Editorial

Liebe Leser*innen,

Die aktuellen Debatten rund um den KI-Chatbot Grok auf X machen deutlich, wie eng digitale Geschäftsmodelle, mangelnde Schutzstandards und geschlechtsspezifische Gewalt zusammenhängen. Dass sexualisierte Deepfakes massenhaft generiert werden können, zeigt ein strukturelles Problem – befeuert von einer Tech-Kultur, die Innovation oft über Sicherheit stellt.

In dieser Ausgabe verbinden wir diese Entwicklungen mit unserem Plattform-Monitoring: Wo Verharmlosen Plattformen Risiken? Warum bleiben Meldewege schwer zugänglich? Und was braucht es, damit der Digital Services Act Betroffene tatsächlich schützt? Neben unserem Themenschwerpunkt findet ihr Einblick in unsere politische Arbeit, neue Fachinformationen, Medienbeiträge und kommende Fortbildungen.

Viel Spaß beim Lesen wünscht das bff: Aktiv gegen digitale Gewalt – Team:

Elizabeth Ávila González, Sandra Boger, Michaela Burkard

Inhalt

Aus unserem Team

- Aus unserem Plattform-Monitoring, genauer gesagt einer Analyse der Risikoberichte nach Art. 34 des Digital Services Act (DSA), ist ein Policy Paper hervorgegangen. Darin zeigen wir auf:
    - Welche Lücken es in den Risikoanalysen der Plattformen gibt und dass geschlechtsspezifische Gewalt darin systematisch verharmlost wird
    - Dass Meldewege und Kontaktmöglichkeiten auf den Plattformen nicht den Anforderungen des DSA entsprechen, da sie schwer oder gar nicht auffindbar sind, Nutzer*innen in eine Click-Fatique leiten und ihnen damit den Zugang zu ihren Rechten verwehren
    - Was es braucht, um Betroffenen von digitaler Gewalt wirklichen Schutz zu bieten: Feministische Standards, intersektionale Perspektiven und Meldewege, die tatsächlich leicht zugänglich sind

  Flankiert wurde unser Policy Paper von einer Social Media-Kampagne, die ihr auf Instagram findet und gerne teilen und kommentieren könnt!

- Gemeinsam mit Hate Aid reichten wir bei der Bundesnetzagentur eine Beschwerde gegen verschiedene Social Media Plattformen ein: Facebook, Instagram, Tik Tok und Snapchat; außerdem auch gegen die Pornoplattformen XVideos, Pornhub und Stripchat. All diese Anbieter verstoßen unserer Ansicht nach gegen Art. 12 des Digital Services Act (DSA). Dieser sieht vor, dass Plattformen eine Kontaktstelle bereithalten müssen, die niedrigschwellig erreichbar ist. Bei einigen Anbietern war überhaupt keine Kontaktstelle auffindbar, bei anderen müssen sich Nutzer*innen mühselig durch irreführende Menüs klicken oder bekommen nur den Kontakt zu einem Chatbot, nicht jedoch zu Mitarbeiter*innen. Dies ist bei digitaler Gewalt, insbesondere bei bildbasierter sexualisierter Gewalt, jedoch essentiell, um schnell eine Löschung zu veranlassen bzw. die Weiterverbreitung verletzender Inhalte zu unterbinden.
- Wir haben eine Fachinformation für unsere Mitglieder erstellt, die über die Datensammlung und -Auswertung von sog. einfachen Sensoren berichtet, also etwa Licht-, Temperatur- oder Bewegungssensoren. Aufgrund der sensiblen Inhalte ist das Dokument im geschützten Bereich der bff-Webseite abrufbar.
- Wusstest du, dass du für unser Projekt spenden kannst? Zu einer öffentlichen Förderung gehört fast immer auch ein Eigenanteil, den der Träger mit Spenden und anderen Einnahmen stemmt. Weitere Infos dazu findest du auf der Webseite des bff.
- Wir planen unsere Vorträge 2026. Derzeit gehen erste Anfragen für die Zeit rund um den 25.11. ein. Du möchtest einen Vortrag, Workshop oder eine Schulung von uns? Melde dich gern bei uns, damit wir ggf. auch langfristiger planen können.

Das Team von *Aktiv gegen digitale Gewalt* in den Medien

07.03.26 | Unser Projekt wird am 07.03 um 13:05 im Breitband-Podcast von deutschlandfunkkultur zu hören sein. Schaltet gerne ein!

