



STELLUNGNAHME ANHÖRUNG ZUM THEMA „ENTSCHLOSSEN GEGEN DIGITALE GEWALT: DEEPPFAKES UND PORNFAKES STOPPEN!“

Mechthild Appelhoff, Leiterin Abteilung Medienorientierung

09. Januar 2025



1. HINTERGRUND

Der Einsatz von Künstlicher Intelligenz (KI) durchdringt viele Lebensbereiche und bietet sowohl Chancen als auch Risiken. Eine aktuelle Entwicklung sind sogenannte Deepfakes. Damit werden u. a. Bilder und Videos bezeichnet, die mithilfe von KI erstellt wurden und täuschend echt aussehen. Häufig werden diese ohne die Zustimmung der abgebildeten Personen erstellt. Dabei handelt es sich meistens um bekannte Menschen wie zum Beispiel Politikerinnen und Politiker. Mithilfe von KI werden diesen Menschen Worte, die sie nie gesagt haben, in den Mund gelegt, Fotos werden verändert und Videos so bearbeitet, dass sie Situationen zeigen, die nie stattgefunden haben. Diese täuschend echten KI-Ergebnisse können Meinungen beeinflussen und gesellschaftliche und demokratische Auswirkungen haben. Ein Beispiel, das zeigt, wie einfach Deepfakes erstellt werden können und welche problematischen Auswirkungen diese haben können, ist ein [YouTube-Video des AfD-nahen Influencers Eric Ahrens](#). In diesem erklärt er, wie man harmlose Tanzvideos von Dritten ohne deren Wissen und Zustimmung so bearbeiten kann, dass es wirkt, als sei das Video eine Performance zur Unterstützung der AfD. Solche Deepfakes dienen der politischen Einflussnahme.

Laut einer [Studie](#) der Firma Security Hero sind 98 % aller Deepfakes pornografischer Natur und werden missbräuchlich eingesetzt, hier spricht man auch von Pornfakes. Pornfakes sind Bilder und Videos, die mithilfe von KI erstellt oder manipuliert wurden, um Gesichter und Körper ohne Einwilligung in pornografische Bilder oder Videos einzufügen. In 99 % der Pornfakes sind Frauen die Ziele der Fälschungen. Die Betroffenen sind meistens prominente Frauen oder auch Frauen, deren Ex-Partner sich rächen möchten. Die Erstellung von Deepfakes und Pornfakes ist mit den entsprechenden Tools mittlerweile auch ohne IT-Kenntnisse für nahezu jede und jeden möglich.

Die Urheber von politischen Deepfakes möchten gezielt Desinformation und Unsicherheit verbreiten, sowie Meinungen beeinflussen. Zielgruppe ist die breite gesellschaftliche Masse und insbesondere diejenigen, die in ihrer politischen Meinung schwanken. Pornfakes verfolgen dagegen das Ziel, den betroffenen Frauen willentlich zu schaden und/oder zur Unterhaltung der konsumierenden Männer zu dienen.

In der oben genannten Studie wurden zudem 1.500 amerikanische Männer gefragt, ob sie sich bei dem Konsum von Pornfakes schuldig fühlen, dies wurde von 74 % verneint. Als Gründe nannten sie u. a., dass sie wüssten, dass es sich nicht um die reale Person handelt, deren Gesicht zu sehen ist. Außerdem sind die befragten Männer der Meinung, dass es niemandem wehtun würde, solange sie den Konsum nur im Sinne ihres eigenen Interesses verfolgen und Pornfakes einfach eine realistischere Version von sexueller Vorstellungskraft wären. Die Männer wurden zudem befragt, was sie tun würden, wenn sie wüssten, wenn jemand, den sie gut kennen, ungefragt in einem Pornfake auftauchen würde. 68 % wären schockiert und wütend und 73 % würden das Bild/Video bei Behörden melden wollen. Einer von fünf Nutzenden hat zudem angegeben, dass Pornfakes den Konsum von traditioneller Pornographie für ihn komplett ersetzt haben. Im Jahr 2023 waren 550 % mehr Pornfakes im Umlauf als im Jahr 2019 (insgesamt 95.820).

