Stellungnahme des cnetz e.V.

zum Antrag R06 „Digitale Öffentlichkeit ordnen – Demokratie, Jugend und Medienvielfalt wirksam schützen“

im Rahmen des 38. CDU-Bundesparteitages

19. Februar 2026

„Unser Ziel ist es, die Digitalisierung so zu gestalten, dass sie die Freiheit und Selbstbestimmung des Einzelnen sowohl im digitalen als auch im analogen Raum bewahrt und stärkt. Wir sind überzeugt: Freiheit gewinnt erst durch Verantwortung ihre wahre Bedeutung. Sie ist kein Selbstzweck, sondern bildet auf der Grundlage eines festen Wertefundaments – das Frieden, Freiheit und Fortschritt miteinander vereint – das Rückgrat unserer freiheitlich-demokratischen Grundordnung. Wir möchten dazu beitragen, Menschen zu stärken und zu befähigen, diese Freiheit verantwortungsvoll zu leben, insbesondere in einer zunehmend digitalisierten Gesellschaft, in der künstliche Intelligenz eine immer größere Rolle spielt." (Präambel der Satzung des cnetz, 29.11.2025)

Entsprechend der Grundausrichtung der satzungsgemäßen Ziele und Aufgaben des cnetz und basierend auf der im Verband organisierten Digitalexpertise, nimmt das cnetz zum Antrag R06 „Digitale Öffentlichkeit ordnen – Demokratie, Jugend und Medienvielfalt wirksam schützen", welcher im Rahmen des 38. CDU-Bundesparteitages beraten werden soll, wie folgt Stellung.

1 Gesamteinschätzung

Das cnetz begrüßt ausdrücklich die Zielsetzung des Antrags, die demokratische Diskurskultur zu stärken und Kinder und Jugendliche vor den negativen Auswüchsen der Plattformökonomie zu schützen. Vor allem sind diese auch im bekannten Rahmen vor psychologischen Nebenwirkungen zu schützen. Die Problemanalyse, insbesondere hinsichtlich der Zentrierung digitaler Infrastrukturen und der Algorithmen-Logik, ist dem Kern in dem Zusammenhang (Verstärkung und Konzentration des Informationsflusses) nach zutreffend, da die Datenauswertungen zu entsprechender Wirkung führen (können).

Gleichzeitig ist Machtkonzentration von oligopolartigen, häufig nicht Europäischer Digitalplattformen a) kein neues Phänomen und b) nicht originär auf den digital-technologischen Raum beschränkt. Der ökonomische Erfolg digitaler Plattformen und deren großen Betreiber liegt vor allem in ihrer Skalierbarkeit bzw. der Skalierungsfähigkeit begründet, die schon in den frühen 2000er Jahren in wenig regulierten Märkten (im Kern Nordamerika und Asien) begründet wurden. Daher ist es nicht verwunderlich, dass europäische Angebote, die unserem Wertekanon eher entsprechen in der Vergangenheit (bspw. StudiVZ) aufgrund der fragmentierten Regulierungslandschaft in der EU deutlich höhere Anpassungskosten im Zuge ihrer Expansion zu leisten hatten als jene Angebote, die ihre initialen Markteintritt in einem deutlich größeren Binnenmarkt verzeichnen konnten. Kurzgefasst: Es gab und gibt bis dato kaum eine Chance für nationale bzw. europäische Player.

Die Folge war und ist, dass kaum europäische Alternativen zu den großen nordamerikanischen und asiatischen Angeboten existieren, die auch tatsächlich eine kritische Masse und somit auch Kapitalstärke für den globalen Wettbewerb erreicht haben und dabei unsere Werte vertreten. Dasselbe wiederholt sich gerade im Markt für Large Language Models speziell und vielfach KI allgemein.

