

Die Entkernung der Demokratie

Wie wir die digitale Öffentlichkeit vor den Oligarchen retten können

Von **Markus Beckedahl**

Die reichsten und mächtigsten Menschen der Welt reihen sich hinter einem autoritären Herrscher ein, dessen Regierung die US-Demokratie zerstört. Der rechte Autoritarismus schreitet voran – politisch, gesellschaftlich, technologisch. Das wird in den USA besonders deutlich, ist aber längst ein globaler Trend. Ein zentrales Element dabei ist der Aufbau neuer Gegenöffentlichkeiten im Netz. Rechtspopulisten – und zunehmend Rechtsradikale – nutzen digitale Kanäle und ihre Mechanismen gezielt, um journalistische Medien zu umgehen und selbst zu Sendern zu werden. Auch in Deutschland hat sich am rechten Rand ein neues mediales Ökosystem gebildet – als Scharnier zwischen Konservatismus und Extremismus. Es reicht von Nius über Tichys Einblick bis zur „Welt“ und wird unterstützt von zahllosen Nutzer:innen auf großen Plattformen wie Facebook, Youtube, Tiktok oder X, die sich dort algorithmisch verstärken.

Das führt zu einer schleichenden, aber systematischen Diskursverschiebung nach rechts außen. Die Techoligarchen aus dem Silicon Valley stellen dafür die Infrastruktur bereit – teils bewusst und mit politischen Absichten, teils aus Gleichgültigkeit und Profitinteresse. Sie können sich dabei der extremen Machtkonzentration im Digitalen bedienen: 99 Prozent der Verwaltungscomputer laufen auf Microsoft. Bei Cloud-Infrastrukturen teilen sich Google, Microsoft und Amazon den Markt auf. Über 80 Prozent der Menschen in Deutschland benutzen WhatsApp.

Wenige Unternehmen, teilweise in der Hand einzelner Personen, kontrollieren unsere digitalen Kommunikationsräume. Sie entscheiden, wie wir uns informieren, worüber wir diskutieren – und letztlich auch, wie sich ein großer Teil der Öffentlichkeit strukturiert. Diese Plattformen sind schon lange keine neutralen Kanäle mehr, sondern Gatekeeper, Zensoren, Architekten des Diskurses – mitunter gelenkt von Geschäftsinteressen und ideologischen Launen einzelner Milliardäre. Stellen wir uns die drastischen Konsequenzen vor, wenn Plattformen journalistische Inhalte noch gezielter diskriminieren – algorithmisch und manuell –, wenn die Pressefreiheit weiter beschnitten wird, wenn Informationsfreiheitsgesetze und Datenschutzstandards abge-

* Dieser Text basiert auf einer Keynote des Autors auf der Jahrestagung des Netzwerk Recherche im Juni 2025.

räumt werden. Die autoritären Drehbücher dafür kennen wir: Die USA zeigen uns derzeit, wie schnell demokratische Institutionen untergraben werden können. In Ungarn war es bereits zu beobachten, ebenso in Polen. Wir müssen aufhören, Dystopien als hypothetisch zu betrachten. Die Realität hat die Fiktion oft längst eingeholt.

Ein Software-Putsch

Die USA haben keinen normalen Regierungswechsel erlebt. Es war eine Art Putsch – nicht mit Panzern, sondern mit Software. Elon Musk, ausgestattet mit einer präsidentialen Blankovollmacht, durchstreifte mit seinem DOGE-Team US-Behörden und kopierte massenhaft Daten über Wohnorte, Einkommen, polizeiliche Befragungen und natürlich das Wahlverhalten der US-Bürger:innen. Als einige Gerichte später das Kopieren der Daten für illegal erklärten, war es längst zu spät. Die Informationen waren bereits auf Notebooks gespeichert – außerhalb jeglicher demokratischen Kontrolle. Viele Medien fielen auf das Framing der Regierung herein, das Ziel von DOGE seien Einsparungen und Bürokratieabbau.

