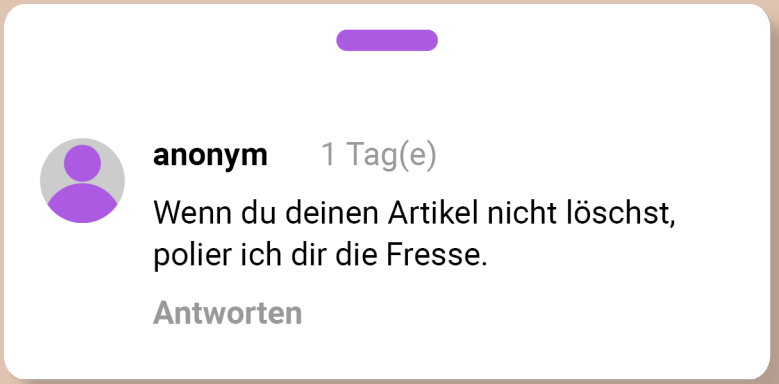
HateAid

Hass, Gewalt & Lügen im Netz sind nicht Teil des Jobs

Ein Leitfaden zum Umgang mit digitaler Gewalt

Für Kommunalpolitiker*innen und alle, die sich vor Ort engagieren, von Feuerwehr bis Flüchtlingshilfe



40 % der Bürgermeister*innen geben an, dass sie oder Personen aus ihrem privaten Umfeld aufgrund ihrer Tätigkeit schon **beleidigt, bedroht oder tätlich angegriffen** worden sind.[1]

38 % der Kommunalpolitiker*innen haben Erfahrungen mit **verbalen und digitalen Anfeindungen** gemacht.[2]

39 % der Bürgermeister*innen schätzen ein, dass der **Umgang** in ihrer Gemeinde zunehmend **verroht**.[3]

13 % der Kommunalpolitiker*innen haben schon darüber nachgedacht, sich aus **Sorge um ihre Sicherheit und die ihrer Familie aus der Politik zurückzuziehen**.[4]

61,5 % der Amts- und Mandatsträgerinnen (in Brandenburg) geben 2022 an, von einer Anzeige von bspw. Beleidigungen oder Bedrohungen häufig abgesehen zu haben, aus **mangelndem Glauben an Strafverfolgung und effektive Verurteilungen**.[5]

Nein, das ist nicht Teil des Jobs.

Mehr als die Hälfte der Internetnutzer*innen **bekennt sich aus Angst im Netz seltener zur eigenen politischen Meinung (57 %)**, beteiligt sich seltener an Diskussionen (55 %) und formuliert Beiträge bewusst vorsichtiger (53 %).[6]

8 % der Amtsträger*innen, die Anfeindungen erlebt haben, ziehen für sich die Konsequenz, ihre Meinung nicht mehr wie bisher im politischen Diskurs beziehungsweise bei der Amtsausübung frei zu äußern. 5 % erwägen eine **Abmeldung ihrer Accounts in den sozialen Medien**, um potenzielle Anfeindungen via Social Media zu vermeiden.[7]

9 % der Amtsträger*innen haben in Reaktion auf die erlebte Anfeindung konkret darüber nachgedacht, ihr Amt beziehungsweise Mandat niederzulegen. 10 % erwägen einen **Rückzug aus dem Amt**, indem sie nicht erneut kandidieren werden.[8]

Inhalt

1 Was Sie über Hass im Netz wissen müssen

Hass als politische Strategie

Stellen Sie sich vor, Sie organisieren eine Wahlkampfveranstaltung in Ihrem Wohnort und kündigen diese auf Ihrem Facebook-Profil an. Plötzlich erreichen Sie zahlreiche Nachrichten: In einer lokalen Facebook-Gruppe werden Sie mit Beleidigungen wie „Stück S******“ oder „typischer Volksverräter“ überzogen. Zuerst ignorieren Sie die Angriffe vielleicht, bis Sie eine Morddrohung in Ihrem E-Mail-Postfach finden. Sie fühlen sich bedrängt und überfordert, vor allem machen Sie sich Sorgen um Ihre Sicherheit und die Ihrer Familie. Solche Erfahrungen sind leider Teil des Alltags vieler politisch oder kommunal Engagierter. Hass wird gezielt eingesetzt, um Menschen aus politischen Debatten zu drängen und sie zum Schweigen zu bringen, oft online und manchmal auch offline.

In extremen Fällen schrecken Täter*innen auch nicht vor Brandanschlägen oder körperlicher Gewalt zurück. Oder sogar vor Mord – wie im Fall des Kasseler Regierungspräsidenten Walter Lübcke.

Diese Angriffe sind oft Teil von Hasskampagnen, die politische Debatten beeinflussen wollen. Die Auslöser können vielfältig sein, von lokalen Themen wie der Aufstellung eines Windrads bis hin zur gesamtdeutschen Asylpolitik. Oft werden Einzelpersonen für gesellschaftliche Tatsachen oder Entscheidungen verantwortlich gemacht. Dabei wird der Ärger über diese Dinge auf die betroffenen Personen projiziert. Sie werden angefeindet.

Die Studie „Hass auf Knopfdruck“ vom Institute for Strategic Dialogue und dem Verein #ichbinhier zeigt, dass solche Hasskampagnen oft organisiert sind. Häufig sind es Rechtsextremist*innen, die sie online in geschlossenen Foren planen, sich vernetzen und mehrere Accounts anlegen um so Politiker*innen und politisch Engagierte anzugreifen.[9]

Rechtsextreme und Personen aus dem verschwörungsideologischen Milieu vernetzen sich im digitalen Raum nicht mehr nur in geschlossenen Foren. Sie nutzen dafür zunehmend gängige Plattformen. Besonders seit der Pandemie haben sich dafür reichweitenstarke, öffentliche Telegram-Kanäle etabliert.[10]

Laut Bundeskriminalamt wurden im Jahr 2023 etwa 45 % aller verzeichneten Hasspostings dem Bereich Rechtsextremismus zugeordnet.[11]

Hasskampagnen zielen darauf ab, Menschen einzuschüchtern, die eine bestimmte politische Meinung vertreten und/oder sich für demokratische Werte einsetzen. Durch den Hass sollen sie zum Schweigen gebracht werden. Dieses Phänomen wird auch Silencing genannt. Häufige Reizthemen können Migration, Rechtsextremismus, Feminismus, Diskriminierungskritik und Klimapolitik sein. Die Folge ist eine Verschiebung des politischen Diskurses, da sich viele Menschen nicht mehr trauen, sich in sozialen Medien für Demokratie und gegen Ausgrenzung einzusetzen. Die Strategie zeigt Wirkung: 13 % aller 2024 befragten ehrenamtlichen Bürgermeister*innen haben aus Sorge um ihre Sicherheit bzw. die ihrer Familie schon einmal konkret darüber nachgedacht, sich aus der Politik zurückzuziehen. Von denjenigen, die bereits Anfeindungen oder Übergriffe erlebt haben, hat rund jede*r Vierte aufgrund von Sicherheitsbedenken bereits einen Rückzug aus der Politik erwogen.[12] **Das stellt eine Gefahr für unsere Demokratie und die gesamte Gesellschaft dar.**

Hass und analoge Gewalt gegen politisch Engagierte

Wir beobachten, dass Gewalt, die Engagierte online erleben, häufig politisch motiviert ist. Sie richtet sich auch immer wieder gegen jene, die sich auf kommunaler Ebene für unsere Demokratie einsetzen. Zwar dokumentiert das Bundeskriminalamt Hass-Postings als solche erst seit 2017, dennoch zeigt sich, dass politisch motivierte Kriminalität in Form von digitalem Hass insgesamt immer weiter zunimmt.[13]

Hass und Gewalt bleiben jedoch nicht „nur im Netz“. **Besonders auf kommunaler Ebene besteht die Gefahr, dass digitale Gewalt in analoge Gewalt übergeht.** Angefeindete Personen und Täter*innen leben oft in räumlicher Nähe zueinander. Nicht selten kennen die Täter*innen die haupt- oder ehrenamtlich Engagier-

ten in ihrem Ort und wissen, wo sie wohnen, wo ihre Kinder zur Schule gehen oder in welchen Vereinen sie aktiv sind. Das erschwert es den Betroffenen, sich durch Anonymität und Abgrenzung zu schützen. Ehrenamtliches Engagement ist oft kaum vom Privatleben zu trennen und persönliche Kontaktdaten sind oft öffentlich bekannt.

- Die polizeilich registrierten Fallzahlen von Hasspostings haben sich zwischen 2022 und 2023 mehr als verdoppelt.[14]

- Straftaten gegen Amts- bzw. Mandatsträger*innen haben 2023 gegenüber dem Vorjahr um 29,12 % zugenommen.[15]

- 40 % der Bürgermeister*innen geben an, dass sie oder Personen aus ihrem privaten Umfeld aufgrund ihrer Tätigkeit schon einmal beleidigt, bedroht oder tätlich angegriffen wurden.[16]

- 38% der befragten ehrenamtlichen Bürgermeister*innen und Landrät*innen haben zwischen Mai und Oktober 2023 Anfeindungen erlebt. 72% erlebten verbale/schriftliche Anfeindungen, 26% Hasspostings, 2% tätliche Übergriffe.[17]

Wen trifft der Hass besonders häufig?

Hass kann alle treffen.

Sie müssen selbst nicht aktiv auf Social Media sein, um digitale Gewalt erfahren zu können. Insbesondere Kommunalpolitiker*innen und engagierte Bürger*innen werden oft per E-Mail oder SMS angegriffen.[18]

Auch wenn der Hass jeden treffen kann, gibt es Menschen, die häufiger und anders im Netz angefeindet werden. Personen werden aufgrund ihres Namens, ihres Aussehens, ihres vermuteten Geschlechts oder ihrer Sexualität angegriffen.

Frauen erleben im Netz oft stark sexualisierte Gewalt, die bis hin zu detaillierten Vergewaltigungs- und Folterfantasien reicht. Oft sind die Kommentare enorm sexistisch und erniedrigend. Dies betrifft auch Menschen, die aufgrund ihrer Zugehörigkeit zu bestimmten Gruppen mit gruppenbezogener Menschenfeindlichkeit wie Rassismus, Antisemitismus, LGBTIQ*-Feindlichkeit oder Klassismus angegriffen werden.[19]

Oft werden Betroffene sogar mehrfach angegriffen. Sie erleben verschiedene Diskriminierungsformen, die sich gegenseitig verstärken. Werden sie etwa wegen ihrer Hautfarbe, ihres Geschlechts und ihrer Sexualität angefeindet, sind sie oft auf besonders schwere Weise von digitaler Gewalt betroffen.

Geschlechtsspezifische digitale Gewalt

Kommunal engagierte Frauen geben häufiger als Männer an, dass sie selbst oder Personen aus ihrem privaten Umfeld schon einmal aufgrund ihres Amtes beleidigt, bedroht oder tätlich angegriffen worden sind.[20]

Geschlechtsspezifische digitale Gewalt bezeichnet die Verwendung digitaler Medien, um Personen aufgrund ihres Geschlechts zu schikanieren, zu bedrohen oder zu erniedrigen. Diese Form von Gewalt zielt überwiegend auf Frauen ab, insbesondere auf solche, die öffentlich auftreten oder politisch aktiv sind. Auch queere Menschen sind überproportional oft von geschlechtsspezifischer Gewalt betroffen.[21] Die Gewalt ist oft durch sexistische und sexualisierte Inhalte gekennzeichnet. Sie umfasst neben sexistischen Beleidigungen, nicht einvernehmlich geteilten Penis-Bildern oder Vergewaltigungsdrohungen auch die Verbreitung manipulierter Bilder oder Videos, einschließlich Deepfakes und Deepnudes, die den Ruf und die Integrität der Betroffenen schädigen sollen. Werden dabei Bilder oder Videos verwendet, spricht man auch von bildbasierter sexualisierter Gewalt. Sie können auch Teil von politischen Desinformationskampagnen sein.

Deepnudes sind eine Art von Deepfake-Technologie, die darauf abzielt, Bilder von Personen so zu manipulieren, dass sie nackt erscheinen, selbst wenn sie ursprünglich bekleidet waren. Diese Technologie wird oft zur Erstellung

pornografischer Inhalte ohne Zustimmung der betroffenen Personen verwendet.

Heute werden meist Face-Swap-Apps oder ähnliche Programme verwendet, mit denen per Bildbearbeitung sehr einfach Gesichter auf fremde Körper gesetzt werden und Deepnudes innerhalb weniger Augenblicke erstellt werden können.

Die Auswirkungen dieser Form digitaler Gewalt sind gravierend, da sie nicht nur die Privatsphäre und Sicherheit der Betroffenen beeinträchtigen, sondern auch ihre psychische Gesundheit belasten können. Vor allem Frauen und queere Personen ziehen sich aufgrund des Risikos digitaler Gewalt aus den sozialen Medien zurück.[22]

Bisher gibt es noch keinen eigenständigen Straftatbestand, der das Erstellen und Verbreiten von Deepfakes mit sexuellen Inhalten als solches unter Strafe stellt. Wer Deepnudes bzw. Deepfakes mit sexuellem Inhalt verbreitet, kann sich dennoch – je nach Einzelfall – strafbar machen. So kann z. B. eine Beleidigung, eine Verleumdung oder eine Verletzung des Rechts am eigenen Bild vorliegen. Deshalb sollten solche Inhalte auch konsequent zur Anzeige gebracht werden.

Die Verbreitung intimen Bildmaterials kann durch die Erstellung eines Hashes unter stopncii.org eingeschränkt werden. **Das Tool erstellt s.g. Hashes von intimen Bildern/Videos, das sind einzigartige digitale Fingerabdrücke.** StopNCII.org teilt diese Hashes mit unterschiedlichen kooperierenden Plattformen, um die Bilder zu erkennen und zu entfernen, bevor und nachdem sie online geteilt wurden.
Allerdings bietet auch dieses Tool keinen vollständigen Schutz vor der Verbreitung sexualisierten Bildmaterials.

Wer steckt hinter dem Hass im Netz?

Der zunehmende Hass im Netz nimmt verschiedene Formen an, von themenspezifischen Shitstorms bis hin zu Einzelpersonen, die andere online stalken. Oft sind es auch organisierte politische Gruppierungen, die bestimmte Menschen als Feinde darstellen und sie dann gezielt angreifen. Meist scheint es dann als sei es eine breite Masse oder gar eine vermeintliche Mehrheit der Bevölkerung, die jemanden angreift. Es ist jedoch oftmals nur ein kleiner – jedoch hochaktiver – Kreis an Personen. **Laut der Studie „Hass auf Knopfdruck“ kommen 50 % der Likes unter Hasskommentaren von gerade einmal 5 % der Hater*innen.**[23] Die Datenanalysen von HateAid zu Shitstorm-Situationen bestätigen diese Zahlen.[24]

Organisierte Hasskampagnen sind nicht immer leicht zu erkennen. Sie werden meist in geschlossenen Foren oder Chats entwickelt und orchestriert. Die folgenden Merkmale können Ihnen helfen, eine Hass-Kampagne zu identifizieren:

1. **Wenige hochaktive Accounts / Profile**: Wenn Sie von einer großen Hasswelle betroffen sind, sind es oft wenige Accounts, die Sie kontinuierlich und immer wieder angreifen. Zögern Sie nicht, diese sofort zu melden und zu blockieren.

2. **Die Accounts sind untereinander vernetzt**: Diese Accounts beziehen sich oft aufeinander und manchmal ergeben sich sogar direkte Zusammenhänge aus ihren Konten. Sie sind auf der jeweiligen Plattform miteinander verbunden, teilen oft dieselben Inhalte und antworten sich gegenseitig in den Kommentarspalten. Zögern Sie nicht, auch hier großflächig zu blockieren.

3. **Die Familie bzw. das Private als „Schwachstelle“**: Zwar werden Sie für Ihre Ideen und Ihr politisches Handeln angegriffen, doch werden dabei Sie persönlich und oft auch Ihre Familie bzw. Ihr*e Partner*in angegangen – häufig mit Bezug auf Merkmale wie Aussehen, vermeintliche Herkunft, geschätztes Geschlecht oder vermutete Sexualität.

Allerdings werden nicht nur in organisierten politischen Hasskampagnen Merkmale genutzt, die Ihnen zugeschrieben werden, um Sie anzugreifen. Es gibt auch Einzelpersonen, die Online-Profile nur dazu aufbauen, um damit Andere lächerlich zu machen und zu attackieren. Das gilt insbesondere für sogenannte „Trolle“.

Trolle sind Menschen, die in den sozialen Medien sehr aktiv sind. Sie mischen sich mit dem einzigen Ziel in Diskussionen ein, diese zu stören, vom eigentlichen Thema abzulenken und sachliche Debatten unmöglich zu machen. Oft sind sie in organisierte Hasskampagnen involviert und verfügen über mehrere erfundene Identitäten, sogenannte Fake-Accounts.

Erkennen Sie den Troll und reagieren Sie nicht auf ihn – denn in solchen Diskussionen verschwenden Sie nur Zeit und Energie. Machen Sie rechtssichere Screenshots (siehe S. 50f.) von den Troll-Kommentaren, wenn Sie rechtlich gegen diese vorgehen wollen und melden bzw. löschen Sie sie dann.

So erkennen Sie einen Troll

- Postet kontroverse Kommentare und Bilder, um Diskussionen zu provozieren.
- Ist häufig anonym. Das Profil ist oft nicht gepflegt und enthält wenig bis keinen Inhalt zur Person.
- Rassismus, Sexismus, Antisemitismus etc. – der Troll verbreitet gruppenbezogene Menschenfeindlichkeit.
- Führt die Diskussion ewig weiter – will sich gar nicht einigen.
- Wenn es keine inhaltlichen Angriffspunkte mehr gibt, greift der Troll eine Person oft aufgrund ihres Aussehens oder ihres Namens an.
- Ist fast zu jeder Zeit sehr aktiv auf diversen Kanälen.