Es wird sich zeigen, ob tatsächlich ein Anbieter, wie Mistral (Frankreich) oder DeepL (Deutschland) gegen die Finanzstärke von Google, Open AI, Anthropic oder auch Microsoft bestehen können. Konsequenterweise müsste aber gerade an dieser Stelle auch hierüber im Antrag gesprochen werden, was leider nicht erfolgt. Der den Modellen der großen Player innewohnende Bias in deren KI-Modellen können aber ggf. noch viel gravierendere Folgen haben. Man sieht z. B. gerade im Predictive Policing die Folgen solcher Modelle, die nicht mit europäischen Daten trainiert wurden. Ein zielführender Antrag muss aber genau hier ansetzen und den Blick weiten.

Der Antrag vermengt zudem gleichzeitig unterschiedliche Ebenen und sucht nach alternativen Finanzierungsmodellen des lokalen und regionalen Journalismus durch Digitalabgaben. Es ist eine in der Tat unglückliche Verknüpfung, denn die regulatorische Frage ist von der ökonomischen zu entkoppeln. Daher erteilt das cnetz a priori der Digitalabgabe zugunsten der Medienanbieter eine Absage, solange nicht nachweislich die Plattformanbieter diese marktlich beeinträchtigen. Allein der Verweis auf die Werbeeinnahmen, die anders kanalisiert werden, kann nicht als Marktversagen, welches regulatorische Eingriffe erlaubt, interpretiert werden. Anders sieht es aus, wenn die Plattformen gezielt und wissentlich Urheberrechte missachten und daraus zusätzliche Erträge generieren und nicht an die originären Rechteinhaber abführen. Das wurde aber hier nicht thematisiert. Auch hierzu gibt es bestehendes EU-Recht, u.a. das Leistungsschutzrecht und das neue Urheberrecht, welches politisch hart errungen wurde. Hier mangelt es mehr an Um- und Durchsetzung als an fehlender Regulierung.

Gleichzeitig ist festzuhalten, dass neben dem öffentlich-rechtlichen Rundfunk, die Medienlandschaft in Deutschland (v.a. im „Print-Bereich“) aufgrund der historischen Erfahrung, marktlich organisiert ist. Daher ist es nicht verwunderlich, dass es auch regelmäßig zu Konflikten zwischen öffentlich-rechtlichen und privaten Medienanbietern kommt. Man könnte daher so weit gehen, dass die Marktmachtkonzentration in Teilen ein hausgemachtes Problem darstellt, welchem man nicht mit auf den ersten Blick populären Lösungen beikommen kann.

Schließlich fordert der Antrag zudem eine Klarnamenpflicht. Auch hier stellt sich die Frage, ob und wie diese mit welchen Folgen und Zielen umgesetzt werden kann und auch, wie die Kontrolle der Einzelfälle erfolgen soll. Faktisch wäre dies nur mit einer echten Zwei-

Faktorenauthentifizierung, die eine Registrierung erfordert, umsetzbar. Man kommt damit gefährlich nahe an chinesische Systemvorstellungen.

Das entbindet aber nicht den Kommunikator von der Haftung für Schäden seiner Kommunikation Dritten gegenüber – ganz im Gegenteil. Die Regulierung muss also da ansetzen, wo die Folgen real sind. Hierzu bedarf es grundlegender Überlegungen, die aufgrund ihrer Komplexität selbstverständlich nicht mit dem Antrag einhergehen können. Eine Bearbeitung sollte daher im Rahmen einer umfänglichen Fachbehandlung erfolgen.

Das geforderte Social Media Verbot wird zudem – davon kann man auch auf Basis der ersten Erfahrungen aus Australien – höchstens zu vielfachen Umgehungstatbeständen führen. Die Folge ist eine nicht zielführende Problemverlagerung. Die schädliche Wirkung bestimmter kommunikativer Angebote – z.B. im Bereich Selbstbilder, Desinformation etc. – anerkennend bedarf es eben wirksamer und nicht symbolischer Verbesserungen.