Pornfakes sind Formen digitaler Gewalt. Sie verbreiten sich schnell und unkontrolliert über pornografische Websites und digitale Medien und können gravierende Folgen haben: Die Betroffenen kämpfen mit Angstzuständen, Depressionen und einem Gefühl des Kontrollverlustes. Viele erleben zudem soziale Stigmatisierung und berufliche Schwierigkeiten (Quellen: Studie [„Image-based Sexual Abuse“](#) und Studie [„Shattering Lives and Myths“](#)).



2. AKTIONSFELDER

Die Folgen von Deepfakes und Pornfakes können verheerend sein. Deepfakes, die dazu verwendet werden, um Meinungen zu beeinflussen, indem sie zum Beispiel Aussagen von Politikerinnen und Politikern fälschen, sorgen dafür, dass sich Desinformation rasant verbreitet, da die Aussagen häufig zu einer Emotionalisierung und daher auch zu einer unreflektierten Weiterverbreitung führen. Eine weitere Folge kann ein erhöhtes Misstrauen in mediale Berichterstattung sein. Dies kann sich ebenfalls darauf auswirken, wie und wo sich Menschen informieren und welchen Informationen sie Glauben schenken.

Was braucht es also, um Deepfakes im Netz angemessen begegnen zu können, diese zu enttarnen und nicht unbedacht weiterzuleiten? Die **Förderung von Medienkompetenz** spielt hier eine entscheidende Rolle. Menschen, die in der Lage sind, digitale Medien selbstbestimmt, fair und reflektiert zu nutzen, laufen weniger Gefahr, auf Fälschungen hereinzufallen. An erster Stelle gilt es also Nutzenden die Hintergründe zu erläutern, die den Einsatz von Deepfakes und Desinformation auslösen und sich stets zu fragen, wem es nutzen könnte, wenn Menschen die (Falsch)Information glauben. Dies fördert die Motivation, sich mit dem Thema zu beschäftigen und Fakes zu entlarven.

Aktuell gibt es bei Bildern und Videos häufig noch Elemente, auf die geachtet werden kann, um herauszufinden, ob sie echt sind oder nicht. Dazu gehören Unschärfen, merkwürdig geformte Hände oder Münder, deren Bewegungen nicht ganz zum Gesagten passen. Jedoch entwickelt die Technologie sich rasant weiter, sodass auch diese kleinen Fehler zeitnah ausgebessert werden und die Fälschungen nicht mehr verraten. Dann wird eine Kernkompetenz noch wichtiger werden: Das Innehalten und Reflektieren der Dinge, die man online sieht. Es braucht die Fähigkeit des kritischen Hinterfragens und des Hörens auf das eigene Bauchgefühl: Wer könnte davon profitieren, dass Menschen dieses oder jenes glauben? Kann diese Information überhaupt stimmen? Und was könnte dafür sprechen, dass es sich um eine Fälschung handelt? Darüber hinaus ist es wichtig, dass Menschen wissen, woran sie eine glaubwürdige Quelle erkennen, bei welchen sprachlichen Formulierungen sie aufhorchen sollten und auf welchen Kanälen sie zuverlässige Informationen finden. Jede und jeder trägt bei dem kritischen Umgang mit Informationen im Netz Verantwortung für unsere Demokratie.

Im Kontext von Pornfakes ist auch der Blick auf die Betroffenen wichtig: Wie können sie Deepfakes zur Anzeige bringen, wie kann man Frauen für den Ernstfall Möglichkeiten zum aktiven Handeln aufzeigen und wie können Frauen sich vor Deepfakes aktiv schützen? Welche Möglichkeiten der Prävention kann man Frauen an die Hand geben?