Aber Techmedien wie „Wired“ erkannten früh: Es ging hier nicht um eine Verwaltungsreform, sondern um die digitale Infrastruktur für spätere Massendeportationen.¹ Die abgeschöpften Daten landen nun in den Analysemaschinen großer Techunternehmen wie Palantir – ein Konzern, der seit Jahren an der systematischen, digitalen Überwachung der Gesellschaft arbeitet. In den Händen autoritärer Regime wird Software wie diese zur perfekten Waffe, die analysiert, bewertet, sortiert und Profile nach „Gefährlichkeit“ und „Nützlichkeit“ erstellt. Laut Recherchen von Medien wie „Wired“ und CNN werden damit Abschiebungen algorithmisch optimiert, „von der Identifizierung bis zur Entfernung“². Was effizient klingt, ist in Wahrheit der technokratische Alptraum schlechthin – und ein Traum für autoritäre, antidemokratische und fremdenfeindliche Parteien.

Wer jetzt glaubt, das sei ein rein US-amerikanisches Problem, unterschätzt die Geschwindigkeit, mit der autoritäre Technologien und Ideologien exportiert werden. Palantir wird längst in Deutschland eingesetzt – von Polizeibehörden in mehreren Bundesländern.³ Die Ausweitung dieser Systeme ist geplant, während unklar bleibt, was mit den Daten passiert, die dort einfließen. Deutschland ist theoretisch nur eine Wahl davon entfernt, dass rechts-extreme Akteure an die Schaltstellen der Macht gelangen, zumindest in einzelnen Landesregierungen. Ein solches Szenario rückt noch näher, wenn umgesetzt wird, was nach Aussagen der Whistleblowerin Sarah Wynn-Williams⁴ im Board, einer Art Aufsichtsrat, von Facebook diskutiert wurde:

1 Makena Kelly u.a., Inside Elon Musk's „Digital Coup“, wired.com, 13.5.2025.

2 Vgl. Priscilla Alvarez u.a., DOGE is building a master database for immigration enforcement, sources say, cnn.com, 25.4.2025.

3 Vgl. Sonja Peteranderl, Das Überwachungsimperium, in: „Blätter“, 8/2025, S. 91-96.

4 Sarah Wynn-Williams, Careless People: A Cautionary Tale of Power, Greed, and Lost Idealism, New York 2025.

Man könne in Staaten wie Deutschland doch Parteien wie die AfD boosten, um sich ein besseres Regulierungsklima zu schaffen. Im Board damals dabei: Die beiden rechtsradikalen Techoligarchen Peter Thiel, Mitgründer und größter Anteilseigner von Palantir, und Marc Andreessen.

Wenn Politiker der AfD in entsprechende staatliche Machtpositionen gelangen, dann hätten sie nicht nur direkten Zugriff auf die Überwachungssoftware von Palantir, die sie nutzen könnten, um ihre Macht zu festigen und Kritiker:innen zu bekämpfen, sondern auch auf weitere Systeme, die Schwarz-Rot gerade einführen will, von Vorratsdatenspeicherung bis zu biometrischer Videoüberwachung. Wenn in einem solchen Szenario Behördenleitungen ausgetauscht, Regeln ignoriert und Prozesse beschleunigt werden, hilft nur noch ein bürokratisches Relikt, welches oftmals als lästiger Hemmschuh für Innovationen verrufen wurde: Datenschutz. Dieser wird als Brandschutz für die Demokratie fungieren, während Datensparsamkeit der Notausgang sein wird, wenn das System brennt. Denn letzten Endes bestimmen die Menge der Daten und wer Zugriff auf diese hat, wie verwundbar der oder die einzelne Bürger:in ist. Das gilt für Angriffe von innen und von außen.

