oftmals eine fortdauernde Gefährdung, da digital gespeicherte Aufnahmen auch noch Jahre später öffentlich gemacht werden können, d.h. auch dann, wenn sie sich in Sicherheit wiegen.

Digitale Angriffe gegen öffentliche Personen und Unterstützungseinrichtungen

Nicht nur Einzelpersonen, sondern auch Wissenschaftler*innen und Journalist*innen, feministische Initiativen, Institutionen und Gruppen wurden in den letzten Jahren mittels digitaler Gewalt attackiert. So wurden z.B. Hatestorms ausgelöst oder Einzelpersonen diskreditiert und beleidigt, nicht selten bis hin zu offensiven Vergewaltigungsandrohungen. In den Fokus solcher Angriffe können auch sehr schnell Fraueneinrichtungen und Gleichstellungsbüros gelangen. Auch die Arbeit von Beratungsstellen kann davon betroffen sein. Vor einigen Jahren wurde ein Werbebild unserer fortlaufenden Kampagne »Soforthilfe nach Vergewaltigung« in einem rechten Portal eingestellt und massenhaft kommentiert. Es zeigte eine Ärztin mit Migrationsgeschichte und wurde genutzt, um rechtsextreme und rassistische Vorstellungen darüber zu transportieren, wer in Deutschland die Täter- und wer die Opfergruppen von sexualisierter Gewalt sind, wer versorgt werden sollte – und wer nicht. Wir meldeten die Kommentare dem hessischen Verfassungsschutz und erstatteten Anzeige. Diese wurde eingestellt, der Server stehe unerreichbar im Ausland. Solche Angriffe gehören für uns auch zu dem Themenkomplex digitale Gewalt.[6]

6 Informationen zum Umgang damit können betroffene Einrichtungen in der Broschüre »Wachsam Sein! Zum Umgang mit rechten und rechtsextremen Einschüchterungsver-

Ausblick

Die Beratung von Frauen und Mädchen bei digitaler geschlechtsspezifischer Gewalt kann sehr gut an die Expertise feministischer Beratungsstellen anknüpfen. Notwendiges technisches und rechtliches Wissen sollte u.a. durch das Hinzuziehen von Expert*innen eingeholt werden. Der Aufbau von entsprechenden Kooperationen und Netzwerken ist dringend notwendig. Trotz aller Spezifika des Feldes, wie etwa Kenntnisse um Apps und Medien, umfassen die Delikte, die unter digitaler Gewalt gefasst werden, bereits bekannte Straftatbestände. Berater*innen können beispielsweise die Broschüre »Digitale Gewalt« (vgl. Beratungsstelle Frauennotruf Frankfurt 2017b) vorbereitend sowie während der Beratung zur Hilfe nehmen. So können sie sicher sein, dass sie die relevanten Themen und Vorgehensweisen ansprechen.[7]

Auch die Strukturen einer Beratungsstelle müssen dem Thema digitale Gewalt gerecht werden. Diskutiert werden muss, wie sich die Einrichtung und auch die einzelnen Berater*innen digital präsentieren, die Frage des Datenschutzes ebenso wie die datenrechtliche Ansprache der Klient*innen, bevor die eigentliche Beratung beginnt. Das Recht auf die datenbezogene Selbstbestimmung Anderer gilt auch für die Mitarbeiter*innen der Beratungsstellen. So muss sichergestellt werden, dass die Beratung nicht aufgezeichnet wird.

Anknüpfend an eine feministische Tradition der Aneignung des öffentlichen Raums bzw. der Verweigerung sich aus diesem Zurückzuziehen, ist letztlich das Ziel all unserer Bemühungen, Mädchen, Frauen und Betroffene von digitaler Gewalt dabei zu unterstützen, einen bewussten Umgang mit ihren Daten und Medien zu pflegen. Es ist uns wichtig, dass Mädchen und Frauen sich nicht aus dem digitalen Raum zurückziehen, sondern sich diesen aktiv und solidarisch aneignen.

---

suchen und Bedrohungen« (vgl. Verein für Demokratische Kultur in Berlin und Mobile Beratung gegen Rechtsextremismus Berlin 2017) oder in Beratungsstellen zu rechter Gewalt finden.

7 Auf der Plattform https://*www.aktiv-gegen-digitale-gewalt.de* finden sich weitere relevante Informationen und Sicherheitshinweise für Berater*innen und Betroffene von digitaler Gewalt.

Literatur

Beratungsstelle Frauennotruf Frankfurt (Hg.) (2017a): »Digitale Gewalt«. Flyer. https://frauennotruf-frankfurt.de/fileadmin/redaktion/pdf/FNR-Flyer-Digitale-Gewalt-2017-06.pdf [Zugriff: 15.1.2020].

Beratungsstelle Frauennotruf Frankfurt (Hg.) (2017b): »Digitale Gewalt«. Broschüre. https://frauennotruf-frankfurt.de/fileadmin/redaktion/pdf/FNR-Broschuere-Digitale-Gewalt-2017-06.pdf [Zugriff: 15.1.2020].

bff: Bundesverband Frauenberatungsstellen und Frauennotrufe (Hg.) (2013): »Handreichung zur Qualitätsentwicklung und Qualitätssicherung in der Beratungsarbeit der Frauennotrufe und Frauenberatungsstellen«. https://frauennotruf-mainz.de/files/downloads/bff_qualitaetsstandards_2.auflage.pdf [Zugriff: 15.1.2020].

bff: Bundesverband Frauenberatungsstellen und Frauennotrufe (Hg.) (2017): »Fachberatungsstellen und die Digitalisierung geschlechtsspezifischer Gewalt. Ergebnisse einer Umfrage unter Frauenberatungsstellen und Frauennotrufen im bff«. https://frauen-gegen-gewalt.de/de/aktuelle-studien-und-veroeffentlichungen.html [Zugriff: 15.1.2020].

bff: Bundesverband Frauenberatungsstellen und Frauennotrufe (Hg.) (o.J.): »Sicher mit Smartphone«. https://frauen-gegen-gewalt.de/de/digitale-gewalt-material/sicher-mit-smartphone.html [Zugriff: 15.1.2020].

Döll-Hentschker, Susanne (2012): »Scham und Gewalt«, in: Beratungsstelle Frauennotruf Frankfurt (Hg.), Tätigkeitsbericht 2011, S. 8-9.

Verein für Demokratische Kultur in Berlin/Mobile Beratung gegen Rechtsextremismus Berlin (Hg.) (2017): »Wachsam Sein! Zum Umgang mit rechten und rechtsextremen Einschüchterungsversuchen und Bedrohungen«. https://mbr-berlin.de/wp-content/uploads/2017/03/mbr_broschuere_wachsamsein_Web_klein.pdf [Zugriff: 22.2.2020].

Das Internet der Dinge
Die Auswirkungen »smarter« Geräte auf häusliche Gewalt

Leonie Maria Tanczer

Digitale Gewalt beschreibt wie digitale Medien (z.B. Handys oder das Internet) zur Belästigung oder Kontrolle von Personen genutzt werden. Im Zusammenhang mit häuslicher Gewalt und Gewalt in der Partnerschaft kann digitale Unterdrückung viele Formen annehmen (vgl. Dragiewicz u.a. 2018; Harris/Woodlock 2018; Woodlock 2017). Sie kann obszöne oder ungewollte Nachrichten oder Anrufe umfassen, bildbasierte Grenzüberschreitungen wie ›Rache Pornos‹ (vgl. Citron/Franks 2014; McGlynn/Rackley/Houghton 2017) sowie Aufspürgeräte, sogenannte Tracker, welche durch Mobiltelefone oder andere Systeme steuerbar sind. Digitale Gewalt ist hier als ein großes ›Sammelbecken‹ vorstellbar, in dem sowohl technisch ›einfache‹ Delikte sowie technisch anspruchsvollere Vergehen zusammenkommen. Die Letzteren beinhalten zum Beispiel unautorisierte Zugriffe auf E-Mail-Konten oder die Verwendung von dedizierter Spionagesoftware (Spyware)[1].

Das Internet der Dinge

Der rasante Technologiewandel bietet Täter*innen immer mehr Instrumente zur Kontrolle von Opfern und Betroffenen. Insbesondere der Anstieg von »smarten« Internet-verbundenen Geräten – auch bekannt als das »Internet der Dinge« (Internet of Things, kurz: IoT) – sollte genauer unter die Lupe genommen werden. IoT ist ein Überbegriff für verschiedene Technologien.

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

Die Bezeichnung beschreibt Objekte – häufig Produkte, die zuvor offline und daher analog waren – welche jetzt netzwerkfähig sind. Solche miteinander verbundenen »Dinge« sind die direkte Erweiterung des Internets in eine Reihe von Geräten und Waren (vgl. Tanczer u.a. 2019b: 37). Das sich manifestierende neue digitale Umfeld – wie etwa das »Smart Home« – besteht somit nicht mehr nur aus Internet-verbundenen Telefonen, Laptops und Computern, sondern vielen anderen alltäglichen Gegenständen wie etwa Türen, Heizungen und Glühbirnen. Unsere »smarte« Zukunft zeichnet sich deshalb erstens durch eine Ausbreitung von verschiedenen Gebrauchsgegenständen aus, die scheinbar unsichtbar Daten sammeln; zweitens durch Systeme, die diese gesammelten Informationen interpretieren und nutzen; und drittens durch Antriebselemente, die auf Basis dieser Daten ohne direkte menschliche Handlung Maßnahmen ergreifen.

Solche »intelligenten« oder »digital aufgerüsteten« Produkte (vgl. Mattern/Floerkemeier 2010: 107) sind jedoch nicht nur die typischen Gadgets, die wir mit dem Begriff IoT verbinden. Neben gewohnten IoT-Geräten wie smarte Toaster, Türschlösser oder Kühlschränke, beschreibt der Begriff IoT auch winzige Sensoren, die Daten wie die Feuchtigkeit, Temperatur oder Luftqualität messen. Darüber hinaus bezeichnet IoT auch größere cyberphysische Systeme, die sowohl untereinander als auch mit dem Menschen kommunizieren können. Ein Beispiel hierfür wären selbstfahrende, autonome Fahrzeuge. Die Anwendungsbereiche des IoT sind daher breit gefächert und reichen von Geräten zur Steigerung der persönlichen Fitness, Produkte für die Unterstützung von betreutem Wohnen bis hin zu umfangreichen Verkehrsmanagement- und Verkehrsinfrastrukturen (vgl. Tanczer u.a. 2018e: 1). Die endlosen Möglichkeiten, die sich aus der Kommunikation zwischen Geräten und der damit assoziierten Datensammlung ergeben, erklärt, warum IoT-Systeme mit dem Begriff smart (im Sinne von klug) in Verbindung gebracht werden. Die Netzwerkfunktionalität birgt jedoch auch erhebliche Risiken, die einer genaueren Prüfung bedürfen. Auf den folgenden Seiten werden Erkenntnisse aus dem Forschungsprojekt Gender and IoT (GIoT) besprochen (vgl. Lopez-Neira u.a. 2019; Parkin u.a. 2019; Tanczer u.a. 2018b). GIoT ist ein interdisziplinäres Projekt am University College London (UCL) in Großbritannien. Das Forschungsteam hat die Veränderungen, die digitale Gewalt im Kontext von häuslicher Gewalt unterläuft, im Laufe der letzten drei Jahre genauer untersucht. Einige der Ergebnisse dieser Forschungsaktivitäten beinhalten Handlungsempfehlungen für Beratungsstellen, politische

Akteur*innen sowie IoT-Entwickler*innen (vgl. Tanczer u.a. 2018b; Tanczer u.a. 2018c; Tanczer u.a. 2019c).

Dieser Artikel enthält deshalb Informationen zu den Eigenschaften und denkbaren Auswirkungen von IoT-Systemen im Rahmen von häuslicher Gewalt. Daran anschließend folgt eine Auflistung möglicher Interventionsmöglichkeiten. Diese sollen vor allem den Betroffenen dienlich sein, mögen aber auch Hilfseinrichtungen, Industrievertreter*innen und Politiker*innen nützliche Ideen bieten. Alle besprochenen Vorschläge sollten selbstverständlich stetig neu bewertet, kontinuierlich verbessert und durchgehend getestet werden. Nur ein sich wiederholender, reflektierter sowie Trauma-informierter Interventionsprozess, basierend auf Forschungsdaten sowie den Bedürfnissen von Betroffenen, kann evidenzbasierte Lösungen sowie gut informierte Entscheidungen (von denen es leider immer noch nicht genug gibt) garantieren. Der Artikel präsentiert demnach hoffentlich eine geeignete Grundlage für Leser*innen, die sowohl in der Wissenschaft als auch der Praxis tätig sind. Er stellt Orientierungshilfen dar, um diese neue Form der IoT-unterstützten digitalen Gewalt besser zu verstehen und souveräner bekämpfen zu können.

Anstieg und Auswirkungen des Internets der Dinge

Trotz der zunehmenden Verbreitung digitaler Technik in unserem täglichen Leben gibt es immer noch wenig Forschung und Gutachten zu der wachsenden Bedrohung, die von digitaler Gewalt ausgeht (vgl. Henry/Powell 2018: 196). Bis heute ist die britische Frauenberatungsstelle Refuge eine der wenigen Organisationen in Großbritannien (wenn nicht sogar die Einzige), die digitale Gewalt explizit in ihrem Archiviersystem vermerkt. Als Folge dieser Dokumentation weist Refuge darauf hin, dass im Jahr 2019 72 % ihrer Klient*innen Gewalt durch digitale Systeme erlebten (vgl. Refuge 2020a: o.S.). Bedenkt man, dass dies nur die Erfahrung einer einzigen Beratungsstelle in Großbritannien ist, so muss davon ausgegangen werden, dass die Anzahl, der von digitaler Gewalt betroffenen Frauen, sehr hoch sein dürfte. Leider lässt die Statistik die Nuancen von digitaler Gewalt nicht erkennen und erlaubt es daher nicht, zwischen verschiedenen Formen, Ausprägungen und Schweregraden zu unterscheiden.

Die Analyse von Refuge verweist auf die gegenwärtigen Bemühungen zum Thema digitale Gewalt. Diese Bestrebungen setzen sich primär mit ›konventionellen‹ digitalen Risiken wie dem Missbrauch auf Social Media

Plattformen oder dem Vorbehalt von Geräten wie Laptops und Telefonen durch Täter*innen auseinander (vgl. Douglas/Harris/Dragiewicz 2019: 555). Allerdings verändert sich die Risikolandschaft für Betroffene ständig. Dies wird u.a. durch den zunehmenden Einsatz von Drohnen, Trackern oder »Hacker-for-Hire-Diensten«[2] in Gewaltbeziehungen immer deutlicher. IoT im Speziellen beschreibt eine Entwicklung von Technologien, welche die Risikoverläufe für Betroffene von häuslicher Gewalt erweitern können. Zugleich verschmilzt IoT mit einem ganzen Spektrum von anderen Anwendungsgebieten und Innovationen, einschließlich digitaler Zahlungssysteme, Blockchain-Technologien oder dem ominösen Begriff der künstlichen Intelligenz (vgl. Banerjee/Lee/Choo 2018). Letzteres kann als »Maschinelles Lernen« beschrieben werden und erklärt die Verwendung von statistischen Modellen, um Muster zu identifizieren und Präferenzen von Nutzer*innen besser einschätzen zu können.

Genau wie Handys und Laptops Teil unseres Lebens geworden sind, so können wir davon ausgehen, dass IoT gekommen ist, um zu bleiben. Schätzungen zufolge wird die Zahl der weltweit angeschlossenen IoT-Geräte jährlich um durchschnittlich 12 % steigen und voraussichtlich von fast 27 Milliarden im Jahr 2017 auf 125 Milliarden im Jahr 2030 wachsen (vgl. IHS Markit 2017: o.S.). Während diese Produkte noch nicht Teil jedes Haushalts sind und wir auch noch nicht über die exakten Daten zu ihrem Missbrauch in häuslichen Gewaltvorfällen verfügen (vgl. Tanczer u.a. 2018b: o.S.), sollte sich die Gesellschaft dennoch auf ihre missbräuchliche Verwendung vorbereiten. Eine ähnliche Dynamik haben wir auch im Zuge der Ausweitung digitaler Gewalt durch das Internet und Smartphones gesehen. In diesem Fall nahmen die Missbrauchsmuster parallel zu der steigenden Verfügbarkeit und Erschwinglichkeit dieser Systeme zu (vgl. Gámez-Guadix/Borrajo/Calvete 2018; Harkin/Molnar/Vowles 2020)[3]. In Anbetracht dieser Tatsache ist es von entscheidender Bedeutung, sich für die IoT-unterstützte Gewalt zu wappnen, vor allem, da ihr Gebrauch stetig wächst, ihre Funktionalität konstant zunimmt und die Kosten für diese Geräte immer weiter sinken.

---

2 Hacker-for-Hire-Dienste beschreiben Leistungen, welche gezielte Angriffe auf zum Beispiel E-Mail-Konten für jene bieten, die bereit sind für solche illegalen Aktivitäten zu bezahlen (vgl. Mirian 2019).

3 Siehe Beitrag: Erfahrungen mit der Beratung von betroffenen Mädchen und Frauen im Kontext digitaler Gewalt.

Was IoT-Systeme einzigartig macht, ist ihre Konnektivität, also ihre Verbundenheit untereinander. Mit diesen smarten Geräten können verschiedene Produkte miteinander verknüpft werden. Dadurch entsteht ein voneinander abhängiges Netzwerk, in dem im Grunde genommen alle einzelnen Gegenstände miteinander »sprechen« (vgl. Tanczer u.a. 2019b; Taylor u.a. 2018). Während viele IoT-Systeme gegenwärtig immer noch eine Form menschlichen Handelns erfordern – beispielsweise durch das Drücken einer Taste oder der Aktivierung über eine App – wird erwartet, dass sie bald ohne direktes menschliches Eingreifen operieren und die Gewohnheiten der Nutzer*innen im Laufe der Zeit ›lernen‹. Aufgrund ihrer Palette an Funktionen (einschließlich ihrer Fähigkeit ferngesteuert zu werden, Video- und Audioaufzeichnung zu tätigen und Standortinformationen zu teilen), haben IoT-Geräte das Potenzial, sowohl unser Verhältnis als auch unsere Interaktion mit digitalen Systemen sowie mit anderen Menschen zu verändern.

Die Risiken, die IoT für Betroffene von häuslicher Gewalt mit sich bringen, haben unter anderem Wissenschaftler*innen wie Leitão (2019), Strengers u.a. (2019) und Slupska (2019) begonnen zu erforschen. Deren Studien zeigen, welche Auswirkungen IoT auf die Sicherheit und Privatsphäre von Betroffenen digitaler Gewalt hat. In ähnlicher Weise führte das GioT-Forschungsteam eine »Usability«-Analyse[4] von persönlichen Sprachassistenten wie Google Home und Amazon Echo durch (vgl. Parkin u.a. 2019) und veröffentlichte eine Broschüre für Betroffene sowie Beratungsstellen (vgl. Tanczer u.a. 2018c). In beiden Publikationen wurden einige der häufigsten Risiken von IoT-Geräten zusammengefasst. Zu den Gefahren, die der gegenwärtige Stand der Literatur aufzeigt, gehören unter anderem der Missbrauch von smarten Technologien, um andere Menschen auszuspionieren, ihre Bewegungen zu verfolgen oder Kontrolle über sie auszuüben. Zum Beispiel ermöglicht die Fernsteuerung von Heizung, Beleuchtung und Jalousien es Täter*innen, ihre Opfer durch deren ungeahnten Einsatz aus der Ferne einzuschüchtern. Internet-verbundene Sicherheitskameras oder Smart TVs bieten die Gelegenheit Betroffene zu überwachen oder zu stalken. Intelligente Sicherheitssysteme wie Bluetooth-fähige Türschlösser bieten eventuell Zugang zu Immobilien. Alle diese Beispiele weisen auf die Fähigkeit von IoT-Systemen hin, ein Werkzeug für »Gaslighting« zu werden. Das letztgenannte Konzept beschreibt eine Form der psychischen

4 Eine Usability-Analyse beschreibt einen Gebrauchstauglichkeitstest, der Software- und Hardwareprodukte auf ihre potenzielle Verwendung sowie Missbrauch evaluiert.

Gewalt, die ein Opfer gezielt desorientiert und manipuliert, damit Betroffene sukzessive an deren Realität und Selbstbewusstsein zu zweifeln beginnen (vgl. Sweet 2019).

Parallel zu der missbräuchlichen Nutzung von IoT-Fähigkeiten fehlt es smarten Systemen häufig an etablierten Sicherheits- und Datenschutzstandards (vgl. Brass u.a. 2018; DeNardis 2020; DeNardis/Raymond 2017; Schneier 2017). In der Tat sind sie häufig mangelhaft konzipiert, bieten keine regelmäßigen Software-Updates und fordern Benutzer*innen oftmals nicht auf, Standardkennwörter zu ändern. Außerdem basieren IoT-Geräte auf der inhärenten Annahme, dass sich alle Benutzer*innen eines kommunalen Haushalts gegenseitig vertrauen und einen gleichen Kenntnisstand über den Umgang mit diesen Technologien haben. Dies berücksichtigt weder die in einer Gewaltbeziehung vorherrschende Machtdynamik zwischen Täter*in und Opfer (vgl. McCarthy/Mehta/Haberland 2018), noch dass Mitbewohner*innen gegebenenfalls unterschiedliche Präferenzen oder Datenschutzanforderungen haben (vgl. Muir/Joinson 2020).

Ferner durchläuft unsere Gesellschaft auch aktuell einen Wandel: weg von persönlichen zu gemeinschaftlichen, kollektiven Geräten. Diese Verschiebung weist darauf hin, dass wir Wege finden müssen, um digitale Produkte besser zu sichern. Zum einen bedeutet das, dass es nun nicht nur einzelne, personenbezogene Daten zu schützen gilt. Vielmehr müssen Daten über jede Person, die einen IoT-unterstützten Haushalt betritt, effektiv gesichert, aber auch gelöscht und modifiziert werden können. Zum anderen verändern solche »Gruppengeräte« die Dynamiken eines Haushaltes (vgl. Strengers u.a. 2019). Da in vielen Familien primär Männer – wie etwa Partner oder Söhne – für den Kauf, Installation und Wartung von technischen Systemen verantwortlich sind, kann eine solche Besitz- und Nutzungsverlagerung dazu führen, dass Frauen noch stärker von relevanten Entscheidungen sowie der Verwendung von digitalen Technologien ausgeschlossen werden.

Auch wenn smarte Produkte sicherlich auch positive Effekte für Betroffene von häuslicher Gewalt bieten können (vgl. Burdon/Douglas 2017: o.S.), die Allgegenwart, Reibungslosigkeit und Verbreitung von unseren neuen *immeran*-Geräten beschreibt einen besorgniserregenden Trend. Vor diesem Hintergrund werden im folgenden Abschnitt einige mögliche Interventionsoptionen erörtert. Diese Empfehlungen können hoffentlich dazu beitragen, den Missbrauch von IoT-Systemen gegen Betroffene von häuslicher Gewalt zu bekämpfen.

Interventionsmöglichkeiten

Viel zu häufig folgt der Entdeckung von Problemen, die durch Technik hervorgerufen wird, ein Aufruf nach noch mehr Technik. Doch kaum ein gesellschaftliches Übel – sei es häusliche Gewalt, Gewalt in der Partnerschaft oder sexueller Missbrauch – kann, noch sollte es, durch technische Mittel allein gelöst werden. Stattdessen sollte eine Mischung aus sozio-technischen Interventionsmöglichkeiten zum Einsatz kommen.

Menschenbezogene Interventionen

Partnergewalt ist kein neues Phänomen. Es ist ein grundsätzlich komplexes, systemisches und strukturelles Problem. Es umfasst eine Reihe von kontrollierenden und einschränkenden Verhaltensweisen, die nicht einfach durch eine App oder eine »Anti-Rape Technology«[5] bewältigt werden können. Eine tiefgreifendere Einsicht, die es in Hinblick auf digitale Gewalt zu teilen gibt, ist, dass es Interventionen benötigt, die sich an dem Bedarf der betroffenen Personen orientieren. Diese müssen die soziale Dynamik von Gewaltmustern berücksichtigen und sollten *von* Menschen *für* Menschen eingesetzt werden.

Betroffene digitaler Gewalt

Die aktuelle Bandbreite an ›raschen Lösungen‹, um digitaler Gewalt entgegenzuhalten, ist häufig belastend für die Betroffenen. Gegenwärtige Ansätze fordern von Betroffenen zu agieren, ihr Verhalten zu ändern und pro- sowie reaktive Maßnahmen zu treffen (vgl. Harris/Woodlock 2018: 539). Solche Interventionen sind zeitaufwändig, anspruchsvoll und kreieren zusätzliche Bürden für Personen, die bereits mit einer Palette von Stressfaktoren und Überlegungen konfrontiert sind. Derlei Lösungen umfassen Apps zum Protokollieren von Gewaltvorfällen[6], Webseiten, Beratungsdatenbanken und

5 Anti-Rape Technologies oder zu Deutsch Anti-Vergewaltigungstechnologien bezeichnen eine Bandbreite an Produkten, die zum Zweck der Verhinderung oder Abschreckung von Vergewaltigung erfunden wurden. Beispiele umfassen Keuschheitsgürtel, Anti-Fummel-Sticker, reißresistente Kleidung, Schnelltests die Drogen in Getränken evaluieren können bis hin zu »smarten« Ringen, die einen Panikknopf zum Alarmieren von Bekannten enthalten (vgl. Harris 2019: o.S.).

6 Siehe hierzu die Hestias Bright Sky-App und die NO STALK-App vom Weißen Ring.

Checklisten zum Nachlesen, wie auf digitale Gewalt reagiert werden kann[7] sowie Online-Beschwerdeformulare, um beispielsweise die Verwendung von nicht einvernehmlich geteilten Bildern zu melden.[8] Tatsächlich ist sogar das GIoT-Forschungsteam dieser Dynamik gefolgt und hat einen IoT-Überblick (vgl. Tanczer u.a. 2018d) sowie eine Ressourcenliste (vgl. Tanczer u.a. 2019c) veröffentlicht. Obgleich gut gemeint, kreieren all diese Maßnahmen Annahmen zum ›richtigen‹ Umgang mit Technologien und verschieben die Verantwortung, sich gegen solche Vorgehen zu wehren, an die Opfer anstelle der Verursacher*innen von Gewalt.

Eine stärkere Betonung sollte deshalb – wie auch bei analoger Gewalt – auf Opfer-zentrierte Lösungen gelegt werden. Vorgeschlagene Maßnahmen sollten nicht verlangen, dass Betroffene etwas zu lesen, melden oder verändern hätten. Vielmehr müssen Ansätze geschaffen werden, die ihre Situation erleichtern. Dies kann etwa durch die Bereitstellung von »One-Stop« Konzepten – sprich die Zentralisierung von verschiedenen Anlaufstellen, welche auch technische Unterstützung bieten – erreicht werden (vgl. Rising Sun 2020: o.S.). Ebenso mag die Einführung spezialisierter digitaler Gewalt-Hotlines, gezielter digitaler Gewalt-»Kliniken« (Havron u.a. 2019) sowie der Ausbau technischer Fähigkeiten im Beratungssektor dienlich sein (Tanczer u.a. 2018b: 6).

Die Kritik an der technischen ›Aufrüstung‹ und ›Reformierung‹ von Opfern durch Trainings oder durch die Vermittlung anderer Ratschläge ist von großer Relevanz in Bezug auf IoT. Smarte Geräte sind vielfältig. Ihre Einstellungen und Funktionen unterscheiden sich häufig und oft kann ein einziges Softwareupdate die Nutzer*innenoberfläche verändern. Solche Modifizierungen können dazu führen, dass Betroffene veröffentlichte schriftliche Anleitungen oder YouTube Videoerklärungen nicht Schritt für Schritt folgen können. Bedenkt man in welcher Belastungssituation sich Gewaltopfer befinden, so wird deutlich, wie problematisch und womöglich sogar unrealistisch solche Erwartungshaltungen sein können.

Das GIoT-Forschungsteam war immer darauf bedacht, Betroffenen keine universellen technischen ›Ratschläge‹ zu geben. Jede Empfehlung muss die

7 Siehe hierzu eSafety Women und bff-Webseite www.aktiv-gegen-digitale-gewalt.de. Auf dieser Plattform finden Betroffene von geschlechtsspezifischer digitaler Gewalt Informationen und Beratungsangebote in Fachberatungsstellen.

8 Siehe hierzu den Priority Channel der spanischen Datenschutzbehörde.

einzigartige Situation des Opfers berücksichtigen und sich an deren jeweiligem Risikoprofil ausrichten. Es empfiehlt sich zum Beispiel einer Person nicht schlichtweg die Anregung zu geben, ihr Passwort zu ändern; vor allem nicht, wenn die Möglichkeit besteht, dass der/die Täter*in heimlich Kontrolle über jene Technologie hat. Die Anweisung solche Einstellungen zu revidieren, kann bei gewalttätigen Partner*innen Verdacht und Misstrauen auslösen. Dies wiederum kann dazu führen, dass eine Gewaltsituation weiter eskaliert und sich das Opfer in einer noch brenzligeren Situation vorfindet. Die Berücksichtigung der verschiedenen Phasen der Gewalt in der Partnerschaft und die konkrete Situation, in der ein Opfer ist, sind daher von entscheidender Bedeutung (vgl. Matthews u.a. 2017b: 2193). Das Knowhow, das der Beratungssektor in Bezug auf die Evaluierung von Gewaltkontexten derzeit hat, darf deshalb nicht unterschätzt werden. Des Weiteren bieten diese Organisationen nicht nur risikobasierte Unterstützung für Betroffene, sondern ein professionelles und menschliches Element, das kein Chatbot, keine App oder Ressourcenliste jemals in der Lage sein wird zu geben.

Täter*innen

Daten und Informationen über digitale Gewalt und insbesondere, IoT-unterstützten Missbrauch sind rar. Evidenzbasierte Einblicke in das Verhalten und den Umgang von Gewalttäter*innen können daher nicht angeboten werden. Nichtsdestotrotz gibt es eine wachsende Zahl von Literatur, die sich auf Täter*innen fokussiert – einschließlich Veröffentlichungen zu der Verbreitung von nicht einvernehmlich geteilten Bildern und Videos (vgl. Eaton u.a. 2020), digitale Gewalt-bezogene Deliktfaktoren (vgl. Duerksen/Woodin 2019; Muncaster/Ohlsson 2019; Reyns 2019) und Studien zu Straftäter*innen, die beispielsweise in »Cyber-Sextortion«, sprich Erpressungsmechanismen, involviert sind (vgl. O'Malley/Holt 2020). Diese Untersuchungen müssen erweitert werden.

In Großbritannien arbeitet das Drive-Projekt mit Täter*innen von häuslicher Gewalt zusammen, um die Sicherheit von Opfern und Betroffenen zu erhöhen (vgl. Hester u.a. 2019: o.S.). Weniger als ein Prozent der Täter*innen unterziehen sich spezieller Interventionen und Rehabilitierungsprozesse, um ihr Verhalten zu ändern (vgl. Drive Partnership 2020: o.S.). Aufgrund dieser geringen Zahl wird eine wichtige Gelegenheit verpasst, Täter*innen daran zu hindern ihr Opfer weiter zu bedrohen sowie neue potenzielle Opfer zu finden. Da Täter*innen eine Reihe von Werkzeugen zur psychologischen, körperli-

chen, sexuellen, finanziellen und emotionalen Gewalt zur Verfügung stehen, müssen Interventionen sich auch zunehmend damit auseinandersetzen, welchen Einfluss neue Technologien auf Täter*innen haben. Daher haben zum Beispiel mehr als 70 Unterzeichner*innen im Jahr 2020 die britische Regierung dazu aufgefordert in eine explizite Täter*innen-Strategie zu investieren (vgl. Drive Partnership 2020: o.S.). Sofern diese Strategie Umsetzung findet, kann hoffentlich auch ein stärkerer Fokus auf digitale Gewalttäter*innen gelegt werden.

Beratungsstellen und Polizei

Im Zuge des GIoT-Projekts stellte das Forschungsteam einen Mangel an Bewusstsein und Kapazität rund um das Thema digitale Gewalt fest. Beratungsstellen sind sich zwar der Folgenschwere von digitaler Gewalt bewusst, aber ihre Expertise, sich insbesondere den Risiken durch aufkommende Technologien wie dem IoT zu stellen, ist eingeschränkt (vgl. Lopez-Neira u.a. 2019: 25). Staatliche Stellen sowie Beratungsstellen fühlen sich noch nicht einmal in der Lage zufriedenstellend oder umfassend auf ›konventionelle‹ Formen von digitaler Gewalt zu reagieren; wie zum Beispiel die Beratung von Betroffenen von Spyware oder online Belästigungen. Dieser Mangel an Fachwissen ist besorgniserregend, insbesondere da noch stärkeres technisches Potenzial erforderlich sein wird, um IoT-unterstützte Missbrauchsfälle zu bewältigen. Das Wissen und die Kompetenz des Sektors müssen deshalb erhöht werden. Während Beratungsstellen begonnen haben Trainingseinheiten zur sicheren Nutzung von digitaler Technik für Betroffene zur Verfügung zu stellen, braucht der Sektor mehr Unterstützung sowie finanzielle Förderung. Diese Zuwendungen erlauben Organisationen in die notwendigen Ressourcen zu investieren und auf die vorhandenen Schwachstellen in Hinblick auf die Bandbreite digitaler Gewaltmuster zu reagieren (vgl. Powell/Henry 2018; Snook/Chayn/SafeLives 2017; Think Social Tech/Snook/SafeLives 2019).

Es bedarf der Schulung von Beratungspersonal und dem Zugang zu technischem Knowhow. Dies kann beispielsweise über die Einrichtung einer speziellen digitalen Gewalt-Hotline für Betroffene (vgl. Tanczer u.a. 2018b: 6) und dem Sicherheitscoaching von Beratungsstellen erreicht werden (vgl. Tanczer 2018a: o.S.). Darüber hinaus werden zusätzliche Mittel benötigt, um die steigenden Schulungskosten und Qualifizierungsbemühungen auszugleichen. Dies ist vor allem deshalb erforderlich, da diese Trainings kontinuierlich durchgeführt und aktualisiert werden müssen. So erhielt

beispielsweise eine der größten Frauenberatungsstellen in Großbritannien einen dreijährigen Förderzuschuss, um das interne, organisationstechnische Wissen zum Thema digitale Gewalt von Grund auf aufzubauen (vgl. Refuge 2020b: o.S.). Die Institution zählt nun zu einer der führenden Akteur*innen in diesem Gebiet in Großbritannien, hat speziell dafür vorgesehene »Tech Abuse Leads« und ihr Beratungsrepertoire umgekrempelt und gibt auch international wichtige Impulse.

Während es nicht ausreicht, die Verantwortung für den Erhalt solcher Mittel einzelnen Organisationen zu überlassen, müssen nachhaltige Subventionen für die Umsetzung solcher spezialisierten Dienste garantiert werden. Diese Bemühungen betreffen auch die Strafverfolgung und Justiz. Beispielsweise Polizeieinheiten, die sich sowohl auf häusliche Gewalt als auch auf Internetkriminalität fokussieren, sind aufgefordert enger zusammenzuarbeiten. Zusätzlich muss ermöglicht werden, dass auf digitale Gewaltvorfälle rasch und professionell reagiert wird. Polizeisektionen brauchen die notwendigen technischen Fähigkeiten, um die Vielzahl an digitalen Geräten, welche durch den Zuwachs an smarten Systemen weiter steigen werden, effektiv und zeitgerecht zu analysieren. Nur die zügige Evaluation dieser Produkte ermöglicht Klarheit für Betroffene sowie eine prompte Ahndung von Täter*innen.

Letzten Endes muss auch das Risiko von digitaler Gewalt in der Gefährdungsbeurteilung und Sicherheitsplanung von Betroffenen einbezogen werden (vgl. Tanczer u.a. 2018b: 6). Das GIoT-Forschungsteam stellte hierbei fest, dass digitale Gewalt gegenwärtig weder bei Beratungsstellen noch bei der Polizei ausreichend in diesen Gefährdungsbeurteilungen und noch weniger in der Sicherheitsplanung von Opfern berücksichtigt wird. Selbst wenn digitale Gewalt bedacht wird, so beinhalten diese Leitfäden kaum Referenzen zu neuen Technologien. Diese Mängel bergen ein Risiko für Betroffene, welche aufgrund ihrer individuellen Bedürfnisse womöglich nicht die richtige Beratung und Anweisungen erhalten.

Technologie- und designorientierte Intervention

Anstatt *mehr* Technik zu fordern, appelliert das GIoT-Forschungsteam an die Industrie, sich auf die Erarbeitung *besserer* technischer Lösungen zu konzentrieren. Dazu gehört auch die Verbesserung der Sicherheitsfunktionen, die Leichtigkeit, mit der Privatsphäre-Änderungen umgesetzt werden können und die allgemeine Weiterentwicklung der Nutzer*innenfreundlichkeit

von IoT-Geräten (vgl. Parkin u.a. 2019). Unternehmen müssen proaktiv den Missbrauch ihrer Systeme voraussehen und mit Bedacht verhindern. Um die Auswirkungen von digitaler Gewalt in der Partnerschaft besser berücksichtigen zu können, empfiehlt es sich eine Kooperation zwischen der Wirtschaft und dem Beratungssektor anzustreben. Informatiker*innen und Informationssicherheitsspezialist*innen ist es empfohlen, eng mit Sozialarbeiter*innen und anderen Akteur*innen, die Betroffene von häuslicher Gewalt unterstützen, zusammenzuarbeiten. Solch ein Austausch ermöglicht es Risiken und Schwachstellen, die im Kontext der Gewalt in der Partnerschaft gefährlich werden könnten, zu erkennen und dagegen zu intervenieren (vgl. Slupska/Tanczer im Erscheinen). Des Weiteren können die Sicherheits- und Privatsphäre-Bedürfnisse von Betroffenen in der Entwicklung von IoT Systemen priorisiert werden (vgl. Arief u.a. 2014; Matthews u.a. 2017a; Matthews u.a. 2017b).

Es wäre kurzsichtig davon auszugehen, dass eine einzige technische Optimierung und Designänderung dieses ungemein komplexe, sozio-technische Problem ›lösen‹ wird. Selbstverständlich sind Vorschläge wie die gezielte Verwendung von Eingabeaufforderungen, die standardmäßige Lieferung von Produkten mit der höchsten Sicherheits- und Privatsphäre-Einstellung oder die Fähigkeit von Benutzer*innen die Zugangsberechtigungen von verschiedenen IoT-Geräten zu überprüfen, willkommen. Diese technischen Ansätze werden jedoch niemals allen möglichen Missbrauch-Szenarien vorbeugen können. IoT-Entwickler*innen sind daher aufgefordert zu eruieren, welche pro- und reaktiven Maßnahmen eine Firma in Kraft setzen kann. Mögliche Optionen wären hierbei digitale Gewalt-Leitfäden für Mitarbeiter*innen, die im Kundendienst arbeiten und womöglich in Kontakt mit Betroffenen kommen (vgl. Communications Alliance Ltd. 2018). Ebenso sollten Unternehmen sich die Frage stellen, wie sie auf die mögliche gewaltbezogene Verwendung ihrer Systeme reagieren würden.

Legislative und politikzentrierte Interventionen

Zusätzlich zu den menschenbezogenen sozialen und technischen Interventionsoptionen müssen sowohl die Gesetzgebung als auch die Politik die potenziellen Risiken von IoT-unterstützter digitaler Gewalt berücksichtigen. Relevante Akteur*innen sind hierbei nicht nur die nationalen Regierungen, sondern auch Bundesländer, Gemeinden bis hin zu Wohnungsbaugesellschaften. Letztere werden in Zukunft IoT Technologien in geplante Bauten installieren.

All diese Institutionen sollten von dem sogenannten »Zuckerbrot und Peitsche« Zugang Gebrauch machen. Ersteres betrifft beispielsweise Anreize zur Erhöhung der Sicherheit von IoT Geräten durch freiwillige Programme oder Steuervorteile (vgl. Department for Digital, Culture, Media and Sport 2018: o.S.). Letzteres beschreibt strafbare Maßnahmen wie etwa die Durchsetzung verbindlicher Vorschriften und Strafen. Global haben die Regierungen auch damit begonnen, spezielle Einheiten einzurichten, die sich mit dem Thema der digitalen Sicherheit beschäftigen. Die *eSafety*-Kommission in Australien ist ein solches Beispiel. Das Büro leitet und koordiniert die Sicherheitsbemühungen zwischen Commonwealth-Abteilungen, Industrievertreter*innen und Behörden. eSafety hat auch die Befugnis Beschwerden von Einzelpersonen nachzugehen. Ihr Handlungsrahmen beinhaltet u.a. bildbasierte Vergehen wie ›Rache Pornos‹ (vgl. eSafety Commissioner 2020: o.S.). Die Kommission hat ebenfalls begonnen eine separate Frauensektion einzurichten, die sich mit der Sicherheit, Privatsphäre und den Bedürfnissen von Frauen online auseinandersetzt.