Die Landesanstalt für Medien NRW wird in diesem Kontext beispielsweise aktiv, wenn politische Deepfakes im Rahmen von regelmäßig aktiven Nachrichtenangeboten präsentiert werden, da diese gegen die journalistische Sorgfaltspflicht verstoßen. Nutzende können diese auf der Website der Landesanstalt für Medien NRW melden. Bei der Anzeige und Verfolgung von Pornfakes sind dagegen die betroffenen Personen gefragt und können hier vom Zivilrecht Gebrauch machen, da ihre Fotos/Videos ohne ihr Einverständnis missbräuchlich verwendet werden (Verstoß gegen das Persönlichkeitsrecht).

Angesichts der aktuellen Entwicklung bei sehr großen Online-Plattformen wie vor allem Meta und X wird zunehmend deutlich, dass die Anbieter solcher Plattformen nach eigenem Bekunden ihre Bemühungen reduzieren werden, Phänomene wie Falschinformationen aller Art zu bekämpfen.



In Fällen eines systemischen Versagens der Plattformen gibt der Digital Services Act der Europäischen Kommission die Möglichkeit, die Plattformen zu entsprechenden Maßnahmen aufzufordern und gegebenenfalls ein fehlendes Tätigwerden zu sanktionieren. Erwägenswert wäre es, dass Mitgliedsstaaten wie die Bundesrepublik die Kommission in ihrem Bestreben bestärken.

Die Landesanstalt für Medien NRW greift darüber hinaus die Themen Deepfakes und Pornfakes in ihren Medienkompetenzangeboten ZEBRA, Medienscouts NRW, Eltern und Medien und Internet ABC in unterschiedlicher Weise mit dem Ziel auf, aufzuklären, zu sensibilisieren und zur Handlungsfähigkeit bei verschiedenen Zielgruppen beizutragen (s. Punkt 3).

3. ANGEBOTE DER LANDESANSTALT FÜR MEDIEN NRW

Die Landesanstalt für Medien NRW hat das Ziel, dass sich alle Menschen in Nordrhein-Westfalen sicher und souverän in der Medienlandschaft bewegen können. Den damit verbundenen Herausforderungen begegnet die Landesanstalt für Medien NRW mit der Bereitstellung zielgruppengerechter Formate zur Medienorientierung, mit denen die Bürgerinnen und Bürger bei Fragen und Problemen zur Nutzung digitaler Medien unterstützt werden.

In diesem Kontext wird auch das Themengebiet „Deepfakes und Pornfakes“ zielgruppengerecht behandelt, um eine breite Sensibilisierung und Aufklärung bei Kindern und Jugendlichen, Eltern sowie pädagogischen Fachkräften zu fördern.

A. ZEBRA

ZEBRA ist das Frage-Antwort-Angebot der Landesanstalt für Medien NRW, das sich auf die individuelle Beantwortung von Medienfragen spezialisiert. Nutzende können über verschiedene Kanäle wie Website, WhatsApp, Instagram oder TikTok Fragen zu Medienthemen stellen und erhalten unabhängige, sachkundige und zielgruppenorientierte Antworten. Auf diese Weise kann sowohl Heranwachsenden unterschiedlichen Alters, als auch Eltern oder pädagogischen Fachkräften gezielt geholfen werden. Um insbesondere die junge Zielgruppe zu erreichen, werden zudem auf den Social-Media-Plattformen Instagram und TikTok informative und unterhaltsame Texte, Videos und Memes ausgespielt, die sowohl zur Medienbildung der Zielgruppe beitragen, als auch dafür sorgen, dass diese sich mit ihren persönlichen Anliegen an ZEBRA wendet.

Aktivitäten zum Thema Deepfakes und Pornfakes:

- **Aufklärung und Information:**
 - Website: Auf der ZEBRA-Website befindet sich die Themenwelt Künstliche Intelligenz, die viele Fragen zum Thema KI und Deepfakes beantwortet, darunter zum Beispiel:
 - Ist künstliche Intelligenz gefährlich?
 - Wie kann man mit KI Bilder generieren?
 - Müssen Inhalte gekennzeichnet werden, die mit KI erstellt wurden?
 - Was sind Deepfakes und wie kann ich sie erkennen?
 - Wo finde ich Material, um Jugendlichen Deepfakes zu erklären?
 - Kann KI unsere Demokratie gefährden?

