Digitale Gewalt

Kurztitel

Digitale Gewalt

Autoren

Benjamin Thull, Christina Dinar und Felix Ebner

Supplementarische Information $SI\,(5.2)$
zum Kapitel „Soziale Medien, digitale Daten und ihre Auswirkungen auf den einzelnen Menschen“
von den AutorInnen: Cornelia Sindermann, Felix Ebner, Christian Montag, Roland W. Scholz, Sina Ostendorf, Philip Freytag, Benjamin Thull
Unter der Mitarbeit von (in alphabetischer Reihenfolge): Christina Dinar, Hanna Gleiß, Roland Heß, Norbert Kersting, Lisa-Maria Neudert, Christopher Reher, Anna Schenk, Hans-Jörg Sippel

Soziale Kommunikation und Interaktion finden zunehmend digital, ohne direkten Kontakt statt. Möglich machen dies insbesondere die Dienste des Social Web (soziales Internet) und Messengerdienste, über die NutzerInnen leicht miteinander in Kontakt treten und Inhalte jeglicher Art (Texte, Fotos, Videos) austauschen können. Diese Kommunikation über Social Media Dienste, die auch „Disembodied Communication“ genannt wird, führt zu veränderten Rahmenbedingungen und somit einer veränderten physischen Umwelterfahrung (Büchi, Festic, & Latzer, 2018) sowie zu positiven (Boulianne, 2015) und negativen Effekten (Brooks, 2015) auf das Wohlbefinden einzelner Individuen. Während sozialen Medien im Zusammenhang mit den politische Umbrüchen des sogenannten Arabischen Frühlings in Tunesien und Ägypten 2011 noch eine hoff-

nungsvolle Rolle im Sinne der umfassenden Partizipationsmöglichkeiten, der Mobilisierung und der demokratieförderlichen Wirkung zugeschrieben wurde, hat sich diese Einschätzung in der öffentlichen Wahrnehmung mittlerweile eher ins Gegenteil verkehrt: Die Nachrichtenlage wird von Berichten über die massive Zunahme der Verbreitung von hasserfüllten, irreführenden, diskriminierenden und menschenverachtenden Beiträgen über Facebook, Twitter, Instagram und Co. dominiert, welche in Einzelfällen sogar zu gewaltsamen Übergriffen in der offline Welt führten, wie etwa im Fall des Attentats von Halle oder des Mordanschlages auf den Kasseler Regierungspräsidenten Walter Lübcke. Dieses Zusammenfallen einer hohen Relevanz der Interaktion über Social Media Dienste einerseits und der Zunahme zu beobachtender digitaler Gewalthandlungen als „Unseens" dieser Kommunikation andererseits lassen einen genaueren Blick auf die verschiedenen Formen der digitalen Gewalt, ihre Ursachen sowie Maßnahmen zur ihrer Eindämmung sinnvoll erscheinen. Dabei ist zu berücksichtigen, dass es sich lediglich um eine allgemeine Beschreibung der mit dem Bereich der digitalen Gewalt verbundenen Phänomene handelt und insbesondere im Hinblick auf die möglichen Auswirkungen auf das Individuum zu berücksichtigen ist, dass es hier stets bestimmte persönliche Voraussetzungen und gesellschaftlich strukturelle Umweltfaktoren gibt, welche Wirkungen begünstigen oder reduzieren, und eventuell sogar verhindern können. Generell wird digitale Gewalt als eine Formen von Gewalt eingeordnet, die sich technischer Hilfsmittel und digitaler Medien (Handy, Apps, Internetanwendungen, Mails etc.) bedient und im digitalen Raum, z.B. auf Online-Portalen oder sozialen Plattformen stattfindet. Digitale Gewalt funktioniert nicht getrennt von „analoger Gewalt", sondern ist meist eine Fortsetzung oder Ergänzung von bereits existierenden Gewaltverhältnissen und -dynamiken (Hartmann 2017).

Beschreibung der Unseens „Digitale Gewalt"

Dem Unseen „Digitale Gewalt" lassen sich folgende Mechanismen der sozialen Deprivation und Verletzung zuordnen[1]:

Die geschlechtsspezifische digitale Gewalt, die dem Social Pressure zugeordnet werden kann, bildet sich sowohl im Nahbereich als auch in digitalen öffentlichen Räumen ab. Die Betroffenengruppen sind in beiden Fällen mehrheitlich Frauen*, vereinzelt sind auch Männer Opfer. Bei Anwendung digitaler Gewalt in persönlichen Beziehungen (Nahbereich) sind Opfer und Täter einander bekannt – meist handelt es sich um Einzeltäter, oft um ehemalige oder aktuelle Beziehungspartner. Ziel der gesamten Umsetzung der digitalen Gewalt ist es, Kontrolle über die

Kommentiert [MOU1]: Beckedahl:

- Ich bin bei der Anonymitätsdebatte vorsichtiger. Gerade viele marginalisierte Stimmen haben erst durch Pseudonyme / Anonyme Nutzung überhaupt die Chance, ihre Meinung kommunizieren zu können. Das Argument kommt nicht vor, ist aber wichtig, weil man sonst zu dem Ergebnis kommen könnte, dass wir eine Klarnamenspflicht brauchen, um das Problem zu lösen. Gleichzeitig zeigen viele Nazi-Seiten auf Facebook, dass Menschen ihren Hass gerne auch mit Klarnamen und Baby auf dem Arm im Profilbild verbreiten. Siehe https://netzpolitik.org/2018/16-beispiele-warum-pseudonymitaet-im-netz-unverzichtbar-ist/ (Wird später auf Seite 23PDF differenzierter dargestellt)
- Ich finde die Idee von institutionalisierten Beiräten gut, aber ohne klare definition, welche rolle die dann haben, kann das auch eine beschäftigungstherapie mit whitewashing werden.
- Und überhaupt: wo ist der unterschied zu dem neuen aufsichtsboard über content-moderation, was sich facebook gegeben hat (und wo imho sehr gute leute drin sitzen), aber mehr als empfehlungen können die auch nicht geben?
- Den Satz verstehe ich nicht: „Eine Beurteilung, z.B. von Vertretern des Europäischen Parlaments oder anderen erarbeiteten Vorschläge und Gesetzen, sollte ebenfalls Gegenstand von partizipativer Begutachtung werden". Jede EU-Initiative hat das eingebaut, das ist ein demokratischer Prozess.
- Punkt 6: Den Nummerschild-Ansatz halte ich für sehr gefährlich, denn damit wird die Möglichkeit zur Massenüberwachung ausgebaut. Und ich kann mir nicht vorstellen, wie der Zugriff auf diese Daten gesichert werden soll.

andere Person durch Bedrohung, Erpressung oder Diffamierungen auszuüben. Dies erfolgt über technische Möglichkeiten wie Spyware, Fotos, die verschickt werden, oder auch beleidigende Nachrichten in Messengerdiensten und Social Media, die meist nach einem Identitätsdiebstahl im Namen der Betroffenen verschickt werden. Im öffentlichen Raum der Social Media Dienste wird digitale Gewalt häufig in Form von Hassrede und herabwürdigenden Äußerungen sichtbar. Ein bekanntes Beispiel ist die Grünenpolitikerin Renate Künast, die sich im September 2019 gerichtlich gegen die verbalen Angriffe auf ihre Person wehrte. Digitale Gewalt / Hatespeech wird auch häufig gegen gesellschaftliche Minderheiten verübt (unabhängig davon ob sie sich selbst als solche identifizieren) – also MigrantInnen, Geflüchtete, Women of Color, Personen mit anderer Hautfarbe, LGBT*QI, JüdInnen, MuslimInnen oder auch Personen mit Behinderung. Alle diese Faktoren können die Angriffsfläche für digitale Gewalt als Hatespeech begünstigen. Häufig wird diese Potenzierung der Anfälligkeit für diese Mechanismen digitaler Gewalt im öffentlichen Diskurs jedoch übersehen. In den öffentlichen Räumen, anders als im Nahbereich, sind sich Opfer und Täter selten bekannt, vielmehr geht es um digitale Gewalt als ein Instrument der gesellschaftlich-strukturellen Unterdrückung (bff e.v. 2020). Hier geht es um das Verfügen über öffentliche Räume und Ressourcen und die Sichtbarkeit von auch streitbaren Meinungen.. Diese Form der digitalen Gewalt ist häufig gefährdend für einen vielfältigen Diskurs und eine demokratische Diskussionskultur – in der jede*r sich beteiligen darf und sollte – aber in einem schützenden und respektvollen Miteinander. Digitale Gewalt oder im speziellen Hatespeech gegen Frauen (auch als Cybersexismus bezeichnet) werden normalisiert und häufig im Kontext der Anonymität getätigt – auch weil die TäterIn sich sicher fühlen und meist keine weitere soziale Ächtung, Ausschluss aus den Sozialen Netzwerken oder Strafverfolgung im „real Life“ befürchten müssen. Für Betroffene digitaler Gewalt geht die Erfahrung des sozialen Drucks häufig sowohl mit psychischen Belastungen , als auch mit somatischen Erscheinungen wie Kopfschmerzen, Übelkeit und Erbrechen und Hautkrankheiten sowie Ängsten, Depressionen und Suizidgedanken einher. Die Erfahrung digitaler Gewalt kann existenzbedrohend für die Betroffen sein und erhebliche Ressourcen binden (Lembke 2017) und führt vielfach dazu, entweder sich selbst und die eigenen Aussagen bei Sozialen Netzwerken einer Selbstzensur zu unterziehen, (sog. „Silencing“), oder auch die Sozialen Netzwerke gänzlich zu verlassen (Geschke et. al.2019).

Neben solchen Prozessen und deren Folgen ergeben sich in sozialen Medien weitere unerwünschte Konsequenzen hinsichtlich sozialen Drucks durch beispielsweise „Online-Trolling“, und „Cyber-Mobbing“. Jede dieser Verhaltensweisen soll zu einer Herabsetzung mindestens einer Person führen – kann sich aber auch gegen ganze Gruppenzuschreibungen wenden. Finden sich in sozialen Medien vermehrt menschenverachtende Äußerungen, kann dies in einer Spirale aus sich verstärkenden Hassbotschaften münden und dadurch ein Klima entstehen, in dem Diskriminierung und Gewalt legitim erscheinen und die Meinungsvielfalt insgesamt leidet, da sich Minderheiten und auch Frauen zunehmend aus öffentlichen Debatten zurückziehen oder sich online immer weniger beteiligen – wie das Beispiel der Online-Enzyklopädie Wikipedia belegt, die seit Jahren einen AutorInnenschwund beklagt und bei der insbesondere Frauen unterrepräsentiert sind. Dies wirkt sich unweigerlich auch auf die Wissensproduktion und Vielfalt von bereitgestellten Informationen aus.