02.03.26 | Die Lesubia-Studie liefert auch erstmals belastbare Zahlen zur Verbreitung digitaler Gewalt in Deutschland. Gleichzeitig wirft sie auch Fragen auf: wir haben die Ergebnisse auf Netzpolitik.org aus der Beratungssicht eingeordnet.

06.02.26 | Das fehlt beim Schutz vor digitaler Gewalt: verschiedene NGOs aus dem Bereich Gewaltschutz und Netzpolitik zeigen auf, welche Lücken es aktuell im Umgang mit digitaler Gewalt gibt, und was es für einen umfassenden Schutz von Betroffenen braucht.

13.02.26 | „Er wusste immer genau, wo ich war“: Netzpolitik.org zeichnet die Geschichte einer Frau nach, die von jahrelangem digitalen Stalking betroffen war.

17.02.26 | Meta, TikTok, Pornhub und Co. verstoßen gegen den Digital Services Act: bff und Hate Aid haben bei der Bundesnetzagentur Beschwerde gegen große Plattformen eingereicht.

Themenschwerpunkt: Warum wir uns für eine feministische Cybersecurity einsetzen sollten

Von Elizabeth Ávila González. Dieser Artikel zu zuerst auf dem Blog des Gunda-Werner Instituts erschienen.

Als Mina Camira Anfang Juni ihren Instagram-Namen googelte, stieß sie auf etwas, das ihr den Boden unter den Füßen wegzog: Zwischen üblichen Treffern tauchten Links zu Pornoseiten auf. Dort fand sie ihre eigenen Fotos – ursprünglich harmlose Vinted-Bilder, die sie zum Verkauf von Kleidung hochgeladen hatte. Die Bilder waren aus dem Kontext gerissen, sexualisiert, mit erniedrigenden Kommentaren versehen oder mithilfe von Software so bearbeitet, dass sie wie Nacktbilder wirkten. Mina entschied sich, ihre Geschichte öffentlich zu machen. Sie war auf Jobsuche und wusste, dass Personalabteilungen sie googeln würden. Ihr Reel ging viral: Hunderttausende reagierten mit Entsetzen und Solidarität. Recherchen von NDR, WDR und der Süddeutschen Zeitung zeigten später eine größere Dimension: Fotos von Vinted-Nutzer*innen werden massenhaft in Telegram-Kanälen kopiert, sexualisiert und verbreitet. Betroffenen berichteten von Belästigungen, dem Gefühl permanenter Beobachtung und davon, dass Meldungen ins Leere laufen.

In meiner Arbeit beim bff, dem Bundesverband der Frauenberatungsstellen und Frauennotrufe, beobachten wir seit Jahren, wie sich sexualisierte und häusliche Gewalt digitalisiert. Überwachung, Kontrolle und Erniedrigung verlagern sich von physischen Räumen auf Apps, Geräte und Plattformen. Minas Erfahrung spiegelt ein Muster: Digitale Gewalt ist reale Gewalt – verwurzelt in Machtverhältnissen, die sich im Digitalen fortsetzen. Besonders junge FLINTAs sind davon überproportional betroffen – genau jene Zielgruppe, die Vinted anspricht. Die Plattform verweist in Minas Fall auf vorhandene Meldewege.

Polizei und Justiz fehlt hier häufig das technische Verständnis für wirksame Rechtsdurchsetzung. Viele Täter bleiben ohne Konsequenzen, während Betroffene den Großteil der Beweis- und Handlungsarbeit selbst übernehmen – Screenshots sichern,

Meldewege durchklicken, Öffentlichkeit herstellen. Die Verantwortung liegt bei denen, die Gewalt erleben, während Plattformen profitieren. Außerdem werden Betroffene mit Victim-Blaming konfrontiert: Warum sie „überhaupt solche Bilder hochgeladen" hätten, als läge die Schuld bei ihrer Sichtbarkeit statt bei den Tätern. Dieses Narrativ entlastet Täter, ignoriert Plattformverantwortung und verschiebt die Zuständigkeit erneut auf Betroffene. Auch in Minas Fall wurde die Anzeige eingestellt, „Täter nicht ermittelbar". Seitdem nutzt Mina ihre Reichweite, um auf diesen Sexismus aufmerksam zu machen und fordert Politik und Plattformen heraus. In einer Petition verlangt sie Screenshotsperren, Verifizierungspflichten, besseren Schutz von Adressdaten und wirksame Filter gegen belästigenden Nachrichten.