Erschwerend für politische Akteur*innen ist, dass es derzeit keine konsistente quantitative Erfassung von digitaler Gewalt gibt (vgl. Tanczer u.a. 2018b: 5). Dieser Mangel macht es schwierig, das volle Ausmaß und den Schweregrad des Problems einzuschätzen sowie evidenzbasierte Interventionen durchzuführen. Daten sind erforderlich, um den Umfang des Problems zu verstehen und potenzielle Veränderungen im Laufe der Zeit zu überwachen. Hierbei könnte es sehr hilfreich sein, wenn Betreuungsstellen, einschließlich Polizeikräften und Beratungsstellen im Kontext häuslicher Gewalt, ihre Berichterstattungsmuster beziehungsweise Dokumentation überdenken. Änderungen von Archivierungssystemen und Dokumentationsbemühungen müssen – um dem komplexen Thema gerecht zu werden – nicht nur die Anzahl, sondern die genauen Arten von Technologien, die im Kontext von digitaler Gewalt zum Einsatz kommen, vermerken. Diese Modifikation würde es nicht nur erlauben eine fundierte Basis digitaler Gewaltdaten zu generieren, sondern den Finger auf jene Firmen und IoT-Entwickler*innen zu richten, welche sich als primäre Plattformen für digitale Gewalt herausstellen. Eine nationale Analyse von digitaler Gewalt in der jährlichen »Crime Survey for England and Wales«, die vom Statistischen Bundesamt (ONS) oder Regulierungsbehörden wie dem Amt für Kommunikation (OFCOM) in Großbritannien durchgeführt werden würde, könnte helfen solche Informationen über die Jahre hinweg zusammenzustellen.

Zuletzt muss auch gewährleistet werden, dass sowohl das Internetrecht als auch das Gewaltschutzgesetz zukunftssicher gemacht werden. Dies ist vor allem in Hinblick auf das erwartete Wachstum an IoT-Geräten gekoppelt (vgl. Tanczer 2019a: o.S.). Eine Gesetzgebung wie zum Beispiel das bevorstehende »Online Harms White Paper« und »Online Safety Bill« in Großbritannien (vgl. HM Government 2019, 2020) muss die Risiken von digitaler Gewalt in der Partnerschaft durch smarte Systeme explizit adressieren. Alle politischen Entscheidungen, die diese aufkommende Bedrohung ignorieren, riskieren Schwachstellen, die in Anbetracht des langwierigen Gesetzgebungsprozesses schwer revidiert werden können. Kritiker*innen, die argumentieren, dass ein solcher Ansatz Innovation bremsen würde, bedenken nicht, dass neue Erfindungen auch in einer reflektierten, achtsamen Umgebung kreiert werden können. Ein Verweis zur Umsetzung der Datenschutz-Grundverordnung (DSGVO) in der Europäischen Union ist hierbei hilfreich. Anstatt der Horrorszenarien, welche Konkurse und ein »Ende der Innovation« vorahnten, hat sich vielmehr gezeigt, dass die Wirtschaft sich nicht nur mit der Situation zurechtgefunden hat, sondern dass sogar Privatsphäre-garantierende Innovationen ermöglicht worden sind (vgl. Martin u.a. 2019). Eine ähnliche Sichtweise könnte für IoT-Produkte herangezogen werden. Zu bedenken gilt, dass Unternehmen seit fast über einem Jahrhundert generellen Gesundheits- und Hygienestandards unterliegen, so kann es doch nicht zu viel verlangt sein, ähnliche Sicherheitsstandards von IoT-Geräten zu erwarten.

Fazit

In diesem Kapitel wurden Informationen zu den Eigenschaften und möglichen Auswirkungen von IoT-Systemen in Zusammenhang mit häuslicher Gewalt diskutiert. Einsichten des britischen GIoT-Forschungsprojekts wurden besprochen und Interventionsmöglichkeiten für unterschiedliche Interessengruppen skizziert. Letztere umfassen eine Mischung aus sozialen, technischen und politischen Lösungsvorschlägen wie etwa die Notwendigkeit statistische Evaluierungen über dieses aufkommende Phänomen zu generieren. Im Allgemeinen drängen wir Akteur*innen, die sowohl in der Forschung als auch in der Praxis aktiv sind, dazu einen erweiterten Blickwinkel auf das Problem der digitalen Gewalt zu werfen. ›Konventionelle‹ Technologien wie Mobiltelefone und Laptops gehören zwar nach wie vor wahrscheinlich zu den prominenteren Geräten, durch die Gewalt in der Partnerschaft ausgeführt

wird. Nichtsdestotrotz kann der Anstieg an smarten Produkten nicht unkritisch gegenübergestanden werden. Ich hoffe daher hier Denkanstöße angeboten zu haben und einen ersten Einblick in die Zukunft von häuslicher Gewalt zu liefern. Interessierte Leser*innen, die sich gerne weiter mit diesem Thema beschäftigen wollen, sind herzlich dazu eingeladen sich für unseren monatlichen GIoT E-Mail-Newsletter auf der *UCL STEaPP* Webseite zu registrieren. Im Zuge dieses Rundbriefes werden neuste wissenschaftliche Veröffentlichungen, Strategien zur Unterstützung von Betroffenen sowie aktuelle politische und technische Geschehnisse geteilt.

Danksagung

Das GIoT Forschungsprojekt erhielt Fördergelder von UCLs Collaborative Social Science Domain, dem NEXTLEAP Projekt (688722), dem PETRAS IoT Forschungshub (EP/N02334X/1) und UCL Public Policy. GIoT läuft in Zusammenarbeit mit dem Londoner VAWG Consortium, Privacy International und dem PETRAS National Centre of Excellence for IoT Systems Cybersecurity. Die Autorin bedankt sich bei ihren GIoT Kollegin*innen Dr. Simon Parkin, Dr. Trupti Patel, Isabel Lopez Neira, Professor George Danezis und Julia Slupska für ihre stetige Unterstützung sowie allen Personen und Institutionen, die in den letzten drei Jahren mit dem GIoT Projekt aktiv zusammengearbeitet haben.

Literatur

Arief, Budi/Coopamootoo, Kovila/Emms, Martin/van Moorsel, Aad (2014): »Sensible Privacy: How We Can Protect Domestic Violence Survivors Without Facilitating Misuse«, in: Proceedings of the 13th Workshop on Privacy in the Electronic Society, WPES '14. New York, NY: ACM, S. 201-204.

Banerjee, Mandrita/Lee, Junghee/Raymond Choo, Kim-Kwang (2018): »A Blockchain Future for Internet of Things Security: A Position Paper«, in: Digital Communications and Networks, Vol. 4 Nr. 3, S. 149-160.

Brass, Irina/Tanczer, Leonie Maria/Carr, M./Elsden, M./Blackstock, J. (2018): »Standardising a Moving Target: The Development and Evolution of IoT Security Standards«, in: Living in the Internet of Things: Cybersecurity of the IoT – 2018. London: IET.

Burdon, Mark/Douglas, Heather (2017): »The Smart Home Could Worsen Domestic Abuse. But the Same Technology May Also Make Us Safer«. The Conversation. https://theconversation.com/the-smart-home-could-worsen-domestic-abuse-but-the-same-technology-may-also-make-us-safer-82897 [Zugriff: 3.7.2020].

Citron, Danielle/Franks, Mary Anne (2014): »Criminalizing Revenge Porn«, in: Wake Forest Law Review, Nr. 49, S. 345-391.

Communications Alliance Ltd. (Hg.) (2018): »G660:2018 Assisting Customers Experiencing Domestic and Family Violence Industry Guideline«. Sydney: Communications Alliance Ltd. https://commsalliance.com.au/__data/assets/pdf_file/0003/61527/Communications-Guideline-G660-Assisting-Customers-Experiencing-Domestic-and-Family-Violence.pdf [Zugriff: 3.7.2020].

DeNardis, Laura (2020): »Internet in Everything. Freedom and Security in a World with No Off Switch«. New Haven/London: Yale University Press.

DeNardis, Laura/Raymond, Mark (2017): »The Internet of Things as a Global Policy Frontier«, in: School of Law, Nr. 51, Davis: University of California, S. 475-497.

Department for Digital, Culture, Media and Sport (Hg.) (2018): »Code of Practice for Consumer IoT Security«. London: Department for Digital, Culture, Media & Sport. https://gov.uk/government/publications/code-of-practice-for-consumer-iot-security [Zugriff: 3.7.2020].

Douglas, Heather/Harris, Bridget/Dragiewicz, Molly (2019): »Technology-Facilitated Domestic and Family Violence: Women's Experiences«, in: The British Journal of Criminology, Vol. 59 Nr. 3, S. 551-570.

Dragiewicz, Molly/Burgess, Jean/Matamoros-Fernández, Ariadna/Salter, Michael/Suzor, Nicolas P./Woodlock, Delanie/Harris, Bridget (2018): »Technology Facilitated Coercive Control: Domestic Violence and the Competing Roles of Digital Media Platforms«, in: Feminist Media Studies, Vol. 18 Nr. 4, S. 609-625.

Drive Partnership (2020): »A Domestic Abuse Perpetrator Strategy for England And Wales. Call to Action«. London: Drive Project (Hg.). https://driveproject.org.uk/wp-content/uploads/2020/01/Call-to-Action-Final.pdf [Zugriff: 3.7.2020].

Duerksen, Kari/Woodin, Erica (2019): »Technological Intimate Partner Violence: Exploring Technology-Related Perpetration Factors and Overlap with in-Person Intimate Partner Violence«, in: Computers in Human Behavior, Nr. 98, S. 223-231.

Eaton, Asia/Noori, Sofia/Bonomi, Amy/Stephens, Dionne/Gillum, Tameka (2020): »Nonconsensual Porn as a Form of Intimate Partner Violence. Using the Power and Control Wheel to Understand Nonconsensual Porn Perpetration in Intimate Relationships«, in: Trauma, Violence, & Abuse, Vol 20. Nr. 10, S. 1-15. https://doi:10.1177/1524838020906533

eSafety Commissioner (2020): »Our Legislative Functions«. Australian Government (Hg.). https://esafety.gov.au/about-us/who-we-are/our-legislative-functions [Zugriff: 30.3.2020].

Gámez-Guadix, Manuel/Borrajo, Erika/Calvete, Esther (2018): »Partner Abuse, Control and Violence Through Internet and Smartphones: Characteristics, Evaluation and Prevention«, in: Papeles Del Psicólogo – Psychologist Papers, Vol. 39 Nr. 3, S. 218-227.

Harkin, Diarmaid/Molnar, Adam/Vowles, Erica (2020): »The Commodification of Mobile Phone Surveillance: An Analysis of the Consumer Spyware Industry«, in: Crime, Media, Culture, Vol. 16 Nr. 1, S. 33-60.

Harris, Bridget (2019): »Anti-Rape Devices May Have Their Uses, but They Don't Address the Ultimate Problem«. The Conversation (Hg.). https://theconversation.com/anti-rape-devices-may-have-their-uses-but-they-dont-address-the-ultimate-problem-123011 [Zugriff: 30.3.2020].

Harris, Bridget/Woodlock, Delanie (2018): »Digital Coercive Control: Insights from Two Landmark Domestic Violence Studies«, in: The British Journal of Criminology, Vol. 59 Nr. 3, S. 530-550.

Havron, Sam/Freed, Diana/Chatterjee, Rahul/McCoy, Damon/Dell, Nicola/Ristenpart, Thomas (2019): »Clinical Computer Security for Victims of Intimate Partner Violence«, in: 28th USENIX Security Symposium. Santa Clara, CA, S. 105-122.

Henry, Nicola/Powell, Anastasia (2018): »Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research«, in: Trauma, Violence, & Abuse, Vol. 19 Nr. 2, S. 195-208.

Hester, Marianne/Eisenstadt, Nathan/Ortega-Avila, Ana/Morgan, Karen/Walker, Sarah-Jane/Bell, Juliet (2019): »Evaluation of the Drive Project – A Three-Year Pilot to Address High-Risk, High-Harm Perpetrators of Domestic Abuse«. Bristol: University of Bristol. https://driveproject.org.uk/wp-content/uploads/2020/01/Drive-Evaluation-Report-Executive-Summary-Final.pdf [Zugriff: 3.7.2020].

HM Government (Hg.) (2019): »Online Harms White Paper«. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf [Zugriff: 3.7.2020].

IHS Markit (Hg.) (2017): »The Internet of Things: A Movement, Not a Market«. Englewood, Colorado: IHS Markit. https://cdn.ihs.com/www/pdf/IoT_ebook.pdf [Zugriff: 3.7.2020].

Leitão, Roxanne (2019): »Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse«, in: ACM Conference on Designing Interactive Systems, S. 527-539. https://doi:10.1145/3322276.3322366

Lopez-Neira, Isabel/Patel, Trupti/Parkin, Simon/Danezis, George/Tanczer, Leonie Maria (2019): »Internet of Things: How Abuse Is Getting Smarter«, in: Safe – The Domestic Abuse Quarterly, Vol. 63, S. 22-26.

Martin, Nicholas/Matt, Christian/Niebel, Crispin/Blind, Knut (2019): »How Data Protection Regulation Affects Startup Innovation«, in: Information Systems Frontiers, Vol. 21 Nr. 6, S. 1307-1324.

Mattern, Friedemann/Floerkemeier, Christian (2010): »From the Internet of Computers to the Internet of Things«, in: Sachs, Kai/Petrov Ilia/Guerrero, Pablo (Hg.), From Active Data Management to Event-Based Systems and More, Lecture Notes in Computer Science, Berlin/Heidelberg: Springer, S. 242-259.

Matthews, Tara/O'Leary, Kathleen/Turner, Anna/Sleeper, Manya/Palzkill Woelfer, Jill/Shelton, Martin/Manthorne, Cori/Churchill, Elizabeth F./Consolvo, Sunny (2017a): »Security and Privacy Experiences and Practices of Survivors of Intimate Partner Abuse«, in: IEEE Security Privacy, Vol. 15 Nr. 5, S. 76-81.

Matthews, Tara/O'Leary, Kathleen/Turner, Anna/Sleeper, Manya/Palzkill Woelfer, Jill/Shelton, Martin/Manthorne, Cori/Churchill, Elizabeth/Consolvo, Sunny (2017b): »Stories from Survivors: Privacy & Security Practices When Coping with Intimate Partner Abuse«, in: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, CHI '17. New York, NY, S. 2189-2201.

McCarthy, Katharine/Mehta, Ruchi/Haberland, Nicole (2018): »Gender, Power, and Violence: A Systematic Review of Measures and Their Association with Male Perpetration of IPV«, in: PLoS One, Vol. 13 Nr. 11, o.S. https://doi:10.1371/journal.pone.0207091

McGlynn, Clare/Rackley, Erika/Houghton, Ruth (2017): »Beyond ›Revenge Porn‹: The Continuum of Image-Based Sexual Abuse«, in: Feminist Legal Studies, Vol. 25 Nr. 1, S. 25-46.

Mirian, Ariana (2019): »Hack for Hire«, in: Communications of the ACM, Vol. 62 Nr. 12, S. 32-37.

Muir, Kate/Joinson, Adam (2020): »An Exploratory Study Into the Negotiation of Cyber-Security Within the Family Home«, in: Frontiers in Psychology, Vol. 11 Nr. 424, S. 1-14.

Muncaster, Laura/Ohlsson, Ioan (2019): »Sexting: Predictive and Protective Factors for Its Perpetration and Victimisation«, in: Journal of Sexual Aggression, S. 1-13. https://doi:10.1080/13552600.2019.1645220

O'Malley, Roberta Liggett/Holt, Karen (2020): Cyber Sextortion: An Exploratory Analysis of Different Perpetrators Engaging in a Similar Crime. Journal of Interpersonal Violence, S. 1-26. https://doi:10.1177/0886260520909186

Parkin, Simon/Patel, Trupti/Lopez-Neira, Isabel/Tanczer, Leonie Maria (2019): »Usability Analysis of Shared Device Ecosystem Security: Informing Support for Survivors of IoT-Facilitated Tech-Abuse«, in: Proceedings of the New Security Paradigms Workshop, NSPW '19. San Carlos, Costa Rica: Association for Computing Machinery, S. 1-15.

Powell, Anastasia/Henry, Nicola (2018): »Policing Technology-Facilitated Sexual Violence against Adult Victims: Police and Service Sector Perspectives«, in: Policing and Society, Vol. 28 Nr. 3, S. 291-307.

Refuge (Hg.) (2020a): »72 % of Refuge Service Users Identify Experiencing Tech Abuse«. https://refuge.org.uk/72-of-refuge-service-users-identify-experiencing-tech-abuse/ [Zugriff: 1.3.2020].

Refuge (Hg.) (2020b): »Tech Abuse and Empowerment Service«. https://refuge.org.uk/our-work/our-services/tech-abuse-empowerment-service/ [Zugriff: 29.3.2020].

Reyns, Bradford W. (2019): »Online Pursuit in the Twilight Zone: Cyberstalking Perpetration by College Students«, in: Victims & Offenders, Vol. 14 Nr. 2, S. 183-198.

Rising Sun (Hg.) (2020): »One Stop Shops«. https://risingsunkent.com/services/one-stop-shops/ [Zugriff: 29.3.2020].

Schneier, Bruce (2017): »The Internet of Things Will Upend Our Industry«, in: IEEE Security Privacy, Vol. 15 Nr. 2, S. 108-11s8.

Slupska, Julia (2019): »Safe at Home: Towards a Feminist Critique of Cybersecurity«, in: St Antony's International Review, Nr. 15, S. 83-100.

Slupska, Julia/Tanczer, Leonie Maria (im Erscheinen): »Intimate Partner Violence (IPV) Threat Modeling: Tech Abuse as Cybersecurity Challenge in the Internet of Things (IoT)«, in: Bailey, J./Flynn, A./Henry, N. (Hg.), Handbook on Technology-Facilitated Violence and Abuse: International Perspectives and Experiences, Bingley: Emerald Publishing.

Snook/Chayn/SafeLives (2017): »Tech vs Abuse: Research Findings 2017«. London: Comic Relief (Hg.). https://safelives.org.uk/sites/default/files/resources/Tech%20vs%20abuse%20report.pdf [Zugriff: 3.7.2020].

Strengers, Yolande/Kennedy, Jenny/Arcari, Paula/Nicholls, Larissa/Gregg, Melissa (2019): »Protection, Productivity and Pleasure in the Smart Home: Emerging Expectations and Gendered Insights from Australian Early Adopters«, in: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, CHI '19, New York, NY: ACM, S. 645:1-645:13.

Sweet, Paige (2019): »The Sociology of Gaslighting«, in: American Sociological Review, Vol. 84 Nr. 5, S. 851-875.

Tanczer, Leonie Maria (2018a): »Tackling Tech Risks for Domestic Violence and Abuse«. https://medium.com/policy-postings/tackling-tech-risks-for-domestic-violence-and-abuse-581a07b41020 [Zugriff: 24.6.2020].

Tanczer, Leonie Maria/Lopez-Neira, Isabel/Parkin, Simon/Patel, Trupti/Danezis, George (2018b): »Gender and IoT (G-IoT) Research Report: The Rise of the Internet of Things and Implications for Technology-Facilitated Abuse«. London: University College London.

Tanczer, Leonie Maria/Lopez-Neira, Isabel/Patel, Trupti/Parkin, Simon/Danezis, George (2018c): »Gender and IoT (G-IoT) Policy Leaflet: Tech Abuse – Smart, Internet-Connected Devices Present New Risks for Victims of Domestic Violence & Abuse«. London: University College London.

Tanczer, Leonie Maria/Patel, Trupti/Parkin, Simon/Danezis, George (2018d): »Gender and IoT (G-IoT) Tech Abuse Guide: How Internet-Connected Devices Can Affect Victims of Gender-Based Domestic and Sexual Violence and Abuse«. London: University College London.

Tanczer, Leonie Maria/Steenmans, I./Elsden, M./Blackstock, J./Carr, M. (2018e): »Emerging Risks in the IoT Ecosystem: Who's Afraid of the Big Bad Smart Fridge?«, in: Living in the Internet of Things: Cybersecurity of the IoT – 2018, London: IET.

Tanczer, Leonie Maria (2019a): »The Government Published Its Draft Domestic Abuse Bill, but Risks Ignoring the Growing Threat of Tech Abuse«. https://medium.com/policy-postings/the-government-published-its-draft-domestic-abuse-bill-but-risks-ignoring-the-growing-threat-of-368a6fb70a14 [Zugriff: 27.2.2020].

Tanczer, Leonie Maria/Brass, Irina/Elsden, Miles/Carr, Madeline/Blackstock, Jason (2019b): »The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape«, in: Ellis, Ryan/Mohan, Vivek (Hg.), Rewired: Cybersecurity Governance, Hoboken, New Jersey: Wiley, S. 37-56.

Tanczer, Leonie Maria/Patel, Trupti/Parkin, Simon/Danezis, George (2019c): »Gender and IoT (G-IoT) Resource List: How Internet-Connected Devices Can Affect Victims of Gender-Based Domestic and Sexual Violence and Abuse«. London: University College London.

Taylor, P./Allpress, S./Carr, Madeline/Lupu Emil/Norton, J./Smith, L./Blackstock, Jason/Boyes Hugh/Hudson-Smith, A./Brass, Irina/Chizari, H./Cooper, R./Coulton, Paul/Craggs, B./Davies, N./De Roure, David/Elsden, Miles/Huth, M./Lindley, Joseph/Maple, Carsten/Mittelstadt, Brent/Nicolescu, Razvan/Nurse, Jason/Procter, Rob/Radanliev, Petar/Rashid, A./Sgandurra, D./Skatova, A./Mariarosaria, Taddeo/Tanczer, Leonie Maria/Vieira-Steiner, R./Watson, Jeremy/Wachter, Sandra/Wakenshaw, Susan Y. L./Carvalho, Graca/Thompson, Rob/Westbury, P. (2018): »Internet of Things: Realising the Potential of a Trusted Smart World«. London: Royal Academy of Engineering (Hg.).

Think Social Tech/Snook/SafeLives (2019): »Tech vs Abuse: Research Findings 2019«, in: Comic Relief, The Clothworkers' Foundation and Esmée Fairbairn Foundation (Hg.). https://d1c4e1f2-14ed-423b-8bab-01c0ad397d8f.filesusr.com/ugd/464d6d_b465be597dee4e04b8fac09363e4ef62.pdf [Zugriff 6.7.2020].

Woodlock, Delanie (2017): »The Abuse of Technology in Domestic Violence and Stalking«, in: Violence Against Women, Vol. 23 Nr. 5, S. 584-602.

Der Feind in der eigenen Tasche
Stalkerware und digitale Überwachung im Kontext von Partnerschaftsgewalt

Chris Köver

Es gibt Branchen, die erfordern eine gewisse moralische Flexibilität, hierzu gehören die Branchen, die Überwachungssoftware vertreiben, die dazu dient, die eigenen Kinder oder Partner*innen auszuspähen. In wenigen Minuten lässt sich so ein Programm auf dem Telefon der Zielperson – auch heimlich – installieren. Besondere technische Fähigkeiten sind dazu nicht notwendig. Die entsprechende App läuft danach unbemerkt im Hintergrund und schneidet dort Telefonate, Chat-Nachrichten, Fotos, Videos und den Standort mit. Die Kund*innen –also diejenigen, die die App installiert haben – bekommen all diese Informationen in einem Browserfenster angezeigt und können sich dort durch das gesamte Telefon der überwachten Person scrollen. Ein tieferer Einblick in die Privatsphäre eines anderen Menschen ist kaum vorstellbar.

Die Firmen vermarkten ihre Apps öffentlich vor allem als Trackingsoftware für besorgte Eltern, die immer wissen wollen, wo ihre Kinder sind und was sie auf dem Smartphone tun (vgl. Parsons u.a. 2019: 67). Diese Verkaufsstrategie ist klug gewählt, denn das Abhören einer anderen Person ohne deren Wissen und Einverständnis ist in Deutschland und vielen anderen Ländern eine Straftat. Ein Produkt zu diesem Zweck dürfte gar nicht auf dem Markt sein. Wie viele Menschen Stalkerware einsetzen und wie viele von der illegalen Spionage betroffen sind, ist nicht erfasst. Aus bisherigen Recherchen (siehe z.B. Locker/Hoppenstedt 2017), Studien (siehe z.B. Chatterjee u.a. 2018) und den regelmäßig auftretenden Datenlecks der Apps, bei denen massenweise sensible Daten ins Internet gelangen, lässt sich jedoch einiges ableiten. Hierdurch ist zum Beispiel erkennbar, dass die meisten Nutzer dieser Apps männlich sind und dass sie die Apps vor allem nutzen, um (Ex-)Beziehungspartner*innen auszuspionieren.

Oft richten Männer die Geräte ein

Viele Beratungsstellen für Partnerschaftsgewalt kennen die Apps inzwischen durch ihre tägliche Arbeit. Frauen, die beispielsweise von einem Partner oder Ex-Partner bedroht und verfolgt werden, berichten dort regelmäßig, dass der Gewalttäter auch Spionagesoftware auf ihren Geräten installiert hat – oder dass sie dies zumindest vermuten. Nur so ist oft zu erklären, wie der Gewalttäter immer über Informationen darüber verfügt, wo sich die (Ex)-Partnerin befindet, mit wem sie spricht, was sie tut, um nur einiges zu nennen. Eine solche Form der Überwachung stellt eine Verletzung der Privatsphäre dar, die in Deutschland auch von der Verfassung geschützt wird. Diese Verletzung kann auch physische Gewalt als Folge haben, so z.B. wenn der Gewalttäter über das Ausspähen des Telefons von Trennungsabsichten der Partnerin erfährt – eine bekannte Hochrisikosituation – oder eine bereits geflohene Frau mit Hilfe der Geräteortung im Frauenhaus aufspürt, um ihr gegenüber gewalttätig zu sein. Expert*innen aus Beratungsstellen berichten, dass solche verdeckt arbeitenden Apps in den vergangenen Jahren zu einer massiven Bedrohung für die Sicherheit ihrer Klient*innen geworden sind. »Bei acht von zehn Fällen haben wir inzwischen eine digitale Komponente dabei« (bff 2019: o.S.), sagt Beate Köhler vom Anti-Stalking Projekt, einer Beratungsstelle in Berlin. Die Frauen kämen häufig bereits aus gewalttätigen Beziehungen, den Partnern gehe es vor allem um Kontrolle. Diese weiten sie über die Geräte aus – bis die Frauen selbst an ihrer geistigen Gesundheit zweifelten.

Teil des Problems ist die Wahrnehmung von Technologie als ›Männersache‹. In cis-/heterosexuellen Partnerschaften sind Männer häufig diejenigen, die Geräte einrichten, Computer installieren, Passwörter verwalten und damit diesen ganzen Bereich in der Regel kontrollieren. Anette von Schröder von der Hamburger Beratungsstelle Patchwork bestätigt diese Erfahrung und kommt zum dem Schluss, dass die Unsicherheit vieler Frauen im Umgang mit Technologie das Problem verschärft. Die Folge dieser einseitigen Arbeitsteilung ist, dass in einer Trennungs- oder Gewaltsituation Frauen dann teils gar nicht wissen, wie sie die Kontrolle über ihre Geräte oder Accounts zurück erlangen können.

Täter*innen fassen: Rechtlich möglich, praktisch schwierig

In Deutschland ist der Einsatz eines solchen Programms ohne die Zustimmung der überwachten Person – im Regelfall – eine Straftat. Das Strafgesetzbuch verbietet das Abhören von Gesprächen und das unerlaubte Fotografieren, auch das Ausspähen von Daten ist untersagt. Auch wenn diese Bestimmungen aus einer Zeit stammen lange bevor jede*r Spionage-Apps für wenige Euro im Internet kaufen konnte, so gelten sie auch für diese Form des unerlaubten Abhörens. Theoretisch ist die Rechtslage für Betroffene in Deutschland also gut. Zu Anklagen kommt es jedoch trotzdem so gut wie nie. Einzelne Fälle stellen eine Ausnahme dar, so wie die Verurteilung eines jungen Mannes in Stuttgart, der Spyware auf dem Handy seiner Ex-Partnerin installiert hatte und sich deshalb wegen »Abfangens von Daten« vor Gericht verantworten musste (vgl. o.A. 2015: o.S.). Dass es so wenig Verurteilungen gibt, ist erstaunlich, da aus Datenlecks der einschlägigen Firmen bekannt ist, dass solche Apps in Deutschland – konservativ gerechnet – tausendfach genutzt werden (Locker/Hoppenstedt 2017: o.S.). Warum ist es also so schwer Täter*innen juristisch zur Verantwortung zu ziehen, die andere mit solchen Methoden überwachen und terrorisieren? Praktisch scheitern Konsequenzen häufig schon daran, dass die meisten Betroffenen nie erfahren, dass sie überwacht werden. Selbst wenn ein konkreter Verdacht besteht, etwa weil eine Person merkt, dass ihr*e Partner*in Dinge weiß, die er nur durch eine heimliche Überwachung erfahren haben kann, ist es für Betroffene kaum möglich Stalkerware auf ihrem Telefon nachzuweisen: Den Fachberatungsstellen fehlt häufig das Personal und das technologische Wissen, um forensische Analysen der Geräte durchzuführen.

Die Polizei hätte zwar die technischen Möglichkeiten (vgl. Meister 2018: o.S.). Sie untersucht aber in der Regel keine Geräte zur Beweissicherung in Fällen von Partnerschaftsgewalt. An vielen Stellen fehlt den Beamt*innen auch schlicht das Verständnis, so berichten Betroffene, die versuchten Anzeige zu stellen. Und selbst wenn der Beweis erbracht werden kann, dass Stalkerware auf dem Telefon installiert ist, muss noch eine Verbindung zu der Person nachgewiesen werden, die die Daten abfängt. Ohne eine Rechnung, die den Kauf der App bestätigt, eine*n Zeug*in oder ein Geständnis haben Betroffene kaum etwas in der Hand, um ein Gericht zu überzeugen. Stalkerware-Fälle gelten den Staatsanwaltschaften somit als schwierig und sind entsprechend unbeliebt (vgl. ebd.).

Was das kanadische Citizen Lab[1] 2019 für Kanada forderte, gilt auch für Deutschland: Beamt*innen, Staatsanwaltschaften und Gerichte müssen besser geschult werden und brauchen mehr Personal, um solchen Fällen nachgehen zu können. Sonst können Täter*innen weiterhin in Ruhe illegal überwachen, ohne Konsequenzen fürchten zu müssen (vgl. Köver 2019a: o.S.).

Verantwortung von Hersteller*innen

Die meisten Stalkerware-Firmen verkaufen ihre Produkte vordergründig als Software zur Überwachung der eigenen Kinder – ein Szenario, das tatsächlich legal, wenn auch nicht legitim ist. In ihren Nutzungsbedingungen weisen sie darauf hin, dass die App nur mit ausdrücklicher Zustimmung der zu überwachenden Person installiert werden darf. Das macht es schwer, rechtlich gegen solche so genannten »Dual-Use«[2]-Produkte vorzugehen. Die Firmen berufen sich darauf, dass sie nichts Illegales täten. Für Straftaten, die mit ihren Apps begangen werden, seien allein die Täter*innen verantwortlich.

Auch die deutschen Datenschutzbehörden kommen an die Firmen kaum ran. Zwar gilt in Deutschland seit 2018 die Datenschutzgrundverordnung (DSGVO). Wer dagegen verstößt, begeht eine Ordnungswidrigkeit und kann mit Strafen von bis zu 20 Millionen Euro oder 4 % des Jahresumsatzes belegt werden. Dies gilt selbst dann, wenn die Firmen außerhalb der EU sitzen.[3] Allerdings kennt die DSGVO keine Herstellerhaftung für Datenschutzverstöße. »Verantwortlicher im datenschutzrechtlichen Sinne ist grundsätzlich die Person, die die Software einsetzt« schreibt Johannes Pepping von der Landesdatenschutzbehörde Niedersachsen (vgl. Köver 2019b: o.S.). Und die Person begeht weit mehr als eine Ordnungswidrigkeit, denn das illegale Ausspähen ist eine Straftat. Selbst wenn den Firmen nachgewiesen werden kann, dass sie selbst Daten erheben, etwa weil sie diese auf ihren Servern speichern, stehen die Chancen, eine Firma mit Sitz außerhalb der EU tatsächlich zu

1 Das Citizen Lab in Kanada ist ein interdisziplinärer Forschungs-Zusammenschluss, der sich mit Fragen an den Schnittstellen von Kommunikationstechnologie, Menschenrechten und globaler Sicherheit befasst, siehe dazu https://citizenlab.ca/about/.

2 Der Begriff Dual-Use steht sinngemäß für den doppelten Verwendungszweck eines Produktes und wird vorrangig benutzt, um Waren zu beschreiben, die für zivile Zwecke verwendet werden, sich aber auch für militärische Zwecke eignen und hierfür missbraucht werden.

3 Siehe hierzu Art. 3 DSGVO »Räumlicher Anwendungsbereich«.

fassen zu bekommen, sehr schlecht. Realistisch – so Pepping – sei das nur in Ländern, in denen es überhaupt Datenschutzbehörden gebe, wie etwa Kanada. Sonst bräuchte es Rechtshilfeabkommen mit dem jeweiligen Land (vgl. ebd.).

Viel effektiver könnte hier die Bundesnetzagentur eingreifen: Sie kann, anders als die Datenschützer, Produkte tatsächlich verbieten. In der Vergangenheit ist das etwa bei der vernetzen Puppe Cayla[4] passiert, die von der Agentur als verbotene »Abhöranlage« eingestuft wurde (vgl. Kühl 2017: o.S.). Die Bundesnetzagentur hat allerdings keine Rechtsgrundlage um gegen Apps vorzugehen. Ihre Verbote basieren auf dem § 90 Missbrauch von Sende- oder sonstigen Telekommunikationsanlagen des Telekommunikationsgesetzes (TKG), der den Missbrauch von »Sende- oder sonstigen Telekommunikationsanlagen« regelt. Der Paragraf richtet sich damit ausschließlich gegen Hardware. Stalkerware-Apps auf einem Telefon fallen nicht darunter – obwohl sie der Funktion nach das gleiche und noch viel mehr erlauben. Zu überlegen wäre, ob im Kampf gegen Stalkerware nicht eine Erweiterung des Mandats dieser Behörde hilfreich sein könnte, oder ob analog zu der Behörde nicht eine Institution den Auftrag haben sollte Apps verbieten zu dürfen, sofern diese zumindest mehrheitlich missbräuchlich genutzt werden.

Auf der Suche nach Lösungen

Das Citizen Lab, ein Forschungsinstitut an der University of Toronto, hat die Branche in zwei ausführlichen Berichten untersucht (siehe Parsons u.a. 2019; Khoo u.a. 2019). Auf mehr als 300 Seiten analysierte ein Team aus Jurist*innen, Politikwissenschaftler*innen und Tech-Expert*innen, wie diese Programme funktionieren, wie sie vermarktet werden und vor allem: wie ihnen mit einem Netz aus Maßnahmen beigekommen werden kann. Die Autor*innen des Berichts betonen: Selbst wenn Herstellende ihre Software als

4 Cayla ist eine Spielzeugpuppe aus den USA, die mit Netzwerkzugang, Mikrofon und Spracherkennungs-Software ausgestattet ist. Da der Zugriff auf das Mikrofon über eine ungesicherte Bluetooth-Verbindung erfolgt, wurde sie 2017 in Deutschland nach § 90 Telekommunikationsgesetz als »verbotene Sendeanlage« eingestuft. In Österreich wurde die Puppe dagegen nicht verboten, da es keine entsprechende gesetzliche Grundlage gab. Siehe hierzu: https://futurezone.at/digital-life/spionage-im-kinderzimmer-puppe-cayla-wird-verboten/247.055.266 [Zugriff: 29.6.2020].

legale Dual-Use-Produkte anbieten, könnten diese zur Verantwortung gezogen werden. So könnten die Firmen zum Beispiel vom Gesetzgeber gezwungen werden den »Tarn-Modus« zu entfernen, also die Möglichkeit, eine App unsichtbar im Hintergrund auf einem Telefon laufen zu lassen, ohne dass die überwachte Person dies mitbekommt. Schließlich gibt es keinen legalen Anwendungsfall, für den so eine Funktion nötig wäre. Wenn eine Person der Überwachung zugestimmt hat, muss die Software nicht vor ihr versteckt werden. Wenn es um das eigene Kind geht, kann auch dieses über die App informiert werden. Zusätzlich könnten die Programme regelmäßig auf ihre Aktivität hinweisen, etwa mit Push-Mitteilungen auf dem Telefon oder einem »Zustimmungsdialog«, in dem die überwachte Person regelmäßig explizit ihr Einverständnis erteilt. Beides würde eine heimliche Überwachung verhindern.

Hersteller*innen müssten außerdem dafür sorgen, dass Betroffene auf ihren Seiten Anleitungen finden, wie sie das entsprechende Programm auf ihrem Telefon erkennen und deinstallieren können. Derzeit finden sich auf keiner der Firmen-Websites solche Hinweise. Sie richten sich ausschließlich an die potentiellen Kund*innen, also Überwacher*innen oder jene, die es werden wollen. Firmen sollen Betroffene zudem benachrichtigen müssen, wenn deren Daten im Zuge eines Sicherheitslecks öffentlich werden. Diese Lecks treten regelmäßig auf (vgl. Franceschi-Bicchierai 2019: o.S.). Nach der europäischen Datenschutzgrundverordnung und auch der kanadischen Entsprechung sind Firmen dazu verpflichtet, Nutzer*innen auf solche Verstöße gegen den Datenschutz hinzuweisen. Die Firmen beschränken sich allerdings bisher darauf, ihre Kund*innen und damit die Täter*innen zu informieren.

Technologische Lösungen haben allerdings ihre Grenzen. In vielen Fällen von häuslicher Gewalt übt der Partner ganz offen Kontrolle aus und zwingt entweder die Partnerin dazu, sich überwachen zu lassen oder erklärt dies zu einem ›Liebesbeweis‹ aus ›Sorge‹, dem die Partnerin zustimmt. In solchen Fällen hilft auch keine Push-Mitteilung. Solche verpflichtenden Designauflagen könnten laut dem Citizen Lab deswegen nur ein Faden in einem »Netz von Einschränkungen« sein, die um die Branche gelegt werden, um Betroffene vor Stalkerware zu schützen.

»Träumst du davon, das Telefon deiner Gattin auszuspionieren?«

Die Forscher*innen des Citizen Lab haben auch das Marketing der Produkte untersucht, also die Frage, wie Stalkerware-Firmen potentielle Kund*innen per Suchmaschinenoptimierung und bezahlten Anzeigen auf ihre Webseiten lotsen. Die Firma »mSpy« zum Beispiel geht dabei besonders dreist vor. Sie hat im HTML-Code ihrer Seite mehrere Textblöcke versteckt, die nicht auf der Website angezeigt werden. Dennoch werden sie von Suchmaschinen wahrgenommen und bei der Suche nach Stalkerware in den Suchergebnissen beachtet. Für Betrachter*innen werden sie nur sichtbar, wenn sie sich den Quelltext der Seite anschauen würden. Dort steht zum Beispiel: »Obwohl dieser Tracker für Eltern entwickelt wurde, die ihren rebellischen Teenager kontrollieren wollen, kann er auch von Partnern genutzt werden, um ihre bessere Hälfte auszuspionieren […].« (Parsons u.a. 2019: 67, Übersetzung C.K.) Auf einer anderen Blogseite versteckt sich der Text: »Träumst du davon, heimlich das Telefon deines Gatten/deiner Gattin auszuspionieren, um zu erfahren, ob er/sie dich betrügt?« (ebd.)

Um die Firmen zu entlarven, war es in vielen Fällen jedoch gar nicht nötig nach versteckten Texten und Schlagworten zu suchen. Sechs der neun im Bericht untersuchten Firmen bewarben ihre Produkte ganz offen als Hilfsmittel für Partnerschaftsgewalt. In diesen Fällen kann kaum von Dual-Use gesprochen werden, schreiben die Autor*innen plakativ (vgl. ebd.: 76), so müssten die Szenarien umgedreht werden: Diese Software sei in erster Linie ein Werkzeug für Stalking und Partnerschaftsgewalt – und könne nur zweitrangig für legale Zwecke genutzt werden.

