WIEN / 16. September 2026

Digitaler Ausweiszwang – Audiovisuelle Mediendienste-Gesetz, KommAustria-Gesetz, Änderung (132/ME)

Für epicenter.works
Sebastian Kneidinger
Arya Gerda Haager
Josef Hörmandinger
Thomas Lohninger
Elisabeth Kury

EPICENTER .WORKS
for digital rights

VORWORT UND KURZFASSUNG

Wir bedanken uns für die Möglichkeit, im Rahmen des Begutachtungsverfahrens[1] nachfolgende Stellungnahme abgeben zu können, auch wenn wir es bedauern, dass der Entwurf später als angekündigt veröffentlicht wurde und somit diese wichtige Diskussion in die Sommermonate verlegt wurde.

Der Begutachtungsentwurf sieht neue „Jugendschutzbestimmungen" für Video-Sharing-Plattformen vor. Minderjährigen unter 14 Jahren soll der Zugang zu Diensten mit bestimmten Empfehlungssystemen, Interaktionsanreizen und anderen erfassten Funktionen verwehrt werden. Zur Durchsetzung dieser Altersgrenze müssen die Anbieter eine wirksame Altersverifikation einsetzen. Was daher vor allem als Social-Media-Verbot für Kinder diskutiert wird, betrifft tatsächlich die gesamte Nutzer:innenschaft. **Aus einem Verbot für einen Teil der Bevölkerung wird ein digitaler Ausweiszwang für alle.**

Kinder und Jugendliche vor schädlichen Geschäftspraktiken und suchtfördernden Plattformmechanismen zu schützen, ist eine dringende gesellschaftliche und politische Aufgabe. **Umso schwerer wiegt, dass der Entwurf gerade diese Gefahrenquellen weitgehend unangetastet lässt.** Infinite Scroll, Autoplay und problematische Empfehlungssysteme können nicht nur Kinder, sondern die gesamte Bevölkerung betreffen. Statt diese Mechanismen zu regulieren, verschiebt der Entwurf die Debatte hin zur Frage, wer Zugang erhält. Der Menschenrechtskommissar des Europarats bringt die Alternative mit der Forderung „Regulate online platforms, not children"[2] auf den Punkt.

Darin liegt das grundlegende Problem des Entwurfs. Reguliert werden in erster Linie die Nutzer:innen und ihr Zugang, nicht die schädlichen Mechanismen der Plattformen. Dieses Problem besteht unabhängig davon, wie die Altersverifikation technisch ausgestaltet wird oder wie einzelne Bestimmungen des Entwurfs nachgebessert werden.

Gerade die gesellschaftliche Bedeutung dieser Dienste macht einen solchen Zugangszwang grundrechtlich sensibel. **Was im alten Athen die Agora und in Österreich über Jahrzehnte der Stammtisch im Gasthaus war, sind heute für viele Menschen digitale Plattformen.** Hier werden Informationen ausgetauscht, Meinungen gebildet und politische Debatten geführt. Der Zugang zu solchen Kommunikationsdiensten wird nun von einer vorherigen Altersverifikation abhängig gemacht.

Der digitale Ausweiszwang greift daher in die Grundrechte der gesamten Nutzer:innenschaft ein. Er berührt Privatsphäre und Datenschutz ebenso wie die Meinungs- und Informationsfreiheit. Der Verfassungsgerichtshof hat bereits in anderem Zusammenhang auf die grundrechtliche Bedeutung eines „*Gefühls der Überwachung*"[3] hingewiesen. **Schon der Eindruck, beim Zugang identifizierbar, beobachtbar oder nachverfolgbar zu sein, kann Menschen von der Nutzung legaler Informations- und Kommunikationsangebote abhalten.**

1 https://www.parlament.gv.at/gegenstand/XXVIII/ME/132 und https://technical-regulation-information-system.ec.europa.eu/en/notification/28351
2 https://www.coe.int/en/web/portal/-/regulate-online-platforms-not-children
3 G 72-74/2019 , Seite 65

Frankreich zeigt, wie weitreichend dieser Effekt ist. Dort erklärte der Conseil constitutionnel im August 2026 eine zentrale Bestimmung für verfassungswidrig.[4] Dabei beanstandete er ausdrücklich, dass zur Durchsetzung der Altersgrenze auch Erwachsene ihr Alter nachweisen müssten.

Kinder unter 14 Jahren werden aus diesen Kommunikationsdiensten sogar vollständig ausgeschlossen. Dabei sind sie eigenständige Träger von Grund- und Menschenrechten. Maßnahmen zu ihrem Schutz müssen daher stets auch ihre Rechte auf Information, Teilhabe und persönliche Entwicklung berücksichtigen und mit diesen in Einklang gebracht werden.