Don’t feed the troll!

Viel Hass in kurzer Zeit – die Rolle von Hashtags

Plattformen wie X (ehemals Twitter) verwenden Hashtags (#), um Verlinkungen herzustellen. Idealerweise ermöglichen diese das Ordnen von unzähligen Beiträgen zu einem bestimmten Thema. Wenn Sie sich beispielsweise für Tattoos interessieren und unter einem Beitrag zum Thema das Hashtag #tattoolove anklicken, werden Ihnen alle anderen Posts angezeigt, die auch #tattoolove verwenden.

Das Problem: Hashtags können beliebig unter einen Beitrag gesetzt werden, um schnell viele Menschen online zu erreichen und damit zu mobilisieren. Die Recherche "Kein Filter für Rechts" von Correctiv[25] zeigt, wie rechte Mobilisierungsstrategien rechtsextreme Inhalte und Symbole subtil mit unverfänglichen Hashtags wie #tattoolove verbinden, um diese in die breite Gesellschaft zu bringen und zu

normalisieren. Hashtags sollen auch die Themen widerspiegeln, die digital häufig diskutiert werden, und werden von Plattformen wie X als Trends angezeigt, basierend darauf, wie oft sie verwendet werden.

So können Hashtags strategisch genutzt werden, um politische Inhalte, Narrative oder organisierte Hass- und Desinformationskampagnen zu verbreiten. Ein vermeintlich unproblematischer Hashtag wie #notallmen wird oft in Reaktionen auf Diskussionen über sexuelle Belästigung oder geschlechtsspezifische Gewalt verwendet. Damit soll betont werden, dass nicht alle Männer solche Taten begehen. Obwohl der Hashtag zunächst harmlos erscheinen mag, lenkt er die Aufmerksamkeit vom eigentlichen Problem ab. Anstatt sich auf die Erfahrungen der Betroffenen zu konzentrieren und eine Diskussion über systemische Probleme zu ermöglichen, trägt er dazu bei, diese zu untergraben und die Problematik herunterzuspielen.[26]

Ein anderes Beispiel: Hinter #Kriegstreiber verbirgt sich eine Kampagne, die Personen oder Institutionen, die Solidarität mit der Ukraine zeigen, verunglimpft. Den Betroffenen wird unterstellt, Schuld am Ausbruch des Kriegs in der Ukraine zu tragen. Zudem wird ihnen vorgeworfen, den Krieg zu befeuern oder sogar einen dritten Weltkrieg voranzutreiben.[27]

Täter*innen und ihre Strategien erkennen

Menschen, die in der Öffentlichkeit über politische Reizthemen, wie z. B. Klimapolitik, Migration oder soziale Ungleichheit sprechen oder in diesen Bereichen arbeiten, werden besonders häufig angefeindet.[28] Zu diesen besonders kontroversen Themen entstehen Narrative, die sich immer weiter verbreiten. Stereotype werden stetig reproduziert. Das kann online und offline eine Stimmung schaffen, in der Diskussionen in Hass und Gewalt umschlagen.

Kommunalpolitiker*innen sind davon besonders oft betroffen. Sie sind eine Projektionsfläche für den politischen Gegner oder allgemein „die Politik".

Incels

Stellen Sie sich vor, Sie sind Kommunalpolitikerin und entdecken nach der Eingabe Ihres Namens in der Google-Bildersuche ein gefälschtes Nacktbild von sich. Diese Art von Angriffen kann aus der Incel-Community kommen. **Das ist eine Gruppe überwiegend männlicher Personen, die unfreiwillig ohne sexuelle Kontakte zu Frauen leben und aus ihrem Frust über fehlende Beziehungen starken Hass gegen Frauen und andere Minderheiten entwickeln.** Sie sehen sich als Opfer von Frauen und einer Gesellschaft, die ihnen angeblich sexuelle und romantische Chancen verweigert. Incels verbreiten in ihren Foren eine Ideologie der männlichen Überlegenheit und der eigenen Abwertung, die häufig in extremen Gewaltfantasien gegen Frauen mündet. Diese digitale Gewalt kann real werden, wie der Anschlag in Halle 2019 zeigt. Zudem werden regelmäßig Fotos von Frauen aus sozialen Medien in Incel-Foren missbraucht, um Vergewaltigungsfantasien zu verbreiten oder gefälschte Nacktaufnahmen zu erstellen und zu veröffentlichen. Das Ziel: Frauen gezielt öffentlich schaden und zum Schweigen bringen.[29]

Krisenbedingte Entstehung neuer Täterschaften

Neben dauerhaft extremistischen Akteur*innen von digitaler Gewalt gibt es auch solche, die sich krisen- und situationsbedingt zu solchen entwickelt haben. Dazu gehören unter vielen anderen auch pro-russische Akteure und Querdenker*innen. Ihre Bewegungen können Überschneidungen mit (rechts)extremen Gruppen haben oder sie werden von ihnen übernommen.[30]

Pro-Russische und Kreml-nahe Akteur*innen

Angriffe aus dem pro-russischen Lager treffen nicht nur Behörden oder die kritische Infrastruktur. Betroffene können von der Bürgermeisterin über den Aktivisten bis zur Bundesministerin alle sein. **Denn online versuchen pro-russische Akteur*innen spätestens seit dem Überfall auf die Ukraine unsere Demokratie zu destabilisieren, Politiker*innen zu diskreditieren und Menschen gegeneinander aufzuhetzen.** In unserer Arbeit begegnen uns vor allem russische Desinformationskampagnen, Deepfakes von öffentlichen Personen und russische Fake-Accounts auf sozialen Netzwerken.[31]

Bei digitaler Gewalt durch russische Akteure handelt es sich häufig aber auch um Cyberangriffe auf hochrangige Betriebssysteme, wie beispielsweise auf die SPD-Zentrale[32] und Desinformationskampagnen, die von staatlichen oder staatsnahen russischen Gruppen ausgeführt werden. Diese Aktivitäten zielen darauf ab, politische Prozesse zu beeinflussen und so die Interessen der russischen Regierung global zu fördern.[33] Ein prominentes Beispiel war die Verbreitung des Hashtags #BaerbockRuecktritt, welcher im September 2022 rasant und zeitgleich auf unterschiedlichsten Social-Media-Plattformen verbreitet wurde. Recherchen ergeben, dass die Desinformationskampagne gegen Annalena Baerbock gezielt von pro-russischen und kreml-nahen Accounts gefördert worden seien. Besorgniserregend ist dabei, dass Social-Media-Plattformen kaum Maßnahmen ergriffen haben, womit die meisten der gemeldeten Beiträge online blieben.[34]

Querdenker*innen und Selbstverwalter*innen

Die „Querdenken"-Bewegung erstarkte in Deutschland während der COVID-19-Pandemie und machte sich schnell einen Namen durch ihre Proteste gegen die staatlichen Maßnahmen zur Bekämpfung des Virus. **Die Bewegung vereint verschiedenste Gruppen und Personen, Impfskeptiker*innen bis hin zu Anhänger*innen von Verschwörungstheorien**. Häufig steht die Querdenken-Bewegung in Verbindung mit **rechtsextremen Gruppen** und der Verbreitung von **Desinformation**.[35]

Selbstverwalter*innen, auch als Reichsbürger*innen bekannt, lehnen die Legitimität der Bundesrepublik Deutschland ab und erkennen ihre Gesetze nicht an. Sie behaupten, das Deutsche Reich bestehe fort.[36] **Zwischen Selbstverwalter*innen und staatlichen Behörden kommt es immer wieder zu widerständigen und teilweise gewaltsamen Auseinandersetzungen**.[37]

Das zeigen auch die Polizeistatistiken: Selbstverwalter*innen werden vom BKA entweder als rechtsextrem oder in der Kategorie „PMK nicht zuzuordnen" bzw. „sonstige Zuordnung"[38] geführt. In letzterer Kategorie werden die mit Abstand meisten Angriffe auf Amts- und Mandatsträger*innen erfasst.[39]

Sprachstrategien der Rechten[40]

Hasskampagnen sind oft an Rhetorik und Sprachstil erkennbar. Die Extremismusforscherin Natascha Strobl erkennt folgende Sprachmuster und -strategien, mit denen rechtsextreme Ideologien die Gesellschaft (in-)direkt beeinflussen wollen:

Entmenschlichung durch Naturkatastrophen

Gruppen von Menschen werden sprachlich mit Naturkatastrophen verglichen und damit als bedrohliche, anonyme Masse dargestellt. So sollen sie nicht mehr als einzelne menschliche Individuen gesehen werden (etwa, wenn Geflüchtete als „Flut“ oder „Welle“ bezeichnet werden).

Kriegsbegriffe

Um eine Gefahrensituation zu konstruieren, werden Kriegsbegriffe und -symbole verwendet (Corona-Schutzmaßnahmen werden als „Klimadiktatur“[41] oder „Impfangriff“[42] bezeichnet.)

Verschwörungsmythen

Der Große Austausch ist eine Erzählung der sogenannten Neuen Rechten, die behauptet, es gäbe einen geheimen Plan, die weiße Mehrheitsgesellschaft durch Nicht-Weiße sowie Muslim*innen und jüdische Menschen zu ersetzen. Diese Verschwörungstheorie konstruiert eine vermeintliche Bedrohung und greift jene an, die angeblich daran beteiligt sind. Insbesondere werden Personen im Asyl- und Flüchtlingsbereich sowie weiße Frauen, die keine Kinder bekommen oder Abtreibungsrechte unterstützen, angefeindet. Der Hashtag #DefendEurope wird oft in diesem Kontext verwendet. Er bezieht sich beispielsweise auf eine Kampagne, die auf dem Verschwörungsmythos des „großen Austauschs“ beruht, der sich ein Ende der Aufnahme von Geflüchteten in Europa zum Ziel setzt.

Framing

„Framing“ ist eine Technik, die sich auf das sprachliche Einrahmen von Themen fokussiert, sodass diese immer im Zusammenhang gedacht werden. Zum Beispiel werden alle Menschen, die nicht weiß sind, als Geflüchtete „geframed“, obwohl sie das nicht zwangsläufig sind. Wenn nicht-weiße Menschen dann zum Beispiel über rassistische Erfahrungen in unserer Gesellschaft sprechen, kann schnell vom Thema abgelenkt werden, statt über Rassismus wird dann plötzlich über Geflüchtete gesprochen.

Neologismen

Neue Wörter werden erfunden, um von Inhalten abzulenken und Gegenargumente zu delegitimieren (wie etwa beim Begriff der „Umvolkung“).

Mimikry

Bei dieser Technik werden bestimmte Debatten, die nicht Teil eines rechtsextremen Weltbilds sind, scheinbar weitergeführt. Allerdings wird dabei der Ursprung der Debatte durch einen anderen Fokus ersetzt und zugunsten rechtsextremer Ideen umgebogen. Ein Beispiel ist die breite Diskussion über Gewalt gegen Frauen, die Jahrzehnte lang von Feminist*innen vorangetrieben wurde. Obwohl Feminist*innen normalerweise von rechten Extremist*innen angefeindet werden, wurde ihre Debatte 2017 (im Laufe der #metoo-Bewegung) plötzlich auch von Rechtsextremist*innen übernommen. Allerdings nur dann, wenn Geflüchtete oder nicht-weiße Männer tatverdächtig waren. Das Ziel der Debatte war so nicht länger, die Rechte von Frauen zu stärken, sondern z. B. unter dem Hashtag #120 Dezibel Hass gegen Geflüchtete zu verbreiten.

Umkehr

Bei diesem rhetorischen Trick werden Begriffe im umgekehrten Kontext verwendet, wie etwa bei „Linksfaschismus“. Hier werden Linke diskreditiert und der Begriff Faschismus relativiert.

Falsches Bedauern

Bei dieser rhetorischen Strategie wird das Leid anderer auf emotionaler Ebene anerkannt, um dann die vermeintlich sachliche Unmöglichkeit von Hilfeleistungen zu betonen. (Beispiel etwa: „Wir können nicht alle aufnehmen.“ oder „Das Boot ist voll.“)

Neben Rechtsextremen gibt es auch andere politisch motivierte Gruppierungen, die vermehrt digitale Gewalt ausüben. Häufig weisen ihre Ideologien große Überschneidungspunkte auf. So zeichnen sie sich beispielsweise ebenso durch Rassismus, Misogynie und antidemokratische Haltungen aus.

2 Wie Sie sich im Netz schützen & mit digitaler Gewalt umgehen können

2.1 Präventive Schutzmaßnahmen

Digitale Gewalt kann alle treffen, ohne Vorankündigung. Dabei ist es egal, ob Sie besonders aktiv im Netz sind oder sich eher zurückhalten. Anfeindungen können Sie per E-Mail erreichen oder über Messenger-Dienste wie Telegram oder WhatsApp. Genauso wie auf Blogs oder in einschlägigen Online-Medien, die falsche Informationen über Sie verbreiten. **In all diesen Fällen ist es wichtig, sich selbst zu schützen**, idealerweise auch präventiv.

Schützen Sie sich präventiv, bevor Sie betroffen sind.

Ressourcen für Social Media identifizieren

Um sich bestmöglich auf digitale Gewalt und Hass im Netz vorzubereiten, sind klare Zuständigkeiten und Strukturen innerhalb Ihrer Organisation oder Verwaltung wichtig.

Besonders auf kommunaler Ebene arbeiten viele ehrenamtlich und haben keine ausreichenden Ressourcen, um eine Person zu beschäftigen, die sich um den Social-Media-Auftritt kümmert.

Hinweise für alle, die ihre Social-Media-Kanäle selbst betreiben:

- Social Media kann sehr zeitintensiv sein. Achten Sie daher darauf, dass Sie Ihre Zeit hier begrenzen und sich feste Zeiten für die sozialen Medien setzen. Das kann etwa eine halbe Stunde morgens oder mittags sein plus eine halbe Stunde zum Feierabend. Das definieren Sie selbst, je nachdem, wie lange Sie für Ihre anderen Aufgaben brauchen. Planen Sie aber ausreichend Zeit ein.
- Beispiel: Für zwei bis drei Posts auf mehreren Kanälen samt Community Management sollten Sie etwa 20 Stunden pro Woche einplanen.
- Falls Sie nur einmal die Woche posten und täglich kurz nach einer kleinen Community schauen, reichen zehn Stunden.
- Legen Sie Pausen in Ihrer Beschäftigung mit Social Media ein.
- Sorgen Sie für digitale und analoge Sicherheit. Stellen Sie sicher, dass Ihr Name anonym bleibt, Ihre Wohnadresse nicht öffentlich im Netz steht und verwenden Sie, wenn möglich, ein Diensthandy und einen Dienstlaptop.

Wenn Sie oder Ihr Team viel Inhalt auf Social Media teilen (etwa drei Beiträge pro Woche) und eine große Community haben (ab 5.000 Follower*innen), dann planen Sie eine Stelle für die Social-Media-Koordination in Ihr Budget mit ein. Ist das aus finanziellen Gründen nicht möglich, erkundigen Sie sich: Manche Social-Media-Manager*innen arbeiten ehrenamtlich für die gute Sache und unterstützen zeitweise.

Krisenplan: Konkrete Szenarien definieren und ein Krisenteam aufstellen

Eine Krisensituation ist ein akuter Zustand von Überforderung, Spannung oder Bedrohung, bei dem die Anforderungen der Situation die eigenen Ressourcen und Möglichkeiten übersteigen.[43]

Um einer Krise möglichst gut vorzubeugen, hilft es sehr, einen Krisenplan zur Hand zu haben. Er verschafft Ihnen und allen im Unterstützungsnetzwerk Beteiligten in akuten Krisensituationen etwas Ruhe. So können Sie Angriffe besser bewältigen. Es ist also ratsam, präventiv einen solchen Plan zu erstellen.

In unserer Broschüre zur Erstellung eines persönlichen Krisenplans finden Sie detaillierte Anleitungen und Tipps, um mögliche Krisenszenarien für sich zu identifizieren, sich effektiv auf Krisensituationen vorzubereiten und zu reagieren:

- **Definition persönlicher Krisenszenarien**: Identifizieren Sie mögliche Krisensituationen, die Sie betreffen könnten.
- **Krisenteam und Verantwortlichkeiten**: Bestimmen Sie Ihr persönliches Krisenteam und legen Sie fest, wer welche Aufgaben übernimmt.
- **Social-Media-Management**: Deaktivieren Sie bei Bedarf Ihre Social-Media-Accounts oder schränken Sie die Kommentarfunktionen ein, um Ihre Online-Präsenz zu kontrollieren.
- **Umgang mit grenzüberschreitenden Kommentaren**: Reagieren Sie auf gewaltvolle oder grenzüberschreitende Kommentare durch Gegenrede, Community Management und proaktiv mit einer Netiquette.
- **Kontaktliste für Krisensituationen**: Erstellen Sie eine Liste mit wichtigen Kontaktstellen, die Ihnen in Krisensituationen helfen können, z. B. HateAid.
- **Sicherheitsmaßnahmen**: Planen Sie sowohl analoge als auch digitale Sicherheitsmaßnahmen, um sich vor persönlichen Bedrohungen zu schützen.

Argumentationssammlung vorbereiten

Viele Online-Diskussionen und Anfeindungen wiederholen sich und richten sich gezielt gegen Geflüchtete, Frauen, Menschen jüdischen Glaubens, Politiker*innen oder die Regierung. Wenn Sie dazu online Stellung beziehen, werden Sie wahrscheinlich merken, dass Sie immer wieder ähnlich argumentieren. **Es spart daher Zeit und Kapazität, einmalig eine Argumentationssammlung mit Fakten und empirischen Daten vorzubereiten.** Diese können Sie selbst oder mithilfe bestehender Argumentationssammlungen erstellen und allen Mitarbeitenden Ihrer Organisation zur Verfügung stellen.

