


Stephan Dreyer

Instagram, TikTok und Co.: Mehr Schutz für Kinder und Jugendliche

Stellungnahme zu dem
Entschließungsantrag von SPD und
Bündnis 90/Die Grünen
(Niedersächsischer Landtag Drs. 19/7489)

Hamburg, Januar 2026



Inhalt

Inhalt	2
1. Zur Einordnung	3
2. Einführung eines Mindestalters für Social-Media-Plattformen	3
3. Kinder- oder Jugendprofile für Social-Media-Plattformen	6
4. Förderung von Awareness und Medienkompetenz	7
5. Verpflichtung von Anbietern zur Schaffung von Datenzugängen für die Medienaufsicht	8
6. Erleichterung datenschutzrechtlicher Auskunftsansprüche	9
7. Erleichterung von Auskunftsansprüchen Privater oder Aufsichtsbehörden gegenüber digitalen Diensten	11
8. Vorbehalt der Einführung einer Klarnamenpflicht	12
9. Wirtschaftliche Entflechtung von TikTok	13
10. Fazit und Ausblick	13

1. Zur Einordnung

Im Juni 2026 haben die Fraktionen von SPD und Bündnis 90/Die Grünen einen Entschließungsantrag in den Niedersächsischen Landtag eingebracht, der unter dem Titel „Instagram, TikTok und Co.: Mehr Schutz für Kinder und Jugendliche – Falsch- und Desinformationen eindämmen“ ein Bündel von Maßnahmen vorschlägt. Der Antrag reagiert auf die wachsende Besorgnis über die Auswirkungen sozialer Medien auf Minderjährige, ähnliche Überlegungen und Diskussionen sind derzeit auch in anderen Bundesländern, auf Bundesebene sowie auf Ebene der EU zu beobachten.

In den letzten Jahren haben Einzelereignisse und eine Reihe von Studien die Risiken der Nutzung von Online-Plattformen durch Minderjährige betont: Kinder und Jugendliche können dort mit Desinformation, Hassrede, extremistischen Inhalten, Cybermobbing und sexualisierter Ansprache konfrontiert werden. Zugleich mehren sich Studien, die Zusammenhänge zwischen bestimmten Formen der Social-Media-Nutzung und psychischen Beeinträchtigungen oder Störungen sehen, wie z.B. verstärkter Leistungs- und Schönheitsdruck, der wiederum mit Körperunzufriedenheit, Angst- oder Essstörungen oder Depressionen korrelieren. Als Reaktion erleben wir (wieder) verstärkt Regulierungsdebatten: Griechenland hat seit Oktober ein Mindestalter von 15 Jahren für die Nutzung von Social Media eingeführt, Dänemark und Frankreich planen für 2026 ein Verbot sozialer Netzwerke für dieses Alter und in Australien gilt das Social-Media-Mindestalter von 16 seit Anfang Dezember. Derweil diskutieren Expert*innenkommissionen auf EU- und auf Bundesebene über mögliche Regelungen für Europa bzw. Deutschland.

Parallel dazu gilt in der EU seit Februar 2024 der Digital Services Act (DSA), der für Online-Plattformen Pflichten zur Einziehung struktureller Maßnahmen zum Schutz Minderjähriger und strengere Pflichten zur Minimierung systemischer Risiken bei sehr großen Online-Plattformen vorsieht. Der niedersächsische Entschließungsantrag muss als Teil dieser Entwicklungen gesehen werden, in der Gesetzgeber nach neuen Schutzinstrumenten und -mechanismen suchen. Diese Stellungnahme bewertet die einzelnen Forderungen und Vorschläge aus Sicht der Medienforschung und mit Blick auf die bereits bestehenden Ordnungsrahmen.

2. Einführung eines Mindestalters für Social-Media-Plattformen

Der Entschließungsantrag regt in Nr. 1 an, auf Bundesebene die Debatte über ein „gesetzliches Mindestalter von 14 Jahren für die Nutzung von sozialen Medien“ anzustoßen. Die gesetzliche Verpflichtung von Online-Plattformen durch eine Regelung auf Bundesebene trifft allerdings auf den Anwendungsvorrang der EU-Vorgaben durch den DSA. Der DSA ist vollharmonisierend, d.h. abschließend mit Blick auf mitgliedstaatliche Vorschriften, die gleiche Regelungszwecke wie der



DSA verfolgen. Da der DSA auch das Ziel des Minderjährigenschutzes auf Online-Plattformen hat, **sind nationale Gesetzesvorschriften, die Online-Plattformen zu diesem Zweck verpflichten, nicht anwendbar.**

Eine Möglichkeit, ein Mindestalter für Social-Media-Angebote auf nationaler Ebene einzuführen und anzuwenden, zeigt allerdings das Beispiel aus Griechenland. Dort werden – anders als in Australien eingeführt und in Frankreich und Dänemark geplant – nicht die Plattformanbieter zur Umsetzung der Einhaltung des Mindestalters verpflichtet, sondern neue Endgeräte (insb. Smartphones) werden mit einer vom Staat entwickelten und vorgehaltenen App ausgestattet, auf der Eltern für sich oder für ihre Kinder einen elektronischen Altersnachweis hinterlegen. Ist die Nutzerin bzw. der Nutzer des Endgeräts unter 15 Jahre alt, sorgt die App auf dem Gerät dafür, dass Social-Media-Apps nicht installiert bzw. gestartet werden und die Angebote in einem Browser nicht aufgerufen werden können. Da sich das griechische Gesetz nicht an die Anbieter von Online-Plattformen richtet, weist es einen anderen Anwendungsbereich als der DSA auf und begegnet (jedenfalls in dieser Hinsicht) nicht den beschriebenen europarechtlichen Bedenken.