Ein derart weitreichender Grundrechtseingriff ist nur verhältnismäßig, wenn kein gleich wirksames gelinderes Mittel zur Verfügung steht. Hier bestehen jedoch solche Alternativen. Problematische Plattformfunktionen können unmittelbar reguliert und Eltern mit einfachen technischen Werkzeugen unterstützt werden. epicenter.works hat bereits 2025 einen gerätebasierten Ansatz vorgeschlagen[5], bei dem lediglich ein Alterssignal an Apps und Websites übermittelt wird, ohne die gesamte Bevölkerung einem individuellen digitalen Ausweiszwang zu unterwerfen. Die Verantwortung der Plattformanbieter bleibt dabei bestehen.

Auch hohe gesetzliche Anforderungen an Datenminimierung, Nichtverfolgbarkeit und Unverknüpfbarkeit beseitigen die Risiken einer flächendeckenden Altersverifikation nicht. Wo Identitätsdaten oder Ausweisdokumente verarbeitet oder gespeichert werden, entstehen attraktive Angriffsziele. Ein Datenleck kann eine große Zahl von Menschen betreffen.[6] Anders als Passwörter lassen sich zentrale Identitätsmerkmale danach nicht einfach austauschen.

Zu diesen grundsätzlichen Einwänden kommen erhebliche Probleme der konkreten Ausgestaltung des Entwurfs hinzu. Es bestehen Zweifel, ob die vorgesehene Zugangsbeschränkung von der AVMD-RL getragen wird und ob Österreich im durch den DSA harmonisierten Bereich zusätzliche Pflichten für Plattformanbieter schaffen darf. Zudem bleibt teilweise unklar, welche Dienste und Funktionen überhaupt erfasst werden. **Auch die französische Debatte zeigt, dass die unionsrechtlichen Grenzen nationaler Plattformregulierung keine bloß theoretische Frage ist.**

Der Begutachtungsentwurf sollte daher in seiner derzeitigen Form nicht weiterverfolgt werden. **Wirksamer Kinder- und Jugendschutz muss bei den schädlichen Mechanismen der Plattformen ansetzen und darf nicht zu einem digitalen Ausweiszwang für die gesamte Bevölkerung führen.**

Inhaltsverzeichnis

Vorwort und Kurzfassung....2
1. Zum Begutachtungsentwurf....4
2. Regulierung der Nutzer:innen statt Regulierung schädlicher Plattformfunktionen....5
3. Grundrechtliche Auswirkungen des digitalen Ausweiszwangs und der Zugangsbeschränkung....6
3.1 Privatsphäre und Datenschutz....6

4 https://euractiv.com/de/news/franzosisches-verfassungsgericht-erklart-social-media-verbot-fur-unter-15-jahrige-fur-verfassungswidrig/
5 https://epicenter.works/content/altersverifikation-neu-gedacht-ein-moeglicher-loesungsansatz
6 https://techcrunch.com/2026/09/10/id-verification-giant-idscan-confirms-data-breach-with-more-than-150-million-drivers-licenses-stolen/

3.2 Gefühl der Überwachung und Meinungsfreiheit....8
3.3 Kinder als Träger von Grund- und Menschenrechten....8
3.4 Verhältnismäßigkeit mit Maß statt Maximum....9
4. Technische Ausgestaltung der Altersverifikation....12
4.1 ID Austria und zertifizierte Drittanbieter....12
4.2 Hohe Anforderungen an die praktische Umsetzung....13
4.3 Hacks und Datenlecks....14
5. Unionsrechtliche und legistische Bedenken....15
5.1 AMD-G und AVMD-RL als taugliche Rechtsgrundlage?....16
5.2 Grenzen nationaler Plattformregulierung....17
5.3 Unklarer Anwendungsbereich und Bestimmtheit....18

1. ZUM BEGUTACHTUNGSENTWURF

Der vorliegende Begutachtungsentwurf sieht im Audiovisuelle Mediendienste-Gesetz neue Jugendschutzbestimmungen für Video-Sharing-Plattformen vor. Minderjährigen unter 14 Jahren soll der Zugang zu solchen Plattformen verwehrt werden, wenn diese bestimmte, im Gesetz näher bezeichnete Funktionen aufweisen. Zur Durchsetzung dieser Altersgrenze müssen die Plattform-Anbieter eine wirksame Altersverifikation einsetzen.