Europas digitale Souveränität in weiter Ferne

Digitale Souveränität ist das Stichwort, unter dem der Schutz vor Zugriff auf Daten von außerhalb der EU diskutiert wird. Bereits vor zwölf Jahren gab es in dieser Frage ein kurzes Momentum, als die Enthüllungen von Edward Snowden dokumentierten, wie Big Tech mit US-Geheimdiensten kooperiert, um ein System der Totalüberwachung zu schaffen. In Deutschland herrschte zwei Wochen lang Empörung, als herauskam, dass auch Angela Merkels Handy überwacht wurde. Obama versprach ihr kurz danach, zumindest das nicht mehr abzuhören, was die Debatte darüber beendete, wie wir eigene unabhängige digitale Infrastrukturen aufbauen, die ohne diese Schnittstellen zu NSA und Co. auskommen.

Business as usual lief weiter, nur erweitert um die Frage, auf welchem der drei großen US-Hyperscaler Amazon, Microsoft oder Google man seine zukünftige Cloud betreiben will. Das ist immer noch die Kernfrage vieler Unternehmen und öffentlicher Verwaltungen, auch in Zeiten des US-Cloud-Acts, der US-Unternehmen und ihre Tochterfirmen im Ausland verpflichtet, mit US-Geheimdiensten zusammenzuarbeiten.

Was das bedeuten könnte, wird plastisch, wenn wir uns vorstellen, dass investigative Journalist:innen in den nächsten Panama Papers Material über die Trump-Familie finden. Sind ihre Redaktionen vorbereitet, falls Präsident Trump dann Sanktionen gegen sie erlässt und ihre Microsoft-IT-Infrastruktur abgeschaltet wird? Der demokratische Diskurs steht und fällt mit unabhängigen Medien. Wenn deren Daten aber auf US-Servern lagern und sie von Software aus dem Silicon Valley abhängen, dann können sie problemlos ausgespäht, mit Sanktionen überzogen oder ihrer Infrastruktur beraubt werden.

Gegenüber einem solchen Szenario scheint der momentane Einfluss von X in Deutschland geradezu harmlos. Aber Musks Plattform zeigt ebenfalls, wie wenig es Europa gelingt, seine digitale Souveränität aufzubauen und eine demokratische Öffentlichkeit zu verteidigen. Ich war lange ein großer Fan von Twitter. In den besten Zeiten hatte ich über 400 000 Follower, heute poste ich dort nichts mehr. Seit der Übernahme durch Elon Musk ist aus Twitter das geworden, was viele befürchtet hatten: eine Plattform, bei der Inhalte, Reichweiten und Sichtbarkeit manipuliert werden – im Dienst der geschäftlichen und politischen Interessen eines Einzelnen. Unzählige Analysen und Enthüllungsgeschichten zeigen: Musk hat seinen eigenen Account algorithmisch bevorzugt, zum Beispiel im Wahlkampf, als er Donald Trump vehement unterstützte. Das ist Machtmissbrauch und ein Angriff auf den demokratischen Diskurs. Viele bleiben trotzdem auf X – aus Angst, vermeintliche Relevanz zu verlieren. Politiker:innen bleiben, weil Journalist:innen dort sind. Journalist:innen bleiben, weil die Politiker:innen dort sind. Ein toxischer Kreislauf der gegenseitigen Bestätigung. Dabei gäbe es eine Exitstrategie: einfach X-Posts nicht mehr zitieren, Links auf X nicht mehr einbetten. Politiker:innen posten in der Regel auch auf anderen Plattformen. Wir könnten X allmählich die vermeintliche Bedeutung entziehen – wenn wir wollten.