Erkenntnisse des Citizen Lab für Deutschland

Das Citizen Lab sitzt in Kanada und schaut vor allem auf die dortige Rechtslage. Die Erkenntnisse sind jedoch auch aus deutscher Perspektive interessant. Erstens, weil einige der untersuchten Programme wie »FlexiSpy« und »mSpy« auch in Deutschland rege vermarktet und genutzt werden (vgl. Locker/Hoppenstedt 2017: o.S.). Dies ist bekannt aufgrund der zahlreichen Datenlecks der vergangenen Jahre, bei denen auch Nutzer*innendaten öffentlich wurden (vgl. ebd.). Und zweitens, weil viele der Beobachtungen sich fast eins zu eins auf Deutschland übertragen lassen. So kommen die Jurist*innen des Citizen Lab ebenfalls zu dem Schluss, dass Kanada theoretisch über eine ausreichen-

de Gesetzesgrundlage verfügt, um der Gewalt und dem Missbrauch durch Stalkerware zu begegnen. In der Realität führe dies aber nicht dazu, dass Betroffenen tatsächlich geholfen wird. Die Autor*innen führen dies zurück auf einen »Mangel an sozio-kulturellem und/oder technologischem Bewusstsein« (Khoo/Robertson/Deibert 2019: 150) für technologie-gestützte, geschlechtsspezifische Gewalt. Dies gelte entlang der gesamten Kette, angefangen bei den Polizeibeamt*innen, die Fälle aufnehmen, bis hin zu den Anwält*innen, Gerichten und den Gesetzgeber*innen, die die Fälle verhandeln.

Vergleichbares berichten Expert*innen für geschlechtsspezifische Gewalt in Deutschland, etwa der Bundesverband der Frauenberatungsstellen und Frauennotrufe (bff)[5] oder die Anti-Stalkingberatung des Frieda Frauenzentrums in Berlin[6].

Für Kanada wie für Deutschland gilt daher: Polizei und Staatsanwaltschaft müssen anfangen, den Einsatz von Stalkerware konsequent strafrechtlich zu verfolgen.

Die Rolle von PayPal

Ein weiterer Akteur im Geflecht von Stalkerware ist PayPal. Die Branche gedeiht auch deswegen so prächtig, weil sie von der einfachen Zahlung mit wenigen Klicks profitiert (vgl. Köver 2019a: o.S.). Wer Stalkerware verkauft, verstößt damit eigentlich gegen die Nutzungsbedingungen der Plattform. Immer wieder sperrt PayPal daher die Konten von Stalkerware-Firmen, zuletzt etwa von »Hellospy«. Die Firma bewirbt ihr Produkt offen als Lösung, um vermeintlich untreue Partner*innen auszuspionieren. Illustriert wird das auf der Website mit dem Foto eines Mannes, der eine Frau am Handgelenk packt – ihr Gesicht voller Blutergüsse. Eine Sperrung des PayPal-Kontos passierte allerdings erst in Folge von journalistischen Recherchen und Berichterstattung. In diesem Fall hatte die Tech-Nachrichtenseite »Motherboard« über den Fall berichtet (vgl. Cox,/Franceschi-Bicchierai 2019: o.S.). Und ebenso schnell wie die Firmen gesperrt werden, sind sie meist wieder da. Sie melden sich dafür

5 bff im Podcast siehe: https://netzpolitik.org/2019/npp-168-wenn-maenner-stalken-drohen-und-abhoeren/ [Zugriff: 29.6.2020].

6 Frieda Frauenzentrum Berlin zu Cyber-Stalking siehe: https://netzpolitik.org/2019/cyber-stalking-beraterinnen-fordern-staatliche-meldestelle/[Zugriff: 29.06.2020].

einfach unter einem neuen Firmennamen an. So wird das Melden von Anbietern zu einem Katz-und-Maus-Spiel, das sich endlos weiterspielen lässt.

Warum so ein offensichtlicher Täuschungsversuch eines bereits gesperrten Händlers nicht erkannt wird, will PayPal sich nicht äußern. Dabei kann es für Zahlungsdienstleister nicht so schwer sein zu erkennen, dass es sich um dasselbe Produkt handelt, dessen Verkauf auf der Plattform schon einmal verboten wurde. Offen bleibt auch, warum PayPal HelloSpy rauswirft, aber zahlreiche andere Spionage-Apps des gleichen Herstellers nach wie vor über die Plattform bezahlt werden können. Derzeit wickeln etwa ein Dutzend weitere Stalkerware-Firmen ihre Zahlungen über PayPal ab (vgl. Heasley 2019: o.S.).

Antivirenprogramme als Werkzeuge zur digitalen Selbstverteidigung

Bei digitaler Gewalt spielen auch Antivirenprogramme eine wichtige Rolle. Die großen Hersteller*innen wie z.B. »Kaspersky«, »Norton«, »ESET« und »Avira« haben Stalkerware als Bedrohung lange Zeit nicht ernst genommen – wohl, weil diese Programme in der engeren Definition tatsächlich keine Viren sind. Dabei könnten diese Firmen entscheidend dazu beitragen, Stalkerware auf Geräten auszuspüren. Eine Studie der Cornell University aus dem Jahr 2018 hatte untersucht, wie zuverlässig die Programme Stalkerware auf Telefonen finden. Das ernüchternde Ergebnis: Unter den großen Anbietern war keiner, der Spionage-geeignete Apps zuverlässig erkannt hätte. »Vermutlich reflektiert [dieses Ergebnis] die Designziele«, resümieren die Autor*innen, »die das Aufspüren von Spyware für intime Partnerschaftsgewalt nicht unbedingt mit einschließen, geschweige denn von Dual-Use-Apps« (Chatterjee 2018: 12, Übersetzung C.K.).

Diese Haltung ändert sich derzeit durch eine Initiative der Sicherheitsforscherin Eva Galperin. Galperin arbeitet bei der digitalen Bürgerrechtsorganisation Electronic Frontier Foundation und beschäftigt sich dort auch mit Partnerschaftsgewalt und deren digitalen Werkzeugen. Sie hat es mit hartnäckiger Lobbyarbeit geschafft, eine internationale Kampagne loszutreten. Teil dieser Bewegung ist auch die Softwarefirma Kaspersky Lab. Sie warnt ihre Nutzer*innen mit einer besonderen Nachricht, wenn Spionage-Software auf ihrem Telefon entdeckt wurde: »Diese App könnte dazu genutzt werden, um ihre persönlichen Daten zu kompromittieren, etwa ihre Anrufe mit-

zuhören, ihre E-Mails und Textnachrichten zu lesen, ihren Standort festzustellen oder ihre Kommunikation auf sozialen Netzwerken mitzuschneiden.« (Köver 2019c: o.S.) Galperin kritisiert, dass Programme, die direkten Zugriff auf das Telefon erfordern, von vielen Expert*innen bislang nicht als echtes Hacking anerkannt wurden. Dass eine Bedrohung für die Sicherheit von Frauen häufig nicht von fremden Hacker*innen oder gar Regierungsbehörden ausgeht, sondern von Menschen aus ihrer eigenen Familie, das lag für viele Sicherheitsforscher*innen außerhalb ihrer Horizonts (vgl. Köver 2019c: o.S.). Dies ändert sich derzeit. Nach dem Vorstoß von Kaspersky sind inzwischen auch Avira und Norton Teil der von Galperin initiierten Coalition Against Stalkerware[7].

Es bleibt zu hoffen, dass die gemeinsame Arbeit der Koalition tatsächliche Verbesserungen für Betroffene von geschlechtsspezifischer Gewalt mit sich bringt und auch andere Vertreiber*innen von IT-Sicherheitsprodukten sowie Legislative und Judikative hier ihre Verantwortung erkennen und zukünftig dem Schutz vor geschlechtsspezifischer Gewalt einen höheren Stellenwert einräumen.

Literatur

bff: Bundesverband Frauenberatungsstellen und Frauennotrufe (2019): »Workshop zur Erstellung eines Leitfadens zum Umgang mit Spionage-Apps auf Smartphones und Tablets im Zusammenhang mit Stalking und häuslicher Gewalt«. 25.3.2019, Berlin.

Chatterjee, Rahul/Doerfler, Periwinkle/Orgad, Hadas/Havron, Sam/Palmer, Jackeline/Freed, Diana/Levy, Karen/Dell, Nicola/McCoy, Damon/Ristenpart, Thomas (2018): »The Spyware Used in Intimate Partner Violence«. 2018 IEEE Symposium on Security and Privacy (SP) (Hg.). San Francisco, CA, 2018, S. 441-458. https://doi:10.1109/SP.2018.00061 [Zugriff: 29.6.2020].

7 Neben IT-Firmen beteiligen sich mehrere Organisationen an der Koalition, die zu geschlechtsspezifischer Gewalt arbeitet und Betroffene unterstützt. Der bff: Bundesverband Frauenberatungsstellen und Frauennotrufe ist im Mai 2020 der Koalition beigetreten siehe: https://frauen-gegen-gewalt.de/de/aktuelles/nachrichten/nachricht/bff-unterstuetzt-koalition-gegen-spionagesoftware-coalition-against-stalkerware-40-cas-41.html [Zugriff: 29.6.2020].

Cox, Joseph/Franceschi-Bicchierai, Lorenzo (2019): »PayPal Processes Payments for ›Stalkerware‹ Software Sold to Abusive Partners«. https://vice.com/en_us/article/7xnwa9/paypal-payments-stalkerware-software-abusive-partners [Zugriff: 29.6.2020].

Franceschi-Bicchierai, Lorenzo (2019): »This Spyware Data Leak Is So Bad We Can't Even Tell You About It«. https://vice.com/en_us/article/j573k3/spyware-data-leak-pictures-audio-recordings [Zugriff: 30.6.2020].

Heasley, Cian (2019): »PayPal is Handling Stalkerware Blood Money«. https://medium.com/@nscrutables/paypal-is-handling-stalkerware-blood-money-dc75acfad12c [Zugriff: 29.6.2020].

Khoo, Cynthia/Robertson, Kate/Deibert, Ronald (2019): »Installing Fear. A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications«. Citizen Lab Research (Hg.). Report No. 120, Toronto. https://citizenlab.ca/docs/stalkerware-legal.pdf [Zugriff: 29.6.2020].

Köver, Chris (2019a): »Spionage-Apps sind in erster Linie ein Werkzeug für Partnergewalt«. https://netzpolitik.org/2019/spionage-apps-sind-in-erster-linie-ein-werkzeug-fuer-partnergewalt/ [Zugriff: 29.6.2020].

Köver, Chris (2019b): »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: 29.6.2020].

Köver, Chris (2019c): »Werden Virenschutz-Programme zu Verbündeten im Kampf gegen Stalkerware?«. https://netzpolitik.org/2019/werden-virenschutz-programme-zu-verbuendeten-im-kampf-gegen-stalkerware/ [Zugriff: 29.6.2020].

Kühl, Eike (2017): »Vernichten Sie diese Puppe«. https://zeit.de/digital/datenschutz/2017-02/my-friend-cayla-puppe-spion-bundesnetzagentur [Zugriff: 29.6.2020].

Locker, Theresa/Hoppenstedt, Max (2017): »Mehr als tausend Deutsche nutzen Spionage-App: 100 Prozent Erfolg – übermorgen ist meine Scheidung«. https://vice.com/de/article/ezjdbj/mehr-als-tausend-deutsche-nutzen-spionage-app-100-prozent-erfolg-uebermorgen-ist-meine-scheidung [Zugriff: 3.5.2020].

Meister, Andre (2018): »Mit diesen sieben Programmen liest die Polizei Smartphone-Daten aus«. https://netzpolitik.org/2018/digitale-forensik-mit-diesen-sieben-programmen-liest-die-polizei-smartphone-daten-aus/ [Zugriff: 29.6.2020].

o.A. (2015): »Handy-Spionage: Misstrauen unter Partnern kann strafbar sein«. https://sueddeutsche.de/wissen/technik-handy-spionage-misstrauen-unter-partnern-kann-strafbar-sein-dpa.urn-newsml-dpa-com-20090101-151209-99-189070 [Zugriff: 29.6.2020].

Parsons, Christopher/Molnar, Adam/Dalek, Jakub/Knockel, Jeffrey/Kenyon, Miles/Haselton, Bennett/Khoo, Cynthia/Deibert, Ronald (2019): »The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry«. Citizen Lab Research (Hg.). Report No. 119, Toronto. https://citizenlab.ca/docs/stalkerware-holistic.pdf [Zugriff: 29.6.2020].

Individuelle Strategien im Umgang mit geschlechtsspezifischer digitaler Gewalt

Jenny-Kerstin Bauer und Ans Hartmann

Der Umgang mit technik- oder medienbasierten Gewalterfahrungen ist individuell sehr unterschiedlich. Nicht für alle Betroffenen kommen polizeiliche und rechtliche Maßnahmen in Betracht. Zudem mangelt es staatlichen Schutzmaßnahmen derzeit noch häufig an Effektivität. So sind Betroffene regelmäßig darauf angewiesen, für sie funktionierende und hilfreiche Wege der Bewältigung zu finden. Einige dieser Bewältigungsstrategien und Handlungsoptionen werden im Rahmen dieses Artikels dargestellt. Fiedler (2006) beschreibt aktives Handeln von (Stalking-)Betroffenen – neben der Suche nach sozialer Unterstützung und professioneller Beratung – als einen von drei proaktiven Faktoren, der das Ausmaß psychischer Belastungen nach Gewalterfahrungen mindern kann. Aus der feministischen Beratungsarbeit ist bekannt, dass solch proaktives Handeln nach Gewalterfahrungen keineswegs allein in der individuellen Verantwortung der Betroffenen liegt oder ausschließlich von deren Willen abhängig ist. Ob bestimmte Strategien überhaupt eine hilfreiche Option sein können, ist immer auch abhängig vom Kontext der Gewalterfahrung und der konkreten Art und Intensität der digitalen Angriffe[1]. Demnach können die hier vorgestellten Ansätze nur exemplarische Beispiele sein. Ihre Darstellung basiert vorrangig auf Erfahrungen aus der feministischen Beratungsarbeit zu geschlechtsspezifischer Gewalt und online-aktivistischen Zusammenhängen. Welche Strategien übertragbar sind, bleibt immer vom Einzelfall abhängig und kann idealerweise in einem unterstützendem (Beratungs-)Setting herausgefunden werden.

1 Siehe Beitrag: Formen geschlechtsspezifischer digitaler Gewalt.

Der Kontext der Gewalterfahrung

Digitale geschlechtsspezifische Gewalt ist komplex und »stellt meist eine Ergänzung oder Verstärkung von Gewaltverhältnissen und -dynamiken dar« (bff 2020: o.S.). Der gesellschaftliche und individuelle Kontext von Gewalterfahrungen ist relevant für deren Verarbeitung. Digitale Angriffe ereignen sich nicht im luftleeren Raum. Ob bestimmte Gegenmaßnahmen für Betroffene hilfreich oder überhaupt umsetzbar sind, entscheidet sich beispielsweise daran, ob noch eine Partnerschaft mit der gewaltausübenden Person besteht, die nicht beendet werden soll oder ob ein gewisses Maß an Kommunikation aufrechterhalten werden muss, da es gemeinsame Kinder und ein geteiltes Sorgerecht gibt. Entscheidend ist außerdem, ob der Bewältigung überhaupt Priorität eingeräumt werden kann oder (zunächst) andere Aspekte wie die Sicherstellung des Einkommens, die Versorgung von Angehörigen und andere Care Arbeit oder der Umgang mit anderen Verletzungen und Diskriminierungserfahrungen drängender sind. In manchen Situationen haben schlicht der physische Schutz und die körperliche Sicherheit der Betroffenen und damit beispielsweise die Suche nach einem Frauenhausplatz Vorrang. Wenn digitale Gewalt ein Teil andauernder Gewaltdynamiken ist, müssen auch darin begründete Abhängigkeitsverhältnisse berücksichtigt werden. Gehören massive Kontrolle und Überwachung zur Täterstrategie, können Maßnahmen zur Unterbindung der Überwachung und Loslösung eine Zuspitzung der Gewalt bewirken, die mitunter lebensbedrohlich sein kann. Diese Gefahr ist Betroffenen häufig auch bewusst, sodass einfache Techniktipps oder die Fähigkeit Spyware zu identifizieren als Umgangsstrategie allein nicht ausreichen und vielmehr zu einer zusätzlichen Gefährdung führen können.

Es ist zu vermuten, dass ein wesentlicher Anteil derjenigen, die digitale Gewalt erleben, bereits zuvor Erfahrungen mit geschlechtsspezifischer Gewalt gemacht haben. Angeeignetes Erfahrungswissen, bereits etablierte Umgangsstrategien und andere Auswirkungen, die Gewalterfahrungen auf die Lebenssituation Betroffener haben, können bei der Bewältigung digitaler Gewalt von wesentlicher Bedeutung sein. Zurückliegende negative Erfahrungen mit Behörden, Gerichten und der Polizei oder die Befürchtung von Repressionen können dazu führen, dass Strategien, die einen erneuten Kontakt mit diesen Stellen nötig machen könnten, von vornherein keine Option darstellen. Auch die zugrundeliegende Technologie und die involvierten Medien bestimmen, welcher Handlungsspielraum für technische Gegenmaßnahmen und den Schutz der digitalen Privatsphäre genutzt werden kann. Die psychischen

Auswirkungen von digitaler Gewalt können enorm sein, dazu trägt auch die Viktimisierung unter extremer Öffentlichkeit bei, beispielsweise beim Teilen intimer Bilder im Internet (vgl. Katzer 2014: 16ff.). Nicht immer wissen Betroffene, dass sie heimlich gefilmt wurden oder intime Bilder von ihnen kursieren. Je später sie davon erfahren, umso weiter ist die Verbreitung der Bilder vermutlich vorangeschritten. Fehlende nachhaltige Löschoptionen beschränken die Möglichkeiten, die Verbreitung einzudämmen und können zu einer Endlosviktimisierung beitragen (vgl. ebd.). Bei der Erarbeitung von Bewältigungskonzepten, die diese Faktoren berücksichtigen, sollte jeder betroffenen Person die Möglichkeit auf Beratung und Unterstützung zugestanden und der barrierefreie Zugang dazu ermöglicht werden.

Strukturelle Benachteiligung und Diskriminierung limitieren Handlungsoptionen und den Zugang zu Unterstützung

Inwiefern Bewältigungsstrategien entlastend wirken, wird vor allem auch durch die Lebenssituation der betroffenen Person bestimmt. Auf welche Handlungsoptionen und Unterstützungsmöglichkeiten zurückgegriffen werden kann, ist u.a. maßgeblich davon abhängig, ob der betroffenen Person zeitliche, finanzielle und soziale Ressourcen zur Verfügung stehen, ob ein unterstützendes Umfeld oder der Zugang zu professionalisierter Beratung vorhanden sind (vgl. Dobash/Dobash 1992: 225ff., Piispa 2002). Strukturelle Benachteiligungen und andere Diskriminierungserfahrungen zwingen Betroffene ihr Leben lang dazu, sich Umgangs- und Überlebensstrategien anzueignen. Die daran gebundenen Kapazitäten können Handlungsoptionen nach digitaler Gewalt limitieren. Menschen, die von intersektionaler Diskriminierung betroffen sind und strukturelle Gewalt erfahren, sind besonders vulnerabel in Bezug auf digitale Gewalt, fallen aber auch besonders häufig durch das Raster von Unterstützungsstrukturen. Dennoch stehen sie selten im Fokus, wenn es um politische Maßnahmen zum Schutz vor geschlechtsspezifischer Gewalt geht (vgl. Hartmann 2017: 6). So kann besonders das Benennen und öffentliche Sichtbarmachen erlebter digitaler Gewalt, beispielsweise auf von Dritten einsehbaren Social Media Kanälen, eine weitere Gefährdung bedeuten und zusätzliche Gewalt etwa in Form von Hate Speech und Belästigung mit sich bringen. Ob das öffentliche Teilen oder Berichten über digitale Gewalterfahrungen als eine hilfreiche Strategie in Betracht kommt, hängt demnach auch davon ab, ob Betroffene mit positiver

Resonanz und solidarischen Reaktionen rechnen können. Für Betroffene, die gerade im Zentrum eines Hatestorms stehen oder keine unterstützende online-Community mit entsprechender Vernetzung im Rücken haben, mag eine solche Strategie nicht vielversprechend wirken.

Auch wenn sich jede*r mit Internetzugang im Netz äußern und Content produzieren kann, werden nicht alle Stimmen gleich wahrgenommen. Auf Geschichten von gewaltbetroffenen Frauen, die im Internet viel Reichweite erlangen, folgen mittlerweile in einigen Fällen auch Berichte und journalistische Auseinandersetzungen auf anderen Medien. Dennoch lässt sich vermuten, dass vor allem solche ›Geschichten‹ breiter rezipiert werden und Empörung hervorrufen, die eine Identifizierung der Mehrheitsgesellschaft mit der Betroffenen ermöglichen. Betroffene, die sich wehrhaft zeigen und gesellschaftliche Mitschuld an der erlebten Gewalt hinterfragen, entsprechen seltener den gängigen Erwartungen daran, wie Gewaltbetroffene zu sein und sich zu verhalten haben.

Es ist wichtig zu beachten, dass der Großteil der hier aufgeführten Handlungsmöglichkeiten und Strategien die selbstbestimmte Nutzung von IKT und ein gewisses Verständnis digitaler Medien oder zumindest den Zugang zu Wissen darüber voraussetzen. Barrieren in Sprache und Technikanwendung können für viele Menschen ein Ausschlusskriterium bestimmter Strategien im Umgang mit digitaler Gewalt sein. Menschen, die bei der Nutzung digitaler Medien auf Unterstützung und Assistenz angewiesen sind, müssen darauf vertrauen können, dass sie die Kontrolle behalten und die Unterstützung im Umgang mit erlebter Gewalt nicht zu weiteren Grenzverletzungen u.ä. führen.

Bewältigung als emanzipatorischer Prozess

Nach geschlechtsspezifischen Gewalterfahrungen geht es vielen Betroffenen in ihrem Bewältigungsprozess zunächst darum, ein Gefühl von Kontrolle und Handlungsfähigkeit wieder zu erlangen. Forschung zu Traumaverarbeitung und feministischer Beratungsarbeit[2] hebt hervor, dass es für eine erfolgreiche Bewältigung des Erlebten von wesentlicher Bedeutung ist, welche Erfahrungen Betroffene nach der erlebten Gewalt machen. Nicht nur die Form und der

2 Mehr zur Darstellung des partizipativen Forschungsprojektes zur Arbeit feministischer Fachberatungsstellen als kontextualisierte Traumaarbeit siehe Brenssell (2020).

Kontext der Gewalterfahrung an sich sind ausschlaggebend, sondern ebenso wie das soziale Umfeld reagiert, ob das Erlebte (gesellschaftlich) als Unrecht anerkannt wird oder beispielsweise ob Abhängigkeits- und unsichere Lebensverhältnisse bestehen. Auch nachfolgende Auseinandersetzungen mit staatlichen Institutionen und Behörden erschweren häufig den Bewältigungsprozess. Nicht selten wird die Glaubhaftigkeit Betroffener in Frage gestellt oder negiert, dass entstandene Belastungen eine Folge der Gewalt und ihrer erschwerten Verarbeitung sind (vgl. Brenssell/Hartmann 2017: 36f.).

Auch bei den hier diskutierten Strategien und der Unterstützung nach digitaler Gewalt sollte die Selbstbestimmung der Betroffenen im Fokus stehen. Die gesellschaftlichen Bedingungen von geschlechtsspezifischer Gewalt zu hinterfragen und mit dem individuell Erlebten in Beziehung zu setzen, ist für viele Frauen und andere marginalisierte Geschlechter ein selbstermächtigender Prozess. Die Verantwortung bei den Täter*innen und den vorherrschenden gewaltbegünstigenden strukturellen Ungleichheiten verorten zu können, hilft gegen Vereinzelung, sogenannte Opfermythen und Schuldzuschreibungen (»Victim Blaming«) anzukommen (ebd.). Der Austausch und die Vernetzung mit anderen Betroffenen ist grundlegend für die meisten Bewältigungsstrategien im digitalen Raum und kann eine wichtige Rolle dabei spielen, opferfeindliche Narrative aufzubrechen und sich selbst als handelndes wehrhaftes Subjekt wahrzunehmen.

Betroffene geschlechtsspezifischer digitaler Gewalt sind nie handlungsunfähige Menschen, die keine Überlegungen, Wünsche oder Anforderungen haben (vgl. Lehmann 2016: 32). Oft sind sie selbst im Netz aktiv, nutzen soziale Medien und kennen deren Mechanismen genau. Dieses Wissen macht sie handlungsfähig und ermöglicht es ihnen an manchen Stellen sogar Täter*innen in Verantwortung zu nehmen. Für den Bewältigungsprozess kann es sehr gewinnbringend sein, eigens geschaffene Gestaltungsspielräume zu nutzen und als selbstwirksam zu empfinden (vgl. Siepelmeyer/Ortiz-Müller 2017: 44). Auch an dieser Idee können sich Beratungs- und Unterstützungsangebote orientieren.

Individuelle Bewältigungsstrategien

Digitale Gewalt benennen und proaktiv erklären

Gewalterfahrungen zu benennen und damit nicht allein zu bleiben, kann Kontrolle über die Situation zurückbringen. Betroffene teilen ihre Erfah-

rungen mit ihren Freund*innen, ihrer Familie oder ihren Kolleg*innen am Arbeitsplatz. Auch können so nahestehende Personen gewarnt und vorbereitet werden, denn eine gängige Täterstrategie in Gewaltbeziehungen ist es, Freund*innen, Verwandte und Arbeitgeber*innen zu kontaktieren, um die Betroffene mit falschen Aussagen zu diffamieren.

Veröffentlichung digitaler Gewalterfahrungen (im Internet)

Frauen und andere marginalisierte Geschlechter weisen regelmäßig in ihrem Online-Status oder im Rahmen von Posts und Stories in sozialen Medien darauf hin, dass sie digitale geschlechtsspezifische Gewalt oder andere Diskriminierung erleben. Dies sorgt zum einen dafür, dass sie und ihre Anliegen sichtbarer werden und sie mehr Unterstützung erleben. Vor allen Dingen sorgen diese Veröffentlichungen aber auch dafür, dass andere Betroffene informiert werden und dadurch erfahren, dass sie nicht alleine mit ihren Erfahrungen sind. Betroffene informieren beispielsweise darüber, dass unter ihrem Namen Fakeprofile angelegt worden sind und dass ihre Online-Freund*innen darauf achten sollen, keine erneuten Freundschaftsanfragen von diesen Profilen anzunehmen oder Inhalte ungeprüft zu teilen.

Um Gewalt sichtbar zu machen, posten Betroffene auch Listen von Verboten, die der (Ex-)Partner ausgesprochen hatte oder Bilder, die Verletzungen und Wunden dokumentieren. Dazu werden häufig persönliche Texte gepostet, in der die Gewaltbeziehung und der eigene Aufarbeitungsprozess beschrieben werden. Auch Humor in Verbindung mit eigenen Stärken und Fähigkeiten kann eine Strategie der Selbstermächtigung sein. So tanzte beispielsweise eine Betroffene von häuslicher Gewalt zu den aggressiven Sprachnachrichten ihres Ex-Freundes und stellte dieses Video online (vgl. Monecke 2019).

Auch wissenschaftlich oder didaktisch aufbereitete Informationen können nicht ohne Zusammenarbeit und Austausch mit Betroffenen entstehen. Für die Beteiligten kann es empowernd sein, dass dank ihrer Sichtbarkeit anderen Betroffenen geholfen und Unterstützungspersonen qualifiziert werden können. Online verfügbare, wissenschaftlich aufbereitete Fallstudien stehen beispielsweise auf der Internetseite der australischen Universität Queensland zur Verfügung (vgl. The University of Queensland 2017). Dort zeigen Ingrid und Susan, zwei Betroffene von digitaler Gewalt auf, welche rechtlichen Interventionen für sie erfolgreich waren und ihnen ermöglichten, die Gewaltbeziehungen hinter sich zu lassen. Auf der Webseite des australischen eSafety-

Projektes gibt es diverse Videos, in denen Betroffene anhand ihrer Erfahrungen zu spezifischen Formen digitaler Gewalt informieren (vgl. eSafety Commissioner 2020: o.S.).

Shaming

»Shaming« (engl. für jemanden beschämen) ist eine Strategie der Gegenwehr und für Betroffene von digitaler Gewalt eine Möglichkeit, eine – ansonsten häufig auch ausbleibende – Form der sozialen Ächtung zu erwirken. Dazu nehmen sie beispielsweise Kontakt mit Familienangehörigen des Täters, häufig der Mutter[3] auf, oder informieren Vorgesetzte über das erlebte gewalttätige Verhalten. Problematisch erweist sich u.a. hierbei, dass Äußerungen in solch einem Kontext in den strafrechtlich relevanten Bereich einer Verleumdung fallen können. Erfahrungsgemäß scheuen sich viele gewaltausübende Personen nicht, die notwendigen Mittel dafür vorzubringen und juristisch dagegen vorzugehen.

Anna Gensler wurde beispielsweise bei der Nutzung der Dating-App Tinder regelmäßig belästigt. Die Belästigungen beinhalteten grobe und auf sexuelle Handlungen oder auf ihren Körper bezogene private Nachrichten (vgl. Hess 2014). Um den Männern, die diese unerwünschten, objektivierenden Botschaften mehrfach sendeten, etwas entgegen zu setzen und dem Ziel Aufmerksamkeit auf sexuelle Belästigung in Sozialen Netzwerken zu lenken, begann sie diese ebenfalls in einen entpersonalisierenden, sexualisierten Kontext zu stellen. Sie benutzte deren Profilbild, zeichnete sie nackt und versah

3 Die dahinterliegende Idee, die wirksamste Sanktion geschehe durch das in Kenntnissetzen der Mutter oder die Annahme, nur sie sei in der Lage die Gewalt zu stoppen, bringt einen Beigeschmack mit sich und verdeutlicht gleichwohl, dass Verursachende digitaler Gewalt selten gesellschaftliche Sanktionen befürchten müssen und sich Betroffene von geschlechtsspezifischer Gewalt nicht darauf verlassen können, dass andere schockiert genug wären, um zu intervenieren oder Position zu beziehen.

das Bild des Belästigers mit einem anzüglichen Satz aus den privaten Nachrichten, die sie zuvor erhalten hatte und postete sie auf deren Profil[4].

Technische Kompetenzerweiterung
Betroffene suchen häufig selbst erfolgreich nach Informationen, wie sie ihre Geräte und ihre Benutzer*innenkonten bzw. die ihrer Kinder sicherer gestalten können. Dadurch erhöhen sie ihr subjektives Sicherheitsgefühl. Die Tatsache, dass sie sich selbst helfen können, kann sehr selbstermächtigend sein. Die Sicherheitshinweise vom National Network To End Domestic Violence (NNEDV) geben dazu einen Überblick und bieten Hinweise dazu, wie Social Media trotz einer Gewaltbeziehung genutzt werden kann (vgl. NNEDV 2014).

Online Ablenkung bei physischer Verfolgung
Eine Strategie kann auch darin bestehen, dass Betroffene Bilder und Inhalte posten, die nicht der Wahrheit entsprechen, um von sich abzulenken und Gewalttäter*innen zu verwirren oder auf eine falsche Fährte zu locken. Dazu werden beispielsweise Bilder mit falschen Standortübermittelungen geteilt, Fotos von einem anderen Ort hochgeladen oder falsche Statusmeldungen auf Social Media genutzt.

Fluten
Beim Fluten werden die Ergebnisse zu einem Begriff oder Namen in einer Suchmaschine mit neuen Informationen und Bildern geflutet und nicht erwünschte Inhalte auf den ersten Ergebnissuchseiten verdrängt durch Inhalte, die die betroffene Person selbst gewählt hat. Ein sehr bekanntes Beispiel dieser Vorgehensweise ist Emma Holten. 2011 wurden intime Aufnahmen von ihr ohne ihre Zustimmung veröffentlicht und weiterverbreitet. Die Bilder gingen schnell viral. Daraufhin trugen unbeteiligte Dritte persönliche Informationen (wie z.B. Privatadresse) über Emma Holten zusammen und machten sie

4 Umgangsstrategien, die mit bildlichen Darstellungen von Tätern arbeiten oder mit Metaphern den Spieß umdrehen sollen, basieren häufig ebenfalls auf gesellschaftlichen Diskriminierungspraxen, wie der lookistischen und inter-/queerfeindlichen Bezugnahmen auf Penisgrößen, feminisierten und damit trans-/queerfeindlichen Darstellungen von cis-Männern oder ableistischen und klassistischen Einordnungen des Täters. Auch Betroffene von geschlechtsspezifischer Gewalt müssen sich der Frage stellen, inwieweit ihre Handlungen zur Selbstermächtigung wiederum andere Menschen verletzen können und Gewalt reproduzieren.

öffentlich. Dieses »Doxing« führte zu weiterer massiver, nicht einzugrenzender Belästigung und Bedrohung. Jahre später veröffentlichte Emma Holten online ihr eigenes Fotoprojekt »Zustimmung« mit Nacktaufnahmen von sich im Alltag. Mit diesen neuen Bildern flutete sie die Suchmaschinen mit dem Ziel, dass nicht die geleakten Fotos zuerst gezeigt werden, sondern die Bilder, die sie selbst veröffentlichte. Seitdem spricht sie über diese Gewalterfahrung und macht anderen Betroffenen Mut, sich aktiv zur Wehr zu setzen und die Medien und Funktionsweisen des Internets auch für die Bewältigung der Gewalterfahrung einzusetzen (vgl. Holten 2016).

Gegenrede und gemeinsame Hashtags

Der Grundgedanke von Strategien zur Gegenrede ist, dass effektives Kontern von Hate Speech[5] eine Gegenöffentlichkeit und Entkräftung von menschenfeindlichen Äußerungen im Netz und letztendlich ganzer menschenfeindlicher Online-Diskurse bewirkt. Gegenrede erweist sich als ein reichhaltiger und komplexer Weg des Widerstandes gegen Belästigung im Internet (vgl. Stroud/Cox 2018: 294). Als Reaktion auf die zunehmende Online-Gewalt und Hate Speech gibt es eine Vielzahl von Initiativen von Einzelpersonen oder Gruppen gegen Hass im Netz. Betroffene vernetzen sich über diverse Plattformen und Medien und setzen dabei auf Strategien wie Deeskalation, Gegenrede, Meldung und Hilfsstellungen für Betroffene (vgl. Lehning 2020: 200).

Unter #IchBinHier vernetzen sich User*innen und posten Gegenrede als Reaktion auf Hasskommentare, Diskriminierung oder beispielsweise Verschwörungserzählungen, immer mit dem Ziel so viel unterstützenden Content und Aufmerksamkeit wie möglich zu generieren, um Hasskommentator*innen und ihre Inhalte zu verdrängen. Sie machen sich dabei die Logik der meisten Kommentarfunktionen zunutze, deren Algorithmen u.a. Beiträge mit mehr Resonanz prominenter platzieren.

Unter gemeinsamen Hashtags vernetzen sich Menschen, die ähnliche Erfahrungen online oder offline machen. Spezifische (Gewalt)Erfahrungen, die mit einem gemeinsamen Hashtag markiert und von anderen Betroffenen (weltweit) geteilt und verbreitet werden, verdeutlichen anschaulich, dass es sich bei diesen Erfahrungen nicht um Einzelfälle, sondern um strukturell verankerte und gesellschaftlich gewollte, zumindest geduldete, Unterdrückungsmechanismen handelt. Nicht selten sind virale Hashtags

5 Siehe Beitrag: Strategien im Umgang mit Online Hate Speech.

Anlass weiterer medialer und gesellschaftlicher Auseinandersetzungsprozesse. Auch wenn diese Praxis zunächst von Betroffenen von Hate Speech verwendet wurde, so findet sie immer mehr Anwendung im Bereich der (digitalen) Gewalt aus dem sozialen Nahraum; ein sehr bekannter Hashtag aus dem Bereich der sexualisierten Gewalt (im Arbeitsleben) ist #MeToo. Weitere Beispiele der letzten Jahre mit Bezug zu geschlechtsspezifischer Gewalt und Diskriminierung waren u.a.: #Aufschrei, #Ausnahmslos, #MeTwo, #MeQueer, #WirSindViele #WasIhrNichtSeht, #SayHerName, #NiUnaMenos, #KeineMehr, #BLM, #BlackLivesMatter, #BlackTransLivesMatter, #MyBodyIsNotYourPorn oder die Instagramseite @antiflirting2.

Pause machen: (vorübergehender) Rückzug aus dem digitalen Raum

Erste Reaktionen auf einen digitalen Angriff können Angst, Hemmungen, Starre, Verunsicherung oder Beklommenheit sein, häufig begleitet von Ohnmachtsgefühlen und einem immensen Gefühl von Kontrollverlust. Die langfristigen Folgen können starke psychische Belastungen wie Panikattacken, Schlafstörungen und Depressionen bis hin zum Suizid sein (vgl. Amnesty International 2018: o.S.). Viele Betroffenen ziehen sich aus dem Internet zurück, schränken den Gebrauch von Geräten und Online-Diensten zunächst zur Gänze ein oder machen eine Pause vom digitalen Raum und der damit verbundenen Gewaltform (vgl. Matthews u.a. 2017: 2194; Amnesty International 2018; Citron 2019). Es bleibt zu bedenken, dass diese Strategie häufig sehr effektiv, aber ebenso von den meisten Täter*innen intendiert sein dürfte. Der Verzicht auf digitale Medien und das Internet schließt Gewaltbetroffene von zahlreichen Informations- und Kommunikationsmöglichkeiten aus, isoliert sie von sozialen Kontakten und ist zwangsläufig mit beruflichen/schulischen Nachteilen verbunden. Eine solche Einschränkung an Teilhabemöglichkeiten kann keine gesellschaftlich gewollte oder langfristige Antwort auf digitale Gewalt sein.

Selbstbestimmter Umgang mit digitaler Gewalt

Die angeführten Beispiele zeigen kreative Lösungen und Bewältigungsstrategien, die Betroffene etablieren, um erlebte digitale Gewalt zu verarbeiten. Ziel der Betroffenen ist es dabei meist, die eigene Souveränität, Selbstbestimmung und Handlungsfähigkeit wiederzuerlangen, der erlebten Entmündigung und Ohnmacht eigene Narrative und Handlungen entgegenzusetzen. Prekarisierung, Ausgrenzung, Diskriminierung und fehlende (staatliche) Un-

terstützung schränken die Möglichkeiten zur Bewältigung für viele Betroffene ein. Auch wenn Bewältigungsstrategien in ihrem Nutzen individuell sind, liegt es nicht allein in der individuellen Verantwortung Betroffener, sich solche anzueignen und erfolgreich umzusetzen. Es besteht eine staatliche und gesamtgesellschaftliche Verantwortung dahingehend, Frauen, trans und inter* Personen sowie Kinder vor geschlechtsspezifischer Gewalt im weitesten Sinne zu schützen. Mit der Ratifizierung menschenrechtlicher Verträge wie CEDAW (Convention on the Elimination of All Forms of Discrimination Against Women) und dem Übereinkommen des Europarats zur Verhütung und Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt (die sogenannte Istanbul-Konvention) hat sich die Bundesrepublik Deutschland und damit alle staatlichen Organe wie Gesetzgeber*innen, Gerichte und Strafverfolgungsbehörden, verpflichtet, geschlechtsspezifische Gewalt zu bekämpfen.

Aus der Geschichte der zweiten Frauenbewegung ist bekannt (vgl. Hagemann-White 2002: 29ff.), dass sich Betroffene geschlechtsspezifischer Gewalt Räume gesucht und gestaltet haben, um mit Gewalterfahrungen umzugehen. Damals waren es vor allem selbstorganisierte Selbsthilfegruppen, autonom verwaltete Frauennotrufe, Frauenberatungsstellen oder Frauenhäuser – da keine entsprechenden Beratungs- und Unterstützungsangebote vorhanden waren. Der Leitsatz der damaligen Zeit kann aus heutiger Sicht erweitert werden – Das Private ist politisch – das Internet ist es auch! Und es bietet Zugang zu Räumen, die eine selbstbestimmte Auseinandersetzung und Unterstützung innerhalb eigener Communities – ortsunabhängig – ermöglichen. Eine Verständigung beispielsweise über erlebte geschlechtsspezifische, rassistische, queerfeindliche und behindertenfeindliche (digitale) Gewalt findet immer zuerst selbstorganisiert und entlang gemeinsam geteilter Diskriminierungserfahrungen statt. Marginalisierte Menschen sind gezwungen, Strategien zur Selbstverteidigung und Bewältigung selbst zu erproben, meist mit einem sehr großen Bewusstsein darüber, welche strukturellen Ungleichheiten ihren Erfahrungen zugrunde liegen. Diese Erfahrungen sollten an erster Stelle gehört und berücksichtigt werden, wenn es darum geht, inwieweit staatliche Institutionen und die Mehrheitsgesellschaft Verantwortung übernehmen und die Situation Betroffener verbessert werden können.

Es bedarf eines gesellschaftlichen Diskurses darüber, wie ein gewaltfreies Internet für alle ermöglicht werden kann. Es ist unabdingbar dabei zu diskutieren, welche gesellschaftlichen Gruppen besonders vulnerabel für digitale Angriffe sind und welche Rolle die Digitalisierung geschlechtsspezifischer Gewalt im sozialen Nahraum – also u.a. durch (Ex-)Partner*innen oder Kol-

leg*innen – dabei spielt. Der Zugang zu Internet und digitalen Medien sollte für alle barrierefrei möglich sein, die Aneignung von sicherheitsspezifischer Medienkompetenz darf dabei aber keine Bedingung für den Schutz vor Gewalt sein. Im Gegenteil sollten es gerade Informations- und Kommunikationstechnologien Gewaltbetroffenen ermöglichen, sich Unterstützung und Hilfe zu suchen sowie durch Vernetzung und sicher gestaltete Online-Räume gegen Ausgrenzung und soziale Isolation anzugehen.