Die Zugangsbeschränkung knüpft damit nicht allgemein an „soziale Medien", sondern an den bereits im AMD-G verwendeten Begriff der Video-Sharing-Plattform an. Dieser Begriff ist weiter als der umgangssprachliche Begriff einer Videoplattform. Erfasst werden Dienste, bei denen die Bereitstellung von Sendungen oder nutzergenerierten Videos Hauptzweck, trennbarer Teil oder eine wesentliche Funktion des Dienstes ist, ohne dass der Plattform-Anbieter dafür redaktionelle Verantwortung trägt. Der Anbieter bestimmt jedoch die Organisation der Inhalte, etwa durch automatische Mittel oder Algorithmen. Daher können nach den Erläuterungen auch soziale Netzwerke als Video-Sharing-Plattformen einzustufen sein. Reine Abrufdienste, bei denen der Anbieter redaktionelle Verantwortung für die bereitgestellten Inhalte trägt, fallen hingegen nicht unter die neue Zugangsbeschränkung.

Das AMD-G enthält bereits Schutzbestimmungen für Minderjährige auf Video-Sharing-Plattformen. Insbesondere müssen Inhalte, die die körperliche, geistige oder sittliche Entwicklung Minderjähriger beeinträchtigen können, Schutzmaßnahmen unterliegen. Für Inhalte mit grundloser Gewalt sowie Inhalte, die sich überwiegend auf die unreflektierte Darstellung sexueller Handlungen beschränken, besteht bereits eine Zugangskontrolle für sämtliche Minderjährige unter 18 Jahren. Der Entwurf ergänzt dieses inhaltsbezogene Schutzsystem um ein von den Erläuterungen als „funktionales Zugangsverbot"[7] bezeichnetes Modell für Minderjährige unter 14 Jahren. Die bestehenden Schutzmaßnahmen bleiben daneben insbesondere für die Altersgruppe der 14- bis 18-Jährigen aufrecht.

Die neue Zugangsbeschränkung knüpft an bestimmte Funktionen der erfassten Video-Sharing-Plattformen an. § 54e Abs. 3 Z 5 AMD-G nennt insbesondere Empfehlungssysteme, bei denen mehr als ein Drittel der vorgeschlagenen oder angezeigten Inhalte nicht von selbst ausgewählten Kontakten stammt, automatisch abgespielte oder fortlaufend nachgeladene Inhalte, Anreize zur Steigerung der Interaktion mit der Plattform, bestimmte Push-Benachrichtigungen sowie die direkte Übermittlung von

7 Seite 6 der Erläuterungen des Gesetzesentwurfs

Inhalten an Personen, zu denen kein gegenseitiges Kontaktverhältnis besteht. Nach den Erläuterungen handelt es sich dabei um eine demonstrative und damit nicht abschließende Aufzählung. Plattform-Anbieter können zugleich einen ohne Altersverifikation zugänglichen Bereich anbieten, sofern dort keine der erfassten Funktionen eingesetzt wird.

Ist eine Zugangsbeschränkung anzuwenden, hat der Plattform-Anbieter sie durch eine wirksame Altersverifikation sicherzustellen. Der Entwurf schreibt dafür keine spezielle technische Lösung vor. Verlangt wird eine Methode, die nach dem Stand der Technik zu den datensparsamsten verfügbaren Methoden zählt und aus einer Registrierungs- und einer Präsentationskomponente besteht. Für ihre Ausgestaltung sieht der Entwurf unter anderem die Trennung zwischen Plattform-Anbieter und Anbieter der Altersverifikation, Nichtbeobachtbarkeit und Nichtverfolgbarkeit der Altersnachweise, Kollusionsresistenz, Datenminimierung und selektive Offenlegung sowie den Ausschluss einer zentralen Nutzungsprotokollierung vor. Erfolgt der Zugang über ein individuelles Nutzerkonto, soll die Altersverifikation grundsätzlich nur einmal durchgeführt werden.