Beispiel: tagesschau.de/faktenfinder

Solidaritätsnetzwerk aufbauen

Bauen Sie ein Solidaritätsnetzwerk auf, das Ihnen im Falle von Angriffen helfen kann – digital und analog. Die Mitglieder können gegenseitig Solidarität bei digitaler Gewalt zeigen und sich präventiv austauschen. Kommunalpolitiker*innen können z. B. ein digitales Solidaritätsnetzwerk aufbauen, indem sie eine Chatgruppe mit ihren Parteikolleg*innen einrichten. Darin können sich alle schnell informieren und direkt in den Kommentarspalten unterstützen, wenn ein Mitglied digital angegriffen wird. Solidarität herzustellen, ist nicht nur als präventive Maßnahme sinnvoll, sondern hilft auch in akuten Fällen, um Gegenrede zu steuern. Dabei ist es wichtig, selbst keine Hassbotschaften zu verbreiten und eine vorab definierte Netiquette einzuhalten.

Netiquette

Eine Netiquette ist so etwas wie die Hausordnung für Ihre Social-Media-Kommunikation. In einem kurzen Text mit wenigen Stichpunkten definieren Sie, welches Verhalten und welche Sprache Sie sich auf Ihren Profilen wünschen, was Sie nicht wollen und wie Sie mit Verstößen gegen Ihre Netiquette umgehen werden.

Das können Sie mit Ihrer Netiquette konkret erreichen:

- Schaffen Sie einen sicheren Raum, an dem Hass, Rassismus und Diskriminierung keinen Platz haben. Sie können damit Menschen zu durchaus kontroversen, aber gewaltfreien Diskussionen motivieren.
- Informieren Sie User*innen darüber, welches Verhalten auf Ihren Seiten erwünscht ist und welches nicht.
- Klären Sie, wann Sie Inhalte melden, löschen oder blockieren und dass Sie rechtswidrige Inhalte nicht tolerieren.

Basics für eine Netiquette

- Fotos von Menschen dürfen nicht ohne deren Einwilligung gepostet werden.
- Rechtswidrige Inhalte und Inhalte, die gegen die Nutzungsbedingungen und die Community Standards verstoßen, werden ausnahmslos gemeldet bzw. gelöscht.
- Die Löschung diffamierender Kommentare, insbesondere rassistischer, antisemitischer, faschistischer, antiziganistischer, klassistischer, LGBTIQ*-feindlicher, ableistischer oder anderer extremistischer Inhalte wird angekündigt.
- Es wird um einen sachlichen Diskurs gebeten.

Mehr dazu in der MBR-Broschüre „Handlungssicher im digitalen Raum“.
Sie können sich auch an der Netiquette von HateAid orientieren:
hateaid.org/netiquette

Social-Media-Plattformen verstehen

Zum Schutz vor digitaler Gewalt gehört auch, soziale Plattformen zu kennen, sie zu verstehen und die Formen der vorherrschenden digitalen Gewalt zu kennen. Das ist wichtig, um etwa zu wissen, wie schnell sich Hasskampagnen verbreiten können, wie man darauf reagieren kann und welche Schutzmaßnahmen durch die AGBs vorgesehen sind. Das Wissen ist auch hilfreich, wenn Sie die Plattformen selbst nicht nutzen.

Unsere 2024 erschienene Studie „Lauter Hass, leiser Rückzug“ zeigt, dass auf Twitter, TikTok und Facebook besonders viel digitale Gewalt erlebt und beobachtet wird.

X (ehemals Twitter) & Hassrede

Zahlreiche Untersuchungen des CCDH (Center for Countering Digital Hate) haben ergeben, dass der Anteil von Tweets mit diffamierenden Inhalten seit der Übernahme von X durch Elon Musk im Oktober 2022 um bis zu 202 % zugenommen hat – und das, obwohl dieser Anteil zuvor schon vergleichsweise hoch war. Die Untersuchungen zeigen auch: Es hat sich etwa die Zahl der Tweets mehr als verdoppelt, die sich gegen Personen aus der LGBTQIA+-Community richten und ihnen vorwerfen, Kinder zu sexualisieren oder belästigen. Zudem wurde eine deutliche Zunahme von Inhalten und Accounts festgestellt, die den Klimawandel leugnen. **Der Algorithmus von X befeuert außerdem die Verbreitung von Rassismus, Antisemitismus und Sexismus.** Die Plattform-Betreiber*innen bleiben in 99 % der Meldungen von Hass inaktiv. Es wurde zudem beobachtet, dass gegen Hasskommentare von Twitter-Blue-Abonnent*innen nicht angemessen vorgegangen und die Verbreitung dieser zusätzlich vom Algorithmus vorangetrieben wird.[44]

TikTok & Desinformation

TikTok, das zum chinesischen Unternehmen ByteDance gehört, stand 2024 im Fokus einer Untersuchung der EU-Kommission bezüglich der Einhaltung des Digital Services Act (DSA). Es ging dabei vor allem um den Umgang von TikTok mit Jugendschutz, Datenschutz und Werbung.

Auch HateAid hat bereits eine Beschwerde gegen TikTok bei der Bundesnetzagentur eingereicht. Nach Einschätzung der Organisation ist der von der Plattform eingerichtete Meldeweg nicht benutzerfreundlich und nicht leicht genug zugänglich. Das verstößt gegen den DSA.[45]

Im Gegensatz zu anderen Sozialen Netzwerken funktioniert TikTok nicht nach dem Social-Circle-Prinzip: Während bei Facebook oder Instagram Nutzer*innen zunächst ein Profil anlegen und dann reale oder virtuelle Bekanntschaften aktiv hinzufügen müssen, schlägt TikTok von Anfang an eine Vielzahl von Videos oder auch Profilen vor, mit denen bisher keine Verbindung besteht.[46] Diese Funktionsweise ermöglicht eine schnelle Verbreitung von Desinformation, da der verbreitete Inhalt nur schwer seinem Kontext zugeordnet werden kann. Im Vergleich zu Plattformen wie YouTube erkennt TikTok Desinformation oft schlecht. TikTok wird vor allem von jungen Menschen oft als Suchmaschine genutzt und Suchanfragen führen häufiger zu irreführenden Inhalten als es bspw. bei Google der Fall ist.[47]

Die Plattform bietet zudem Funktionen wie die Möglichkeit, Audios mit wenigen Klicks zu verändern und die Stitch-Funktion[48], die ebenfalls zur Dekontextualisierung von Inhalten führen kann. Auch die fehlende Transparenz bezüglich der Informationen zur*m Ersteller*in eines Videos trägt dazu bei, dass die Glaubwürdigkeit von Inhalten schwer zu überprüfen ist.

Bisher müssen Nutzer*innen selbst überprüfen, ob Inhalte glaubwürdig sind. Prüfen Sie anhand folgender Aspekte:

- Welche Behauptungen werden in den Videos getätigt?
- Werden Quellen angegeben?
- Berichten seriöse Nachrichtenseiten über das Thema?

Überprüfen Sie die Metadaten von Bildern und machen Sie die Rückwärtssuche. Metadaten enthalten Informationen wie das Erstellungsdatum und den Aufnahmeort einer Datei, die helfen können, die Echtheit der Angaben zu bestätigen.[49]

Die Rückwärtssuche von Bildern ermöglicht es, ähnliche oder identische Bilder im Internet zu finden, um die ursprüngliche Quelle oder mögliche Manipulationen aufzudecken.[50]

Als Nutzende müssen Sie die Verfassenden oft selbst um Erläuterungen und Belege zu deren Inhalten bitten.

Facebook & geschlossene Gruppen

Auf Facebook findet digitale Gewalt auch in geschlossenen Gruppen statt. Laut Facebook sollen diese Gruppen zu mehr Privatheit und einem angeregteren Austausch führen. **Tatsächlich dienen sie jedoch häufig als Echokammern für Hass und Rechtsextremismus.** Bereits 2020 wurde die Anzahl rechtsextremer geschlossener Facebook-Gruppen auf 138 geschätzt.[51]

Recherchen des BR, WDR und NDR haben gezeigt, dass allein in diesen Gruppen über zehntausend Beleidigungen zu finden waren. Diese wurden zwar gemeldet, von Facebook aber nicht gelöscht. Ein Teil des Problems ist das eigene Empfehlungssystem von Facebook, das oft selbst extremistische Gruppen vorschlägt.[52]

So hat beispielsweise die Deutsche Umwelthilfe (DUH) bisher vergeblich versucht, Meta zu verpflichten, zwei Facebook-Gruppen zu schließen, in denen zu Gewalt, Folter und Mord gegen Mitarbeiter*innen der DUH aufgerufen wurde. Das Landgericht Berlin wies die Klage mit der Begründung ab, dass die derzeit geltende Rechtslage die begehrte Gruppenschließung nicht hergebe. Die DUH plant, in Berufung zu gehen und fordert dringend eine gesetzliche Regelung für Plattformen wie Facebook, die einen ausreichenden Schutz für Opfer von systematischer Hetze und Verfolgung in solchen Gruppen sicherstellt.[53]

Datensicherheit

Digitale Gewalt kann auch in Form von Datenmissbrauch stattfinden. Durch folgende präventive Maßnahmen schützen Sie Ihre E-Mail- und Social-Media-Konten und machen es Angreifenden schwer, in diese einzudringen:

Zwei-Faktor-Authentifizierung

Eine wichtige Maßnahme zur Sicherung Ihrer Online-Konten ist die Einrichtung einer Zwei-Faktor-Authentifizierung (2FA), wo immer möglich. Durch die Verwendung von 2FA wird ein **zusätzlicher Sicherheitsschritt** eingeführt, der es schwieriger macht, auf Ihre Konten zuzugreifen, selbst wenn jemand Ihr Passwort kennt.

So wird für eine Anmeldung neben dem Passwort z. B. ein Code angefordert, der durch die Verknüpfung mit Ihrer Mobilnummer auf Ihr Smartphone gesendet wird. Dies kann ein wichtiger Schutzmechanismus sein, um Ihre persönlichen Daten und Ihre Online-Identität zu sichern.

Sichere Passwörter

Zum Schutz vor Hasskampagnen oder Cyberstalking ist es absolut unerlässlich, Ihre Programme und Profile mit sicheren Passwörtern zu schützen. Sonst gelangen Angreifer*innen schnell an Ihre persönlichen Daten, die sie dann online verbreiten oder gezielt nutzen können, um in Ihrem Namen Nachrichten zu verschicken oder falsche Informationen zu streuen. Um das zu verhindern, beachten Sie Folgendes:

Hinweise zum Umgang mit Passwörtern

- Ein sicheres Passwort zeichnet sich dadurch aus, dass es komplex, lang, unvorhersehbar und einzigartig ist.
- Achten Sie darauf, keine persönlichen oder leicht zugänglichen Informationen in Ihre Passwörter einzubauen.
- Sollten Sie eine Benachrichtigung von einer Plattform oder einem anderen Anbieter erhalten, dass es einen Versuch gab, sich in Ihr Konto einzuloggen, sollten Sie umgehend handeln. Dies gilt auch für den Fall, dass Sie ungewöhnliche Aktivitäten auf Ihren Konten beobachten. Bitte beachten Sie hierzu auch unsere Tipps zum Thema Phishing.
- **Verwenden Sie außerdem niemals dasselbe Passwort für unterschiedliche Seiten oder Programme, weil ein gestohlenes Passwort Angreifer*innen den Zugang zu all Ihren anderen Konten ermöglicht.**

TIPP:
Für die Erstellung sicherer Passwörter und die Verwaltung unterschiedlicher Passwörter für unterschiedliche Dienste können Sie auch einen Passwortmanager verwenden. Alternativ können Sie auf Pass-Sätze[54] zurückgreifen. Denken Sie sich einfach einen Satz aus und machen Sie ihn zu einer Kombination aus verschiedenen Zeichen:

„Dieses Jahr will ich drei neue Städte besuchen und an den Strand!“
→ „DJwi3nSb+adS!“

Für die jeweilige Plattform fügen Sie entsprechende Buchstaben z. B. am Anfang und Endes des Passworts hinzu:
→ Instagram: IDJwi3nSb+adS!M
→ Facebook: FDJwi3nSb+adS!K

Schutz vor Phishing

Politische Akteur*innen werden immer häufiger zum Ziel von teils politisch motivierten Phishing-Attacken.[55] **Phishing bezeichnet den Versuch, Daten (wie Passwörter oder Kreditkartennummern) abzugreifen. Dies geschieht mittels gefälschter Webseiten, per E-Mail oder SMS.** Deswegen ist es wichtig, dass Sie sich und Ihre Mitarbeitenden regelmäßig dafür sensibilisieren.

So funktioniert Phishing:

- Sie bekommen eine E-Mail, einen Anruf oder eine SMS, die meistens so aussehen, als würden sie von einem Dienst kommen, bei dem Sie angemeldet sind, etwa Ihrer Bank, einem Paketlieferdienst oder einem digitalen Abo-Dienst.
- In der E-Mail werden Sie aufgefordert, sich einzuloggen, weil z. B. eine Sicherheitsüberprüfung anstehe oder jemand angeblich Zugriff auf Ihr Konto hatte. Zum Login werden Sie aufgefordert, auf eine Schaltfläche zu klicken. Dabei wird meistens Dringlichkeit suggeriert.
- Wenn Sie auf diese Schaltfläche klicken, gelangen Sie auf eine Login-Seite, die exakt so aussieht wie die Originalseite des Dienstes. In Wirklichkeit ist sie aber ein Nachbau. Wenn Sie sich dann bei dieser gefälschten Login-Seite einloggen, haben die Angreifenden sofort Ihr Passwort „gefischt“ und können sich damit selbst einloggen und auf alle Ihre Daten zugreifen.
- Oder aber Sie erhalten eine Mail mit Links oder Dateien von Schadsoftware. Zum Beispiel in Form von Spyware, mit der sensible Daten ausspioniert werden können. Eine andere Form der Schadsoftware stellt Ransomware dar, die Ihre Daten so verschlüsseln kann, dass Sie selbst keinen Zugriff mehr auf Ihre Konten oder Geräte haben. Beides kann zu Erpressungsversuchen führen.

So erkennen Sie Phishing-Mails:

- Sind Inhalt, Zeit oder Absender*in der E-Mail wirklich glaubhaft und nachvollziehbar?
- Stimmen die Mailadressen und URLs mit den Originaladressen und originalen URLs überein?
- Wird ein dringender Handlungsbedarf suggeriert?
- Werden Sie dazu aufgefordert, Dateien oder Links zu öffnen?

Präventiver Schutz vor Phishing

Niemals auf Links in Mails klicken. Versuchen Sie die Seite, zu der der Link angeblich führen soll, im Browser selbst einzugeben und dort zu öffnen.

Achtung: Falls Sie doch einmal auf einen Link klicken und aufgefordert werden, sich neu einzuloggen, tun Sie das auf keinen Fall! Denn hier könnten Ihr Username und Passwort abgegriffen werden. Schließen Sie zur Sicherheit die Seite und den Browser, öffnen danach eine neue Seite und loggen sich noch einmal direkt bei der Plattform ein. Wenn Sie dann wieder auf den Link in der Mail klicken und Ihr Passwort wird ERNEUT angefordert, könnte hier ein Phishing-Versuch vorliegen. **Ändern Sie in diesem Fall präventiv Ihre Passwörter. Und beobachten Sie möglicherweise unautorisierte Aktivitäten auf Ihren Konten.**

Auch große Unternehmen werden Opfer von Phishing und Daten-Leaks. Wenn Sie dort in der Kundendatenbank geführt werden, können auf diese Weise auch Ihre Daten in die Hände Dritter gelangen. Ob auf diesem Weg möglicherweise eines Ihrer Passwörter „abgefischt“ wurde, können Sie herausfinden, indem Sie Ihre E-Mail-Adressen auf einer dieser Webseiten eingeben und prüfen lassen:

- Have I been pwned?: haveibeenpwned.com
- Hasso-Plattner-Institut: sec.hpi.de

Wenn Sie von einem Daten-Leak betroffen sind, wechseln Sie sofort das Passwort und richten Sie eine Zwei-Faktor-Authentifizierung ein.

Halten Sie Ihre Updates auf dem neuesten Stand und fertigen Sie regelmäßig Backups an.

Informieren Sie sich regelmäßig über aktuelle Phishing-Maschen unter:

- verbraucherzentrale.de
- bsi.bund.de/DE
- watchlist-internet.at/

Schulen Sie sich und Ihr Personal mit der Hilfe von Unternehmen mit IT-Expertise oder fordern Sie zur Übung Phishing-Simulationen an.

Nutzen Sie Virenscanner, Datenscanner oder Fake-Website-Checker und informieren sich über aktuelle Empfehlungen und Phishing-Maschen bei der Verbraucherzentrale und dem Verbraucherschutz-Newsletter des BSI.

→ **Achtung: Diese Verfahren bieten keinen hundertprozentigen Schutz und sollten nicht als Alleinstellungsmerkmal zur Erkennung von Phishing-Versuchen verstanden werden.**

IT-Expertise einholen

Mangelnde IT-Kenntnisse sind leider häufig ein Einfallstor für Angriffe. Sie müssen aber kein*e Expert*in in diesem Bereich sein. Es ist nur wichtig, regelmäßig – und vor allem in Verdachtssituationen von Datenmissbrauch – IT-Sicherheitsexpertise einzuholen.

Wichtige Fragen sind:

- Wie erkennen Sie, ob Ihre Geräte angegriffen wurden?
- Wie können Sie Ihre Geräte schützen?
- Wie erkennen Sie, ob Ihre Konten sicher sind?
- Wie können Sie einen Hacking-Versuch nachweisen?
- Welche Maßnahmen sollten Sie nach einem Angriff ergreifen?

