

# **Digitale Gewalt**

## **Ein Überblick**

**Formen. Phänomenbereiche. Handlungsstrategien.**

Das Glossar wurde im Rahmen des Projektes „Niedersachsen. Stark. Gegen digitale Gewalt.“ des Niedersächsischen Justizministeriums gefördert. Die Veröffentlichung stellt keine Meinungsäußerung des Niedersächsischen Justizministeriums dar. Für inhaltliche Aussagen tragen die Autor\*innen die Verantwortung.

## Einleitung

Täglich erleben Menschen Gewalt im Internet. Digitale Gewalt kann unterschiedliche Auswirkungen haben: **physisch, psychisch, aber auch sozial und gesellschaftlich.** Sie gefährdet sowohl **persönliche Rechte** einzelner Personen als auch das **demokratische Zusammenleben** von uns allen. Es gibt verschiedenste Formen und Phänomene, wie digitale Gewalt verbreitet wird. Doch es existieren auch viele Möglichkeiten, sich davor zu schützen und dagegen zu wehren. Was digitale Gewalt ist, in welchen Formen sie auftritt und welche Handlungsstrategien es für Betroffene von digitaler Gewalt gibt, findest du in diesem Glossar.

## Was ist digitale Gewalt?

Der Begriff digitale Gewalt meint **verschiedene Formen von Belästigung, Herabwürdigung, Diskriminierung oder sozialer Isolation im Internet oder mit Hilfe elektronischer Kommunikationsmittel**. Die Orte digitaler Gewalt sind vielseitig: Soziale Netzwerke, Messenger Apps, Chat-Räume, Gaming-Plattformen oder das E-Mail-Postfach sind nur einige davon. Im Internet greifen geltende Gesetze, weswegen Fälle von digitaler Gewalt strafbar sein können.

## Analoge und digitale Gewalt

Digitale Gewalt hängt häufig **mit analoger zusammen**. Manchmal überträgt sich analoge Gewalt in den digitalen Raum. Beispielsweise, wenn antisemitische Einstellungen gegenüber jüdischen Menschen nicht nur am sprichwörtlichen Stammtisch verbreitet werden, sondern auch auf Social-Media-Plattformen ein Millionenpublikum erreichen. In anderen Fällen wird aus digitaler Gewalt eine analoge Gefahr: Drohungen, die zunächst im E-Mail-Postfach landen, können schnell zu Belästigungen und tätlichen Angriffen vor der eigenen Haustür führen.

Ob im Netz oder auf der Straße, **gewalttätige Angriffe lösen bei vielen Betroffenen Angst, Scham oder Wut aus**. Anders als analoge Gewalt spielt sich digitale Gewalt oft rund um die Uhr vor einem riesigen Publikum ab. Täter\*innen können dabei **anonym agieren** und **Angriffe gezielt planen**.

## Formen und Phänomene digitaler Gewalt – von A bis Z<sup>1</sup>

### Bildbasierte (sexualisierte) Gewalt

Bildbasierte sexualisierte Gewalt bezeichnet das **Verbreiten, Teilen oder Anfertigen von intimen oder sexualisierten Bildern oder Videos ohne die Zustimmung der abgebildeten Person**. Dazu zählt zum Beispiel, wenn so genannte **Rache pornos**<sup>2</sup> mit dem Gesicht der betroffenen Person im Internet auftauchen oder Personen **ungefragt ein Dickpic** erhalten. Auch **sexualisierte Deepfakes**<sup>3</sup> (vgl. S. 10), **heimliche Aufnahmen** (wie Upskirting<sup>4</sup>), aber auch das **unerlaubte Weiterleiten privater Aufnahmen** werden unter diesem Begriff gefasst. Diese Form digitaler Gewalt verletzt die Intimsphäre der Betroffenen und kann schwerwiegende psychische und soziale Folgen haben, beispielsweise Isolation, Rückzug, Angst, Schwierigkeiten im Aufbau von neuem Vertrauen in andere Menschen, insbesondere in zwischenmenschliche Nähe. Einige dieser Formen bildbasierter sexualisierter Gewalt sind **strafbar** und können **zur Anzeige** gebracht werden. Neben dem strafrechtlichen Weg besteht zudem die Möglichkeit, dass Betroffene **zivilrechtliche Schritte** einleiten und ihre eigenen **Persönlichkeitsrechte** einfordern können.<sup>5</sup>

Betroffene sollten **Inhalte sichern** (zum Beispiel Screenshots), die Verbreitung sofort **bei Plattformen melden**, gegebenenfalls **spezialisierte Meldestellen** wie [StopNCII.org](https://stopncii.org) nutzen und **rechtliche Schritte prüfen** (§ 184k und § 201a StGB). Beratungsstellen bieten zusätzlich emotionale und rechtliche Unterstützung.

