

# technologie & pressefreiheit

2. – 8. mai 2026 taz panterstiftung



editorial

## Technik fordert Medien heraus

Medienkompetenz, Regulierung der IT-Konzerne und gemeinwohlorientierte digitale Strukturen sind heute wichtiger denn je

Die Warnung unter den Suchergebnissen zu Technologie und Pressefreiheit lautet lapidar: „KI-Antworten können Fehler enthalten.“ Heißt es in der Arzneimittelwerbung noch pflichtschuldig: „Zu Risiken und Nebenwirkungen lesen Sie die Packungsbeilage und fragen Sie Ihre Ärztin, Ihren Arzt oder in Ihrer Apotheke“, lässt die KI Nutzende mit ihren Zweifeln allein. Nicht nur Journalisten machen Fehler, auch Künstliche Intelligenz ist nicht perfekt: Weil sie vielleicht selektiv oder gar manipulativ mit Inhalten gefüttert wurde und weil Algorithmen Relevanz quantitativ werten, aber nicht qualitativ einordnen können.

Soziale Medien, Internetplattformen und KI-Programme wollen selbst erklärend sein, profitieren aber davon, dass Nutzende nur begrenztes Wissen über den Umgang mit ihnen haben. Die Weiterentwicklung digitaler Technologien in Medien und Gesellschaft ist alternativlos. Die willkommenen Hilfsmittel sind gefährlich, wenn sie selbst über Inhalte entscheiden und zu Desinformation, Manipulation und Überwachung beitragen. Ohnehin hat sich die Situation für Journalisten und Medienschaffende weltweit verschlechtert, wie die neue Rangliste der Pressefreiheit von Reporter ohne Grenzen zeigt. Den stärksten Rückgang gab es demnach im rechtlichen Bereich, auch wird Journalismus immer häufiger kriminalisiert.

Gut ist die Situation nur noch in 7 von 180 Ländern. Zwar hat sich in Syrien die Situation nach dem Sturz des Assad-Regimes stärker als in allen anderen Ländern verbessert. Das ist erfreulich, trotzdem liegt Syrien nur auf Rang 141. Wie die Tabelle auf der nächsten Seite zeigt, sind Länder mit massiver krimineller Gewalt wie Mexiko besonders tödlich für Journalisten. In streng autoritär regierten Staaten wie Russland, Belarus, China und Vietnam bringen dagegen missbräuchlich angewandte Gesetze auffällig viele Reporter ins Gefängnis.

Um die Pressefreiheit zu schützen, müssen unabhängige Medien gestärkt und bedrohte Journalisten geschützt werden, nicht nur vor autoritären Regimen, sondern auch immer mehr vor den Gefahren moderner Digitaltechnologie. Die Stärkung von Demokratie, Pluralismus, faktenbasiertem Wissen und die Verhinderung von Meinungs- und Technologiemonopolen sollten dabei zentrale Ziele sein. *Sven Hansen*

## Führt die KI zum K.o. der Pressefreiheit?

Künstliche Intelligenz wird im Journalismus zum Hilfsmittel, das den wirtschaftlichen Druck erhöht. Doch die größte Gefahr ist nicht, dass KI uns ersetzt, sondern die Strukturen verändert, in denen wir Realität wahrnehmen

Von Andre Wolf

Künstliche Intelligenz ist für die einen der Heilsbringer, für die anderen die größte Katastrophe. Dabei wissen wir nicht konkret, worüber wir eigentlich reden. Denn wenn wir über KI sprechen, tun wir so, als wäre KI nur ein Ding. Doch es ist mehr als das. Der Begriff KI, die übrigens auch nicht wirklich intelligent ist, ist ein Sammelbegriff für viele unterschiedliche Systeme. Sprechen wir von KI, meinen wir etwa Chatbots wie ChatGPT. Aber KI sind auch Bildgeneratoren, Algorithmen, kognitive oder generell autonome Unterstützungssysteme, Robotiksysteme.

Wir sind überfordert mit dem, was KI ist, was sie kann und vor allem, wie schnell sie sich entwickelt. Die Arbeitsweise, auch die Geschwindigkeit, mit der KI arbeitet, und die Ergebnisse, die dabei entstehen, seien es Deepfakes oder Bilder, können uns auch überfahren. Und wir können zum Teil gar nicht richtig mit dem umgehen, was KI uns liefert.

Technisch ist KI in einzelnen Bereichen komplett verschieden. Es sind unterschiedliche Systeme, und wir selbst können nicht genau einschätzen, was KI alles ist. Deswegen verstehen wir KI oft nicht nur falsch, sondern systematisch falsch. Wir übertragen oft falsche Erwartungen auf KI, oder auf die falschen Systeme innerhalb von KI. Das, was wir sehen, ist nur das Ergebnis. Der KI-Prozess selbst, also das, was zur Verarbeitung passiert, bleibt uns verborgen. Das nennt man Blackbox-KI. Und diesen Blackbox-Effekt können selbst Expertinnen und Experten oft nicht im Detail erklären, weil er schlicht nicht einsehbar ist. Verstehe ich nicht, wie etwas funktioniert, verliere ich die Kontrolle. Da-

raus entsteht die Angst davor, wie KI arbeitet, warum sie so arbeitet, welche Ergebnisse sie liefert und was diese mit uns machen können. Und welche gesellschaftlichen Probleme unbemerkt entstehen können.

KI selbst kann im klassischen Sinn keine Zensur ausüben. Zensur geht im bisherigen Verständnis von Menschen oder Organisationen aus, die Systeme gestalten und steuern. Lange Zeit war sie vor allem ein Instrument von Staaten, doch heute wird sie auf parastaatlicher Ebene auch durch Plattformen, Konzerne oder andere Machtstrukturen umgesetzt. KI übernimmt dabei nicht die Entscheidung, sondern die Umsetzung. Und dabei geht es um schnelle, menschenlose Umsetzung. Sie filtert, gewichtet und sortiert Inhalte entlang von Vorgaben, die von Menschen definiert wurden.

Wenn ich auf Social Media etwas poste oder Inhalte veröffentliche, wird KI diese filtern. KI kann Inhalte



Foto: mimikama.org/Nadja Buechler

**Andre Wolf** ist Sprecher und deutscher Autor und Social-Media-Experte beim Verein Mimikama in Wien, der sich der Aufklärung von Desinformation, der digitalen Medienkompetenz und der Betrugsprävention im Internet widmet.

nach Kriterien sortieren. Taucht ein bestimmter Begriff auf, bekommt ein Inhalt mehr oder weniger Reichweite. KI kann Inhalte verstärken, indem sie sie häufiger verbreitet und sie dadurch für andere Systeme als relevant erscheinen lässt. Und so können künstliche Intelligenzen in Form von Algorithmen die öffentliche Meinung beeinflussen. Wir wissen, dass Social Media und große Tech-Konzerne genau das tun.

Bestimmte Themen und Emotionen bekommen mehr Reichweite als andere. Vor allem aggressive Emotionen werden stärker verbreitet, weil Plattformen darauf ausgelegt sind, dass wir möglichst lange und intensiv mit ihnen interagieren. Moderate, sachliche und informationsbasierte Inhalte gehen dabei häufig unter. Das wird gezielt ausgenutzt.

Das ist keine klassische Zensur, wie sie ein Staat ausübt, aber eine Form stiller Steuerung. Und diese kann dazu führen, dass sich unser Bild von der Realität verschiebt, weil wir omnipräsent Krawall wahrnehmen. Das ist eines der zentralen Probleme: KI kann unser Verständnis von Öffentlichkeit verändern.

Doch was passiert, wenn KI im Journalismus ankommt? Ist KI ein Jobkiller oder eine Chance für bessere Qualität im Journalismus? Die große Angst ist, dass KI Texte schreibt und diese direkt veröffentlicht werden. Ja, das ist möglich. Standardisierte Inhalte können automatisiert erzeugt werden. Agenturmeldungen, Zusammenfassungen oder einfache Analysen lassen sich problemlos generieren. Das erhöht den Druck auf Journalistinnen und Journalisten, die plötzlich in Konkurrenz zu maschinell erzeugter Massenproduktion stehen. Das kann dazu führen, dass Journa-

lismus wirtschaftlich stärker unter Druck gerät und langfristig ausgehöhlt wird.

Doch genau hier liegt auch eine Chance. Denn KI kann vieles nicht: Nicht menschlich bewerten, nicht wirklich recherchieren, nicht mit Menschen sprechen, keine langfristig tiefgehenden Texte entwickeln. Sie kann nur punktuell Inhalte erzeugen. Vor allem kann sie keine Verantwortung übernehmen. Sie kann nicht reflektieren, was sie schreibt. Sie versteht keine gesellschaftlichen Konsequenzen. Sie kann nicht beraten, nicht einordnen und nicht bewerten. Genau das ist die Aufgabe des Journalismus. Denn Journalismus ist mehr als Textproduktion, bedeutet Einordnung, Kontext und Verantwortung. Genau dort muss Journalismus wieder stärker ansetzen.

KI kann als Werkzeug genutzt werden. Als Hilfsmittel beim Schreiben, als Korrekturinstanz. Aber sie darf nicht Aufgaben übernehmen, die sie ohnehin nicht leisten kann. Bewertung, Haltung, Einordnung, auch subjektive Formate wie Kolumnen oder Satire. All das bleibt menschlich. Und hier kann und muss der Journalismus punkten! Die größte Gefahr ist nicht, dass KI uns ersetzt, sondern dass KI die Strukturen verändert, in denen wir Realität wahrnehmen. Durch Algorithmen, durch (gezielt?) falsche Gewichtung, durch eine beeinflusste Informationsökologie auf Social Media entsteht ein verzerrtes System, das unsere Wahrnehmung der Realität verformt. Wir bemerken diese Veränderung oft erst, wenn sie bereits voll wirksam ist.