Eine Alternative zur Umsetzung der Forderung Nr. 1 kann der Anstoß von Aktivitäten und Initiativen auf Bundesebene sein, sich wiederum auf Ebene der EU für die Einführung eines Mindestalters einzusetzen. Die **Bundesregierung hat hier bereits Position in diese Richtung bezogen** (siehe etwa die von den Bundesminister*innen Prien und Wildberger unterzeichnete Jutland Declaration v. 10.10.2025¹).

Die Effektivität und Verhältnismäßigkeit der Schaffung einer gesetzlichen starren Altersgrenze für Onlineangebote, die eine große Vielzahl unterschiedlicher und überwiegend jugendschutzrechtlich irrelevanter oder gar positiver Inhalte vorhalten, ist allerdings umstritten. Befürworter argumentieren, dass Jüngere besonders schutzbedürftig sind und von beeinträchtigenden Inhalten und Funktionen konsequent ferngehalten werden sollten. So zeigen Untersuchungen, dass gerade in der Altersgruppe ab 10 soziale Medien vermehrt (Instagram: 26%; TikTok: 46%) und ab 12 intensiv (Instagram: 46%; TikTok: 71%) genutzt werden² und Eltern oft Schwierigkeiten haben, die Nutzung zu begleiten oder zu begrenzen. Ein gesetzlich bestimmtes Einstiegsalter könnte hier eine Art „Puffer“ schaffen, in dem die Persönlichkeitsentwicklung stabiler verläuft, bevor Jugendliche auf sämtliche Inhalte und Funktionen von sozialen Medien treffen.

Gleichwohl ist fraglich, ob ein gesetzliches Verbot unter 14 in der Praxis durchsetzbar ist. Dafür erforderlich wäre faktisch eine **flächendeckende Altersüberprüfung bei neuen und existierenden Accounts**. Deren Einführung wiederum wirft Verhältnismäßigkeitsfragen auf (s. dazu ausführlich Abschnitt 3).

¹https://www.digmin.dk/Media/638956829775203140/DIGMIN_The%20Jutland%20Declaration%20Shaping%20a%20Safe%20Online%20World%20for%20Minors%20101025.pdf

² mpfs, KIM-Studie 2024, <https://mpfs.de/app/uploads/2025/05/KIM-Studie-2024.pdf>, S. 46.

Zudem könnte eine starre Altersgrenze **Elternrechte berühren**: Nach Art. 6 Abs. 2 GG haben Eltern das Primat der Erziehung. Manche Eltern gestatten ihren Kindern bewusst früher eine beschränkte (teils beaufsichtigte oder gar begleitete) Social-Media-Nutzung, um Medienkompetenz und soziale Vernetzung zu fördern. Ein gesetzliches Verbot schränkte ihren Gestaltungsspielraum ein. Es müsste daher mit Blick auf den Verhältnismäßigkeitsgrundsatz geprüft werden, ob mildere Mittel – insbesondere eine Pflicht zur altersangemessenen Gestaltung von Online-Plattformen – den Schutzzweck ebenso erreichen könnten. Schließlich verlangt Art. 3 UN-KRK, dass bei allen Maßnahmen das Kindeswohl im Vordergrund steht; dazu gehört auch der **Ausgleich zwischen Schutz und Teilhaberechten**. Kinder haben gemäß Art. 13 UN-KRK ein Recht auf freie Meinungsäußerung und gemäß Art. 17 ein Recht auf Informationen aus vielfältigen Quellen. Ein pauschales Nutzungsverbot bis 14 stellte – jedenfalls für 13-Jährige, die in den Nutzungsbedingungen vorgesehene Mindestalter erreicht haben – einen Eingriff in diese Beteiligungsrechte dar, der nur zulässig wäre, wenn er zum Schutz der Gesundheit oder Entwicklung der Kinder **erforderlich und angemessen** ist. Dafür wäre auf empirische Evidenz abzustellen, die Studienlage kann hier aber keine eindeutige kausale Verbindung zwischen der allgemeinen Nutzung von Social Media-Angeboten von 13-Jährigen und nachhaltigen Entwicklungsstörungen ziehen. Dafür sind die Störungen bzw. Erkrankungen und die Wirkungszusammenhänge mit der Nutzung digitaler Medien zu komplex. Die Verhältnismäßigkeit einer Mindestaltersregelung hinge also davon ab, ob Entwicklungs- oder Gesundheitsgefahren unterhalb der intendierten Altersgrenze hinreichend nachgewiesen werden und keine mildereren Alternativen bestehen.

Schließlich würde die Schaffung eines Mindestalters die Plattform **aus der bestehenden Verantwortung entlassen**: Die Pflicht zur Schaffung altersangemessener Angebote war und ist ein gesetzliches Gebot aus Art. 28 Abs. 1 DSA, das dann leerläuft, wenn die Plattformanbieter Jüngere von ihren Plattformen fernhalten müssen. Zusammen mit den Möglichkeiten der leichten Umgehung der Altersüberprüfung betrachtet, würde ein gesetzliches Verbot für Nutzer unterhalb des Mindestalters, die sich dennoch Zugang zu einer Plattform verschaffen, das **Schutzniveau insgesamt verringern**. Alternativ könnten sich zu junge Nutzerinnen und Nutzer Plattformangebote außerhalb des räumlichen Anwendungsbereichs, die sich den deutschen und europäischen rechtlichen Vorgaben zum Jugendschutz vollständig entziehen. Auch das wäre mit Blick auf das Schutzniveau für die betroffenen Kinder eine Entwicklung in die falsche Richtung.