## Cybermobbing

Zu Cybermobbing oder auch Cyberbullying zählen unterschiedliche Handlungen, die Betroffene über einen **längeren Zeitraum** niedermachen, verletzen und ausgrenzen sollen. **Beleidigungen, Bedrohungen, Schikane, Belästigung, Bloßstellen oder das Veröffentlichen von Bild- und Videomaterial** gehören zu diesen Handlungen. Cybermobbing kennt viele Orte, unter anderem **Messenger Chats, Social-Media- oder Gaming-Plattformen**.

Cyberbullying kann, genauso wie analoges Mobbing, **schwere psychische Folgen** für Betroffene haben. In Extremfällen führen Mobbingattacken **zum Suizid**. Die **Cyberlife IV-Studie** liefert aktuelle belastbare Daten aus dem deutschsprachigen Raum. Sie belegt, dass nahezu **25 % der Betroffenen** suizidale Gedanken entwickeln (Bündnis gegen Cybermobbing, 2022). Ob strafrechtlich relevant oder nicht, Cybermobbing verletzt, erniedrigt und grenzt aus. Deswegen gilt in jedem Fall, dass Betroffene **sich wehren sollten**: Es ist wichtig, Beweise in Form von rechtssicheren **Screenshots** zu sichern, die Tatperson ggf. zu **blockieren** und die Inhalte bei der Plattform zu **melden**. Zudem kann es hilfreich sein, den eigenen Standpunkt beispielsweise im Rahmen eines Social Media Posts zu verbalisieren und zu sagen oder schreiben, dass man verletzt ist. Hierbei kann die Unterstützung von Freund\*innen oder anderen sozialen Bezugspersonen helfen.

## Cyberstalking

Als Cyberstalking wird das **Auflauern, Nachstellen, Überwachen und Verfolgen** einer anderen Person mit digitalen Hilfsmitteln bezeichnet. Mit dem technischen Fortschritt der letzten Jahre hat sich auch Cyberstalking weiterverbreitet – unter anderem durch den Einsatz von **Stalking-Apps** oder durch die **Veröffentlichung privater Bilder**. Hierdurch werden die Betroffenen – wie beim analogen Stalking – erheblich eingeschüchtert.

Stalking ist **explizit strafrechtlich verboten** (§ 238 StGB). Der bereits bestehende Straftatbestand der Nachstellung wurde an die neuen Ausprägungen des Cyberstalkings angepasst: Neben dem wiederholten Aufsuchen der räumlichen Nähe einer Person schließt er mittlerweile unter anderem die Nachstellung durch die (versuchte) Kontaktaufnahme durch digitale Kommunikationsmittel oder die Veröffentlichung von Bildern im Internet mit ein.

## Deepfakes

Deepfakes, aus den englischen Begriffen „deep learning“ und „fake“ zusammengesetzt, sind Video- oder Audiodateien, die mithilfe von **künstlicher Intelligenz manipuliert** werden. KI-Programme oder Apps ermöglichen es, verfälschte bewegte Bilder oder Tonaufnahmen zu produzieren. Unter anderem setzen Täter\*innen damit Gesichter auf fremde Körper oder erstellen Imitate von Stimmen und belegen sie mit neuem Text. So versetzen sie Betroffene in **andere Kontexte** oder legen ihnen **fremde Aussagen** in den Mund.

Gerade das Verfälschen von Bildmaterial in sexualisierte Szenarios ist ein **wachsendes Problem**. Sexualisierte **Deepfakes**, auch Deepnudes bezeichnet, machen 98 Prozent aller Deepfake-Videos im Internet aus (Security Hero, 2024). Davon sind vor allem Frauen betroffen. Täter\*innen fügen die Gesichter der Betroffenen mittels Deepfake- oder Nudify-Apps und anderen Programmen in pornografische Darstellungen ein. Diese sehen **häufig täuschend echt** aus.