### Impressum

**Konzept und Redaktion:** Sven Hansen, Gemma Terés Arilla  
**Grafik:** Yorgos Konstantinou  
**Übersetzungen:** Sven Hansen  
**Layout:** Nadine Fischer

**Korrektur:** Rosemarie Nünning  
**Dokumentation:** Sigrud Deitelhoff

Die Artikel geben nicht unbedingt die Meinung der Redaktion wider.

taz panterstiftung

RSF REPORTER OHNE GRENZEN

Plattformmacht und Regulierung:

# Transparenz gegen Werbemanipulation

Beim Entwurf für das Politische-Werbung-Transparenz-Gesetz (PWTG) sind nicht nur Umsetzungs- und Definitionsprobleme sichtbar, sondern es fehlt auch der explizite Verweis auf den Schutz der Pressefreiheit

Von Alina Clasen

Politische Werbung spielt zur Vermarktung von Ideen und Persönlichkeiten eine wichtige Rolle in der Meinungsbildung und kann gesellschaftliche und demokratische Prozesse maßgeblich beeinflussen. Durch den technologischen Wandel hat sich die Form politischer Werbung von traditionellen Medien zu grenzüberschreitenden digitalen Werbeanbietern weiterentwickelt. Daraus leitet sich eine höhere Verantwortungs- und Sorgfaltspflicht ab, über Vorgänge und Fakten von öffentlichem Interesse zeitnah zu informieren und ihr Handeln offenzulegen.

Transparenzanforderungen ermöglichen, dass Informationen, zum Beispiel wer die geschaltete Werbung sponsert, bereitgestellt werden müssen. Nutzer\*innen können so irreführende Werbeanzeigen besser erkennen, ihr Bewusstsein hinsichtlich der gezielten Beeinflussung schärfen und sich eine eigene Meinung bilden. Transparenz hilft, manipulative Targeting-Strategien der digitalen Plattformen offenzulegen, möglicher ausländischer Einflussnahme entgegenzuwirken und demokratische Debatten besser zu schützen.

Die seit Oktober 2025 geltende EU-Verordnung über die Transparenz und das Targeting politischer Werbung (TTPW-VO) hat in der EU einen einheitlichen Regelungsrahmen zu Transparenz- und Sorgfaltspflichten eingeführt. Das ist mit Blick auf die wachsende gesellschaftliche Polarisierung dringend erforderlich. Jedoch muss sichergestellt werden, dass sich Plattformen wie Google und Meta diesen neuen Pflichten nicht durch ein simples Verbot entziehen können und die Sichtbarkeit gesponserter politischer Inhalte im digitalen Raum gewährleistet wird.

Meta und Google reagierten auf die neuen Transparenzanforderungen nämlich mit umfassender Einschränkung: Die Plattformen lassen die Ausspielung von Anzeigen „zu gesellschaftlich relevanten Themen“ nicht mehr zu. Begründung: Die Verordnung schaffe Rechtsunsicherheit. Diese Einschränkungen wirken jedoch unpräzise, weil sie über das, was nach der TTPW-VO als politisch zählt, hinausgehen. Zudem funktioniert die Sperre durch den Algorithmus nicht umfassend und nicht alle Anzeigen werden erkannt und blockiert.

Damit entziehen sich die Plattformen ihrer Verantwortung unter der TTPW-VO, beschneiden den Zugang zu Wahlinformationen für Bürger\*innen und beeinträchtigen die Möglichkeit zivilgesellschaftlicher Organisationen, sich am demokratischen öffentlichen Diskurs beteiligen und zum Beispiel Fundraisingkampagnen schalten zu können. So wurden auch Anzeigen von Reporter ohne Grenzen auf Meta-Plattformen blockiert. Die Gefahr: Je mehr diesem Beispiel folgen, desto mehr wird die Möglichkeit einer Beteiligung am politischen Diskurs und der politischen Meinungsbildung geschwächt.

Die Entscheidungsmacht darüber, was bezahlte politische Wer-

## Rangliste der Pressefreiheit 2026

Auswahl der gefährlichsten Länder für Journalist:innen und Medienschaffende  
Erfassungszeitraum 1. 1.–31. 12. 2025

Rang (Veränderung zum Vorjahr)	Getötet (zusätzl. verschwunden oder entführt)	Inhaftiert (davon inzwischen frei)
Ukraine 55 (+7)	3 (0)	-
Sierra Leone 79 (-23)	1 (0)	-
Israel 116 (-4)	-	26 (6)
Mexiko 122 (+2)	9 (29)	-
Ecuador 125 (-31)	3 (0)	-
Hongkong 140 (0)	-	6 (4)
Syrien 141 (+36)	0 (45)	2 (0)
Peru 144 (-14)	4 (2)	-
Bangladesch 152 (-3)	2 (1)	8 (3)
Paläst. Gebiete 156 (+7)	25 (2)	-
Indien 157 (-6)	1 (1)	7 (5)
Sudan 161 (-5)	2 (1)	3 (0)
Türkei 163 (-4)	-	27 (26)
Belarus 165 (+1)	-	46 (20)
Myanmar 166 (+3)	-	59 (9)
Russland 172 (-1)	-	59 (11)
Vietnam 174 (-1)	-	30 (3)
Afghanistan 175 (0)	0 (1)	25 (0)
Iran 177 (-1)	-	18 (6)
China 178 (0)	-	115 (2)

Weltweit 60 (148) 667 (224)

Quelle: Reporter ohne Grenzen (Rangliste/Barometer), Stand: 28. 4. 2026 taz grafik: planet-neun.de | L.N.

bung ist, liegt damit weiter bei privaten Digitalkonzernen. Während Google und Meta einen immer größeren Anteil des Werbemarktes für sich beanspruchen, verlieren Medien immer mehr an Seitenaufrufen und stehen unter wachsendem wirtschaftlichem Druck. Die Medienvielfalt und der Zugang zu vertrauenswürdiger Information geraten zunehmend in Bedrängnis. Mit der Einführung von KI-Anwendungen in der Suchmaschine hat sich diese Abhängigkeit verschärft. Das Kernproblem, dass privatwirtschaftliche Unternehmen über die informelle Grundversorgung der digitalen Öffentlichkeit bestimmen, bleibt ungelöst.

Politisch relevante Inhalte und Meinungsäußerungen, die im redaktionellen Kontext geäußert werden und unbezahlt sind, werden nicht erfasst. Erst wenn Medienhäuser politische Inhalte gegen Bezahlung in ihren Publikationen veröffentlichen, agieren sie laut der Gesetz-

gebung als Herausgeber und unterliegen den Bestimmungen der Verordnung.

Die Kritik der Plattformen ist jedoch nicht aus der Luft gegriffen. Es gibt Umsetzungsprobleme und Rechtsunsicherheiten durch die sehr weitreichenden Definitionen des Begriffs „politische Werbung“. So könnte es zur Überregulierung politischer Äußerungen durch einen breit gefassten Begriff kommen. Akteure, die Werbung schalten wollen, könnten aus Sorge vor Sanktionen im Vorfeld von einer womöglich politischen Werbung Abstand nehmen. Es braucht eine differenzierte Definition, um den verschiedenen Formen politischer Werbung im digitalen Raum gerecht zu werden.

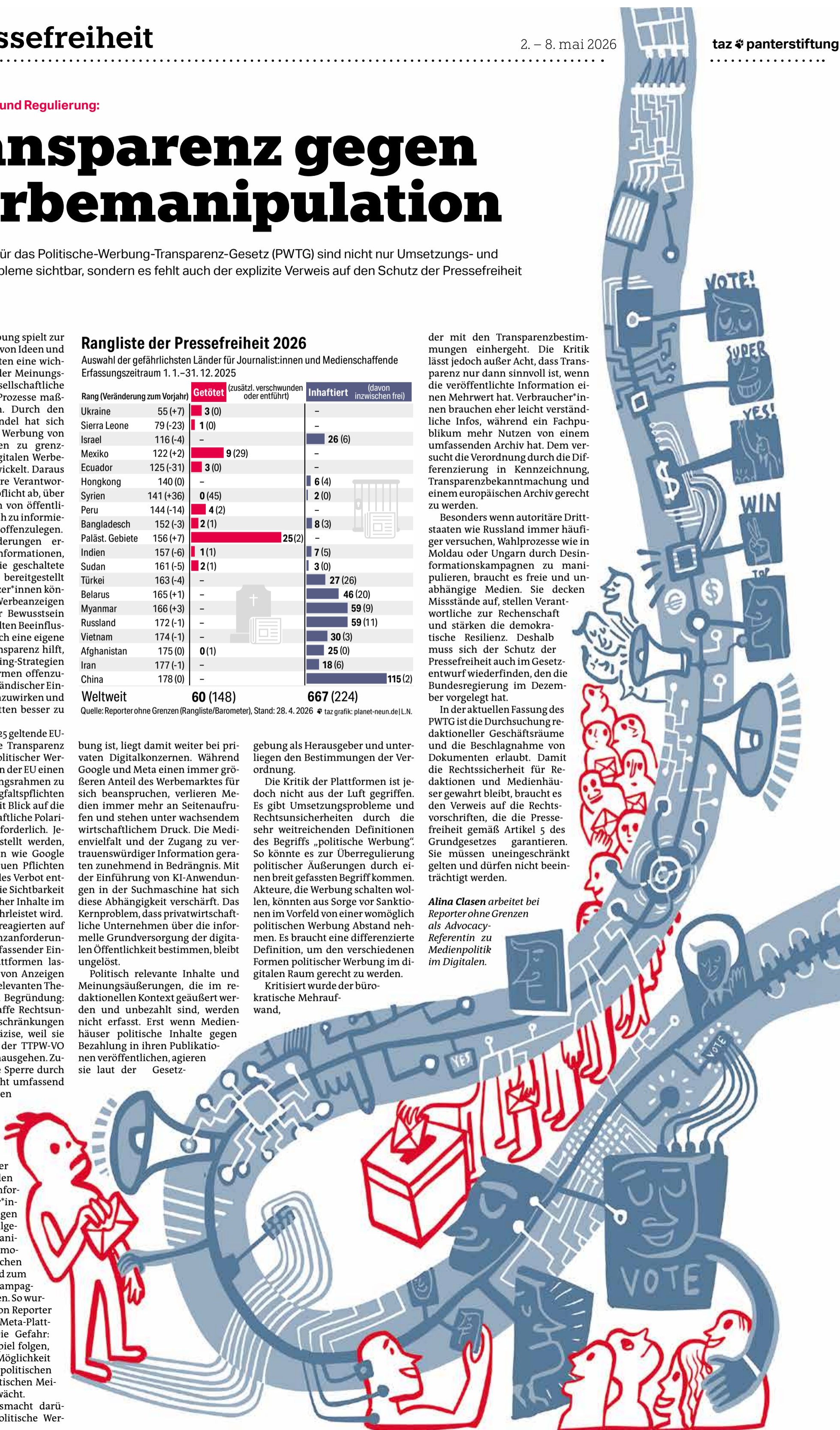
Kritisiert wurde der bürokratische Mehraufwand,

der mit den Transparenzbestimmungen einhergeht. Die Kritik lässt jedoch außer Acht, dass Transparenz nur dann sinnvoll ist, wenn die veröffentlichte Information einen Mehrwert hat. Verbraucher\*innen brauchen eher leicht verständliche Infos, während ein Fachpublikum mehr Nutzen von einem umfassenden Archiv hat. Dem versucht die Verordnung durch die Differenzierung in Kennzeichnung, Transparenzbekanntmachung und einem europäischen Archiv gerecht zu werden.