Europäische Regulierung – Hoffnung und Realität

Der Export autoritärer Kontrolltechnologien nach Europa, die strategische Unterwanderung öffentlicher Diskurse durch Plattforminteressen und der Aufbau repressiver Dateninfrastrukturen treffen hierzulande auf eine gefährliche Mischung aus politischer Naivität und wirtschaftlichem Pragmatismus. In diesem Spannungsfeld wird Datenschutz plötzlich viel mehr als ein Schutz für Einzelne, er wird zum letzten Bollwerk einer offenen Gesellschaft – nicht als technisches Detail oder bürokratisches Hindernis, sondern als Schutzmechanismus gegen Machtmissbrauch. Gerade weil durch den US-Cloud-Act, durch private Sicherheitssoftware in öffentlichen Händen und durch den Druck auf kritische Medien die digitale Souveränität Europas untergraben wird, braucht es eine radikale Re-Politisierung des Datenschutzes. Die europäische Datenschutz-Grundverordnung (DSGVO) ist dabei mehr als ein juristisches Regelwerk: Sie ist der Versuch, Freiheitsrechte in einer Welt zu verteidigen, in der Daten zur Waffe geworden sind. Die Frage ist allerdings, ob sie dieser Aufgabe gewachsen ist.

Daher ruhen seit Jahren auch große Hoffnungen auf den neuen EU-Regelungen, wie dem Digital Services Act (DSA) und dem Digital Markets Act (DMA). Ein Gegenmodell zur Selbstregulierung, aber noch kein Grund zum Feiern: Beim DSA erleben wir bisher nur zaghafte Durchsetzungsversuche, die vor allem gegenüber Porno-Plattformen und TikTok greifen. Zwar musste die EU-Kommission auch bei den großen DMA-Fällen gegen Apple und Meta handeln, weil sie es bereits ein Jahr zuvor angekündigt hatte, aber abgesehen von diesen Einzelaktionen zeigt sich ein demokratietheoretisches Problem

in der Praxis: Die EU-Kommission ist gleichzeitig Regulierungsbehörde und Handelsakteur. Sie verhandelt über Zölle – und soll gleichzeitig die Demokratie schützen. Das führt früher oder später zu einem Zielkonflikt, wenn beispielsweise unter dem Druck der USA regulatorische Maßnahmen aufgeweicht werden, um in Handelsfragen voranzukommen. Und der jüngste Zoll-deal zeigt, wie anfällig die EU-Kommission dabei für Druck aus den USA ist.

Beim Datenschutz ist die Lage nicht besser: Die DSGVO wäre stärker, wenn sie endlich durchgesetzt würde. Doch zuständig ist vor allem Irland – und verdient indes gut daran, dass große Techfirmen dort ihren Sitz haben. Das Ergebnis sind Verzögerungen, Untätigkeit, politische Rücksichtnahme. Die frustrierten Datenschutzbehörden in den Mitgliedsstaaten müssen hilflos zusehen. Vor ähnlichen Problemen steht jetzt schon der gerade erst in Kraft getretene AI-Act zur Einhegung der Risiken von KI. Er ist keineswegs ein perfektes Gesetz, trotzdem wird er aktuell noch weiter abgeschwächt, bevor er überhaupt Wirkung entfalten kann. Unter dem Deckmantel der „Entbürokratisierung“ schreitet hier ebenfalls die Deregulierung voran.

Dabei bräuchten wir mehr Regeln, nicht weniger: Wo bleiben die Vorgaben für transparente und nachvollziehbare algorithmische Filtersysteme? Hier gibt es zu viel Manipulationspotential, wenn aus kommerziellen oder ideologischen Gründen bestimmte Inhalte angezeigt, andere wiederum ausgeblendet werden. Warum wird weiterhin toleriert, dass Plattformen bestimmte Links, Inhalte oder User:innen aus ihren Ökosystemen heraus blockieren oder einfach nur algorithmisch bestrafen? Warum gibt es noch keine besseren Gesetze zum Schutz vor Deepfakes? Diese werden zunehmend gegen Journalist:innen eingesetzt und gefährden damit auch die Pressefreiheit, weil sie Vertrauen rauben, Reputationen zerstören und Angst einflößen. Die Plattformen, die zumindest die Verbreitung verhindern könnten, zucken hier oftmals nur mit den Schultern. Deshalb braucht es zumindest einen besseren rechtlichen Schutz der Journalist:innen durch Medienorganisationen, vor allem von freien Mitarbeitenden.