Es gibt zahlreiche Beispiele, die zeigen, dass Deepfakes **kränken, diskriminieren, verleumden, Karrieren zerstören, Leben ruinieren oder Bürger\*innen aufhetzen** können.

Mit den Lügen im Nachhinein aufzuräumen, ist oft unmöglich, denn Desinformation erreicht in vielen Fällen mehr Menschen als die Richtigstellung. Darüber hinaus ist es schwierig, Deepfakes, die einmal im Internet verbreitet wurden, wieder vollständig aus dem digitalen Raum zu entfernen. Das Vertrauen in andere Menschen, in Fakten und demokratische Institutionen **soll so erschüttert** werden.

## Doxxing

Der Begriff „Doxxing“ (auch „Doxing“ geschrieben) stammt aus dem Englischen und leitet sich von „dox“, kurz für „documents“, ab. Er bezeichnet das **systematische Sammeln und anschließende Veröffentlichen privater und personenbezogener Daten einer anderen Person im Internet**. Der Begriff kann auch auf das Enthüllen der tatsächlichen Identität einer Person hinter ihrem anonymen Online-Alias verweisen.

Genau bedeutet Doxxing, dass jemand persönliche Daten, Chatverläufe, private Fotos oder auch amtliche Dokumente einer anderen Person sammelt und diese – ohne deren Zustimmung – im Netz publiziert. Diese Daten können dabei sowohl aus **öffentlich zugänglichen Suchmaschinen** wie Google oder Social-Media-Profilen gefiltert oder aber auch aus **gehackten Konten** zusammengetragen oder durch Phishing (vgl. S. 17) illegal beschafft werden. **Doxxing, Phishing und Hacking (vgl. S. 14) gehen oft miteinander einher**. Unter gewissen Umständen kann Doxxing auch strafbar sein (§ 126a StGB). Als präventive Maßnahme kann es hilfreich sein, eine **Auskunftssperre im Melderegister** eintragen zu lassen.

Mehr Informationen zur Melderegisterauskunft und wie du sie sperren lassen kannst, findest du [hier](#).

## Desinformationen

Angeichts der überwältigenden Flut an Informationen im Internet fällt es zunehmend **schwer, zwischen vertrauenswürdigen und irreführenden Inhalten zu unterscheiden**. Desinformation beschreibt **gezielte Strategien**, die genau diesen Umstand ausnutzen, um absichtlich falsche oder manipulierte Inhalte – sogenannte Falschnachrichten – zu streuen. Ziel ist es, **Zweifel an seriösen Informationsquellen** zu säen. Selbst wenn solche Falschmeldungen nicht vollständig geglaubt werden, hinterlassen sie Wirkung: Sie fördern ein **Misstrauen gegenüber anderen Quellen oder Fakten, streuen gezielt bestimmte Narrative und Informationen** und schwächen so das Vertrauen in die öffentliche Debatte. Dies kann zur weiteren Spaltung der Gesellschaft beitragen.

Bei der Verbreitung von Desinformationen kann es sich strafrechtlich um eine **Verleumdung** (§ 187 StGB) oder um eine **üble Nachrede** (§ 186 StGB) handeln. Betroffenen kann gegebenenfalls ein Anspruch auf Richtigstellung zustehen, wenn es sich um **personalisierte Falschnachrichten** durch Medien handelt.

## Hacking

Beim Hacking greifen Personen mithilfe technischer Mittel in Computersysteme oder Netzwerke ein. Sie nutzen dabei gezielt **Schwachstellen oder Schlupflöcher im Sicherheitssystem**, um **Zugang zu Daten zu erhalten**. Es gibt verschiedene Formen von Hacking:

- White Hat Hacking: Die Hackenden handeln legal und unterstützen dabei, die IT-Sicherheit zu verbessern.
- Black Hat Hacking: Die Hackenden verfolgen eigene oder kriminelle Interessen und handeln ohne Erlaubnis.
- Grey Hat Hacking: Die Hackenden sind in einem rechtlichen Zwischenbereich, sie handeln zwar ohne Zustimmung, weisen aber später auf Schwachstellen hin.

Die Ziele beim Hacking sind also unterschiedlich und reichen von **Datendiebstahl** bis hin zur **Aufdeckung von Sicherheitsrisiken**.