Besonders wenn autoritäre Drittstaaten wie Russland immer häufiger versuchen, Wahlprozesse wie in Moldau oder Ungarn durch Desinformationskampagnen zu manipulieren, braucht es freie und unabhängige Medien. Sie decken Missstände auf, stellen Verantwortliche zur Rechenschaft und stärken die demokratische Resilienz. Deshalb muss sich der Schutz der Pressefreiheit auch im Entwurf wiederfinden, den die Bundesregierung im Dezember vorgelegt hat.

In der aktuellen Fassung des PWTG ist die Durchsuchung redaktioneller Geschäftsräume und die Beschlagnahme von Dokumenten erlaubt. Damit die Rechtssicherheit für Redaktionen und Medienhäuser gewahrt bleibt, braucht es den Verweis auf die Rechtsvorschriften, die die Pressefreiheit gemäß Artikel 5 des Grundgesetzes garantieren. Sie müssen uneingeschränkt gelten und dürfen nicht beeinträchtigt werden.

Alina Clasen arbeitet bei Reporter ohne Grenzen als Advocacy-Referentin zu Medienpolitik im Digitalen.



## Mit künstlich erzeugter Pornografie gegen journalistische Integrität

Mit sexualisierten Deepfakes wird versucht, kritische Journalist\*innen mundtot zu machen. Betroffen sind vor allem Frauen

Von Noelia Sanchez Barón

Julia Mengolini hat im Juli 2025 den argentinischen Präsidenten angezeigt. Javier Milei soll ein pornografisches Deepfake von ihr auf X verbreitet haben. Auslöser war eine satirische Bemerkung: Die Journalistin hatte in einer Comedy-Show geäußert, Milei sei „in love“ mit seiner Schwester Karina, der derzeitigen Generalsekretärin der Präsidentschaft. Daraus entwickelte sich eine Hetzkampagne gegen Mengolini. Online-Trolle verbreiteten ein manipuliertes Video, in dem sie mit ihrem eigenen Bruder beim Geschlechtsverkehr zu sehen gewesen sein soll. Milei, der im Mai 2025 öffentlich erklärte, man hasse Journalist:innen „nicht genug“, soll die Kampagne verstärkt haben und ihr laut Berichten an einem einzigen Wochenende 93 Tweets gewidmet haben.

Mengolini ist eine von 100 Journalist:innen aus 27 Ländern, die aufgrund ihrer Arbeit Opfer von Deepfake-Kampagnen wurden. Laut Reporter ohne Grenzen (RSF) waren in 74 Prozent der zwischen 2023 und 2025 analysierten Fälle Frauen betroffen. Ihre Stimmen wurden geklont, um falsche politische Statements oder Desinformation zu verbreiten – oder, noch schlimmer: ihr Körper wurde in pornografischen Deepfakes digital missbraucht. Wie leicht sich solche Inhalte erstellen lassen, zeigt die Debatte über Grok – den Chatbot von Elon Musk oder wie die *Washington Post* titelte: den „Porn-Generator“. In Sekunden konnten Nutzer auf X Bilder generieren, in denen Frauen mit wenig Kleidung oder nackt zu sehen waren. Inzwischen ermittelt die EU-Kommission.

Welche Reichweite haben sexualisierte Deepfakes von Journalistinnen in Deutschland? Dazu antwortet Reporter ohne Grenzen, dass sich seit November 2023 deshalb niemand hilfesuchend an die Organisation gewandt habe: „Das sagt jedoch nicht unbedingt etwas über das Volumen des Problems aus: Auch bei Diffamierungen, Shitstorms und Hasswellen aus dem Netz wenden sich Journalist\*innen häufig erst im absoluten Extremfall an RSF oder andere Institutionen wie die Gewerkschaften.“

Judith Strieder von HateAid, die als Psychologin Betroffene nach Deepfake-Angriffen berät, sagte gegenüber der taz: „Die größte Angst, die Betroffene haben, ist die, dass sie nicht ernst genommen werden.“ Viele seien bereit, Anzeige zu erstatten. Auch Journalistinnen suchen dort Hilfe. Wichtig sei: Die Arbeit hinter der Kamera schützt nicht. Es reicht ein Profilbild, das heruntergeladen und manipuliert werden kann. Manipulierte Inhalte im Journalismus sind gefährlich und politisch relevant. „Deepfakes können gezielt genutzt werden, um Frauen aus dem öffentlichen Diskurs zu drängen.“ So wie es bei Mengolini der Fall ist. Will sich eine Frau dagegen wehren, stößt sie in Deutschland auf Hürden. Strieder betont: „Ich glaube, eine große Sorge ist, dass die Erfahrung, Konsequenzen zu spüren, auf der Seite der Betroffenen bleibt, vor allem psychische Konsequenzen, aber auch soziale Folgen, und dass der Täter unbeschadet davon kommt.“

In Deutschland gibt es bisher keinen klaren eigenen Straftatbestand für Deepfakes. Doch im April legte Justizministerin Stefanie Hubig einen Gesetzentwurf gegen digitale Gewalt vor: Nicht nur das Verbreiten, auch das Erstellen pornografischer KI-Inhalte soll strafbar werden. Betroffene sollen mehr Rechte erhalten. So könnten sie etwa Account-Sperren von Deepfake-Urhebern gerichtlich erwirken. In Frankreich gilt seit 2024: Wer sexualisierte Inhalte einer Person nicht einvernehmlich verbreitet, kann zu bis zu zwei Jahren Haft und einer Geldstrafe verurteilt werden. Das ist laut aktuellem Gesetzentwurf auch in Deutschland vorgesehen. Eine Klarnamenpflicht, um Täter leichter aufspüren zu können, jedoch nicht.

Noelia Sanchez Barón ist freie Journalistin, Moderation und Social-Video-Reporterin in Berlin. 2024 war sie mit dem Daniel-Haufler-Stipendium der taz panterstiftung in den USA.

Fake News und Manipulation

## Effektive Meme-Warfare

Im Krieg macht jetzt auch KI staatliche Propaganda, wobei Memes ihn als kalkulierte Kommunikationsinstrumente zu einer scheinbar harmlosen Unterhaltung machen

Von Katja Muñoz

Wer in den letzten Monaten soziale Medien genutzt hat, ist künstlich generierten Lego-Animationen über Militärschläge begegnet, die wie harmlose Internetkultur wirken, aber dennoch Millionen erreichen. Dahinter stecken jedoch keine Teenager, sondern Staaten.

Künstliche Intelligenz (KI) verändert nicht nur, was kommuniziert wird, sondern auch, wie politische Realität wahrgenommen wird. KI ist ein Werkzeug zur Inhaltserstellung und bestimmt über Plattformalgorithmen, welche Informationen Menschen erhalten, wie sie diese verarbeiten und bewerten. Diese Entwicklung vollzieht sich nicht nur in Wahlkämpfen oder auf den Konten anonymer Trolle. Sie findet heute auf den offiziellen Kanälen von Staaten statt, mitten im Krieg, in Echtzeit und mit millionenfacher Reichweite.

Im Kontext des Krieges mit Iran kann man sehen, wie alle Kriegsparteien damit begonnen haben, KI-generierte Inhalte als Teil ihrer offiziellen Kommunikation einzusetzen. Im Vordergrund stehen dabei Memes, also Medieninhalte, die sich vorrangig im Internet verbreiten und oft humorvoll oder satirisch sind.

Der Iran nutzt unter anderem Lego-Animationen, sogenannten KI-Slop, der minderwertige, massenhaft KI-erzeugte Inhalte ohne Mehrwert darstellt. Die USA teilen SpongeBob- und Iron-Man-Memes, um geopolitische Eskalationen zu kommentieren. Memes sind dabei keine Randerscheinung mehr, sondern ein kalkuliertes Kommunikationsinstrument.

Das Kalkül dahinter ist einfach: Ein Lego-Format löst keine Abwehrreflexe aus. Eine Animation wirkt nicht wie eine Pressemitteilung des Außenministeriums. Genau das ist der Punkt. Die Flachheit dieser Inhalte ist das Prinzip. Inhalte, die unterhaltsam genug sind, um jeden kognitiven Widerstand zu umgehen, erreichen Zielgruppen, die klassische staatliche Kommunikation längst weggeklückt hätten.

Hinzu kommt ein Effekt, dessen politische Wirkung unterschätzt wird: Schadenfreude. Niemand, der den westlichen Diskurs beobachtet, steht hinter dem iranischen Regime. Und dennoch schauen viele gebannt auf iranische Meme-Propagandavideos, die die USA effektiv vorführen und ins Lächerliche ziehen. Man lacht, teilt und kommentiert. Dabei wird man unfreiwillig zum Multiplikator einer staatlichen Botschaft.

Was diese Inhalte so wirksam macht, ist nicht nur ihre Form, sondern auch ihre Verbreitung. Soziale Medien fungieren dabei als globaler Distributionsvektor. Offizielle Kanäle stellen die Inhalte bereit, doch die eigentliche Reichweite entsteht durch Millionen von Reshares, Reaktionsvideos und Kommentaren.

Besonders wirkungsmächtig sind dabei kurze Clips, da sie plattformübergreifend funktionieren, ohne Kontext konsumiert werden können und sich innerhalb von Stunden viral verbreiten. Dadurch können potenziell auch jene erreicht werden, die sich stark mit solchen Themen beschäftigen.

Ein außenpolitischer Referent, der sich tagsüber intensiv mit diplomatischen Ana-

lysen beschäftigt, stößt abends privat auf die iranischen Lego-Videos. Am nächsten Morgen sind die Memes noch in seinem Kopf, und zwar mindestens genauso präsent wie das tagespolitische Geschäft. Wer glaubt, professionelle Distanz schützt vor dieser Form der Beeinflussung, unterschätzt, wie tief sich unterhaltsame Inhalte ins menschliche Gedächtnis einschreiben.

Sprechen wir hier über Meme-Warfare? Oder über klassische Propaganda? Uns fehlen noch die richtigen Begriffe, um bestehende Konzepte anzupassen. Wann ist koordinierte staatliche Kommunikation eine Einflusskampagne und wann ist sie legitime Außenpolitik? Die alten Kriterien greifen nicht mehr, wenn Propaganda wie ein Meme aussieht und ein Meme wie Propaganda wirkt.