Ein generelles Schul-Social-Media-Verbot kann hier zumindest deutlich schneller und nachhaltiger wirksam werden als generisch leicht aushebelbare Maßnahmen (Stichworte: VPN, falsche Identitäten, laxe Kontrollen der Plattformen etc.). Auch hier empfiehlt es sich, zunächst mehr Anstrengung in die Entwicklung tragfähiger Lösungen zu stecken, um die gewünschten Effekte zu erzielen. Man fühlt sich an manche historische Diskussion zum Jugendmedienschutz erinnert, die auch vielfach eben nicht die gewünschten Wirkungen entfaltet haben (insbesondere im Bereich der Computer- und Videospiele zeigt sich das Systemversagen sehr drastisch), da man letzten Endes eher Anreize zur Umgehung als Einsicht generiert hat.

In Summe: Die vorgeschlagenen Instrumente (Klarnamenpflicht, Algorithmuskontrolle, Social-Media-Verbot ab 16, nationale Digitalabgabe) sind so, wie politisch vorgeschlagen a) als Paket und b) auch in den Einzelfragestellungen kritisch zu betrachten, da sie teilweise nicht nur im Widerspruch zu bisherigen Positionen einer liberal-konservativen Netzpolitik stehen, sondern auch technisch schwer umsetzbar und entsprechend wissenschaftlicher Evidenz nur eine geringe Wirksamkeit aufweisen.

In Summe fordert das cnetz daher eine umfängliche Befassung unter Einbeziehung von wissenschaftlich gestützter Fachexpertise sowie einem breiten Diskurs, um tatsächliche Verbesserungen gegenüber dem Status quo zu erreichen. Wir teilen also sehr wohl einige Ziele aber nicht die vorgeschlagenen Wege im Antrag.

Zudem fordert das cnetz eine Digitalabgabe, wenn überhaupt, nicht zweckgebunden für nationale Medienanbieter, sondern diese gemeinwohlorientiert einzusetzen. Sollte es sich zukünftig um eine echte Digitalsteuer handeln, sind zudem Überlegungen hinsichtlich der Kompensationswirkung entfallender Steuereinnahmen zu berücksichtigen.

Die vorgeschlagene Algorithmen-Kontrolle ist dringend in Bezug auf ihre Rechtmäßigkeit (Betriebsgeheimnisse), Umsetzbarkeit (wer kontrolliert zu welchen Kosten und Lasten) sowie der Wirksamkeit (faktische Wettbewerbsverzerrung) zu überdenken. Das cnetz fordert hier ebenfalls eine holistische Betrachtung, die dem KI-Zeitalter gerecht wird.

2 Zur algorithmischen Transparenz und Kontrolle

Der Antrag R06 fordert, dass *„algorithmische Steuerung nicht länger ein blinder Fleck demokratischer Kontrolle bleiben darf“*. Es wird verlangt, dass Nutzer nachvollziehen können, „warum ihnen bestimmte Inhalte angezeigt werden“, und dass „verbindliche gesetzliche Regelungen“ geschaffen werden, um die Auswirkungen auf den demokratischen Diskurs offenzulegen.

Die Grundannahme, dass die auf „Engagement“ und „Aufmerksamkeit“ optimierten Algorithmen zur Polarisierung beitragen, ist auch seitens des cnetz unstrittig und vielfach belegt. Die Forderung nach einer bloßen „Offenlegung“ oder „Transparenz“ des Algorithmus greift jedoch technisch zu kurz und ist regulatorisch faktisch wirkungslos (das sogenannte „Transparenz-Paradoxon“), denn die Forderung nach Offenlegung der Funktionsweise suggeriert lediglich, dass man durch Einsicht in den Quellcode manipulative Absichten erkennen könnte. Das geht an der Realität vorbei und verursacht zudem unnötig Kosten und Lasten. Zudem können Sicherheitslücken entstehen, die durch die Offenlegung durch Dritte ausgenutzt werden können. Damit würden sogar negative externe Effekte auftreten.

Black-Box-Problem (Deep Learning): Moderne Empfehlungssysteme basieren auf künstlichen neuronalen Netzen (KNNs), die sich dynamisch anpassen. Selbst die Entwickler bei Meta oder TikTok können oft nicht erklären, warum ein spezifisches Video viral geht – es ist das Ergebnis von Milliarden Parametern in Echtzeit. Ein „Einblick in den Code“ liefert hier keine Erkenntnis. Darüber hinaus entwickelt inzwischen Code – Code (Stichworte Claude/Opus 4.6 von Anthropic und Gemini/Complexity 5.3 von Google, im Kontext Vibe Coding). Mit anderen Worten Code kann sehr schnell immer wieder verändert werden.