Literatur

Amnesty International (2018): »Toxic Twitter – A Toxic Place For Women«. https://amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/ [Zugriff: 17.5.2020].

bff: Bundesverband Frauenberatungsstellen und Frauennotrufe (2020): »bff: aktiv gegen digitale Gewalt«. https://frauen-gegen-gewalt.de/de/bff-aktiv-gegen-digitale-gewalt.html [Zugriff: 20.08.2020].

Brenssell, Ariane (2020): »Kontextualisierte Traumaarbeit – Ein communitybasiertes, partizipatives Forschungsprojekt«, in: Brenssell, Ariane/ Lutz-Kluge, Andrea (Hg.), Partizipative Forschung und Gender –Emanzipatorische Forschungsansätze weiterdenken. Opladen/Berlin/Toronto: Barbara Budrich, S. 71-94.

Brenssell, Ariane/Hartmann, Ans (2017): »Kontextualisiertes Traumaverständnis in der Arbeit gegen Gewalt an Frauen«, in: Familiendynamik, Vol. 42 Nr. 1, S. 28-39.

Citron, Danielle (2019): »Cyber Mobs, Disinformation, and Death Videos: The Internet as It Is (And As It Should Be)«. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3435200 [Zugriff: 6.8.2020].

Dobash, Russell P./Dobash, Emerson (1992): Women, violence and social change. London/New York: Routledge.

eSafety Commissioner (2020): »Your Stories«. https://esafety.gov.au/key-issues/image-based-abuse/stories [Zugriff: 21.8.2020].

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

Hagemann-White, Carol (2002): »Gewalt im Geschlechterverhältnis als Gegenstand sozialwissenschaftlicher Forschung und Theoriebildung: Rückblick, gegenwärtiger Stand, Ausblick«, in: Dackweiler, Regina-Maria/Schäfer, Reinhild (Hg.), Gewaltverhältnisse. Feministische Per-

spektiven auf Geschlecht und Gewalt. Frankfurt/New York: Campus Verlag, S. 29-52.

Hartmann, Ans (2017): »Fachberatungsstellen und die Digitalisierung geschlechtsspezifischer Gewalt. Ergebnisse einer Umfrage unter Frauenberatungsstellen und Frauennotrufen im bff«, in: bff: Bundesverband Frauenberatungsstellen und Frauennotrufe (Hg.). https://frauen-gegen-gewalt.de/de/aktuelle-studien-und-veroeffentlichungen.html [Zugriff: 21.8.2020].

Hess, Amanda (2014): »How to get revenge on online dating creeps: Draw them naked«. https://slate.com/human-interest/2014/04/anna-gensler-gets-back-at-tinder-and-okcupid-creeps-by-drawing-them-naked.html [Zugriff: 3.4.2020].

Holten, Emma (2016): »Emma Holten (Activist) | TNW Conference | The Power of Consent«. https://youtube.com/watch?v=xMu1Nt2-ypI [Zugriff: 21.8.2020].

Katzer, Catarina (2014): Cybermobbing. Wenn das Internet zur W@ffe wird. Berlin/Heidelberg: Springer Spektrum Verlag.

Lehmann, Katrin (2016): Professionelles Handeln gegen häusliche Gewalt. Der Platzverweis aus der Sicht von Polizei, Beratung und schutzsuchender Frauen. Wiesbaden: Springer Fachmedien.

Lehning, Lukas (2020): Digitale Kommunikation aus der Perspektive des Sozialbehaviorismus. Eine Untersuchung digital vermittelter Selbst-Wahrnehmung nach George Herbert Mead. Baden-Baden: Tectum Verlag.

Matthews, Tara/O'Leary, Kathleen/Turner, Anna/Sleeper, Manya/Palzkill Woelfer, Jill/ Shelton, Martin/Churchill, Elizabeth F./Consolvo, Sunny (2017): »Stories from Survivors: Privacy & Security Practices when Coping with Intimate Partner Abuse.« https://mshelt.onl/p/matthews_et_al_2017.pdf [Zugriff: 21.8.2020].

Monecke, Nina (2019): »Auf TikTok tanzen junge Frauen zu übergriffigen Sprachnachrichten ihrer Exfreunde«. https://ze.tt/auf-tiktok-tanzen-junge-frauen-zu-uebergriffigen-sprachnachrichten-ihrer-exfreunde/?utm_medium=sm&utm_source=facebook_zettaudev_int&wt_zmc=sm.int.zettaudev.facebook.ref.zett.redpost_zett.link.sf&utm_content=zett_redpost_zett_link_sf&utm_term [Zugriff: 21.8.2020].

NNEDV: National Network To End Domestic Violence (2014): »Privacy & Safety on Facebook: A Guide for Survivors«. https://nnedv.org/resources-library/h_privacy-safety-facebook-guide/ [Zugriff: 21.8.2020].

Piispa, Minna (2002): Complexity of Patterns of Violence Against Women in Heterosexual Partnerships, in: Violence Against Women, Vol. 8 Nr. 7, S. 873-900.

Siepelmeyer, O./Ortiz-Müller, W. (2017): »Prävalenz, Demographie und Typologien des Stalkings«, in: Ortiz-Müller, Wolf (Hg.), Stalking – das Praxishandbuch. Opferhilfe, Täterintervention, Strafverfolgung. Stuttgart: W. Kohlhammer Verlag, S. 34-44.

The University of Queensland (2017): »Domestic Violence Case Studies«. https://law.uq.edu.au/research/our-research/using-law-and-leaving-domestic-violence/domestic-violence-case-studies [Zugriff: 21.8.2020].

Walker, Lenore E. (1979): The Battered Woman. New York: Harper & Row.

Strategien im Umgang mit Online-Hate Speech

Harald Klant

Während in der Politik in den letzten Jahren insbesondere juristische Möglichkeiten und Maßnahmen der Plattformbetreiber*innen diskutiert wurden, beschäftigen sich zahlreiche Aktivist*innen und Organisationen mit Selbstschutzstrategien und Präventionsarbeit gegen Online-Hate Speech. Hate Speech definiere ich in Anlehnung an Liriam Sponholz als eine Kommunikationsform, bei der intentional und/oder bewusst diskriminierende Botschaften (Bilder, Texte, Videos etc.) verbreitet und ganze ›Gruppen‹[1] von Menschen abgewertet werden (vgl. Sponholz 2018: 48). Die Botschaften richten sich gegen Menschen, die bereits aufgrund gesellschaftlicher Herrschafts- und Diskriminierungsverhältnisse wie Rassismen, Sexismus, Ableismus und/oder Homo- und Transfeindlichkeit marginalisiert werden oder gegen solche, die sich mit diesen Menschen solidarisch zeigen (vgl. Lembke 2017: 4). Mit Bezug zur Definition von »Digitaler Gewalt« nach Ans Hartmann verstehe ich unter Online-Hate Speech alle Formen von Hate Speech, die sich digitaler Medien bedienen und/oder im digitalen Raum z.B. auf Online-Portalen oder sozialen Plattformen stattfinden (vgl. Hartmann 2017: 2).

Der Umgang von Betroffenen mit Online-Hate Speech ist vielfältig und alles andere als passiv, jedoch wird dies selten im öffentlichen Diskurs sichtbar. Daher werden im Rahmen dieses Artikels Interventions- und Umgangsstrategien vorgestellt, welche zu einem Großteil von direkt betroffenen Individuen und Organisationen entwickelt wurden. Die Sammlung dient als Inspiration für Betroffene von Online-Hate Speech, aber auch für Betroffene digitaler

1 ›Gruppen‹ schreibe ich in Anführungszeichen, um aufzuzeigen, dass es sich nicht notwendigerweise um tatsächliche soziale Gruppen, sondern konstruierte Gruppen handelt.

Gewalt im sozialen Nahfeld, und gibt beratend tätigen Menschen die Möglichkeit, auf bereits erprobtes Wissen im Umgang mit Online-Hate Speech zurückzugreifen.

(Online-)Aktivismus

Aktivismus kann als (politische) Handlungsform verstanden werden, mithilfe derer auf konkrete Missstände und Defizite hingewiesen und die Veränderung bestehender Verhältnisse erwirkt werden soll (vgl. Würdemann 2013). Dabei bedient sich Aktivismus verschiedenster Strategien, zu denen unter anderem Öffentlichkeitsarbeit, Boykottaufrufe und Demonstrationen gehören. Durch digitale Technologien ergeben sich weitere Strategien wie Hashtag-Aktivismus[2], Hacktivismus[3] und Online-Petitionen. Ziele von Aktivismus in Bezug auf Online-Hate Speech können sein:

- Für Hate Speech sensibilisieren und Diskriminierung und Herrschaftsverhältnisse kritisieren.

2 Ein Hashtag ist ein Schlagwort, welches mit dem »#«-Zeichen versehen wird. Nutzer*innen können mithilfe von Hashtags ihre Posts einem Thema zuordnen. Suchen Menschen auf Online-Plattformen nach einem Hashtag, werden alle mit diesem Hashtag markierten Beiträge angezeigt. Eine erfolgreiche Hashtagkampagne in Deutschland war die von zahlreichen feministischen Aktivist*innen initiierte Kampagne »#ausnahmslos«. Die Kampagne wurde als Reaktion auf die Vorfälle in der Silvesternacht in Köln 2015/16 und die von Rassismus und Sexismus geprägte Berichterstattung ins Leben gerufen (vgl. Bündnis #ausnahmslos 2016). Vorteile einer Hashtag-Kampagne sind, dass sie theoretisch von jedem gestartet werden kann und – außer eines internetfähigen Gerätes – keiner finanziellen oder technischen Voraussetzungen bedarf. Eine Herausforderung für Hashtag-Kampagnen ist, dass sie leicht von gegnerischen Nutzer*innen gekapert werden können. Der Hashtag #ausnahmslos wurde beispielsweise in einer geplanten Aktion von anonymen Gruppen gekapert, welche auf Twitter sexualisierte Bilder von Frauen* (das »*« macht hierbei auf die soziale Konstruiertheit der Geschlechterkategorien aufmerksam) kombiniert mit sexistischen Sprüchen posteten und diese ebenfalls mit dem Hashtag #ausnahmslos markierten (vgl. Kramper 2016).

3 Hacktivismus ist politisch motiviertes Hacken (mithilfe der Nutzung von Computerprogrammen unberechtigt in andere Computersysteme eindringen). Dazu zählt das unberechtigte Verändern einer Webseite oder das absichtliche Überlasten eines Servers, damit eine bestimmte Webseite zeitweilig nicht mehr aufgerufen werden kann.

- Plattformbetreiber*innen unter Druck setzen, klare, menschenrechtsorientierte Community-Regeln aufzustellen, barrierearme Beschwerdemechanismen zu etablieren und für die Durchsetzung der Community-Regeln zu sorgen.
- Diskriminierungssensible Moderation von Plattformbetreiber*innen einfordern, welche spezifische oder indirekte Formen von Hate Speech und digitaler Gewalt erkennt.
- Gesetzgeber*innen unter Druck setzen, effektive, auf die digitale Welt abgestimmte Gesetze zu erarbeiten, die den Schutz der Menschen- und Grundrechte online garantieren – dabei aber nicht die Privatsphäre von Menschen verletzen und/oder die Möglichkeit der Anonymität im Internet[4] zerstören.
- Unternehmen, Politiker*innen und Personen des öffentlichen Lebens auffordern, Haltung zu zeigen und für demokratische Werte einzustehen sowie Hate Speech zu sanktionieren.[5]
- Unternehmen, Politiker*innen, Personen des öffentlichen Lebens unter Druck setzen, nicht mit demokratie- und/oder menschenfeindlichen, Hate Speech verbreitenden Organisationen und Plattformen zusammenzuarbeiten.[6]
- Einzelpersonen motivieren und befähigen, sich gegen Hate Speech sowohl online als auch offline zu engagieren.
- Geld sammeln, um Initiativen gegen Hate Speech oder direkt von digitalen Angriffen betroffene Personen zu unterstützen.

In Deutschland gibt es mehrere Einzelpersonen und Organisationen, die sich aktivistisch gegen Online-Hate Speech engagieren. Eines der größten Projek-

---

4 Anonymität im Internet ist ein Gut, welches marginalisierten Menschen ermöglicht, sich über ihre Erfahrungen auszutauschen, ohne im analogen Leben Stigmatisierung zu fürchten. Gesetze, die Online-Hate Speech regulieren, sollten daher die Möglichkeit sich online anonym zu bewegen, nicht grundsätzlich einschränken (vgl. Quinn 2015: Minute 3:39-4:23).

5 Beispielsweise finanzierte die Firma Intel, nachdem sie aufgrund der sexistischen »GamerGate«-Kampagne in Kritik geriet, ein »Diversity in Technology«-Programm, welches zur besseren Repräsentation von Frauen* in der Gaming-Industrie beitragen sollte (vgl. Wingfield 2015). Mehr zur »GamerGate«-Kampagne siehe Burns 2017.

6 Eine Möglichkeit hierfür ist, Unternehmen unter Druck zu setzen, auf rechtsextremen Blogs und Nachrichtenseiten keine Werbung zu schalten oder bestimmte Hate Speech verbreitende YouTube-Kanäle nicht mit Werbung zu finanzieren.

te in Deutschland ist das als Jugend-Kampagne vom Europarat initiierte »No Hate Speech Movement« (vgl. Council of Europe 2019). Ziel des Projektes ist es insbesondere, für die Problematik von Online-Hate Speech zu sensibilisieren und Nutzer*innen zur Gegenrede zu ermutigen (vgl. Neue Deutsche Medienmacher e.V. o.J.). Hierfür stellt die Kampagne auf ihrer Webseite umfassende Informationsmaterialien und Memes[7] zum Kontern von Hate Speech zur Verfügung. Des Weiteren bietet die Kampagne explizit Medienschaffenden Ressourcen, um mit Online-Hate Speech umzugehen (vgl. ebd.). Auch Einzelpersonen machen mit Aktionen auf das Phänomen Online-Hate Speech aufmerksam. Beispielsweise machte die US-amerikanische Künstlerin Whitney Bell mit ihrer Ausstellung »A Lifetime of Dick Pics« auf das Problem sexueller Belästigung online aufmerksam. Inhalt der Ausstellung sind eine Vielzahl an unerwünscht erhaltenen »Dickpics« (Fotos von Penissen), ausgestellt in einem Raum, der dem Zuhause der Künstlerin nachempfunden ist. Hiermit verdeutlicht Bell die Allgegenwärtigkeit der Belästigung und das Eindringen in ihre Privatsphäre (vgl. Stevenson 2016).

Von digital zu analog

Verschiedene Akteur*innen haben im Umgang mit Online-Hate Speech bereits versucht, Debatten, in denen besonders viel Hate Speech verbreitet wird, vom digitalen in den analogen Raum zu verschieben. Dies kann einer Polarisierung der Meinungen entgegenwirken und Internetdynamiken, die zur Entmenschlichung (politischer) Gegner*innen beitragen, aufheben. Eine begrenzte Anzahl an Diskussionsteilnehmer*innen, feste, vorab vereinbarte Diskussionsregeln und Themen verhindern störende Kommunikationsstrategien wie Themenhopping oder Hatestorms, die allein aufgrund der Anzahl der Beiträge nicht zu bewältigen sind.

Gelungen ist eine solche Verlagerung in den analogen Raum der Alice Salomon Hochschule Berlin (ASH). Die Hochschule stand 2017 aufgrund einer Diskussion um ihre Fassadengestaltung im Fokus der Öffentlichkeit. Die ›überhitzte‹ Debatte wirkte polarisierend und wurde von Hate Speech Kom-

7 Memes sind kurze, aussagekräftige Motive, Bilder oder Video-Schnipsel – häufig mit einem Text versehen.

mentaren in sozialen Medien und Nachrichtenforen begleitet.[8] Daraufhin organisierte die ASH gemeinsam mit dem Haus für Poesie eine Podiumsdiskussion. Laut der damaligen Prorektorin Bettina Völter hatte die Podiumsdiskussion einen positiven Einfluss auf die öffentliche Debatte. Die Darstellungen in der Presse seien nach der Veranstaltung sachlicher und differenzierter geworden, der Ton habe sich insgesamt etwas beruhigt (vgl. Völter 2017: 7). Dazu beigetragen hat laut Völter auch die szenische Lesung der Studierenden zu Beginn der Veranstaltung, in welcher Ausschnitte aus Artikeln und Stellungnahmen vorgelesen und so den anwesenden Medienvertreter*innen die »Überhitzung« der Debatte gespiegelt wurde (vgl. ebd.).

Diese Strategie ist gleichzeitig mit einigen Herausforderungen verbunden:

- Anonymität ist für manche Online-Akteur*innen eine Voraussetzung für ihr Handeln. Für ein Treffen im analogen Raum ist zumindest ein gewisser Grad an De-Anonymisierung notwendig. Insbesondere Personen, die sich bewusst sind, dass ihre Aussagen strafrechtlich relevant sein oder arbeitsrechtliche Konsequenzen mit sich bringen könnten, werden sich nicht auf ein de-anonymisiertes Gespräch einlassen.
- Es muss sich im Voraus auf einen Ort, Rahmenbedingungen (wie Moderation oder Mediation) und auch das Thema der Diskussion geeinigt werden.
- Auch bei einer analogen Diskussion kann es zur Verbreitung von Hate Speech kommen.

Während die Strategie, eine Diskussion vom digitalen in den analogen Raum zu verlegen, für größere Organisationen oder Institutionen durchaus effektiv sein kann, so ist sie für Individuen ohne öffentliche Plattform schwer umsetzbar und wenig sinnvoll. Denn die Verlagerung vom digitalen in den analogen Raum kann zwar dazu beitragen eine sowieso schon vor/mit einer breiten Öffentlichkeit geführte Debatte positiv zu beeinflussen. Allerdings wird sie (insbesondere anonyme) Täter*innen nicht davon abhalten, Individuen mit Hate Speech und anderen Formen der digitalen Gewalt zu belästigen.

8 Ausführliche Informationen zur Fassaden-Debatte: Alice Salomon Hochschule Berlin o.J.

Täter*innenschaft sichtbar machen

Täter*innen sichtbar zu machen, kann bedeuten, deren Namen, Foto, Profile[9], Aussagen und z.B. auch deren Arbeitgeber*in zu veröffentlichen, um diese über die Tätigkeit ihrer Beschäftigten zu informieren. Dies ist eine vielfach genutzte Strategie gegen Hate Speech allgemein und Online-Hate Speech speziell.[10] Ziel der Taktik kann es sein, die (soziale) Anonymität der Täter*innen aufzuheben. Fotos und Klarnamen machen die Täter*innen greifbarer, stellen sie in den Fokus und können einer empfundenen Hilflosigkeit gegen Online-Hate Speech entgegenwirken. Durch das öffentliche ›an den Pranger stellen‹ wird das direkte Umfeld, Familienmitglieder, Freund*innen und Arbeitgeber*innen auf die Aussagen der Täter*innen aufmerksam gemacht und es besteht die Möglichkeit, dass sich die Täter*innen vor diesen rechtfertigen müssen. Eine Folge der Veröffentlichung kann auch sein, dass die Täter*innen ihren Job verlieren[11] oder sich die Arbeitgeber*innen öffentlich positionieren müssen. Des Weiteren kann die Methode Einzelne ermutigen, Anzeige gegen die Täter*innen zu erstatten und die Justiz unter Druck setzen, strafrechtlich relevante Aussagen im Sinne des Volksverhetzungsparagraphen direkt zu verfolgen. Vom Melden und Löschen von Inhalten unterscheidet sich die Strategie darin, dass die Täter*innen hierbei in den meisten Fällen keine Konsequenzen im analogen Leben fürchten müssen. Auch mögliche Rechtfertigungszwänge im direkten sozialen Umfeld oder vor Arbeitgeber*innen bleiben aus. Ihre Kommentare ›verschwinden‹ lediglich und dies wird von ihnen eher als ungerechtfertigte/willkürliche ›Zensur‹ bewertet – im Vergleich zu einem Gerichtsverfahren oder einer direkten Auseinandersetzung mit Personen aus ihrem sozialen Umfeld. Kritisch zu reflektieren ist, dass das Zusammentragen und Veröffentlichen von Daten ebenfalls eine Strategie ist, die häufig gegen marginalisierte Menschen verwendet wird.[12] Vor diesem Hintergrund ist zu diskutieren, in welchen Kontexten der Ansatz als Gegenwehr und Selbstverteidigung gerechtfertigt ist. Des Weiteren ist der gewünschte

9 Profile sind die persönlichen Seiten in sozialen Netzwerken.

10 Beispiel hierfür ist die Webseite »Perlen aus Freital« https://perlen-aus-freital.tumblr.com/ [Zugriff: 14.9.2020].

11 Beispielsweise kündigte ein Porschehändler in Österreich seinem Lehrling, nachdem bekannt wurde, dass dieser rassistische Hate Speech gegen Geflüchtete online gepostet hatte (vgl. o.A. 2015).

12 Siehe Beitrag: Individuelle Strategien im Umgang mit geschlechtsspezifischer digitaler Gewalt.

Effekt sozialer Sanktionen auch vom gesellschaftlichen Verständnis von ›akzeptablem‹ und ›verwerflichem‹ (online) Verhalten abhängig. Letztlich kann die Sichtbarmachung der Täter*innen auch zu Solidarisierungseffekten, vermehrter Hate Speech als Folge oder direkten Gewaltandrohungen gegen die Personen, welche die Namen der Täter*innen veröffentlichen, führen.[13]

Weitere Beispiele für das Sichtbarmachen von Täter*innenschaft sind unerwünscht erhaltene sogenannte Dickpics an Verwandte oder Partner*innen der Täter*innen weiterzuleiten oder eine öffentliche Bildergalerie mit den Profilbildern der Täter*innen, die unerwünschte Sex-Anfragen schicken, mit den jeweiligen Nachrichten als Zitat oder Screenshot bei Facebook zu eröffnen.

Counter Speech

Ziel von Counter Speech (dt. Gegenrede) ist es, den sich menschenfeindlich äußernden Gruppen und Individuen den digitalen Raum nicht zu überlassen, für eigene politische und moralische Werte einzustehen und solidarisch mit Betroffenen zu handeln. Dabei wird davon ausgegangen, dass zu den Akteur*innen online auch »stille Mitleser*innen« gehören, die es zu ermutigen gilt, Hate Speech in Frage zu stellen, für demokratische Grundwerte einzustehen und sich an der Diskussion zu beteiligen. Durch Counter Speech kann ein Gegengewicht zur empfundenen Dominanz von Hate Speech in den sozialen Netzwerken entstehen (vgl. Dinar u.a. 2016: 9).

Diverse Methoden für gelungene Counter Speech schlagen sowohl die Amadeu Antonio Stiftung als auch das »No Hate Speech Movement« vor. Zu ihnen gehören unter anderem: Rückfragen stellen, Diskriminierung und Pauschalisierung benennen und Debunking[14] (vgl. ebd.: 9ff.). Hilfreich für Counter Speech sind nicht nur Gesprächsmethoden, sondern auch, sich über die häufigsten Vorurteile und menschenfeindlichen Narrative, die on- und offline

13 Beispielsweise erhielten die anonymen Betreiber*innen von »Perlen aus Freital« sowohl Doxing-Drohungen als auch Morddrohungen als Reaktion auf ihre Webseite (vgl. Meisner 2015).

14 Mit Debunking ist das Entlarven von Falschinformationen, Gerüchten und Verschwörungsmythen gemeint und richtet sich dabei nicht nur an die Person direkt, sondern insbesondere an stille Mitleser*innen, die noch kein gefestigtes Meinungsbild zu dem jeweiligen Thema haben (vgl. Dinar u.a. 2016: 12).

verbreitet werden, zu informieren.[15] Es kann nützlich sein, sich eine Datenbank an Gegenargumenten und Antworten anzufertigen. Des Weiteren werden von verschiedenen Organisationen regelmäßig Argumentationstrainings gegen Rechtsextremismus, Rechtspopulismus und Anti-Feminismus angeboten, welche die Counter Speech erleichtern.

Counter Speech kann auch als Gruppe betrieben werden. Beispiel hierfür ist die Facebook-Gruppe »#ichbinhier«, die täglich Kommentarspalten von Nachrichtenplattformen aufsucht, sich gegen Hate Speech positioniert und sich dabei gegenseitig positiv durch weitere Kommentare oder Likes bestärkt.[16] Als geschlossene Gruppe in eine Online-Diskussion einzutreten ermöglicht, dass sich Einzelne in der Gruppe auf unterschiedliche Themen und Stichworte spezialisieren können und so nicht alle für jedes Thema gewappnet sein müssen.

Counter Speech kann jedoch sowohl emotional als auch zeitökonomisch aufwendig sein. Des Weiteren kann Counter Speech dazu beitragen, dass sich noch mehr Hater*innen in die Diskussion einklinken und die Aufmerksamkeit durch die erhöhte Diskussionsteilnahme dazu nutzen, weitere Hate Speech zu verbreiten. Sich gegen Hate Speech zu stellen und online einzumischen kann bedeuten, selbst zur Zielscheibe zu werden. Daher empfiehlt es sich, gegebenenfalls zuvor den eigenen Account zu schützen und für Unbekannte unzugänglich zu machen. Auch Debunking kann das Gegenteil vom gewünschten Effekt bewirken – nämlich, dass sich die »Menschen, deren Weltbild maßgeblich von menschenfeindlichen Ideologien bestimmt wird« (Dinar u.a. 2016: 13) sogar in ihren Überzeugungen gestärkt fühlen (vgl. ebd.).

Neben dem ernsthaften Diskutieren kann auf Hate Speech auch mit Humor, Ironie und Memes reagiert werden. Dabei kann auf die Absurdität der Beiträge hingewiesen und Frust abgelassen werden. Durch eine solche Reaktion wird kein Dialog ermöglicht und sie kann dazu beitragen, dass sich die »Fronten verhärten« (Baldauf u.a. 2015: 22).[17] Eine weitere Möglichkeit auf

15 Es gibt beispielsweise die österreichische »Stammtisch-App«, welche es sich zur Aufgabe gemacht hat, gängige rassistischen Behauptungen richtig zu stellen.

16 Weitere Informationen zu der Gruppe gibt es auf ihrer Facebook-Seite: https://facebook.com/groups/718574178311688/ [Zugriff: 5.2.2020].

17 Ein Phänomen, das ich häufig im Umgang mit Online-Hate Speech beobachtet habe, ist, dass viele Personen, die sich gegen Hate Speech stellen und ironisierend auf die Beiträge der Hater*innen reagieren, die Rechtschreibung der Täter*innen korrigieren und/oder sich über grammatikalisch falsche Aspekte der Ausdrucksweise der Täter*innen lustig machen. Während ich, insbesondere bei Hater*innen, die sich für ›die wah-

Online-Hate Speech zu antworten und dabei ein Zeichen gegen Menschenfeindlichkeit und insbesondere Rechtsextremismus zu setzten, bietet die unfreiwillige Spendenaktion »Hass hilft«. Das Projekt wandelt jeden an sie gemeldeten »Hass-Kommentar« auf Sozialen Netzwerken in eine 1€-Spende um. Die von verschiedenen Unternehmen bereitgestellten Spenden gehen an die Projekte »Aktion Deutschland hilft« und »EXIT Deutschland« – ein Nazi-Aussteiger*innen Projekt (vgl. ZDK Gesellschaft Demokratische Kultur gGmbH o.J.).

Counter Narratives

Aktivist*innen wie Kübra Gümüşay haben sich dazu entschieden, nicht mehr nur auf Hate Speech zu reagieren (Counter Speech), sondern die eigenen Narrative und Ideen zu verbreiten (Counter Narratives), in den Vordergrund zu stellen und zu fördern. Hierfür plädierte Gümüşay unter dem Schlagwort »#organizedlove«. Mit dem Konzept »Organisierte Liebe« ist gemeint, nicht mehr menschenfeindliche Ideen zu diskutieren, sondern die eigene (positive, menschenrechtsorientierte) Agenda zu forcieren, einander öffentlich Zuneigung, Anerkennung und Unterstützung zu zeigen, »digitalen Applaus zu performen« (Gümüşay 2017: Minute 13:30-13:33, Übersetzung H.K.), wohlwollende und solidarische Auseinandersetzungen zu führen und gemeinsam zu diskutieren, wie wir eigentlich leben wollen (vgl. ebd.: Minute 12:50-16:50). Da, so Gümüşay, weder Freiheit, Gerechtigkeit noch friedliches Zusammenleben einfach gegeben sind, müssen diese Werte erkämpft und »Liebe organisiert« werden (vgl. ebd.: Minute 11:56-12:08). Für Gümüşay gilt: »Sich im Angesicht des Hasses gegenseitig zu lieben und zu unterstützen, wird zu einem Akt des politischen Handelns, zu einem Akt des politischen Protests.« (Ebd.: Minute 12:11-12:25, Übersetzung H.K.)

---

ren Deutschen‹ halten, nachvollziehen kann, dass diese damit bloßgestellt und auf die Ironie ihrer eigenen Aussagen hingewiesen werden sollen, halte ich das Vorgehen dennoch für kritisch, da es sich des Klassismus und Ableismus bedient, um andere zu erniedrigen.

Melden, Moderieren, Anzeigen und Monitoring

Bei allen großen sozialen Netzwerken (Facebook, Twitter, Instagram, YouTube etc.) lassen sich gegen die Community-Standards verstoßende Inhalte melden. Die Meldung ist anonym – die gemeldete Person wird also nicht erfahren, wer sie gemeldet hat (vgl. Dinar u.a. 2016: 6). Die Betreiber*innen prüfen den gemeldeten Inhalt und entfernen ihn gegebenenfalls. Bei wiederholtem Posten gegen die Standards verstoßender Inhalte kann der Account der Person temporär oder dauerhaft gesperrt werden. Das seit Oktober 2017 wirksame Netzwerkdurchsuchungsgesetz (NetzDG) verpflichtet Betreiber*innen gewinnorientierter Netzwerke mit mehr als zwei Millionen Nutzer*innen zusätzlich »offensichtlich rechtswidrige Inhalte«, wenn sie ihnen gemeldet werden, zeitnah zu entfernen oder zu sperren und ein wirksames Beschwerdeverfahren hierfür einzurichten (vgl. Lembke 2017: 12). Sowohl bei Facebook, YouTube und Twitter verstoßen »Hassrede« (Facebook 2019), »Hasserfüllte Inhalte« (YouTube 2019) und »Hass schürendes Verhalten« (Twitter 2019) gegen die Community-Richtlinien. Allerdings ist das Melden zeitaufwendig[18] (insbesondere bei hoher Anzahl der Beiträge) und oft wird Hate Speech von den Betreiber*innen nicht als solche erkannt und nicht gelöscht. Des Weiteren operieren die Plattformbetreiber*innen in Bezug auf das NetzDG undurchsichtig und inkonsistent. Es kann passieren, dass der gleiche Beitrag, der bei der einen Plattform gelöscht wird, bei der anderen nicht als rechtswidrig gilt und online bleibt (vgl. Schillat/Wüstenberg 2018). Letztlich ist auch die Effektivität des Melde- und Löschverfahrens zu hinterfragen. Auf YouTube ist es beispielsweise gängige Praxis, die Videos anderer Nutzer*innen zu »mirrorn« (dt. spiegeln) – also Kopien des Videos auf ihren eigenen Accounts hochzuladen, wenn deren Accounts oder einzelne Videos zeitweilig gesperrt werden (vgl. Alshater 2018) – damit bleiben die Videos öffentlich zugänglich.[19]

---

18 Für das Melden eines einzelnen, gegen die Community Standards verstoßenden Posts auf Facebook sind derzeit 12(!) Klicks notwendig. Auch das NetzDG-Meldeverfahren auf Facebook ist nicht Nutzer*innen-freundlich, intransparent und aufwendig gestaltet.

19 Manche Nutzer*innen sehen durch die Melde- und Löschverfahren der Plattformen ihre Meinungsfreiheit gefährdet. Viele rechte YouTuber*innen und solche, die Verschwörungsmythen verbreiten, nutzen deshalb zusätzlich das Netzwerk »DTube« (https://d.tube/), auf dem Hate Speech und gewaltvolle Inhalte ohne Einschränkungen geteilt werden können. Ende 2017 kündigte beispielsweise das rechte »Compact«-Magazin an, wegen vermeintlicher Unfreiheit im Internet (vgl. Compact 2017) ihre Ver-

Auch Betreiber*innen von kleineren Plattformen, wie beispielsweise Diskussionsforen auf Nachrichtenseiten, können Community-Richtlinien, sogenannte Netiquetten erstellen, um die digitalen Diskussionen zu moderieren.[20] Auf Basis dieser Regeln können sowohl Hate Speech als auch Beleidigungen oder destruktive und »Off-Topic«-Kommentare gelöscht oder verschoben werden (vgl. Baldauf u.a. 2015: 22). Der Vorteil von moderierten Foren besteht darin, dass »Räume für plurale Debatten und echten Austausch« (ebd.) geschaffen werden und marginalisierte Menschen nicht durch Hate Speech und andere digitale Gewalt aus den Diskussionen ausgeschlossen werden (vgl. ebd.). Zu beachten ist, dass effektive Moderation oft aufwendig und teuer ist (vgl. ebd.). Des Weiteren kann es zu einer verzerrten Darstellung der Debatten kommen, wenn problematische Beiträge kommentarlos gelöscht werden (vgl. ebd.). Laut Baldauf u.a. stellt sich hierbei die Frage, ob »Nutzer*innen wissen [sollten], dass der freundliche Honigbienen-Experte auch gerne mal rassistisch argumentiert?« (ebd.)[21]

Es gibt außerdem die Möglichkeit Online-Hate Speech zur Anzeige zu bringen.[22] Online-Hate Speech anzuzeigen kann zur Folge haben, dass die Täter*innen mit finanziellen Konsequenzen oder sogar Haftstrafen rechnen müssen.[23] Teilweise haben Betroffene auch Anspruch auf Schadensersatz (vgl. Lembke 2017: 19). Laut Lembke gibt es jedoch Probleme bei der Einordnung der digitalen Gewalt sowie bei der tatsächlichen Strafverfolgung (vgl. ebd.: 6). Es könne bei den Behörden zur Verharmlosung der Gewalt kommen und wenn eine Anzeige erfolgreich ist und es zur Klage kommt, kann ein solcher Prozess viel Zeit, Energie und weitere Ressourcen verlangen (vgl. ebd.: 5). Unterstützt werden können Betroffene unter anderem von der Organisation »HateAid«. Diese bietet Prozesskostenfinanzierung und anwaltliche Beratung

---

breitung über die sozialen Medien auszubauen und daher die Dienstanbieter »Steemit« und »DTube« zu nutzen, in welchen keine Inhalte gelöscht werden (vgl. ebd.).

20 Ein Beispiel für eine solche Netiquette findet sich auf der taz.-Webseite: https://taz.de/!118006/ [Zugriff: 5.1.2020].

21 Hinweise zur sinnvollen Gestaltung der eigenen Netiquette sind hier zu finden: Baldauf u.a. 2015: 35

22 Anzeige kann bei der Polizei oder Staatsanwaltschaft mündlich, schriftlich und auch online erstattet werden. Wie eine solche Anzeige aussehen kann und Tipps, die beim Anzeigen beachtet werden sollten, sind hier zu finden: Dinar u.a. 2016: 8. Ausführlicher hierzu weiter: No Hate Speech Movement Deutschland o.J. und Lembke 2017.

23 Beispielsweise musste ein 34-jähriger Berliner wegen anonymer Hate Speech 4.800€ Strafe zahlen (vgl. No Hate Speech Movement Deutschland o.J.).

an – unter der Voraussetzung, dass das Verfahren Erfolgschancen hat und potentielle Schadensersatzzahlungen zurück in den Prozessfinanzierungsfond fließen (vgl. HateAid gGmbH o.J.).

Neben den drei vorgestellten Strategien Hate Speech an Betreiber*innen zu melden, zu moderieren und anzuzeigen, kann Online-Hate Speech auch an verschiedene organisierte Stellen weitergeleitet werden. Seit Juli 2017 gibt es beispielsweise »respect! die Meldestelle für Hetze im Netz« im Demokratiezentrum Baden-Württemberg, an die Online-Hate Speech weitergeleitet werden kann. Dort wird geprüft, ob die Inhalte strafrechtlich relevant sind und die Täter*innen werden ggf. angezeigt. Außerdem werden Betroffene dabei unterstützt, in Fällen von Beleidigung und übler Nachrede selbst Anzeige zu erstatten (vgl. Demokratiezentrum Baden-Württemberg o.J.). Den Jugendschutz gefährdende Hate Speech kann auch an das Projekt *www.jugendschutz.net* gemeldet werden. Dies ist insbesondere dann von Vorteil, wenn es sich bei der Hate Speech nicht um einen einzelnen Facebook-Kommentar, sondern beispielsweise um einen ganzen Blog, auf dem Hate Speech verbreitet wird, handelt. Das Projekt kooperiert sowohl mit Service-Provider*innen, als auch der Polizei und internationalen Nerzwerken bei der Beseitigung der Jugendschutz gefährdenden Online-Hate Speech (vgl. Glaser o.J.).

Abschließend kann es auch sinnvoll sein, Online-Hate Speech allein zum Zweck des Monitorings, also der systematischen Erfassung und Messung, an Organisationen weiter zu reichen. Hierfür bietet sich unter anderem die Webseite des »No Hate Speech Movement« an.

Selbstermächtigung und Selbstschutz

(Selbst-)Ermächtigung (engl. [self-]empowerment) zielt im Kontext von Sozialer Arbeit darauf ab, Menschen zum selbstbestimmten und selbstbewussten Handeln zu befähigen, indem auf vorhandene Ressourcen aufmerksam gemacht und Handlungsstrategien aufgezeigt werden (vgl. Diamond/Pflaster/Schmid 2017: 72). Im Zusammenhang mit politischer Arbeit ist der Begriff mit den Kämpfen von Schwarzen Menschen und People of Color sowie deren Umgang mit rassistischen Diskriminierungserfahrungen verbunden (vgl. ebd.).[24] In Deutschland wird die Bezeichnung zusätzlich für diverse

24 Dabei wurde der Begriff »Empowerment« Ende der 1950er-Jahre im Kontext der US-amerikanischen Bürgerrechtsbewegung (civil rights movement) genutzt, um die

Praktiken genutzt, mithilfe derer sich verschiedene und auf mehreren Ebenen marginalisierte Personen und Gruppen selbstermächtigen, ihr Selbstbewusstsein stärken und ihre Handlungsfähigkeit erweitern (beispielsweise Fat-Empowerment und Empowerment für Inter*) (vgl. ebd.).

Von Online-Hate Speech und/oder gezielten Troll-Angriffen betroffen zu sein, kann Hilflosigkeit und Ohnmachts-Gefühle hervorrufen. Selbstermächtigung ist ein möglicher Schritt, sich sowohl in der Öffentlichkeit als auch in der eigenen Wahrnehmung von dem »erzwungenen Objektstatus wieder in den Status eines menschlichen, fühlenden Subjekts zu bringen« (Baldauf u.a. 2015: 27). Viele Personen, die online zur Zielscheibe von Hate Speech werden, haben hierfür eine Bandbreite an Umgangs-Strategien entwickelt:

- Sowohl die Offline- als auch Online-Community einbeziehen, um Unterstützung bitten, Hate Speech verbreitende Nutzer*innen zu melden, auf die Hate Speech-Kommentare zu antworten oder um finanzielle Unterstützung bitten, wenn beispielsweise die Wohnsituation oder der Arbeitsplatz durch die digitalen Angriffe gefährdet sind.[25]
- Sich mit anderen Personen, die von Hate Speech betroffen sind, vernetzen und über die eigenen Erfahrungen austauschen. Sollte diese Vernetzung online stattfinden, ist es sinnvoll, dies in einem geschlossenen privaten Forum zu tun, um sich vor weiteren Hate Speech Angriffen zu schützen.
- Sowohl online als auch offline »safe spaces« aufsuchen, in denen die eigene Existenz nicht in Frage gestellt wird.
- Die Gewalt, welche die Person online erfährt, sichtbar machen, indem beispielsweise die Hate Speech (anonymisiert oder nicht anonymisiert) veröffentlicht wird.[26]

Kämpfe der Schwarzen Bevölkerung zu bezeichnen (black empowerment) (vgl. Schwalb/Theunissen 2009: 26).