Was bleibt, ist eine dringende Aufgabe. Medienkompetenz im klassischen Sinne, Fakten prüfen, Quellen hinterfragen, greift hier zu kurz. Wer die Echtheit eines Lego-Clips prüft, verpasst die eigentliche Frage. Was wir brauchen, ist die Fähigkeit zu erkennen, wann Unterhaltung als Überzeugung arbeitet, bevor wir bereits mitgelacht haben.

Katja Muñoz forscht bei der Deutschen Gesellschaft für Auswärtige Politik (DGAP) in Berlin zu sozialen Medien, KI, Demokratie und Sicherheit.



Überwachung und digitale Sicherheit

# Wie Peking alles unter Kontrolle hat

Chinas Zensurapparat ist aufgrund des technologischen Wandels so umfangreich wie in keinem anderen Land

Von Fabian Kretschmer

Zur belebten Mittagsstunde, als die Verkäufer am Dahanji-Markt im Südwesten Pekings ihre Waren anpreisen, rast ein gelber Bulldozer mit voller Geschwindigkeit in eine Menschenmenge. Er hinterlässt eine Spur der Verwüstung, Dutzende Passanten bleiben regungslos auf dem Asphalt liegen.

Das mutmaßliche Attentat mit etlichen Toten würde in den meisten Staaten der Welt auf den Titelseiten der Zeitungen stehen. In China hingegen findet das Ereignis vom 29. März keine Erwähnung: In den sozialen Medien wurden dazu sämtliche Videoaufnahmen gelöscht, den unter staatlicher Kontrolle stehenden Verlagen ein Maulkorb verpasst. Dass die Außenwelt überhaupt von der Tragödie erfährt, ist dem Aktivismus aufmerksamer Auslandschinesen zu verdanken: Schnell haben sie die Smartphone-Aufnahmen von Augenzeugen des Dahanji-Marktes mitgeschnitten und auf der westlichen Plattform X hochgeladen. Darauf hat Chinas Zensurapparat keinen Zugriff.

Beispiele wie dieses zeigen jedoch eindrücklich, dass die Informationskontrolle des chinesischen Staats zumindest innerhalb der eigenen Landesgrenzen nahezu umfassend ist. Dabei gelingt es der Parteiführung nicht nur, Terroranschläge oder politische Demonstrationen aus dem kollektiven Gedächtnis zu löschen, sondern auch zentrale

Kapitel der modernen Geschichte des Landes. Von der blutig unterdrückten Demokratiebewegung des Jahres 1989 vom Pekingener Tiananmen-Platz weiß kaum ein Jugendlicher in China. Woher auch? Wer auf Baidu Baike, dem chinesischen Wikipedia-Äquivalent, danach sucht, erhält keine Resultate. Und wer den Chatbot DeepSeek nach den Ereignissen von damals befragt, wird von der KI aufgefordert, das Thema zu wechseln.

Möglich geworden ist die Effizienz der Zensur nicht trotz, sondern dank der technologischen Möglichkeiten, insbesondere von künstlicher Intelligenz. In den alten Tagen der Internetzensur, als diese noch rein durch menschliche Hände ausgeführt wurde, bereitete allein die schiere Datenflut den Zensoren riesige Probleme. Neben dem immensen Arbeitsaufwand gab es auch praktische Herausforderungen: Livestreams in Minderheitensprachen wie etwa Uigurisch oder Tibetisch konnten schlechter überwacht werden, weil den Behörden die Sprachkompetenz fehlte. Dies resultierte nicht selten in Vorschlaghammermethoden – dass etwa Liveübertragungen zu bestimmten Themen nur in Mandarin, dem weitverbreiteten Hochchinesisch, stattfinden durften.

Hinzu kam, dass die meist jungen, äußerst cleveren Internetnutzer im Reich der Mitte ihre Zensoren

mit einer gehörigen Portion Kreativität überlisten konnten. Ein klassisches, schon etliche Jahre altes Beispiel: Da das Datum des Tiananmen-Massakers – der 4. Juni – im öffentlichen Raum nicht erwähnt werden darf, sprach man vom „35. Mai“.

Eine andere Methode: Kritische Beiträge wurden auf den Online-Plattformen Wechat oder Weibo nicht mehr als Textbeitrag gepostet, sondern als spiegelverkehrter Screenshot. Zuletzt wurden zu sensiblen Themen nur mehr Kerzen-Emojis gepostet, die klarmachen, dass man über gewisse Repressionen trauert, aber seine Gefühle wegen der Zensur nicht in Worte kleiden darf. Die größte politische Demonstrationbewegung in China der letzten Jahre – online sowie analog – spielte genau darauf an: Die „Weißblattproteste“, mit denen Ende 2022 junge ChinesInnen gegen die rigiden Null-Covid-Maßnahmen revoltierten, trugen das Symbol der inneren Selbstzensur bereits im Namen: ein leeres Blatt Papier. Doch natürlich haben selbst die raffiniertesten Codes, Anspielungen und Tricks nur eine geringe Haltbarkeitsdauer. Denn irgendwann kommen die Zensoren dahinter.

Mittlerweile sitzen die Autoritäten beim Katz-und-Maus-Spiel um Informationskontrolle am längeren Hebel. Denn Internetnutzer müssen längst nicht mehr geschulte Bürokraten überlisten, sondern auch eine technisch überlegene KI-Software. Sie kann riesigste Datenmengen in Sekundenbruchteilen verarbeiten und auch feinste ironische Anspielungen erfassen. Und vor allem ermöglicht die Technologie, dass die Algorithmen der sozialen Medien derart subtil manipuliert werden, dass die meisten Nutzer in einer Propagandawelt leben,

ohne dies zu merken. Die Zensur ist in China gerade deshalb so effizient, weil sie den meisten Leuten im Alltag kaum mehr auffällt.

Zudem nutzt die Parteiführung die technischen Fähigkeiten mehrgleisig aus. Während die Technologie im Inneren dabei hilft, kritische Information zu zensieren, wird sie auf ausländischen Online-Plattformen dafür missbraucht, Desinformation und Propaganda zu verbreiten.

„Wumao“ hat man die klassischen Propagandatrolle genannt, die en masse Parteinhalt auf den sozialen Medien gepostet haben – und dafür, so lautet die ironische Namensbezeichnung, „fünf Groschen“ (chinesisch: *wumao*) erhalten haben. Mittlerweile generiert die künstliche Intelligenz Abertausende Profile in den sozialen Medien, und das ganz ohne Bezahlung. Wer insbesondere bei X über China debattieren möchte, wird unweigerlich unter seinen Beiträgen etliche Antworten finden, von denen die meisten nicht von menschlichen Personen geschrieben wurden.

Fabian Kretschmer ist Ostasienkorrespondent der taz und anderer Medien mit Sitz in Seoul.



## Europäische Gesichtserkennung für brasilianische Schulkinder

Eine slowakische Software scannt täglich Hunderttausende Kinder in Paraná. In Europa sind solche Systeme kaum denkbar – exportiert werden sie trotzdem problemlos

Von Nico Schmidt und Leonardo Coelho

Der Unterricht an 1.700 Schulen im südbrasilianischen Bundesstaat Paraná beginnt mit einem Ritual: Die Lehrkraft öffnet eine App, fotografiert das Klassenzimmer, und in Sekunden gleicht ein Algorithmus die Gesichter mit einer biometrischen Datenbank ab. Wer erkannt wird, gilt als anwesend. Seit 2023 ist diese Gesichtserkennung in Paraná im Einsatz, um täglich fast eine Million Kinder zu identifizieren. Doch das System irrt. Eine Lehrerin erzählt von einer Schülerin, die im Unterricht war, sich aber in der App als abwesend fand. „Ich markiere sie nicht als abwesend“, habe der Lehrer gesagt. „Das macht die Kamera.“ Für manche Familien ist so ein Fehler fatal. Denn die Sozialleistung Bolsa Família hängt vom Schulbesuch der Kinder ab. In Paraná werden diese Daten weitgehend von einem Algorithmus erzeugt.

Entwickelt wurde die Software von dem slowakischen Unternehmen Innovatrics. Das kann eine Recherche von Investigate Europe zeigen, die in Deutschland exklusiv in der taz erscheint. In der EU wäre ein vergleichbarer Einsatz hochproblematisch. Schwedens Datenschutzbehörde verhängte 2019 ein Bußgeld gegen eine Schule, die 22 Schüler:innen per Gesichtserkennung erfasst hatte. Die Begründung: Kinder könnten der biometrischen Überwachung nicht frei zustimmen, weil das Machtgefälle zu groß sei. Im französischen Marseille stoppte ein Gericht im Jahr 2020 zwei Pilotprojekte an Schulen aus ähnlichen Gründen.

Die EU hat mit der DSGVO und dem KI-Gesetz von 2024 Gesichtserkennung streng reguliert, aber nicht grundsätzlich verboten. Der Export der Technologie in Drittstaaten ist nicht beschränkt. Das Europäische Parlament hatte ein Ausfuhrverbot für in der EU als „inakzeptabel“ eingestufte Systeme gefordert, konnte sich aber nicht durchsetzen. Caitlin Bishop von Privacy International verweist darauf, dass Brasiliens Datenschutzgesetz dem europäischen ähnelt: „Aber bei der Durchsetzung gibt es ein riesiges Problem.“ Die zuständige Behörde verhängt Sanktionen erst seit 2023.

In Paraná trieb der frühere Bildungsminister Renato Feder, zuvor Tech-Unternehmer, die Digitalisierung der Schulen voran. 2022 un-

terzeichnete die staatliche IT-Firma Celepar einen Vertrag mit dem brasilianischen Dienstleister Valid, der Innovatrics ins Boot holte. Innovatrics wirbt mit 80 Prozent Zeitersparnis beim Aufruf der Anwesenheitsliste und dass Eltern stets den Status ihres Kindes einsehen können. Das Unternehmen erhielt 2018 und 2019 rund 200.000 Euro EU-Forschungsgelder für biometrische Bildanalyse.

Eine Studie ergab 2025 eine Trefferquote von 91,1 Prozent, weniger als die vertraglich zugesicherten 95 Prozent. Laut einer Umfrage halten acht von zehn Lehrkräften das System für weniger effektiv als den klassischen Namensaufruf. Paraná's Bildungsbehörde erklärt, die Nutzung sei für Lehrkräfte freiwillig, Schüler:innen könnten ohne Nachteile widersprechen, und technische Fehler führten nicht automatisch zum Abwesenheitseintrag. Vor Einführung sei eine Datenschutz-Folgenabschätzung erstellt worden. Die IT-Firma Celepar verweist auf „mehrere Sicherungsebenen“, manuelle Korrekturmöglichkeiten und die ständige Anpassung des Algorithmus.