Auch das so genannte „Doxxing“ (engl.: dox, Abkürzung für documents), bei dem persönliche Daten in bösartiger Absicht ins Netz gestellt werden, stellt nicht nur einen Eingriff in die Privatsphäre dar, sondern wird häufig genutzt, um eine Person bloßzustellen und u.U. weiteren Angriffen auch in der Offlinewelt auszusetzen. Auch Phänomene wie „Cyberstalking“, ungewünschte Kontaktaufnahmen, „Revenge-Porn“, „Upskirting“ (engl. unter den Rock blicken, heimliche Fotos des Intimbereichs) und viele weitere können Grundlage negativer Emotionen und im Allgemeinen unerwünschter Konsequenzen für NutzerInnen sein. Nicht zu unterschätzen sind dabei die technischen Hilfsmittel, die angewandt werden, wie etwa Mikrokameras oder Spyware auf Handys. Eine internationale Studie zu Intimate Partner Violence (IPV) zeigt sehr deutlich, dass 71% im Kontext von Partnerschaftsgewalt ihre Partner über Computer überwachen (IVP reports, 2019).

Ursachen und Erklärung zur Entstehung dieses Unseens / Rebounds

Die Ursachen und Auslöser jeglicher Form von physischer und psychischer Gewalt sind vielfältig, von Fall zu Fall unterschiedlich und können daher hier nicht allumfassend beschrieben werden. Grundsätzlich lässt sich jedoch feststellen, dass Gewalt-

akte oftmals auf einen spezifischen emotionalen Zustand auf Seiten der TäterInnen zurück zu führen sind, der in unterschiedlicher Intensität und auch Kombination von Gefühlen wie Unzufriedenheit, Unmut, Verzweiflung, Angst, Bedrohung, Verärgerung, Überforderung oder Unwissenheit geprägt ist. Nicht jeder ist in gleichem Maße in der Lage, mit diesen Emotionen reflektiert, besonnen oder sozialadäquat umzugehen, weshalb zuweilen als (einzig) möglicher Ausweg aus dieser krisenhaften Situation nur der - im wahrsten Sinne des Wortes - gewaltsame Befreiungsschlag gesehen wird. Aber auch extremistische Gruppen oder Polit-Strategen üben bewusst Gewaltakt aus, um Personen(-gruppen) mundtot zu machen, zu bedrohen oder anzugreifen. Ziel ist dabei oftmals die Atomisierung der Gesellschaft in Individuen, um diese dann gezielter manipulieren und eine neue Gesellschaft nach den eigenen Vorstellungen aufbauen zu können. Mit dem Aufkommen von Social-Media Diensten und den damit verbundenen Möglichkeiten der digitalen Interaktion sind nun neuartige Kommunikationskanäle hinzugekommen, die sich aufgrund ihrer Ausgestaltung offensichtlich besonders für die Ausübung digitaler Gewaltakte eignen. Einige dieser strukturellen Merkmale von Social-Media- Diensten, die digitale Gewaltakte begünstigen, sollen im Folgenden aufgezeigt und beschrieben werden.

- Eine wichtige Neuerung im Umfeld der sozialen Medien im Vergleich zur analogen („offline“) Kommunikation stellt die eingeschränkte Bereitstellung privater, personenbezogener Daten für andere NutzerInnen dar. Aus der so entstehenden Anonymität von NutzerInnen entsteht ein **Konflikt zwischen Anonymität versus Verantwortung** im sozialen Umgang. Durch die gesteigerte Anonymität, aber auch durch die räumliche Distanz zu anderen NutzerInnen, können antisoziale Verhaltensweisen verstärkt werden, die schon aus der Offlinewelt bekannt sind. Wie bei der Übernutzung gibt es hier eine größere Anzahl von psychologischen Mechanismen, die es erlauben NutzerInnen in ihrem Selbstbild zu beeinflussen, sie zu beleidigen, deprivieren, verletzen, mobben, in verschiedener Art unter Druck zu setzen oder zu entwürdigen. Wichtig ist, dass diese Verhaltensweisen im Internet und sozialen Medien aufgrund der Anonymität und der räumlichen Distanz (dem Opfer nicht in die Augen sehen zu müssen), noch wesentlich

Kommentiert [SN2]: Mir bereitet dieser Absatz latent Bauchschmerzen weil er sich ein bisschen wie TäterInnen-Entlastung liest, also als ob viele TäterInnen im Prinzip aus einer Notlage heraus agieren würden usw. – das finde ich unglücklich. Motive sind sicher auch im Fall von digitaler Beziehungsgewalt oft Macht-Streben und (männliche) Aggressivität usw.

Kommentiert [SN3]: Es würde der differenzierteren Darstellung helfen auch darauf hinzuweisen, dass die Möglichkeit online unter Pseudonym soziale Kontakte zu pflegen usw. auch auf der anderen Seite eine Schutz-Funktion darstellt für Menschen, die unter Bedrohungen leiden. Daher kämpfen diverse Gruppen (und Aufsichtsbehörden) auch schon lange für das „Recht auf Pseudonymität im Netz“.

schlimmer ausfallen, als in der Offlinewelt. Ein Effekt, der auch „**Online-Enthemmungseffekt**“ genannt wird.