Schutz vor digitaler Gewalt auf Online-Veranstaltungen

Der Bildschirm wird plötzlich schwarz, mitten in einer Veranstaltung werden pornografische Bilder gezeigt oder Trolle fluten die Kommentarspalten, sodass keine Diskussion mehr denkbar ist – mögliche Störungen digitaler Veranstaltungen sind vielfältig. Es ist wichtig, dass Sie als Politiker*in oder Sprecher*in auf einer Online-Veranstaltung immer den Aspekt der digitalen Sicherheit mitbedenken und sich darüber informieren, inwiefern die Veranstaltenden sich damit auseinandergesetzt haben.

Wenn Sie selbst Veranstalter*in sind, sollten Sie Folgendes beachten:

- Nur angemeldete Personen bekommen den Link zur Veranstaltung.
- Auch im interaktiven Live-Teil einer digitalen Diskussion gilt die Netiquette und wer dagegen verstößt, muss den Raum verlassen.
- Die von Ihnen definierten Kommunikationsregeln können Sie im Voraus an die Teilnehmenden per E-Mail schicken und nochmal zu Beginn der Veranstaltung erläutern.
- Benennen Sie eine Person für die technische Sicherheit und schnelles Ausschließen von störenden Akteur*innen. Diese Rolle können auch Ehrenamtliche übernehmen. Erinnern Sie auch die Moderation aktiv daran, störenden Menschen und diskriminierenden Inhalten keinen Raum zu geben.
- Begrenzen Sie die Möglichkeit zu aktiven Audio- oder Video-Beiträgen von Teilnehmenden. Denn diese Funktionen können missbraucht werden, um durch Zwischenrufe oder das Zeigen unerlaubter Bilder und Symbole zu stören. Das ist besonders bei Veranstaltungen mit hoher Teilnehmendenzahl wichtig.
- Bereiten Sie einen Krisenplan vor und beantworten Sie sich vorab Fragen wie: Können die Täter*innen schnell identifiziert und ausgeladen werden? Ist ein Link für einen neuen digitalen Raum vorbereitet, der bei Bedarf schnell an die Teilnehmenden verschickt werden kann?
- Informieren Sie die Teilnehmenden im Vorfeld, dass für den Fall einer Störung die Veranstaltung aufgezeichnet wird, um Beweise zu sichern.

Diese Tipps und mehr finden Sie in dem Handout „Auch digital sichere Räume schaffen“ der Mobilen Beratung gegen Rechtsextremismus Berlin (MBR).[56]

Doxxing

Doxxing bezeichnet die ungefragte Veröffentlichung privater Daten einer Person im Internet. Bei den veröffentlichten Informationen kann es um Daten wie die private Wohnadresse, die Handynummer, Chatverläufe, Fotos und amtliche Dokumente gehen. Die Daten können aus öffentlichen Quellen oder gehackten Konten stammen oder anderweitig illegal beschafft werden. **Oft werden sie missbräuchlich verwendet, um Betroffene oder ihre Familienmitglieder zu belästigen, zu bedrohen oder zu erpressen.** Doxxing kann zu Belästigung, Telefonterror, der Gefährdung der Privatsphäre und sogar zu Gewaltaufrufen gegen die Betroffenen führen. **Teilweise landen geklaute Informationen auf extremistischen Todes- oder Feindeslisten.**[57] Oder Täter*innen setzen **falsche Notrufe** ab, um einen Einsatz der Polizei, der Rettung oder der Feuerwehr am Wohn- oder Arbeitsort der betroffenen Person zu provozieren („Swatting“).

Analoge Sicherheit

Wenn Menschen online zu Gewalt gegen Sie aufrufen, kann dies auch zu analoger Gewalt führen. Daher ist es wichtig, dass Sie vorsichtig mit Ihren Daten umgehen und private Daten (wie Wohnadresse, Geburtsdatum oder Ihren privaten Kalender) nicht ins Netz stellen. Diese Daten können leicht missbraucht werden.

Melderegisterauskunftssperre / Übermittlungssperre

Das Risiko, auch von analoger Gewalt betroffen zu sein, steigt, wenn Angreifende Ihre Adresse kennen. Daher ist es wichtig, Ihre private Wohnadresse geheim zu halten. Diese kann jedoch durch eine einfache Melderegisterauskunft gem. § 44 BMG bei den Meldebehörden in Erfahrung gebracht werden. Dafür braucht es in der Regel nur die Angabe bestimmter personenbezogener Informationen wie beispielsweise Ihren Namen, Ihr Geburtsdatum und/oder Ihre frühere Wohnadresse. **Wenn Sie aktiv von einer Hetzkampagne betroffen oder Zielscheibe bestimmter Gruppen sind, empfehlen wir Ihnen, eine sogenannte Melderegisterauskunftssperre gem. § 51 BMG zu beantragen.**

Damit diese durch die Meldebehörden eingetragen werden kann, müssen Sie in Ihrem Antrag erklären, welche triftigen Gründe (z. B. Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen) Sie dafür haben, eine Auskunftssperre zu beantragen. Diese Sperre wird auf zwei Jahre befristet und kann auf Antrag verlängert werden.

Die Auskunftssperre muss für jeden Wohnsitz einzeln beantragt werden.

HateAid kann Sie mit einem Begleitschreiben unterstützen, das Ihre Situation erläutert und die Notwendigkeit einer Melderegisterauskunftssperre in Ihrem Fall begründet.

Privatsphäre-Checks machen und private Daten schützen

So können Sie ihre privaten Daten schützen und Ihre eigene Sicherheit erhöhen:

- Denken Sie daran, Ihre Wohnadresse von Ihrer E-Mail-Signatur zu entfernen. Kommunalpolitiker*innen sollten prüfen, ob ihre Wohnadresse aus dem Ratsinformationssystem[58] und, wenn möglich, auch von Wahllisten genommen werden kann. Alternativ können Sie auch versuchen, wenn möglich, eine Adresse anzugeben, an der Sie zuverlässig erreichbar sind.
- Ist Ihre Wohnadresse im Impressum Ihrer Webseite veröffentlicht? Informieren Sie sich, ob Sie in diesem Fall eine andere Adresse verwenden können, an der Sie zuverlässig erreichbar sind, z. B. die Adresse Ihres oder Ihrer Arbeitgebers*in.
- Wer kennt Ihre oder die Wohnadresse Ihrer Familienmitglieder und könnte sie in bestimmten Kreisen verbreiten? Kontaktieren Sie diese Personen und sensibilisieren Sie sie für das Thema Sicherheit.
- Reden Sie mit Ihrem oder Ihrer Arbeitgeber*in darüber, dass Ihre persönlichen Informationen und Daten geheim bleiben sollen.
- Kommunizieren Sie keine Hinweise zu Ihrem Wohnort oder -viertel öffentlich und stellen Sie keine Fotos von Ihrer Straße oder Ihrem Haus ins Netz.

Wenn Sie nicht mehr wissen, wann und wo Ihre Adresse im Netz auftauchen könnte, dann suchen Sie Ihren Namen in Kombination mit einigen persönlichen Daten mit gängigen Suchmaschinen.
Einen Leitfaden finden Sie unter:
hateaid.org/privatsphaere-check/

Veranstaltungen bei der Polizei im Vorfeld melden

Durch unaufgeforderte Wortergreifung versuchen vor allem Rechtsextremist*innen, Menschen mit anderen politischen Meinungen die Bühne zu stehlen und sie so zum Schweigen zu bringen. Oft verwendete Methoden, um Veranstaltungen zu stören, sind: Flugblätter in den Saal werfen, andauerndes Hineinrufen oder das Abspielen lauter Musik. So sollen unliebsame Reden, Diskussionen oder auch Theaterstücke behindert werden. Das können Sie dagegen tun:

Maßnahmen gegen Störungen:

- Bevor Sie als Sprecher*in zu einer Veranstaltung gehen, fragen Sie die Veranstaltenden nach deren Sicherheitsmaßnahmen.
- Sind die Technikverantwortlichen über dieses Thema und die potenzielle Gefahr informiert? Ist die Moderation darauf vorbereitet?
- Um Wortergreifungen zu vermeiden, achten Sie darauf, dass die Moderation auch bei Fragen aus dem Publikum immer das Mikrofon und damit die Kontrolle behält.
- In Städten mit starken rechtsextremen Strukturen ist es wichtig, die Veranstaltung schon im Vorfeld bei der Polizei anzumelden.
- Die Sicherheit Ihrer Gäste geht vor, daher ist es besonders bei öffentlichen Veranstaltungen empfehlenswert, auch Sicherheitsexpert*innen am Einlass zu platzieren, die Extremist*innen erkennen, ihnen keinen Zugang gewähren oder bei Angriffen intervenieren.
- Wenn Sie selbst eine Veranstaltung planen, ist es wichtig, einen Sicherheitsplan zu entwickeln, der diese Punkte beachtet.

Die Mobilen Beratungsteams gegen Rechtsextremismus, die im Bundesverband Mobile Beratung vernetzt sind, können Sie diesbezüglich umfassend beraten und unterstützen.

2.2 Handlungsmöglichkeiten in akuten Situationen

Konsequenzen von digitaler Gewalt auf die Psyche

Die Kommunikation auf Social-Media-Kanälen erfolgt auf Distanz – oft kennen Betroffene die angreifende Person nicht. Dennoch kann sich ein Angriff sehr persönlich anfühlen. Angegriffene berichten, dass sie sich bloßgestellt, allein und hilflos gefühlt haben. Viele erleben starke Schamgefühle. **Leider werden digitale Angriffe häufig kleingeredet und nicht als psychische Gewalt anerkannt, obwohl sie oft öffentlich und unerwartet verübt werden.** Gerade das macht es Betroffenen schwer, sich emotional davon abzugrenzen. Teilweise werden Betroffene sogar selbst für die Angriffe verantwortlich gemacht, z. B. von ihren Arbeitgeber*innen oder von Institutionen wie der Polizei.

In diesen Fällen spricht man von Victim blaming bzw. Opferbeschuldigung. Betroffene hören dann oft Aussagen wie: „Warum sind Sie überhaupt darauf eingegangen?“, „Vielleicht haben Sie die Situation ja selbst provoziert?“ oder „Wenn Sie auf Social Media aktiv sind, dann müssen Sie mit sowas rechnen.“

Eigene Psyche schützen

Auch wenn sich digitale Angriffe online abspielen, haben sie vieles mit analoger Gewalt gemeinsam: **Betroffene sind teilweise einer enormen psychischen Belastung ausgesetzt, die sich in Form von Ängsten, sozialer Isolation, depressiven Stimmungen und Suizidgedanken äußern kann.** Hohe Belastungszustände können zu psychosomatischen Erscheinungen wie Kopfschmerzen, Übelkeit oder Erbrechen führen. Diese Zusatzbelastungen spielen bei Politiker*innen eine große Rolle, da sie in ihrem Arbeitsbereich häufig sehr exponiert sind.

Außerdem können existenzielle Konsequenzen von digitaler Gewalt, wie zum Beispiel Rufschädigung oder Berufsverlust, starke psychische Belastungen für die Betroffenen und alle ihnen nahestehenden Personen verursachen. Wenn Sie selbst betroffen sind, machen Sie sich klar:
Digitale Gewalt ist psychische Gewalt. Nehmen Sie sie sehr ernst und machen Sie sich bewusst, dass Sie eine Gewalterfahrung erleben, wenn Sie im Internet angegriffen werden. Seien Sie in einem solchen Fall aufmerksam mit sich selbst und achten sie darauf, Ihre eigenen Grenzen und Kapazitäten zu erkennen. Fragen Sie sich immer zuallererst:

„Was macht die Situation mit mir?

Was brauche ich jetzt?

Was würde mir jetzt ein gutes, sichereres Gefühl geben?“

Wenn es Ihnen nicht gut geht, überlegen Sie sich, ob Sie mit einer Person aus Ihrem Umfeld oder aus Ihrem Team darüber sprechen können. Wichtig ist, dass Sie den emotionalen Druck, den das Erleben von digitaler Gewalt verursachen kann, nicht unterschätzen. Schaffen Sie sich den Raum, um die Situation zu begreifen und zu verarbeiten.

Hasskampagnen oder Drohmails können eine traumatische Erfahrung sein. Sprechen Sie mit Expert*innen darüber.

Unterschätzen Sie nicht die psychische Belastung von digitalem Hass

Sie können HateAid in solchen Akutsituationen zu unseren Sprechzeiten per Telefon oder Chatberatung auf unserer Webseite und jederzeit per Mail oder Meldeformular kontaktieren. Unsere Berater*innen unterstützen Sie durch emotional-stabilisierende Erstberatung dabei, Ihre Gedanken zu ordnen und eine individuelle Strategie zu entwickeln, wie Sie mit der Situation umgehen können.

Kommunikation

Wenn Sie von digitaler Gewalt betroffen sind, fühlen Sie sich am Anfang vielleicht überfordert und hilflos. Wichtig ist jetzt, sich aktiv daran zu erinnern, dass Sie auch in akuten Situationen handlungsfähig sind und Ihnen verschiedene Möglichkeiten zur Reaktion offenstehen.

Gegenrede (Counter Speech)

Eine der Strategien zum Umgang mit problematischen Kommentaren besteht darin, auf sie zu reagieren. Wenn Sie die emotionalen Kapazitäten dazu haben, ist es wichtig, Gegenrede zu leisten.

Wann? Reagieren Sie auf sachliche und konstruktive Kommentare und nicht auf reine Provokationen.

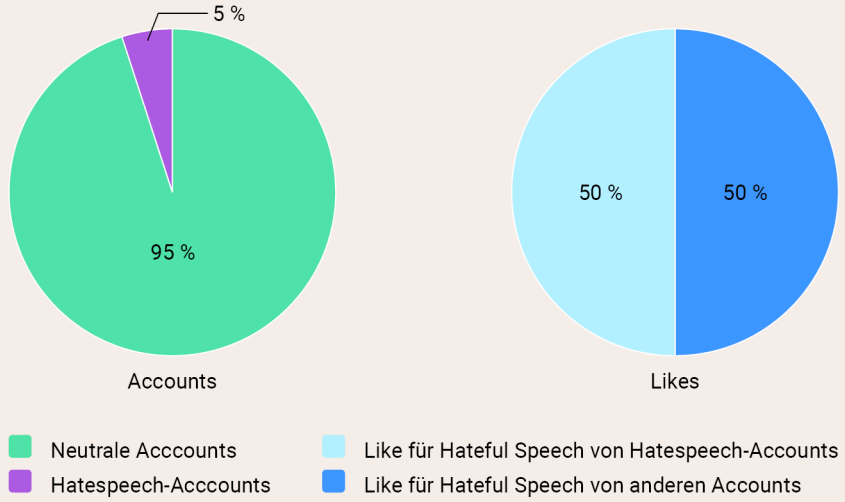
Wie? Besonders für Politiker*innen und Personen des öffentlichen Lebens ist es wichtig, genau zu überlegen, was sie schreiben und wie. Grundsätzlich empfehlen wir Folgendes:

- **Priorisierung**: Nicht alle Kommentare müssen beantwortet werden. Suchen Sie die Themen aus, die von mehreren Menschen in den Kommentaren angesprochen wurden oder beantworten Sie zuerst die Kommentare, die viele Likes bekommen haben – solange es keine provokanten Kommentare sind.
- **Gehen Sie nicht auf provokante Kommentare ein**: Sie führen fast nie zu einer politischen Diskussion, sondern sind nur zur Ablenkung und Ressourcenverschwendung gedacht.
- **Klar und verständlich positionieren**: Verwenden Sie einfache, kurze und deutliche Formulierungen.
- **Deeskalieren**: Bleiben Sie bei Ihrem Ziel, eine gute Diskussionskultur und -atmosphäre zu schaffen. Bleiben Sie respektvoll und sachlich. Verwenden Sie keine Kategorien wie „wahr / unwahr" oder „falsch / richtig". Wenn mit Fakten und Zahlen argumentiert wird, fordern Sie die Quellen ein und verwenden Sie selbst empirische Daten für Ihre Argumente. Wenn Sie eine Argumentationssammlung haben, können Sie diese hier einsetzen.
- **Keine Endlosdiskussionen**: In der Regel können Sie davon ausgehen, dass eine Person, die nach drei Kommentaren nicht auf Sie zugeht, kein Interesse an einem Meinungsaustausch hat. Lassen Sie sich also nicht auf Endlosdiskussionen ein, sondern beenden Sie diese nach etwa drei Antwortkommentaren.

→ Mehr zu Kommunikationsstrategien auf Seite 12f. und 24f.

Warum? Es handelt sich bei den Menschen, die Hass im Netz verbreiten, meist um eine sehr kleine Minderheit – jedoch um eine laute. Daneben gibt es weit mehr still Mitlesende, die die hitzigen Diskussionen im Netz nur passiv verfolgen. Für diese Menschen reagieren Sie auf Kommentare und leisten Gegenrede. Denn so zeigen Sie, wie sichere Debattenkultur funktioniert und motivieren im Idealfall die Stillen zum Interagieren.

Laut der Studie „Hass auf Knopfdruck" sorgen gerade mal 5 % der hoch aktiven Accounts für 50 % der Likes unter Hasskommentaren.[59]



Quelle: Institute for Strategic Dialogue, #ichbinhier. (2018). Hass auf Knopfdruck.

Ein Statement veröffentlichen

Schweigen ist auch eine Antwort und kann manchmal negative oder sogar gefährliche Konsequenzen nach sich ziehen – zum Beispiel, wenn falsche Tatsachen über Sie verbreitet werden. Eine Möglichkeit sich zu wehren, ist ein Statement zu verfassen. Ein Statement kann etwa als kurzer Kommentar auf einer Social-Media-Plattform unter einem Beitrag geteilt (und gepinnt) werden. Es kann aber auch als ausführlicher Text prominent auf Ihrer Webseite oder Ihren Social-Media-Kanälen veröffentlicht werden. Wichtig ist, sich folgende Frage zu stellen und ein paar Dinge zu beachten:

Zu welchem Zeitpunkt wollen Sie Ihr Statement veröffentlichen? Tun Sie es dann, wenn Sie voraussichtlich auch die emotionalen und zeitlichen Kapazitäten dafür haben, falls es zu starken Gegenreaktionen kommt.