Bei einer Million erfasster Kinder täglich können auch kleine Feh-

lerquoten Zehntausende betreffen. Zwar ist bisher kein Fall dokumentiert, bei dem eine fälschliche Abwesenheit direkt zum Verlust von Bolsa-Família-Zahlungen geführt hätte. Möglich sei dies aber, warnen Lehrkräfte. Im April 2025 klagte ein Staatsanwalt gegen die Landesregierung, das Urteil steht noch aus. Paraná's Bildungsbehörde erklärte, das System entspreche dem Datenschutzrecht. Inzwischen nutzen 7 von Brasiliens 27 Bundesstaaten Gesichtserkennung an Schulen. 2024 wurde das Paraná-System drei Monate lang an einer Privatschule in Lissabon getestet. Portugals Datenschutzbehörde leitete eine offizielle Untersuchung ein, genutzt werde das System nicht mehr. Innovatrics und Ex-Bildungsminister Feder reagierten nicht auf Anfragen, Valid lehnte eine Stellungnahme ab.

Dieser Beitrag entstand in Kooperation mit dem AI Accountability Network des Pulitzer Center.

Nico Schmidt ist Journalist bei Investigate Europe in Berlin. Leonardo Coelho ist freier Journalist in Brasilien.





Schutz von Journalisten durch KI

# Reale Infos von virtuellen Sprechern

In Venezuela überlebt der Journalismus Zensur und Repression mithilfe von Kooperationen, technologischer Innovation und der Unterstützung aus dem Exil

Von **Ronna Rísquez** und **Gabriela Ramírez**

Um 1:50 Uhr morgens waren erste Schüsse zu hören, berichtete Jonathan Gutiérrez, Mitbegründer des Digitalmediums *Historias que Laten*, das zusammen mit *Efecto Cocuyo*, *Caracas Chronicles*, *Cazadores de Fake News*, *El Pitazo*, *Tal Cual* und *Runrunes* an der Übertragung teilnahm, wobei Letztere Teil der redaktionellen Koalition *Alianza Rebelde Investiga* sind. „Unter Zeitdruck starteten wir einen Livestream auf YouTube. Aus Sicherheitsgründen standen drei Kollegen aus der venezolanischen Diaspora vor der Kamera, während drei Redakteure im Hintergrund von Caracas aus die lokalen Produzenten waren. Wir berichteten live von den Ereignissen, die wir aus den Fenstern unserer Wohnungen beobachten konnten, überprüften Informationen und sendeten Berichte in Echtzeit. Durch diesen Stream erfuhren die Venezolaner und die Welt, dass Nicolás Maduro vom US-Militär auf Befehl von Donald Trump festgenommen und aus Venezuela herausgebracht wurde“, sagte Gutiérrez der taz panterstiftung. „Die Notwendigkeit zu berichten hat uns in diesem historischen Moment vereint. Die journalistische Berichterstattung war innovativ und beispiellos.“

Die Übertragung erhielt den Namen „La Conversa con La Luz“ (Gespräch mit dem Licht) – die wöchentlichen Talkshows von *Alianza Rebelde Investiga* und *Efecto Cocuyo* –, die über Streamyard ausgestrahlt werden. Doch war es nicht das erste Mal, dass sich Journalisten aus Venezuela zusammenschlossen, um in einem von Zensur geprägten Umfeld weiterhin zu berichten. Vielmehr waren kollaborativer Journalismus und die Kooperation mit Journalisten im Exil entscheidend für das Überleben der Medien im Land.

Im Jahr 2024, nachdem Maduro das Ergebnis der Präsidentschaftswahlen vom 28. Juli nicht anerkannt hatte, schlossen sich 13 venezolanische Medienplattformen unter der Koordination der Organisation *Connectas* zusammen, um weiterzuberichten. Sie gründeten die *Allianz La Hora de Venezuela* mit dem Ziel, im In- und Ausland über die Nichtanerkennung des Wahlergebnisses sowie die Repression zu berichten und die Sicherheit der Journalisten zu stärken.

Als die Regierung Maduro im August 2024 Journalisten festnahm und ausländische Korrespondenten auswies, schuf ein venezolanisches Medienkollektiv mit künstlicher Intelligenz zwei Nachrichtensprecher, genannt „La Chama“ (Junge Frau) und „El Pana“ (Der Kumpel). Immer gleichgeklei-

det, mit leicht roboterhaften Bewegungen, aber mit venezolanischem Akzent verkündeten beide Avatare unverblümt: „Wir sind nicht real. Wir wurden durch künstliche Intelligenz generiert, aber unsere Inhalte sind echt, verifiziert, qualitativ hochwertig und von Journalisten erstellt.“ Jede Folge von „La Chama y El Pana“ dauert etwa drei Minuten, speziell für die Verbreitung über WhatsApp konzipiert, einem der wichtigsten Informationskanäle für Venezolaner in Zeiten der Zensur.

Das Projekt *Operación Retuit* wurde von der Plattform *Connectas* zusammen mit einem Dutzend venezolanischer Medien gestartet, die sich in den Bündnissen *Venezuela Vota* und *La Hora de Venezuela* zusammengeschlossen haben. „Es ist eine gemeinschaftliche Initiative, die die Ressourcen zahlreicher Teilnehmer bündelt und die Arbeit von mehr als 100 Kollegen verstärkt. Künstliche Intelligenz wird genutzt, um Zensur und Unterdrückung zu umgehen – nicht als Modeerscheinung, sondern als Notwendigkeit im Kontext zunehmender Repression“, sagt César Batiz, Direktor des unabhängigen Medienunternehmens *El Pitazo*, in einem Interview mit TN.

Während die Avatare digital agierten, leistete eine andere Initiative physischen Widerstand: *El Bus TV*. Das Projekt entstand 2017 während heftiger landesweiter Proteste, bei denen mehr als 100 Menschen durch die Repression der Polizei ums Leben kamen.

Ursprünglich war der Schwerpunkt, Fahrgästen des öffentlichen Nahverkehrs journalistische Informationen offline zu vermitteln. In den inzwischen fast zehn Jahren seines Bestehens hat sich das Medium in mindestens 10 der 28 Bundesstaaten Venezuelas mit einem Face-to-Face-Modell etabliert, das vor allem eine lokale, dienstleistungsorientierte redaktionelle Linie verfolgt.

In diesem Sinne „gewinnt der persönliche

Kontakt einen Wert des Widerstands, einen symbolischen Wert, einen Wert der Rückkehr zum Realen“, sagt Laura Helena Castillo, Direktorin und Mitbegründerin von *El Bus TV*. Darüber hinaus kann dieses Modell auch zur Medien- und Demokratiekompetenz beitragen, insbesondere in der jetzigen Situation des Landes, in der die Möglichkeit eines demokratischen Übergangs besteht: „Wir haben Orte, an denen Debatten, Gespräche und Begegnungen gefördert werden.“

Hinter den sichtbarsten Initiativen verbergen sich alltägliche Praktiken, die den venezolanischen Journalismus der letzten Jahre prägen. Die Journalisten löschen WhatsApp-Unterhaltungen nach jedem sensiblen Austausch, speichern die Namen ihrer Quellen unter zufälligen Pseudonymen in ihren Kontaktlisten und verlagern ihre Kommunikation auf Signal mit programmierten Selbstzerstörungsnachrichten.

Eine weitere Sicherheitsmaßnahme sind Veröffentlichungen ohne Namensnennung oder unter kollektiven Signaturen. Angesichts der schrecklichen und zunehmenden Verfolgung nach den Wahlen war dies der logischste Schritt. „Den Autorennamen wegzulassen bedeutet, sich seiner Identität zu berauben. Die Repression hat uns unsichtbar gemacht. Der Stolz unseres Namens wurde uns genommen; selbst das nimmt dir die Regierung weg“, kommentierte eine Journalistin.

**Ronna Rísquez** ist preisgekrönte Investigativjournalistin aus Caracas und war 2024 mit dem *Rest & Resilience Fellowship* der *taz panterstiftung* und von *Reporter ohne Grenzen* in Berlin.

**Gabriela Ramírez** ist preisgekrönte venezolanische Multimediajournalistin und Redakteurin bei *Unbias the News/Hostwriter* in Berlin.

In den frühen Morgenstunden des 3. Januar 2026 wurden die Venezolaner durch Explosionen geweckt. Während US-Militärs strategische Orte in Venezuela bombardierten und Präsident Nicolás Maduro und seine Frau gefangen nahmen, suchten verängstigte Venezolaner in den sozialen Netzwerken nach Informationen darüber, was gerade geschah. Journalisten im Inland und im Exil bekamen verzweifelte Anrufe von Familienangehörigen, Freunden und Kollegen. Doch es gab keine Informationen. Unsicherheit und Angst beherrschten die Lage.

In Venezuela sind in den letzten 20 Jahren mehr als 400 Medien geschlossen worden, und auf Anordnung der autoritären Regierung von Maduro wurde der Zugang zu weiteren 43 unabhängigen Medien und digitalen Nachrichtenplattformen gesperrt. Zu Jahresbeginn saßen rund 20 Journalisten wegen der Ausübung ihres Berufes in Haft.

Innerhalb kürzester Zeit beschloss eine Gruppe von sechs im Exil lebenden Journalisten zusammen mit fünf weiteren, die in Venezuela geblieben waren, einen Livestream zu starten, um über die Geschehnisse zu berichten und der offiziellen Zensur entgegenzuwirken. Über mehr als zehn Stunden berichteten sie ununterbrochen über die Ereignisse.

Transnationale  
Repression

# Wie Hanoi gegen Trung Khoa Lê in Berlin vorgeht

Der von Berlin aus publizierende deutsch-vietnamesische Chefredakteur von Thoibao.de muss sich ständig gegen Angriffe der Regierung in Hanoi und ihrer dortigen wie hiesigen Handlanger wehren. Ein Tagebuch

Von Marina Mai

**Dezember 2017** Zur „Reinigung des Internets von feindlichen Inhalten“ stockt Vietnams Regierung das Militär um 10.000 sogenannte Cybersoldaten auf. Unter fadenscheinigen Vorwänden werden erstmals Facebookposts von Thoibao gelöscht.

**Januar 2018** Lês Auftritt bei einem taz-Talk wird mit einem Stinkbombenanschlag bedroht, die Polizei schützt die Veranstaltung.

