Bayerischer Landtag

19. Wahlperiode 21.05.2026 **Drucksache** 19/**12101**

Dringlichkeitsantrag

der Abgeordneten **Katrin Ebner-Steiner, Ulrich Singer, Christoph Maier, Richard Graupner, Andreas Winhart, Johannes Meier, Gerd Mannes, Benjamin Nolte, Markus Walbrunn, Florian Köhler, Oskar Lipp** und **Fraktion (AfD)**

Digitale Freiheitsräume sichern – Meinungsfreiheit, Transparenz und grundrechtsschonenden Jugendmedienschutz im Digitale Medien-Staatsvertrag verankern!

Der Landtag wolle beschließen:

Die Staatsregierung wird aufgefordert,

– sich im Rahmen der Verhandlungen zum zweiten Teil des Digitale Medien-Staatsvertrags dafür einzusetzen, dass digitale Plattformen und digitale Plattformmärkte im Sinne der Meinungsfreiheit, der Transparenz, der Medienvielfalt und eines grundrechtschonenden Jugendmedienschutzes reguliert werden;

– sich dafür einzusetzen, dass die Regulierung sozialer Netzwerke und digitaler Plattformen nicht auf unbestimmte politische Begriffe wie „Desinformation“, „Hass“, „Hetze“ oder „Delegitimierung“ gestützt wird, sondern sich bei rechtlichen Eingriffen strikt an klar bestimmten gesetzlichen Grenzen orientiert, insbesondere an Strafrecht, Jugendmedienschutz, Persönlichkeitsrecht und Datenschutz;

– sich dafür einzusetzen, dass ein pauschales Social-Media-Verbot oder ein generelles Nutzungsverbot sozialer Medien für Kinder und Jugendliche nicht eingeführt wird;

– sich dafür einzusetzen, dass der Schutz von Kindern und Jugendlichen im digitalen Raum vorrangig an der Erziehungsverantwortung der Eltern nach Art. 6 Grundgesetz ausgerichtet wird und staatliche Maßnahmen diese Verantwortung unterstützen, aber nicht ersetzen;

– sich dafür einzusetzen, dass digitale Plattformen nach dem Prinzip „Safety by Design“ verpflichtet werden, ihre Dienste von Anfang an minderjährigengerecht zu gestalten und suchtfördernde oder manipulative Funktionen wie Infinite Scrolling, Autoplay, unvorhersehbare Benachrichtigungen sowie verhaltensbasierte Beeinflussung Minderjähriger zu verbieten, stark einzuschränken oder einer strengen regulatorischen Überprüfung zu unterziehen;

– sich dafür einzusetzen, dass für Konten Minderjähriger standardmäßig wirksame Schutzmechanismen gelten, insbesondere leicht verständliche Begrenzungen von Onlinezeiten, Nutzungsunterbrechungen nach bestimmten Zeitspannen, Nachtzeitsperren sowie einfache elterliche Konfigurationsmöglichkeiten für Social-Media-Zugänge;

– sich auf Bundes- und EU-Ebene dafür einzusetzen, dass Betriebssystemhersteller einfache, verständliche und wirksame gerätebasierte Alters- und Schutzkonfigurationen bereitstellen, damit Eltern und Schulen Geräte altersgerecht einstellen können, ohne personenbezogene Daten an Plattformen, Drittanbieter oder zentrale Stellen weiterzugeben;

– sich dafür einzusetzen, dass Altersnachweise nur dort verlangt werden, wo sie sachlich zwingend notwendig sind, und dass sie dezentral, datensparsam, ohne zentrale Identitätsdatenbanken und ohne Verknüpfung von Onlineaktivitäten mit realen Identitäten ausgestaltet werden;

– sich dafür einzusetzen, dass zentrale Stellen die Bürger für die Nutzung des Internets oder einzelner digitaler Dienste „freigeben“ sowie zentrale Identitätsdatenbanken für digitalen Jugendmedienschutz ausgeschlossen werden;