Doch während Plattformen immer wieder Angriffsflächen für Gewalt bieten, bleiben Schutzmechanismen mangelhaft. Eine Studie von Das NETTZ zeigt erhebliche Defizite bei den nach dem Digital Services Act (DSA) vorgeschriebenen Meldewegen. Statt „einfach zugänglich" und „benutzer*innenfreundlich" zu sein, sind sie schwer auffindbar, hinter juristischen Formulierungen versteckt, und so gestaltet, dass Nutzende bei vermeintlichen „Falschmeldungen" Haftung befürchten. Jede vierte Meldung über den DSA-Weg wird abgebrochen. Selbst Beratungsfachkräfte wissen oft nicht, dass es unterschiedliche Meldewege gibt – hier besteht großer Aufklärungsbedarf. Eine Peer-Expertin mit Lernschwierigkeiten beschreibt, dass die Möglichkeit zu melden sie zwar bestärkt, das Navigieren jedoch nahezu unmöglich – wer auf einfache Sprache oder Barrierefreiheit angewiesen ist, wird faktisch ausgeschlossen.

Diese Unwissenheit hat Gründe: Die Europäische Kommission bestätigte jüngst, dass Plattformen wie Instagram, Facebook und TikTok setzen sogenannte „deceptive patterns" einsetzen – also eine manipulative Oberflächengestaltung benutzen, die davon abhält, Inhalte zu melden oder Schutzfunktionen zu finden. Digitale Dienste folgen einer Logik, in der Sichtbarkeit, Verweildauer und Datensammlung wirtschaftlichen Wert erzeugen. Gewalt, Belästigung und Hetze sind hier keine Fehler, sondern Bestandteile eines Geschäftsmodells. Schutz, Moderation und Transparenz werden als Kostenfaktor statt als Grundfunktion verstanden. Der DSA erkennt an, dass Plattformen eine besondere Schutzverantwortung haben und verpflichtet große Anbieter auch, sich mit „systemischen Risiken" auseinanderzusetzen – darunter geschlechtsspezifische Gewalt. Doch viele Plattformen sehen dieses Risiko weiterhin als isoliert digitales Problem und nicht als gesellschaftliches.

Gerade im sozialen Nahraum zeigt sich die enge Verknüpfung: Digitale Gewalt ist selten anonym; Täter sind häufig (Ex-)Partner, Familienmitglieder oder Personen aus dem Umfeld. Wer Passwörter oder Zugriff auf Accounts hat, kann Kontrolle und Überwachung digital fortsetzen. Die Gefahr sitzt oft buchstäblich am Küchentisch.

Um digitale Gewalt ernst zu nehmen, müssen wir uns fragen, wie Plattformen Cybersecurity verstehen. Digitale Gewalt ist ein Machtproblem, das sich in Technologie, Geschäftsmodellen und gesellschaftlichen Strukturen widerspiegelt. Feministische Cybersecurity stellt Selbstbestimmung, Datenschutz, intersektionales Gewaltverständnis und Transparenz ins Zentrum. Nutzer*innen müssen nachvollziehen können, wie ihre Daten genutzt werden und wie Algorithmen, Moderation und Design Entscheidungen Gewalt begünstigen oder verhindern. Schutz darf nicht von individueller technischer oder juristischer Expertise abhängen, sondern muss systemisch gesichert sein. Plattformen müssen Verantwortung übernehmen und

mit den Menschen in Dialog treten, die sie nutzen – besonders für FLINTAs und marginalisierte Gruppen. Feministische Cybersecurity fordert genau diese Verantwortungsumkehr: Weg vom Paradigma „Nutzer*in als Schwachstelle“ hin zu digitalen Räumen, die Sicherheit für alle ermöglichen. Nur so kann Gewaltschutz vor Profit stehen.