- [Wie gehe ich verantwortungsbewusst mit KI um?](#)
- [Was sind Deepnudes?](#)
- [Was kann ich tun, wenn jemand Deepnudes von mir erstellt?](#)
- Social Media: Sowohl auf Instagram als auch TikTok werden die Themen behandelt, zum Beispiel hier:
 - [TikTok | Kennzeichnung von KI](#)
 - [Instagram | KI auf dem Prüfstand](#)
 - [Instagram | Zukunft von Sora \(bildbasierte KI\)](#)

B. MEDIENSCOUTS NRW

Das Angebot [Medienscouts NRW](#) unterstützt weiterführende Schulen in Nordrhein-Westfalen dabei, Herausforderungen wie Cybermobbing, Hassrede und Cybergrooming präventiv anzugehen. Im Rahmen einer mehrtägigen Qualifizierung werden Jugendliche zu Medienscouts ausgebildet und beraten anschließend ihre Mitschülerinnen und Mitschüler zu Fragen und Problemen im digitalen Alltag. Durch die Peer-to-Peer-Beratung ermöglichen die Medienscouts einen sicheren und verantwortungsvollen Umgang mit digitalen Medien.

Seit diesem Jahr werden Medienscouts auch an [Grundschulen](#) ausgebildet. Die jungen Medienscouts sollen jedoch nicht beraten, sondern haben einen Wissensvorsprung und kennen sich mit einigen Medienthemen sehr gut aus. Sie machen Wissen aus dem [Internet-ABC](#) für ihre Mitschülerinnen und Mitschüler spielerisch anwendbar und vermitteln dieses auf Peer-to-Peer-Ebene.

Das Angebot Medienscouts NRW wird vom Ministerium für Schule und Bildung Nordrhein-Westfalen seit dem Schuljahr 2019/20 unterstützt und gefördert.

Aktivitäten zum Thema Deepfakes und Pornfakes:

- **Weiterführende Schule:**
 - Im Rahmen der Qualifizierung werden die Medienscouts NRW zu dem Thema Desinformation aus- und fortgebildet. Der Schwerpunkt Deepfakes spielt dabei eine große Rolle. Die Medienscouts lernen zum Beispiel, woran sie ein Deepfake erkennen können und wie sie ihre Mitschülerinnen und Mitschüler für das Thema sensibilisieren.
- **Grundschule:**
 - In der Ausbildung der Grundschul-Medien-scouts wird das Thema Informationskompetenz ebenfalls behandelt, dafür wird ein kindgerechter Rahmen gewählt. Die Medienscouts lernen zunächst, welche Kindersuchmaschinen es gibt und welche Suchbegriffe sich eignen. Für 2025 ist geplant, weiteres Material zu diesem Thema zu entwickeln, darunter auch ein Angebot zum Thema Desinformation. Im Mittelpunkt steht hier das kritische Hinterfragen von Bildern, die eine scheinbar spannende Geschichte erzählen. Die Medienscouts sollen herausfinden, ob die Bilder echt sind oder nicht und diese Reflektionskompetenz auch an ihre Mitschülerinnen und Mitschüler vermitteln.



C. ELTERN UND MEDIEN

Digitale Angebote und Geräte spielen im Leben von Kindern und Jugendlichen eine wichtige Rolle. Für Eltern ergeben sich hieraus viele Fragen: Was mache ich, wenn mein Kind gemobbt wird? Wie schütze ich mein Kind vor (sexueller) Belästigung im Internet? Wie kann ich mein Kind stärken, damit es nicht auf Desinformation hereinfällt? Immer mehr Erziehungsberechtigte suchen nach praktischen Antworten.

Hier setzt das Angebot [Eltern und Medien](#) an. Es unterstützt pro Jahr bis zu 650 Kitas, Schulen und andere Einrichtungen aus Nordrhein-Westfalen bei der Planung, Organisation sowie Durchführung von Elternabenden zur Medienerziehung und stellt kostenfrei eigens qualifizierte Referierende zur Verfügung.