Im Ergebnis erscheint die Forderung gut gemeint, in der Umsetzung aber juristisch und faktisch anspruchsvoll. Sie berührt die Grundrechte der Kinder und der Eltern, sowie durch eine flächendeckende Altersüberprüfung auch die Informations- und Kommunikationsrechte aller erwachsenen Bürgerinnen und Bürger.



3. Kinder- oder Jugendprofile für Social-Media-Plattformen

Nr. 2 des Entschließungsantrags regt an, im Zuge der Mindestalterdebatte zu prüfen, ob Minderjährigen der Zugang zu sozialen Medien **ausschließlich über spezielle Kinder- und Jugendkonten** ermöglicht werden kann. Derartige Jugendprofile sollen durch „*verbindliche, staatlich gestützte Altersverifikation*“ abgesichert sein. Die Idee dahinter ist, ein *Zwei-Klassen-System* von Benutzerkonten zu schaffen: Verifizierte Minderjährige dürften nur einen eingeschränkten, besonders geschützten Accounttyp nutzen, während Erwachsenen ein normales Konto inklusive aller Funktionen offensteht. Praktisch könnte dies bedeuten, dass z.B. Inhalte ab 18 für Jugendkonten ausgefiltert, Kontaktfunktionen beschränkt, algorithmische Feed-Zusammenstellungen altersgerecht zusammengestellt oder Zeitlimits implementiert werden.

Einige Social Media-Plattformen verfolgen bereits solche Ansätze einer altersgerechten Ausgestaltung – etwa Instagram, das neue Nutzer unter 16 standardmäßig auf *privat* setzt und Fremdkontakt erschwert (sog. Teen Accounts). Aus Sicht des Verfassers ist eine solche Einführung besonders geschützter Profile für Jüngere bislang gesetzlich nicht gefordert worden, könnte aber bei einer streng kinderrechtsorientierten Interpretation bereits jetzt aus Art. 28 Abs. 1 DSA zu lesen sein. Würde die EU-Kommission als zuständige Aufsichtsbehörde für sehr große Online-Plattformen sich einer solchen Sichtweise anschließen, könnte sie auf entsprechende Kinder- oder Jugendprofile auf den sehr großen Online-Plattformen hinwirken. In diese Richtung sind auch die Leitlinien der EU-Kommission zu Art. 28 Abs. 1 DSA zu lesen. Besonders abgesicherte Minderjährigenprofile, die mit steigendem Alter mehr Funktionen und Inhalte freigeschaltet bekommen, erscheinen als **gute Praxis altersangemessener Angebotsgestaltung** und sind zu unterstützen.

Kernherausforderung im Umfeld solcher Kinderprofile bliebe aber die Frage einer gesetzlich verpflichtenden **Altersüberprüfung**: Je nach den konkreten Vorgaben für ihre Umsetzung können eine Reihe widerstreitender Rechtspositionen und die Grundfrage der Verhältnismäßigkeit einer solchen gesetzlichen Vorgabe berührt sein. Eine *verbindliche Altersverifikation* könnte verschiedene Formen annehmen, so etwa die Vorlage von Ausweisdokumenten, eine Altersschätzung anhand einer Webcam-Aufnahme oder die Nutzung eines digitalen Alters- oder Identitätsnachweises. Im Beschluss wird hier die geplante *EU-Digital Identity Wallet* ins Spiel gebracht, die eine datenschutzfreundliche Altersbestätigung ermöglichen soll. Diese technische Lösung steht bislang noch am Anfang, das derzeit laufende Pilotprojekt ist bisher nur geeignet für den Nachweis der Volljährigkeit (d.h. Altersgrenze 18). Von einer breiten Verfügbarkeit der Technologie, die eine flächendeckende Altersüberprüfung aber implizieren würde, kann derzeit nicht ausgegangen werden. Aktuell greifen verfügbare Altersüberprüfungsansätze auf Dokumenten-Uploads, biometrische Altersschätzung oder Kreditkartendaten zurück – alles **Methoden, die jeweils**

Schwachstellen aufweisen, etwa im Hinblick auf die Verarbeitung sensibler Kreditkarten- oder Ausweisdaten oder biometrische Verfahren mit möglicher Fehlerquote.

Die derzeitigen Verfahren können zudem relativ leicht von versierten Kindern **umgangen werden**, etwa durch den Einsatz von VPN-Diensten, durch die Nutzung elterlicher Dokumente bzw. Kreditkarten oder durch die Verwendung von erwachsen aussehenden KI-Avataren (Beispiel Großbritannien).

Die **Verhältnismäßigkeit** einer gesetzlich vorgegebenen Altersüberprüfung für Social Media-Angebote **hängt stark von ihrer konkreten Ausgestaltung ab**. Aus Sicht des Verfassers muss die Implementation einer solchen Pflicht vor der Entscheidung einer gesetzlichen Grundlage vollständig zu Ende gedacht sein, um im Rahmen einer Gesetzesfolgenabschätzung die Verhältnismäßigkeit der Maßnahmen gut nachweisen zu können.