25 Die Web-Comic-Zeichner*in Sophie Labelle wurde 2017 Zielscheibe eines trans*feindlichen digitalen Angriffs, bei dem eine große Anzahl an Personen in einem abgesprochenen Zeitraum Hate Speech, Beleidigungen und Drohungen auf ihrer Facebookseite posteten, letztlich ihren Account hackten, jahrelange Arbeit löschten und ihre Privatadresse veröffentlichten. Daraufhin musste Labelle sowohl eine Veranstaltung absagen als auch in eine neue Wohnung umziehen (vgl. Beaumont 2017). Nach dem Angriff bat Labelle auf ihrer Facebook-Seite um finanzielle Unterstützung, um umziehen und ihre Arbeit wieder aufnehmen zu können (vgl. Labelle 2017).

26 Auf Instagram nutzen beispielsweise einige Personen, die von Hate Speech betroffen sind, die Story-Funktion (bei der das veröffentlichte Bild nur 24 Stunden zu sehen ist),

- Die Täter*innen zur Schau stellen, um den Fokus weg von den objektifizierten Betroffenen, hin auf die Täter*innen und ihre Taten zu lenken.
- Die eigenen Emotionen sichtbar machen und sich damit auch der Erwartung widersetzen, nur eine humorvolle, abgeklärte Reaktion auf Hate Speech sei valide.
- Blogs und Artikel über die eigene Erfahrung schreiben, oder Artikel von anderen Personen mit ähnlicher Erfahrung teilen.
- Sich in politischen Bewegungen engagieren, die sich für die eigenen Rechte einsetzen.
- Sich bewusst machen, dass Hate Speech nichts mit der eigenen Person zu tun hat, sondern vielmehr eine Projektion gesellschaftlicher Verhältnisse und Problematiken darstellt.
- Auch Selfies (Selbstportraits) können ermächtigend wirken und sogar widerständig sein, wenn dadurch Menschen sichtbar werden, denen die Gesellschaft ein Existenzrecht abspricht (vgl. Yaghoobifarah 2014).

Neben der Selbstermächtigung ist Selbstschutz eine wichtige und notwendige Strategie für Individuen, die von Hate Speech und digitaler Gewalt betroffen sind. Hierzu gehört:

- Die eigenen Accounts sichern und Vorkehrungen gegen Doxing treffen.[27]
- Täter*innen in den sozialen Netzwerken blocken, so dass diese keine Kommentare oder Privatnachrichten schreiben können.
- Die Kommentarfunktion zeitweilig ausstellen oder – wenn möglich – Profile auf »privat« stellen.[28]
- Sich Hilfe bei Freund*innen, Familie, Beratungsstellen oder Therapeut*innen holen.[29]

---

um die Gewalt, die sie erfahren per Screenshot für andere sichtbar zu machen, zu kommentieren und zu verarbeiten.

27 Informationen zum Daten schützen gibt es hier: https://privacysalon.lu/erste-hilfe/und in englischer Sprache: https://crashoverridenetwork.com/accountsecurity.html [Zugriff: 5.2.2020].

28 Beispielsweise schließen einige Online-Nachrichtenportale ihre Kommentarspalten nachts grundsätzlich.

29 Hierfür hat das »Crash Override Netzwerk« einen Guide entwickelt, wie Betroffene mit Angehörigen und auch mit der Polizei über digitale Gewalt sprechen können (in englischer Sprache): https://crashoverridenetwork.com/familyandpolice.html [Zugriff: 5.2.2020].

- Die Taten mit Screenshots dokumentieren.
- Ggf. Anzeige erstatten.
- Informationen über die Täter*innen sammeln, um die Gefahr, die von ihnen ausgeht, besser einschätzen zu können.
- Auseinandersetzung und Recherche zu Strukturen hinter organisierten Hatestorms.

Wichtig sowohl für Selbstermächtigung als auch Selbstschutz ist, die Hate-Speech-Angriffe und deren individuelle Auswirkungen ernst zu nehmen und nicht herunterzuspielen. Dies gilt sowohl für Betroffene selbst als auch für Freund*innen, beratende Personen, Eltern, Sozialarbeitende und Therapeut*innen (vgl. Quinn 2015: Minute 1:52-2:39).[30] Betroffenen lediglich zu raten, sich (wenn auch nur zeitweilig) aus dem Internet zurück zu ziehen, ist weder eine kurzfristige noch eine langfristige Lösung und kann ggf. sogar negative Konsequenzen für die Betroffenen haben (vgl. ebd.).

Literatur

Alice Salomon Hochschule Berlin (Hg.) (o.J.): »Pressespiegel über die Debatte der Hochschulfassade«. https://ash-berlin.eu/hochschule/organisation/referat-hochschulkommunikation/pressespiegel-fassadendebatte/ [Zugriff: 1.5.2020].

Alshater, Samira (2018): »Die Vulgäre Analyse: Plumpe Provokation und Hass auf YouTube«. https://belltower.news/artikel/die-vulgaere-analyse-plumpe-provokation-und-hass-auf-youtube-1319 [Zugriff: 31.12.2019].

Baldauf, Johannes/Banaszczuk, Yasmina/Koreng, Ansgar/Schramm, Julia/Stefanowitsch, Anatol (2015): »›Geh sterben!‹ Umgang mit Hate Speech und Kommentaren im Internet«. https://amadeu-antonio-stiftung.de/w/files/pdfs/hatespeech.pdf [Zugriff: 31.12.2019].

Beaumont, Hilary (2017): »This Canadian cartoonist is just the latest target of anti-transgender trolls«. https://news.vice.com/en_ca/article/j5d9pk/canadian-cartoonist-is-just-the-latest-target-of-anti-transgender-trolls [Zugriff: 31.12.2019].

30 Die US-amerikanische Programmiererin Ashe Dryden hat einen Artikel geschrieben, wie Angehörige sie im Falle von Troll-Angriffen unterstützen können: https://ashedryden.com/trolling-threats-and-abuse-how-you-can-help-me [Zugriff: 25.5.2020].

Bündnis #ausnahmslos (Hg.) (2016): »Gegen sexualisierte Gewalt und Rassismus. Immer. Überall. #ausnahmslos«. https://ausnahmslos.org/post/136955076055/gegen-sexualisierte-gewalt-und-rassismus-immer [Zugriff: 31.12.2019].

Burns, Katelyn (2017): »Die Spiele-Entwicklerin Zoe Quinn über Gamergate und Hass im Netz«. https://vice.com/de/article/8x8nkv/fuer-zoe-quinn-ist-gamergate-noch-nicht-vorbei-und-der-hass-im-netz-nimmt-zu [Zugriff: 31.12.19].

Compact (Hg.) (2017): »Wegen Zensur: Compact ab sofort auch auf steemit und D.tube«. https://compact-online.de/wegen-zensur-compact-ab-sofort-auch-auf-steemit-und-d-tube/ [Zugriff: 30.12.2019].

Council of Europe (Hg.) (2019): »What is the No Hate Speech Movement?«. https://coe.int/en/web/no-hate-campaign [Zugriff: 31.12.2019].

Demokratiezentrum Baden-Württemberg (Hg.) (o.J.): »respect! – Die Meldestelle für Hetze im Netz«. https://demokratiezentrum-bw.de/demokratiezentrum/vorfall-melden/#respect [Zugriff: 31.12.2019].

Diamond, Darla/Pflaster, Petra/Schmid, Lea (Hg.) (2017): Lookismus. Normierte Körper. Diskriminierende Mechanismen. (Self-)Empowerment, Münster: UNRAST-Verlag.

Dinar, Christina/Mair, Theresa/Rafael, Simone/Rathje, Jan/Schramm, Julia (2016): »Hetze gegen Flüchtlinge in sozialen Medien. Handlungsempfehlungen«. https://amadeu-antonio-stiftung.de/w/files/pdfs/hetze-gegen-fluechtlinge.pdf [Zugriff: 31.12.2019].

Facebook (Hg.) (2019): »Zu unseren Richtlinien«. https://facebook.com/help/1735443093393986?helpref=hc_global_nav [Zugriff: 31.12.2019].

Glaser, Stefan (o.J.): »Was jugendschutz.net tut«. https://jugendschutz.net/was-jugendschutznet-tut/ [Zugriff: 1.5.2020].

Gümüşay, Kübra (2017): »Organised love | Kübra Gümüşay | TEDxBerlin-Salon«, in: TEDx Talks. https://youtube.com/watch?v=ZXgp6E53TIE [Zugriff: 31.12.2019].

Hartmann, Ans (2017): »Fachberatungsstellen und die Digitalisierung geschlechtsspezifischer Gewalt. Ergebnisse einer Umfrage unter Frauenberatungsstellen und Frauennotrufen im bff«. https://frauen-gegen-gewalt.de/de/aktuelle-studien-und-veroeffentlichungen.html?file=files/userdata/downloads/studien/bff_Digitalisierung_geschlechtsspezifischer_Gewalt_Expertise_hartmann.pdf [Zugriff: 1.5.2020].

HateAid gGmbH (o.J.): »Sie haben Rechte«. https://hateaid.org/prozesskostenfinanzierung/ [Zugriff: 31.12.2019].

Kramper, Gernot (2016): »#ausnahmslos gegen #falschesgrau. Porno-Piraten kapern den Feminismus-Hashtag #ausnahmslos«. https://stern.de/digital/online/hashtag--ausnahmslos---porno-piraten-kapern-feminismus-hashtag-6651890.html [Zugriff: 31.12.2019].

Labelle, Sophie (2017): Ohne Titel. [Facebook] https://facebook.com/sophievlabelle/posts/1884795725128609 [Zugriff: 31.12.2019].

Lembke, Ulrike (2017): »Kollektive Rechtsmobilisierung gegen digitale Gewalt«. https://gwi-boell.de/de/2018/01/09/kollektive-rechtsmobilisierung-gegen-digitale-gewalt [Zugriff: 30.12.2019].

Meisner, Matthias (2015): »Blog ›Perlen aus Freital‹. Morddrohung gegen Flüchtlingsaktivisten«. https://tagesspiegel.de/politik/blog-perlen-aus-freital-morddrohung-gegen-fluechtlingsaktivisten/12048210.html [Zugriff: 31.12.2019].

Neue Deutsche Medienmacher e.V. (o.J.): »Neue deutsche Medienmacher*innen gegen Hassrede im Netz«. https://neuemedienmacher.de/projekte/no-hate-speech-movement/ [Zugriff: 31.12.2019].

No Hate Speech Movement Deutschland (Hg.) (o.J.): »Wissen. Welche Gesetze gibt es gegen Hate Speech?«. https://no-hate-speech.de/de/wissen/ [Zugriff: 31.12.2019].

o.A. (2015): »Hetz-Kommentar auf Facebook. Porsche kündigt Lehrling wegen Fremdenhass«. https://spiegel.de/panorama/gesellschaft/oesterreich-porsche-entlaesst-lehrling-wegen-hass-kommentar-a-1045306.html [Zugriff: 5.12.2019].

Quinn, Zoë (2015): »Anita Sakeesian UN Speech«. https://youtube.com/watch?v=V3m-bcaCVbM [Zugriff: 30.12.2019].

Schillat, Florian/Wüstenberg, Daniel (2018): »NetzDG im Selbstversuch. Wir haben uns bei Facebook und Twitter beschimpft: Was gesperrt wurde – und was nicht«. https://stern.de/digital/online/twitter-und-facebook--wann-greift-das-netzdg--wann-nicht--ein-test-7815606.html [Zugriff: 26.12.2019].

Schwalb, Helmut/Theunissen, Georg (2009): »Einführung – Von der Integration zur Inklusion im Sinne von Empowerment«, in: Schwalb, Helmut/Theunissen, Georg (Hg.), Inklusion, Partizipation und Empowerment in der Behindertenarbeit. Best-Practice-Beispiele: Wohnen – Leben – Arbeit – Freizeit, Stuttgart: W. Kohlhammer Verlag, S. 11-36.

Sponholz, Liriam (2018): Hate Speech in den Massenmedien. Theoretische Grundlagen und empirische Umsetzung, Wiesbaden: Springer VS.

Stevenson, Alison (2016): »This Woman Turned Her Collection of Unsolicited Dick Pics into an Art Show«. https://vice.com/en_ca/article/ppxjem/this-woman-turned-her-collection-of-unsolicited-dick-pics-into-an-art-show [Zugriff: 10.12.2019].

Twitter (Hg.) (2019): »Unsere Regeln«. https://about.twitter.com/de/safety/enforcing-our-rules.html [Zugriff: 27.12.2019].

Völter, Bettina (2017): »Kategorienfehler im System. Ein (weiterer) Beitrag zur Deeskalation und Entpolarisierung der Fassadendebatte«. https://ash-berlin.eu/fileadmin/Daten/Gemeinschaftsordner/Downloads_Pressestelle/Kategorienfehler_im_System_Bettina_Voelter.pdf [Zugriff: 1.12.2019].

Wingfield, Nick (2015): »Intel Allocates $300 Million for Workplace Diversity«. https://nytimes.com/2015/01/07/technology/intel-budgets-300-million-for-diversity.html [Zugriff: 4.12.2019].

Würdemann, Ulrich (2013): »Aktivismus als Form politischen Handelns«. https://2mecs.de/wp/2013/08/aktivismus/ [Zugriff: 31.12.2019].

Yaghoobifarah, Hengameh (2014): »Selfie-Empowerment«. https://queervanity.com/2014/09/25/selfie-empowerment-2/ [Zugriff: 1.12.2019].

YouTube (Hg.) (2019): »Richtlinien und Sicherheit«. https://youtube.com/intl/de/yt/about/policies/#community-guidelines [Zugriff: 27.12.2019].

ZDK Gesellschaft Demokratische Kultur gGmbH (Hg.) (o.J.): »Hass hilft. Rechts gegen rechts. Die unfreiwillige online Spendenaktion«. https://hasshilft.de/ [Zugriff: 31.12.2019].

Digitale Erste Hilfe:
Prävention und Intervention

Digitale Erste Hilfe und Sicherheitsprinzipien für Berater*innen bei digitaler Gewalt

Jenny-Kerstin Bauer und Helga Hansen

Die Beratung von Frauen, die von digitaler Gewalt betroffen oder bedroht sind, bringt einige Herausforderungen mit sich, denn digitale Angriffe gegen Frauen sind vielfältig: Manche sind technisch ausgefeilt, andere sehen nur so aus. Zudem ist das Internet ein schnelllebiges Medium, welches Täter*innen immer neue Möglichkeiten bietet digitale Gewalt auszuüben. In diesem Artikel finden Berater*innen zunächst eine kurze Checkliste mit drei Punkten, um schnell digitale Erste Hilfe leisten zu können. Anschließend erklären wir grundlegende Sicherheitsprinzipien für den Umgang mit digitalen Geräten und der Internetnutzung. Die Sicherheitsprinzipien sind aus der psychosozialen Beratungsarbeit mit Frauen, die von digitaler Gewalt betroffen sind, entstanden und mit Wissen aus der Informations- und Kommunikationstechnologie weiterentwickelt worden.

Um auf dem neuesten Stand zu bleiben ist es sinnvoll, sich regelmäßig z.B. bei Technik-Magazinen zu informieren. Leider ist deren Schwerpunkt oft die Absicherung gegen gewiefte Hacker*innen oder staatliche Datensammlung. Bei Angriffen aus dem sozialen Umfeld können völlig andere Maßnahmen nötig sein. In der Beratung müssen mit den betroffenen Frauen Lösungen gefunden werden, die in der jeweiligen Situation tatsächlich umsetzbar sind. Um das Thema digitale Gewalt im sozialen Nahraum vermehrt in die Technik-Magazine zu bringen ist es sinnvoll, die Probleme und Strategien in Leser*innenbriefen an die Technik-Journalist*innen zurückzugeben. Spezielle Informationen zur Sicherheit für Betroffene von digitaler Gewalt finden Sie auch auf der Seite des bff: Bundesverband Frauenberatungsstellen und Frauennotrufe *www.aktiv-gegen-digitale-gewalt.de* und auf dem Infoportal für sichere Handynutzung *www.mobilsicher.de*.

Checkliste: Erste-Hilfe

Bestandsaufnahme machen

Um effektiv Erste Hilfe zu leisten, muss zunächst geklärt werden, ob die gewaltausübende Person oder jemand anderes Zugriff auf die persönlichen elektronischen Geräte wie das Smartphone, Fitnessarmband, den Router oder Rechner hatte. Wenn ja, sollten diese Geräte als erstes auf Spyware und Freigaben geprüft werden. Fitnessarmbänder sollten dann nicht mehr getragen werden. Auch die elektronischen Geräte und »smarte Spielzeuge« der Kinder (wie zum Beispiel sprachgesteuerte Teddybären und alles, was mit einer App verbunden ist) sollten gesichtet und überprüft werden.

Wenn die Betroffene mit dem Gewalttäter zusammengewohnt hat oder er smarte Elektronikgeräte im Haushalt installiert hat, müssen außerdem SmartHome-Geräte wie etwa smarte Türöffner, Jalousien oder Heizungssysteme überprüft und möglichst der Internet-Router zurückgesetzt werden.

Ein erhöhtes Sicherheitsrisiko für die Betroffene besteht, wenn der Gewalttäter über Wissen aus dem Bereich der Informations- und Kommunikationstechnologien verfügt. Dieses sollte in der Beratung gezielt abgefragt werden, relevant sind hierbei Berufstätigkeit oder auch Hobbys und Interessen.

Sicherheitsbasis schaffen

Um sich einen Überblick zu verschaffen, ist es notwendig, systematisch alle vorhandenen Online-Konten (E-Mail-Adressen, Social Media Accounts, Online-Dienste oder Online-Dating-Accounts) aufzulisten und zu vermerken, welche E-Mail-Adressen und Handynummern die betroffene Frau bzw. ihre Kinder dafür verwenden. Als erstes ist es wichtig, bei allen alten E-Mail-Adressen die Passwörter zu ändern. Deutlich sicherer ist hierbei die sogenannte Zwei-Faktor-Authentifizierung – also ein zweistufiges Anmeldeverfahren.[1]

Zentral für weitere Schritte ist ein eigenes E-Mail-Postfach, auf das niemand sonst Zugriff hat, da praktisch jeder Online-Dienst zur weiteren Kommunikation die Angabe einer E-Mail-Adresse verlangt. Eventuell muss daher eine neue E-Mail-Adresse eingerichtet werden und diese als Kontakt in den

1 Siehe hierzu die Ausführungen zu »Sichere Passwörter und Codes« im weiteren Verlauf dieses Artikels. Siehe außerdem Beitrag: Digitale Sicherheit für frauenspezifische Einrichtungen.

vorhandenen Online-Konten und Diensten geändert werden. Anschließend sollten alle weiteren Passwörter geändert werden: Vom heimischen WLAN über den Internet-Router bis hin zu Social Media Accounts und Diensten wie Netflix oder Einkaufsdiensten (wie z.B. Amazon). Letzteres ist wichtig, damit der Täter der betroffenen Person nicht noch ökonomischen Schaden zufügen kann. Damit die Betroffene online handlungsfähig bleibt, ist es wichtig sie mit dem privaten Modus von Internet-Browsern vertraut zu machen.[2] Dies ermöglicht ihnen den eigenen, aber auch fremde Rechner zu nutzen, ohne Spuren zu hinterlassen. Wenn nicht ausgeschlossen werden kann, dass der Gewalttäter heimlich mitliest, bzw. smarte Geräte überwacht, sollte auf das Speichern von sensiblen Daten auf den Geräten verzichtet werden.[3]

Beweissicherung

Bei all diesen Maßnahmen ist es wichtig, die von digitaler Gewalt Betroffenen dabei zu unterstützen, die Beweise genau zu dokumentieren.[4] Wie bei analoger Gewalt ist es durchaus vorstellbar, dass es für die Betroffenen zunächst ausgeschlossen erscheint gegen die Gewalt juristisch vorzugehen. Auch in diesem Fall ist es wichtig, die Beweise für alle Fälle zu sichern.

(Präventive) Sicherheitsprinzipien bei digitaler Gewalt

Sichere Passwörter

Passwörter sind die wichtigste Sicherheitshürde. Sie verhindern, dass eine gewaltausübende Person die Benutzer*innenkonten in sozialen Netzwerken oder E-Mail-Konten einer betroffenen Frau einsehen kann. Der erste Schritt ist, für jeden passwort-geschützten Dienst ein anderes Passwort zu verwenden. Passwörter sind umso sicherer, je länger sie sind. Viele Online-Dienste prüfen das Passwort inzwischen schon beim Erstellen auf Länge und weitere Kriterien und geben eine eigene Sicherheitsabschätzung ab.

---

2 Siehe hierzu die Ausführungen zu »Surfen mit privater Sitzung« im weiteren Verlauf dieses Artikels.

3 Siehe hierzu die Ausführungen zu »Speicherung sensibler Daten« im weiteren Verlauf dieses Artikels.

4 Siehe hierzu die Ausführungen zu »Beweissicherung und Kontaktaufnahme Seitenbetreiber*innen« im weiteren Verlauf dieses Artikels.

Ein sicheres Passwort hat mindestens zwölf Zeichen. Es enthält Groß- und Kleinbuchstaben, Ziffern und geläufige Sonderzeichen wie »!« und »?« (vgl. klicksafe/Institut für Digitale Ethik (IDE) der Hochschule der Medien Stuttgart 2018: o.S.). Wichtig ist, dass es sich nicht aus dem eigenen Namen, dem einer nahestehenden Person, einem Geburtsdatum oder einer Telefonnummer ableiten lässt. Eine Möglichkeit ist, verschiedene Worte und Zahlen zu kombinieren wie: *Kabel-Wetterballon!2020*. Alternativ lässt sich auch ein Satz als Ausgangsbasis nehmen: *H*eute *w*erde *i*ch *m*it *v*iel *F*reude *E*is *u*nd *S*chokolade *e*ssen. Aus den Anfangsbuchstaben der Wörter ergibt sich mit der Kombination von einem Sonderzeichen «!« und einer Jahreszahl: *HwimvFEuSe!2023*. Diese Passwörter können in abgewandelter Form für jedes Konto angepasst werden, wobei Sie möglichst mehrere Teile verändern. Beispielsweise für Facebook gilt: *HwimvFEuSe!2023* und für das E-Mail-Konto gilt: *M*orgen *w*erde *i*ch *m*it *v*ielen *n*etten *M*enschen *P*izza *u*nd *P*asta *e*ssen = *MwimvnMPuPe?2022* oder *Kabel-Flugzeug?2020*. Wird kein Passwortmanager verwendet, ist das sicherste Passwort eines, das sich die Person merken kann, ohne es sich aufschreiben zu müssen. Es nützt nichts, wenn es regelmäßig zurückgesetzt werden muss oder die Person sich selbst von ihren Accounts aussperrt.

Bei Einbrüchen und Hacks von Webseiten und sozialen Netzwerken werden gerne Passwörter entwendet, die von fahrlässigen Betreiber*innen offen abgespeichert wurden – diese können auch in die Hände der gewaltausübenden Person geraten. Einige Dienste bieten an, diese Datenlecks auf eigene Informationen zu untersuchen, wie etwa der »Identity Leak Checker« des Potsdamer Hasso-Plattner-Instituts. Auf *https://sec.hpi.de/ilc/search?lang=de* können Sie anhand ihrer E-Mail-Adresse abfragen, welche Zugangs- oder Identitätsdaten und Passwörter im Internet offengelegt werden. Zu überprüfen sind auch alte E-Mail-Adressen, die die Betroffene vielleicht seit Jahren nicht mehr genutzt hat.

Wurde ein Passwort bei mehreren Accounts genutzt, ist es in einem Leck veröffentlicht worden oder hat die gewaltausübende Person Kenntnis von Passwörtern, sollten diese unbedingt geändert werden. Ohne konkreten Anlass ist es ansonsten selten sinnvoll, Passwörter zu ändern oder dies sogar regelmäßig zu tun. Die Anzahl der zu merkenden Passwörter wird schnell so groß, dass es schwierig ist, den Überblick zu behalten und die Gefahr steigt, sich schließlich aus einem eigenen Account komplett auszusperren. Stattdessen macht der Einsatz eines Passwortmanagers Sinn. Diese Programme, wie etwa »1Password«, speichern die Zugangsdaten zu verschiedenen Konten und schlagen sichere Passwörter vor. Um sie zu nutzen, muss man sich nur

das Master-Passwort merken und ggf. einen zweiten Faktor nutzen. Ein Passwortmanager ermöglicht das Merken der ansonsten schwer zu merkenden langen, aber sicheren Passwörter. Verschafft die gewaltausübende Person sich allerdings Zugriff auf das Smartphone und das Passwort zum Passwortmanager, sind alle dort gespeicherten Zugangsdaten für sie einsehbar. Eine Sicherheitsmaßnahme ist daher, nur eher unwichtige Passwörter dort abzulegen und das E-Mail-Passwort weiter per Hand einzugeben.

Sichere Codes

Ein Zugriffs- oder Passcode schützt zum Beispiel ein Smartphone in Form eines Zifferncodes, eines Musters, durch Gesichtserkennung oder einen Fingerabdruck vor fremden Zugriffen auf das Telefon. Eine starke Bildschirmsperre besteht aus mindestens sechs, besser aus acht Ziffern. Der Code sollte nicht geläufige Ziffernfolgen wie das Geburtsdatum des Kindes oder die eigene Postleitzahl enthalten. Muster als Zugriffscodes sind relativ leicht zu erraten, vor allem, wenn die gewaltausübende Person häufig die Gelegenheit hat, die Eingabe zu beobachten.

Die praktische Entsperrung mit dem Fingerabdruck ebenso wie die Gesichtserkennung (Face ID) ist umstritten. Fingerabdrücke und das Gesicht sind grundsätzlich öffentlich sichtbar und damit eher wie Benutzer*innennamen zu betrachten. Werden sie verlangt, ist es allerdings schwerer, das Smartphone heimlich zu entsperren. Durch die Eingabe des Zugriffscodes lassen sie sich schließlich aber meist umgehen.

Passwort-Wiederherstellung

Eine häufige Taktik zum Kapern eines Accounts ist der Versuch, das Passwort zurücksetzen zu lassen. Dabei wird meist ein neues Passwort von den Seitenbetreiber*innen in einer E-Mail verschickt, weshalb es so wichtig ist, über ein E-Mail-Konto ohne Zugriff der gewaltausübenden Person zu verfügen. Manchmal gibt es auch Sicherheitsfragen nach dem Namen des ersten Haustiers oder dem Namen des Kindes. Diese sind für Personen aus dem Umfeld leicht zu erraten. Daher sollte bei den Antworten gelogen werden – aber nachvollziehbar, denn man muss sich die Antwort schließlich selbst merken können. Sinnvoll ist ein System, wenn Facebook nach dem Geburtsort fragt, wie etwa F-Hannover und A-Hannover wenn die gleiche Frage bei Amazon auftaucht.

Zwei-Faktor-Authentifizierung

Ist ein Benutzer*innenkonto durch eine Zwei-Faktor-Authentifizierung (2FA) oder auch zweistufiges Anmelden geschützt, erfolgt das Einloggen in zwei Schritten. Zuerst wird, wie gewohnt, das Passwort eingegeben und dann eine zweite Methode bzw. ein zweiter Faktor genutzt. Beispielsweise wird ein zeitlich begrenzt gültiger Sicherheitscode per E-Mail oder SMS verschickt, der nach dem Passwort eingegeben werden muss. Viele Online-Dienste (Soziale Netzwerke, Messengerdienste oder E-Mail-Anbieter*innen) ermöglichen mittlerweile diese Funktion. Die Aktivierung erfolgt meist unter Einstellungen im Menü zu Sicherheit und Privatsphäre. Durch die zwei Schritte ist das Benutzer*innenkonto theoretisch sehr gut vor dem Zugriff der gewaltausübenden Person geschützt, weil es nicht mehr ausreicht nur das Passwort zu kennen. Praktisch gibt es in den unterschiedlichen Methoden jeweils Schwächen, sodass der Einsatz abgewogen werden muss. In Zukunft sollte sich hier noch einiges verbessern.

Am sichersten sind unabhängige Geräte, wie etwa ein TAN-Generator beim Online-Banking. Es gibt zum Beispiel die »YubiKeys« – kleine Schlüssel, die auf den ersten Blick an USB-Sticks erinnern. Sie können am Schlüsselbund getragen und über USB mit dem Rechner oder Smartphone verbunden werden, um sich beim Anmelden bei verschiedenen Diensten zu identifizieren. Trotz hohem Sicherheitsstandard sind solche Hardware-Schlüssel bisher nur begrenzt bei Online-Diensten nutzbar – Apple und Google haben in den letzten Monaten beständig daran gearbeitet Hardware-Schlüssel zu unterstützen. Mit IOS 14 soll das z.B. für iCloud kommen und seit kurzem funktionieren YubiKeys auch mit Google-Apps auf iPhones.

Eine Alternative sind spezielle Apps wie »Google Authenticator« oder »Authy«. In dieser App werden die gewünschten Dienste registriert. Bei jeder Anmeldung wird von der App ein Code als zweiter Faktor generiert. Wie die Hardware-Schlüssel werden die Apps allerdings auch noch nicht von allen Diensten unterstützt. Ein weiterer Nachteil von beiden Methoden: Geht der Hardware-Schlüssel oder das Smartphone mit der App verloren, ist der Zugang zu den Diensten verloren. Inzwischen wird eine Kombination aus zwei aktivierten 2FA-Methoden empfohlen.

Schließlich gibt es die Möglichkeit einen Einmal-Code per SMS oder E-Mail zu bekommen. Das ist derzeit die am weitesten verbreitete 2FA-Methode, aber auch die unsicherste. Mit einem Anruf bei der Mobilfunkfirma und persönlichen Informationen kann sich die gewaltausübende

Person neue SIM-Karten für bekannte Telefonnummern beschaffen. SMS und Anrufe landen danach auf der neuen Karte – wer ansonsten nur über Messenger telefoniert und schreibt, merkt dies unter Umständen nicht einmal. Bis Anfang 2020 konnten Nutzer*innen bei Facebook über die für die Zwei-Faktor-Authentifizierung angegebene Telefonnummer gefunden werden, auch wenn sie die Nummer von ihrem Profil verbergen ließen.

Smartphone-Einstellungen absichern

Über GPS und die Standortübermittlung können die Bewegungen anderer Personen überwacht und kontrolliert werden. Auch Mikrofone und Kameras können über entsprechende Apps zum Spionieren genutzt werden. Gerade Android-Smartphones mit älteren Betriebssystemen geben Apps viele Freiheiten. Als erstes sollten daher in der Beratung alle installierten Apps einzeln durchgegangen werden.[5] Wichtig ist hierbei zu klären, ob die betroffene Person alle Apps selbst heruntergeladen hat bzw. ob jede App und jedes Programm einen Nutzen für sie hat. Unbekannte oder nicht mehr genutzte Apps sollten gelöscht werden. Werden sie später doch noch einmal gebraucht, können sie meist einfach wieder installiert werden. Auch ist es wichtig, die Freigaben für Ortungsdienste, Mikrofon und Kamera in den Einstellungen zu überprüfen. Mobilitäts-Apps wie von der Bahn finden mit dem aktuellen Standort schneller den nächsten Bus, ein Spiel wie »Candy Crush« benötigt ihn aber nicht. Daher sollten unnütze Freigaben konsequent abgeschaltet und dauerhafte Standortabfragen gekappt werden, wenn das Programm selbst geschlossen ist. Manch ältere Android-App verweigert anschließend ihre Funktion; im Zweifelsfall ist es sicherer, sich ein alternatives Programm zu suchen. Es ist durchaus möglich, Apps den direkten Zugriff auf alle eigenen Bilder und Videos zu verweigern und diese bei Bedarf trotzdem zu verschicken. In den Bilder-Apps gibt es dafür die Share-Funktion, die ohne Freigaben auskommt und das Bild nur gezielt weitergibt.

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. Wenn betroffene Frauen diese Funktion weiterhin nutzen wollen, um

5 Siehe hierzu die Ausführungen zu »Spionage-Software« im weiteren Verlauf dieses Artikels.

Geräte bei Verlust aus der Ferne sperren zu lassen, gibt es auch eine Alternative ohne Ortung. Nötig ist dafür die IMEI (*I*nternational *M*obile Station *E*quipment *I*dentity) Nummer des Smartphones. Sie wird angezeigt, wenn die Tastenkombination *#06# angerufen wird. Mit dieser Nummer kann das Smartphone bei Verlust durch den Netzbetreiber bzw. die Polizei gesperrt werden.

Neben der Ortungsfunktion ist es wichtig, die Webcams bei Laptops und Computern im Blick zu haben und möglichst abzudecken, damit beispielsweise die gewaltausübende Person diese nicht durch Hacken oder eine Spionage-Software kontrollieren und somit ständig überwachen kann. Dafür eignet sich bereits ein kleines Monitorputztuch mit Kleberückseite oder ein einfaches Post-it. Sollte das Statuslicht der Kamera unerwartet angehen, ist dies ein Hinweis darauf, dass die am Computer arbeitende Person und ihre Umgebung von außen betrachtet und gehört wird.

Spionage-Software

Während einige Apps nur aus Bequemlichkeit Mikrofone und Kameras anschalten und damit das Gegenüber überwachen, ist dies der Hauptzweck von sogenannten Spionage-Softwares, Spy-Apps oder Stalkerware.[6] Die gängigsten Möglichkeiten eine Spionage-Software unerkannt auf einem Smartphone oder einem Computer zu installieren sind:

- Spionage-Software wurde durch eine E-Mail oder einem Nachrichten-Anhang unabsichtlich selbst heruntergeladen, weil die Software beispielsweise als Katzenbild oder wichtiges Dokument getarnt war.
- Anti-Diebstahl-Software (wie z.B. »Cerberus«), die auf den ersten Blick sinnvoll und praktisch wirkt, kann als Spionage-Software missbraucht werden.
- Die gewaltausübende Person hatte einmal direkten physischen Zugriff auf das elektronische Gerät und hat in dieser Zeit Spionage-Software installiert, z.B. kurz nach einem Telefonat und vor der Sperrung des Bildschirms.
- Die gewaltausübende Person hatte Zugang zu Cloud-Diensten der Person, die sie überwachen will und die Spionage-Software funktioniert über diesen Dienst.

6 Siehe Beitrag: Individuelle Strategien im Umgang mit geschlechtsspezifischer digitaler Gewalt.

Ein möglicher Hinweis auf die Existenz von Spionage-Software auf einem Smartphone ergibt sich, wenn Klient*innen berichten, dass der gewaltausübenden Person viele Informationen und Aufenthaltsorte bekannt sind. Auch ein sehr schnell entleerter Akku kann ein Indiz für eine Spionage-Software sein, denn durch das ständige Abfangen und Auslesen der Daten werden die Geräte spürbar langsamer als gewohnt und der Akku ist schneller leer (vgl. Bleich 2018: 76). Hier ist es wichtig in den Benachrichtigungen zu überprüfen, ob das Smartphone den Ortungsdienst erlaubt, wenn kein Programm offen ist.

Für die Installation von Spionage-Apps sind meist spezielle Rechte nötig. Bei Android-Smartphones heißt diese unautorisierte Veränderung »Rooten« und beim iPhone »Jailbreak«. Android-Smartphones lassen sich mit der App »Rootchecker« überprüfen. Ein weiterer Hinweis auf Android-Spionage-Apps sind Einträge in den Sicherheits-Einstellungen zum Standort. Dort sollten nur »Mein Gerät finden« und »Google Pay« zu sehen sein. Weitere Einträge sollten deaktiviert werden. »Jailbreaks« sind derzeit nur auf älteren Versionen des iPhone-Betriebssystems möglich. Verdächtige Apps heißen »Cydia«, »Electra« und »Pangu« und sind etwa auf der Seite *www.zjailbreak.com* zu finden. Manche Apps wie das Spiel »Pokémon Go« verweigern die Arbeit, wenn sie einen Jailbreak erkennen und können so Hinweise geben. Neuere iPhones sind vor allem über die iCloud anfällig. Anti-Viren-Programme waren lange nutzlos in diesem Zusammenhang. Seit einiger Zeit nehmen die Hersteller*innen das Problem aber ernster: »Kaspersky« und »TrendMicro« erkennen inzwischen geläufige Spionage-Programme (vgl. Coalition Against Stalkerware 2019: o.S.; Gierow 2019: o.S.).

Das Zurücksetzen bzw. das Neuaufsetzen von Geräten kann eine wirkungsvolle Strategie sein, um sich der Überwachungssoftware zu entledigen. Trotzdem wird nicht jede Software damit nachhaltig gelöscht. Im Zweifelsfall sollten IT-Spezialist*innen hinzugezogen bzw. die Geräte ausgetauscht und die Passwörter geändert werden.

Speicherung sensibler Daten

Falls sich eine gewaltausübende Person Zugriff zu einem Smartphone der (Ex-)Partner*in verschafft hat, kann sie dort alle abgespeicherten, sensiblen Daten einsehen. Vom Abfotografieren von Dokumenten (wie etwa Krankenkassenkarten, Briefe mit Terminen bei Behörden oder Gerichten) oder der Pässe der Kinder ist daher abzuraten. In der Beratung sollte daher gemein-

sam besprochen werden, wo Klient*innen ihre sensiblen Daten speichern und wie sie eine Sicherheitskopie ihrer Daten und möglicher Beweise erstellen können. Optionen dafür sind deutsche Cloud-Dienste (wie »MagentaCloud«), die den Anforderungen der europäischen Datenschutz-Grundverordnung (DSGVO) entsprechen, externe Festplatten oder USB-Speichersticks. Letztere sollten nach Möglichkeit neu gekauft werden, da die gewaltausübende Person über vorhandene Sticks Spionage-Software auf einen Rechner schleusen kann. Smartphone-Backups sollten über Kabel auf dem Rechner erstellt werden.

Um Smartphones und Tablets nutzen zu können, sind eine Apple-ID (iPhone) oder ein Google-Konto (Android) nötig, die mit dem jeweiligen Gerät verknüpft werden. Darüber drängen die beiden Anbieter ihren Nutzer*innen auch gleich die eigenen Cloud-Services auf, von denen allerdings abzuraten ist. Ist der gewaltausübenden Person das Passwort bekannt, können sensible Daten von anderen Rechnern oder Smartphones eingesehen werden. Gerade bei iPhones ist die iCloud eine Schwachstelle, über die etwa Spionage-Software installiert werden kann, obwohl Apple ansonsten oft die besseren Sicherheitseinstellungen vorgibt.

Hat die gewaltausübende Person wichtige Dateien gelöscht, können diese gegebenenfalls wiederhergestellt werden; hier lohnt ein Blick in den Papierkorb des Geräts. Solange der nicht geleert wurde, können die Daten einfach zurückgelegt werden. Sind Dateien dort nicht mehr zu finden, sollten am Rechner keine weiteren Aktionen durchgeführt werden, weil die Speicherbereiche von Windows-Rechnern oft nur zum Überschreiben freigegeben, aber nicht physisch gelöscht werden. Solange die Daten nicht überschrieben wurden, können sie mit kostenlosen Tools wie »TestDisc« und »Disk Drill« wiederhergestellt werden, die es im Internet gibt.

Router, Bluetooth und WLAN als Sicherheitsrisiko

Grundsätzlich gilt derzeit: Kabel sind sicherer als drahtlose Verbindungen. Wenn möglich sollten daher der Internetzugang und Geräte wie Tastaturen oder Lautsprecher über Kabel angeschlossen werden. Die nächstbesten Alternativen sind verschlüsselte Verbindungen, die die Eingabe eines Passworts oder Pins erfordern. Egal ob zu Hause Kabel oder WLAN genutzt wird – der Internetanschluss sollte gut abgesichert werden. Bereitgestellt wird er heute meist von einem Router, alle Einstellungen können nur hierüber verändert werden. Dazu muss das Smartphone oder ein Rechner über das WLAN oder

ein Kabel mit dem Router verbunden sein. Anschließend wird die Router-Adresse im Browser aufgerufen. Diese besteht meist aus einer Zeichenfolge wie 192.168.1.1 oder 192.168.0.1 oder bei einer »Fritzbox« über fritz.box – die passende Adresse steht meist auf der Unterseite des Routers oder im Handbuch. Mit dem Hersteller*innennamen und der Typenbezeichnung lässt sie sich auch im Internet ermitteln. Anschließend verlangt der Router eigene Zugangsdaten (einen Benutzer*innennamen und ein Passwort), die meist ebenfalls auf der Unterseite des Geräts vermerkt sind. Wurden die Daten bereits geändert oder sind nicht auffindbar, lässt sich der Router über den Reset-Knopf zurücksetzen und nutzt dann vorgegebene Zugangsdaten wie den Benutzer*innennamen »admin« und das Passwort »password«. In den Router-Einstellungen müssen diese Standardangaben dann gleich wieder geändert werden. Außerdem kann man in den Einstellungen überprüfen, welche Computer, Smartphones und Smart-Home-Geräte den Internetzugang nutzen.