1. Welche Sprache wird in Ihrem Statement verwendet, um die gewünschte Zielgruppe anzusprechen? Achten Sie darauf, dass Sie im emotionalen Stress selbst keine diffamierenden oder abwertenden Inhalte oder Formulierungen verwenden.

2. Involvieren Sie andere Akteur*innen, die das Statement mitunterzeichnen. Das gibt Ihnen und Ihrem Statement ein größeres Gewicht. Das hilft, besonders wenn falsche Tatsachen verbreitet wurden, diese schnell zu korrigieren.

3. Bitten Sie Bekannte oder Freund*innen, die sich mit dem Thema auskennen, das Statement gegenzulesen und Ihnen ein neutrales Feedback zu geben. So gehen Sie sicher, dass Ihr Statement nicht nur eine kurzfristige emotionale Reaktion ist, sondern wirklich das Anliegen transportiert, das Sie kommunizieren wollen.

HateAid kann Sie bei diesem Prozess mit psychosozialer Kommunikationsberatung unterstützen.

Solidarität aktivieren

Gemeinsam ist es einfacher, Gegenrede zu leisten. Besonders, wenn Sie gerade eine Hasskampagne erleben oder auf eine Verleumdung reagieren wollen.

Wenn Sie akut betroffen sind und noch kein Solidaritätsnetzwerk aufgebaut haben, ist es mit viel Aufwand verbunden, einzelne potenzielle Verbündete anzusprechen. Suchen Sie daher gezielt nach Menschen, mit denen Sie bereits in Kontakt sind, sowie Personen, die Sie unterstützen und andere Menschen aktivieren können. Dabei zählt zuerst die Qualität der Unterstützung, nicht die Anzahl der Unterstützenden.

An die Empathie appellieren

Empathie ist eine besonders effektive Strategie zur Eindämmung von Hasskommentaren im Internet. Stop Hate Speech hat die Studie „Gegen Hassrede hilft Empathie“ initiiert, die von Forscher*innen der ETH und der Universität Zürich durchgeführt wurde. Sie zeigt, dass Appelle an das Mitgefühl der Hassverfasser*innen wie etwa „Stell dir vor, wie schmerzhaft so ein Kommentar für eine Person sein muss, die trans* ist.“ am ehesten dazu beitragen können, ihr Verhalten zu verändern.[60]

Mit Humor reagieren

Es ist wichtig, Menschen, die Hass im Netz verbreiten, keine Bühne zu bieten. Wenn Sie aber auf sie reagieren, kann es sowohl für Sie als auch für andere sehr stärkend sein, wenn Sie auf die problematischen Inhalte humorvoll reagieren. Somit schaffen Sie für sich Distanz und nehmen den Kommentaren gleichzeitig die Ernsthaftigkeit. Auf der Seite No Hate

Speech finden Sie Graphiken und Memes zu unterschiedlichen Themen, mit denen Sie schnell auf Nachrichten reagieren können: no-hate-speech.de/.

Aber Achtung, Humor ist eine wirksame Strategie für Gegenrede, insbesondere wenn es darum geht, die Mitlesenden zu erreichen und sich selbst zu bestärken. Bei den Hater*innen hingegen bewirkt man damit nicht, dass sie weniger Hass verbreiten, wie die Studie „Gegen Hass hilft Empathie“ zeigt.[61]

Melden
bzw. Löschen

Bei manchen Kommentaren ist klar, dass es den Verfassenden von vornherein nicht um eine konstruktive Diskussion ging, sondern nur um Diffamierung. Lassen Sie sich davon nicht verunsichern und denken Sie an die eigene Netiquette, in der die Regeln klar und deutlich definiert sind. Alles, was gegen die Netiquette verstößt, darf konsequent gemeldet bzw. gelöscht werden, auch wenn der Kommentar bereits Likes bekommen hat. Das sollten Sie auch transparent kommunizieren und umsetzen. Das ist wichtig, um zu zeigen, dass Sie sich an die Regeln halten und den sicheren Ort, der Ihre Seite für Sie und für alle andere Nutzer*innen sein soll, schützen können. Aber Achtung! Bevor Sie Kommentare löschen, erstellen Sie rechtssichere Screenshots von ihnen, für den Fall, dass Sie später rechtliche Schritte gegen die Verfassenden einleiten wollen.

→ Anleitung auf Seite 50f.

HateAid kann Sie bei Fragen zur Anfertigung rechtssicherer Screenshots unterstützen.

Melden – Community Richtlinien,
Digital Services Act

Sie möchten, dass die Plattform bestimmte Kommentare löscht? Sie können grundsätzlich zwei Möglichkeiten nutzen, um Kommentare auf Plattformen zu melden. Hierfür gibt es meist direkt beim betreffenden Kommentar eine Meldeoption – oft mit einem Flaggensymbol oder einem Ausrufezeichen gekennzeichnet. Wenn Sie daraufklicken, schlagen Ihnen die Plattformen unterschiedliche Meldegründe vor. Diese können sich je nach Plattform unterscheiden: Meldungen wegen Verstößen gegen die plattforminternen Community-Richtlinien, z. B. Desinformation oder Formen von Hetze, die bestimmte Plattformen auf Basis der eigenen Geschäftsbedingungen angeben, nicht zu dulden, oder um Meldungen von rechtswidrigen Inhalten auf Grundlage des Digital Services Act. Bei Letzterem handelt es sich um eine Verordnung der Europäischen Union, die Online-Plattformen regulieren und digitale Gewalt reduzieren soll.

Weitere Informationen zum Digital Services Act
finden Sie in unserem DSA-User-Guide.

Beachten Sie: Je nachdem, welchen Meldegrund Sie auswählen, sind die Plattformen zu unterschiedlichen Reaktionen auf Ihre Meldungen verpflichtet.

Möglichkeiten für Meldungen

- **Meldung nach Community-Richtlinien**
  Jede Plattform definiert ihre eigenen Community-Richtlinien. Wenn Sie einen Kommentar melden, weil er Ihres Erachtens gegen diese Community-Richtlinien verstößt, wird die Plattform überprüfen, ob dem tatsächlich so ist und den Kommentar entsprechend löschen oder nicht.
- **Meldungen auf Grundlage des Digital Services Act (DSA)**
  Wenn Sie einen Kommentar als rechtswidrig melden, muss die Plattform prüfen, ob der Kommentar nach nationalem Recht rechtswidrig ist. In Deutschland sind etwa Beleidigung, üble Nachrede, Volksverhetzung oder Bedrohung strafbar. Sofern es sich um einen solchen rechtswidrigen Inhalt handelt, sind die Plattformen verpflichtet, diesen zu entfernen.

Reagiert die Plattform nicht auf Ihre Meldung, dauert die Rückmeldung zu lange oder wird Ihre Meldung abgewiesen, können Sie nach der Meldung auf Grundlage des DSA verschiedene weitere Maßnahmen ergreifen:

- Sie können den internen Beschwerdeweg nutzen, um eine erneute Überprüfung Ihrer Meldung zu verlangen.
- Wenn Ihre Meldung nicht erfolgreich war, können Sie sich an bestimmte zivilgesellschaftliche Organisationen mit einem sog. „Trusted-Flagger-Status“ wenden. Diese können Sie bei der Meldung über einen privilegierten Meldeweg aufgrund ihres Status unterstützen. Eine Liste der Trusted Flagger der Europäischen Kommission finden Sie auf der Webseite der Europäischen Union.
- Sie können für eine unabhängige Bewertung Ihres Falles auch eine sog. außergerichtliche Streitbeilegung einfordern.[62]
- Sie können Beschwerde bei der Koordinierungsstelle für digitale Dienste einlegen, wenn Sie den Eindruck haben, dass der Digital Services Act missachtet wird. In Deutschland ist das die Bundesnetzagentur.[63]

Manche Plattformen fordern Sie bei der Meldung von rechtswidrigen Inhalten dazu auf, einzuschätzen, welche Straftat hier vorliegt. Hier können Sie einfach Ihre Vermutung angeben. Sie müssen nicht sicher wissen, um welche Straftat es sich handelt. Die Plattform ist in jedem Fall verpflichtet, Ihrer Meldung nachzugehen und den Kommentar zu prüfen.

Warum ist es wichtig, sich auch rechtlich zur Wehr zu setzen?

Man kann diskriminierende und beleidigende Kommentare immer wieder melden, doch für eine strukturelle und langfristige Veränderung reicht das nicht. Dafür ist es wichtig, Hasskommentare und digitale Gewalt auch anzuzeigen. Denn:

- § Strafverfolgung hat einen starken Abschreckungseffekt und kann dazu führen, dass potenzielle Täter*innen sich in Zukunft aus Sorge vor möglichen Konsequenzen dagegen entscheiden, digitale Gewalt zu verüben.
- § Ermittlungsbehörden können in vielen Fällen die Identität der Täter*innen herausfinden. Dies ist z. B. wichtig, wenn Sie auch zivilrechtlich gegen Angreifende vorgehen wollen.
- § Mehr Anzeigen steigern das Bewusstsein der Strafverfolgungsbehörden, dass hier ein strukturelles Problem vorliegt. Anzeigen wegen digitaler Gewalt fließen außerdem in die Kriminalstatistik ein. Dadurch wird digitale Gewalt besser dokumentiert. So erhält das Thema auch mehr Aufmerksamkeit in der Politik und Gesetzgebung.
- § Anzeigen machen deutlich, dass es sich nicht um (vernachlässigbare) Einzelfälle handelt, sondern um ein umfassendes strukturelles Problem und eine Gefahr für unsere Demokratie.

Um rechtlich gegen digitale Gewalt vorgehen zu können, ist es sehr hilfreich, Beweise, z. B. rechtssichere Screenshots, zu erstellen und aufzubewahren.

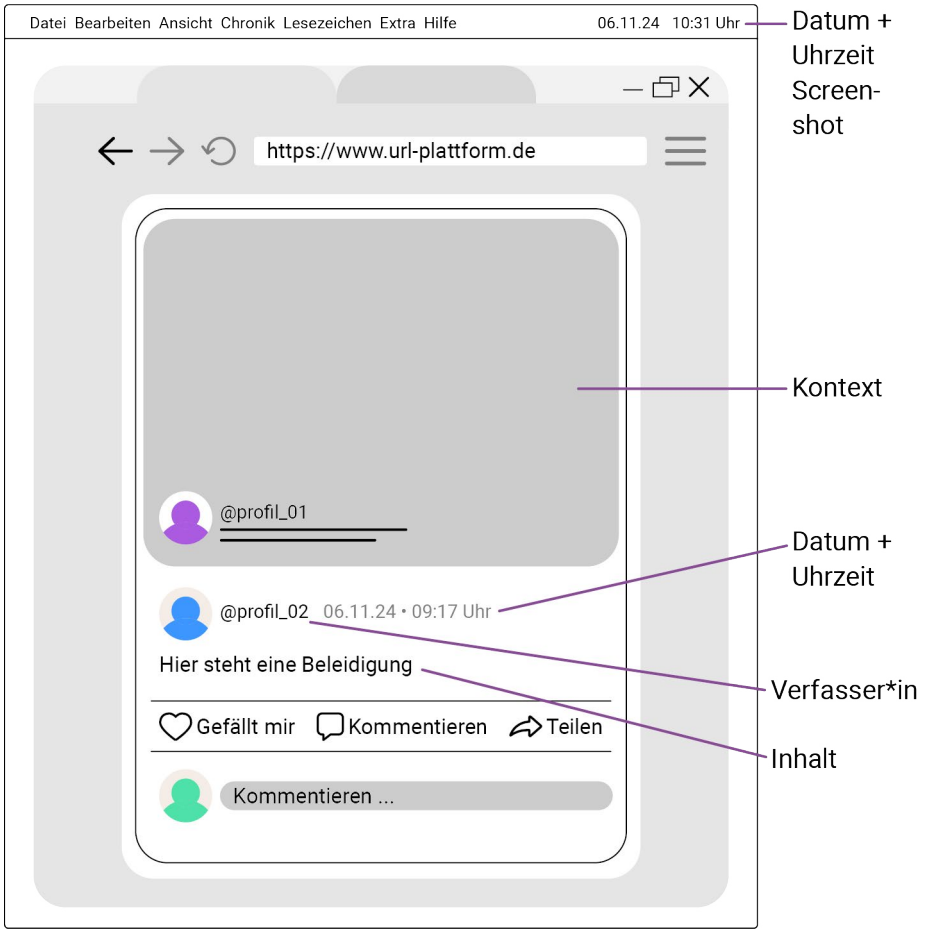
Beweissicherung (rechtssichere Screenshots)

Als Beweis für einen digitalen Angriff sind rechtssichere Screenshots (also Bildschirmfotos) von dem Kommentar oder Inhalt, den Sie zur Anzeige bringen wollen, von großer Bedeutung. Auf dem Screenshot sollten folgende Informationen zu sehen sein:

- **Inhalt** (also etwa der Hasskommentar oder Blogbeitrag, der angezeigt werden soll – oder die Bedrohung in einer E-Mail)
- **Kontext des Inhalts** (beispielsweise die Kommentare oder Statements, auf die sich der Hasskommentar bezieht, oder das Video, worunter der Kommentar steht. Oft sind deshalb mehrere Screenshots erforderlich, um den Kontext nachvollziehbar abbilden zu können.)
- **Datum**
(Wichtig: im Format tt.mm.jjjj)
- **Uhrzeit**
(Wichtig: im Format ss:mm)
- **Verfassende Person**, ggf. separater Screenshot des Profils inkl. URL
- **URL des Kommentars**, ggf. URL des Ausgangsposts

Achtung: Bei Mails zusätzlich Headerdaten und Mail als Datei sichern! Headerdaten in Mails sind Metadaten, die Informationen über die Absender*innen, Empfänger*innen, den Betreff, den Versandzeitpunkt und den Übertragungsweg der E-Mail enthalten.

Eine Anleitung zur Erstellung rechtssicherer Screenshots auf unterschiedlichen Plattformen finden Sie auch auf unserer Webseite unter hateaid.org/rechtssichere-screenshots.



Wir empfehlen zur Anfertigung von rechtssicheren Screenshots die kostenlose Google-Chrome-Erweiterung Atomshot.[64] Das ist ein Screenshot-Tool mit dem man Bildschirmfotos von einer Internetseite erstellen kann. Das Tool versieht den Screenshot mit der genauen URL, dem Datum und der atomuhrgenauen Uhrzeit.

Zeug*innen kontaktieren

Sollten Sie keine rechtssicheren Screenshots haben, kann es sinnvoll sein, potenzielle Zeug*innen zu kontaktieren. Zeug*innen können sein:

- Personen aus Ihrem Umfeld, die evtl. rechtssichere Screenshots von den Angriffen gegen Sie gemacht haben.
- Personen aus Ihrem Umfeld, die die Situation, den Kommentar oder die Nachricht gesehen haben.
- Menschen, die sich in einer Kommentarspalte mit Ihnen solidarisch gezeigt haben.

Kontaktieren Sie diese Personen und bitten Sie um Unterstützung.

3 Möglichkeiten der Rechtsdurchsetzung

3.1 Strafrecht und Zivilrecht

Um sich rechtlich gegen digitale Gewalt zu wehren, gibt es in Deutschland vor allem zwei Möglichkeiten: Betroffene können strafrechtlich und / oder zivilrechtlich gegen die mutmaßlichen Täter*innen vorgehen.

Strafrecht

Bei einem Strafverfahren geht es in erster Linie darum, dass Täter*innen für ihr rechtswidriges Verhalten zur Verantwortung gezogen werden, indem sie zum Beispiel zu einer Freiheitsstrafe oder einer Geldstrafe verurteilt werden. Diese Aufgabe übernehmen die zuständigen Strafverfolgungsbehörden und die Gerichte. Das Ziel eines Strafverfahrens ist es dabei aber nicht, dass Hasskommentare entfernt werden oder Sie als geschädigte Person eine Entschädigung erhalten.

Zivilrecht

Ein zivilrechtliches Vorgehen hingegen dient, anders als das Strafrecht, zur Durchsetzung Ihrer persönlichen Rechte und Ansprüche gegen Täter*innen. Das kann ein Anspruch auf Löschung von Hasskommentaren sein, die Verpflichtung der Täter*innen zur Unterlassung solcher Hasskommentare gegen Sie in der Zukunft oder, bei schweren Persönlichkeitsrechtsverletzungen, auch eine Geldentschädigung. Für ein zivilrechtliches Vorgehen brauchen Sie die Unterstützung durch eine*n Anwält*in. Anders als das Strafrecht sind zivilrechtliche Schritte nicht kostenlos. Das Kostenrisiko, z. B. für die Anwalts- und Gerichtskosten, tragen Sie.

3.2 Straftatbestände im Überblick

Beleidigung

„Halt du mal deine Fresse linke Vo***."

Eine Beleidigung (§ 185 StGB) liegt vor, wenn eine Person eine missachtende oder herabwürdigende, ehrverletzende Meinung über Sie äußert. Das kann verbal, durch Gestik, Schrift oder Bilder geschehen. Unter bestimmten Voraussetzungen kann auch ein ganzes Kollektiv als solches oder Personen als Teil einer Gruppe beleidigt werden. Die Tat wird grundsätzlich nur dann verfolgt, wenn die verletzte Person das mittels Strafantrag beantragt.

Hinweis: Ein Strafantrag ist Ihre ausdrückliche Erklärung, dass Sie die Strafverfolgung wünschen. Er muss innerhalb von drei Monaten ab Kenntnis von Tat und Täter*in gestellt werden. Wenn Sie keinen Strafantrag stellen, die Frist versäumen oder den Antrag zurücknehmen, können die Strafverfolgungsbehörden das Verfahren nicht mehr ohne Weiteres fortsetzen.