## Hasskriminalität

Hasskriminalität bezeichnet Straftaten, die sich gezielt gegen Personen richten, weil ihnen eine **tatsächliche oder vermutete Zugehörigkeit zu einer bestimmten gesellschaftlichen Gruppe** (bezogen zum Beispiel auf Religion, ethnische Herkunft, sexuelle Orientierung) zugesprochen wird. Nach § 46 Abs. 2 StGB müssen solche Motive bei der Strafzumessung berücksichtigt werden. Damit Hasskriminalität statistisch erfasst und angemessen verfolgt werden kann, ist es wichtig, dass Polizei und Staatsanwaltschaft diese als solche erkennen. Laut Nr. 86 Abs. 2 RiStBV liegt in der Regel ein **öffentliches Interesse an der Strafverfolgung** vor, sodass die Staatsanwaltschaft die Straftaten regelmäßig von Amts wegen verfolgen muss.

## Hassrede / Hatespeech

Hatespeech (im Deutschen als „Hassrede“ übersetzt) ist ein Oberbegriff für verbal oder schriftlich geäußerte, **gruppenbezogene Menschenfeindlichkeit**. Dazu zählen verschiedene Abwertungsmuster, wie **Rassismus**, **Sexismus** oder **Antisemitismus**, die einen gemeinsamen Kern haben: die **Ideologie der Ungleichwertigkeit** als **Legitimation für Diskriminierung** – bis hin zur Gewalt. Unter Hatespeech fallen Beleidigungen, Aufrufe zur Gewalt, Drohungen und weitere Äußerungen, **unabhängig davon, ob diese strafbar sind oder nicht**. Der Begriff Hatespeech ist nicht klar definiert und wird manchmal auch dann verwendet, wenn ganz allgemein Hass im Internet gemeint ist.

**Gruppenbezogene, menschenfeindliche Äußerungen** können in den Bereich der verhetzenden Beleidigung (§ 192a StGB) oder sogar in den der **Volksverhetzung** (§ 130 StGB) fallen und damit strafbar sein. Hatespeech online ist also digitale Gewalt. Aber nicht jede Form digitaler Gewalt ist Hatespeech.

## Phishing

Der Begriff „Phishing“ (von engl. „password“ und „fishing“) beschreibt den **Identitätsdiebstahl über Kommunikationswege** wie E-Mails, Websites oder SMS. Cyberkriminelle zielen mit gefälschten E-Mails, Chat-Nachrichten und Websites auf **persönliche Informationen** wie Kontodaten, Kreditkartennummern, Steuer- und Krankenakten sowie sensible Geschäftsdaten wie Kundennamen und Kontaktinformationen ab.

Phishing-Mails sehen denen von realen Unternehmen zum Verwechseln ähnlich. Sie verwenden ähnliche Redewendungen und verweisen auf **Links, die täuschend echt aussehen**. Über diese gelangen die Empfänger\*innen auf gefälschte Websites, wo sie ihre persönlichen Daten in betrügerische Dateneingabeformulare eingeben.

## Sextortion

Der Begriff „Sextortion“ vereint die englischen Wörter „sex“ und „extortion“ („Sex“ und „Erpressung“). Bei der sexuellen Erpressung bauen Täter\*innen über Social-Media- oder Dating-Plattformen **Vertrauensverhältnisse** zu den Betroffenen auf, um diese dann gegen sie zu verwenden.

In den Chats überreden sie zumeist ihre Opfer, ihnen **Nacktbilder zu schicken** oder **in Videocalls sexuelle Handlungen zu vollziehen**. Davon machen die Täter\*innen Screenshots und drohen danach, die Bilder an die Kontakte oder die Follower\*innenliste zu schicken, wenn die Betroffenen kein **Lösegeld** zahlen.

Bei einer anderen Variante täuschen die Täter\*innen in willkürlich verschickten Erpressungsnachrichten per E-Mail oder DM lediglich vor, Nacktbilder der Betroffenen zu besitzen. Auch mit Deepfakes gelingt es ihnen, Geld zu erpressen – **ganz ohne echtes Bildmaterial**.