4. Förderung von Awareness und Medienkompetenz

Punkt 3 des Entschließungsantrags fordert eine „zielgerichtete Förderung von Medienkompetenz im schulischen Kontext“, um die **Informations- und Nachrichtenkompetenz** von Kindern und Jugendlichen breit zu verbessern. Insbesondere sollen junge Menschen lernen, bewusst mit sozialen Medien umzugehen, Desinformation zu erkennen sowie Schutz vor Cybermobbing und Onlinegefahren zu entwickeln. Diese Bildungsziele sollen im Rahmen der Lehrpläne weiter gestärkt werden, u.a. durch die Zusammenarbeit mit externen Partnern wie der NLM und der Landeszentrale für politische Bildung. Auch Eltern sollen im Kontext ihres Erziehungsauftrags durch Erwachsenenbildung gezielt unterstützt werden. Dieser Schwerpunkt auf präventiver Bildung spiegelt das Prinzip wider, dass **Medienkompetenz eine Schlüsselstrategie** ist, um Jugendliche (und auch Eltern) zu resilienten und reflektierten Nutzern digitaler Medien zu machen.

Die Bedeutung von *Awareness* und *Medienkompetenz* beim Aufbau von Resilienz und zur Prävention wird in der Forschung einhellig betont. Studien zeigen, dass reine Verbote oder technische Schutzmechanismen allein nicht ausreichen; Jugendliche müssen auch selbst die Fähigkeiten entwickeln, mit problematischen Online-Inhalten umzugehen. Die Förderung von Awareness und Medienkompetenz ist aus wissenschaftlicher Sicht daher unumgänglich. Auch im Hinblick auf die Verhältnismäßigkeit begegnen entsprechende Maßnahmen und Initiativen keinen Bedenken: Sie greift nicht repressiv in Rechte ein, sondern **ermöglicht die Ausübung von Rechten**. Kinder werden dadurch etwa in die Lage versetzt, ihr Recht auf Information und freie Meinungsäußerung (Art. 5 GG, Art. 13 UN-KRK) sicherer auszuüben. Mittelbar kann Kompetenz auch die **Demokratie schützen**, weil junge Bürger lernen, Informationen kritisch zu prüfen und Manipulation zu erkennen – was angesichts gezielter politischer Desinformationskampagnen essenziell ist. Wichtig ist



die **nachhaltige Umsetzung**: Schulen benötigen aktualisierte Lehrpläne, Lehrkräfte Fortbildungen, und außerschulische Partner langfristige Finanzierung. Der Beschluss adressiert dies richtigerweise und fordert eine Intensivierung bereits bestehender Programme. Es sollte dabei allerdings evaluiert werden, welche Formate tatsächlich Verhalten ändern (z.B. praktische Workshops vs. bloßer Frontalunterricht); auch neue innovative Wege wie Gamification, projektbasiertes Lernen oder Co-Creation-Ansätze erscheinen hier erfolgversprechend.

5. Verpflichtung von Anbietern zur Schaffung von Datenzugängen für die Medienaufsicht

Unter Punkt 6 des Antrags wird eine gesetzliche Verankerung der Verpflichtung von Betreibern sehr großer Social-Media-Plattformen gefordert, der **Medienaufsicht automatisierte Datenzugänge** zu ermöglichen. Konkret sollen die Aufsichtsbehörden in Form der Landesmedienanstalten öffentliche Informationen auf den Plattformen (Posts/Inhalte, Kommentare, Accountnamen, Datum- und Reichweitendaten) per Schnittstelle durchsuchen und dokumentieren können. Es geht also um einen umfassenden *Schnittstellen-Zugang* für Aufsichtszwecke. Zudem wird erwähnt, die Landesmedienanstalt solle in diesem Zusammenhang gestärkt werden und datenschutzrechtliche Auskunftsansprüche der Nutzer verbessert werden (zu letzterem Thema siehe Abschnitt Nr. 5).

Die Forderung eines Datenzugangs für die Medienaufsicht muss zunächst **vor dem Hintergrund des bestehenden Regulierungsrahmens** durch den Digital Services Act betrachtet werden. **Artikel 40 Abs. 1 DSA** Mechanismen vor, um Behörden Zugang zu Plattformdaten zu geben. Die nationalen Koordinatoren für digitale Dienste und die EU-Kommission können darüber Auskünfte und Zugang zu Daten von den Diensten verlangen, um deren Compliance mit den Vorgaben des DSA zu überprüfen. Als über § 12 Abs. 2 DDG für konkrete Einzelmaßnahmen berechnete Stellen sind die Landesmedienanstalten über Art. 40 Abs. 1 DSA berechnigt, zur Klärung möglicher Verstöße gegen den DSA Datenzugang bei Online-Plattformen zu beantragen.

Der Antrag zielt vor diesem Hintergrund wohl darauf ab, den **Aufsichtsapparat mit besseren Werkzeugen** auszustatten. Ohne konkreten Verdacht können die Landesmedienanstalten derzeit keinen Antrag nach Art. 40 DSA stellen; Medienaufseher müssen bislang manuell nach möglichen Verstößen suchen oder auf Meldungen reagieren. Ein **Schnittstellenzugriff** würde erlauben, automatisiert etwa nach bestimmten rechtswidrigen Inhalten zu scannen (z.B. Gewaltverherrlichung, Pornografie, Volksverhetzung) und die Beweise zu sichern; einen entsprechenden Ansatz verfolgen die Landesmedienanstalten mit dem KI-basierten Tool KIVI. Im Vergleich zu den derzeitigen Aufsichtsinstrumenten kann ein unbeschränkter API-Zugriff in der **Skalierung und Geschwindigkeit** des Datenzugangs zu sehen sein; hier stoßen bisherige Kontrollen an Grenzen.