Für das heimische WLAN sollte der Netzwerkname so gewählt sein, dass kein Rückschluss auf das verwendete Router-Modell möglich ist. Wichtig ist auch die Netzwerkverschlüsselung, um keine Daten offen einsehbar zu verschicken. Dabei sollte das Protokoll WPA2 (oder wenigstens WPA) ausgewählt werden. Schließlich muss ein sicheres Passwort für das WLAN vergeben werden. Offene, nicht-passwortgeschützte WLAN-Netzwerke bieten Möglichkeiten für Fremde und damit auch für gewaltausübende Personen, besuchte Seiten auszuspionieren, wenn sich ein Laptop oder Smartphone mit diesen verbindet. Am einfachsten ist es, die WLAN-Funktion grundsätzlich zu deaktivieren und nur dann einzuschalten, wenn ein bekanntes, sicheres WLAN genutzt wird. Wird dennoch ein offenes WLAN eines seriösen Anbieters genutzt, etwa in einer Bücherei, sollte darauf geachtet werden, keine unbekannte Software herunterzuladen und Anmeldedaten nur dann auf einer Webseite einzugeben, wenn diese verschlüsselt aufgerufen wurde – also https in der Adresse steht. Danach sollte das WLAN aus der Liste bekannter Netzwerke gelöscht werden, um späteres, ungewolltes Verbinden zu verhindern. Das gleiche gilt für den Umgang mit Bluetooth. Auch diese Funktion sollte nur zum Gebrauch eingeschaltet und anschließend wieder deaktiviert werden. In den Bluetooth-Einstellungen lässt sich ebenfalls überprüfen, welche Geräte bereits angeschlossen waren und sich automatisch verbinden würden. Werden neue Geräte angeschlossen (das sogenannte Pairing), sollten diese möglichst die Eingabe eines Pins verlangen. Achtung: »Deaktiviert« ist nicht immer »deaktiviert«. Es reicht nicht aus, im Kontrollmenü der Smartphones die Bluetooth- oder WLAN-Funktion auszuschalten. Das Kontrollmenü

ist ein Schnellzugriff zu den Einstellungen des Smartphones und lässt sich durch Wischen von oben oder unten auf dem Display anzeigen. Um die Funktionen wirklich abzuschalten, muss im Einstellungsmenü des Smartphones »WLAN deaktivieren« und »Einstellungen – Bluetooth deaktivieren« ausgewählt werden. Ansonsten aktivieren sich Bluetooth und WLAN immer wieder von selbst.

Smart-Home-Geräte

Weniger Stromverbrauch, bequeme Steuerung von Elektrogeräten aus der Ferne und stromintensive Arbeiten zu günstigen Zeiten erledigen: Intelligente Haushaltsgeräte versprechen viel Komfort, können in unbefugten Händen aber zum Alptraum werden. Ähnlich wie beim Einsatz von Spionage-Software weiß die Person, die die Geräte installiert hat, genau Bescheid, wer wann zu Hause ist und welche Geräte wie lange nutzt. Außerdem können sie dafür sorgen, dass elektronische Geräte sich merkwürdig verhalten, indem sie scheinbar wie von selbst angehen oder etwa mitten in der Nacht Musik abspielen. Dies kann eine Fehlfunktion sein oder der bewusste Versuch, Personen zu destabilisieren, indem sie beginnen an ihrer Wahrnehmung zweifeln; ein Verhalten das als »Gaslighting« bekannt ist. Daher kann es hilfreich sein nach Vorfällen zu fragen, wenn Klient*innen angeben, an »ihrem Verstand zu zweifeln«. Sie können auch ein Hinweis auf digitale Gewalt durch Smart-Home-Geräte sein. Um diese Fernsteuerung zu unterbinden, ist es am wichtigsten zu wissen, ob und welche Dinge im Haus »smart« sind. Im besten Fall sind sie allen Bewohner*innen eines gemeinsamen Haushalts bekannt. Recht verbreitet sind inzwischen Glühbirnen, Steckdosen, Bewegungsmelder und Lautsprecher wie Amazons »Alexa«, die meist auch über ein Mikrofon verfügen. Glühbirnen können einfach rausgedreht und mit der aufgedruckten Bezeichnung im Internet überprüft werden, ob es sich um eine einfache oder intelligente Birne handelt. Lautsprecher und Bewegungsmelder sind manchmal sehr unauffällig, aber meist in Hör- und Sichtweite aufgestellt – in einer selten genutzten Abstellkammer macht ein Bewegungsmelder schließlich keinen Sinn. Smarte Steckdosen fallen derzeit noch gut auf, weil es sich meist um Zwischenstecker handelt. Dennoch ist es sinnvoll in der Beratung bei Verdacht auf digitale Gewalt nachzufragen, ob eine Steckdose ausgetauscht wurde und alle angeschlossenen Geräte zu überprüfen. Jedes smarte Gerät braucht Strom und das meist mehr, als eine Batterie zur Verfügung stellen könnte. Außerdem brauchen smarte Geräte meist Internetzugang und hin-

terlassen so nachverfolgbare Spuren im Router. Schauen Sie auch, ob es in der Umgebung ein offenes oder neues WLAN gibt, über das die Geräte laufen könnten, so kann sich ein Überblick über die möglichen bestehenden smarten Geräte verschafft werden.

Das einfachste Mittel gegen unerwünschte SmartHome-Geräte ist den Stecker zu ziehen. Sollen sie grundsätzlich weiter betrieben werden, hilft ähnliches Vorgehen wie bei Smartphones und Rechnern: Zurücksetzen auf Werkseinstellungen, sichere Passwörter nutzen, Zwei-Faktor-Authentifizierung einrichten, Tracking-Berechtigungen ausschalten und gegebenenfalls die Hersteller*innen um Hilfe bitten. So sollte etwa das Mikrofon smarter Lautsprecher ausgeschaltet sein, wenn niemand zu Hause ist. Bei tragbarer Elektronik wie Fitnessarmbändern und Smartwatches gelten diese Regeln ebenfalls. Wer Kontrolle über seine SmartHome-Geräte hat, kann diese auch gezielt nutzen und z.B. zufällig Lichter angehen lassen, wenn niemand zu Hause ist, um Anwesenheit vorzutäuschen.

Datenlecks vermeiden

Um zu verhindern, dass Passwörter, Fotos und andere sensible Daten versehentlich verraten werden, gibt es noch weitere Maßnahmen, die umgesetzt werden können. Hierzu gehört das Löschen gemeinsamer Accounts mit der gewaltausübenden Person in den sozialen Netzwerken sowie von Accounts, die nicht mehr genutzt werden. So verschwinden alte Bilder und Passwörter aus dem Internet. Wichtig ist hierbei darauf zu achten, dass die Konten tatsächlich geschlossen und nicht nur deaktiviert werden, sonst können diese schnell wieder mit allen Informationen und Fotos hergestellt werden. Manchmal sind dazu extra Anfragen bei den Betreiber*innen nötig.

Besondere Vorsicht ist geboten, wenn unaufgefordert E-Mails kommen, mit denen Passwörter von Accounts zurückgesetzt werden können. Wenn es sich um eine echte E-Mail des Online-Dienstes handelt und das Passwort zuvor selbst geändert wurde, ist dies ein Hinweis dafür, dass noch jemand anderes eingeloggt war, der gerade erfolgreich ausgesperrt wurde. Möglich ist auch, dass jemand anderes versucht das Passwort zu ändern, um der Klientin den Zugang zu einem Dienst zu versperren. Um dies zu verhindern, ist ein E-Mail-Konto ohne fremden Zugriff essenziell wichtig für Betroffene von digitaler Gewalt. In diesem Fall sollte man sich noch einmal vergewissern, dass das Passwort lang genug und sicher ist und nicht in fremde Hände gelangt ist. Sinnvoll ist auch ein Screenshot der E-Mail zur Beweissicherung.

Mehr technisches Wissen erfordert das sogenannte Phishing, eine Wortkreation aus dem Englischen (dt. Passwort fischen). Dazu werden Lock-E-Mails mit der Aufforderung geschickt einen Link anzuklicken, der auf eine gefälschte Webseite führt. Werden dort Zugangsdaten eingegeben, können diese ausgelesen und ohne Einverständnis weiterverwendet werden. Statt verdächtige Links zu öffnen, ist es ratsam den Mauszeiger auf den Link zu platzieren und einen Augenblick zu warten, dann wird die eigentliche Linkadresse in der Vorschau angezeigt. Oft werden beim Phishing auch Anhänge mitgeschickt, um deren Öffnung gebeten wird. Von verdächtigen E-Mails sollte zur Beweissicherung nur ein Screenshot gemacht werden, um sie anschließend komplett zu löschen. Inzwischen versteckt sich Schadsoftware[7] nicht nur in Dateien, die auf »EXE« enden, sondern auch in Office-Dateien, wobei sich diese nur verraten, weil zur Installation eine Fehlermeldung angezeigt wird, die sich beim Nachprüfen als gefälscht erweist, also keine offizielle Fehlermeldung von Office ist. Aus der Beratungspraxis ist bekannt, dass Gewalttäter vermeintlich wichtig erscheinende E-Mail-Anhänge für Behördentermine bzw. Sorgerechtsangelegenheiten an die (Ex-)Partnerin versenden, um Schadsoftware mitzuschicken. Um E-Mail-Angriffe schneller zu erkennen und abzuwehren, ist es hilfreich, Spam konsequent zu markieren und Spamfilter einzusetzen. Eine weitere Maßnahme ist das Abbestellen von Newslettern.

Sicherheitseinstellungen in sozialen Netzwerken

Facebook[8] ist – laut eigener Angaben – das beliebteste Soziale Netzwerk in Deutschland. Nach viel Kritik aufgrund fragwürdiger Datenschutzpraktiken bietet die Firma heute einige sinnvolle Sicherheits- und Privatsphäre-Einstellungen für seine Nutzer*innen. Unter *https://facebook.com/safety/tools* werden Empfehlungen und Erklärvideos zur Verfügung gestellt, um das eigene Profil sicherer zu gestalten. Es wird auf Möglichkeiten wie sichere Passwörter, Anmeldewarnungen, die angesprochene zweistufige Authentifizierung, abmelden, gehackte Konten, Beiträge posten, Profilgestaltung, Markierung auf Fotos, Markierungsüberprüfung, Chronikü berprüfung, sein

7 Siehe hierzu die Ausführungen zu »Rechner sichern« im weiteren Verlauf dieses Artikels.

8 Das National Network To End Domestic Violence (NNEDV) hat einen umfangreichen Leitfaden für Betroffene von häuslicher und digitaler Gewalt für die Privatsphäre- und Sicherheitseinstellungen auf Facebook veröffentlicht (vgl. NNEDV 2014).

Publikum (»Freunde«) kennen, entfreunden und blockieren von Freund*innen eingegangen. Die Seite bietet aufschlussreiche Informationen für Betroffene digitaler Gewalt und steht in verschiedenen Sprachen zur Verfügung. Grundsätzlich lässt sich festhalten, dass die Privatsphäre- und Sicherheitseinstellungen von Facebook bei einer Erstanmeldung sehr offen gehalten sind. Immer wenn neue Nutzungsbedingungen von sozialen Netzwerken wie Facebook erscheinen oder Updates erfolgen, sollten nochmals alle Sicherheitseinstellungen überprüft werden. Es kann sein, dass neue Funktionen hinzugekommen sind, die eine gewaltbetroffene Frau gefährden könnten, oder dass vorgenommene Einstellungen rückgängig gemacht worden sind.

Unter »Einstellungen« auf Facebook und »Sicherheit und Login« lassen sich wichtige Funktionen für Betroffene von digitaler Gewalt konfigurieren:

- »Wähle Freunde, die du kontaktieren kannst, wenn du dich ausgesperrt hast« – Diese Funktion soll es Facebook-Nutzer*innen leichter machen sich einzuloggen, wenn sie ihr Passwort vergessen haben, indem die eingetragenen »Freunde« die Anfrage über einen Code verifizieren. Hier ist es wichtig zu überprüfen, ob eine gewaltausübende Person eingetragen ist. Wenn dies der Fall ist, sollte die Person sofort aus der Funktion gelöscht werden. Danach sollten die Passwörter so schnell wie möglich geändert werden und die Zwei-Faktor-Authentifizierung aktiviert werden. Die Passwörter können unter »Passwörter ändern« und »Verwende die Zweistufige Authentifizierung« geändert werden.
- »Wo bist du gerade angemeldet?« – Unter dieser Funktion lässt sich einsehen, wo und mit welchem Gerät das Facebook-Profil angemeldet ist. So kann eingesehen werden, ob sich eine unbefugte Person Zugang zu dem Profil verschafft hat. Manchmal handelt es sich auch um ältere Anmeldungen, bei denen man sich selbst nicht ausgeloggt hat. Über die drei Punkte neben jeder Angabe und »Das bist nicht Du?« gibt es ggf. noch weitere Informationen. Außerdem gibt es dort den Button zum »Abmelden«. Im Zweifelsfall kann man sich auch »Von allen Sitzungen abmelden«. Hat jemand Fremdes Zugriff, sollten so schnell wie möglich die Passwörter geändert und eine Zwei-Faktor-Authentifizierung aktiviert werden.
- »Anmeldewarnungen bei Logins über unbekannte Geräte erhalten« – Die Aktivierung dieser Funktion ist für gewaltbetroffene Frauen sinnvoll, denn sie verschickt eine Benachrichtigung (per E-Mail oder SMS) mit einem Warnhinweis, wenn eine unbefugte Person versucht, sich

von einem anderen Internetbrowser oder Gerät als gewöhnlich in dem Benutzer*innenkonto anzumelden.
- Unter »Einstellungen« und in den »Privatsphäre-Einstellungen« sollte beachtet werden, dass alle möglichen Funktionen auf »Freunde« statt auf »Öffentlich« gestellt sind, damit nicht alle geteilten Informationen und Bilder für die gesamte Internetöffentlichkeit und möglicherweise die gewaltausübende Person einsehbar sind und somit eine Gefahr für die Sicherheit der betroffenen Person darstellen.
- Unter »Einstellungen« und »Deine Facebook-Informationen« können alle Informationen und Daten per E-Mail abgerufen werden. Diese Datensammlung enthält u.a. alle Nachrichten (teilweise auch gelöschte) sowie alle Posts und Fotos. Diese Funktion eignet sich hervorragend als Mittel zur Sicherung von Beweisen, die über Facebook eingegangen sind.

Achtung: In der Beratung sollte geklärt werden, mit wem die betroffene Frau und ihre Kinder in den sozialen Netzwerken »befreundet« sind und ob diese »Freundschaften« sie gefährden können. Wichtig ist hierbei zu klären, ob die Facebook »Freunde« tatsächlich Freund*innen aus ihrem realen Leben sind, oder ob es sich um Personen handelt, die Kontakt mit der gewaltausübenden Person haben. Wenn das Facebook-Profil gehackt wurde, kann dies unter *www.facebook.com/hacked* gemeldet werden. Das Profil kann vorübergehend gesperrt bzw. ein neues Passwort vergeben werden.

Außerdem hat sich in der Beratung gezeigt, dass gewaltausübende Personen und/oder deren Freund*innen gefälschte Profile erstellen, in denen sie vorgeben die betroffene Frau zu sein. Sie nutzen das Profil, um Gerüchte zu streuen, intimes Bildmaterial zu veröffentlichen oder die Frau zu diffamieren. Für die Meldung eines Fake-Profils benötigt die meldende Person einen Facebook-Account, um das gefälschte Profil abzurufen. Dort muss auf das Titelbild geklickt werden, dann unter »Support erhalten« oder »Profil melden«, »Nachahmung« oder »gefälschtes Profil« auswählen. Facebook prüft nach eigenen Angaben zeitnah, ob das Profil gegen die Facebook »Gemeinschaftsstandards« verstößt. Sollte keine Reaktion folgen bzw. die Meldung abgelehnt werden, sollte ein*e Anwält*in hinzugezogen werden.

Die hier vorgestellten Tipps und Hinweise wurden exemplarisch für Facebook erläutert; sie gelten ebenso für andere soziale Netzwerke, obwohl sich die Einstellungsmöglichkeiten im Detail meist unterscheiden.

Messenger sicher nutzen

Ein weiterer Dienst von Facebook ist der beliebte Messenger WhatsApp, der sicherheitstechnisch inzwischen auch angezogen hat. In den Privatsphäre-Einstellungen lässt sich zum Beispiel begrenzen, wer das Profilfoto sehen kann und ob man ungefragt zu Gruppen hinzugefügt werden kann. Weiterhin lassen sich dort Telefonnummern sperren, sodass diese keinen Kontakt mehr aufnehmen können. Dieser Vorgang muss für jeden einzelnen Messengerdienst sowie SMS und normale Anrufe wiederholt werden. Empfehlenswerte Alternativ-Messenger sind »Threema« und »Signal«, die mit Gruppenchats und Sprachnachrichten einen ähnlichen Funktionsumfang aufweisen. In Threema lässt sich sogar die eigene Telefonnummer verbergen.

Die Vorschau von Messenger-Nachrichten auf dem Startbildschirm kann auf gesperrten Smartphones sensible Details verraten. Daher ist es sinnvoll diese Einstellung zu verändern, damit z.B. eine möglichst wenig aussagekräftige Meldung wie »1 neue Nachricht« angezeigt wird. Es ist sinnvoll dies auch bei allen Apps zu minimieren oder diese sogar ganz auszuschalten.

Rechner absichern

Viren, Würmer, Trojaner und andere sogenannte Malware (dt. schadhafte Software) können großen Schaden in Geräten anrichten und zu Datenverlust führen. Erfahrungsgemäß werden diese oft über zweifelhafte E-Mail-Anhänge verschickt. Werden diese unabsichtlich geöffnet, kann die Schadsoftware im Hintergrund der Geräte agieren. Eine gewaltausübende Person kann so Macht über die betroffene Frau erlangen, indem sie Geräte durch den Virenbefall unbrauchbar werden lässt.

Unter Windows 8 und Windows 10 ist der eingebaute »Windows Defender« inzwischen eine gute Abwehr gegen unerwünschte Downloads. Auch Mac-Rechner brauchen kaum ein zusätzliches Anti-Virus-Programm. Wer dennoch zusätzlichen Schutz wünscht, wird bei »Bitdefender«, »Kaspersky« oder »Norton« fündig, die jeweils direkt beim Hersteller heruntergeladen werden sollten und kostenpflichtige Abos erfordern. Leider kursieren im Internet auch Programme, die Anti-Virenschutz nur vorgaukeln und selbst Malware sind. Kostenlose Virenscanner gibt es von »Avast« und »AVG« – die einem bei der Installation leider noch andere Software aufdrängen, derzeit z.B. den Browser »Google Chrome«. Dessen Installation kann durch das Entfernen eines Häkchens aktiv verhindert werden.

Eine schnelle Kontrollmöglichkeit bietet der Blick auf aktuell laufende Programme. Auf Windows-Rechnern sind die in der Leiste unten rechts, beim Mac oben rechts zu finden. Dort befinden sich in der Regel Programme beispielsweise zum Antivirenschutz, zur Monitoreinstellung, zur Drucker- oder Scannereinstellung, zur Desktop- oder Googlesuche, zur Kamerafunktion, zum Batteriestatus oder für Bildimporte. Es gibt jedoch Programme wie z.B. »Refog« oder »BestKeylogger«, die alle Tastatureingaben wie Texte und Passwörter protokollieren (sogenannte Keylogger) und dann meist über das Internet direkt weitersenden. Weiterhin gibt es Programme, die den kompletten Bildschirm auf einen anderen Rechner übertragen (z.B. »VNC«, »Teamviewer«). Sollte sich in der Leiste ein unbekanntes Programm befinden, kann der Name ermittelt werden, indem die Maus draufgehalten wird. Informationen über die Programme finden sich im Internet. Gibt es eine mitlesende Person, kann das Programm mit der rechten Maustaste beendet werden.

Wichtig ist vor allem, die jeweils aktuellen Updates zu laden, sowohl der Betriebssysteme von Rechner und Mobilgeräten, wie auch der installierten Software. Komfortablerweise bieten viele Programme inzwischen eine automatische Update-Funktion an. Meist werden die Updates des Betriebssystems nachts durchgeführt, wenn das Smartphone gerade geladen wird oder der Rechner abends nicht heruntergefahren wurde. Anwendungsprogramme wie Bildbearbeitungssoftware bitten das Update beim Schließen des Programms zu installieren und stören so deutlich weniger als früher.

Im Internet surfen ohne Beobachtung

Durch das Einsehen des Seitenverlaufs des Browsers (»Internet Explorer/Edge«, »Google Chrome«, »Mozilla Firefox« oder »Safari«) werden genaue Informationen zum Surfverhalten sichtbar. Dort ist beispielsweise zu sehen, welche Internetseiten besucht und nach welchen Suchbegriffen (z.B. Frauenberatungsstelle) gesucht wurde. Der Verlauf kann zwar gelöscht werden, noch effektiver ist es jedoch, von vornherein – zumindest bei gemeinsam genutzten Geräten – den privaten Modus zu nutzen und die Speicherung des Verlaufs zu verhindern. Dies funktioniert auf Computern und Smartphones. Dazu wird ein neues Fenster im Internet-Browser als private Sitzung geöffnet. Im Internet Explorer und Edge heißt es »InPrivate-Modus«, für Chrome »Inkognito-Modus«, für Firefox »Neues Privates Fenster« und für Safari »privates Fenster«. Allerdings werden die Informationen erst gelöscht, wenn das Fenster bzw. der genutzte Tab geschlossen werden.

Der private Modus hat noch weitere Vorteile: Der Browser löscht die gesetzten Cookies, mit denen viele Seiten ihre Besucher*innen tracken – also verfolgen sowie Eingaben, die er sonst für die Autovervollständigung von Formularen und ähnlichem speichern würde. Über »Einstellungen« und »Sicherheit« sind die auf einem Rechner gesetzten Cookies einsehbar. Ein vorhandener Cookie ist kein Beweis für den Besuch einer Seite – durch das Einbinden von Werbung, Videos und SocialMedia-Inhalten werden heute oft zahlreiche, unterschiedliche Cookies gespeichert, ohne die Seiten selbst aufgerufen zu haben. Der private Modus ist leider kein Garant dafür, dass die Person komplett anonym im Internet unterwegs ist. Sobald man sich bei Online-Diensten einloggt, speichern die dahinterstehenden Firmen den Besuch. Auch bei Facebook sind Nutzer*innen trotz des privaten Modus für Facebook-Freund*innen dennoch erkennbar online, solange die Sichtbarkeit nicht in den Facebook-Einstellungen geändert wurde. Für zusätzliche Sicherheit ist es notwendig, sich vor dem Schließen des Tabs aus genutzten Diensten auszuloggen. Eventuell getätigte Einkäufe werden von Online-Shops ganz normal bearbeitet und heruntergeladene Dateien bleiben ebenfalls auf dem Rechner.

Beweismaterial und Kontakt mit Seitenbetreiber*innen

Die Beweissicherung bei digitaler Gewalt ist sehr wichtig und kann sehr umfangreich sein.[9] Im Falle von übergriffigem und gewalttätigem Verhalten empfiehlt es sich ein Tagebuch zu führen. Dort sollte alles erfasst werden zu Art, Umfang und Häufigkeit von Vorfällen. Hilfreich ist das Notieren möglicher Zeug*innen, aber auch die psychischen oder physischen Reaktionen der Angriffe bei der betroffenen Person. Zu den dokumentierbaren Übergriffen zählen Nachrichten und Drohungen, Fake-Profile in sozialen Netzwerken und anderen Plattformen, unerlaubt verbreitete Bilder sowie unerlaubt bearbeitete Bilder, unerwünscht installierte Programme und weitere ungewöhnliche Vorfälle. Jede Handlung sollte mit Beweismaterial gestützt werden. Je nachdem, wo und wie ein Übergriff passiert ist, bieten sich unterschiedliche Vorgehensweisen an. Eine einfache Sofortmaßnahme sind Screenshots, die zunächst im Vollbildformat und ohne Bearbeitung abgespeichert werden sollten, damit z.B. das Datum erkennbar ist. Viele

9 Für weitere Informationen siehe bff: Bundesverband Frauenberatungsstellen und Frauennotrufe (Hg.) (o.J.): »Wie dokumentiere ich?«. https://aktiv-gegen-digitale-gewalt.de/de/wie-dokumentiere-ich-richtig.html [Zugriff: 2.7.2020].

Programme benennen die Dateien automatisch mit einem Datums- und Zeitstempel. Es ist sinnvoll diesen bestehen zu lassen und nur ggf. mit einem Hinweis auf den Inhalt wie »Twitter-Nachricht mit Bildmontage« zu ergänzen, um die Datei später besser auffinden zu können. Um persönliche Informationen bei der Weitergabe zu schützen, sollte eine Kopie angelegt und eventuell erkennbare Infos in der Kopie unkenntlich gemacht werden.

Die Organisation Weißer Ring bietet mit »NO STALK« eine App für Android-Smartphones und iPhones an, um Foto-, Video- oder Sprachaufnahmen zu sichern. Die App richtet sich vor allem an Betroffene von Online-Stalking und bietet ihnen die Möglichkeit, Vorfälle wie in einem Tagebuch zu beschreiben. Die Daten werden in einem Rechenzentrum in Deutschland gespeichert und laut Weißem Ring vor Gericht anerkannt. Zu finden ist die App auf *www.nostalk.de* und in den gängigen App Stores.

Ob Facebook-Profile, Kommentare auf Facebook oder einzelne Tweets auf Twitter – oft sind Inhalte auf Webseiten und sozialen Netzwerken über *einen spezifischen Link* (URL) zu finden, wie etwa https://twitter.com/bff_gegenGewalt/status/1207997598419881988. Um etwa diesen Tweet zu sichern, muss dieser Link in einem Browser geöffnet werden, um dann im dessen Menü »Seite speichern unter…« die »komplette Seite« abzuspeichern. Außerdem sollte ein Screenshot gemacht werden, bei dem der komplette Link (sofern möglich) gut sichtbar ist. Das ist wichtig, falls der Inhalt des Posts nicht mehr abrufbar ist, wenn der Post von dem*der Urheber*in gelöscht wird.

In Messengern empfangene Sprachnachrichten können für weitere Verwendung exportiert werden. Die Android-Version von WhatsApp speichert die Nachrichten selbstständig im Dateimanager des Smartphones ab. Auf iPhones muss jede Sprachnachricht einzeln abgespeichert werden. Dazu drückt man lange auf die Nachricht, um zur Option »Weiterleiten« zu kommen. Über das Teilen-Icon kann die Nachricht auf dem Telefon oder einem externen Cloud-Dienst wie Dropbox gespeichert werden. Auch hier besteht der Dateiname aus Datum und Zeit der Aufnahme und sollte höchstens um einen aussagekräftigen Hinweis am Ende ergänzt werden.

Bei E-Mails empfiehlt es sich, diese mit einem E-Mail-Programm wie »Thunderbird«, »Outlook« oder »Apple Mail« abzurufen und zu sichern. Wichtig ist die Speicherung im Dateiformat .eml, das den »Mail Header« umfasst. Der Mail-Header bietet der Polizei wichtige Meta-Daten für die Strafermittlung, etwa über die verwendeten E-Mail-Server. Je nach Programm muss beim Speichern »Reine Datei der E-Mail«, »Outlook-Nachrichtenformat – Unicode« oder »Mail-Dateien« ausgewählt werden. Auch hier bieten sich

Datum und Hinweis auf den Inhalt als Dateiname an. Webmail-Oberflächen bieten manchmal ebenfalls einen eml-Download an, aber nicht immer; das GMX-Webmail speichert E-Mails nur als html-Dateien ohne Mail-Header. Die Header können im Web-Interface (Webansicht) separat angeschaut und dann als Textdatei extra gespeichert werden. Um sie einzusehen, muss meist auf »Header«, »Kopfzeile« oder »Original anzeigen« geklickt werden. Wird eine E-Mail weitergeleitet, entsteht übrigens ein neuer Mail-Header, der nur noch die Weiterleitung beinhaltet.

Viele Online-Dienste bieten Möglichkeiten, die Aktivitäten des eigenen Kontos zu exportieren. Dies kann nützlich sein, wenn die gewaltausübende Person Zugriff hatte und zum Beispiel Nachrichten darüber verschickt hat. So kann aus den Twitter-Einstellungen ein Archiv der eigenen Daten heruntergeladen werden; Google bietet unter *takeout.google.com* gleich verschiedene Archivformate für eine Sicherung an. Auch der Browserverlauf eignet sich zur Beweissicherung, wenn etwa der Browser genutzt wurde, obwohl die betroffene Person gar nicht zu Hause war. Hier ist es wichtig Screenshots inklusive des Datums zu machen, ohne die angezeigten Webseiten erneut aufzurufen oder anzuklicken, da die Seite sonst aus dem Verlauf vergangener Tage ans obere Ende ins »Jetzt« rutscht. Je nachdem, ob und wie Sie eine Anzeige erstatten wollen, können Beweise wie Screenshots und E-Mails, inklusive des Headers, neben der digitalen Sicherung ausgedruckt und analog abgelegt werden. Für das weitere Vorgehen und etwaige Nachfragen sollten die digitalen »Originale« sicher aufbewahrt werden.

Digitale Beweismaterialien können als Hinweise zu einer Anzeige über die Online-Wache der Polizei in fast allen Bundesländern unter *https://online-strafanzeige.de* vermerkt, jedoch nicht hochgeladen werden. Die Beweise sollten nicht an andere Personen weitergeleitet werden, um Manipulationen auszuschließen, ausgenommen sind natürlich Rechtsanwält*innen oder Beratungsstellen. Wenn die Beweise gesichert sind, sollte unverzüglich gemeinsam mit der betroffenen Person Kontakt mit den Seitenbetreiber*innen aufgenommen werden, um unerwünschte Informationen wie Posts, Fotos, Nachrichten, Daten oder Fake-Profile von Internetseiten oder in sozialen Netzwerken löschen zu lassen. Schließlich können personenbezogene Daten aus der Google-Suche oberflächlich gelöscht werden. Google bietet dazu ein Antragsformular unter: *https://google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf*. Falls die Kontaktaufnahme mit den Seitenbetreiber*innen keinen Erfolg hat, sollte ein*e Anwält*in hinzugezogen werden.

Geräte zurücksetzen oder neu installieren

Für einen digitalen Neuanfang können elektronische Geräte meist auf die Werkseinstellungen zurückgesetzt oder sogar das Betriebssystem neu installiert werden. Sowohl für das Smartphone als auch für Computer, Laptop und Tablets gilt dabei, dass zunächst alle persönlichen Daten extern gesichert werden müssen. Bei der Neu-Installation oder dem Zurücksetzen werden die installierten Programme und gespeicherten Daten gelöscht. Letztere sind danach nur in Ausnahmefällen mit spezieller Software wiederherzustellen. Für gängige Smartphones ist es möglich, unter »Einstellungen«, unter »Allgemein« oder »Allgemein verwalten« das Telefon in die Werkseinstellungen zurückzusetzen.

Im Internet finden sich Anleitungen, wie Computer oder Laptops ohne große IT-Kenntnisse neu aufgesetzt werden können. Unter Windows 10 geht dies inzwischen aus den »Einstellungen« heraus. Unter »Updates und Sicherheit« muss die »Wiederherstellung« ausgewählt werden. Dabei gibt es die Möglichkeit, die eigenen Dateien zu erhalten oder wirklich alles zu entfernen. Am sichersten ist es, die Dateien vorher gezielt zu sichern und anschließend alles zu löschen. Eine Neueingabe des Lizenzschlüssels ist bei diesem Vorgehen normalerweise nicht nötig. Bei älteren Windows-Versionen oder der Neu-Installation von Windows 10 ist eine Installations-DVD oder ein USB-Stick mit einer Installationsdatei nötig. Am einfachsten geht es, wenn ein Zugriff auf eine mitgelieferte Installations-DVD und den Lizenzschlüssel (auch »Product Key« genannt) gewährleistet ist. Dann sollte der Rechner das System von der DVD starten und das Betriebssystem direkt neu installiert werden. Wer den eigenen Lizenzschlüssel nicht kennt, muss diesen vor der Neuinstallation auslesen – auch dazu gibt es Gratis-Programme und Anleitungen im Netz. Oft ist er auf einem Aufkleber auf dem Rechner oder im mitgelieferten Benutzerhandbuch zu finden. Gibt es keine Installations-DVD, kann ein USB-Stick mit mindestens vier GB Speicher als Installations-Stick genutzt werden. Microsoft bietet dafür die »Windows USB/DVD-Download Tools« auf *https://microsoft.com/de-de/download/details.aspx?id=56485* an. Die deutsche Sprachversion ist mit de-DE gekennzeichnet. Neben dem Tool muss noch die passende Windows-Version als Datenträgerabbild bzw. ISO-Datei von https://microsoft.com/de-de/software-download/ heruntergeladen werden. Die ISO-Datei wird über das USB/DVD-Download Tool auf den Stick geladen, der nun ein »bootfähiger USB-Stick« ist, von dem aus die Installation startet. Dafür wird er beim Rechnerneustart als

»1st Boot Device« festgelegt. Bei einer Neuinstallation wird der USB-Stick allerdings automatisch wieder formatiert. Soll damit ein weiterer Laptop zurückgesetzt werden, muss das Prozedere von vorn begonnen werden. Mit dem USB/DVD-Download Tool kann alternativ eine Installations-DVD gebrannt werden. Computerzeitschriften bieten auch regelmäßig Notfall-Windows-DVDs an, die Heften beiliegen oder deren Inhalt aus dem Internet geladen werden kann, um bootfähige USB-Sticks zu erstellen.

Mac-Rechner lassen sich seit OS X Lion (10.7) direkt zurücksetzen. Dafür ist nur eine Internetverbindung nötig. Kann die bisherige Apple-ID weiterverwendet werden, müssen während eines Neustarts des Rechners die Tasten CMD und R gleichzeitig gedrückt werden. In den macOS-Dienstprogrammen kann die Option »macOS erneut installieren« gewählt werden. Für den Fall, dass künftig eine neue Apple-ID genutzt werden soll, muss die alte Apple-ID vor der Neu-Installation aus iTunes, iCloud und iMessage abgemeldet werden. Wurde die Festplatte in Partitionen (verschiedene Laufwerke) unterteilt, muss nach dem Neustart in den macOS-Dienstprogrammen zunächst das Festplattendienstprogramm ausgewählt werden. Hier können die Partitionen gelöscht werden. Schließlich kann auch die gesamte Festplatte gelöscht werden, bevor das System neu installiert wird. Dabei werden alle Daten so überschrieben, dass sie nicht mehr zu retten sind.

Ausblick

Aus der Beratung bei digitaler Gewalt ist bekannt, dass ein frühzeitiges, systematisches und schnelles Vorgehen zentral für den Schutz und die Handlungsfähigkeit von Betroffenen ist, um weitere Angriffe zu unterbinden bzw. bestehende Gefährdungen wie veröffentlichte Nacktbilder oder eine veröffentlichte Adresse für die betroffene Person abzuwenden. Die Bearbeitung dieser Gewaltform ist für die Berater*innen besonders zeitintensiv und bindet personelle Ressourcen, die in ambulanten Fachberatungsstellen oft noch unzureichend finanziert sind. Ebenso verfügen nicht alle Beratungsstellen über die fachliche Expertise für eine solche Beratung.

Nach Ansätzen der feministischen parteilichen Beratung ist es kontraproduktiv, Betroffenen digitaler Gewalt die Schuld zuzuweisen. Zum einen tun dies Betroffene oft genügend selbst, zum anderen findet hier eine Täter-Opfer Umkehr statt – ein Phänomen, das bei Gewalt gegen Frauen immer auftaucht. Wie bei allen Gewaltformen müssen auch bei digitaler Gewalt Be-

troffene ernstgenommen werden, sodass sie nach dem Kontrollverlust durch digitale Gewalt wieder in Handlungsfähigkeit gelangen können.

Neben der Wiedererlangung der Kontrolle gilt es, Betroffene über die grundlegenden Sicherheitsprinzipien ihrer digitalen Geräte aufzuklären, Beweise zu sichern, das physische und psychische Wohlbefinden zu schützen und die digitale Medienkompetenz zu stärken. Ein weiteres Ziel feministischer Intervention in diesem Bereich ist es, den gesellschaftlichen Diskurs über digitale Gewalt voranzutreiben, damit die Strafverfolgungsbehörden, Sozialen Netzwerke, Pornoplattformen und Spionage-Software-Firmen digitale Gewalt ächten und schnell auf sie reagieren.

Literatur

bff: Bundesverband Frauenberatungsstellen und Frauennotrufe (Hg.) (o.J.): »Wie dokumentiere ich?«. https://aktiv-gegen-digitale-gewalt.de/de/wie-dokumentiere-ich-richtig.html [Zugriff: 2.7.2020].

Bleich, Holger (2018): »Alptraum Handy-Wanze: Smartphone-Spionage-Apps als Stalker-Werkzeuge«, in: c't, Nr. 18, S. 76. https://heise.de/select/ct/2018/18/1535416499320900 [Zugriff: 5.1.2020].

Coalition Against Stalkerware (Hg.) (o.J.): »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: 5.5.2020].

Gierow, Hauke (2019): »Spionage-Apps: Schutz vor Überwachung ist möglich«. https://mobilsicher.de/ratgeber/spionage-apps-schutz-vor-partner-spyware-ist-moeglich#9 [Zugriff: 28.10.2019].

klicksafe/Institut für Digitale Ethik (IDE) der Hochschule der Medien Stuttgart (Hg.) (2018): »Neu bei klicksafe: Digital Safety Compass«. https://klicksafe.de/service/aktuelles/news/detail/neu-bei-klicksafe-digital-safety-compass/ [Zugriff: 1.3.2020].

NNEDV (National Network To End Domestic Violence) (Hg.) (2014): »Privacy and Safety on Facebook: A Guide for Survivors«. https://nnedv.org/mdocs-posts/privacy-safety-on-facebook-a-guide-for-survivors/ [Zugriff: 2.7.2020].

Digitale Sicherheit für frauenspezifische Einrichtungen

Helga Hansen

Neben Strategien und Tipps, die die Betroffenen von digitaler Gewalt und ihre Sicherheit in den Fokus nehmen[1], ist es wichtig, sich die digitale Sicherheit von Organisationen und Einrichtungen genauer anzuschauen. Einige grundsätzliche Hinweise, etwa zur Erstellung sicherer Passwörter, gelten wie zuvor beschrieben. An anderer Stelle müssen aber andere Entscheidungen getroffen werden.

Im ersten Schritt geht es um mögliche Bedrohungsszenarien, deren konkrete Bewertung vermutlich in jeder Einrichtung unterschiedlich abläuft. Der in diesem Artikel beschriebene Plan zur digitalen Sicherheit ist adaptiert aus dem Guide »Your Security Plan« (2019) der US-amerikanischen Bürgerrechtsorganisation Electronic Frontier Foundation (EFF), die zu Themen wie Datenschutz und Überwachung aufklären sowie Betroffene vor Gericht vertreten. Anschließend folgen Tipps zum strukturierten Absichern der digitalen Infrastruktur, angelehnt an die CIS Controls V7.1 (2019) – Empfehlungen des Center for Internet Security (CIS), einem Zusammenschluss von Firmen, Organisationen und Forschungseinrichtungen rund um das Thema Internet-Sicherheit.

Bedrohungsszenarien

Je mehr Zeit und Geld zur Verfügung stehen, umso bessere digitale Sicherheitsmaßnahmen können umgesetzt werden – aufgrund der eingeschränkten

1 Siehe Beitrag: Digitale erste Hilfe und Sicherheitsprinzipien für Berater*innen bei digitaler Gewalt.

Finanzierung von frauenspezifischen Einrichtungen ist beides oft Mangelware. Dennoch lassen sich mit einigen einfachen Überlegungen wichtige Grundlagen schaffen. Um vernünftig einschätzen zu können welche Maßnahmen realistisch sind, gilt es zunächst, die eigene Lage hinsichtlich möglicher Bedrohungen zu bewerten. Die EFF schlägt dafür im Security Plan fünf Fragen vor, die übrigens auch bei der Sicherheitsbetrachtung nicht-digitaler Güter funktionieren.

Was gilt es zu schützen?
Zu den digitalen Gütern, die geschützt werden müssen, gehören zum einen Informationen wie Kontaktdaten, Nachrichten, E-Mails und Dateien. Zum anderen können dies auch elektronische Geräte sein, wie z.B. Diensttelefone. Welche (sensiblen) Daten in europäischen Beratungsstellen gesammelt, gespeichert und weitergegeben werden, muss seit der Einführung der Datenschutzgrundverordnung (DSGVO) bereits dokumentiert sein. Die DSGVO bietet einen guten Anlass, die Praxis der Datensammlung und -verarbeitung zu überprüfen und gegebenenfalls zu überdenken.

Vor wem müssen Daten/Geräte geschützt werden?
Diese Überlegung ist grundlegend für einen umfassenden Plan. Hierbei kann es sich um Personen handeln (z.B. Partner von Klientinnen, Antifeminist*innen) oder aber Vereinigungen, die feministischen Organisationen schaden wollen (z.B. antifeministische und/oder rechte Gruppen). Je nach den Schwerpunkten ihrer Arbeit und konkreten Fällen könnten auch Behörden wie die Polizei oder Ausländerbehörde ein Interesse haben auf ihre Informationen zurück zu greifen. Schließlich können selbst zufällige Hacker*innen-Angriffe oder die Datenauswertung durch Internetfirmen prinzipiell ein Problem darstellen.