## Shadowbanning

Ein **Shadowban** bedeutet, dass Beiträge oder ganze Profile innerhalb einer Online-Plattform weniger oder überhaupt **nicht mehr sichtbar** sind. Die Betroffenen werden darüber nicht informiert. Das geschieht nicht durch andere Nutzer\*innen, sondern **durch die Plattform** selbst. Die Blockadefunktion stammt ursprünglich aus den frühen 2000er-Jahren und wurde in Internetforen genutzt, um gezielt gegen Trolle,<sup>6</sup> Spam und Bots vorzugehen. Damals wurden Beiträge so verborgen, dass nur die Verfasser\*innen sie noch sehen konnten – für alle anderen waren sie unsichtbar.

Heute wird der Shadowban weiterhin eingesetzt, jedoch **fehlt Transparenz** darüber, wann und warum er angewendet wird, obwohl das europäische Gesetz über digitale Dienste (DSA) die Plattformen dahingehend verpflichtet. Besonders häufig betroffen scheinen **marginalisierte Creator\*innen**, etwa Menschen mit Behinderung, queere Personen oder übergewichtige Nutzer\*innen (Hyun Kim, 2019). Viele merken den Bann erst, wenn ihre Reichweite plötzlich stark sinkt oder ihre Inhalte kaum noch Likes erhalten.

TikTok räumte bereits ein, Inhalte solcher Personen bewusst weniger sichtbar gemacht zu haben. Instagram wurde – laut einem Bericht des Guardian vom November 2019 – dafür kritisiert, ähnliche Praktiken anzuwenden. Da Plattformen kaum offenlegen, wie ihre Algorithmen arbeiten, bleibt vieles im Unklaren und basiert auf Vermutungen.

## Shitstorm

Ein Shitstorm beschreibt eine Situation, in der sich viele Menschen gleichzeitig – spontan oder gezielt – **kritisch und oft wütend gegen eine bestimmte Person, ein Unternehmen oder eine Organisation wenden**. Häufig geschieht dies, um auf einen tatsächlichen oder vermeintlichen Missstand aufmerksam zu machen und **Veränderungen** zu fordern.

Allerdings kann ein Shitstorm auch **gezielt eingesetzt werden, um Schaden anzurichten**. In solchen Fällen steht nicht die sachliche Kritik im Vordergrund, sondern es kommt zu **gezielter Diffamierung, Hassrede, Beleidigungen und Drohungen**. Das Ziel: Personen oder Organisationen zum Schweigen zu bringen. Für die Betroffenen kann das schwerwiegende psychische Belastungen mit sich bringen. Auch Unternehmen oder Organisationen können wirtschaftliche Einbußen erleiden sowie an Ansehen und Vertrauen verlieren.

Besonders problematisch sind **koordinierte Shitstorms**, die von bestimmten politischen oder ideologischen Gruppen ausgehen. Solche Kampagnen werden zum Beispiel in rechtspopulistischen Facebook-Gruppen, Messenger-Diensten, über rechtsalternative Plattformen oder über Troll-Foren organisiert. Oft steht dabei im Mittelpunkt, demokratische Stimmen gezielt zu diskreditieren, zu provozieren oder sie aus öffentlichen Diskussionen zu verdrängen.

# Was tun bei digitaler Gewalt?

Strategien im Umgang mit digitaler Gewalt sind vielfältig, denn **alle Betroffenen gehen individuell und nach ihren spezifischen Bedürfnissen mit einem Angriff um**. Einigen Betroffenen ist es wichtig, sich aktiv mit den Bedrohungen zu beschäftigen. Andere wahren lieber Abstand und greifen auf Unterstützung zurück.

Wenn du selbst von digitaler Gewalt betroffen bist oder andere unterstützen möchtest, die Hass im Netz erleben, findest du hier nützliche Tipps und Anlaufstellen.

## Fünf Möglichkeiten, mit digitalen Angriffen umzugehen:

**1. Eine bewusste Auszeit nehmen:** Shitstorms haben ihren Höhepunkt in den ersten drei bis vier Tagen. Danach ebbt die Welle der digitalen Gewalt meist ab. Um sich selbst zu schützen, kann es helfen, sich in dieser ersten Zeit nicht mit den Hater\*innen auseinanderzusetzen und den eigenen Accounts fernzubleiben.

**2. Unterstützung holen:** Vielleicht können Freund\*innen, Kolleg\*innen oder Familienangehörige zur Seite stehen? Sie könnten beispielsweise die Social Media Accounts übernehmen, die Beweissicherung machen

oder einfach für die betroffene Person da sein. Auch professionelle Hilfe, wie HateAid und andere Beratungsstellen, sollte in Erwägung gezogen werden, um eine bestmögliche Unterstützung zu bekommen.