- Die **effektive Rechtsdurchsetzung** gegenüber den UrheberInnen strafrechtlich relevanter Inhalte wie Volksverhetzung, Holocaustleugnung etc. kann auch höchst problematisch werden. TäterInnen nehmen die digitale Sphäre häufig als quasi rechtsfreien Raum wahr, in dem sie ungehemmt auch strafbare Inhalte posten können, ohne Konsequenzen fürchten zu müssen – auch weil Ihnen die Plattform eine gewisse Anonymität bietet. Das Netzwerkdurchsetzungsgesetz (NetzDG) hilft bei der Rechtsdurchsetzung[2] – es verpflichtet soziale Netzwerke mit über 2 Millionen NutzerInnen zu handeln und binnen einer Fristen von 24 Stunden bis einer Woche den Post auf Grundlage von Kriterien herunterzunehmen. Darüber hinaus sind die Plattformen verpflichtet, regelmäßig Berichte über gelöschte und gemeldete Inhalte zu veröffentlichen. Insgesamt wird das Gesetz aber als privatisierte Rechtsdurchsetzung kritisiert, da nun außerhalb des Legalitätsprinzips stehende Unternehmen darüber entscheiden, ob ein Inhalt strafrechtlich relevant ist oder nicht. Ferner führt vielfach das schnelle Löschen von problematischen Inhalten in Kombination mit dem Ausbleiben strafrechtlicher Konsequenzen auch zum Ausbleiben eines generalpräventiven Effektes auf Seiten der TäterInnen. Eine neue, im Juni 2020 vom Bundestag verabschiedete Fassung des NetzDG sieht daher vor, dass bestimmte, strafrechtlich relevante Inhalte zukünftig nicht nur gelöscht, sondern durch die sozialen Netzwerke zur Strafverfolgung auch an das Bundeskriminalamt weitergeleitet werden müssen. Diese gesetzlichen Maßnahmen müssen jedoch auch mit einem Aufstocken der Ressourcen bei Polizei und Strafverfolgungsbehörden einher gehen, um in der Praxis Wirkung zu entfalten.

- Ein weiteres strukturelles Merkmal von Social-Media-Diensten, welches diese als Kommunikationskanal für die Verbreitung digitaler Gewalt attraktiv macht, ist die nahezu **unbegrenzte Reichweite**, die mit jeglicher Äußerung erzielt werden kann. Über soziale Netzwerke kann potenziell jeder jedem zu jeder Zeit jeden Inhalt in Sekundenschnelle zugänglich machen. Gleich-

zeitig ist es nahezu unmöglich, einen einmal im digitalen Raum verbreiteten Inhalt gänzlich zu löschen, unzugänglich zu machen oder seine Weiterverbreitung zu unterbinden. Der digitale Gewaltakt über Social-Media Dienste kann damit eine massive und nachhaltige Wirkmacht erlangen – insbesondere weil vielfache Kopien trotz Löschung entstehen und an andere Stelle im Netz verbleiben oder immer wieder auftauchen können – dies gilt z.B. auch für das veröffentlichen privater Daten (Doxxing). Dadurch ergeben sich häufig auch noch lange nach den eigentlichen Angriffen andauernde Probleme für die Betroffenen solcher Attacken.

- Social-Media Dienste ermöglichen in einer noch nie zuvor dagewesenen Art und Weise die Möglichkeit, Menschen mit gleichen Interessen und gleicher Gesinnung zu finden, sich mit diesen zu vernetzen und sich gegenseitig – im positiven wie im negativen Sinne - zu bestärken. Auch diese Form der **„Solidarität“** kann die Verbreitung digitaler Gewalt befeuern, nämlich dann, wenn bei den TäterInnen der Eindruck entsteht, dass es noch ganz viele andere Mitmenschen gibt, die die gleichen Ansichten vertreten und die diese somit in ihrem Tun zusätzlich bestärken und zum Weitermachen animieren.
- Ein weiteres wichtiges Merkmal von Social-Media Diensten ist die **Emotionalisierung der Kommunikation**. Das Systemdesign der einschlägigen Plattformen ist nicht primär auf sachlichen Austausch oder gar Konsensbildung ausgerichtet, sondern auf die Erzeugung von positiven Emotionen auf Seiten der NutzerInnen. Machen diese beständig positive emotionale Erfahrungen bei der Nutzung des Dienstes, kehren sie auch regelmäßig zu ihm zurück und sichern somit den Erfolg des Geschäftsmodells. Die Dienste richten daher ihr gesamtes Design genau auf diesen Aspekt aus: über „Like-Buttons“ unterschiedlicher Ausprägung lassen sich Anerkennung, Zustimmung oder Bewunderung zum Ausdruck bringen. Um diese wertvolle digitale Emotionswährung zu erhalten, muss man sich möglichst von der Vielzahl der gepostеten Beiträge abheben und diese im besten Fall übertreffen. Somit entsteht eine Art digitaler Bieterwettbewerb beim Buhlen um virtuelle Anerkennung, was mit Blick auf die Verbreitung

digitaler Gewaltakte nicht selten dazu führt, dass diese immer extremer werden, in der Hoffnung, von der eigenen Community oder auf digitalen Plattformen allgemein möglichst viel Aufmerksamkeit, Zustimmung und Anerkennung zu erhalten. Dazu kommt eine algorithmische technische Strukturierung der Plattform, so dass den UserInnen immer thematisch Ähnliches angezeigt wird bzw. besonders polarisierende Beiträge stärker gewichtet und diese z.B auf der Startseite des Angebotes prominent platziert werden und damit ihre Auffindbarkeit durch die Einflussnahme der digitalen Plattform künstlich erhöht wird.

Kommentiert [SN4]: Hier sollte evtl. noch auf den Mechanismus der algorithmischen Verstärkung immer emotionaler aufgeladener Inhalte hingewiesen werden, also dass sozuagen eine Spirale der Emotion und Zuspitzung in die Systeme einprogrammiert wird.

An welchen Zielen orientiert sich ein Umgang mit den Unseens

Bei der Frage der Zielorientierung im Umgang mit dem Unseen „Digitale Gewalt" gilt es, die Bedarfe auf Seiten der involvierten Akteure – TäterInnen, Betroffene, Social-Media Provider und den Strafverfolgungsbehörden – zu berücksichtigen

Auf Seiten der TäterInnen muss ein Bewusstsein geschaffen werden, dass das Netz nicht mehr als rechtsfreier Raum wahrgenommen wird und dass ihr Handeln nicht folgenlos bleibt. Über eine verstärkte Rechtsdurchsetzung mit Hilfe des NetzDG[3] (NetzwerkDurchsetzungsGesetz– NetzDG, seit 2017) hinaus müssen Effekte erzielt werden, der potenzielle TäterInnen von der Ausübung digitaler Gewaltakte abhält. Dies kann über verstärkte Präventionsarbeit erfolgen.