Aktivitäten zum Thema Deepfakes und Pornfakes:

- Für weiterführende Schulen wird ein Elternabend mit dem Titel „Demokratie im Netz“ angeboten. Dieser behandelt u.a. die Themen „KI & Algorithmen“ und „Desinformation“. Dabei wird besprochen, welche Chancen und Risiken KI und insbesondere Deepfakes für Kinder und Jugendliche beinhalten und woran man Desinformation erkennen kann.

D. INTERNET-ABC

Das [Internet-ABC](#) bietet als zuverlässige, werbefreie und sichere Plattform für Kinder von 5-12 Jahren digitale Lernangebote zu Themen wie Mediensucht, Cybermobbing, Soziale Medien oder Fake News. Mit dem Internet-ABC können Kinder das Basiswissen für den sicheren Umgang mit dem Internet erlernen und gleichzeitig in einem geschützten und moderierten Bereich verschiedene Formen der Netzkommunikation einüben.

Aktivitäten zum Thema Deepfakes und Pornfakes:

- Informationen für Kinder:
 - [Artikel „Gefälschte Bilder und Videos“](#): Der Artikel erklärt, was ein Deepfake ist und welche Gefahren damit verbunden sind.
 - [Artikel „Neun Schritte gegen Deepfakes – falsche Inhalte im Internet“](#): Hier werden Fragen präsentiert, die Kinder sich stellen können, um herauszufinden, ob ein Bild/Video echt ist oder nicht.
 - [Digitale Pinnwand zum Thema KI](#): Auf der digitalen Pinnwand können Kinder Fragen zu Themen stellen und von ihren eigenen Erfahrungen berichten, außerdem gibt es eine eigene Pinnwand zum Thema KI, die von den Kindern gern genutzt wird.
- Informationen für Lehrkräfte und Eltern:
 - [Artikel „Deepfakes – Gefälschte Videos“](#) : Hier wird erklärt, was Deepfakes sind.



4. FAZIT

Neben den Maßnahmen zur Prävention ist auch ein **effektiver Jugendmedienschutz** wichtiger Bestandteil bei dem Vorgehen gegen Deepfakes und Pornfakes. KI-Systeme, die eine Erstellung von Pornfakes ermöglichen, müssen in die Verantwortung genommen werden. Plattformanbieter, die ein unkontrolliertes Hochladen und Weiterverbreiten entsprechender Bilder und Videos erlauben, tragen ebenfalls eine enorme Verantwortung und sollten ihre Systeme so weiterentwickeln, dass dem Einhalt geboten wird. Die Begleitung, Befähigung und Unterstützung insbesondere von jungen Menschen beim Umgang mit digitalen Medien ist und bleibt ein zentraler Baustein der Gefahrenprävention, jedoch müssen auch die Plattformanbieter ihren Teil zu einer sicheren digitalen Umgebung beitragen. Ein nachhaltiger Jugendmedien- und Nutzerschutz kann daher nur gelingen, wenn die Anbieter von digitalen Diensten in die Pflicht genommen werden.

Die **aktuelle Entwicklung bei sehr großen Online-Plattformen wie vor allem Meta und X** macht deutlich, welche große Rolle der Digitale Services Act auch zukünftig bei der Bekämpfung von Falschinformation spielen wird. Hier hat die Europäische Kommission die Möglichkeit zu handeln und die Plattformen zu entsprechenden Maßnahmen aufzufordern.

Im Sinne eines sicheren und selbstbestimmten Aufwachsens mit digitalen Medien bedarf es also einer **effektiven Zusammenarbeit** zwischen Eltern, Bezugspersonen, pädagogischen Fachkräften, Aufsichtsinstanzen, der Politik und Plattformanbietern. Die Landesanstalt für Medien NRW will hierzu im Rahmen ihrer Netzwerkarbeit einen entsprechenden Beitrag leisten.