„Adversarial Attacks“: Eine vollständige Transparenz der Ranking-Faktoren würde es Desinformations-Akteuren, Pishing-Spezialisten und Spammern ermöglichen, ihre Inhalte perfekt auf den Algorithmus zu optimieren („Adversarial Attacks“), was das Problem der Manipulation und des Missbrauchs eher verschärft als löst. Zudem können Sicherheitslücken ausgenutzt werden.

Die Antragstellerin fordert ferner nationale gesetzliche Regelungen. Dies ignoriert aber die bereits geltende europäische Rechtslage. Der Digital Services Act (DSA) der EU verpflichtet „Very Large Online Platforms“ (VLOPs) bereits in Artikel 27 zur Transparenz der Empfehlungssysteme und in Artikel 40 zum Datenzugang für die Forschung. Echte Kontrolle entsteht nicht durch öffentliche Einsicht, sondern durch den Zugang für geprüfte Wissenschaftler („Vetted Researchers“), die empirisch untersuchen können, ob ein Algorithmus systematisch Desinformation bevorzugt (Auditierung). Nationale Alleingänge würden hier Kollisionen mit dem EU-Recht erzeugen und auch den Aufbau komplexer Verwaltungsstrukturen mit erheblichen Kosten auslösen.

Mit Blick auf die marktbeherrschenden Oligopole wäre aus gegebenen empirischen Beobachtungen allerdings auch intensiver über algorithmische Rechenschaftspflicht (Accountability) und Wahlfreiheit (Interoperabilität) zu diskutieren. Statt den einen Algorithmus staatlich zu kontrollieren (was zudem Fragen der Zensur aufwirft), sollte die Monopolstellung des Algorithmus gebrochen werden.

In diesem Kontext schlagen Francis Fukuyama und Forscher der Stanford University das Middleware-Modell vor. Dabei lagern Plattformen die Kuration der Inhalte an Drittanbieter ohne Eigeninteresse aus. Nutzer könnte wählen, ob sie den „Standard-Algorithmus“ von X/Twitter, oder einen Algorithmus der „Tagesschau“ (faktengewichtet), eines Sportverbandes oder einer NGO zur Anwendung bringen wollen. Dies fördert Innovation und nimmt den Plattformen die alleinige Macht über die Sichtbarkeit, ohne dass der Staat in die Inhalte eingreift.

3 Zur Klarnamenpflicht

Der Antrag fordert eine allgemeine Klarnamenpflicht zur Bekämpfung von Hass und Hetze. Wir warnen deutlich vor einer pauschalen und generellen Klarnamenpflicht im Frontend (öffentliches Profil). Diese gefährdet, zusätzlich zu den schon genannten Nachteilen, vulnerable Gruppen (z.B. Opfer von Stalking, politische Aktivisten in Autokratien) und die freie Meinungsäußerung. Stattdessen befürworten wir eine Auskunftsfähigkeit (Identifizierbarkeit im Backend), damit Strafverfolgungsbehörden bei Straftaten Täter ermitteln können (Grundsatz: „Anonymität für den Nutzer, Identifizierbarkeit für den Staat“).

Mit Blick auf vulnerable Gruppen setzt diese Lösung einen im Sinne der verbrieften Grundrechte tadellos funktionierenden Rechtsstaat voraus. Aktuelle Entwicklungen in anderen Rechtsräumen zeigen, dass eine Identifizierbarkeit für den Staat eben auch zu lasten vulnerabler Gruppen missbraucht werden kann und statt eines Verursacherprinzips eine Einschränkung von Freiheitsrechten unbescholtener einhergeht. Entsprechend sorgfältig gilt es die Argumente abzuwägen. Anders als die Antragstellerin beantragt, ist sogar im

Teledienstedatenschutzgesetz (TDDDK) das exakte Gegenteil geregelt. Nach §19 (2) hat der Anbieter die anonyme oder pseudonyme Nutzung sogar zu ermöglichen.