Im Lichte des Verhältnismäßigkeitsgrundsatzes müsste ein solcher Zugang zu Zwecken automatisierten Content-Monitorings strengen Anforderungen genügen, da eine allgemeine Aufsicht über eine gesamte Plattform per Datenschnittstelle nicht mehr ohne Weiteres von Art. 40 Abs. 1 DSA umfasst wäre: Ein legitimer Zweck (Jugendschutzaufsicht, Strafverfolgung) und die Geeignetheit lägen (wohl) vor. Ob ein vollständiger Datenzugang aber erforderlich und vor allem **angemessen wäre, bedürfte einer tiefergehenden Prüfung**. Eine eng umrissene Nutzung mit Datenschutzkonzept könnte hier eher angemessen sein als eine *pauschale Dauerüberwachung*. Zu erwarten ist zudem, dass sich auf Bundesebene Koordinierungsfragen stellen, um Überschneidungen mit der für den DSA zuständigen BNetzA und der für Art. 28 Abs. 1 DSA zuständigen BzKJ zu vermeiden.

6. Erleichterung datenschutzrechtlicher Auskunftsansprüche

Der Antrag fordert in Punkt 6, **datenschutzrechtliche Auskunftsansprüche der Benutzer*innen zu verbessern** und tatsächliche Hürden für deren Ausübung abzubauen. Gemeint sind hier insbesondere die Rechte, die Nutzer nach der Datenschutz-Grundverordnung (DSGVO) haben, namentlich das **Recht auf Auskunft** über die vom Anbieter verarbeiteten personenbezogenen Daten (Art. 15 DSGVO), ggf. Berichtigung, Löschung etc.

In der Praxis stoßen Nutzer – gerade junge Nutzer oder ihre Eltern – bei Social Media-Angeboten auf Schwierigkeiten, diese Rechte wahrzunehmen: Die Verfahren sind kompliziert, Fristen werden von Unternehmen überzogen oder es werden nur unvollständige Datenauskünfte geliefert. Die Beschlussformulierung deutet an, dass möglicherweise rechtspolitische Initiativen erwogen werden, um diese individuellen Rechte zu stärken. Daneben fällt in diesen Bereich auch das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG), das besondere Auskunftsansprüche konkret benannter Stellen in §§ 21-24 TDDDG enthält. Mögliche Gesetzesinitiativen könnten darauf abzielen, die Inanspruchnahmefähigkeit dieser Rechte durch Private zu erweitern.

Nach Art. 15 DSGVO kann jede Person von einem Dienst verlangen, „eine Bestätigung darüber zu erhalten, ob sie betreffende personenbezogene Daten verarbeitet werden, und wenn ja, welche und zu welchen Zwecken“. Dieses Auskunftsrecht umfasst auch Informationen über die Herkunft der Daten, Empfänger und geplante Speicherdauer. In sozialen Netzwerken bedeutet das: Ein Nutzer kann theoretisch erfahren, welche Daten (Profilangaben, Beiträge, Metadaten, Logs etc.) gespeichert sind. In der Praxis stellen die Plattformen meist Self-Service-Tools („Download your data“) zur Verfügung. Doch Studien und Beschwerden haben gezeigt, dass diese Datenauszüge oft **lückenhaft** sind, etwa im Hinblick auf abgeleitete Daten (Inferenz) oder interne Metriken. Nutzer wissen oft nicht, wie sie konkret an die gewünschten Informationen kommen oder wie sie feststellen können, ob etwas fehlt. Zudem ist vielen Jugendlichen gar nicht bewusst, dass sie ein solches Recht haben.



Ein Problem dabei ist die **Komplexität der Antragstellung**. Große Anbieter verweisen auf Online-Formulare in englischer Sprache oder verlangen Identitätsnachweise, was abschreckend wirken kann. Die **Umsetzungsfristen** (i.d.R. 1 Monat, verlängerbar auf 3) werden manchmal überschritten, oder die Antwort erfolgt in juristisch-technischer Sprache, die für Laien kaum verständlich ist. Verbesserungen könnten hier ansetzen, etwa durch gesetzliche Vorgaben für **standardisierte, leicht verständliche Datenauskünfte** (ggf. altersgerecht aufbereitet für Minderjährige). Auch denkbar ist ein *zentrales Portal* unter Aufsicht der Datenschutzbehörden, über das Nutzer gebündelt Auskunftersuchen an verschiedene Dienste stellen können – was gerade für Jugendliche hilfreich wäre, die nicht jeden Anbieter einzeln anschreiben wollen. Das Stichwort hier lautet **Interoperabilität der Rechtsausübung**.

Eine weitere Hürde ist die **Durchsetzung**: Nutzer, auch Jugendliche, scheuen oft den Rechtsweg, wenn ein Unternehmen dem Auskunftersuchen nicht nachkommt. Die DSGVO sieht für solche Fälle Beschwerdemöglichkeiten bei Aufsichtsbehörden vor. Hier könnten Verbesserungen ansetzen, etwa dass Datenschutzbehörden *proaktiv* kontrollieren, ob große Plattformen eingehende Auskunftersuchen ordnungsgemäß bearbeiten (als Form der Auditierung). Alternativ oder zusätzlich könnte das **Verbandsklagerecht** erweitert werden, sodass Verbraucherschutz- oder Jugendorganisationen stellvertretend für Betroffene Auskünfte einklagen können. So könnten z.B. Jugendorganisationen testen, ob TikTok vollständige Auskunft über die gesammelten Nutzungsdaten gibt, und bei Mängeln als Verband Beschwerde einreichen.