§ Strafe

- Freiheitsstrafe bis zu einem Jahr oder Geldstrafe.
- Wenn die Beleidigung öffentlich begangen wird, in einer Versammlung oder durch das Verbreiten eines Inhalts z. B. im Netz, dann kann sie mit einer Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft werden.
- Richtet sie sich gegen Personen des politischen Lebens, wie bspw. kommunal Engagierte oder Kommunalpolitiker*innen, kann die Freiheitsstrafe unter bestimmten Voraussetzungen sogar bis zu drei Jahren betragen (§ 188 StGB).

Üble Nachrede und Verleumdung

„Blockt das Profil von facebook.com, sie ist ein Spitzel von Facebook, die nur eure Bilder ins Netz stellen will!"

Eine üble Nachrede (§ 186 StGB) oder Verleumdung (§ 187 StGB) kann vorliegen, wenn unwahre Tatsachen über Sie verbreitet werden. Die unwahre Tatsache muss dabei geeignet sein, Sie herabzuwürdigen oder Sie zu diffamieren.

- Anders als bei der Beleidigung wird hier eine unwahre Tatsache (objektiv beweisbar) und keine rechtswidrige Meinungsäußerung (subjektives Werturteil) verbreitet.
- Es spielt keine Rolle, ob die Person selbst glaubt, dass die Behauptung wahr ist oder ob sie die Behauptung von einer dritten Person (z. B. durch das Teilen in sozialen Netzwerken) ungeprüft übernommen hat.
- Üble Nachrede: Wenn jemand eine abwertende Tatsache über Sie behauptet, diese allerdings nicht bewiesen werden kann, dann handelt es sich in der Regel um üble Nachrede.
- Verleumdung: Weiß die Person sogar, dass es sich um eine falsche Tatsache handelt und verbreitet sie dennoch, dann liegt in der Regel eine Verleumdung vor.
- Auch Organisationen (Vereine, Verbände etc.) können verleumdet werden.
- Die Tat wird nur dann verfolgt, wenn die verletzte Person das beantragt (Strafantrag).

§ Strafe

- Bei übler Nachrede droht eine Freiheitsstrafe bis zu einem Jahr oder Geldstrafe.
- Bei Verleumdung droht eine Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.
- Wenn sie öffentlich begangen wird, in einer Versammlung oder durch das Verbreiten eines Inhalts z. B. im Netz, kann
  - üble Nachrede mit einer Freiheitsstrafe von bis zu zwei Jahren oder mit Geldstrafe geahndet werden und
  - Verleumdung mit einer Freiheitsstrafe bis zu fünf Jahren oder einer Geldstrafe.
- Bei Personen des politischen Lebens, wie z. B. kommunal Engagierten oder Kommunalpolitiker*innen, kann die Freiheitsstrafe bei übler Nachrede drei Monate bis fünf Jahre betragen, bei einer Verleumdung sechs Monate bis zu fünf Jahre. Eine Geldstrafe ist nicht möglich (§ 188 StGB).

Nötigung

„Wenn du deinen Artikel nicht löschst, polier ich dir die Fresse."

Eine Nötigung (§ 240 StGB) liegt vor, wenn Sie jemand mit Gewalt oder durch Drohung gegen Ihren Willen zu einem bestimmten Verhalten zwingen will.

- Das Verhalten kann in Handeln, Dulden oder Unterlassen bestehen.
- Die Drohung muss dabei im Verhältnis zum angestrebten Verhalten verwerflich sein.
- Der Versuch einer Nötigung ist strafbar.

§ Strafe

- Eine Nötigung kann mit einer Freiheitsstrafe bis zu drei Jahren oder mit einer Geldstrafe geahndet werden.

Bedrohung

„Dich Penner werde ich bekommen. Ich stech dich ab!"

Eine Bedrohung (§ 241 StGB) liegt vor, wenn jemand Sie oder eine Ihnen nahestehende Person mit einer bestimmten rechtswidrigen Tat bedroht. Dies kann entweder ein Verbrechen sein, das heißt eine schwere Straftat, die mit mindestens einem Jahr Freiheitsstrafe geahndet wird, oder eine andere in § 241 StGB aufgeführte Tat, zum Beispiel die Androhung einer Vergewaltigung oder Körperverletzung oder in bestimmten Fällen sogar eine Sachbeschädigung.

- Auch die Vortäuschung eines Verbrechens ist strafbar, etwa wenn man Sie glauben lässt, dass ein Verbrechen gegen Sie begangen wird.
- Die Bedrohung muss ernst zu nehmend sein. Das bedeutet, dass objektiv der Eindruck der Ernstlichkeit erweckt werden muss. Dabei ist es nicht relevant, ob die betroffene Person die Bedrohung tatsächlich ernst nimmt. Vielmehr kommt es darauf an, ob die Bedrohung aus Sicht eines durchschnittlichen Beobachtenden ernst zu nehmen sein könnte.

§ Strafe

- Bedrohung mit einem Verbrechen kann mit Geld- oder Freiheitsstrafe bis zu zwei Jahren bestraft werden.
- Bedrohung mit einer bestimmten anderen rechtswidrigen Tat kann mit einer Geld- oder Freiheitsstrafe bis zu einem Jahr bestraft werden.
- Wenn sie öffentlich begangen wird, in einer Versammlung oder durch das Verbreiten eines Inhalts z. B. im Netz, kann sie mit einer Freiheitsstrafe bis zu zwei beziehungsweise drei Jahren (bei Bedrohung mit Verbrechen) oder mit Geldstrafe geahndet werden.

Belohnung und Billigung von Straftaten

„Dann wünsche ich dir, dass du von all deinen geliebten „Flüchtlingen“ mal so richtig ran genommen wirst, ohne dass du das möchtest.“

Der Straftatbestand Belohnung und Billigung von Straftaten (§ 140 StGB) wurde im Jahr 2021 durch das Gesetzespaket zur Bekämpfung von Rechtsextremismus und Hasskriminalität maßgeblich abgeändert. Damit wurde eine wichtige Regelungslücke geschlossen. Denn bisher war nur die Billigung einer bereits begangenen Straftat strafbar. Nicht erfasst waren hingegen Fälle, in denen Personen Straftaten befürwortet hatten, die (noch) nicht begangen worden waren. Somit waren bisher zum Beispiel Vergewaltigungswünsche nicht strafbar.

Inzwischen ist die öffentliche oder durch Verbreitung von Inhalten begangene Billigung von bestimmten, im Gesetz aufgezählten Straftaten, wie etwa Vergewaltigung oder schwere Körperverletzung, strafbar. Und zwar auch dann, wenn sie noch nicht begangen wurden.

Die Belohnung einer Straftat z. B. mit einer Geldzahlung oder einer Auszeichnung, setzt hingegen weiterhin voraus, dass eine Straftat bereits begangen wurde.

§ Strafe

- Freiheitsstrafe bis zu drei Jahre oder Geldstrafe.

Nachstellung / Stalking

Wenn eine andere Person Sie unbefugt und wiederholt auf eine Weise verfolgt, die Sie in Ihrem Alltag stark beeinträchtigt, macht sie sich der sogenannten Nachstellung (§ 238 StGB) strafbar, besser bekannt als Stalking.

Verfolgung kann in verschiedenen Formen auftreten. So kann es Stalking sein, wenn jemand Sie wiederholt aufsucht oder Ihnen immer wieder Nachrichten sendet. Wenn jemand Sie telefonisch terrorisiert oder Dritte dazu auffordert, Sie zu kontaktieren oder auch, wenn jemand Ihre Daten missbraucht und in Ihrem Namen Bestellungen aufgibt. Letzteres erfahren häufig Betroffene von Doxxing (Seite 36). Auch das Verbreiten von Bildmaterial, das Sie betrifft, oder das Anlegen eines Fake-Profils in Ihrem Namen können hierunter fallen.

§ Strafe

- Freiheitsstrafe bis zu drei Jahre oder Geldstrafe, in besonders schweren Fällen mit Freiheitsstrafe von drei Monaten bis fünf Jahren.

Volksverhetzung

„Das sind keine Flüchtlinge, sondern Parasiten!“

„Armes armes Deutschland, wo sind wir nur hier angelangt, wenn Kan***en wie Sie jetzt auch noch höhere politische Ämter bekleiden dürfen.“

Volksverhetzung (§ 130 StGB) liegt meist dann vor, wenn gegen eine bestimmte Bevölkerungsgruppe (zum Beispiel Geflüchtete, Menschen jüdischen Glaubens, Migrant*innen, LGBTIQ* oder Frauen) zu Hass aufgestachelt oder zu Gewalt aufgerufen wird. Volksverhetzung kann auch dann vorliegen, wenn eine solche Gruppe in einer Art und Weise beschimpft oder verleumdet wird, dass sie in ihrer Menschenwürde angegriffen wird.

Es gilt auch als Volksverhetzung (mit geringerer Strafandrohung), wenn hetzende Inhalte öffentlich verbreitet, beworben oder angeboten werden. Dafür müssen Täter*innen nicht die Urheber*innen der Inhalte sein.

§ Strafe

- Volksverhetzung ist kein Kavaliersdelikt. Sie wird mit Freiheitsstrafen von bis zu fünf Jahren geahndet.

Die Bestrafung von Volksverhetzung dient nicht nur dem individuellen Schutz vor Hetze, sondern auch allgemein dem friedlichen gesellschaftlichen Zusammenleben.

4 Was Institutionen & Arbeitgeber*innen tun können

Unternehmen können mit ihrer Reichweite viel bewirken, z. B. wenn sie sich öffentlich für demokratische Werte einsetzen. Dabei können Mitarbeitende jedoch zur Zielscheibe von digitaler Gewalt werden, etwa weil sie als Angestellte online erkennbar sind. **Entscheiden sich Unternehmen dafür, sich öffentlich zu positionieren, sollten sie von Beginn an den Schutz ihrer Mitarbeitenden mitdenken – präventiv und in akuten Krisen.**

Folgende Maßnahmen können Arbeitgeber*innen und Institutionen treffen, um für ihre haupt- und ehrenamtlich Engagierten Verantwortung zu übernehmen:

Datenschutz

- Richten Sie Ihren Mitarbeitenden separate E-Mail-Adressen für Ehrenämter und Mandate ein, um ihre Privatsphäre weitgehend zu schützen. Sie sollten nicht mit privaten E-Mail-Adressen arbeiten.
- Behandeln Sie die Telefonnummern vertraulich und ermöglichen Sie, wo immer möglich, Firmenhandys.
- Bleiben Sie in enger Abstimmung mit Ihren Mitarbeitenden dazu, welche Daten (Foto, Name, etc.) auf Ihrer Website oder in der Öffentlichkeit kommuniziert werden sollen oder dürfen.

Positionierung

Wenn Betroffene sich auf ein unterstützendes positionsstarkes Umfeld verlassen können, können sie engagiert und handlungsfähig bleiben.

- Formulieren Sie Grundsätze für Ihre Organisation, auf die sich alle einheitlich bei Angriffen berufen können. Sie verständigen sich zum Beispiel darauf, dass die Sicherheit der Betroffenen an erster Stelle steht oder dass eine andere Person deren Kanäle betreut.
- Unterstützen Sie Ihre Mitarbeitenden bei Angriffen. Veröffentlichen Sie in dem Fall ein Statement, das Ihre Mitarbeitenden verteidigt und für Ihre Werte als Organisation steht.
- Treten Sie als Organisation oder Behörde gemeinsam und geschlossen auf, wenn Einzelne mit Hass und Hetze verfolgt werden. Hier sollten Sie als Institution kommunizieren und das nicht Einzelpersonen überlassen.

Kommunikation

- Formulieren Sie eine Richtlinie (interne Kommunikation) sowie eine Netiquette (externe Online-Kommunikation), auf die sich bei Anfeindungen und digitaler Gewalt alle berufen können.
- Schulen Sie Ihre Kommunikationsabteilung präventiv, wie bei Anfeindungen zu verfahren ist.
- Regeln Sie die externe Kommunikation so arbeitsteilig, dass nicht nur Wenige einem eventuellen Angriff allein ausgesetzt sind.
- Im besten Fall gibt es in Ihrem Betrieb geschulte Personen, die das Community Management für Ihre Social-Media-Kanäle übernehmen und Ihre Netiquette dort durchsetzen. Diese Leute können dann auch strafrechtlich relevante Nachrichten als Beweise sichern und andere Verstöße konsequent löschen.

Empowerment

Handeln Sie nicht erst, wenn Ihre Mitarbeitenden betroffen sind.

Vorbereitung auf digitale Gewalt macht einen Unterschied. Das gilt sowohl für persönliche als auch für systematische Prävention. Oft trägt die richtige Vorbereitung dazu bei, dass Betroffene widerstandsfähiger sind und handlungsfähiger bleiben können – auch in Krisensituationen. Deshalb:

- Bieten Sie Mitarbeitenden aktiv Unterstützung und Mentoring an: vor der Übernahme einer Funktion, eines (Ehren-)Amts oder Mandats sowie währenddessen.
- Informieren und unterstützen Sie Ihre Mitarbeitenden bei der Melderegisterauskunftssperre.
- Nehmen Sie als Organisation Beratungs- und Trainingsangebote zum Thema digitale Gewalt in Anspruch und aktualisieren Sie regelmäßig Ihren Wissensstand. Wenden Sie sich dazu an eine Beratungsstelle oder an HateAid. Wir können Sie bei der Vorbereitung unterstützen und Ihre Mitarbeitenden schulen.
- Bieten Sie Supervision oder kollegiale Beratung für die Social-Media-Zuständigen in Ihrer Organisation an, damit diese über die erlebten Fälle sprechen und sich austauschen können.

Solidarität

Allein sind Betroffene deutlich angreifbarer als die gesamte Organisation.

- Personen, die von gruppenbezogener Menschenfeindlichkeit betroffen sind, werden besonders stark angefeindet. Schützen und unterstützen Sie diese Menschen besonders.
- Ermöglichen Sie es allen, die von Diskriminierungsformen wie Rassismus, Sexismus, Ableismus, Antisemitismus, Antiziganismus, LGBTIQ*-Feindlichkeit oder anderen Formen von gruppenbezogener Menschenfeindlichkeit betroffen sind, sich innerhalb Ihrer Strukturen zu organisieren, sich auszutauschen und zu vernetzen.
- Bauen Sie präventiv Netzwerke der Solidarität auf – mit anderen lokalen Akteur*innen aus der Zivilgesellschaft, innerhalb ihrer Partei, anderen Organisationen und Privatpersonen.

Struktureller und finanzieller Support

Sie bieten die Struktur an, in der sich Ihre Mitarbeitenden bewegen. **Sie haben den Gestaltungsspielraum, einen Rahmen zu schaffen, in dem Engagierte angstfrei wirken und arbeiten können.**

- Entwickeln Sie mit Hilfe der Zivilgesellschaft, anderen Organisationen und geschulten Sicherheitsbehörden einen Krisenplan, wie bei (digitalen) Angriffen auf Sie und Ihre Mitarbeitenden zu verfahren ist.
- Bauen Sie organisationsübergreifend Anlaufstellen und Beratungsangebote für Betroffene auf oder vernetzen Sie sich mit bestehenden Initiativen und Angeboten.
- Fordern Sie für sich und Ihre Mitarbeitenden Unterstützung durch höhere Instanzen (wie Bundes- oder Landesverbände, Kreis- und Landtag, etc.) an, indem Sie dort Erfahrungsberichte sowie ggf. finanzielle Ressourcen einholen.
- Bieten Sie Ihren haupt- und ehrenamtlich Engagierten Unterstützung bei straf- und zivilrechtlichen Schritten durch höhere Organisationsinstanzen an.
- Unterstützen Sie bei der Anfertigung rechtssicherer Screenshots. Dies kann für die Betroffenen selbst sehr belastend sein.
- In extremen Fällen: Unterstützen Sie Betroffene bei der Kostenübernahme von Sicherheitsmaßnahmen und planen Sie diese Kosten in Ihrem Jahresbudget mit ein.

5 Schnelle Hilfe: Das Unterstützungsangebot von HateAid

Beratungsangebote

Emotional stabilisierende Beratung

Es ist emotional belastend, digitale Gewalt zu erleben. Damit müssen Sie nicht allein umgehen. Oft hilft es, Unterstützung in Anspruch zu nehmen und gemeinsam mit jemandem, der schon Erfahrung in dem Bereich hat, herauszufinden, was Sie brauchen und welche nächsten Schritte infrage kommen. HateAid kann Sie telefonisch oder per Chat unterstützen und emotional auffangen.

Kommunikationsberatung

Es gibt verschiedene Möglichkeiten im Umgang mit digitaler Gewalt: Darauf reagieren, Gegenrede leisten, ein Statement veröffentlichen, mit Unterstützenden eine Gegenaktion organisieren oder sich ganz zurückziehen. Die Kommunikationsberatung von HateAid kann Sie darin unterstützen, eine stimmige Strategie für sich und Ihre Situation zu entwickeln.

Sicherheitsberatung

In der Sicherheitsberatung geht es sowohl um den Schutz Ihrer Geräte und Daten im Netz als auch um die Evaluation Ihrer analogen Sicherheitssituation, einschließlich präventiver Maßnahmen zum Schutz Ihrer Wohnadresse. HateAid bietet Ihnen:

- Einschätzung der digitalen Sicherheitssituation
- Einordnung und Verweisberatung zur analogen Sicherheitssituation
- Unterstützung zur selbstständigen Durchführung eines Privatsphäre-Checks zur Identifizierung von personenbezogenen Daten im Netz und ggf. deren Löschung
- Identifizierung von Sicherheitslücken und Beratung zum Umgang mit personenbezogenen Daten im Netz und ggf. Unterstützung bei deren Löschung
- Meldung von Kommentaren
- Beratung zu Privatsphäre-Einstellungen auf Social-Media-Plattformen
- Begleitschreiben zur Beantragung einer Melderegisterauskunftssperre
- Sicherheitsberatung zu Standardmaßnahmen zur Sicherung Ihrer Geräte, zum Schutz vor Hacking- und Phishing-Attacken

Vermittlung an lokale Beratungsstellen

Da digitale Gewalt besonders auf kommunaler Ebene oft mit analoger Gewalt verknüpft ist, kooperiert HateAid mit einem bundesweiten Netzwerk an Organisationen und Beratungsstellen, die zu unterschiedlichen Themen und teilweise vor Ort beraten.