Wissen & Impulse: Digitale Gewalt im Fokus

Artikel, Videos, Veranstaltungen, Infobroschüren - aktuelle Debatten rund um digitale Gewalt

Die Fernuni Hagen hat in ihrer Video-Reihe „digitale_kultur“ einen Infofilm über die Gewalt im Smart Home. Episode 03: IoT, Kontrolle & Gewalt zeigt, wie smart Home Geräte, insbesondere Sprachassistent*innen funktionieren, welches Risiko sie im Bereich häusliche Gewalt bedeuten und wie wir als Gesellschaft mit der sich immer weiter ausdifferenzierenden Technik umgehen sollten. Der Beitrag ist sehr sehenswert für alle, die sich noch nicht intensiv mit Gewalt im smart Home auseinandergesetzt haben.

Ohne Datum | Anne Roth: Die Betroffenen-Zahlen von digitaler Gewalt sind eklatant hoch. Der Podcast „Wir sind das Web!“ von dem BERIT Beratungszentrum ist grundsätzlich hörenswert. In dieser Folge zeigt Digitalexpertin Anne Roth auf, was digitales Stalking ist und wie Betroffene Hilfe bekommen.

02.12.26 | EuGH nimmt Plattformen bei Datenschutzverstößen in die Pflicht. Wer haftet, wenn jemand im Namen einer Frau Online-Anzeigen für sexuelle Dienstleistungen veröffentlicht? Der EuGH entschied: Online-Marktplätze tragen eine Mitverantwortung.

24.01.26 | Gewalt und bauchfreie Oberteile. Die Gaming-Plattform Roblox ist beliebt bei Kindern und Jugendlichen. Doch Fälle von Cybergrooming und Inhalte, die Gewalt und sexualisierte Geschlechterbilder zeigen, lassen Zweifel an der Sicherheit für die Nutzer*innen aufkommen.

24.01.26 | Women filmed secretly for social media content – and then harassed online. Der BBC berichtet darüber, wie Frauen mit sog. Smart Glasses gefilmt und das Material online gestellt wurde, teilweise auch mit Veröffentlichung privater Kontaktdaten, und welche gravierenden Folgen dies für die betroffenen Frauen hatte.

30.01.26 | Einen bekleideten Po filmen – ist das bald strafbar? Im vergangenen Jahr ging der Fall Yanni Gentsch durch die Medien: Sie wurde ungewollt mit sexualisierter Absicht von einem Fremden auf den Po gefilmt und startete eine Petition, da dies nicht strafbar ist. Im Januar wurde ein Antrag zur Schließung dieser Schutzlücken in den Bundesrat eingebracht. Der Antrag bezieht sich außerdem auf einen Fall von ungewolltem Filmen in einer Sauna, das ebenfalls nicht strafbar ist.

10.02.26 | Dunkelfeldstudie "Lebenssituation Sicherheit und Belastung im Alltag (LeSuBiA)". Nach über 20 Jahren bringt das BKA wieder eine Dunkelfeldstudie heraus. Darin enthalten ist auch ein Kapitel zu digitaler Gewalt. Seit Herbst 2025 gibt es außerdem ein neues Lagebild „Geschlechtsspezifisch gegen Frauen gerichtete Straftaten 2024", auch darin gibt es eine Fallgruppe digitale Gewalt.

Januar-Februar 26| Bildbasiert, aber unsichtbar und KI ohne Verantwortung? Der Verfassungsblog beleuchtet in zwei Artikeln das Thema sexualisierte Deepfakes, u.a. mit der Frage, wie das deutsche Strafrecht auf sexualisierte Deepfakes reagiert, welche Schutzlücken es gibt, und dass die Verantwortung sowohl bei Einzelpersonen wie auch bei den Infrastrukturen liegt. Welches Ausmaß diese Form sexualisierter bildbasierter Gewalt hat, zeigt das Center For Countering Digital Hate: Ca. 3 Millionen sexualisierte Deepfakes produzierte das KI Tool Grok in den ersten elf Tagen bevor es gesperrt wurde, davon ca. 23.000 Aufnahmen von Minderjährigen.

26.02.26 | (Digitale) Barrierefreiheit ist kein optionales Feature: Zu Gast beim Podcast „Update Verfügbar" des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist in der aktuellen Folge Raúl Krauthausen, Aktivist für Inklusion und Barrierefreiheit.

Ohne Datum | Alptraum Deepfake-Pornos: Arte beleuchtet in der Doku-Reihe „künstliche Intelligenz – Fluch oder Segen?" in einer Folge bildbasierte sexualisierte Gewalt mit manipuliertem Bildmaterial.