**3. Nicht persönlich nehmen:** Hater\*innen greifen zwar meistens persönliche Accounts an, aber der Hass gilt nicht wirklich der betroffenen Person selbst. Denn die betroffene Person ist für die Tatpersonen in Wirklichkeit nur eine Projektionsfläche (zum Beispiel für „die Frauen“ oder „die Ausländer“). Die Gründe für ihren Hass liegen immer in den Hater\*innen selbst. Das bedeutet auch und vor allem: Die betroffene Person ist nicht schuld, wenn sie angegriffen wird.

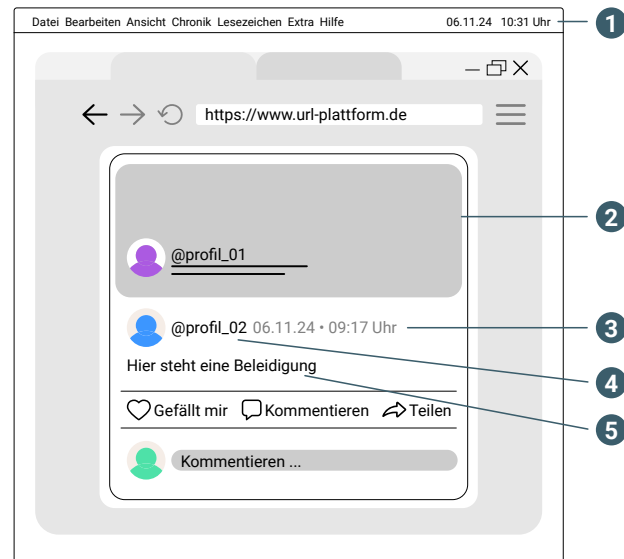
**4. Ablenken:** Sich schöne Dinge im Alltag zu suchen, mit denen sich die betroffene Person von den Angriffen ablenken kann, kann hilfreich sein. Das kann zum Beispiel ein Kinobesuch sein, sich mit Freund\*innen zu treffen oder etwas Gutes zu essen. Es ist wichtig, sich jetzt mehr denn je um sich selbst zu kümmern und zu versuchen, Abstand zu den Angriffen zu finden.

**5. Sich aktiv mit den Angriffen befassen:** Manchen geht es besser damit, statt Ablenkung die aktive Konfrontation mit der Situation zu suchen. Es kann helfen, die Nachrichten zu sammeln, damit an die Öffentlichkeit, zum Beispiel mit einem Statement auf den eigenen Profilen oder einem Blog-Artikel, zu gehen oder die Erlebnisse privat in einem Tagebuch festzuhalten. Reden hilft: mit dem persönlichen Umfeld, Berater\*innen oder auch mit Therapeut\*innen.

## Rechtssichere Screenshots:

Im Internet sind sie so etwas wie **Augenzeug\*innen in der analogen Welt**. Sie belegen die Tat, die begangen wurde. Das Internet hat eine große Reichweite, Hass und Hetze können rasend schnell verbreitet werden – und es ist **schnell-lebig**. Das bedeutet, dass auch Hasskommentare, Verleumdungen, diffamierende Bilder oder andere illegale Inhalte schnell wieder gelöscht werden können. Manchmal beruhigt es uns, dass die Inhalte plötzlich nicht mehr online zu sein scheinen. Gleichzeitig kann aber auch **keine Rechtsverfolgung erfolgen, wenn es keine Beweismittel gibt**. Deshalb ist es so wichtig, möglichst sofort rechtssichere Screenshots von potenziell justiziablen Inhalten zu erstellen.