Eine Stärkung individueller Auskunftsrechte ist an sich positiv im Sinne von **Transparenz und Kontrolle**. Wenn Nutzer – gerade Heranwachsende – besser verstehen, welche Daten über sie gespeichert sind und wie ihr Verhalten getrackt wird, fördert das auch Medienkompetenz. Zum Beispiel würde ein Einblick in das persönliche Profiling (Segmentierung der Interessen für Werbung) vielen erst klar machen, wie viel die Plattformanbieter und Werbenetzwerke über sie wissen. Das kann Verhalten ändern, etwa restriktivere Datenschutzeinstellungen. Allerdings sind auch Grenzen erkennbar: Die gespeicherten Datenmengen sind oft immens und längst nicht alle Daten sind für Laien sinnvoll interpretierbar; junge Nutzer könnten von riesigen Datendownloads überfordert sein. Hilfreich könnte daher auch die **didaktische Aufbereitung** sein, etwa in Form digitaler Assistenten, die einen Auskunftsbericht erklären.

Eine rechtspolitische Möglichkeit ist auch, *kollektive Auskunftsansprüche* einzuführen. So könnten Plattformen verpflichtet werden, allgemeine Auswertungen zu veröffentlichen, z.B. welche Altersgruppe wie viel Zeit auf der Plattform verbringt, welche Kategorien von Daten gesammelt werden und wie diese genutzt werden; der DSA gibt hier schon Pflichten zur Erstellung von Transparenzberichten vor; auch Begründungspflichten und Transparenzpflichten im Rahmen von für Onlinewerbung gegenüber dem Nutzer können die datenschutzrechtlichen Auskunftsansprüche

unterstützen. Dennoch bleibt das Kernstück die DSGVO, und dort sind substantielle Änderungen nur auf EU-Ebene möglich.

7. Erleichterung von Auskunftsansprüchen Privater oder Aufsichtsbehörden gegenüber digitalen Diensten

In Punkt 8 des Antrags geht es vor allem um Auskunftsansprüche, die dazu dienen sollen, **rechtswidrige Inhalte im Netz zurückzuverfolgen**, also etwa die Identität oder Anschrift eines Nutzers zu erfahren, der z.B. beleidigende oder sonst verletzende Inhalte gepostet hat. Der Beschluss formuliert, man solle prüfen, ob die Auskunftsansprüche nach dem Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) auf Bundesebene neu geregelt und so ausgestaltet werden können, „dass sie auch für Privatpersonen nutzbar sind und gegen rechtswidrige Inhalte vorgegangen werden kann“. Zusätzlich soll ein **Auskunftsrecht der Landesmedienanstalten** gesetzlich verankert werden.

Im Kern geht es bei der Forderung damit um Ansprüche gegen Plattformen auf identifizierende Auskunft zu anderen Nutzern; dies erfolgt in der Regel über die Herausgabe von Bestandsdaten. Den rechtlichen Rahmen dafür regeln §§ 21, 22 TDDDG, die unter bestimmten Voraussetzungen die Auskunft über Bestandsdaten durch den Anbieter an berechnigte Stellen erlauben. Darunter fallen etwa Strafverfolgungsbehörden, Landesmedienanstalten – und nach der Rechtsprechung des OLG Schleswig seit 2022 auch Privatpersonen, sofern eine gerichtliche Entscheidung dies gestattet. Das OLG entschied, dass **§ 21 Abs.2 TTDSG (jetzt TDDDG) eine spezialgesetzliche Anspruchsgrundlage für Auskunftsansprüche Privater gegen Social-Media-Plattformen** darstellt. Betroffene können auf dieser Rechtsgrundlage erfolgreich die Herausgabe der Bestandsdaten von Tätern erreichen; eine vorheriges Strafverfahren ist nicht erforderlich. Durch die Entscheidung wurde die Position von Personen, die Opfer von z.B. Hassrede oder Cybermobbing geworden sind, gestärkt. Die **praktische Hürde eines gerichtlichen Beschlusses**, der dem Plattformbetreiber im Rahmen der Auskunft zuzustellen ist, bleibt aber bestehen. Für eine Privatperson, etwa eine gemobbte Schülerin oder deren Eltern, kann das ein hoher Aufwand sein, der mit Anwalts- und Gerichtskosten verbunden ist.

Die EntschlieBung bleibt **unklar, auf welchem Weg die geforderten Verbesserungen erreicht werden sollen**. Hier existierten eine Reihe von Möglichkeiten, die aber teilweise schon im Rahmen der Diskussionen und Entwürfe eines Digitale-Gewaltschutzgesetzes auf Bundesebene vorgebracht worden sind. Es wäre insoweit hilfreich, den Antrag zu konkretisieren, etwa im Hinblick auf eine Vereinfachung des Auskunftsverfahrens oder eine Zentralisierung von Auskunftsersuchen etwa bei den Landesmedienanstalten als Ombudsstellen mit entsprechend erweiterten Auskunftsrechten.