Wie schwerwiegend sind die Konsequenzen, wenn etwas schief geht?
Bei Angriffen durch (Ex-)Partner von Klientinnen besteht die Gefahr, dass eine gewaltausübende Person die neue Telefonnummer oder den Aufenthaltsort ihres Opfers herausfindet und unerwünscht Kontakt aufnimmt bzw. die Person gefährdet. Hacker*innen sind nicht unbedingt an konkreten Informationen interessiert – wenn eine Schadsoftware den Rechner unbenutzbar macht, kann es aber viel Zeit und Geld kosten, bis die Arbeit in der Einrich-

tung wieder möglich ist. Auch bei Angriffen durch Organisationen ist dies eine Gefahr.

Wie wahrscheinlich ist es, dass etwas schief geht?
Ebenso unterschiedlich wie die Auswirkungen sind die Wahrscheinlichkeiten, ob etwas eintritt. Daher ist es wichtig mit Computerfachpersonen Szenarien durchzuspielen und zu überlegen, welche Angriffe vorstellbar oder wahrscheinlich erscheinen.

Wie viele Ressourcen stehen zur Verfügung?
Die letzte Vorüberlegung ist die Frage, wieviel Zeit und Geld aufgewendet werden kann, um Bedrohungen abzuwenden. Dabei gilt: Absicherung kostet, aber etwas Sicherheit ist besser als keine Maßnahme. Wenn das Geld nicht für einen neuen Router reicht, ist eine veraltete Verschlüsselung immer noch besser als keine Verschlüsselung einzurichten. Der Aufwand hingegen ist etwas, was NGOs aufbringen müssten, wenn sie ihre Organisationen auch digital schützen wollen. Mit diesen Überlegungen im Hinterkopf ist es Zeit, die eigene digitale Infrastruktur durchzugehen.

Hardware überprüfen

Mit Hardware sind alle elektronischen Geräte gemeint. Um diese zu überprüfen ist es wichtig, zunächst eine Bestandsaufnahme zu machen; hierzu gehört die Auflistung aller Rechner, Smartphones, Router, Sticks etc., die im Büro oder an anderer Stelle für dienstliche Tätigkeiten genutzt werden. Wie bei Listen für die Verwendung von Schlüsseln ist es wichtig, in der Aufstellung deutlich zu machen, wer über welche Geräte verfügen bzw. nicht verfügen darf. Auch über ihre privaten Smartphones, die sie mit ins Büro bringen, sollten sie einen Überblick haben, um unbekannte Geräte schnell zu erkennen. Sollte jemand in der Beratungsstelle tatsächlich oder vermeintlich eines vergessen haben, ist Vorsicht geboten, denn es könnte zum Ausspionieren genutzt werden. In einem solchen Fall ist es wichtig, das Gerät auszuschalten und sicher aufzubewahren.

Um in der Beratungsstelle die digitale Sicherheit der betroffenen Frauen zu überprüfen und zu verbessern, kann es sinnvoll sein, Internetzugänge für Klientinnen bereit zu stellen. Während für die eigenen Rechner möglichst Kabel genutzt werden sollten, ist das Anschließen von weiteren Rechnern an das

eigene Netzwerk ein Einfallstor für Schadsoftware. Daher ist es sinnvoll ein WLAN für Klientinnen und Besucher*innen einzurichten, das nur in Beratungen genutzt wird und dessen Zugangsdaten regelmäßig geändert werden. Alle drahtlosen Netzwerke sollten nur verschlüsselt genutzt werden. Bei digitalen Notfällen, wie dem Auffinden von Spionagesoftware, sind USB-Sticks und DVDs sehr hilfreich, mit denen ein Rechner neu aufgesetzt werden kann. Es ist daher sinnvoll, diese für sich und Klientinnen vorzuhalten, damit die Geräte schnell wieder einsetzbar sind.

Software überprüfen

Mit Software sind sämtliche Programme gemeint. Ähnlich wie bei der Überprüfung der Hardware ist eine Auflistung der Programme sehr wichtig. Bei Windows-Rechnern ist sie über die Systemsteuerung und bei Mac-Rechnern über den Systembericht zu finden. Wichtig ist regelmäßig zu überprüfen, ob es Programme gibt, die länger nicht genutzt wurden; diese sollten gelöscht werden. Bei Unsicherheiten, ob ein Programm wichtig ist, hilft meist eine Google-Suche weiter.[2] Auch ist zu überlegen, ob die bisher verwendeten Programme die besten Lösungen sind. Ein positives Kriterium ist, dass es regelmäßige Updates gibt, mit denen Sicherheitslücken geschlossen werden. Ein weiteres Kriterium ist etwa, ob Programme oft Ziel von Hacker*innen-Angriffen sind, wie etwa Microsoft Word. Mit dem Einsatz der Open-Source-Software LibreOffice lässt sich das vermeiden – sie nützt aber nichts, wenn die Berater*innen mit dem Programm nicht arbeiten können. Daher gilt es, eine Balance zwischen Sicherheit und realistischen Anwendungsmöglichkeiten zu finden.

Diese Hinweise gelten auch innerhalb von Programmen: In den Einstellungen ist zu sehen, ob und wenn ja, welche Erweiterungen installiert sind. Je nach Programm können diese Zusätze »Plugins« oder »Add-ons« heißen. Besonders im Browser werden Plugins gern beim Download völlig anderer Software als unerwünschte Zugabe installiert, um beispielsweise die Standardsuchmaschine zu ersetzen. Im Zweifelsfall können Browser-Plugins einfach gelöscht werden. Eine Ausnahme sind Plugins zum Blocken von Werbung und Tracking. Über Werbung wird manchmal schädliche Software verbreitet, für

2 Siehe Beitrag: Digitale erste Hilfe und Sicherheitsprinzipien für Berater*innen bei digitaler Gewalt.

deren Ausbreitung man nicht einmal auf die Anzeige klicken muss. Der Fachbegriff dafür lautet »Malvertising«, eine Kombination der englischen Begriffe »Malware« für Schadsoftware und »Advertising« für Werbung. Erweiterungen wie AdBlock Plus oder uBlock Origin blockieren Werbung.

Up-to-date bleiben

Da das Internet ein schnelllebiges Medium ist und ständig neue digitale Geräte erscheinen, ist es wichtig, auf dem Laufenden zu bleiben, um aktuelle Bedrohungen und Gegenmaßnahmen einschätzen zu können. Das gilt auch für die eingesetzte Software, die stets auf dem neusten Stand sein sollte. Dazu kann inzwischen bei vielen Programmen die Funktion Auto-Update aktiviert werden, mit der neue Updates automatisch installiert werden. Wird ein Virenscanner genutzt, sollte dieser sich ebenfalls eigenständig selbst, wie auch die verwendeten Virendefinitionen, regelmäßig aktualisieren.

Immer wieder werden Passwörter von E-Mail- und Social Media-Accounts etc. geknackt und öffentlich gepostet (geleakt). Eine Möglichkeit sicherzugehen, dass Accounts der Beratungsstelle nicht betroffen sind, ist eine Überprüfung bei Diensten wie dem »Identity Leak Checker« des Hasso-Plattner-Instituts. Ebenso ist es wichtig im Blick zu behalten welche Datenlecks bekannt werden. Sinnvoll ist schließlich, regelmäßig sich selbst, bzw. die eigene Einrichtung in Suchmaschinen und Social Media zu suchen, um zu überprüfen, ob die Daten aktuell sind und keine Informationen zu finden sind, die geheim bleiben sollten. Das Einrichten eines »Google Alerts« kann dabei sehr hilfreich sein und viel Zeit sparen. Soziale Netzwerke und Google bieten außerdem Möglichkeiten, um falsche Ergebnisse zu melden – meist sind dazu aber Accounts nötig.

Rechte-Management

Eine grundlegende Frage für jede Organisation sind die Zugriffsrechte, also wer auf was zugreifen darf oder nicht. Neben Beschränkungen für Nutzer*innen-Accounts sind dabei auch Passwörter wichtig. Auch hier sorgt eine Auflistung dafür, dass im Blick bleibt, über welche Netzwerke, Accounts etc. die Beratungsstelle kommuniziert und wer welche Rechte hat oder haben soll. Alte und ungenutzte Konten sollten in diesem Prozess gelöscht werden.

Ob Windows-, Mac- oder Linux-Rechner – auch in Betriebssystemen haben die Nutzer*innen-Konten unterschiedliche Rechte. Admin-Rechte und das entsprechende Passwort ermöglichen die Installation von jeglicher Software. Ein Administrator*innen-Konto ist daher auf jedem Rechner nötig, sollte aber nur bei Bedarf genutzt werden. Für die tägliche Arbeit sollten stattdessen Konten mit begrenzten Rechten eingesetzt werden. Sie erlauben unter Windows immer noch die Installation einiger Software und das Ändern einiger Einstellungen.

Ältere Windows-Versionen umfassen noch Gast-Accounts, mit deren Zugangsdaten keine Software installiert werden kann. Um Gäste-Konten unter Windows 10 zu ermöglichen, muss die Kommandozeile genutzt werden. Das klingt zunächst oft einschüchternd, bedeutet aber in der Praxis nur wenige Klicks, die entsprechende Anleitungen im Internet erläutern. Die Windows-10-Home-Edition unterscheidet immerhin zwischen Familienmitgliedern und »anderen Benutzern«. In den Einstellungen werden diese »Kontotypen« unter »Konten« verwaltet. Inzwischen drängt Hersteller Microsoft dabei auf den Einsatz eines Microsoft-Kontos und die Angabe von Kontaktdaten. Das Anlegen von lokalen Nutzer*innen-Accounts ist aber ohne diese Angaben möglich. Der Schutz vor unerwünschten Zugriffen ist nur effektiv, wenn ein Rechner konsequent gesperrt wird, sobald der Schreibtisch verlassen wird.

Für die Auswahl von Passwörtern gilt, dass diese möglichst lang sein sollten; außerdem sollte für jeden Account ein anderes Passwort gewählt werden. Sie sollten geändert werden, sobald es einen konkreten Anlass gibt, etwa beim Personalwechsel. An dieser Stelle ist der Einsatz von Passwortmanagern unbedingt zu empfehlen, mit denen sehr lange Passwörter generiert und einfach ausgetauscht werden können. Selbst häufige Wechsel durch kurzzeitig tätige Praktikant*innen oder Freiwillige sind dann kein Problem. Neben Programmen, die für Einzelpersonen gedacht sind, gibt es auch Lösungen für Firmen und Organisationen. Diese können so eingestellt werden, dass Nutzer*innen die Zugangsdaten für verschiedene Accounts gar nicht selbst kennen müssen, sondern allein ihr Passwort für den Passwortmanager. Allerdings kosten die Programme Geld: meist handelt es sich um Abos, die abhängig von der Zahl der Nutzer*innen teurer werden. Manche Programme können auf eigenen Servern installiert werden, während andere auf Cloud-Dienste setzten. Hier muss abgewägt werden, welche Lösung für die Einrichtung die sinnvollste ist.

Neben dem Passwort ist bei der Zwei-Faktor-Authentifizierung (2FA) ein zweiter Faktor in Form eines Codes oder Hardware-Schlüssels nötig, um sich in Rechner, Programme oder Konten einzuloggen. Wenn der zweite Faktor

fehlt, da zum Beispiel das Handy verloren gegangen ist, an das ein Code gesendet wird, ist allerdings auch der Zugriff zum Account unmöglich. Sinnvoll ist daher, zwei 2FA-Methoden zu nutzen. Dies können entweder zwei komplett unterschiedliche Methoden sein oder es wird eine Methode doppelt genutzt. Bei Hardware-Schlüsseln hieße dies, zwei Schlüssel zu nutzen und einen stets bei sich zu tragen, während der andere für Notfälle sicher aufbewahrt wird. Wer eine 2FA-App nutzt, sollte die App neben dem Smartphone auf einem zweiten Gerät, wie einem Tablet oder Zweit-Telefon, installieren.

Weitere Einstellungen

Unbekannte Hardware wie USB-Sticks, Festplatten oder CDs sollte grundsätzlich nicht sorglos in Rechner eingesteckt werden. Da es sich manchmal nicht vermeiden lässt und um bei Versehen ein Stück sicherer zu sein, sollte zumindest das automatische Abspielen unterbunden werden. In den Einstellungen von Windows kann dies unter »Geräte« im Punkt »Automatische Wiedergabe« eingestellt werden.

Einige Dokumente und Informationen müssen lange vorgehalten werden. Um sie sicher aufzubewahren, sind wiederkehrende Backups notwendig. Im Idealfall stellt man dies mit der 3-2-1-Regel sicher: Es sollten drei Kopien wichtiger Daten existieren, die auf zwei unterschiedlichen Datenträgern untergebracht sind, wobei jeder Datenträger an einem anderen Ort steht. In der Praxis bedeutet dies beispielsweise die Originaldatei auf dem Rechner, eine Kopie auf einer lokalen Festplatte und eine Kopie in einer Cloud-Lösung. Neben Festplatten sind USB-Sticks und CDs mögliche Backupmedien, die aber jeweils Nachteile haben. Sticks gehen aufgrund ihrer Größe schneller verloren und selbst wiederbeschreibbare CDs können nicht so oft genutzt werden wie Festplatten. Mit der 3-2-1-Regel sollte sowohl beim Verlust oder Diebstahl von Geräten, wie auch bei digitalen Angriffen mindestens eine Kopie erhalten bleiben. Statt die Kopien per Hand anzulegen und zu aktualisieren, sollte eine Software eingesetzt werden, damit die Backups automatisch und regelmäßig erfolgen. Unter Windows lässt sich zum Beispiel das Tool »Duplicati 2« nutzen, während Macs mit »Time Machine« bereits eine vorinstallierte Lösung mitbringen. Beim Einsatz von Backup-Software sollte darauf geachtet werden, welche Ordner und Dateien mitgesichert werden und welche ignoriert werden sollen. Wie bereits angesprochen, spielt dabei auch der Datenschutz eine Rolle. Zu Beginn ging es in den Bedrohungsszenarien darum kritisch zu

schauen, welche Daten tatsächlich gespeichert werden müssen. Die nächste Frage ist: Wo werden sensible Daten gespeichert? Sie sollten möglichst verschlüsselt gespeichert werden. Dabei werden Dateien in einen digitalen Tresor gelegt, der nur durch die Eingabe eines Passworts und ggf. eines zweiten Faktors geöffnet werden kann. Dazu gibt es ebenfalls Programme: Unter Windows etwa »VeraCrypt«, während Macs mit »FileVault« bereits ein Programm von Haus aus mitbringen. Verschlüsselung und Backup werden am besten so kombiniert, dass verschlüsselte Daten ins Backup gehen, wobei wiederum die Hinweise zu sicheren Passwörtern und Zwei-Faktor-Authentifizierung gelten.

Das physische Abschließen ist eine weitere Möglichkeit, also das althergebrachte Aufbewahren von Speicher- und Backupmedien in einem abgeschlossenen Schrank. Ähnlich wie bei Akten sollte schließlich klar sein, wann und wie Daten gelöscht werden, wenn sie nicht mehr vorgehalten werden müssen. Wichtig ist auch hier am Ende, dass eine Lösung gefunden wird, die tatsächlich angewendet wird, statt sich die sicherste Lösung zu überlegen und dann nie umzusetzen. Verschlüsseln lässt sich auch Kommunikation. Leider ist die E-Mailverschlüsselung mit OpenPGP seit jeher etwas umständlich, da einiges an Software installiert und eingestellt werden muss. Inzwischen ist OpenPGP nicht mehr zu empfehlen, da die Einbindung in die meisten E-Mailprogramme fehlerhaft ist. Allerdings funktioniert dies mit E-Mails kaum, so dass sensible Informationen nicht per E-Mail ausgetauscht werden sollten. Eine Alternative sind Messenger-Apps auf dem Smartphone, die Nachrichten von sich aus verschlüsseln.

Schadsoftware und Phishing vermeiden

Trojaner[3] und ähnliche Schadsoftware werden inzwischen in E-Mails versendet, die auf den ersten Blick kaum zu erkennen sind. Sie scheinen von Leuten zu sein, mit denen bereits Kontakt besteht; oft beziehen sie sich sogar auf zuvor selbst geschickte E-Mails. Die problematische Software versteckt sich im Anhang, in Form von Word-Dokumenten oder Archiven. Bei der Textverarbeitungssoftware Word nutzen Angreifer*innen sogenannte Makros aus. Das sind Programme-im-Programm, mit denen sich in Microsoft-Office-Anwendungen die Arbeit vereinfachen lässt. Anstatt immer wiederkehrende

3 Trojaner sehen oberflächlich nach nützlichen Programmen aus, um unerwünschte Funktionen zu verstecken.

Aufgaben jedes Mal von Hand auszuführen, erledigen Makros sie selbsttätig auf Knopfdruck, wie etwa das Einfügen einer speziell vorformartierten Tabelle in Textdokumente. Da sie von Kriminellen oft missverwendet werden, sind Makros heute im Office-Programm standardmäßig deaktiviert. Kommt nun ein Word-Dokument mit Schadsoftware, zeigt diese als Erstes beim Öffnen eine gefälschte Fehlermeldung, damit Makros wieder aktiviert wird und die Schadsoftware ausgeführt werden kann. Eine andere Technik sind Datei-Archive wie ZIP-Dateien, die entpackt und entschlüsselt werden müssen. Der Schlüssel wird praktischerweise in der gleichen Mail mitgesendet. Normalerweise gilt: Wer verschlüsselte Dateien verschickt, sollte den Schlüssel mindestens in einer zweiten E-Mail oder noch besser über einen anderen Weg der Kommunikation verschicken. Derartige sinnlose Sicherheitsmaßnahmen sind ein Hinweis auf unredliche Absichten. Im Zweifelsfall ist es hilfreich, bei ungefragt zugesandten Dokumenten zum Telefonhörer zu greifen und nachzuhaken. Virenscanner erkennen die Schädlinge derzeit leider nicht zuverlässig. Auf keinen Fall sollten Anhänge mit der Endung .exe geöffnet werden. EXE-Dateien sind Windows-Programme, auch wenn die Dateiendung meist ausgeblendet wird. Heute werden Schädlinge allerdings nur noch selten so offen versendet.

Manche Schadsoftware verschlüsselt dafür die eingebauten und angeschlossenen Festplatten und verlangt für die Freigabe der Daten ein Lösegeld. Das lohnt sich bei Beratungsstellen zwar nicht, ist aber keine Garantie, dass es nicht passiert. Deswegen sind Backups wichtig, denn mindestens eine Kopie aller nötigen Informationen ist dann noch vorhanden. Eine Alternative zu Microsoft Office sind die kostenlosen Programme »LibreOffice« und »OpenOffice«, bei denen die Angriffe auf Makros nicht funktionieren.

Im besten Fall erkennt entweder der E-Mail-Provider oder das eigene E-Mail-Programm kritische Mails. Einen Mailcheck stellt die IT-Nachrichtenseite heise online unter https://heise.de/security/dienste/Emailcheck-2109.html bereit. Über die Seiten lassen sich Test-E-Mails verschicken, um zu überprüfen, ob das E-Mail-Programm oder der Virenscanner die Schädlinge erkennt. Wenn ein Rechner infiziert ist, hilft nur, gleich den Internetzugang zu kappen, damit auf keinen Fall weitere Computer gefährdet werden. Anschließend muss das Betriebssystem neu installiert werden[4].

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

Neben Schadsoftware ist Phishing ein Problem. Hierbei werden meist Zugangsdaten für Webseiten kopiert, indem erst E-Mail-Benachrichtigungen von Banken oder Sozialen Netzwerken gefälscht werden und auf ebenso gefälschte Webseiten verweisen. Um sich davor zu schützen, sollten Links in einer E-Mail immer genau angesehen werden, bevor sie angeklickt werden. Noch sicherer ist es, die Adresse der Webseite von Hand im Browser einzutippen. Eine weitere Möglichkeit ist, Links erst zu kopieren und in ein ganz einfaches Textverarbeitungsprogramm, das keine Formatierungen unterstützt, einzufügen, wie den vorinstallierten Microsoft Editor. Er zeigt direkt den eingefügten Text an, sodass man kontrollieren kann, ob die Adresse auf eine vertrauenswürdige oder gefälschte Webseite führt.

Weiterbildung und Notfallpläne

Nachdem mögliche Szenarien erkannt sind und im Idealfall Vorsichtsmaßnahmen getroffen wurden, muss ein Plan für Angriffe erarbeitet werden. Wichtig für diesen Notfallplan ist die erste Ansprechperson. Auch ist es wichtig sich im Vorfeld zu überlegen, wer die Entscheidungen trifft und wer jeweils das Backup erstellt. Hilfreicher Teil eines Notfallplans sind zudem Kontaktdaten von weiteren Einrichtungen, Firmen oder der Polizei an die sie sich wenden könnten. Im Falle eines Angriffs ist eine möglichst genaue Dokumentation der Vorfälle unerlässlich. Diese Dokumentation ist nicht nur für eine eventuelle Strafverfolgung sinnvoll, sondern auch für die eigene Analyse und die Einführung von nötigen Gegenmaßnahmen.

Alle Pläne nützen nichts, wenn sie nur im Schrank liegen und niemand davon Ahnung hat. Stattdessen sollten sie zunächst als Grundlage für eine interne Weiterbildung von Nutzen sein. Alle Mitarbeiter*innen sollten prinzipiell mit der elektronischen Ausstattung der Räume und Geräte und den vorgestellten Best-Practice-Empfehlungen vertraut sein, sowohl zum Schutz der eigenen Arbeit als auch zur Beratung der Klient*innen. Wichtig ist hierbei zu fragen, an welchen Stellen die Mitarbeiter*innen sich Weiterbildungen oder Unterstützung wünschen; vorstellbar ist auch, dass Leitungen diese Fortbildungen verpflichtend einführen.

Literatur

Center for Internet Security (Hg.) (2019): »CIS Controls«. https://cisecurity.org/controls/ [Zugriff: 4.7.2020].

Electronic Frontier Foundation (Hg.) (2019): »Surveillance Self-Defence. Your Security Plan«. https://ssd.eff.org/en/module/your-security-plan [Zugriff: 15.6.2020].

Ausblick

Effektiver Schutz vor digitaler geschlechtsspezifischer Gewalt

Jenny-Kerstin Bauer, Ans Hartmann und Nivedita Prasad

Die Unterscheidung zwischen analoger und digitaler geschlechtsspezifischer Gewalt dürfte mittelfristig obsolet werden. Wenn digitale Medien und digitale Kommunikation noch selbstverständlicher in das Leben integriert sein werden und der Großteil der Bevölkerung mit ihnen aufgewachsen ist, wird eine solche Unterscheidung nicht mehr relevant für die Beschreibung geschlechtsspezifischer Gewalt sein. Digitale geschlechtsspezifische Gewalt im sozialen Nahraum ist weder ein Phänomen von Einzelfällen noch ein neues Phänomen. Vielmehr ist es geprägt von schnelllebigen technologischen Entwicklungen und unterliegt in vielen Bereichen denselben Dynamiken wie analoge Formen geschlechtsspezifischer Gewalt. Hierzu gehört, dass die Gewalt in der Regel von (einst) vertrauten Personen aus dem direkten sozialen Umfeld ausgeht, den Betroffenen häufig eine Mitschuld an das Erlebte zugeschrieben wird und sie in der Durchsetzung ihrer Rechte oft nicht ernst genommen werden.

Bei digitaler Gewalt kommt erschwerend hinzu, dass diese häufig nicht erkannt oder in ihrer Wirkmächtigkeit als solche wahr genommen wird. Eine Anerkennung dieser Gewalterfahrungen in ihrer gesellschaftlichen und politischen Relevanz – etwa durch Politik, Justiz, Plattformanbieter*innen sowie Entwickler*innen und Produzent*innen im Technologiebereich – findet momentan kaum statt. Inwiefern die fortschreitende Digitalisierung einen Effekt auf das Ausmaß von Partnerschaftsgewalt, Stalking und sexualisierte Gewalt haben wird, lässt sich – nicht zuletzt auch mangels spezifischer Forschung in Deutschland – nur vermuten. Fest steht lediglich, dass die Anzahl geeigneter Tatmittel und Verbreitungswege mit der Digitalisierung weiterwächst und internationale Forschungsergebnisse durchaus auf eine Zunahme einzelner Formen digitaler Gewalt hinweisen (vgl. Royal Melbourne Institute of Technology 2020). Die Erfahrungen aus der Praxis verdeutlich zudem,

dass Informations- und Kommunikationstechnologie (IKT) das Potential hat, Gewalterfahrungen zu amplifizieren und die Gefahr einer Reviktimisierung zu erhöhen.

Aus den hier ausgeführten Problemanalysen sollte jedoch nicht geschlussfolgert werden, dass digitale Medien und das Internet per se Gewalt produzieren oder begünstigen. Vielmehr ist geschlechtsspezifische Gewalt ein gesellschaftlich fest verankertes Problem und auch im digitalem Raum Ausdruck eines Konglomerats an strukturell gefestigten Machtverhältnissen und technologie-gewordener Vormachtstellung. Gesamtpolitische Lösungsversuche, die sich ausschließlich auf Digitalisierungs-Effekte konzentrieren, können zu kurz greifen, wenn sie solche vorgelagerten strukturellen Bedingungen nicht mitdenken oder hinterfragen wollen.

Leerstellen – politische Maßnahmen und Forschungsbedarf in Deutschland

Die missbräuchliche Anwendung von IKT im Rahmen von Partnerschaftsgewalt oder sexualisierter Gewalt hat bisher kaum Eingang in politische Debatten[1] über »Cybersicherheit« gefunden. Digitale Sicherheit wird vor allem dann politisch forciert, wenn wirtschaftliche Güter, digitale Infrastruktur oder von klassischen Cybercrime-Delikten betroffene Bürger*innen geschützt werden sollen (vgl. auch Frey 2020: 39). Aber Digitalisierungsprozesse werden zwangsläufig auch weiterhin beeinflussen, wie Gewalt ausgeübt und Diskriminierung reproduziert wird.

Es können zwei zentrale Bereiche beschrieben werden, die wesentliche Leerstellen im Umgang mit geschlechtsspezifischer digitaler Gewalt aufweisen: Auf der einen Seite wird im Kontext geschlechtsspezifischer Gewalt Digitalisierung zu wenig Platz eingeräumt, auf der anderen Seite werden bei neueren technologischen Entwicklungen die Auswirkungen von Gewalt vernachlässigt. Gleichzeitig scheint die Eindämmung geschlechtsspezifischer Gewalt keinerlei Relevanz bei der Umsetzung und Regulierung technologischer Entwicklungen zu haben. Langfristig erfordert ein effektives Vorgehen gegen digitale Gewalt die Expertise diverser staatlicher und nichtstaatlicher

1 Derzeit hat die Bundesregierung nicht einmal eine Definition von digitaler Gewalt. Siehe hierzu Deutscher Bundestag 2018.

Akteur*innen und benötigt möglichst umfassende Maßnahmen auf gesellschaftlichen, politischen, rechtlichen, technologischen und wirtschaftlichen Ebenen (vgl. auch Frey 2020: 21).

Digitalisierung als Leerstelle im Kontext geschlechtsspezifischer Gewalt

Einige Jahrzehnte nach der ersten öffentlichen Skandalisierung geschlechtsspezifischer Gewalt durch die zweite (westdeutsche) Frauenbewegung sind mittlerweile spezialisierte Unterstützungsstrukturen, gesetzliche Regelungen wie das Gewaltschutzgesetz, eine gewisse Expertise und teils Sonderzuständigkeiten bei Polizei und Justiz sowie politische Zuständigkeiten errungen bzw. erkämpft worden. Das spezialisierte Wissen der engagierten Zivilgesellschaft beeinflusst maßgeblich die Fachdebatten und hält zunehmend Einzug in das Handeln anderer relevanter Professionen und Institutionen. Es gilt nun die Herausforderung zu bewältigen, dass technische Anwendungen und digitale Medien als Teil unseres Alltags und damit auch als Teil von Gewaltdynamiken und Mittel einzelner Gewalthandlungen betrachtet und anerkannt werden.

Vorhandene Expertisen stärken und erweitern

Betroffene und die Unterstützungsstrukturen sind im Umgang mit digitaler Gewalt mit spezifischen Problemstellungen konfrontiert. Um Gewaltsituationen zu erkennen, zu beenden und ein Gefühl von Kontrolle und Handlungsfähigkeit wiederherzustellen oder auch zur Beweissicherung sind häufig aktualisiertes technisches Wissen und Medienkompetenz notwendig. Dieses Wissen muss regelmäßig neu erarbeitet, in die bestehende Expertise zum Umgang mit geschlechtsspezifischer Gewalt integriert oder bei verlässlichen externen Expert*innen abgerufen werden können. Gerade aufgrund chronisch mangelnder Ressourcen ist es eine große Aufgabe, alle Bereiche der Unterstützung, Beratung und Prävention entsprechend anzupassen und auch spezifische Online-Beratungs- und Informationsangebote zur Verfügung zu stellen. Ausreichende und bedarfsgerechte staatliche Finanzressourcen für Fachberatungsstellen und Frauenhäuser sind deshalb eine notwendige, aber keine hinreichende Voraussetzung für eine gelingende Unterstützung bei digitaler geschlechtsspezifischer Gewalt.

Ungeklärt ist bisher die Frage, inwieweit und in welchem Ausmaß in jeder einzelnen auf geschlechtsspezifische Gewalt spezialisierten Einrichtung künftig auch Kompetenzen in den Bereichen Techniksicherheit, Digitalisie-

rung und digitalen Angriffsmöglichkeiten vorgehalten werden sollten. Unstrittig ist hingegen, dass ohne ein Grundverständnis digitaler Gewaltphänomene gute Unterstützung bei geschlechtsspezifischer Gewalt künftig nicht mehr möglich sein wird. Bereits jetzt gibt es Formen geschlechtsspezifischer Gewalt – wie z.B. Stalking – die fast immer auch IKT nutzen. Eine fehlende Expertise hierüber kann für die Betroffenen eine unzureichende Unterstützung zur Folge haben. Neben der Beratung von Betroffenen zeigt sich auch die Notwendigkeit, dass jede dieser Einrichtungen ein Konzept zur Absicherung der eigenen Arbeit gegen digitale Angriffe und zum Schutz ihrer Klient*innen benötigen wird. So stellt sich z.B. für Fachberatungsstellen, Frauenhäuser und andere Schutzeinrichtungen das Erfordernis, die Auffindbarkeit der Bewohner*innen mittels digitaler Ortung oder anderer digitaler Spuren zu verhindern. Hieraus ergibt sich ein enormer und dringender Fortbildungsbedarf. Die Erfahrungen des bff aus dem Projekt »Aktiv gegen digitale Gewalt« zeigen, dass Interesse und Bedarf an spezifischen Fortbildungen zum Thema digitale Gewalt auf Seiten der Fachberatungsstellen größer ist, als die durch das Projekt ermöglichten Kapazitäten.

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

Nicht nur vorhandene Expertisen bei nicht staatlichen Akteur*innen benötigen Stärkung. Um die rechtliche Ahndung von geschlechtsspezifischer digitaler Gewalt in Deutschland zu verbessern, bedarf es vor allem einer Verbesserung der Strafverfolgung durch mehr Ressourcen und Sensibilität bei Polizei und Staatsanwaltschaft.[2] Dabei fehlt es nicht unbedingt an anwendbaren Straftatbeständen, sondern an Ansprechpartner*innen und Wissen über

2 Abzuwarten gilt, inwiefern das Gesetzespaket zur Bekämpfung des Rechtsextremismus und der Hasskriminalität sich positiv für Betroffene digitaler Gewalt auswirkt.

geschlechtsspezifische digitale Gewalt und ihre technischen Voraussetzungen. Beispielhaft hierfür ist § 201a StGB, der vor unbefugten Bildaufnahmen in einer Wohnung oder einem gegen Einblick besonders geschützten Raum schützt. Auffällig ist, dass hier Nacktheit als strafverschärfend nur im Kontext von Minderjährigen thematisiert wird. Dabei dürfte die Grenzverletzung solcher Aufnahmen auch bei Erwachsenen wesentlich wirkmächtiger sein, wenn es sich um Nacktaufnahmen oder Aufnahmen im Schlaf- oder Badezimmer handelt. Hier könnte Rechtsprechung für Klarheit sorgen und hätte zudem möglicherweise auch Präventivwirkung.[3] Auch gilt es abzuwarten, ob die neue gesetzliche Reglung zum »Upskirting« (§ 184k StGB), das nunmehr eine Straftat gegen die sexuelle Selbstbestimmung darstellt, auch eine Verbesserung in diesem Bereich mit sich bringen wird.

Staatliche Bemühungen zur Prävention von Cybercrime beziehen sich aktuell vornehmlich auf betroffene Unternehmen und staatliche Infrastrukturen. Dort wird ein neues Problembewusstsein dahingehend benötigt, dass auch gewaltbetroffene Frauen besonders vulnerabel für digitale Angriffe aus ihrem sozialen Nahraum sind.

Öffentlichkeitsarbeit, Sensibilisierung und Prävention

Eine größere Sichtbarkeit des Themas digitale geschlechtsspezifische Gewalt ist notwendig und hat in der Vergangenheit bereits auch konkrete Wirkung gezeigt. Der bff beobachtet beispielsweise, dass nach dezidierter Öffentlichkeitsarbeit oder Kampagnen[4] vor allem Betroffene über Social Media Kontakt aufnehmen und schildern, dass es ihnen dank dieser Informationen möglich

3 Derzeit (2020) laufen Verfahren, betrieben von Veranstalter*innen des »Fusion Festivals« und Besucher*innen des Festivals »Monis Rache« wegen heimlicher Dusch- und Toilettenaufnahmen, die bei Pornoplattformen hochgeladen wurden. Mit großer Spannung wird der Ausgang des Fusionverfahrens erwartet, welches zunächst eingestellt wurde, da die Staatsanwaltschaft die Rechtsauffassung vertritt, dass Duschen unter freiem Himmel mit Plastikplanen als ein öffentlicher Raum gewertet werden kann, in dem auch heimliches Filmen erlaubt sei (vgl. Schlosser 2020: Min. 39:10). Das Unverständnis über diese Rechtauslegung hat inzwischen dazu geführt, dass der Anwalt des Festivals angekündigt hat hiergegen vorzugehen (vgl. ebd. Min. 39:56). Hier wird deutlich, dass eine konservative Auslegung des Gesetzestextes eine faktische Straflosigkeit solcher Taten zur Folge hätte.

4 Zuletzt war das die bff-Social Media Kampange »digital + real« mit Online-Aktivist*innen aus dem Jahr 2020.

war, eigene Gewalterfahrungen als solche zu benennen und nun Unterstützung zu suchen. Möglicherweise hat dies damit zu tun, dass zuvor medien- und technikbasierte Übergriffe – anders als bei direkten körperlichen/sexualisierten Angriffen – nicht als ›richtige‹ Gewalt klassifiziert wurden.

Viele Betroffene, die ihrem Umfeld und in sozialen Netzwerken von digitalen Gewalterfahrungen berichten oder diesbezüglich mit Behörden Kontakt aufnehmen, machen zudem die Erfahrung, dass die Verantwortung für das Erlebte bei ihnen gesucht wird. Ihr Umgang mit persönlichen Daten und digitalen Medien oder schlicht ihre Sichtbarkeit im digitalen Raum dienen hierbei zur Rechtfertigung von Grenzverletzungen. Auch ein fehlendes Verständnis der Funktions- und Nutzungsweise digitaler Medien, welches häufig auch als Generations-Unterschied wahrgenommen wird, scheint geeignet »Victim Blaming« zu verstärken. Da viele Mechanismen digitaler Gewalt zunächst auf psychischen Komponenten beruhen, wird zudem häufig unterschätzt, welche Wirkung sie entfalten können. Dass eine breitere Sensibilisierung der Öffentlichkeit in der Regel mit einem Anstieg an Anfragen und Unterstützungsbedarf verbunden ist, zeigt vor allem auch die Notwendigkeit umfassender Maßnahmen im Umgang mit digitaler Gewalt. Betroffene, Unterstützer*innen und Fachkräfte, die durch aktuelle Debatten eigene Bedarfe identifizieren, sollten folglich auch entsprechende Anlaufstellen vorfinden. Hierbei bleiben analog bewährte Maßnahmen nach wie vor sinnvoll. Informationen die beispielsweise in Supermärkten, Apotheken und anderen Orten des Alltagslebens zur Verfügung stehen, können Betroffenen den Weg zu Unterstützung erleichtern, die etwa aufgrund digitaler Bedrohungen ihre Nutzung von IKT eingeschränkt oder eingestellt haben.

Für die Sensibilisierung der breiten Öffentlichkeit spielen erfahrungsgemäß unabhängige journalistische Recherchen eine bedeutende Rolle. So haben bereits in der Vergangenheit Berichte über Datenleaks (vgl. z.B. Köver 2019a) von Spionage-Apps und deren Vertrieb durch Zahlungsdienste (vgl. z.B. Köver 2019b) oder über den problematischen Umgang von Pornografie-Plattformen mit heimlich aufgenommen Videos und sexualisierter Gewalt (vgl. z.B. Meineck/Alfering 2019) zu einem größeren Problembewusstsein geführt und zudem die Verantwortung der entsprechenden Anbieter*innen in den Fokus gerückt.

Gleichstellung und Digitalisierung

Auch im Bereich politischer Gleichstellung ist das Thema Digitalisierung angekommen. Im Jahr 2020 hat die Bundesregierung erstmalig eine ressortübergreifende Gleichstellungsstrategie veröffentlicht. Darin werden explizit gleichstellungspolitische Ziele für die digitale Welt formuliert, die sich jedoch hauptsächlich auf wirtschaftliche Aspekte beziehen. Der Zusammenhang zwischen Digitalisierungsprozessen und geschlechtsspezifischer Gewalt findet so lediglich in den Punkten »Arbeits- und Diskriminierungsschutz in der digitalen Arbeitswelt« und der Thematisierung von Diskriminierung durch Algorithmen Berücksichtigung. Dass digitale geschlechtsspezifische Gewalt im sozialen Nahraum ebenfalls die Teilhabe und Gleichstellung in der Gesellschaft verhindert, wird leider auch nicht im Rahmen dieser Strategie diskutiert.

Geschlechtsspezifische Gewalt als Leerstelle im Kontext Digitalisierung

Dass die politische Gestaltung und Begleitung des digitalen Wandels eine staatliche Gesamtstrategie notwendig macht, ist inzwischen unumstritten. Dennoch scheint sich der Großteil der politischen Bemühungen auf die damit verbundenen »wirtschaftlichen und ökologischen Potenziale« (Bundesregierung 2020: 8) zu konzentrieren. Auch wenn die Sicherung des sozialen Zusammenhalts und demokratischer Werte und damit einhergehend auch Hate Speech inzwischen Teil der Diskussionen um digitale Transformationsprozesse ist, wird geschlechtsspezifische digitale Gewalt im sozialen Nahraum als übergreifender potentieller Begleiteffekt kaum mitgedacht. Digitalisierungsprozesse werden auch weiterhin beeinflussen, wie Gewalt ausgeübt und Diskriminierung reproduziert wird. Daher muss die Bekämpfung digitaler geschlechtsspezifischer Gewalt ein wesentlicher Bestandteil staatlicher Digitalisierungsstrategien sein und ressortübergreifend berücksichtigt werden.

Der Missbrauch digitaler Technologie und der damit verbundene Ausschluss von gesellschaftlichen Teilhabemöglichkeiten für Betroffene von digitaler Gewalt ist von grundsätzlicher Bedeutung – und dies nicht nur bei der Sicherung digitaler wirtschaftlicher und staatlicher Infrastruktur. Insofern wäre es zu wünschen, wenn staatliche Digitalisierungsstrategien die Gefährdung bestimmter Gruppen, wie z.B. gewaltbetroffener Frauen, auf allen Ebenen berücksichtigen und Wege finden würden, alle beteiligten Akteur*innen dafür in die Verantwortung zu nehmen.