Ein rechtssicherer Screenshot muss neben dem **Kommentar** auch **Datum und Uhrzeit des Kommentars** sowie den **(User\*innen-)Namen der\*des mutmaßlichen Täter\*in** enthalten. Außerdem muss der **Kontext** ersichtlich sein, in dem der Kommentar gepostet wurde. Es reicht also nicht, nur den Kommentar selbst zu sichern. Auch im Nachhinein muss das Posting oder Foto, auf das sich der Kommentar bezieht, zu sehen sein. Eine rechtliche Verfolgung ist nur dann aussichtsreich, wenn zu erkennen ist, **gegen wen sich der Hasskommentar richtet. Es gibt im Internet frei verfügbare Tools, die das Sichern von Inhalten leichter machen.**



- 1 Datum + Uhrzeit Screenshot
- 2 Kontext
- 3 Datum + Uhrzeit
- 4 Verfasser\*in
- 5 Inhalt

Beispiel eines rechtssicheren Screenshots

Mehr Informationen zu rechts-sicheren Screenshots sind hier auf der [Webseite](#) von HateAid zu finden.

## Tipps zur Prävention:



**Social-Media-Privatsphäre prüfen:** Alle Daten, die eine Person online stellt, sind ein potenzielles Risiko. Wenn die Privatsphäre der eigenen Social-Media-Profile so eingestellt ist, dass Außenstehende nichts Relevantes sehen können, bietet dies mehr Schutz.



**Ungewollte Suchmaschinen-Ergebnisse sowie Infos auf Webseiten löschen lassen:** Um zu prüfen, welche Infos über eine Person online sind, kann diese ihren Namen in eine Suchmaschine eingeben. Wenn irgendwo Daten zu finden sind, die nicht öffentlich sein sollen, können die Seitenbetreibenden kontaktiert und darum gebeten werden, die Daten zu entfernen. Unter bestimmten Voraussetzungen besteht auch ein Recht auf Löschung.



**Individuelle, lange Passwörter mithilfe von Passwortmanagern verwenden:** So lassen sich E-Mail- und Social-Media-Konten schwer hacken. Ein Passwortmanager hilft dabei, den Überblick zu behalten.



**Zwei-Faktor-Authentifizierungen nutzen:** Wenn Social-Media-Seiten oder andere Services eine Zwei-Faktor-Authentifizierung anbieten, sollte diese Funktionen genutzt werden. Hierzu meldet man sich nicht nur einmalig mit der Passwordeingabe an, sondern man erhält zum Beispiel noch eine SMS auf das Handy. Erst wenn der dort enthaltene Code eingegeben wird, gelangt man ins Konto. Damit wird die Identität doppelt auf zwei verschiedene Arten geprüft. Das ist einer der sichersten Wege, um die eigenen Daten zu schützen.



**Die eigenen Geräte vor Schad-Software schützen:** Vorsicht ist geboten bei Anhängen und E-Mails von Unbekannten. Anhänge sollten nicht einfach heruntergeladen werden. Auch auf verdächtige Links sollte niemals geklickt werden.

Wie diese Tools funktionieren und was für ein sicheres Passwort beachtet werden sollte, ist [unter diesem Link](#) auf der Webseite von HateAid zu lesen.

## Wichtige Anlaufstellen

### Beratung für Betroffene (digitaler Gewalt)

HateAid:

[hateaid.org/betroffenenberatung/](https://hateaid.org/betroffenenberatung/)

Mit unserer [MeldeHelden-App](#) kannst du Hass im Internet schnell, sicher und anonym zur Prüfung weiterleiten. Zudem erhältst du Unterstützung, wenn du selbst betroffen bist. Weitere Features: Tipps und Tricks sowie wichtige Notfall-Kontakte.

Stiftung Opferhilfe Niedersachsen:  
[opferhilfe.niedersachsen.de/](https://opferhilfe.niedersachsen.de/)

### Meldung und Anzeigen

Meldestelle RESpect!:

[meldestelle-respect.de/](https://meldestelle-respect.de/)

Zentralstelle zur Bekämpfung von Hasskriminalität  
im Internet in Niedersachsen (ZHIN):  
[hassanzeigen.de](https://hassanzeigen.de)

Niedersächsische Landesmedienanstalt,  
Team Regulierung:  
[nlm.de/beschwerde](mailto:nlm.de/beschwerde) ([regulierung@nlm.de](mailto:regulierung@nlm.de))

### Allgemeine Informationen

Koordinierungsstelle Landesprogramm  
für Demokratie und Menschenrechte:  
[kostlp@mj.niedersachsen.de](mailto:kostlp@mj.niedersachsen.de)

## Anmerkungen

1 Die hier aufgeführten Formen und Phänomenbereiche digitaler Gewalt stellen keinen Anspruch auf Vollständigkeit. Die Auswahl basiert vor allem auf den Erfahrungen der Betroffenenberatung von HateAid und mit welchen Formen Betroffene besonders häufig an HateAid herantreten.