Die Logik des Überwachungskapitalismus

DSA, DMA und AI-Act sind nicht vom Himmel gefallen, sondern das Ergebnis einer der größten Lobbykämpfe in der Geschichte der EU-Gesetzgebung. Sie reichen aber nicht aus, um den Kern des Problems wirklich anzugehen: Die Logik des Überwachungskapitalismus – ein System, das jede Aufmerksamkeit monetarisiert, jedes Verhalten trackt, jede Empörung belohnt –, wirkt als Katalysator von Hass, Desinformation und Polarisierung. Denn seine Mechanismen laden zahlreiche Akteure geradezu ein, die entstehenden Echokammern strategisch zu bespielen und ihre Interessen durchzusetzen, während konstruktive, differenzierte Debatten zunehmend aus dem Rahmen dieser Logik fallen. Eine Allianz aus Big Tech und Verlagen verteidigt dieses System vehement, absurderweise im Namen der Pressefreiheit, die ursprünglich als Garant der vierten Gewalt – des unabhängigen Journalismus – gedacht

war. Diese Allianz verteidigt ein intransparentes Werbesystem, über das alle die Kontrolle verloren haben und für das wir komplett durchleuchtet werden. Bis zu mehrere hundert Firmen werden informiert, wenn ich auf einer Medien-Webseite das falsche Cookie akzeptiere. Deshalb genügen ein paar Euro, etwas Know-how und ein bisschen Motivation, um einzelne Menschen zu verfolgen, ihre Wege, ihre Kontakte und ihre Treffen zu kennen. Diese Daten existieren. Die Databroker-Recherchen von netzpolitik.org und dem Bayerischen Rundfunk haben das anschaulich dokumentiert.⁵ Selbstverständlich haben auch die Plattformen diese Daten und nutzen sie. Meta und TikTok haben sie nachweislich eingesetzt – gegen Journalist:innen und Whistleblower. Dieses System ist kaputt. Wir wissen es. Und wir spielen trotzdem weiter mit.

Alternativen denken, digitale Räume demokratisieren

Können demokratische Öffentlichkeiten auch online existieren – jenseits von Big Tech? Oder ist es unabwendbar, dass Mark Zuckerberg die digitalen Straßen besitzt und morgen entscheiden kann, dass auf dem linken Bürgersteig nur noch rückwärts gelaufen werden darf? Es braucht Räume für Debatten, Austausch und Information, die nicht darauf optimiert sind, unsere Aufmerksamkeit durch endlose Dopamin-Kaskaden zu fesseln. Öffentlichkeiten, die nicht privatisiert sind, sondern gemeinwohlorientiert, gestützt auf offene Standards, demokratisch kontrolliert, staatsfern finanziert und betrieben. Diese Infrastrukturen fallen nicht vom Himmel, sie brauchen Investitionen, politische Unterstützung – und eine langfristige Vision.

In einer idealen Welt wäre der öffentlich-rechtliche Rundfunk genau der Ort, an dem solche digitalen Infrastrukturen entwickelt werden. Und es gibt lobenswerte Ansätze, die auf Technologieneutralität abzielen. Der „Public Spaces Incubator“ von ARD, ZDF und öffentlich-rechtlichen Anstalten aus vier weiteren Staaten bringt Medienhäuser und Entwickler:innen zusammen. Das Ziel ist die gemeinsame Entwicklung von Open-Source-Werkzeugen, die etwa konstruktivere Debatten ermöglichen sollen. Auch die Online-Mediatheken dieser Sender setzen auf ein gemeinsames Open-Source-Ökosystem und eine vertrauenswürdige Infrastruktur, auf der die Konten der Nutzer:innen angelegt werden.