Dazu gehören unter anderem die **Mobilen Beratungsteams, die im Bundesverband Mobile Beratung e. V. (BMB)** vernetzt sind, und die **Beratungsstellen vom Verband der Beratungsstellen für Betroffene rechter, rassistischer und antisemitischer Gewalt e. V. (VBRG)**.

Die Initiative **Stark im Amt** ist ganz konkret für kommunal Engagierte und Kommunalpolitiker*innen da und kann Ihnen schnell einen Überblick über die Beratungsstellen vor Ort verschaffen. Hier bekommen Sie Informationen und Tipps zum Umgang mit analoger und digitaler Gewalt.

Im Falle von analoger Gewalt oder falls ein Beratungsgespräch vor Ort gewünscht wird, ermittelt HateAid eine passende Beratungsstelle für Sie und unterstützt Sie dabei, den Kontakt herzustellen.

Workshops

HateAid bietet Unterstützung für Ihre Organisation, Ihren Verein oder Ihre Partei, um Ihre Mitarbeitenden über digitale Gewalt, ihre Formen, Folgen, den Umgang damit und zu präventiven Maßnahmen zu schulen. Zusätzlich ist es möglich, individuell angepasste Workshops mit von Ihnen gewünschten Schwerpunkten zu organisieren, wie z. B. Social Media, Rechtsdurchsetzung, Handlungsstrategien, rassistische digitale Gewalt, digitale Gewalt gegen Frauen, Politiker*innen usw.

Prozesskostenfinanzierung

Gegen Beleidigung, Bedrohung, Verleumdung oder andere Formen digitaler Gewalt können Sie sich auch zivilrechtlich zur Wehr setzen. **Falls Sie sich für zivilrechtliche Schritte entscheiden, übernimmt HateAid in geeigneten Fällen die Kosten für eine anwaltliche Beratung und Vertretung, sowie – falls notwendig – die Kosten des Gerichtsverfahrens.** Hierfür arbeiten wir mit spezialisierten Kanzleien zusammen.

HateAid arbeitet dabei nach dem Solidaritätsprinzip: Ist die Durchsetzung erfolgreich und die Täter*innen werden zur Kasse gebeten, fließt die Geldentschädigung zurück an HateAid, um ein zivilrechtliches Vorgehen auch für andere Betroffene zu finanzieren. **Wer auf diese Weise gegen seine Hater*innen vorgeht, hilft also nicht nur sich selbst, sondern auch vielen anderen dabei, sich zu wehren.**

6 Kontakt

Per Telefon

030 25208838

Die Sprechzeiten der telefonischen Betroffenenberatung entnehmen Sie bitte unserer Webseite.

Per Chat

hateaid.org

Es besteht auch die Möglichkeit, mit uns zu chatten. Um zu unserem Chat zu gelangen, müssen auf unserer Webseite die Cookies aktiviert werden. Dann erscheint rechts unten eine Chat-Bubble.

Die Sprechzeiten unserer Chatberatung entnehmen Sie bitte unserer Webseite.

Per Meldeformular

hateaid.org/meldeformular

Inhalte können per Meldeformular an uns weitergeleitet werden. In der Beschreibung der Meldung sollten alle relevanten Informationen hinzugefügt werden. Dazu gehören etwa rechtssichere Screenshots und Links zu den betreffenden Plattformen, auf denen digitale Gewalt ausgeübt wurde.

Per E-Mail

beratung@hateaid.org

Es ist möglich, uns eine E-Mail zu schicken. Darin sollte der Fall genau beschrieben und alle relevanten Informationen hinzugefügt werden. Dazu gehören rechtssichere Screenshots und Links zu den betreffenden Plattformen, auf denen digitale Gewalt stattfindet.

Auch allgemeine Fragen zu unserer Beratung können per E-Mail an uns gesendet werden.

Per App

hateaid.org/meldehelden-app

Ebenfalls können Sie über unsere kostenlose App MeldeHelden mit uns in Kontakt treten. Die App kann im Google Play Store oder im App Store heruntergeladen werden.

7 Weitere Hilfsangebote

Stark im Amt

Die Initiative Stark im Amt beschäftigt sich spezifisch mit Kommunalpolitiker*innen. Auf der Website finden Sie Informationen und Material zum Schutz und Umgang mit Hass und Gewalt gegen Kommunalpolitiker*innen, aber auch eine Auflistung diverser Beratungsstellen und Organisationen, die Sie unterstützen.
stark-im-amt.de

Bundesverband Mobile Beratung e. V.

Der Bundesverband Mobile Beratung (BMB) ist der Dachverband von rund 50 Mobilen Beratungsteams bundesweit, die zum Umgang mit Rechtsextremismus, Rassismus, Antisemitismus, Antifeminismus und Verschwörungserzählungen beraten. Wenn Sie Fragen haben oder akut betroffen sind, melden Sie sich bei einem Mobilen Beratungsteam in Ihrer Nähe – dort finden Sie professionelle Unterstützung, kostenlos und vertraulich. Auf der Webseite des BMB sind alle Teams aufgelistet:
bundesverband-mobile-beratung.de

0351 500 54 16

Starke Stelle

Die starke Stelle ist eine bundesweite, unabhängige Ansprechstelle für Kommunalpolitiker*innen, die als Orientierungshilfe dazu dient, die für Sie passenden Unterstützungsangebote aus den Bereichen der Sicherheitsbehörden, Justiz und Zivilgesellschaft zu finden.

Sie erreichen die starke Stelle per E-Mail über info@starkestelle.de

0800 – 300 99 44

Aktion Zivilcourage e. V.

Aktion Zivilcourage e. V. entwickelt Schutzkonzepte für kommunal Engagierte vor allem in Fällen von hybriden Angriffen, wo Betroffene Hass im Netz und parallel vor Ort erleben. Hier finden Sie mehr zu ihrem Angebot:
aktion-zivilcourage.de/angebote/verwaltung/schutzkonzepte

VBRG e. V.

Der Verband der Beratungsstellen für Betroffene rechter, rassistischer und antisemitischer Gewalt besteht aus 14 unabhängigen Beratungsstellen, die Sie zu jeder Zeit beraten können. Sie unterstützen Sie und Ihre Bezugspersonen bei Angriffen, Bedrohungen, Brandanschlägen und Überfällen. Hier finden Sie alle Mitglieder aufgelistet:
verband-brg.de

030 33 85 97 77

Meldestelle #REspect!

Die Meldestelle #REspect! wendet sich an alle, die im Netz oder vor Ort auf Hasskommentare stoßen und etwas dagegen unternehmen möchten. Bei einem Verstoß gegen deutsches Recht beantragt REspect! beim Netzwerkbetreiber die Löschung des Beitrags. Verfasserinnen und Verfasser von Volksverhetzung werden konsequent angezeigt.
meldestelle-respect.de/

Amadeu Antonio Stiftung

Bei der Amadeu Antonio Stiftung finden Sie Informationen zu Rechtsextremismus, Antisemitismus, Hatespeech, Desinformation und digitaler Gewalt im Allgemeinen. Wenn Sie nach Material zu diesen Themen suchen oder eine Veranstaltung dazu organisieren möchten, dann fragen Sie die Stiftung an:
amadeu-antonio-stiftung.de

Meldestelle HessenGegenHetze

Die Meldestelle HessenGegenHetze bietet ein einfaches Meldeverfahren über Webformular, E-Mail oder Hotline an. Sie dokumentiert und bewertet gemeldete Inhalte, leitet bei strafrechtlicher Relevanz diese an die Strafverfolgungsbehörden und bei extremistischen Anhaltspunkten an das Landesamt für Verfassungsschutz weiter. Zudem unterstützt sie Betroffene durch Meldungen bei Online-Plattformen, informiert über Ergebnisse und Maßnahmen, vermittelt Ansprechpartner*innen aus ihrem Netzwerk, stellt Informationen zu Hate Speech und Extremismus bereit und klärt über ihre Arbeit auf.
hessengegenhetze.de/

Digitale Helden

Digitale Helden bildet Lehrkräfte und Schüler*innen aus, die jüngere Schüler*innen beim Umgang mit persönlichen Daten im Internet, sozialen Netzwerken und bei der Prävention von Cybermobbing beraten. Wenn Sie im Bereich der Kinder- und Jugendarbeit aktiv sind, kann digitale Helden Webinare oder Workshops mit Ihnen organisieren und veranstalten. Hier finden Sie die Kontaktdaten:
digitale-helden.de

SCICOMM-Support

Hier erhalten Wissenschaftler*innen und Wissenschaftskommunikator*innen Beratung und Unterstützung bei Angriffen und unsachlichen Konflikten in der Wissenschaftskommunikation.
scicomm-support.de

Netzwerk Recherche Helpline

Hier finden Journalist*innen bei Stress, Angst und anderen psychosozialen Herausforderungen Unterstützung durch Journalist*innen. Die Helpline ist eine unabhängige, anonyme und kostenlose Telefonberatung für mental belastete Journalist*innen. Sie steht allen festangestellten und freien Journalist*innen offen.

netzwerkrecherche.org/helpline/

ichbinhier e. V.

Bieten Bildung und Weiterbildung im Bereich der Gegenrede und digitalen Zivilcourage durch Öffentlichkeitsarbeit und Bildungsmaßnahmen für Vertreter*innen aus Medien, Politik, der Zivilgesellschaft und dem Bildungsbereich.

www.ichbinhier.eu

8 Checklisten

Was Sie präventiv tun können:

- [ ] **Privatsphäre-Check** durchführen: Recherchieren Sie, ob Ihre Wohnadresse, Ihr Geburtsdatum oder irgendein Bezug zu Ihrer Familie oder Ihren Freund*innen (z. B. durch Fotos) online auffindbar sind.
- [ ] Ggf. die **Löschung von sensiblen Daten** wie z. B. Wohnadresse, Geburtstag o. Ä. beantragen.
- [ ] **Melderegisterauskunftssperre** beantragen.
- [ ] Sichere, unterschiedliche **Passwörter** auf allen Plattformen verwenden (Passwort-Manager benutzen).
- [ ] **Zwei-Faktor-Authentifizierung** einrichten, überall wo möglich.
- [ ] **Updates** rechtzeitig installieren: Halten Sie Ihre Software auf dem neusten Stand.
- [ ] Erstellen Sie regelmäßig **Backups**.
- [ ] Einen **Krisenplan** für Krisensituationen vorbereiten und Krisenteam gründen.
- [ ] **Netiquette** auf Ihren Social-Media-Kanälen definieren.
- [ ] **Argumentationssammlung** vorbereiten, um auf problematische Kommentare schneller mit Gegenrede reagieren zu können.
- [ ] **Fakten-Checker** recherchieren, um auf Desinformationskampagnen vorbereitet zu sein und diese schnell aufzudecken.

Was Sie akut tun können:

- [ ] Was Ihnen geschehen ist, ist nicht nur digitale Gewalt, sondern auch psychische Gewalt. Versuchen Sie, **Ruhe** zu bewahren, auf Ihre eigenen **Bedürfnisse** zu achten und einen **Ausgleich** zu schaffen.
- [ ] Krisenplan umsetzen: Wenn Sie einen Krisenplan vorbereitet haben und ein **Krisenteam** haben, können Sie beides nun aktivieren.
- [ ] **Mit jemandem darüber sprechen.** Das kann eine befreundete Person sein, ein*e Arbeitskolleg*in oder eine professionelle Anlaufstelle.
- [ ] Beweissicherung: **Rechtssichere Screenshots** erstellen.
  Das kann auch eine vertraute Person für Sie übernehmen.
- [ ] Illegale Inhalte auf Online-Plattformen als rechtswidrig **melden**. Das kann auch eine befreundete Person oder ein*e Kolleg*in für Sie tun.
- [ ] Digital Detox: Bei Bedarf **Pause vom Internet** machen! Lassen Sie Ihre Accounts gegebenenfalls für die erste Zeit von Vertrauten betreuen oder deaktivieren Sie sie vorübergehend.
- [ ] **Anzeige** bei der Polizei erstatten – auch wenn Sie den genauen Strafbestand nicht kennen. Die Einschätzung, ob digitale Gewalt im konkreten Fall strafbar ist, liegt bei den Strafverfolgungsbehörden und der Justiz und ist nicht Ihre Aufgabe.
- [ ] **Netzwerk aktivieren und sensibilisieren** (online und analog): Rufen Sie im Netz zu **Solidarität** auf und ermuntern Sie andere zur **Gegenrede**.
- [ ] Bei mutmaßlichen Hacking-Angriffen **IT-Sicherheitsexpert*innen** und HateAid kontaktieren.
- [ ] Bei Beratungsbedarf vor Ort die **Mobilen Beratungsteams gegen Rechtsextremismus** kontaktieren.

Für Arbeitgeber*innen und Organisationen:

Was Sie präventiv tun können:

- [ ] **Privatsphäre-Check** für die Mitarbeitenden durchführen.
- [ ] **Außenkommunikation** überprüfen: Die persönlichen Daten der Mitarbeitenden gegebenenfalls löschen und nicht nach außen kommunizieren.
- [ ] Möglichst **Dienstgeräte** (bspw. Handys, Laptops) und dienstl. E-Mail-Adressen anbieten.
- [ ] **Solidaritätsnetzwerk aufbauen** und mit anderen Organisationen über die Themen Hass im Netz und Solidarität bei Angriffen sprechen.
- [ ] **Netiquette** auf Ihren Social-Media-Kanälen definieren.
- [ ] **Krisenplan** für Krisensituationen vorbereiten und **Krisenteam** aufstellen.
- [ ] **Supervision** für die Social-Media-Zuständigen in Ihrer Organisation anbieten.
- [ ] **Workshop** zum Schutz vor und Umgang mit digitaler Gewalt für Mitarbeitende anbieten (z. B. mit der Hilfe von HateAid).
- [ ] Mitarbeitende für **IT-Sicherheit** und den Umgang mit sensiblen Daten schulen.

Was Sie akut tun können:

- [ ] Betroffene Mitarbeitende in akuten Situationen **emotional und inhaltlich entlasten** und nach ihren Bedürfnissen fragen.
- [ ] **Krisenplan** abarbeiten und **Krisenteam** aktivieren.
- [ ] Betroffene pragmatisch unterstützen: Bieten Sie Hilfe bei der Erstellung rechtssicherer Screenshots an.
- [ ] Betroffene **finanziell unterstützen**: Anwaltskosten übernehmen, sodass sie sich auch rechtlich gegen digitale Gewalt wehren können.
- [ ] Nutzen Sie Ihr **Netzwerk** (aus Organisationen, Beratungsstellen oder Kontakten zur Polizei) um Mitarbeitende in akuten Situationen zu unterstützen.
- [ ] Digitale Gewalt konsequent zur **Anzeige** bringen.
- [ ] Bei vermuteten Hacking-Angriffen **IT-Sicherheitsexpert*innen** und HateAid kontaktieren.

Anmerkungen

1 Vgl. forsa (2024): Die Situation ehrenamtlicher Bürgermeisterinnen und Bürgermeister. Ergebnisse einer Befragung für die Körber-Stiftung. URL: https://koerber-stiftung.de/projekte/demokratie-beginnt-vor-ort/.

2 DStGB (2023): Positionspapier „Hass, Bedrohungen & Gewalt“. URL: https://www.dstgb.de/publikationen/positionspapiere/hass-bedrohungen-und-gewalt-gegen-kommunalpolitiker-innen/240123-update-hassbedrohungengewalt.pdf?cid=yfp.

3 Vgl. forsa (2024).

4 Vgl. ebd.

5 Vgl. MIK (2022): Kommunalstudie Brandenburg 2022. URL: https://mik.brandenburg.de/sixcms/media.php/9/Kommunalstudie%20BB_finale_Fassung_Auflage1.pdf.

6 Vgl. KPN HiN (2024): Lauter Hass – leiser Rückzug. Wie Hass im Netz den demokratischen Diskurs bedroht. URL: https://kompetenznetzwerk-hass-im-netz.de/wp-content/uploads/2024/02/Studie_Lauter-Hass-leiser-Rueckzug.pdf.

7 Vgl. Kommunales-Monitoring-Bericht-Herbstbefragung-2022 (2023). URL: https://www.staedtetag.de/files/dst/docs/Publikationen/Weitere-Publikationen/2023/Kommunales-Monitoring-Bericht-Herbstbefragung-2022.pdf.

8 Vgl. ebd.

9 Vgl. Institute for Strategic Dialogue und #ichbinhier (2018): Hass auf Knopfdruck. Rechtsextreme Trollfabriken und das Ökosystem koordinierter Hasskampagnen im Netz.

10 Vgl. CeMAS (2021): Die Bundestagswahl 2021 Welche Rolle Verschwörungsideologien in der Demokratie spielen. URL: https://cemas.io/publikationen/die-bundestagswahl-2021-welche-rolle-verschwoerungsideologien-in-der-demokratie-spielen/die-bundestagswahl-2021-welche-rolle-verschwoerungsideologien-in-der-demokratie-spielen.pdf.

11 Vgl. BMI (2024): Politisch motivierte Kriminalität, Bundesweite Fallzahlen 2023. URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/nachrichten/2024/pmk2023-factsheets.pdf?__blob=publicationFile&v=2.

12 Vgl. forsa (2024): Die Situation ehrenamtlicher Bürgermeisterinnen und Bürgermeister. Ergebnisse einer Befragung für die Körber-Stiftung.URL: https://koerber-stiftung.de/projekte/demokratie-beginnt-vor-ort/.