**Von Mai 2018 bis heute** ist Thoibao.de immer wieder massiven Hackerangriffen ausgesetzt. Wegen DDoS-Angriffen muss die Webseite öfter wochenlang vom Netz genommen werden. Das Bundeskriminalamt ordnet die Angriffe staatlichen Quellen zu. Lê stärkt seine IT-Sicherheit.

**April bis Juli 2018** Lê berichtet von dem Prozess gegen einen Entführungshelfer von Trinh Xuân Thanh vor Berlins Kammergericht und erreicht in Vietnam ein Millionenpublikum. Berlins Landeskriminalamt (LKA) erhält einen anonymen Hinweis mutmaßlich aus dem Umfeld von Vietnams Botschaft über eine geplante Tötung Lês mittels Vergiftung oder eines fingierten Verkehrsunfalls. Das LKA stellt Lê unter Personenschutz (bis heute).

**September 2018** Facebook löscht ohne Vorwarnung Lês Facebookseiten wegen „Verstoßes gegen Community-Standards“. Reporter ohne Grenzen schaltet sich ein. Später räumt Facebook ein, dass Lê ohne sein Wissen von Unbekannten zum Administrator einer Facebookseite gemacht worden war, die massiv Community-Standards verletzte. Als Konsequenz aus dem Fall schließt Facebook weltweit diese Sicherheitslücke. Erst im Dezember 2018 kann Lê seine Facebookseiten wieder nutzen.

**2019 bis heute** Vietnamesische Firmen beanspruchen gegenüber Facebook und YouTube Urheberrechte für Medieninhalte von Thoibao.de. Meist haben sie diese selbst von Thoibao.de auf ihre eigenen Seiten kopiert und vordatiert. Facebook und YouTube verwarnten Thoibao.de wegen Urheberrechtsverletzung Dritter. Die finanzielle Beteiligung, die Thoibao.de an Facebooks Werbeeinnahmen wegen der sehr hohen Zugriffsrate auf die Thoibao-Seiten dort erhält, wird öfter an diese Firmen umgeleitet.

**2019/2020 bis heute** Immer wieder löschen Facebook und YouTube Videos von Lê, weil er bei Abbildung hoher Funktionäre angeblich deren Persönlichkeitsrechte verletzt. Nach deutschem Recht müssen Personen des öffentlichen Lebens eine Berichterstattung über sich hinnehmen, anders als Privatpersonen. In Vietnam ist das nicht geregelt.

**Juli 2020 bis 2024** Vietnams Botschaft besteht darauf, dass Lê zur Verlängerung seines Reisepasses persönlich erscheint. Das LKA rät ihm aus Sicherheitsgründen ab. In seinem deutschen Einbürgerungsverfahren verweigert ihm die Botschaft später das Ablegen der vietnamesischen Staatsangehörigkeit.

**Januar 2021** Der Bayerische Rundfunk und die *Zeit* decken auf, dass die in Kontakt mit Vietnams Regierung stehende Hackergruppe Ocean Lotus Spionagesoftware auf Computern vietnamesischer Menschenrechtsverteidiger und deutscher Firmen installiert und dies auch bei einer Mitarbeiterin von Thoibao.de in Deutschland versucht hat.

**Mai 2021** Auf Facebook erscheint eine Todesanzeige für Lê, woraufhin Facebook seine Konten und die von Thoibao.de löscht. Auf Lês Widerspruch reagiert Facebook nur langsam.

**November 2021** Die Facebookseiten von Thoibao.de und vietnamesischsprachigen Medien in den USA und Großbritannien werden von einem in Hanoi ansässigen Mann gekapert, hinter dem Vietnams Geheimdienst vermutet wird. Thoibao.de hat keinen Zugriff mehr auf seine Seiten, der Unbekannte publiziert jetzt dort und hat Zugriff auf alle Nachrichten von Informanten und Lesern. Meta korrigiert erst nach knapp zwei Wochen den Zugriff.

**Anfang 2022** Der vietnamesische Unternehmerverband in Deutschland stellt seine Arbeit ein. Lê war 2019 in dessen Vorstand gewählt worden, doch andere Vorstandsmitglieder verweigerten die Zusammenarbeit. Einige räumten Lê gegenüber ein, auf Druck der vietnamesischen Botschaft zu handeln. Eine Neuwahl des Vorstands scheitert bis heute.

**Oktober 2023** Amnesty International und das Mediennetzwerk European Investigative Collaborations decken einen nur zufällig gescheiterten Versuch auf, bei Thoibao.de die Spionagesoftware Predator zu installieren.

**Januar 2024 bis heute** Meta löscht die Facebookseite Thoibao.news, eine von fünf Facebookseiten des Mediums. Lês Beschwerden bleiben unbeantwortet. Zu Reporter ohne Grenzen sagte Meta im Mai 2024 zu, die Seite wiederherzustellen, was bis heute nicht erfolgt ist. Eine 2025 eingereichte Beschwerde bei der Bundesnetzagentur ist bisher ohne Ergebnis.

**April 2024** Unbekannte brechen in Lês im Dong Xuan Center geparktes Auto ein, ohne etwas zu entwenden.

**August 2025** Facebook stellt die Monetarisierung aller Thoibao.de-Kanäle weitgehend ein, sodass das Unternehmen kein Geld mehr für die von Facebook eingestellte Werbung bekommt, um Mitarbeiter zu bezahlen.

**September 2025 bis heute** Vietnams reichster Mann, Phạm Nhật Vượng, und sein Konzern Vingroup mahnen Lê wegen vier Videos ab. Berlins Landgericht weist drei der vier Klagepunkte ab, eine weitere Klage Vungts weist das Gericht ab. Eine dritte Klage von Phạm Nhật Vượng und seinem Autokonzern Vinfest geht im Januar 2026 unentschieden aus. Einen SLAPP-Fall will das Gericht nicht erkennen.

**November/Dezember 2025** Die Staatsanwaltschaft Hanoi klagt Lê und andere wegen ihrer publizistischen Tätigkeit an. Im Internet gibt es Fahndungsfotos und Aufrufe zur Selbstjustiz und Entführung aus Deutschland. Berlins Polizei verstärkt Lês Schutz. Am 31. Dezember wird er in Hanoi in Abwesenheit zu 17 Jahren Haft verurteilt wegen „Herstellung von Informationen, die sich gegen die Sozialistische Republik Vietnam richten“.

**Dezember 2025 bis März 2026:** Meta sperrt auf Verlangen Hanois alle Facebookseiten von Lê in Vietnam. Dort leben 95 Prozent seiner Nutzer.

*Marina Mai ist freie Journalistin unter anderem für die taz und Thoibao.de.*

**Talk „Zensur ohne Grenzen“** der panterstiftung über transnationale Repression in Deutschland und Gegenstrategien mit Hannah Neumann (MdEP), Trung Khoa Lê (Thoibao.de), Leyla Mustafayeva (Qazetci) und Sven Hansen (taz), Montag, 4. Mai, 19 Uhr, taz Kantine und YouTube. Infos: [taz.de/veranstaltungen](https://taz.de/veranstaltungen)





OSINT als Gegenbewegung

# Mit neuer Technologie den Kriegsverbrechen auf der Spur

Im Ukrainekrieg ist der Einsatz von Open Source Intelligence (OSINT) ein investigatives Instrument der Pressefreiheit. Es ermöglicht, Straftäter zu identifizieren, die sich bisher für unantastbar hielten

Aus Kyjiw **Valeriya Yegoshyna**

„Glaubst du, wir können damit etwas anfangen?“, fragte mein Redakteur, nachdem wir einem abgehörten Telefonat gelauscht hatten, das der ukrainische Sicherheitsdienst veröffentlicht hatte. Es war eine dieser schlaflosen Nächte im Frühjahr 2022. Wir saßen in einem Keller und versteckten uns vor Granatenangriffen.

Auf der Aufnahme sagte eine Frauenstimme zu einem Mann: „Na los, vergewaltige ukrainische Frauen. Ich erlaube es. Benutz nur ein Kondom.“ Im März 2025 sagte ich vor Gericht aus. Wir hatten das Paar hinter diesem Telefonat identifizieren können. Die Frau eines russischen Soldaten wurde verurteilt. Wegen des internationalen Haftbefehls hat sich ihre Welt seitdem auf Russland beschränkt. Meine hatte sich erweitert – denn von einem Keller aus konnte ich per Laptop überall hinschauen, wo Satelliten, Telefonaten, soziale Medien und sogar schwache digitale Spuren funktionierten.

Haben Sie je ein Massengrab mit einem Lineal vermessen? Das Foto eines ermordeten Mädchens studiert, das Ihnen ähnelt? Oder versucht, diejenigen zu identifizieren, die Ihren Kollegen getötet haben? Unsere Redaktion wurde nach Ukraines „Revolution der Würde“ 2014 gegründet, um Korruption zu untersuchen – ein Grund der Proteste. Lange vor der großen Invasion nutzten wir schon Open Source Intelligence (OSINT). Die Social-Media-Beiträge der Kinder eines korrupten Beamten aufzuspüren und ihre Urlaubsfotos zu geolokalisieren, konnte unterhaltsam sein. Hunderte Bilder ermordeter Zivilisten zu geolokalisieren überhaupt nicht.

Doch mussten wir wissen, wer genau an der russischen Invasion beteiligt war – samt Namen und Gesicht. Was in den besetzten Gebieten geschah – im Detail. Wie gestohlenes ukrainisches Getreide transportiert wurde – nach Route. Und alles, während wir weiter unsere eigene Regierung zur Rechenschaft zogen. Der Krieg in der Ukraine ist der am besten dokumentierte Krieg der

Geschichte. Diese wird jetzt nicht mehr nur von den Siegern geschrieben. Da Journalisten die sich ständig weiterentwickelnden Werkzeuge beherrschen (die OSINT-Methoden schreiten in atemberaubenden Tempo voran), kann die Führung des Aggressorstaates die Darstellung der Ereignisse nicht mehr völlig steuern.

Im Jahr 2000 hatte Wladimir Putin noch milde gelächelt, als ihn Larry King von CNN auf den Untergang des U-Bootes „Kursk“ ansprach. Doch schließlich waren Russlands Behörden gezwungen, die Katastrophe und den Tod aller 118 Besatzungsmitglieder anzuerkennen, nachdem norwegische Taucher die Luke des Wracks geöffnet und bestätigt hatten, dass es keine Überlebenden gab.