– sich dafür einzusetzen, dass Betreiber digitaler Plattformen die Grundlogik und Wirkungsweise ihrer Empfehlungs-, Ranking- und Moderationsalgorithmen für Nutzer verständlich offenlegen und leicht auffindbare Opt-out-Möglichkeiten aus personalisierten oder engagement-optimierten Feeds bereitstellen;

– sich dafür einzusetzen, dass Shadow Banning, also die verdeckte Reichweitenbeschränkung, Depriorisierung oder Sichtbarkeitsminderung von Inhalten oder Nutzerkonten ohne nachvollziehbare Mitteilung und Begründung, verboten wird;

– sich dafür einzusetzen, dass Plattformnutzer bei Löschungen, Sperrungen, Reichweitenbeschränkungen und algorithmischen Benachteiligungen eine klare Begründung sowie eine niedrigschwellige, kostenlose und wirksame Beschwerdemöglichkeit erhalten;

– sich dafür einzusetzen, dass keine staatlich oder regulatorisch privilegierte Sichtbarkeit einzelner Medienakteure, „verifizierter Journalisten“ oder sonstiger zertifizierter Meinungsträger eingeführt wird und dass digitale Medienvielfalt einschließlich alternativer Medien, Blogger, unabhängiger Publizisten und neuer journalistischer Formate gewahrt bleibt;

– sich dafür einzusetzen, dass alle Maßnahmen zum Schutz von Kindern und Jugendlichen sowie zur Regulierung digitaler Plattformen einer systematischen Grundrechtsprüfung unterzogen, technologieneutral formuliert und strikt am Grundsatz der Verhältnismäßigkeit ausgerichtet werden.

Begründung:

Der zweite Teil des Digitale Medien-Staatsvertrags soll die Medienordnung der Länder an digitale Plattformen, soziale Netzwerke, KI-Systeme, neue Formen politischer Online-Kommunikation und die veränderte öffentliche Meinungsbildung anpassen. Die Rundfunkkommission der Länder hat hierfür am 22. Oktober 2025 Eckpunkte beschlossen. Diese betreffen unter anderem soziale Netzwerke, Plattformmacht, Manipulation, Auffindbarkeit journalistischer Inhalte, Medienvielfalt, Medienkonzentration und eine modernisierte Medienaufsicht. Für Bayern ist deshalb entscheidend, dass die Verhandlungen nicht zu einer Ausweitung staatlicher oder staatsnaher Kontrolle über digitale Debattenräume führen, sondern die grundrechtlichen Freiheitsgarantien der Bürger sichern. Der Digitale Medien-Staatsvertrag darf nicht zum Instrument einer politischen Steuerung digitaler Sichtbarkeit werden. Er muss Meinungsfreiheit, Medienvielfalt, Transparenz und Jugendmedienschutz miteinander verbinden (Rundfunkkommission der Länder, 22.10.2025).

Soziale Netzwerke, Suchmaschinen, Videoportale und andere digitale Intermediäre bestimmen heute maßgeblich, welche Inhalte sichtbar werden, welche Debatten Reichweite erhalten und welche Stimmen im öffentlichen Raum wahrgenommen werden. Diese Machtstellung rechtfertigt Transparenzpflichten, aber keine staatliche Wahrheitsverwaltung. Der Staat darf nicht selbst oder mittelbar über Plattformen entscheiden, welche rechtmäßigen politischen Meinungen als „Desinformation“, „Hass“ oder „Hetze“ zu behandeln sind. Diese Begriffe sind politisch aufgeladen, rechtlich häufig unscharf und deshalb als Grundlage zusätzlicher Eingriffe in legale Meinungsäußerungen ungeeignet. Maßgeblich bleiben die klar bestimmten gesetzlichen Grenzen: Strafrecht, Jugendmedienschutz, Persönlichkeitsrecht und Datenschutz. Was im analogen Raum

rechtmäßig geäußert werden darf, darf nicht im digitalen Raum unterhalb der Strafbarkeitsgrenze durch unbestimmte Regulierungsbegriffe faktisch verdrängt, herabgestuft oder kriminalisiert werden.