8. Vorbehalt der Einführung einer Klarnamenpflicht

Ebenfalls in Antragspunkt Nr. 8 wird angeregt, zu prüfen, nach Umsetzung der anderen geforderten Maßnahmen noch eine Klarnamenpflicht nötig sei. Dies impliziert, dass die Antragsteller eher skeptisch sind und die Klarnamenpflicht **als ultima ratio** sehen. Die Debatte um mögliche Klarnamenpflichten im Netz läuft seit über zwanzig Jahren; bereits dieser Umstand verweist auf die Komplexität der von einer entsprechenden gesetzlichen Regelung berührten verfassungsrechtlichen Aspekte.

Der geltende Rechtsrahmen sieht mit § 19 Abs. 2 TDDDG vor, dass Anbieter von digitalen Diensten die Nutzung ihrer Dienste „anonym oder unter Pseudonym zu ermöglichen“ haben. Der Ordnungsrahmen geht derzeit also eher von einer Pflicht zur anonymen oder pseudonymen Nutzung von Onlinediensten aus; das entspricht dem Gegenteil einer Klarnamenpflicht. Ohne diese gesetzliche Vorgabe aber würde sich nicht automatisch eine entsprechende Pflicht ergeben; ob und unter welchen Namen Nutzer auf Plattformen Inhalte posten können, hinge auch dann zentral von der Entscheidung des jeweiligen Plattformanbieters ab. Für eine Klarnamenpflicht wäre also die Schaffung einer ausdrücklichen gesetzlichen Vorschrift nötig.

Befürworter einer gesetzlichen Pflicht argumentieren, dass Anonymität im Netz die Hemmschwelle für Hasskriminalität und Beleidigungen senke; Täter fühlten sich im Schutz der Namenlosigkeit sicher. Mit Echtnamen wären sie vorsichtiger, zudem könnten Opfer und Gesellschaft offener diskutieren, wenn die Person des Äußernden klar ist. Auch die Verfolgung von Rechtsverstößen würde erleichtert – man wüsste anhand des Namens sofort, wer Täter ist. Empirisch stützen Beobachtungen diese Annahme nicht: Plattformen mit später eingeführten Realnamenpflichten haben einen kaum gemäßigteren Ton als vollkommen anonyme Foren: Auch mit Klarnamen wird gehetzt.

Kritiker einer Klarnamenpflicht betonen, dass Anonymität ein wichtiges Schutzinstrument der Meinungsfreiheit ist. Insbesondere Whistleblower, Oppositionelle, Aktivisten oder besonders schutzbedürftige Personen können sich nur unter Pseudonym angstfrei äußern. Eine Pflicht zum Realnamen würde ggf. viele dieser Gruppen zum Verstummen bringen (sog. „chilling effect“). Zudem sind unschuldige Nutzer dem Risiko ausgesetzt, im echten Leben belästigt oder bedroht zu werden, wenn ihre Äußerungen sofort zuordbar wären. Studien weisen hier darauf hin, dass Hassrede nicht allein durch Namensnennung verschwindet, weil Menschen auch unter Klarnamen hetzen, solange sie die soziale Ächtung in ihrer Peergroup nicht fürchten müssen. Angesichts der Auskunftsmöglichkeiten der Strafverfolgungsbehörden sind strafrechtlich relevante Äußerungen unter Pseudonym bereits jetzt verfolgbar, während strafrechtlich relevante aber kontroverse Meinungen eventuell aus Angst vor persönlichen Drangsalierungen oder Shitstorms durch Dritte gar nicht mehr geäußert würden, wenn dies nur unter Nennung des Klarnamens möglich ist.

Die Meinungsfreiheit (Art. 5 GG) schützt im Übrigen grundsätzlich auch das **Recht, sich anonym oder unter Pseudonym** zu äußern. Das Bundesverfassungsgericht hat in ständiger Rechtsprechung betont, dass das Gefühl ständiger Identifizierbarkeit Bürger davon abhalten kann, ihre Grundrechte wahrzunehmen. Schon im Volkszählungsurteil 1983 hieß es sinngemäß, *wer befürchten muss, bei abweichender Meinung registriert zu werden, verzichtet eher auf seine Grundrechtsausübung*. Übertragen auf die digitale Öffentlichkeit bedeutet dies, dass eine Klarnamenpflicht ein Klima schaffen kann, in dem manche Gruppen sich aus Sorge vor beruflichen oder sozialen Konsequenzen nicht mehr trauen, Position zu beziehen. **Art. 5 Abs. 1 GG** aber schützt gerade auch unbequeme, unerwünschte oder Minderheitsmeinungen.

Die Einführung einer generellen Klarnamenpflicht im Internet erscheint vor diesem Hintergrund als **verfassungsrechtlich hochproblematisch**. der Entschließungsantrag scheint dies zu erkennen, indem er die Forderung von der Wirksamkeit der übrigen Maßnahmen abhängig macht.

9. Wirtschaftliche Entflechtung von TikTok

Zu der Forderung in Punkt 9 des Entschließungsantrags nimmt der Verfasser keine Stellung.