Antisoziales Verhalten muss bekämpft werden, indem die gefühlte sozial-mediale Distanz zu Betroffenen abgebaut und Empathie eingeübt wird. Dies sollte in die technischen Entwicklung und die Standards von Social Media Plattform Eingang finden und könnte z.B. mittels allgemein und rechtlich anerkannter, transparent überprüfbarer und ethisch begründeter Entwicklungs- und Betriebsprozesse sowie Zertifikaten und Auditierungen seitens der globalen Unternehmen geschehen.

Die Adressaten digitaler Gewalt müssen dazu befähigt werden, sich aus ihrer Betroffenenrolle zu befreien bzw. im besten Fall gar nicht erst zu Betroffenen zu werden. Dazu gehören präventive Maßnahmen wie die Aufklärung über das Phäno-

men selbst als auch die Bekanntmachung von bestehenden Hilfsangeboten – wie z.B. Beratungsstellen, die Betroffene geschlechterspezfischer - auch digitaler - Gewalt beraten und unterstützen oder die zahlreichen Medienkompetenzangebote der Medienanstalten. Ferner müssen psychologische Hilfsangebote zur Verfügung stehen, mit denen negative Folgen digitaler Gewalt professionell begleitet und bewältigt werden können – diese sollten online und offline angeboten werden und auch im Bereich der geschlechtsspezifischen digitalen Gewalt sensibilisiert sein oder auf die professionellen Angebote verweisen können.

Die Provider von Social-Media Diensten sind wirtschaftliche Profiteure der über ihre Plattformen stattfindenden Kommunikation. Sie müssen daher ihrer Verantwortung gerecht werden und über die Ausgestaltung ihrer Dienste dafür sorgen, dass die Verbreitung unterschiedlichster Formen von digitaler Gewalt nicht befördert, sondern weitestgehend verhindert wird. Ein Rückzug auf den Standpunkt, lediglich Anbieter einer technischen Infrastruktur zu sein, ist ungenügend. Es ist nach Verfahren zu suchen, in denen etwa Selbstverpflichtungsmassnahmen von Betreibern von Sozialen Netzwerken zur Unterbindung von kritischen Informationen wirkungsvoll zu Anwendung kommen. Die Einrichtung von Beiräten mit bestimmten Rechten wäre hier eine Option. Facebook beschreitet aktuell diesen Weg über die Einrichtung eines Oversight Boards, welches einen interessanten Diskussionsansatz hinsichtlich der wünschenswerten institutionellen Ausgestaltung (Zusammensetzung, Aufgaben, Rechte etc.) bietet.

Strafverfolgungsbehörden und Polizei benötigen eine Sensibilisierung für das Problem der digitalen Gewalt und müssen ihre Aufgabe erkennen, diese Gewaltakte ernst zu nehmen – auch wenn sie zunächst „nur digital“ erscheinen – so können diese die Fortsetzung von bestehenden Machtverhältnissen darstellen – nur eben mit digitalen Mitteln. Dazu ist es wichtig den Betroffenenschutz auf allen Ebenen zu gewährleisten und nachhaltiger als bisher zu bearbeiten. Immer noch machen Betroffene digitaler Gewalt zu oft die Erfahrung, dass ihren Anzeigen nicht ernsthaft nachgegangen wird oder sie die Empfehlung erhalten, doch einfach soziale Medien nicht mehr zu nutzen (Opfer-Täter-Umkehr, Victimblaming). Hier muss weite-

re Sensibilisierungsarbeit für den Bereich der digitalen Gewalt erfolgen. In diesem Kontext wurde u.a. in NRW bereits 2016 eine erste Schwerpunktstaatsanwaltschaft eingeführt (Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC), die seit 2018 sich auch mit Hassrede beschäftigt. Weitere Bundesländer wie Bayern und Hessen zogen in der Folge mit Sonderdezernaten zu Hatespeech nach.

Welche Maßnahmen sind für welche Ziele sinnvoll

Bei einer Ableitung von Maßnahmen sind eine Reihe von Abwägungsprozessen, Dilemmas und Konflikten zu beachten. Zu letzteren gehören, dass eine große Anzahl (ca. 90%[4]) der Interaktionen (VPN-) verschlüsselt vor sich gehen. So steht etwa der Wunsch nach der Schaffung von rechtlichen Rahmenbedingungen, die es in begründeten Fällen ermöglichen, die Anonymität der TäterInnen aufzuheben und ihre wahre Identität zu ermitteln, in Konflikt mit dem Ziel, durch Verschlüsselung den NutzerInnen Anonymität und (Daten-)Sicherheit zu gewährleisten. Es besteht zudem das Problem, dass die großen Anbieter von sozialen Medien weltweit operieren, es aber verlangt wird, den jeweiligen nationalen Gesetzen zu genügen. Wir denken, dass für diese grundsätzlichen Probleme die EU einen erfolgversprechenderen Rahmen bildet als der nationale Rahmen, da es wenig machbar und sinnvoll erscheint, diverse nationale Regelungen zu realisieren.