Gerade deshalb braucht es eine klare Trennung zwischen der Bekämpfung rechtswidriger Inhalte und der politischen Bewertung rechtmäßiger Meinungen. Illegale Inhalte müssen auf Grundlage geltenden Rechts verfolgt werden. Rechtmäßige, aber unbequeme, scharfe, polemische oder regierungskritische Meinungen sind hingegen vom Schutzbereich der Meinungsfreiheit umfasst. Eine freiheitliche Demokratie lebt davon, dass Bürger sich aus unterschiedlichen Quellen informieren, etablierte Medien kritisch hinterfragen und auch alternative Medien, Blogger, unabhängige Publizisten und neue digitale Formate nutzen können. Eine Bevorzugung bestimmter „verifizierter“ Akteure oder staatlich begünstigter Medienmarken würde den offenen digitalen Meinungsmarkt verzerren und neue Zugangshürden für unabhängige Stimmen schaffen.

Transparenz gegenüber den Nutzern ist dagegen zwingend erforderlich. Plattformen müssen verständlich offenlegen, nach welchen Grundprinzipien Inhalte empfohlen, sortiert, priorisiert, herabgestuft oder verborgen werden. Nutzer müssen eine echte Wahl haben, ob sie personalisierte, hinsichtlich ihres Engagements optimierte Feeds verwenden oder eine neutralere, nicht manipulative Darstellung nutzen wollen. Ein leicht auffindbarer Opt-out aus algorithmischer Personalisierung stärkt Selbstbestimmung, ohne die Kommunikationsfreiheit einzuschränken. Ebenso muss Shadow Banning verboten werden. Eine verdeckte Reichweitenbeschränkung ohne Mitteilung und ohne wirksame Beschwerdemöglichkeit untergräbt die Meinungsfreiheit, weil Betroffene ihre Benachteiligung kaum erkennen und daher nicht effektiv dagegen vorgehen können.

Der Schutz von Kindern und Jugendlichen im digitalen Raum ist ein legitimes und wichtiges Ziel. Er darf jedoch nicht dazu führen, dass alle Bürger einer flächendeckenden digitalen Identifizierung unterworfen werden. Pauschale Social-Media-Verbote für Kinder und Jugendliche oder generelle Alterskontrollen für große Teile des Internets würden tief in die Informationsfreiheit, die Kommunikationsfreiheit, die informationelle Selbstbestimmung und die anonyme Teilhabe am digitalen Raum eingreifen. Ein solcher Ansatz bekämpft zudem nicht die eigentliche Ursache vieler Gefahren, nämlich manipulative und suchtverstärkende Plattformarchitektur. Der wirksamere und grundrechtsschonendere Weg liegt darin, Plattformen zur sicheren Gestaltung ihrer Dienste zu verpflichten.

Das Prinzip „Safety by Design“ setzt genau dort an. Plattformen dürfen Minderjährige nicht durch Endlos-Feeds, Autoplay, unvorhersehbare Benachrichtigungen, variable Belohnungsmechanismen und verhaltensbasierte Beeinflussung möglichst lange an ihre Dienste binden. Solche Funktionen schaffen künstliche Nutzungsschleifen und erschweren bewusste Pausen. Für Konten Minderjähriger müssen deshalb standardmäßig Schutzmechanismen gelten: verständliche Zeitbegrenzungen, Nutzungsunterbrechungen, Nachtzeitsperren, deaktivierte oder eingeschränkte manipulative Empfehlungen sowie einfache elterliche Steuerungsmöglichkeiten. Die DAK-Gesundheit und das Universitätsklinikum Hamburg-Eppendorf betrachten in Deutschland 4,7 Prozent der 10- bis 17-Jährigen als pathologische Nutzer sozialer Medien und sehen bei weiteren 21,1 Prozent ein riskantes Nutzungsverhalten. Diese Zahlen zeigen einen realen Handlungsbedarf, rechtfertigen aber keinen Überwachungsstaat im digitalen Raum (DAK-Gesundheit und Universitätsklinikum Hamburg-Eppendorf, Ergebnisbericht 2024/2025).