Wenn medienpolitisch von einer „europäischen Plattform“ die Rede ist, meinen viele: ein europäisches Facebook oder Twitter. Was wir aber stattdessen brauchen, ist kein Kathedralenbau, sondern ein digitaler Basar: ein vernetztes, dezentrales System auf offenen Protokollen wie ActivityPub, der offene Standard hinter dem Fediverse⁶ oder ATPROTO, das Protokoll hinter

5 Ingo Dachwitz, Sebastian Meineck, Die große Datenhändler-Recherche im Überblick, netzpolitik.org, 16.7.2024.

6 Fediverse ist die Kurzform für „Federated Universe“. Im Gegensatz zu den geschlossenen Netzwerken wie Facebook, Instagram, TikTok und Twitter/X handelt es sich um ein Netzwerk aus vielen unabhängigen Plattformen und Diensten. Die Server des Fediverse verwenden eine Protokoll namens ActivityPub.

Bluesky – mit Kommentar- und Diskursfunktionen in Mediatheken. Warum müssen wir uns auf Youtube oder Facebook austauschen und debattieren? Es braucht Kommunikationsplattformen, die über einen gemeinsamen offenen Standard miteinander kommunizieren können und Daten transparent austauschen. Das ermöglichen gemeinwohlorientierte Infrastrukturen wie das Twitter-ähnliche textbasierte Soziale Netzwerk Mastodon oder die Videoplattform Peertube. Offenen Protokollen sei Dank. Die Mediatheken könnten die Grundlage sein – mit Millionen Nutzer:innenkonten, die auf Datenschutz verpflichtet sind. Und es gibt weitere Lichtblicke: Die SWR X Labs, die Innovationseinheit des SWR, zeigt gerade in Zusammenarbeit mit dem Media Lab Bayern und Mastodon, was möglich ist. Sechs Fellowships à 10000 Euro für Medieninnovationen im Fediverse. Menschen bekommen so die Chance, kleine Innovationen zu entwickeln und als Open-Source mit anderen zu teilen. Auch eine effektive Moderation dieser Debatten wäre machbar: Der öffentlich-rechtliche Rundfunk beschäftigt längst viele Social Media-Manager:innen, die Facebook-, Instagram- und X-Accounts betreiben. Schließlich sollten öffentlich finanzierte Inhalte selbstverständlich auch auf gemeinwohlorientierten Plattformen zu finden sein.

Das öffentlich-rechtliche System – aber auch generell Behörden – sollten verpflichtet sein, neben ihren kommerziellen Accounts mindestens einen offiziellen Account auf einer offenen, dezentralen Plattform zu betreiben, damit Menschen sich informieren und interagieren können, ohne von Plattformen überwacht zu werden, die sie eigentlich meiden wollen. Und damit sich Alternativen überhaupt entwickeln können, denn Plattformen wachsen durch Inhalte und Inhalte durch Sichtbarkeit.

Zehn Prozent für technologische Souveränität

Der Anteil der Initiativen für technologische Unabhängigkeit am Gesamtbudget des öffentlich-rechtlichen System ist bis jetzt verschwindend gering. Wir brauchen eine politische Debatte darüber, wie viel technologischer Gemeinssinn uns unsere Demokratie wert ist. Ich plädiere dafür, zehn Prozent des Budgets des öffentlich-rechtlichen Rundfunks für technologische Souveränität zu nutzen. Für das Entwickeln und Betreiben von Infrastrukturprojekten, die unabhängig, offen, staatsfern und nutzerorientiert sind. Für Infrastrukturen, die wir als Gesellschaft selbst betreiben – nicht globale Konzerne. Das Zeitfenster unserer Handlungsmöglichkeiten schließt sich möglicherweise bald: Wenn die AfD in einzelnen Bundesländern an die Macht kommt und zentrale Reformen auf Bundesebene verhindert, wäre der öffentlich-rechtliche Rundfunk angegriffen, vielleicht sogar gelähmt.