Es braucht eine Form institutionalisierter Schnittstellen (etwa in Form von Beiräten oder Aufsichtsräten) und rechtlicher Rahmenbedingungen, die es erlauben, die Anbieter sozialer Medien wirkungsvoll zur Unterbindung von Digitaler Gewalt zu bringen. Dies würde eine Erweiterung des NetzDG (siehe Vertiefende Anmerkung 2) bedeuten. Eine solche Erweiterung würde eine Erweiterung der Haftungspflicht der Anbieter von sozialen Medien bedeuten. Ob und inwieweit weitergehende Maßnahmen im europäischen Rahmen (und in Einzelfällen national) zu ergreifen sind, sollte in geeigneten Verfahren der öffentlichen Beteiligung (partizipativen Verfahren) mit Vertretern aus allen Stakeholdergruppen vordiskutiert werden. Eine Beurteilung, z.B. von Vertretern des Europäi-

Kommentiert [SN5]: Eine wichtige Sache wird hier nicht thematisiert, bzw. als gegeben angenommen. Nämlich die Tatsache, dass de facto exekutive Gewalt auf die Plattformen „abgewälzt" wird mit dem NetzDG. Es wäre ja alternativ auch möglich, die verfassten Strafverfolgungsbehörden besser auszustatten und derartige Delikte nach Rechtslage verfolgen zu lassen. Die Übertragung derart heikler Rechtsakte (Eingriff in Meinungsfreiheit etc.) auf kommerzielle Anbieter sollte kritisch gewürdigt werden.

schen Parlaments oder anderen erarbeiteten Vorschläge und Gesetzen, sollte ebenfalls Gegenstand von partizipativer Begutachtung werden.[5] Aktuell steigt die EU Kommission hier in die öffentliche Konsultation zum sogenannten „Digital Services Act“ ein, bei dem es u.a. auch um Fragen des zukünftigen Haftungsregimes bei sozialen Netzwrrken sowie den Umgang mit Hassrede und Desinformation gehen soll.[6]

Da jeder potenziell sowohl zum/zur TäterIn als auch zum Betroffenen digitaler Gewalt werden kann, ist eine universelle, präventive Aufklärungsarbeit unerlässlich, um bei allen Akteuren ein Bewusstsein für die Problematik zu schaffen. Diese Art von Aufklärung und Medienkompetenzschulung muss möglichst früh beginnen, da sich Kinder mittlerweile bereits sehr früh im Netz bewegen, dort kommunizieren, jedoch die möglichen Konsequenzen ihres Handelns und die Rahmenbedingungen der digitalen Interaktion aus entwicklungspsychologischen Gründen meist noch nicht einschätzen können. Aber auch die heutige Elterngeneration, die z.T. auch sehr unbedarft mit digitalen Kommunikationsmöglichkeiten umgeht, muss sensibilisiert werden (Stichwort „Sharenting“ und die damit verbundene Verletzung der Persönlichkeitsrechte der Kinder). Ihr Umgang mit Medien beeinflusst maßgeblich das Verhalten ihrer Kinder und deren Vorstellung davon, was erlaubt, möglich und gesellschaftlich akzeptiert ist. In diesen Zusammenhang fällt auch die Stärkung potenzieller Betroffener von digitaler Gewalt: Ihnen müssen Hilfsangebote und Anlaufstellen zur Verfügung gestellt werden, die sie über ihre Rechte und Möglichkeiten aufklären und sie bei der Überwindung ihrer Krise beraten und begleiten. Unerlässlich ist hier auch die gezielte Schulung und Sensibilisierung von psychologischem Fachpersonal.

Provider von Social-Media Diensten sollten transparenter über ihre Löschvorgänge berichten und Meldeverfahren einheitlich und userInnenfreundlich (max. 3 Clicks) gestalten. Ferner müssen die Dienste leicht zugängliche Meldemöglichkeiten für die Betroffenen digitaler Gewalt vorhalten, über die diese eine schnelle Löschung/Beseitigung des Inhalts erwirken können. (Wiederholungs-)TäterInnen müssen konsequent von der Plattform ausgeschlossen werden. Systemdesign-Elemente, die die Verbreitung digitaler Gewalt begünstigen, sollten überarbeitet oder ganz entfernt werden. Auch gegen-

über den NutzerInnen sollte klar kommuniziert werden, dass jegliche Formen digitaler Gewalt zum sofortigen Ausschluss aus dem Dienst führen und dass die entsprechenden Nutzerdaten im Falle von strafrechtlich relevanten Inhalten an die Strafverfolgungsbehörden weiter gegeben werden.
Darüber hinaus sollte eine

- Klärung erfolgen, ob digitale Gewalt als Computerkriminalität (Cybercrime)[7] einzustufen ist,
- unabhängige Clearingstelle zur Klärung von Fällen – vorgeschaltet einem Gerichtsverfahren – geschaffen werden, welche die NutzerInnen über Rechte und Pflichten gegenüber Plattformen und Sozialen Medien informiert,
- eine Verstärkung des Bundesamt für Sicherheit und Informationstechnik so erfolgen, dass gewaltfördernden Aspekten von Technik (z.B. Spyapps/Spyware) stärker eingeschränkt werden und unabhängige, bestehende Beratungsstrukturen gegen Gewalt mit hinreichenden digitalen Kompetenzen und Technik ausgestatt werden.

Begründung für die Orientierungen

Um die Gefahr/das *Unseen* der Digitalen Gewalt zu vermindern, müssen auf europäischer Ebene institutionalisierte Schnittstellen (z. B. Beiräte für soziale Medien) und rechtliche Rahmenbedingungen geschaffen werden. Präventive Medienkompetenzangebote und professionelle Hilfsangebote, wie beispielsweise Notrufzentralen auf nationaler Ebene, sollten verstärkt eingerichtet werden, besonders vulnerable NutzerInnen sind zu berücksichtigen. Dienste sozialer Medien müssen einheitliche und nutzerfreundliche Meldeverfahren anbieten und transparent über Löschvorgänge berichten.