Die vorrangige Verantwortung für die Erziehung von Kindern liegt nach Art. 6 Grundgesetz bei den Eltern. Der Staat hat diese Verantwortung zu achten und zu unterstützen. Er darf sie nicht durch pauschale Verbote, zentrale Freigabestellen oder verpflichtende Identifizierungsinfrastrukturen ersetzen. Eltern und Schulen brauchen praktikable technische Werkzeuge, um Geräte altersgerecht einzurichten, Nutzungszeiten zu begrenzen und altersgemäße Schutzstufen festzulegen. Deshalb sind gerätebasierte Alters- und Schutzkonfigurationen auf Betriebssystemebene vorzugswürdig. Sie ermöglichen wirksamen Schutz unmittelbar am Gerät, ohne dass Kinder, Eltern oder andere Nutzer ihre Identität gegenüber Plattformen, Drittanbietern oder zentralen Stellen offenlegen müssen.

Altersnachweise dürfen nur dort eingesetzt werden, wo sie sachlich zwingend notwendig sind. Wo sie unvermeidbar sind, müssen sie dezentral, datensparsam und ohne Profilbildung funktionieren. Eine Verknüpfung von Onlineaktivitäten mit realen Identitäten muss ausgeschlossen bleiben. Zentrale Identitätsdatenbanken, Ausweis-Uploads, biometrische Gesichtsscans oder zentrale Stellen, die Bürger für den Zugang zum Internet „freigeben“, schaffen erhebliche Datenschutz-, Sicherheits- und Freiheitsrisiken. Mehr als 400 Sicherheits- und Datenschutzwissenschaftler aus über 30 Ländern haben am 2. März 2026 vor den gesellschaftlichen, technischen und grundrechtlichen Risiken umfassender Altersverifikationssysteme gewarnt. Sie verweisen auf zweifelhafte Wirksamkeit, erhebliche Datenschutzrisiken, mögliche Diskriminierung und die Gefahr zentralisierter Zugangskontrolle. (Joint statement of security and privacy scientists and researchers on Age Assurance, 02.03.2026)

Auch der Chaos Computer Club lehnt pauschale Social-Media-Verbote und invasive Altersverifikationssysteme ab. Die Gefahr liegt nicht nur in einzelnen Datenabfragen, sondern in der Schaffung einer dauerhaften Infrastruktur digitaler Identifizierung. Was zunächst mit Jugendschutz begründet wird, kann später auf andere Inhalte, Dienste oder politische Zwecke ausgeweitet werden. Dieses Risiko eines schleichenden Funktionswandels ist bei jeder Regelung mitzudenken. Ein freiheitlicher Jugendmedienschutz muss Kinder schützen, ohne anonyme Kommunikation, vertrauliche Informationssuche und die offene Teilhabe am digitalen Raum zu beschädigen (Chaos Computer Club, 2026).

Internationale Beispiele zeigen zudem, dass harte Altersgrenzen und technische Sperren leicht umgangen werden können und häufig Ausweichreaktionen auslösen. Der britische Online Safety Act führte nach Inkrafttreten strengerer Alterskontrollen zu einem starken Anstieg der VPN-Nutzung. Damit wird deutlich, dass pauschale Sperr- und Identifizierungsmodelle nicht automatisch wirksameren Kinderschutz schaffen, sondern vielfach neue Umgehungsstrategien, neue Datensammlungen und zusätzliche Eingriffe in die digitale Freiheit erzeugen (CNBC, 2025; heise online, 2025).

Der Digitale Medien-Staatsvertrag muss deshalb eine freiheitliche Alternative festschreiben: transparente Plattformregeln statt verdeckter Reichweitensteuerung, Nutzerautonomie statt paternalistischer Feed-Kontrolle, konsequente Anwendung des geltenden Rechts statt unbestimmter Meinungskategorien, Elternrechte statt staatlicher Erziehungsersatz, Safety by Design statt zentraler Altersdatenbanken. Bayern muss sich in den Verhandlungen dafür einsetzen, dass digitale Räume sicherer werden, ohne sie in kontrollierte Zugangszonen umzubauen. Ziel ist ein digitaler Ordnungsrahmen, der Minderjährige wirksam vor manipulativen Plattformdesigns schützt, die Meinungsfreiheit aller Bürger wahrt und die offene, vielfältige und anonyme Teilhabe im digitalen Raum erhält.