10. Fazit und Ausblick

Der Entschließungsantrag in Drs. 19/7489 präsentiert ein ganzes **Maßnahmenbündel**, das technische, regulatorische und pädagogische Ansätze kombiniert. Diese Kombination ist grundsätzlich zu begrüßen, denn die komplexen Herausforderungen – Jugendschutz, Desinformation, mentale Gesundheit – lassen sich nicht mit einem einzelnen Instrument lösen. Aus wissenschaftlicher Sicht erscheint insbesondere der Fokus auf **Medienkompetenzförderung (Abschnitt 3)** als unumgänglich und auch verhältnismäßig. Hier sind positive Effekte zu erwarten, ohne dass Grundrechte beschnitten würden. Auch die Stärkung von **Auskunfts- und Durchsetzungsrechten (Abschnitte 5 und 6)** fügt sich kohärent in einen Ordnungsrahmen ein, der bestehende Normen im digitalen Raum wirksam(er) machen kann. Diese Maßnahmen sind eher Feinjustierungen und Effizienzsteigerungen der Rechtsdurchsetzung und daher mit den Prinzipien der Verhältnismäßigkeit gut vereinbar.

Restriktivere regulatorische Maßnahmen wie die Einführung eines **Mindestalters (Abschnitt 2)**, **verpflichtender Altersüberprüfungen (Abschnitt 3)** oder einer **Klarnamenpflicht (Abschnitt 8)** sind wesentlich eingriffsintensiver und werfen erhebliche verfassungsrechtliche Fragen auf. Sie müssen an strengen Wirksamkeitsnachweisen gemessen werden. Das Prinzip der **Verhältnismäßigkeit** verlangt, dass solche Einschränkungen nur ergriffen werden, wenn mildere Mittel nicht zum Ziel führen. Die **Jugendkonten**-Idee ist innovativ, aber nach kinderrechtsfreundlicher Lesart bereits von Art. 28 Abs. 1 DSA umfasst.



Insgesamt stellt sich die **Frage, ob die aufgelisteten Maßnahmen zusammen ein stimmiges Konzept ergeben**. Prinzipiell decken sie verschiedene Ebenen ab: *Prävention* (Medienbildung, Awareness), *Regulierung/Überwachung* (Datenzugänge, Auskunftsrechte, DSA-Umsetzung) und *interventionistische Eingriffe* (Mindestalter, Klarnamen, Entflechtung). In einem kohärenten Konzept sollten immer erst die Präventionsmaßnahmen und unmittelbar umsetzbare Regulierungsinitiativen ausgeschöpft werden, bevor restriktive Eingriffe erfolgen. Der Beschluss folgt dieser Logik teilweise, etwa indem er Realnamenzwang nur als nachrangige Option benennt. Es ist aber nicht immer klar, ob sich die Einzelmaßnahme nur auf den Jugendschutz bezieht, oder ob alle Nutzer einer Social-Media-Plattform von der Änderung umfasst sein sollen. Auch ist nicht immer deutlich, ob es bei den rechtlichen Änderungsforderungen nur um Social-Media-Plattformen als Regelungsgegenstand geht, oder nicht um alle Vermittlungsdienste oder generell digitale Dienste. Die beantragte **EntschlieÙung bleibt eher unklar**.

Auf EU-Ebene existiert mit dem **Digital Services Act** zudem bereits ein einheitlicher Ordnungsrahmen für Online-Plattformen. Mehrere der geforderten Punkte, u.A. Datenzugänge für die Aufsicht, Schutz von Minderjährigen, Transparenz, sind im DSA oder im angrenzenden EU-Datenschutzrecht (DSGVO) verankert. Der Beschluss drängt folgerichtig auf konsequente Umsetzung des DSA in Deutschland und Europa. In der Tat wird es im Jahr 2026 ff. entscheidend sein, wie die neuen Regeln greifen: Die kommenden Jahre werden geprägt sein von der **Implementierung des DSA**. Hier wird sich zeigen, ob Plattformen wie TikTok, Instagram & Co. freiwillig z.B. ihre Algorithmen entschärfen oder bessere Jugendschutzmaßnahmen standardmäßig einführen. Wenn nicht, könnten die hier diskutierten *schärferen Maßnahmen* wieder auf die Agenda kommen. Wenn die DSA-Maßnahmen dagegen Wirkung entfalten, erledigen sich einige der geforderten Punkte möglicherweise.

Letztlich sollte ein kohärentes regulatorisches Konzept die **Kinderrechte** in den Mittelpunkt stellen: Bestmöglicher Schutz vor Ausbeutung und schädlichen Einflüssen, aber auch Wahrung der Beteiligungsrechte und der Entwicklungschancen der Kinder müssen berücksichtigt sein. Der vorgestellte Maßnahmen-Mix versucht das, er gerät aber insgesamt in ein Fahrwasser, in dem **Schutzmaßnahmen in ein Übermaß** geraten und unbeabsichtigt das Recht der jungen Menschen auf freie Entfaltung und Teilhabe beschneiden können.

Insgesamt ist das Konzept in großen Teilen plausibel als Mehr-Ebenen-Ansatz: Auf EU-Ebene Regulierung harmonisieren und ggf. durchgreifen (DSA, evtl. Eigentumsmaßnahmen), auf Bundesebene Rechtsrahmen justieren (Datenauskunft, Jugendschutzgesetze), auf Landesebene Bildung und Medienaufsicht stärken. Dieser **Mehrebenen-Ansatz** entspricht auch dem föderalen und europäischen Kompetenzgeflecht. Wichtig ist jedoch die ständige Evaluierung: Maßnahmen sollten wissenschaftlich begleitet werden (z.B. untersucht man in ein paar Jahren, ob die Förde-

rung von Medienkompetenz messbar die Resilienz gegen Desinformation erhöht hat, ob Auskunftsansprüche häufiger genutzt wurden und erfolgreich waren etc.). Nur so kann ein Jugendschutz-Konzept **lernend angepasst** werden.

Hamburg, im Januar 2026