Die Auseinandersetzung mit dem Unseen „Digitale Gewalt“ zeigt, dass wir es mit einem Phänomen zu tun haben, das an der Schnittstelle sorgfältig abzuwägender Rechtsfragen bzw. den damit verbundenen Möglichkeiten staatlicher Intervention, der weitergehenden Verantwortungsübernahme privatwirtschaftlich organisierter Unternehmen, der präventiven Aufklärung und (Fort-)Bildung aller Personen, die sich privat oder beruflich mit Social-Media-Diensten beschäftigen sowie der Bereitstellung von Hilfsangeboten für Betroffene zu verorten ist. Alle Überlegungen zur effektiveren Rechtsdurchsetzung, Strafverfolgung und Täteridentifizierung müssen stets sorgsam im Hinblick auf eine Wahrung anderer Rechtsgüter wie Meinungs- und Informationsfreiheit und die möglichen Folgen für unsere freiheitlich-demokratische Grundordnung diskutiert und hinterfragt werden. Hier müssen auch die Anbieter von Social-Media-Diensten über die Ausgestaltung ihrer Dienste und die Ausarbeitung und Evaluierung ihrer Selbstverpflichtungsmaßnahmen einen Beitrag leisten und sich am Diskurs beteiligen. Gleichzeitig muss gewährleistet werden, dass jeglicher Form digitaler Gewalt effektiv begegnet werden kann, insbesondere um Meinungsvielfalt und gewaltfreie Diskurse zu ermöglichen und das Netz zu einem Kommunikationsort zu machen, an dem sich jeder Mensch unabhängig von Alter, Geschlecht, Herkunft, sexueller Orientierung etc. angstfrei beteiligen kann. Wesentlich dazu beitragen kann und muss eine vertiefte Aufklärung aller involvierten AkteurInnen sowohl zu den Ursachen und Formen digitaler Gewalt, als auch zu den zur Verfügung stehenden Handlungsoptionen. Nur durch ein kluges und durchdachtes Zusammenwirken von restriktiven und präventiven Maßnahmen wird zukünftig die Eindämmung von unterschiedlichen Phänomenen digitaler Gewalt möglich sein.

Literatur zu den wesentlichen Aussagen

Appel, H., Gerlach, A. L., & Crusius, J. (2016). The interplay between Facebook use, social comparison, envy, and depression. Current Opinion in Psychology, 9, 44–49. https://doi.org/10.1016/j.copsyc.2015.10.006

Amnesty International, Umfrage Online Missbrauch bei Frauen, 2017 v abgerufen am 08.04.2020

bff e.V. (2020), https://www.frauen-gegen-gewalt.de/de/angriffe-im-oeffentlichen-digitalen-raum.html, abgerufen am 08.04.2020

Boulianne, S. (2015). Social media use and participation: A meta-analysis of current research. Information, Communication & Society, 18(5), 524–538. https://doi.org/10.1080/1369118X.2015.1008542

Brooks, S. (2015). Does personal social media usage affect efficiency and well-being? Computers in Human Behavior, 46, 26–37. https://doi.org/10.1016/j.chb.2014.12.053

Büchi, M., Festic, N., & Latzer, M. (2018). How social well-being Is affected by digital inequalities. International Journal of Communication, 12(0), 21.#

Geschke, Daniel; Klaßen, Anja; Quent, Matthias ; Richter,Christoph: Hass im Netz – Der schleichende Angriff auf unsere Demokratie, IDZ Jena (2019), https://www.idz-jena.de/fileadmin/user_upload/_Hass_im_Netz_-_Der_schleichende_Angriff.pdf, 28

Hartmann, A. (2017) Ergebnisse einer Umfrage unter Frauenberatungsstellen und Frauennotrufen im bff., https://www.frauen-gegen-gewalt.de/de/aktuelle-studien-und-veroeffentlichungen.html, angerbufen am 8.4.20202

Lembke, Ulrike (2017), Kollektive Rechtsmobilisierung gegen digitale Gewalt, Epaper, Gunda-Werner-Institut, heirich Böll Stiftung, 2017

Computer Security and Privacy for Survivors of Intimate Partner Violence Research (2019) https://www.ipvtechresearch.org/research

Vertiefende Anmerkungen

[1] Ebenso sollten folgende Mechanismen beachtet werden, die mit „Gewalt“ im breiteren Sinne zusammenhängen: 1. Sozialer Druck („Social Pressure“) bezieht sich auf zahlreiche Phänomene, die im Internet, im Speziellen in sozialen Medien, von Bedeutung sind. Der soziale Druck muss unter anderem im Kontext von sozialen Vergleichsprozessen betrachtet werden, die zu negativem Affekt führen können. Beispielsweise können NutzerInnen in sozialen Medien ständig mit dem Schönheitsbild von sehr schlanken und sportlichen Models konfrontiert werden. In Bezug darauf stellen sich gerade die häufig bearbeiteten Fotografien von solchen Models auf beispielsweise Instagram als problematisch dar. Dies kann als manipulierte Darstellung von Daten angesehen werden. Die fehlerhafte Darstellung des Körpers und die fehlgeleitete Einschätzung der NutzerInnen, diese Fotografien seien echt (unbearbeitet) und ein Abbild von normalen Personen, können weitreichende unerwünschte Auswirkungen für Individuen haben. Dies ist vor allem bei dem Vorliegen einer wahrgenommenen Diskrepanz der Fall; wenn also der Ist-Zustand (Körper des/der NutzerIn) nicht dem Soll-Zustand (bearbeitete Fotografie des Models) entspricht. Diese wahrgenommene Diskrepanz kann einen negativen Einfluss auf das Selbstbild, das Selbstbewusstsein und Emotionen sowie Affekt (bis hin zur Depression) haben und Neid hervorrufen (Appel, Gerlach, & Crusius, 2016). Auch sonst wird auf sozialen Medien auf Perfektion gesetzt: NutzerInnen werden täglich mit perfekten Wohnungen, perfekten und häufigen Reisen, oder einem idealisierten Lebensstil von Online-Persönlichkeiten (oder auch „InfluencerInnen“) konfrontiert. Die perfekten Darstellungen sind auch in Verbindung mit dem Begriff „Highlight-Reels“ bekannt.
2. Zuletzt beschreibt das Phänomen „Normalisation of the Weirdo“ die Möglichkeit, über soziale Medien sehr einfach Bekanntschaften zu zahlreichen (auch räumlich entfernten) Personen zu schließen, die die gleichen Interessen haben. So finden sich auch Personen mit seltenen, seltsamen oder sogar schädlichen Interessen in einer Interessensgemeinschaft. Das Vorhandensein einer solchen Gemeinschaft führt zu der Wahrnehmung, das eigentlich schädliche Interesse sei normal. Dies kann wiederum zu einer Verstärkung schädlicher Interessen führen (siehe soziale Gruppen wie „Pro Ana“, die sich positiv über Anorexie (Magersucht) äußern).