Empirie zur „Enthemmung“: So zeigen Studien, dass Klarnamenpflichten das Niveau von „Hate Speech“ nicht signifikant senken. Eine Studie der Universität Zürich (Rost et al., 2016) belegt umgekehrt, dass aggressive Kommentare oft unter Klarnamen verfasst werden (Beispiel Facebook), da die soziale Erwünschtheit in polarisierten Gruppen (Echo-Kammern) das Hetzen belohnt.

Dort werden Klagen billigend in Kauf genommen, da diese häufig wegen Nichtigkeit ohnehin eingestellt werden. Löschaufforderungen kommen die Anbieter zudem häufig nicht oder nur extrem zögerlich nach. Hier wäre unserer Meinung nach eindeutlich gewichtigerer Hebel zu sehen.

Beispiel Südkorea: Südkorea führte 2007 eine Klarnamenpflicht („Internet Real-Name System“) ein. Sie wurde 2012 vom Verfassungsgericht als verfassungswidrig gekippt, da sie die Meinungsfreiheit einschränkte und es auch zu empfindlichen Hackerangriffen kam, während der Anteil bösartiger Kommentare nur minimal sank.

Rechtsdurchsetzung: Das Problem ist oft nicht nur die fehlende Identifizierbarkeit (Bestandsdaten sind oft vorhanden), sondern die mangelnde Kapazität der Staatsanwaltschaften und die langsame Kooperation der Plattformen. Regulatorisch greift an der Stelle der Digital Services Act (DSA) der EU bereits, den es konsequent anzuwenden gilt. Es gilt auch hier der Grundsatz, dass zunächst einmal das geltende Recht durchzusetzen ist, anstelle der Schaffung stetig neuer, wenig wirksamer Gesetze, da deren Durchsetzbarkeit von vornherein in Frage zu stellen ist.

4 Zum Social-Media-Verbot unter 16 Jahren

Der Antrag fordert ein gesetzliches Mindestalter von 16 Jahren für offene soziale Netzwerke nach australischem Vorbild.

Ein starres Verbot schließt Jugendliche von gesellschaftlicher Teilhabe, dem Grundrecht auf Information, der Meinungsfreiheit und auch politischer Information unberechtigt aus, ohne wirksam das Problem zu bekämpfen. Vor allem fördert es die Nutzung von Umgehungstechnologien (VPNs) und verlagert Kommunikation in unregulierte Räume („Dark Social“). Diese Entwicklung ist beispielsweise auch in Australien zu beobachten, wo ein entsprechendes Verbot wirksam ist. Zudem haben die Anbieter dort die Schwellen so tief angesetzt, dass ein Umgehen durch simple Veränderung des Geburtsdatums erfolgen kann oder Fake-Identitäten geschaffen wurden, was noch ganz andere Probleme auslöst. Diese Erfahrungen sind schon seit Tag eins in Australien zu beobachten.

Wir plädieren daher für **„Care by Design“** Ansatz, bei dem das psychische Wohlbefinden, die Sicherheit und die mentale Gesundheit der Nutzenden in den Mittelpunkt der Plattformarchitektur gestellt werden. Mit Blick auf vulnerable Gruppen können so auch verpflichtende, altersgerechte Voreinstellungen (z.B. keine algorithmischen Feeds für U16, Zeitlimits), die über Betriebssysteme (Apple/Google) oder Plattformen gesteuert werden.