2 Sprachlich ist der Begriff „Revenge Porn“ umstritten, weil „Porno-Bilder“ im Regelfall mit dem Einverständnis der Abgelichteten entstehen und häufig für eine Veröffentlichung vorgesehen sind, während bei der rachsüchtigen Publikation privaten Materials das absolute Gegenteil der Fall ist. Quelle: <https://taz.de/Ruecktritt-wegen-Revenge-Porn/!5635195/> [Zuletzt abgerufen am 09.07.2025].

3 An dieser Stelle wird bewusst nicht der Begriff „Deepfake-Pornos“ verwendet, da Pornografie meist Freiwilligkeit impliziert. Herkömmliche Pornografie beruht (zumindest idealerweise) auf der Einwilligung der Beteiligten. Bei Deepfakes ist meist das Gegenteil der Fall: Die betroffenen Personen wissen oft nichts von der Existenz solcher Inhalte oder lehnen sie ab. Daher ist es irreführend und verharmlosend, Deepfakes einfach unter die gleiche Kategorie zu stecken wie einvernehmliche Pornografie. Pornografische Deepfakes sehen zwar aus wie Pornos, sind aber keine Pornos im ethischen Sinne.

4 Upskirting bezeichnet das heimliche und unerlaubte Fotografieren oder Filmen intimer Körperbereiche wie Genitalien, Gesäß oder weiblicher Brust – oft unter der Kleidung oder durch die Kleidung hindurch. Die Aufnahmen entstehen meist ohne Wissen der be-

troffenen Person, da moderne Smartphones unauffällig eingesetzt werden können.

5 Diese beiden rechtlichen Wege gelten nicht nur für Fälle von bildbasierter sexualisierter Gewalt im Internet, sondern für alle Fälle der Persönlichkeitsrechtsverletzungen.

6 Als Trolle werden Personen bezeichnet, die in Online-Diskussionen absichtlich provozieren, stören oder andere Nutzer\*innen emotional aufwühlen wollen – meist durch beleidigende, irreführende oder polarisierende Beiträge. Ihr Ziel ist nicht der konstruktive Austausch, sondern Aufmerksamkeit, Reaktionen oder Chaos.

## Literaturverzeichnis

Bündnis gegen Cybermobbing (2022). Cyberlife IV – Cybermobbing bei Schülerinnen und Schülern. Techniker Krankenkasse. <https://www.buendnis-gegen-cybermobbing.de/cybermobbing-studie-cyberlife-iv.html> [Zuletzt abgerufen am 09.07.2025].

Security Hero (2024). The state of deepfakes: A comprehensive look into the threat landscape. <https://www.securityhero.io/state-of-deepfakes/#key-findings> [Zuletzt abgerufen am 09.07.2025].

Hyun Kim, Michelle (2019). TikTok Admits It Suppressed Reach of Queer, Fat, and Disabled Creators. [https://www.them.us/story/tiktok-suppressed-fat-queer-disabled-creators?utm\\_source=chatgpt.com](https://www.them.us/story/tiktok-suppressed-fat-queer-disabled-creators?utm_source=chatgpt.com) [Zuletzt abgerufen am 09.07.2025].

## Impressum

### Herausgegeben von

HateAid gGmbH  
Greifswalder Straße 4  
10405 Berlin

**E-Mail:** [kontakt@hateaid.org](mailto:kontakt@hateaid.org)  
[hateaid.org](http://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:** Emma Bombien und Katharina Heffe

**Korrektorat:** Kerstin Matuszak

**Gestaltung:** Regina Buschmeier

**Druck:** Umweltdruck Berlin

## Spenden

**Wir sind als gemeinnützige Organisation auf Spenden angewiesen.**

Mache das Internet zu einem besseren Ort und werde Dauerspender\*in von HateAid. Deine regelmäßige Spende fließt direkt in unsere tägliche Arbeit – und damit in die Meinungsvielfalt unserer Demokratie.

### Spendenkonto:

Kontoinhaberin: HateAid

Bank: GLS Bank

IBAN: DE04 4306 0967 1231 5982 03

BIC: GENODEM1GLS

[hateaid.org/spenden](http://hateaid.org/spenden)

## Notizen