[2] Das NetzDG hilft Personen, die in den sozialen Medien Opfer geworden sind. Ihnen wird ein Weg eröffnet, gegen die Urheber derartiger Inhalte vorzugehen. Der Anbieter darf im Einzelfall (gerichtliche Anordnung, nach der Novellierung auch eines AG ausreichend) Auskunft über bei ihm vorhandene Daten erteilen, soweit dies zur Durchsetzung zivilrechtlicher Ansprüche erforderlich ist. Darunter fallen regelmäßig IP-Adressen die eine Identifizierung von TäterInnen stark vereinfacht. Zusätzlich soll eine zukünftige Überarbeitung des NetzDG Anbieter dazu verpflichten verschieden Delikte direkt an das Bundeskriminalamt zu melden:

- Verbreiten von Propagandamitteln und Verwenden von Kennzeichen verfassungswidriger Organisationen
- Vorbereitung einer schweren staatsgefährdenden Gewalttat sowie Bildung und Unterstützung krimineller und terroristischer Vereinigungen

- Volksverhetzungen und Gewaltdarstellungen sowie Störung des öffentlichen Friedens durch Androhung von Straftaten
- Belohnung und Billigung von Straftaten
- Bedrohungen mit Verbrechen gegen das Leben, die sexuelle Selbstbestimmung, die körperliche Unversehrtheit oder die persönliche Freiheit
- Verbreitung kinderpornografischer Aufnahmen

Hier sind auch einige der im Vorfeld beschriebenen Tatbestandsmerkmale aufgelistet. Grundsätzlich gilt bei der strafrechtlichen Ermittlung natürlich immer, dass es auch digitale Gewaltdelikte gibt, bei denen eine Staatsanwaltschaft zu ermitteln hat (z.B. Hassdelikte). Bei den Beleidigungstatbeständen (Beleidigung, Üble Nachrede, Verleumdung) handelt es sich jedoch um Antragsdelikte. Beleidigung ist nicht gleich Gewalt. Die juristische Definition von Gewalt ist nach der heutigen Rechtsprechung zu definieren als körperlich wirkender Zwang durch die Entfaltung von Kraft oder durch sonstige physische Einwirkung, die nach ihrer Intensität dazu geeignet ist, die freie Willensentschließung oder Willensbetätigung eines anderen zu beeinträchtigen (z.B. Nötigung). Das trifft so auf eine Beleidigung in der Regel eher nicht zu. Die Nutzung des Begriffs Digitale Gewalt in diesem Text geht über die juristische Definition hinaus.

[3] https://www.bmjv.de/DE/Themen/FokusThemen/NetzDG/NetzDG_node.html

[4] Infotech News. (2019). HTTPS encryption traffic on the Internet has exceeded 90%. Retrieved from https://meterpreter.org/https-encryption-traffic/

[5] Eine die staatliche Autorität verstärkende Variante würde darin bestehen, erweiterte Befugnisse einzuräumen, in dem in rechtlich eindeutigen Fällen entsprechenden legitimierten staatlichen Stellen Zugang zu Nutzerdaten zur Verfügung gestellt werden. Denkbar wäre hier ein Nummernschild-Ansatz in Analogie zum Straßenverkehr: jedem User ist ein Code zugeordnet, der zur Verfügung gestellt wird und über den die Identität der TäterInnen herausgefunden werden kann. So bestünde weiterhin keine Klarnamenpflicht, dennoch könnten User bei klaren Rechtsverstößen durch eine staatlich legitimierte Stelle identifiziert werden. Eine solche Variante ist mit verschiedenen Risiken des Missbrauchs dieser Möglichkeiten durch staatliche und anderer Akteure abzuwägen. Von besonderer Bedeutung ist hier der SanBernadino Fall aus den USA. Ein Terrorist hatte 14 Personen erschossen. Der Geheimdienst FBI verlangte Zugang zum Code des Handy's. Der CEO von Apple, Tim Cook verweigerte den Zugriff, da er den Schutz der Privatheit der Kunden höher einschätzte als die Verfügbarkeit der Daten durch die staatliche Sicherheitsbehörde (siehe: Blakely, T., Elam, K., Langley, D., Morrison, W., & Robinson, D. (2016). Apple's conundrum: Liberty vs. security and modern terrorism. *Intellectual Archive, 5*(3), 32.37.)

[6] https://ec.europa.eu/digital-single-market/en/digital-services-act-package

[7] https://www.landtag.sachsen-anhalt.de/fileadmin/files/drs/wp7/drs/d4785dak.pdf