13 Vgl. BKA (2023): Politisch motivierte Kriminalität im Jahr 2022. URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/nachrichten/2023/05/pmk2022-factsheets.pdf?__blob=publicationFile&v=5.

14 Vgl. BKA (2024): Bundesweites Vorgehen gegen Hasspostings. BKA koordiniert als Zentralstelle den 10. nationalen Aktionstag gegen Hasskriminalität im Netz. URL: https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2024/Presse2024/240606_PM_Hasspostings.html#:~:text=Die%20polizeilich%20registrierten%20Fallzahlen%20von,8.011%20F%C3%A4lle%20mehr%20als%20verdoppelt.

15 Vgl. BMI (2024): Politisch motivierte Kriminalität, Bundesweite Fallzahlen 2023. URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/nachrichten/2024/pmk2023-factsheets.pdf?__blob=publicationFile&v=2.

16 Vgl. forsa (2024): Die Situation ehrenamtlicher Bürgermeisterinnen und Bürgermeister. Ergebnisse einer Befragung für die Körber-Stiftung. URL: https://koerber-stiftung.de/site/assets/files/38220/ergebnisbericht_die_situation_ehrenamtlicher_buergermeister.pdf.

17 Vgl. MOTRA (2023): Kommunales Monitoring: Hass und Hetze gegenüber Amtsträgerinnen und Amtsträgern (KoMo). Auswertung der Herbstergebnisse 2023. URL: https://www.motra.info/wp-content/uploads/2024/04/KoMo_zentrale-Kernbefunde_HB23.pdf.

18 VBRG (2021): Bedroht zu werden gehört nicht zum Mandat. URL: https://verband-brg.de/wp-content/uploads/2021/04/Drohungen_gg_Politik_Verwaltung_DS_WEB.pdf.

19 Vgl. KPN HiN (2024): Lauter Hass – leiser Rückzug. Wie Hass im Netz den demokratischen Diskurs bedroht (2024). URL: https://kompetenznetzwerk-hass-im-netz.de/wp-content/uploads/2024/02/Studie_Lauter-Hass-leiser-Rueckzug.pdf.

20 Vgl. forsa 2024, S. 26.

21 Vgl. BMFSFJ (2023): Gewalt gegen queere Menschen nimmt zu. URL: https://www.bmfsfj.de/bmfsfj/aktuelles/alle-meldungen/queerfeindliche-hasskriminalitaet-und-gewalt-besser-bekaempfen-227188. Und vgl. KPN HiN (2024): Lauter Hass – leiser Rückzug. Wie Hass im Netz den demokratischen Diskurs bedroht. URL: https://kompetenznetzwerk-hass-im-netz.de/wp-content/uploads/2024/02/Studie_Lauter-Hass-leiser-Rueckzug.pdf.

22 Vgl. HateAid (2021): HateAid Report 2021. URL: https://hateaid.org/wp-content/uploads/2022/04/HateAid-Report-2021-DE.pdf.

23 Vgl. Institute for Strategic Dialogue und #ichbinhier (2018): Hass auf Knopfdruck. Rechtsextreme Trollfabriken und das Ökosystem koordinierter Hasskampagnen im Netz. URL: https://www.isdglobal.org/wp-content/uploads/2018/07/ISD_Ich_Bin_Hier_2.pdf.

24 Vgl. HateAid (2023): Rechtsextremismus und Klima. URL: https://hateaid.org/rechtsextremismus-und-klima/.

25 Correktiv (2020): Kein Filter für Rechts Wie die rechte Szene Instagram benutzt, um junge Menschen zu rekrutieren. URL: https://correctiv.org/top-stories/2020/10/06/kein-filter-fuer-rechts-instagram-rechtsextremismus-frauen-der-rechten-szene/.

26 Süddeutsche Zeitung JETZT (2021): Nicht alle, aber zu viele Männer. URL: https://www.jetzt.de/social-media/warum-der-hashtag-notallmen-problematisch-ist#:~:text=Mit%20der%20Aussage%20%E2%80%9Enicht%20alle,sammelte%20sich%20der%20Hashtag%20%23notallmen.

27 HateAid (2022): #Kriegstreiber: Wie ein Hashtag Propaganda streut. URL: https://hateaid.org/kriegstreiber/.

28 Vgl. KPN HiN (2024): Lauter Hass – leiser Rückzug. Wie Hass im Netz den demokratischen Diskurs bedroht (2024). URL: https://kompetenznetzwerk-hass-im-netz.de/wp-content/uploads/2024/02/Studie_Lauter-Hass-leiser-Rueckzug.pdf.

29 Vgl. HateAid (2022): Incels – unterschätzte Gefahr aus der dunklen Ecke des Netzes. URL: https://hateaid.org/incels/.

30 Vgl. CeMAS (2022): Belastungsprobe für die Demokratie: Pro-russische Verschwörungserzählungen und Glaube an Desinformation in der Gesellschaft. URL: https://cemas.io/publikationen/belastungsprobe-fuer-die-demokratie/2022-11-02_ResearchPaperUkraineKrieg.pdf.

31 Vgl. HateAid (2022): Demokratie im Fadenkreuz: Desinformationskampagne #BaerbockRuecktritt. URL: https://hateaid.org/baerbock-ruecktritt-desinformation/. Und vgl. HateAid (2022): Report: Desinformation und digitale Gewalt im Ukraine-Krieg. URL: https://hateaid.org/desinformation-propaganda-ukraine-krieg/.

32 Vgl. BR24 (2024): Russische Cyberangriffe auf Deutschland bestätigt. URL: https://www.br.de/nachrichten/deutschland-welt/russische-cyberangriffe-auf-deutschland-bestaetigt,UBiRBZm.

33 Vgl. HateAid (2022): Report: Desinformation und digitale Gewalt im Ukraine-Krieg. URL: https://hateaid.org/desinformation-propaganda-ukraine-krieg/.

34 Vgl. HateAid (2022): Demokratie im Fadenkreuz: Desinformationskampagne #BaerbockRuecktritt. URL: https://hateaid.org/baerbock-ruecktritt-desinformation/.

35 Fabian Virchow (2022): Querdenken und Verschwörungserzählungen in Zeiten der Pandemie. URL: https://www.bpb.de/themen/rechtsextremismus/dossier-rechtsextremismus/508468/querdenken-und-verschwoerungserzaehlungen-in-zeiten-der-pandemie/.

36 Vgl. BMI: (o.J.): Was ist der Unterschied zwischen „Reichsbürgern“ und „Selbstverwaltern“? URL: https://www.bmi.bund.de/SharedDocs/schwerpunkte/DE/reichsbuerger/faq-unterschied-reichsbuerger-selbstverwalter.html.

37 Vgl. BMI (2022): „Reichsbürger“ und „Selbstverwalter“ – eine zunehmende Gefahr?. URL: https://www.bmi.bund.de/SharedDocs/schwerpunkte/DE/reichsbuerger/topthema-reichsbuerger.html.

38 Vgl. BMK (2024): Politisch motivierte Kriminalität, Bundesweite Fallzahlen 2023. URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/nachrichten/2024/pmk2023-factsheets.pdf?__blob=publicationFile&v=2.

39 Vgl. BMK (2023): Politisch motivierte Kriminalität im Jahr 2022. URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/nachrichten/2023/05/pmk2022-factsheets.pdf?__blob=publicationFile&v=5.

40 Vgl. Bruns, J. / Glösel, K. / Strobl, N. (2014): Die Identitären: Handbuch zur Jugendbewegung der Neuen Rechten in Europa. Münster: Unrast Verlag.

41 Vgl. IDZ (2022): Klimadiktatur? Rechte Ideologie und Verschwörungsnarrative zur Klimapolitik in den sozialen Netzwerken. URL: https://www.idz-jena.de/wsddet/wsd11-07.

42 Vgl. Zeit (2021): Joe Bidens Impfangriff. URL: https://www.zeit.de/politik/ausland/2021-09/coronavirus-usa-joe-biden-impfpflicht-pandemie-rede.

43 Vgl. „Psychosoziale Krise“. Online Lexikon für Psychologie und Pädagogik. URL: https://lexikon.stangl.eu/16034/psychosoziale-krise.

44 Vgl. Tagesspiegel (2023). URL: https://www.tagesspiegel.de/gesellschaft/hetze-und-lugen-beim-twitter-nachfolger-x-elon-musk-unterstutzt-hass-und-rassismus-10261369.html. Und CCDH 2023 URL: https://counterhate.com/wp-content/uploads/2023/09/230907-X-Content-Moderation-Report_final_CCDH.pdf; https://counterhate.com/research/twitter-fails-to-act-on-twitter-blue-accounts-tweeting-hate/#about).

45 Vgl. Spiegel (2024): HateAid reicht Beschwerde gegen TikTok ein. URL: https://www.spiegel.de/netzwelt/hateaid-reicht-beschwerde-gegen-tiktok-ein-a-2db19652-4f70-46dd-ac02-4c999661a53c.

46 Vgl. Belltower News (2023): TikTok als Radikalisierungsmotor. URL: https://www.belltower.news/algorithmus-tiktok-als-radikalisierungsmotor-151187/

47 Vgl. Bayerischer Rundfunk (2023). URL: vgl. https://www.br.de/nachrichten/deutschland-welt/faktenfuchs-warum-sich-desinformation-auf-tiktok-gut-verbreitet,TgONvKv).

48 Ermöglicht es Nutzer*innen, einen kurzen Ausschnitt aus einem anderen TikTok-Video in ihr eigenes Video zu integrieren. So kann direkt auf das Originalvideo reagiert, es kommentiert oder darauf aufgebaut werden.

49 Eine Anleitung zum Auslesen von Meta-Daten finden Sie z. B. unter: https://kb.el.uni-leipzig.de/books/tipps-tricks-und-kniffe/page/metadaten-aus-fotos-auslesen#:~:text=Metadaten%20anzeigen%20und%20auslesen,-Ziehen%20Sie%20ein&text=Klicken%20Sie%20auf%20EXIF%20Daten,I%C3%A4sst%20sich%20der%20Aufnahmeort%20verorten.

50 Eine Rückwärtssuche von Bildern funktioniert, indem Sie ein Bild hochladen oder einen Bildlink eingeben, und die Suchmaschine dann das Internet nach ähnlichen oder identischen Bildern durchsucht, um die Herkunft oder verwandte Inhalte zu finden. Eine Anleitung finden Sie z. B. hier: https://correctiv.org/faktencheck/hintergrund/2022/04/01/so-funktioniert-die-bilderrueckwaertssuche/.

51 Vgl. Norddeutscher Rundfunk (2020): Endloser Hass: Facebooks private Gruppen. URL: https://www.ndr.de/fernsehen/sendungen/zapp/medienpolitik/Endloser-Hass-Facebooks-private-Gruppen,facebook2844.html).

52 Vgl. ebd.

53 Vgl. DUH-Klage gegen Meta erfolglos: Facebook-Gruppen werden nicht geschlossen (2023). URL: (https://www.heise.de/news/Hetze-auf-Facebook-Deutsche-Umwelthilfe-klagt-erfolglos-gegen-Meta-9535614.html).

54 HateAid (2024): “Wd1sPWs”* oder: Wie dich ein sicheres Passwort schützt. URL: https://hateaid.org/sicheres-passwort/.

55 Zeit online (2024): Behörde warnt vor vermehrten Phishingangriffen auf Parteien. URL: https://www.zeit.de/digital/2024-04/cyberangriffe-parteien-desinformation-europawahl-verfassungsschutz.

56 Auch Digital sichere Räume schaffen. Online-Veranstaltungen und -Seminare schützen – Zum Umgang mit rechtsextremen, rassistischen und antisemitischen Störungen und Bedrohungen (2020); 8 Seiten; Hg: MBR/VDK e. V. in Kooperation mit: Bundesverband RIAS e. V. URL: https://mbr-berlin.de/wp-content/uploads/2021/02/200715_MBR_RIAS-Handout-Zoombombing-1.pdf.

57 Todes- oder Feindeslisten sind Aufstellungen, die meist von extremistischen Gruppen erstellt werden und Namen sowie persönliche Informationen von politischen Gegner*innen bzw. Aktivist*innen enthalten. Diese Listen bergen erhebliche Gefahren für politisch Aktive, da sie Zielscheibe für Einschüchterung, Bedrohungen und physische Gewalt werden können, was ihre Sicherheit und ihr Leben ernsthaft gefährdet.

58 Ein Ratsinformationssystem ist eine digitale Plattform, die den Zugang zu Sitzungsunterlagen, Beschlüssen und Informationen kommunaler Gremien für Bürger, Verwaltungsmitarbeiter und Mandatsträger ermöglicht. Vgl. eGovernment (2016): Definition Was ist ein Ratsinformationssystem? URL: https://www.egovernment.de/was-ist-ein-ratsinformationssystem-a-612432/.

59 Vgl. Institute for Strategic Dialogue und #ichbinhier.

60 Vgl. Dominik Hangartner, Gloria Gennaro, Sary Alasiri, Nicholas Bahrich, Alexandra Bornhoft, Joseph Boucher, Buket Buse Demirci, Laurenz Derksen, Aldo Hall, Matthias Jochum, Maria Murias Munoz, Marc Richter, Franziska Vogel, Salomé Wittwer, Felix Wüthrich, Fabrizio Gilardi and Karsten Donnay. (2021): Empathy-based Counterspeech Can Reduce Racist Hatespeech in a Social Media Field Experiment.

61 Vgl. ebd. Und Eidgenössische Technische Hochschule Zürich (ETH Zürich) (2021): Gegen Hassrede hilft Empathie. URL: https://idw-online.de/de/news783631.

62 Bei der außergerichtlichen Streitbeilegung handelt es sich um eine schnelle und einfache Möglichkeit, Konflikte von Nutzer*innen über Entscheidungen von Online-Plattformen zu lösen. Nutzer*innen können sich an eine zertifizierte Streitbeilegungsstelle wenden, wenn sie z. B. die Entscheidung einer Online-Plattform über die Löschung von Inhalten überprüfen lassen wollen. Aufgabe der Streitbeilegungsstelle ist es dann, unabhängig und überparteilich zwischen Nutzer*innen und Online-Plattform zu vermitteln (weiterführende Informationen zur außergerichtlichen Streitbeilegung: https://www.dsc.bund.de/DSC/DE/5Streitb/start.html).

63 Eine solche Beschwerde können Sie über dieses Beschwerdeportal des Digital Services Coordinator einbringen: https://www.dsc.bund.de/DSC/DE/3Verbraucher/3VB/start.html.

64 URL: https://chromewebstore.google.com/detail/atomshot/pjfmllbdhacnbnjgenkeflcmklpkjdcn?hl=de.

Impressum

Herausgegeben von
HateAid gGmbH
Greifswalder Straße 4
10405 Berlin

Telefon: +49 (0) 30 25208802
E-Mail: kontakt@hateaid.org
hateaid.org

Sitz der Gesellschaft: Berlin
Registergericht: Amtsgericht Charlottenburg
Handelsregisternummer: HRB 203883 B
USt-IdNr.: DE322705305

Geschäftsführerinnen:
Anna-Lena von Hodenberg und Josephine Ballon
V. i. S. d. P.: Anna-Lena von Hodenberg (HateAid gGmbH)
Redaktion: Basma Bahgat, Samara Feldmann, Anna-Lena von Hodenberg, Eva Pasch, Anna Wegscheider, Stefanie Zacharias
Gestaltung: Regina Buschmeier
Druck: Umweltdruck Berlin GmbH

Disclaimer
Aus Gründen der Barrierefreiheit verwendet HateAid in diesem Bericht das Gender-Sternchen als gendergerechte Schreibweise. Dieses kann von Sprachausgabeprogrammen, die Menschen mit Sehbeeinträchtigungen nutzen, am besten wiedergegeben werden.

Haftungsausschluss
Die Hinweise in dieser Broschüre wurden nach bestem Wissen und Gewissen formuliert. Diese Handreichung ersetzt keine individuelle (juristische) Beratung. Für die Richtigkeit, Vollständigkeit und Aktualität der Informationen übernehmen die Herausgeber*innen keine Gewähr.

Die erste Auflage dieser Publikation wurde im Rahmen der Förderung des „Kompetenznetzwerkes Hass im Netz“ durch das Bundesprogramm „Demokratie leben!“ des Bundesministeriums für Familie, Senioren Frauen und Jugend im Jahr 2021 entwickelt und gedruckt. Die vorliegende Neuauflage wurde 2024 von HateAid gGmbH eigenverantwortlich und grundlegend überarbeitet und in zweiter Auflage herausgegeben.

Spenden

Als gemeinnützige Organisation sind wir auf Spenden angewiesen.

Machen Sie das Internet zu einem besseren Ort und werden Sie Dauerspender*in von HateAid.

Ihre regelmäßige Spende fließt direkt in unsere tägliche Arbeit – und damit in die Meinungsvielfalt unserer Demokratie.

Schon mit 10 Euro pro Monat machen Sie deutlich:
Hass ist keine Meinung.

Spendenkonto:
Kontoinhaberin: HateAid
Bank: GLS Bank
IBAN: DE04 4306 0967 1231 5982 03
BIC: GENODEM1GLS

hateaid.org/spenden

Ein Leitfaden zum Umgang mit digitaler Gewalt

Hass, Gewalt und Lügen im Netz sind nicht Teil des Jobs.

Kommunales Engagement, also der Einsatz von Bürger*innen in ihren Städten und Gemeinden, ist ein Kern unserer Demokratie. Viele Menschen überall in Deutschland setzen sich täglich auf diese Weise ein – in Parteiverbänden, der Verwaltung, Bürger*innen-Initiativen und Vereinen. Doch leider werden gerade sie immer öfter zur Zielscheibe von Hass und Gewalt.

Aber Sie müssen Hass und Hetze weder akzeptieren, noch aushalten.

Wehren Sie sich!

Wir unterstützen Sie dabei.

HateAid