Die Plattformbetreiber müssen hart aufgefordert werden bestimmte Einflüsse konsequent zu unterbinden, wo die Folgen a priori schon bekannt sind (Extremismus, Hatespeech, Mobbing, Essstörungen, irreführende Werbung etc.). Es geht darum, dass die Plattformbetreiber entweder ihrer Verpflichtung nachkommen oder dann tatsächlich in gestuften Verfahren empfindlich bestraft werden um diese hierzu klar aufzufordern. Hier sind es letzten Endes also die Bereitsteller von Infrastruktur für Kommunikatoren, nicht die Rezipienten, die zu handeln haben. Ein Social-Media-Verbot wirkt wie eine Strafe für die Fehler der Anbieter bzw. der Kommunikatoren nicht erwünschter Inhalte. Außerdem könnten Time-Limits (Automatische Abschaltung nach X-Minuten Nutzung täglich) zudem Suchttendenzen unkritisch entgegenwirken. Weitere Beratungen können zu sehr viel konsentierteren und tragfähigen Lösungen führen – und Akzeptanz!

Medienkompetenz vs. Verbot: Die jüngere Forschung zur Medienkompetenz zeigt, dass Verbote den Erwerb von Risikokompetenz („Media Literacy, Data Literacy, AI Literacy“) verhindern. Jugendliche müssen lernen, mit Risiken umzugehen, statt isoliert zu werden. Dazu bedarf es Hilfestellungen, Aufklärung und vor allem auch ein Erlernen guten Umgangs in geeigneten Institutionen.

Das „Australische Modell“: Der im Antrag als Vorbild genannte „Social Media Ban“ in Australien (Z. 76) ist international höchst umstritten und wenig erfolgreich, wie jüngere Berichte belegen. Experten für digitale Sicherheit warnen, dass die dafür notwendige Altersverifikation (Age Assurance) massive Datenschutzrisiken birgt. Um das Alter effektiv zu prüfen, müssten Millionen Bürger Ausweisdokumente oder biometrische Daten (Face Scanning) an private Konzerne oder Drittanbieter übermitteln.

Verfassungsrechtliche Bedenken: Ein Pauschalverbot könnte zudem gegen die UN-Kinderrechtskonvention (Recht auf Zugang zu Informationen/Medien, Art. 17 UN-Kinderrechtskonvention) verstoßen.

5 Zur Digitalabgabe für Plattformen

Der Antrag fordert eine nationale Abgabe für Plattformen mit mehr als 45 Mio. Nutzern zur Finanzierung des lokalen Journalismus.

Ein starker Lokaljournalismus und Medienvielfalt sind zweifelsohne wichtige Bestandteile des demokratischen Willensbildungsprozesses. Eine nationale Sonderabgabe („Digitalsteuer durch die Hintertür“) ist jedoch rechtlich fragil und könnte im Ergebnis dem Standort Deutschland mehr schaden als nützen zumal diese wettbewerbsrechtlich nicht haltbar sein dürfte, da ein Marktversagen künstlich konstruiert wird.

Auch würde ein Umverteilungssystem etabliert werden müssen, welches die marktwirtschaftlichen Grundprinzipien ad absurdum führen würde. Mit Blick auf die skizzierte Problemlage unfairer Wettbewerbsbedingungen wirken die Durchsetzung des Urheberrechts (Leistungsschutzrecht) und kartellrechtliche Maßnahmen über den Digital Markets Act (DMA) deutlich zielgerichteter.

Dies bedeutet nicht, dass es nicht erforderlich ist, dass digitale Plattformbetreiber, die in der EU generierten Umsätze auch adäquat, ggf. auch deutlich höher als bisher in der EU versteuern müssen. Die Diskussion um eine Digitalsteuer/-abgabe sollte aber nicht mit der Fragen der Quersubvention anderer Medienanbieter vermischt werden.

Link-Tax-Erfahrungen: Versuche in Spanien oder Kanada, Plattformen zur Zahlung für Links zu zwingen, führten in der Vergangenheit oft dazu, dass Plattformen (wie Meta/Google) Nachrichtenangebote in diesen Ländern einfach abschalteten (News Deprioritization). Dies schadete den Verlagen mehr, als es nutzte (Traffic-Einbruch). Die Frage des Leistungsschutzrechts ist weiterhin in der existierenden Form umstritten.

EU-Harmonisierung: Nationale Alleingänge im digitalen Binnenmarkt führen zu Fragmentierung. Lösungen müssen auf EU-Ebene (OECD-Steuerabkommen Pillar 1 & 2) erfolgen.