**Von einem Keller aus kann ich per Laptop überall hinschauen, wo Satelliten, Telefondaten, soziale Medien und digitale Spuren funktionieren**

Am 14. April 2022 versenkten ukrainische Neptun-Raketen den Kreuzer „Moskwa“, das Flaggschiff der russischen Schwarzmeerflotte. Das unterbrach Russlands Vorherrschaft im Schwarzen Meer. Moskau leugnete den Vorfall zunächst, dann folgten Behauptungen über eine „vollständige Evakuierung“ der Besatzung. Innerhalb eines Tages bewiesen wir, dass Wehrpflichtige – deren Kriegsteilnahme der Kreml bestritten hatte – auf dem Schiff ums Leben ge-

kommen waren. Keine Insiderinfos. Keine Taucher. Nur Open-Source-Recherche. Schließlich musste Moskau einen Teil der Wahrheit zugeben. Technologie wurde zu einer Säule der Pressefreiheit.

Doch OSINT kann nicht für sich allein stehen. Es muss mit traditioneller Berichterstattung kombiniert werden, mit Dokumenten, menschlichen Quellen, strenger Überprüfung. Offene Daten liefern einen Anhaltspunkt, Journalismus verwandelt sie in Beweismaterial. Man kann endlos Fotos von russischen Feiern durchforsten und versuchen, den Soldaten zu entdecken, der Zivilisten verschleppte. Aber nur ein Überlebender kann ihn identifizieren, nur ein echtes Dokument seinen Dienst nachweisen.

Die Geschichte des ermordeten Mädchens, das mir ähnelte, recherchierten wir nie. Ihre Angehörigen flehten uns an, nicht weiter daran zu arbeiten, sie fürchteten, die Leiche würde exhumiert. Ich sagte, die Welt müsse doch wissen, was während der Besetzung von Iziom geschah. Sie sagten, ihre Seele verdiene Frieden. Ich zog mich zurück. Denn es geht nicht nur darum, was man aufdecken kann, sondern wie verantwortungsbewusst man diese Erkenntnisse nutzt.

*Valeriya Yegoshyna ist Investigativjournalistin bei Schemes, dem ukrainischen Dienst von RFE/RL, in Kyjiw.*

## Mit Sprachnachrichten im Radio lokale Missstände anprangern

In Südafrika können Lokalradios mit digitaler Technik ihre jeweiligen Gemeinschaften stärken, wie der Sender Alex FM in Johannesburg vormacht

Aus Johannesburg **Dianah Chiyangwa**

In Johannesburgs Township Alexandra morgens um kurz nach sieben: Im Studio des Bürgerradios Alex FM produziert Sally Mmowa die Frühstückssendung. Auf einem Bildschirm das Playout-System, auf einem anderen ein spezieller WhatsApp-Computer. Dann treffen Sprachnachrichten ein. „Hört mal“, lautet eine. „Pick it Up hat seit Ostern keinen Müll mehr abgeholt. Alles stinkt, Menschen werden krank.“ In wenigen Minuten hat Mmowas Team die Müllabfuhr erreicht. Eine Sprachnachricht kommt auf Sendung: „Keine Sorge, wir haben ein Treffen mit den Stadträten. Wir lösen das Problem.“ Das ist investigativer Journalismus: Nur eine WhatsApp-Nachricht, eine Gemeinschaft, die weiß, wohin sie diese schicken muss, ein Sender, der bereit ist zu handeln.

Südafrika hat 290 Community-Radios und 41 kommerzielle und öffentlich-rechtliche Sender. Medienkonzerne kämpfen ums Überleben, der öffentlich-rechtliche Rundfunk SABC ächzt unter Schulden. Fragt man bei Community-Radios, was den Durchbruch brachte, heißt es WhatsApp. In den letzten zehn Jahren hat sich die Zahl südafrikanischer Internetnutzer fast verdoppelt. Laut einer Studie haben Südafrikaner mit 58,2 Prozent ihres Tages weltweit die längste tägliche Bildschirmzeit. „Vor WhatsApp wurden Gesprächsguthaben gekauft, um anzurufen“, sagt Mmowa, „jetzt gibt es überall kostenloses WLAN in Einkaufs- und Gemeindezentren. Zugänge sind viel einfacher, auch dank Facebook, TikTok, Instagram, X und YouTube.“

Der Wandel ist auch redaktionell. Hörer nehmen nun an der Beschaffung von Nachrichten teil. Bei Protesten fordern die Sender Menschen vor Ort auf, Sprachnachrichten mit Beobachtungen, Bildern und Videos aus erster Hand zu senden. Sie werden geprüft und ausgestrahlt. Kommerzielle Sender haben Syndikatsverträge, Marketingbudgets und prominente Moderatoren. Doch: „Wenn in der Gemeinde etwas passiert, erfahren wir das als Erste“, sagt Mmowa. „Unsere Macht ist die des Volkes. Deshalb kommen Politiker zu den Bürgerradios. Sie wissen, dass wir die Gatekeeper der Gemeinde sind.“ Pressefreiheit ist für Mmowa die Antwort auf die Frage, ob ihr Sender dem Publikum die Wahrheit sagen kann. „Unser Fokus liegt auf Rechenschaftspflicht“, sagt sie. „Die Gemeinschaft zieht uns zur Rechenschaft. Sie schlägt vor, wen sie auf Sendung haben will. Geht das nicht, sollten wir wenigstens die Wahrheit sagen.“

Alex FM erreicht über den Äther 350.000 Hörer. Online sind stets mehr als 10.000 Menschen live zugeschaltet. Doch der digitale Wandel mit Zetta-Playout-System, WhatsApp-Computer, Streaming-Infrastruktur kostet echtes Geld. Jahrelang wurde die Lücke mit Freiwilligen und Hoffnung überbrückt. Dann kündigten die Association of Independent Publishers (AIP) und Google im November 2024 den Digital News Transformation Fund mit umgerechnet 5,9 Millionen Euro über drei Jahre an. Südafrikas bisher größte Finanzspritze für Basismedien. Für die AIP-Vorsitzende Anetta Mangxaba ist der Fonds eine „entscheidende Rettungsleine für den unabhängigen Journalismus“. Lokalmedien verschafften „den Bürgern an der Basis Gehör“. Der Medienwissenschaftler Tony Tendai sagt: „WhatsApp und digitale Tools haben eine große Rolle dabei gespielt, Gemeinschaften zusammenzubringen. Aber zu behaupten, sie würden den Community-Journalismus retten, geht zu weit.“ Digitale Plattformen hätten jetzt ein Monopol auf Werbekunden, während Lokalmedien schrumpfende Werbeeinnahmen, begrenzte Mittel und hohe Arbeitsbelastung für kleine Teams hätten.

Um neun Uhr endet die Frühstückssendung. Mmowa fährt den WhatsApp-Computer herunter. Das Müllentsorgungsunternehmen hat live im Radio geantwortet. Ob es tatsächlich auftaucht, ist eine andere Geschichte, die Alex FM verfolgen wird. Denn sonst tut es niemand. „Das ist Radio mit Einfluss“, sagt Mmowa.

*Dianah Chiyangwa ist freie Journalistin im südafrikanischen Johannesburg. 2023 nahm sie am Afrika-Workshop der taz panterstiftung teil.*

## Freie und Open-Source-Initiativen statt proprietärer Digitaltechnologie

Die Entwicklung einer prosperierenden Digitalwirtschaft sollte statt die Monopole besser die Menschenrechte, den Fortschritt und die soziale Gerechtigkeit fördern

Von **Lucas Lasota**

Die Entwicklungsmodelle digitaler Werkzeuge beeinflussen die Kontrolle und Eigentumsrechte über sie. In der Soft- und Hardwareentwicklung dominieren zwei Modelle: Während das „freie und quelloffene“ Modell jedem die Freiheit gibt, Technologie zu nutzen und zu verbessern, verweigert das „proprietäre“ Modell diese Freiheiten. Es behält das Eigentum an der Technologie und schafft Engpässe, an denen Inhalte und Daten nur von demjenigen bestimmt werden, der die Kontrolle hat – sei es eine private Firma oder eine Regierung.

Ein warnendes Beispiel ist X (früher Twitter). Diese Social-Media-Plattform war für Journalisten und Aktivisten wichtig für Nachrichten, Trends und Kontakte zu Politikern, Wissenschaftlern und Prominenten. 2022 wurde die Plattform von einem mit der extremen Rechten verbundenen Milliardär übernommen, der die Moderation von Inhalten stark änderte. Das führte zur Verbreitung von Fake News, Hass und Onlinegewalt. Bei der Integration des KI-basierten Chatbots Grok wurden Algorithmen so konfiguriert, dass sie rechtsgerichtete Inhalte generieren. Die Infrastrukturentwicklung entfernte sich von freien und Open-Source-Elementen.

Viele Journalisten, Akademiker und Aktivisten verließen die für die Meinungsfreiheit wichtige Plattform, begleitet von neuen Debatten über die Kontrolle von Technologie. Können mit der Entwicklung einer prosperierenden Digitalwirtschaft auch Menschenrechte, Fortschritt und soziale Gerechtigkeit gefördert werden? Während große Internetplattformen eine beispiellose globale Vernetzung geschaffen haben, hat die große Dynamik der Digitalwirtschaft, die eine sich ständig konzentrierende Macht von Oligopolen und hohe Datenabhängigkeit ausmacht, starke soziale Auswirkungen: Die umfassende Privatisierung digitaler Technologie verhindert demokratische Steuerung und zementiert strukturelle soziale und wirtschaftliche Benachteiligung.

Digitale Monopole sind schädlich für ein offenes und demokratisches Internet. Die Haltung „Move fast and break things“, gepaart mit der wirt-

schaftlichen Deregulierung der letzten 30 Jahre, gab Technologiekonzernen die Kontrolle über digitale Ökosysteme wie Soft- und Hardware, Daten und Netzwerke. Heute kontrollieren nur fünf Konzerne (Google, Amazon, Apple, Microsoft und Meta) die wichtigsten Engpässe der globalen Digitalwirtschaft.