Der Staat muss bereits jetzt Verantwortung übernehmen: Nicht, indem das Innen- oder Digitalministerium ein neues Facebook startet, denn die Geschichte deutscher Digitalgipfel ist eine lange Geschichte gescheiterter staatlicher IT-Großprojekte. Notwendig ist vielmehr eine gezielte Innovationsförderung für digitale Gemeingüter. Aktuell stellt der Staat 500 Mrd. Euro für

Infrastruktur bereit – warum nicht einen Bruchteil davon für demokratische digitale Infrastrukturen? Warum nicht ein groß gedachtes Projekt nach dem Vorbild der SWR-Labs? Dazu bräuchte es auch Änderungen im Gemeinnützigkeitsrecht, damit Organisationen, die digitale Räume demokratisch gestalten, überhaupt gefördert werden können, und bessere Rahmenbedingungen für digitales Ehrenamt, das Rückgrat vieler alternativer Plattformen.

Die Angriffe auf journalistische und zivilgesellschaftliche Organisationen haben zugenommen und kommen meist von rechts – und sie folgen einem klaren Drehbuch, das wir als autoritäres Playbook aus anderen Staaten kennen: Anzweifeln der Gemeinnützigkeit, Isolation der Organisation, Entziehung ihrer Ressourcen, Bindung in Gerichtsverfahren durch SLAPP-Klagen⁷, Säen von Misstrauen. Die Debatte um Correctiv ist nur eines von vielen Beispielen. Die 551 Fragen zur Gemeinnützigkeit, die CDU/CSU kurz vor der Regierungsübernahme in den Raum stellte, waren ein deutliches Warnsignal und sollten auch ein Weckruf gewesen sein. Es ist noch nicht zu spät, aber an der Zeit, uns auf Worst-Case-Szenarien vorzubereiten. Es kann alles noch viel schlimmer kommen als gedacht. Die USA zeigen das gerade anschaulich. Wir brauchen daher eine stärkere Zusammenarbeit aller, die Demokratie und Rechtsstaat verteidigen wollen. Dazu zählt auch eine stärkere Zusammenarbeit von Zivilgesellschaft und Medienorganisationen, nicht nur bei der Recherche. Journalismus muss endlich gemeinnützig werden, damit das Damoklesschwert wegfällt, dass Finanzämter journalistischen Medien die Finanzierungsgrundlage entziehen können und auch mehr Geld über Stiftungen in das System fließen kann. Es braucht Druck auf die Politik, damit diese unsere Regeln zur demokratischen Gestaltung der Öffentlichkeit gegenüber den mächtigsten Unternehmen der Welt konsequenter durchsetzt. Wir brauchen alternative digitale Infrastrukturen, um morgen die Wahlfreiheit zu haben, uns entscheiden zu können, wo und unter welchen Bedingungen wir kommunizieren und uns informieren wollen.

Dafür setzt sich das neu gegründete Zentrum für Digitalrechte und Demokratie⁸ ein. Wir als Mitarbeitende des Zentrums wollen die Erzählmacht über die Digitalisierung von Big Tech zurückholen und neue Allianzen bauen. Wir wollen nicht zulassen, dass autoritäre Akteure unsere digitalen Räume, unsere Diskurse, unsere Infrastrukturen noch mehr übernehmen. Wir wollen ein analoges und digitales Gemeinwesen verteidigen, das offen, demokratisch und zukunftsfähig ist. Das wird nicht ohne Konflikte gehen, nicht ohne neue Regeln und nicht ohne neue Allianzen. Pressefreiheit, digitale Souveränität und gemeinwohlorientierte Technologie – das sind keine netten Extras. Sie sind die Überlebensbedingungen unserer Demokratie. Ich glaube immer noch daran, dass eine bessere digitale Welt möglich ist – wenn wir dafür kämpfen.

⁷ SLAPP steht für *strategic lawsuit against public participation* (Strategische Klage gegen öffentliche Beteiligung), eine rechtsmissbräuchliche Form der Klage, die den Zweck hat, Kritiker einzuschüchtern und ihre öffentlich vorgebrachte Kritik zu unterbinden. Sie wird in den meisten Fällen von Unternehmen, seltener von Privatpersonen oder Behörden, gegen NGOs oder Individuen angestrengt, welche die Geschäftspraktiken des Unternehmens oder der Behörde öffentlich kritisieren.

⁸ Vgl. digitalrechte.de.