Verantwortlichkeit von Plattformbetreiber*innen und Internetunternehmen

Aus der Beratungspraxis ist bekannt, dass gewaltbetroffene Frauen in der Vergangenheit zu wenig Unterstützung und Verständnis bei der Sicherung und Wiederherstellung ihrer Online-Konten und Geräte nach digitalen Angriffen erhalten haben. Hier könnten Plattformbetreiber*innen und Unternehmen gesellschaftliche Verantwortung zeigen, indem sie beispielsweise für die Betroffenen einen einfacheren Kontakt- und Meldeweg ermöglichen. Auch könnte das Missbrauchspotential von Anwendungen und Diensten bereits bei der Entwicklung von Produkten minimiert werden, ebenso wie bei der Entwicklung von Algorithmen und künstlicher Intelligenz potenziell Betroffene mitgedacht werden könnten (vgl. Benesch 2020; Mijatović 2018). Sollten diese Unternehmen weiterhin diese Verantwortungen nicht übernehmen wollen, wäre die Gesetzgebung in der Verantwortung dies über entsprechende Maßnahmen zu verändern. Ähnliches gilt für Technologien, die digitale geschlechtsspezifische Gewalt ermöglichen oder sogar ausschließlich für diesen Zweck angeboten werden. Sie haben einen finanzstarken Markt hinter sich und Anwender*innen[5], die selten rechtliche oder soziale Sanktionen befürchten müssen. Betroffenenfokussierte Maßnahmen zum Schutz vor Gewalt und barrierefreie, nutzer*innenfreundliche Sicherheitseinstellungen könnten bereits im Design und der Programmierung vieler Produkte verankert werden; es ist kaum nachvollziehbar warum dies nicht umgesetzt wird. So wäre es denkbar, technische Erkennungsmöglichkeiten von Überwachung serienmäßig in Geräten einzubauen, z.B. durch einen Button mit dem die User*innen einen Hinweis erhalten, dass sie von digitaler Überwachung betroffen sind. So können nicht nur Betroffene eine individuelle Gefährdung erkennen, solche Hinweise sorgen auch dafür, dass digitale Gewalt mehr in den Fokus der Gesellschaft rücken könnte.

Eine weitere Möglichkeit Internetfirmen und IT-Dienste zumindest in finanzielle Verantwortung zu nehmen, wäre die Einführung einer Digitalsteuer, wie sie in anderen Ländern, z.B. Frankreich, bereits existiert (vgl. Ketterer 2019) und daran gebundene Abgaben an Fachstellen für Präventions- und Interventionsangebote gegen digitale Gewalt. Dies würde direkt zur Verbesserung der Situation der Betroffenen beitragen.

Das Internet verspricht ein Ort zu sein, in dem alle Menschen sich austauschen und Informationen erhalten können. Dies ist aber nicht für alle Menschen gleichermaßen möglich, so z.B. für blinde Menschen oder Personen,

5 Siehe Beitrag: Formen digitaler geschlechtsspezifischer Gewalt.

die Informationen in leichter Sprache benötigen oder Personen mit wenig Medienkompetenz. Plattformbetreiber*innen und Internetunternehmen wären hier in der Verantwortung dafür zu sorgen, dass das Internet seinem Versprechen folgt und in der Praxis möglichst barrierefrei ist, nicht zuletzt um eine Gefährdung entsprechender Personengruppen zu minimieren.

Forschung und Monitoring

Das Vorkommen digitaler Gewalt im sozialen Nahraum kann in seiner Komplexität derzeit kaum durch staatlich erfasste Daten abgebildet werden. Die Polizeiliche Kriminalstatistik (PKS) erfasst seit 2011 zur Auswertung von Partnerschaftsgewalt auch die Opfer-Tatverdächtigen-Beziehung (vgl. Deutscher Bundestag 2020: 35). Da aber digitale Gewalt ein breites Feld von möglichen Handlungen beschreibt und es keinen expliziten Straftatbestand gibt, aus dem eine digitale Ausübung automatisch hervorgeht, ist nicht nachvollziehbar, welche erfassten Fälle von beispielsweise Körperverletzung oder sexueller Nötigung auch digitale Komponenten aufweisen. Somit bietet dieser Ansatz keine ausreichende Möglichkeit, um einen Eindruck davon zu gewinnen, welche Rolle digitale Gewalt in den zur Anzeige gebrachten Fällen spielt. Bei der statistischen Erhebung von Cyberkriminalität hingegen wird digitale Gewalt lediglich im Kontext von Identitätsdiebstahl kurz erwähnt, indem darauf hingewiesen wird, dass »Mobbing und Stalking häufig mit einem Identitätsdiebstahl verbunden« (Bundeskriminalamt 2019: 12) sind. Zudem handelt es sich bei den Daten der PKS um Daten aus dem sogenannten polizeibekanntem Hellfeld. Bereits die Anzahl der Fälle bei den Beratungsstellen ist deutlich höher, über das Dunkelfeld gibt es allerdings bisher keine seriösen Erhebungen. Monitoring durch Meldestellen, die Gewalterfahrungen unabhängig von einer Anzeige registrieren, existieren für den Bereich Hate Speech und Kinder- und Jugendschutz im digitalen Raum in Deutschland bereits an diversen Stellen und könnten auch zur Erfassung spezifischer Formen digitaler geschlechtsspezifischer Gewalt sinnvoll sein. Die Forschungslandschaft in Deutschland bleibt in Bezug auf digitale Gewalt bisher vereinzelten Aspekten verhaftet und ist wenig interdisziplinär ausgerichtet. Digitale Gewalt wird vorrangig im Kontext von Kinder- und Jugendschutz oder von Hate Speech wissenschaftlich untersucht.

Die Gleichstellungs- und Frauenminister*innenkonferenz (GFMK) hat zum wiederholten Mal die Bundesregierung aufgefordert eine Studie zum Thema digitale Gewalt in Auftrag zu geben (vgl. GFMK 2020); eine solche

Studie wäre hilfreich um einen ersten Einblick in das Ausmaß geschlechtsspezifischer digitaler Gewalt zu erhalten. Prävalenzforschung ist allein schon in Bezug auf geschlechtsspezifische Gewalt rar gesät. Die letzte durch die Bundesregierung in Auftrag gegebene repräsentative Studie zu Gewalt gegen Frauen wurde 2004 veröffentlicht (Schröttle/Müller 2004). Aspekte digitaler Gewalt wurden, bis auf Stalking mittels E-Mails, nicht abgefragt. Die nächste Prävalenzstudie zu Gewalt gegen Frauen käme nicht umhin sich deutlich mehr für das Thema digitale Gewalt zu öffnen. Um digitale geschlechtsspezifische Gewalt in ihrer Komplexität und mit Erkenntnisgewinn (für die Praxis) abzubilden, wäre es notwendig verschiedene Formen digitaler Gewalt im sozialen Nahraum und deren Kontextabhängigkeit zu untersuchen und dabei einen mehrdimensionalen Erklärungsansatz zu verfolgen. Hierbei wären Erkenntnisse über Prävalenz, Wirkmächtigkeit der Gewalt, Auswirkungen, Zugang zum Recht und Hilfesystem sehr wertvoll und könnten dazu beitragen, Präventions- und Unterstützungsangebote an den Bedarfen der Betroffenen zu orientieren.

(Digitale) Gewalt, die patriarchaler Logik innerhalb der Geschlechterverhältnisse folgt, betrifft nicht nur Frauen, sondern auch weitere marginalisierte Geschlechter wie z.B. trans und nicht-binäre Personen sowie genderfluide und agender Personen. Für diese Gruppen gibt es zum einen kaum Unterstützungsstrukturen, zum anderen werden sie in wissenschaftlichen Untersuchungen selten berücksichtigt. Auch innerhalb einzelner Geschlechtskategorien kann die Erfassung spezifischer Betroffenheiten und Erfahrungen in der Auseinandersetzung mit dem Thema Gewalt den Erkenntnisgewinn erhöhen. Daher wäre es wichtig, auch diese Erfahrungen in künftigen Studien zu beleuchten.

Neben Studien zum Ausmaß geschlechtsspezifischer digitaler Gewalt wären auch spezifische Fragestellungen von Bedeutung. So könnte z.B. eine genauere Analyse der Anwendung digitaler Überwachung und Stalkerware dazu beitragen, das Phänomen des Femizides besser zu verstehen und entsprechende Präventionsprogramme zu gestalten. Neben den Erfahrungen und der Sicht der Betroffenen ist zudem sehr wenig von Seiten der Gewaltausübenden bekannt, zudem fehlt es an einer Analyse spezifischer digitaler Täterstrategien im sozialen Nahraum. Dabei wären vor allem Erkenntnisse aus diesem Bereich von wesentlicher Bedeutung für die Prävention digitaler Gewalt. Ebenso wenig ist über die polizeiliche und juristische Sichtweise auf digitale Gewalt bekannt.

Best practice – transdisziplinäre Bündnisse, spezifisches Monitoring, betroffenenfokussierte Ansätze

Die folgenden Beispiele guter Praxis zeigen, dass dem Themenkomplex digitaler geschlechtsspezifischer Gewalt in unterschiedlicher Weise bereits heute gelingend begegnet werden kann. Viele Projekte sind aus Initiativen zur Selbsthilfe oder dank des beharrlichen Einsatzes von Einzelpersonen entstanden. Einige verfügen über eine (staatliche) Finanzierung und Unterstützung, die es ihnen möglich macht, adäquate Hilfsangebote sowie gut aufbereitete, barrierefreie und zielgruppenspezifische Informationen anzubieten. Teilweise sind bei diesen Projekten Meldestellen für Fälle digitaler Gewalt angesiedelt, die ein Monitoring der Entwicklung digitaler Gewalt und einen bedarfsgenauen Austausch mit Forschenden, Behörden, Plattformbetreiber*innen und Legislative ermöglichen. Zukunftsweisend und notwendig sind zudem transdisziplinäre Zusammenschlüsse und Forschungsansätze, die Expertisen aus Bereichen zusammenbringen, die in Deutschland bisher kaum zusammenarbeiten. So werden neben NGOs und staatlichen Institutionen IT-Sicherheitsfirmen und unabhängige Technikexpert*innen, die sich für Gewaltbetroffene engagieren, auch in Zukunft wichtige unabdingbare Verbündete im Einsatz gegen digitale geschlechtsspezifische Gewalt sein.

NNEDV: National Network to End Domestic Violence und The Safety Net Project, USA

NNEDV[6] ist eine NGO mit Sitz in Columbia, USA und hat über 2.000 Mitgliedsorganisationen. Der Zusammenschluss hat zum Ziel, häusliche und sexualisierte Gewalt zu bekämpfen und die Öffentlichkeit zu sensibilisieren. Eines der zahlreichen Projekte von NNEDV ist »The Safety Net Project« mit Fokus auf IKT im Zusammenhang mit Gewalt gegen Frauen und Kinder. Das Safety Net Project setzt sich für eine starke lokale, staatliche, nationale und internationale Politik ein, die die Sicherheit, Privatsphäre und Bürgerrechte aller Betroffenen von geschlechtsspezifischer digitaler Gewalt gewährleistet und schützen soll. Dafür werden Materialen und Beratungsleitfäden erstellt sowie Apps mit Sicherheitshinweisen für eine gelingende Intervention bei digitaler Gewalt entwickelt. Dazu führt das Projekt u.a. Sensibilisierungs-Trainings für Berater*innen, Polizist*innen, (Staats-)anwält*innen und für andere relevante Fachkräfte durch. Das Safety Net Project ist außerdem Teil

6 https://nnedv.org/content/technology-safety/ [Zugriff: 16.9.2020].

von beratenden Beiratsgremien großer Tech-Unternehmen wie beispielsweise Pinterest, Airbnb, Twitter, Facebook und Uber. Durch diesen fachlichen Austausch, die Zusammenarbeit mit großen Unternehmen und der Praxis der Berater*innen, die sich für die Sicherheits- und Datenschutzrechte von Betroffenen einsetzen, wird gemeinsam herausgearbeitet, welche aktuellen und aufkommenden Technologien die Sicherheit der Betroffenen erhöhen können und welche durch die Täter*innen missbraucht werden. Dieses Wissen fließt wiederum in die Trainings- und Öffentlichkeitsarbeit des Projektes zurück.

Hamara Internet, Pakistan

»Hamara Internet«[7] heißt wörtlich übersetzt »unser Internet« und ist die Pionierkampagne der »Digital Rights Foundation« in Pakistan. Das Projekt zielt darauf ab, die Zunahme von Belästigung im Internet ins öffentliche Bewusstsein zu rücken und hat sich zum Ziel gesetzt, ein freies und sicheres digitales Umfeld für alle Menschen aufzubauen. Durch Sensibilisierungsworkshops, technische Schulungen und die Verbreitung digitaler Sicherheitskits sollen die Fähigkeiten von Frauen und ihre Medienkompetenz gestärkt werden. Zusätzlich bietet Hamara Internet seit 2016 Online-Ressourcen auf Englisch und Urdu zu (digitaler) geschlechtsspezifischer Gewalt sowie eine Beratungs-Hotline zu Online-Belästigung an.

eSafety Commissioner, Australien

»eSafety«[8] ist ein umfassendes Programm der australischen Regierung mit dem Ziel, der Bevölkerung eine sichere und positivere Internetnutzung zu ermöglichen. eSafety, unter der Leitung von Commissioner Julie Inman Gran, hat seit 2015 das Mandat, alle Maßnahmen zu leiten und zu koordinieren, die von Regierungs-, Industrie- und Non-Profit-Organisationen zur Erhöhung der digitalen Sicherheit unternommen werden (eSafety Commissioner 2019: o.S.). Zum Angebot von eSafety gehört unter anderem ein Online-Meldetool für Betroffene von bildbasierter Gewalt (vgl. Johnston 2016). Auch andere Gewalterfahrungen wie »Cyberbullying«, »adult cyber abuse« oder illegale, gewaltvolle Netzinhalte können auf der Seite gemeldet werden (vgl. eSafety Commissioner 2020: o.S.). Betroffene erhalten hier zum einen spezifische Unterstützung bei der Bewältigung der Gewalterfahrungen und zum anderen bei technischen Maßnahmen, z.B. um ein Video oder Bild

7 https://hamarainternet.org/ [Zugriff: 16.9.2020].

8 https://esafety.gov.au/ [Zugriff: 16.9.2020].

zu melden und aus dem Netz zu entfernen (vgl. ebd.). Die Informationen zu digitaler geschlechtsspezifischer Gewalt auf der Webseite von eSafety sind sehr spezifisch, multimedial und auch in Leichter Sprache zugänglich. Es werden ebenfalls Informationen für gewaltbetroffene Frauen aufbereitet, welche sich mit der Sicherheit, Privatsphäre und spezifischen Bedürfnissen auseinandersetzen. Zudem sammelt eSafety Fallgeschichten und wertet diese aus und konzipiert darauf aufbauend Materialen für Betroffene und Unterstützer*innen.

International Coalition Against Stalkerware (CAS)

Die internationale Coalition Against Stalkerware (CAS)[9] ist ein bisher einzigartiger internationaler Zusammenschluss von IT-Sicherheits-Firmen und Organisationen, die sich für Betroffene geschlechtsspezifischer Gewalt engagieren. Die Gründungsorganisationen wollen gemeinsam gegen Stalkerware, häusliche Gewalt, Stalking und Belästigung vorgehen, um das Problemfeld durch gemeinsame Öffentlichkeitsarbeit weltweit bekannter zu machen. Zu den Gründungsmitgliedern gehören international agierende Firmen wie Kaspersky, GData, Electronic Frontier Foundation (EFF), NortonLifeLock und Malwarebytes. Dass diese Firmen sich dezidiert für gewaltbetroffene Personen einsetzen, ein gemeinsames Vorgehen auf Grundlage von Wissens- und Technologieaustausch erarbeiten und dabei maßgeblich die Expertise vornehmlich feministischer NGOs einbeziehen, ist ein Meilenstein in diesem Bereich und hoffentlich zukunftsweisend.

Cornell Tech

Seit 2016 dokumentiert eine Gruppe von Forscher*innen der Cornell Tech in New York, wie Technologien in Gewaltbeziehungen missbraucht werden können. Gleichzeitig leitet diese Gruppe die »Computer Security Clinic«, die in Zusammenarbeit mit dem New Yorker Bürgermeisteramt Betroffene bei geschlechtsspezifischer digitaler Gewalt berät, um diese Form der Gewalt nachhaltig zu beenden und die digitale sowie physische Sicherheit wiederherzustellen. Aktuelle Forschungsergebnisse und technisches Wissen dazu, wie beispielsweise Stalkerware[10] auf dem Smartphone zu finden ist und das Wissen

9 https://stopstalkerware.org/de/[Zugriff: 16.9.2020].

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

aus der Beratungspraxis sind hier eng miteinander verknüpft (vgl. Cornell Tech 2019).

#NetzCourage

#NetzCourage[11] ist ein gemeinnütziger Verein mit Sitz in der Schweiz, der sich aktiv gegen Hassrede, Diskriminierung und Rassismus im Internet stellt und dafür eine »Ambulanz« mit psychosozialer Beratung und rechtlicher Vertretung für Betroffene anbietet. Zusätzlich leistet #NetzCourage Aufklärungsarbeit und nimmt an öffentlichen Podiumsdiskussionen und Kongressen teil, um sich mit anderen Expert*innen auszutauschen und Interessierte zu informieren. Des Weiteren bieten sie Präventionsarbeit in Form von Workshops an Schulen und in Unternehmen an und zeigen auf, wie die Mechanismen von Hassrede im Netz funktionieren.

HateAid

HateAid[12] ist eine deutsche Anlaufstelle, die seit 2018 Betroffene von digitaler Gewalt und Hate Speech unterstützt. Sie vermitteln betroffene Personen an Hilfsorganisationen, bieten Informationen zum Umgang mit Hassrede und stehen mit rechtlicher Vertretung Betroffenen zur Seite. Sie bieten eine kostenlose Erstberatung, bei Bedarf Prozesskostenfinanzierung sowie Sicherheits- und Kommunikationsberatung an. Die rechtliche Vertretung erfolgt durch einen Prozesskostenfinanzierungsfond zur Rechtsdurchsetzung, der sich langfristig solidarisch aus den eingeklagten Schmerzensgeldern finanzieren soll.

Digitale Gewalt in Zeiten von COVID-19

Es ist noch zu früh, um umfassend zu bewerten, wie sich das Leben in Lockdowns, sozialer Isolation und unter Quarantäne-Auflagen auf digitale Gewalt auswirkt. Vielfach wird jedoch ein Anstieg (digitaler) Partnerschaftsgewalt vermutet. Bekannte Phänomene, wie ein erhöhtes Gewaltaufkommen in Zeiten, in denen Partner*innen unter Druck stehen, Ressourcen (wie Einkommen) gefährdet sind, Kinderbetreuung und Lohnarbeit neu zu organisieren sind und/oder mehr Zeit in familiärer Enge dürften während der Pandemie

11 https://netzcourage.ch [Zugriff: 16.9.2020].

12 https://hateaid.org [Zugriff: 16.9.2020].

ihre Wirkung entfaltet haben. Auch ist es zu vermuten, dass während Lockdowns und/oder Quarantäne die Möglichkeit der Kontaktaufnahme nach Außen deutlich erschwert ist.

Wenn jede Online-Aktivität im Heimnetzwerk erfolgt, kann sie potentiell stets überwacht werden. Das Suchen nach Informationen und Hilfe wird dadurch immens erschwert. Wenn Betroffene Überwachung vermuten oder sich dieser bewusst sind, werden sie vielleicht davon absehen, sich online nach Hilfe zu erkundigen. Wenn entsprechende Suchverläufe durch den Täter registriert werden, kann sich die Gefährdungslage lebensbedrohlich zuspitzen. Weltweit gab es Meldungen, die ein erhöhtes Aufkommen von Partnerschaftsgewalt im Kontext der Einschränkungen durch die Pandemie vermuteten. Staaten haben vereinzelt mit schnellen und sehr innovativen Maßnahmen hierauf reagiert. Unklar ist jedoch, welche Rolle digitale geschlechtsspezifische Gewalt hierbei gespielt hat.

Die britische Polizei wies im Sommer 2020 daraufhin, dass digitales Stalking während des Ausbruchs der COVID-19-Pandemie zugenommen habe und Täter ihre Strategien an die Situation anpassten. Sogar Gerüchte über Infektionen mit COVID-19 wurden genutzt, um Betroffene online zu diffamieren und ihnen wirtschaftlich zu schaden (vgl. itv.com 2020). Auch auf das Ausmaß bildbasierter Gewalt scheint sich die Verlagerung sozialer Interaktionen in den digitalen Raum im Zuge häuslicher Isolation auszuwirken. Die Meldestelle des australischen eSafety-Projekts verzeichnete zwischen März und Mai 2020 im Vergleich zum Vorjahreszeitraum einen Anstieg um 210 % der ihnen gemeldeten Fälle. Der größte Anstieg war über das Wochenende zu verzeichnen, an dem die Osterfeiertage lagen und wies allein in diesen Zeitraum eine Steigerung von 600 % im Vergleich zum Vorjahr auf (vgl. Powell/Flynn 2020). Entsprechende Meldungen sind in Deutschland nicht bekannt, nicht zuletzt, weil es keine zentralen Stellen gibt, die solche Betroffenenerfahrungen systematisch erfassen. Es gibt jedoch wenig Grund zur Annahme, dass sich die Situation in Deutschland wesentlich anders darstellt.

Die Beendigung geschlechtsspezifischer Gewalt ist eine gesamtgesellschaftliche Aufgabe, die zukünftig noch mehr an das Voranschreiten der Digitalisierung geknüpft sein wird. Die digitale Transformation aller Bereiche unseres Lebens bringt unzählige Vor- und Nachteile mit sich und macht zwangsläufig eine kritische Auseinandersetzung mit den Folgen notwendig. Gewalt und Diskriminierung sollten jedoch keine Begleiterscheinungen sein, die es in Kauf zu nehmen gilt. Wir stehen erst am Anfang davon zu verste-

hen, inwiefern digitale Transformationsprozesse (Ex-)Partnerschaftsgewalt, sexualisierte Gewalt oder Stalking beeinflussen und begünstigen.

Literatur

Benesch, Susan (2020): »Proposals for Improved Regulation of Harmful Online Content«. https://cyber.harvard.edu/story/2020-06/proposals-improved-regulation-harmful-online-content [Zugriff: 22.7.2020].

Bundeskriminalamt (2019): »Cybercrime. Bundeslagebild 2018«. https://bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2018.html?nn=28110 [Zugriff: 3.9.2020].

Bundesregierung (2020): »Umsetzungsstrategie der Bundesregierung zur Gestaltung des digitalen Wandels«. https://bundesregierung.de/resource/blob/992814/1605036/d71af00f84eb2253ec2435d93fda5b6d/digitalisierung-gestalten-download-bpa-data.pdf?download=1 [Zugriff: 3.9.2020].

Cornell Tech (2019): »Cornell Tech Opens Computer Security Clinic for Victims of Tech-Enabled Intimate Partner Violence«. https://tech.cornell.edu/news/cornell-tech-opens-computer-security-clinic-for-victims-of-tech-enabled-intimate-partner-violence/ [Zugriff: 26.5.2020].

Deutscher Bundestag (2018): »Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Anke Domscheit-Berg, Cornelia Möhring, Dr. Petra Sitte, weiter [sic!] Abgeordneter und der Fraktion DIE LINKE«. BT-Drucksache 19/6174. https://dipbt.bundestag.de/dip21/btd/19/061/1906174.pdf [Zugriff: 23.8.2020].

Deutscher Bundestag (2020): »Schriftliche Fragen mit den in der Woche vom 8. Juni 2020 eingegangenen Antworten der Bundesregierung. Drucksache 19/19887«. https://dip21.bundestag.de/dip21/btd/19/198/1919887.pdf [Zugriff: 23.08.2020].

eSafety Commissioner (2019): »eSafety Commissioner«. https://esafety.gov.au/sites/default/files/2019-10/eSafety%20Overview.pdf [Zugriff: 23.8.2020].

eSafety Commissioner (2020): »Report abuse«. https://esafety.gov.au/report [Zugriff: 23.8.2020].

Frey, Regina (2020): »Geschlecht und Gewalt im digitalen Raum. Eine qualitative Analyse der Erscheinungsformen, Betroffenheiten und Handlungsmöglichkeiten unter Berücksichtigung intersektionaler Aspekte.

Expertise für den Gleichstellungsbericht der Bundesregierung«. https://dritter-gleichstellungsbericht.de/de/article/239.geschlecht-und-gewalt-im-digitalen-raum-eine-qualitative-analyse-der-erscheinungsformen-betroffenheiten-und-handlungsm%C3%B6glichkeiten-unter-ber%C3%BCcksichtigung-intersektionaler-aspekte.html [Zugriff: 14.9.2020].

GFMK (2020): »Medien-Info – Chancen der Corona-Krise nutzen – Geschlechtergerechtigkeit umsetzen vom 25. Juni 2020«. https://gleichstellungsministerkonferenz.de/documents/20-06-25-presseinfo-saarland-zur-sonder-gfmk-2020_1593158268.pdf [Zugriff 16.9.2020].

itv.com (2020): »Police warn stalkers are adapting their methods and increasingly moving online«. https://itv.com/news/2020-07-10/police-warn-stalkers-are-adapting-their-methods-and-increasingly-moving-online-incidents-increase-coronavirus-lockdown [Zugriff: 22.7.2020].

Johnston, Rae (2016): »The Australian Government Is Building A ›Revenge Porn‹ Reporting Tool«. https://gizmodo.com.au/2016/10/the-australian-government-is-developing-a-revenge-porn-reporting-tool/ [Zugriff: 1.8.2020].

Ketterer, Alexandra (2019): »Französische Digitalsteuer: Trumps Regierung droht mit Gegenmaßnahmen«. https://netzpolitik.org/2019/franzoesische-digitalsteuer-trumps-regierung-droht-mit-gegenmassnahmen/ [Zugriff: 12.7.2020].

Köver, Chris (2019a): »Spyware-Firma stellt private Daten von Kunden ins Internet«. https://netzpolitik.org/2019/spyware-firma-stellt-private-daten-von-kunden-ins-internet/ [Zugriff: 3.9.2020].

Köver, Chris (2019b): »Paypal wickelt erneut Zahlungen für eine App ab, die gewalttätige Partner für Stalking nutzen«. https://netzpolitik.org/2019/paypal-wickelt-erneut-zahlungen-fuer-eine-app-ab-die-gewalttaetige-partner-fuer-stalking-nutzen/#vorschaltbanner [Zugriff: 3.9.2020].

Meineck, Sebastian/Alfering, Yannah (2019): »Pornhub und xHamster: Sexualisierte Gewalt bleibt erstmal online«. https://vice.com/de/article/43kbxn/pornhub-und-xhamster-sexualisierte-gewalt-bleibt-erstmal-online [Zugriff: 3.9.2020].

Mijatović, Dunja (2018): »Council of Europe. Safeguarding human rights in the era of artificial intelligence – Human Rights Comment by Dunja Mijatović, Commissioner for Human Rights«. https://coe.int/en/web/genderequality/-/safeguarding-human-rights-in-the-era-of-artificial-intelligence [Zugriff: 24.5.2020].

Powell, Anastasia/Flynn, Asher (2020): »Reports of ›revenge porn‹ skyrocketed during lockdown, we must stop blaming victims for it«. https://theconversation.com/reports-of-revenge-porn-skyrocketed-during-lockdown-we-must-stop-blaming-victims-for-it-139659 [Zugriff: 23.7.2020].

Royal Melbourne Institute of Technology (2020): »Study charts rising trend of image-based sexual abuse. Image-based sexual abuse in Australia is increasing, according to new research«. https://rmit.edu.au/news/all-news/2020/feb/image-based-abuse [Zugriff: 7.9.2020].

Schlosser, Patrizia (2020): »Spannervideos - das heimliche Verbrechen«. [Film] https://ardmediathek.de/daserste/video/reportage-und-dokumentation/spannervideos-das-heimliche-verbrechen/das-erste/Y3JpZDovL2Rhc2Vyc3RlLmRlL3JlcG9ydGFnZSBfIGRva3VtZW50YXRpb24gaW0gZXJzdGVuL2EzYjgxZDVlLTQ5MzktNDJjNC1hMTBlLWI3NmU1YjkyOWVlZA/ [Zugriff 3.9.2020].

Schröttle, Monika/Müller, Ursula (2004): »Lebenssituation, Sicherheit und Gesundheit von Frauen in Deutschland. Eine repräsentative Untersuchung zu Gewalt gegen Frauen in Deutschland (Bericht im Auftrag des Bundesministeriums für Familie, Senioren, Frauen und Jugend)«. https://bmfsfj.de/bmfsfj/generator/RedaktionBMFSFJ/Broschuerenstelle/Pdf-Anlagen/Lebenssituation-Sicherheit-und-Gesundheit-von-Frauen-in-Deutschland,property=pdf,bereich=bmfsfj,sprache=de,rwb=true.pdf [Zugriff 30.8.2020].

Autor*innen

Bauer, Jenny-Kerstin hat einen Master of Social Work – Soziale Arbeit als Menschenrechtsprofession absolviert. Sie arbeitet beim bff: Bundesverband für Frauenberatungsstellen und Frauennotrufe als Referentin für das Projekt »Aktiv gegen digitale Gewalt« und in der Presse- und Öffentlichkeitsarbeit mit dem Schwerpunkt Social Media. Seit 2016 ist sie außerdem selbstständig tätig und spezialisiert auf die Durchführung von Bildungsangeboten und Beratung zu digitaler geschlechtsspezifischer Gewalt für Fachkräfte der Sozialen Arbeit, Polizei und Politik.

Bocian, Andrea hat Gesundheits- und Sozialmanagement (B.A.) studiert und ist als Referentin der Beratungsstelle Frauennotruf Frankfurt tätig. Sie arbeitet außerdem in der Fortbildungs- und Öffentlichkeitsarbeit und in der Koordinierung der hessischen Frauennotrufe.

Clemm, Christina ist Fachanwältin für Strafrecht und Familienrecht in Berlin. Einer ihrer Schwerpunkte ist die Vertretung von Verletzten in Verfahren wegen geschlechtsspezifischer, sexualisierter, lgbtiq*-feindlicher, rassistischer oder sonstiger menschenverachtender Straftaten. Mehrfach war sie als Sachverständige im Rechtsausschuss des deutschen Bundestages und Mitglied der Expert*innenkommission des Bundesministeriums der Justiz und für Verbraucherschutz zur Änderung des Sexualstrafrechts.

Dinig, Nadine, Dr., Rechtsanwältin, hat Soziologie, Geschichte und Philosophie an der Universität Heidelberg und Rechtswissenschaft an der Freien Universität und der Humboldt-Universität Berlin studiert und an der Universität Bremen promoviert. Sie war in Frankfurt a.M. bei verschiedenen Wirtschaftskanzleien beschäftigt und ist seit 2015 als selbstständige Rechtsanwältin tätig. Sie ist Mitglied bei der Arbeitsgruppe Geistiges Eigentum und Me-

dien (AGEM) im Deutschen Anwaltsverein und beim Deutschen Juristinnenbund. Ihre Tätigkeitsschwerpunkte sind Presse- und Medienrecht sowie im Wettbewerbs- und Markenrecht.

Hansen, Helga ist Diplom-Ingenieurin und arbeitet als Redakteurin bei der Technikzeitschrift Make. Zuvor war sie im Gleichstellungsbüro der TU Braunschweig tätig und schrieb für verschiedene Blogs über Netzpolitik, Feminismus und Popkultur.

Hartmann, Ans hat Kommunikationspsychologie studiert und ist seit 2013 in der Geschäftsstelle des bff tätig – seit 2017 mit einem Schwerpunkt auf technik- und medienbasierten Formen geschlechtsspezifischer Gewalt. Weitere Arbeitsbereiche sind: Partizipative Forschung zu kontextualisierter feministischer Traumaarbeit in Fachberatungsstellen, Social Media und Datenschutz.

Klant, Harald hat einen Bachelor of Arts in Sozialer Arbeit an der Alice-Salomon-Hochschule Berlin absolviert. Seine Bachelorarbeit zum Thema »Strategien im Umgang mit Online Hate Speech« wurde 2018 ausgezeichnet mit dem Alice-Salomon-Studienpreis für die innovativste Bachelorarbeit. Derzeit studiert er Gender Studies im Master an der Humboldt-Universität zu Berlin und arbeitet als Berater im Checkpoint BLN, einem Zentrum für sexuelle Gesundheit für queere Menschen in Berlin. Er arbeitet unter anderem zum Thema Diskriminierung von trans*, inter* und nicht-binären Personen sowohl in sozialen Medien als auch im Gesundheitssystem und an der Entwicklung von Gegenstrategien.

Köver, Chris ist Redakteurin von netzpolitik.org und beschäftigt sich dort viel mit digitaler Gewalt. Besonders interessant findet sie derzeit, wie automatisierte Entscheidungen und Überwachung das Leben von marginalisierten Menschen prägen. Chris ist auch eine der Gründerinnen des Missy Magazine, hat in der Redaktion der deutschsprachigen WIRED und als freie Autorin gearbeitet. Vorher hat sie in Lüneburg und Toronto Angewandte Kulturwissenschaften studiert. Egal ob sie Panels moderiert, Sachbücher für Jugendliche schreibt oder zu Stalkerware recherchiert: Ihre Neugier und ihr Interesse an intersektionalem Feminismus, Aktivismus und sozialer Gerechtigkeit prägen ihre gesamte Arbeit.

Lembke, Ulrike, Prof. Dr., ist Professorin für Öffentliches Recht und Geschlechterstudien an der Humboldt-Universität zu Berlin und Leiterin der Humboldt Law Clinic Grund- und Menschenrechte. Ihre Forschungsschwerpunkte umfassen Verfassungs- und Verwaltungsrecht, Antidiskriminierungsrecht, Menschenrechte, Rechtstheorie, transdisziplinäre Rechtsforschung sowie rechtliche Geschlechterstudien.

Lütgens, Jessica, Dr., ist promovierte Erziehungswissenschaftlerin und Mitarbeiterin im Team der Beratungsstelle Frauennotruf Frankfurt. Ihre Forschungsinteressen liegen in Jugend-, politische Sozialisations-, Biographie- und Bildungsforschung. Sie ist außerdem in der pädagogischen und theoretischen Arbeit gegen Sexismus, Rechtsextremismus und Antisemitismus aktiv.

Prasad, Nivedita, Prof. Dr., hat an der FU Berlin Sozialpädagogik studiert und an der Carl von Ossietzky Universität in Oldenburg promoviert. Bis 2013 war sie Projektkoordinatorin bei »Ban Ying«, einer Berliner NGO gegen Menschenhandel. Seit 2010 leitet sie den Masterstudiengang »Soziale Arbeit als Menschenrechtsprofession«. Im Jahr 2012 wurde ihr der Anne-Klein-Frauenpreis der Heinrich Böll Stiftung für ihr Engagement gegen Menschenrechtsverletzungen an Migrantinnen verliehen. Seit 2013 ist sie Professorin an der Alice Salomon Hochschule Berlin für »Handlungsmethoden Sozialer Arbeit und genderspezifische Soziale Arbeit«.

Strick, Jasna hat einen Master of Arts in Germanistik absolviert. Sie arbeitet derzeit als Social Media Redakteurin und Autorin. Als feministische Aktivistin war sie an zahlreichen Projekten online und offline beteiligt unter anderem an #aufschrei und #ausnahmslos. Ihre Themenschwerpunkte sind (Netz-)Feminismus, (Online-)Aktivismus, Geschlechtergerechtigkeit und digitale Gewalt. Sie lebt und arbeitet in Berlin.

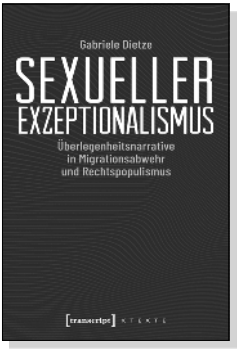
Tanczer, Leonie Maria, Dr., ist Dozentin für »International Security and Emerging Technologies« am Department of Science, Technology, Engineering and Public Policy (STEaPP) des University College London (UCL). Sie ist Mitglied des Beirats der Open Rights Group (ORG), Teil des akademischen Kompetenzzentrum für Cybersicherheitsforschung (ACE-CSR) und ehemaliger Fellow am Alexander von Humboldt Institut für Internet und Gesellschaft (HIIG) in Berlin. Ihre Forschung konzentriert sich auf Fragen der Internetsicherheit und speziell den Schnittpunkten zwischen Technologie,

Sicherheit und Gender. Tanczer leitet das »Gender and IoT« Forschungsprojekt, welches sich mit den Auswirkungen des »Internets der Dinge« (IoT) auf Opfer geschlechtsspezifischer häuslicher Gewalt und Missbrauch auseinandersetzt. Sie ist desweiteren Forschungsmitglied des Netzwerks »Violence, Abuse and Mental Health: Opportunities for Change« (VAMHN) und organisiert regelmäßig digitale Sicherheitstrainings für Frauenberatungsstellen, Akademiker*innen sowie die allgemeine Öffentlichkeit.

Wagner, Angela ist Diplom-Politologin, Geschäftsführerin und Mitarbeiterin im Team der Beratungsstelle Frauennotruf Frankfurt. Sie ist außerdem in der Fortbildungs- und Öffentlichkeitsarbeit und Koordinierung der hessischen Frauennotrufe tätig und als Verbandsrätin im Bundesverband der Frauenberatungsstellen und Frauennotrufe (bff) aktiv.

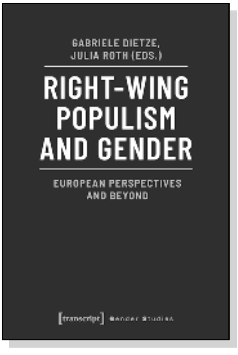
Wizorek, Anne ist freie Beraterin für digitale Strategien, Autorin und feministische Aktivistin. Sie lebt im Internet, in Berlin und ist Gründerin des Grimme Online Award nominierten Gemeinschaftsblogs kleinerdrei.org, den sie fünf Jahre lang als Chefredakteurin leitete. Der von ihr initiierte Hashtag #aufschrei stieß im Jahr 2013 eine Debatte zu Alltagssexismus an und wurde dafür als erster Hashtag mit dem Grimme Online Award ausgezeichnet. In ihrem Buch »Weil ein #aufschrei nicht reicht – Für einen Feminismus von heute«, erschienen im Fischer Verlag, entwirft sie eine moderne feministische Agenda. Unter dem Schlagwort #ausnahmslos veröffentlichte sie im Januar 2016 mit 21 anderen Aktivist*innen ein Statement gegen sexualisierte Gewalt und Rassismus. Als Mitglied der Sachverständigenkommission arbeitete Anne Wizorek am 2. Gleichstellungsbericht der Bundesregierung mit, der im Sommer 2017 veröffentlicht wurde. Im Duden Verlag erschien die Streitschrift »Gendern?!«, in der sie ein Plädoyer für eine geschlechtergerechtere Sprache verfasst hat. Sie ist eine der Initiator*innen des Aufrufs #NetzohneGewalt, der dazu auffordert digitale Gewalt und Hate Speech als gesamtgesellschaftliche Probleme ernst zu nehmen und anzugehen.

Kulturwissenschaft



Gabriele Dietze
Sexueller Exzeptionalismus
Überlegenheitsnarrative in Migrationsabwehr und Rechtspopulismus

2019, 222 S., kart., Dispersionsbindung, 32 SW-Abbildungen
19,99 € (DE), 978-3-8376-4708-2
E-Book: 17,99 € (DE), ISBN 978-3-8394-4708-6



Gabriele Dietze, Julia Roth (eds.)
Right-Wing Populism and Gender
European Perspectives and Beyond

April 2020, 286 p., pb., ill.
35,00 € (DE), 978-3-8376-4980-2
E-Book: 34,99 € (DE), ISBN 978-3-8394-4980-6

Stephan Günzel
Raum
Eine kulturwissenschaftliche Einführung

März 2020, 192 S., kart.
20,00 € (DE), 978-3-8376-5217-8
E-Book: 17,99 € (DE), ISBN 978-3-8394-5217-2

Leseproben, weitere Informationen und Bestellmöglichkeiten finden Sie unter www.transcript-verlag.de

Kulturwissenschaft

María do Mar Castro Varela, Nikita Dhawan

Postkoloniale Theorie

Eine kritische Einführung

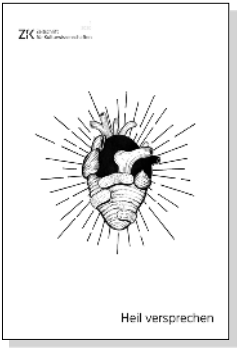
Februar 2020, 384 S., kart.
25,00 € (DE), 978-3-8376-5218-5
E-Book: 22,99 € (DE), ISBN 978-3-8394-5218-9

Thomas Hecken, Moritz Baßler, Elena Beregow,
Robin Curtis, Heinz Drügh, Mascha Jacobs,
Annekathrin Kohout, Nicolas Pethes, Miriam Zeh (Hg.)

POP

Kultur & Kritik (Jg. 9, 2/2020)

Oktober 2020, 178 S., kart.
16,80 € (DE), 978-3-8376-4937-6
E-Book:
PDF: 16,80 € (DE), ISBN 978-3-8394-4937-0



Karin Harrasser, Insa Härtel,
Karl-Josef Pazzini, Sonja Witte (Hg.)

Heil versprechen

Zeitschrift für Kulturwissenschaften, Heft 1/2020

Juli 2020, 184 S., kart.
14,99 € (DE), 978-3-8376-4953-6
E-Book:
PDF: 14,99 € (DE), ISBN 978-3-8394-4953-0

Leseproben, weitere Informationen und Bestellmöglichkeiten finden Sie unter www.transcript-verlag.de