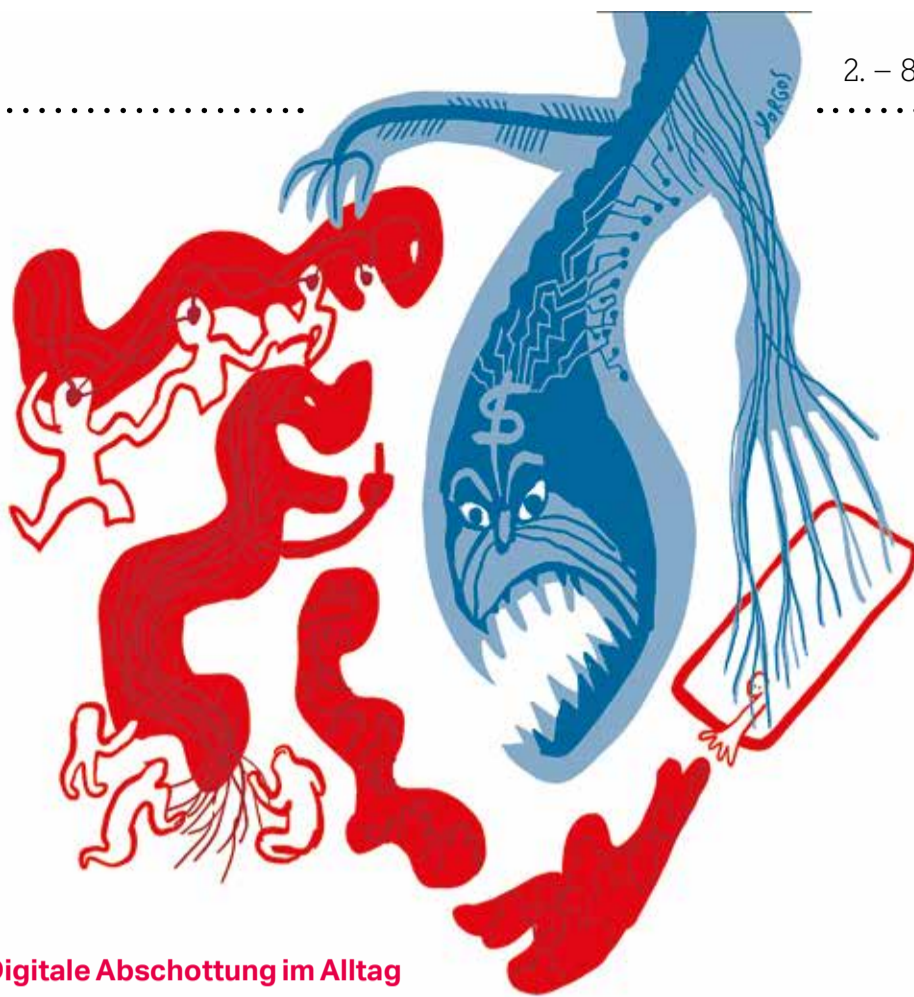
Die Kritik an den Machtverhältnissen über die kritische digitale Infrastruktur sollte einhergehen mit Forderungen nach einer grundsätzlich neuen Art, wie Wohlstand im Digitalzeitalter erzeugt und besessen wird. Freie und Open-Source-Initiativen, die sichere datenschutzfördernde Anwendungen, Tools und Plattformen entwickeln, sind eine Alternative zu proprietärer Technologie. Sie sind die Basis für Technologien, die kollektiven Formen nachhaltigen und dezentralen Eigentums den Vorrang geben.

So werden freie und quelloffene Social-Media-Plattformen wie Mastodon auf Basis dauerhaft offener Protokolle entwickelt. Diese sind interoperabel und verhindern eine zentralisierte Übernahme durch Regierungen oder Unternehmen wie bei Twitter. Für Medienschaffende bedeutet dies mehr Freiheit und Unabhängigkeit bei Erstellung und Weitergabe von Inhalten. Freie und quelloffene Initiativen wie das Guardian Project stellen Tools für die sichere Kommunikation, anonymes Surfen und Mediensicherheit für Medienschaffende in Hochrisikoregionen weltweit bereit.

Das hilft Menschen, sicher und vertraulich zu kommunizieren und sich zu organisieren. Dabei ist ihre Identität geschützt und es können digitale Beschränkungen von autoritären Regimen oder Konzernen umgangen werden. Beispiele hierfür sind das Tor-Netzwerk, das Nutzern das anonyme Surfen im Internet ermöglicht, sowie verschlüsselte Messaging-Apps auf Basis dezentraler XMPP-Netzwerke.

Demokratischere und egalitäre Formen der Technologieentwicklung stärken die Pressefreiheit, indem sie ein offenes und neutrales Internet festigen.

*Lucas Lasota forscht an der Universität Halle-Wittenberg zur Regulierung digitaler Technologien.*



Digitale Abschottung im Alltag

## Vertrauensbruch im Gewand „digitaler Unabhängigkeit“

In Russland ist kaum noch eine private Kommunikation per Messenger möglich, ohne dass dabei der Staat vertrauliche Informationen erfahren kann. Eine kleine Recherche bei den eigenen Verwandten und Freunden

Von **Mascha Blumberg**

Über Weihnachten und Neujahr habe ich meine Verwandten und Freund:innen in Russland besucht. Ich wollte mit ihnen unbedingt darüber sprechen, wie wir weiterhin auf einem sicheren Weg in Kontakt bleiben können. Westliche Messenger-Dienste werden dort seit vier Jahren immer mehr eingeschränkt und blockiert. Freunde berichten, dass Facebook seit mindestens drei Jahren nicht mehr aufrufbar ist. Ich habe selbst erlebt, wie Signal im August 2024 plötzlich keine Nachrichten mehr übermitteln konnte. WhatsApp und Telegram wurden ihrer Anrufunktion im August 2025 beraubt. Ende 2025 konnten nur reine Textnachrichten empfangen werden. Ich schreibe diesen Text Mitte April 2026. Seit zwei Wochen kommen meine Textnachrichten auf Telegram nicht mehr bei meinen Kontakten dort an.

Auch das mobile Internet wird seit 2025 in vielen Regionen Russlands für Stunden unterbrochen. Eine Freundin schrieb mir letzten Sommer, dass sie auf ihrer Datsche nachts kein Internet hatte. Ende des Jahres funktioniert das Internet in den regulären Arbeitsstunden erträglich gut, aber abends und an Wochenenden deutlich langsamer. Viele Internetseiten sind inzwischen zu keiner Tageszeit aufrufbar.

Anfang Dezember 2025 verkündete der Präsident, das Land sei nun nach den USA und China ebenfalls digital unabhängig. Menschen müssen nicht mehr auf Angebote aus „nicht befreundeten Ländern“ angewiesen sein, es gebe die russische Mes-

senger-Alternative Max. Dem Wechsel zu Max wird mit dienstlicher Anweisung und der Blockade von ausländischen Messengern nachgeholfen. Nach allem, was ich weiß, gehört es nicht zu Max-Merkmalen, eine vertrauliche Kommunikation sicherzustellen. Die Kommunikation ist nicht verschlüsselt und erlaubt einen leichten Zugang zu Kontakten, Nachrichten und anderen Inhalten auf dem Smartphone, wie etwa einer permanenten Ortung des Geräts. So stelle ich mir eine private Kommunikation nicht vor. Meine Erwartung an einen Messenger-Dienst ist, dass meine Infos nur bei den Personen ankommen, die ich bestimme. Alles andere ist ein Vertrauensbruch.

Doch die meisten meiner Verwandten und Freund:innen nutzen Max bereits aktiv. Ich war sprachlos. Meine Nachfragen, ob sie über die „Mitlesefunktion“ Bescheid wüssten, wurden nachlässig mit „Was wissen sie denn über uns noch nicht?“ pariert oder damit, dass das Tool immerhin ganz gut funktioniere und günstigere Anrufe ermögliche als über den Mobilfunk.

Eine Cousine sagte, dass für manche offizielle Vorgänge und den Erhalt wichtiger Mitteilungen dieser Messenger Voraussetzung sei. Max ist zudem mit dem Portal staatlicher Dienstleistungen, Gosuslugi, verknüpft, dessen Nutzung ebenfalls unentbehrlich gemacht wurde. Ausweiserneuerung, Steuerbescheide, Renten- und Sozialversicherungsanträge, Vergabe von Arztterminen sind fast nur darüber erreichbar und liefern viele sensible Daten.

Wird WhatsApp in der EU wegen unzureichenden Datenschutzes kritisiert, wäre es in Russland lediglich „das kleinere Übel“. WhatsApp war Kommunikationsmittel Nummer eins zwischen Privatpersonen wie auch zwischen Dienstleister:innen und Kund:innen. Das war das Tool für den Austausch mit dem Schuhmacher um die Ecke, der Hausverwaltung, Bibliothek, sogar einer Bank oder einem Online-Handel. Doch ich wunderte mich über die extreme Verbreitung. Ende 2025 wurde die Nutzung von WhatsApp nach und nach eingeschränkt – technisch und regulatorisch. In einer städtischen Einrichtung hörte ich eine Mitarbeiterin sagen: „WhatsApp ist bei uns nicht mehr erlaubt, aber zu Max sind wir noch nicht verpflichtet.“ Damit sei aber zu rechnen.

Bei einem gemütlichen Beisammensein mit einer Freundin erwähnte diese schmunzelnd, dass sie in der Tram ein Gespräch von zwei älteren Damen gehört habe, die sich Tipps zu VPNs (Software zur Umgehung länderspezifischer Netzblockaden) gaben. Doch Internetprovider sind angehalten, Verbindungen per VPN zu erkennen und zu unterbinden. Momentan bleiben nur ungeschützte Kommunikationskanäle gut zugänglich, die Teil einer Massenüberwachung sind. Was ich lange befürchtet habe, ist eingetreten: Ende der privaten und vertraulichen Kommunikation von und mit Menschen in Russland.

*Mascha Blumberg engagiert sich in der Kampagne Digital Independence Day.*



**Yorgos Konstantinou**

(y0rgos), auch bekannt als ÉPFOC, ist ein visueller Kommunikator aus Thessaloniki, der als Comic- und Cartoonzeichner in mehreren Ländern unterwegs ist. Er arbeitet als Illustrator, visueller Vermittler und Cartoonist für Bücher, Presse und Erklärfilme. Als Aktivist gestaltet er Bilder für Bürgerinneninitiativen und Menschenrechtskampagnen. Er ist Initiator der @MEDfaces und des Bildungskollektivs Irenia-Friedensspiele. Er illustriert talks der taz panterstiftung als Graphic Harvesting.

[www.imagistan.com](http://www.imagistan.com)

taz panterstiftung

# Ja, ich mache mit!

... und unterstütze die Projekte der taz Panter Stiftung

20 €  50 €  100 €  \_\_\_\_\_ €

Jede Spende ist steuerlich absetzbar.

Online spenden unter: [www.taz.de/spenden](http://www.taz.de/spenden)



Vielen Dank für Ihre Unterstützung!