2. REGULIERUNG DER NUTZER:INNEN STATT REGULIERUNG SCHÄDLICHER PLATTFORMFUNKTIONEN

Ausgangspunkt des Begutachtungsentwurfs sind die Risiken bestimmter Funktionen der vom Video-Sharing-Begriff erfassten Plattformen. Die Erläuterungen verweisen insbesondere auf algorithmische Empfehlungssysteme, die emotionale, extreme oder hyperpersonalisierte Inhalte priorisieren können, um die Nutzerbindung zu maximieren, sowie auf suchtfördernde Designmerkmale wie Infinite Scroll, Autoplay und Belohnungssysteme für kontinuierliche Nutzung. Diese Funktionen können nach den Erläuterungen das Entscheidungsverhalten beeinflussen, die Verweildauer erhöhen und Suchtverhalten fördern.[8]

Die vorgeschlagene Regelung setzt jedoch nicht unmittelbar bei diesen Funktionen an. Plattform-Anbieter müssen sie weder entfernen noch für sämtliche Nutzer:innen verändern. Stattdessen dürfen Minderjährige unter 14 Jahren Video-Sharing-Plattformen, die solche Funktionen einsetzen, grundsätzlich nur dann nutzen, wenn ihnen ein Bereich ohne die vom Gesetz erfassten Funktionen zur Verfügung steht. Für Nutzer:innen ab 14 Jahren bleiben die betreffenden Funktionen hingegen grundsätzlich unverändert bestehen. Der Entwurf begegnet den beschriebenen Risiken damit in erster Linie durch eine Zugangsbeschränkung für eine bestimmte Altersgruppe und die zu ihrer Durchsetzung erforderliche Altersverifikation.

Damit greift die Regelung gegenüber dem von ihr selbst beschriebenen Problem zu kurz. Schädliche oder suchtfördernde Designmechanismen verlieren ihre Wirkung nicht mit Vollendung des 14. Lebensjahres. Entsprechende Mechanismen können auch Erwachsene negativ beeinflussen.[9] Die Altersgrenze lässt diese Funktionen für ältere Jugendliche und Erwachsene unangetastet. Ein Beispiel aus den USA verdeutlicht das Erfolgspotenzial gerichtlicher Verfahren zur Abwehr dieser Gefahren. Am 25. März 2026 stellte eine Jury eine Mitverantwortlichkeit von Meta und Google für die psychischen Erkrankungen einer jungen Frau fest, die im Alter von sechs Jahren mit der Nutzung von YouTube

8 Erläuterungen zum Entwurf , Seite 1
9 https://pubs.aeaweb.org/doi/pdfplus/10.1257/aer.20211218

begonnen hatte und in der Folge unter Depressionen, Angstzuständen und Körperdysmorphie litt.[10] Das Urteil stützte sich auf die Feststellung, dass die Plattformbetreiber für das gezielt suchtfördernde Design ihrer Dienste haftbar sind; interne Unternehmensdokumente belegten zudem ein gezieltes Vorgehen zur Gewinnung und Bindung minderjähriger Nutzer:innen trotz bestehender Alterserfordernisse.

Dies ist auch für den Schutz der unter 14-Jährigen relevant. Wird die Altersbeschränkung umgangen, bleiben genau jene Funktionen verfügbar, vor denen der Entwurf schützen will. Gleichzeitig entsteht für Plattform-Anbieter kein unmittelbarer Anreiz, ihre Geschäftspraktiken und suchtfördernden Algorithmen insgesamt zu verändern. Die zugrunde liegenden Plattformstrukturen bleiben bestehen. Reguliert wird in erster Linie, wer Zugang zu ihnen erhält. **Die Verantwortung sollte jedoch dort ansetzen, wo die Risiken entstehen, und Plattform-Anbieter für problematische Funktionalitäten in die Verantwortung nehmen.**

Der Ansatz, problematische Plattformfunktionen unmittelbar zu regulieren, wird auch von fachlichen und kinderrechtlichen Stimmen gestützt. Der Deutsche Ethikrat sieht Plattformanbieter in besonderer Verantwortung, weil Risiken vielfach bereits in der Gestaltung ihrer Produkte und den zugrunde liegenden Geschäftsmodellen angelegt sind.[11] Auch eine Koalition von mehr als 170 Kinderrechtsorganisationen spricht sich dafür aus, Safety-by-Design bei Diensten zu verankern, die Kindern zugänglich sind, anstatt den Schutz primär durch deren Ausschluss herzustellen.[12]

Damit verschiebt der Entwurf den Schwerpunkt der regulatorischen Debatte. Ausgangspunkt sind problematische Plattformfunktionen und Geschäftsmodelle. Daraus wird jedoch vor allem eine Frage der Altersfeststellung und Zugangskontrolle. **Dieser Regelungsansatz lässt nicht nur die eigentlichen Gefahrenquellen weitgehend bestehen, sondern schafft durch die Zugangsbeschränkung und die erforderliche Altersverifikation zugleich neue grundrechtliche Probleme, die im nächsten Kapitel näher erörtert werden.**

3. GRUNDRECHTLICHE AUSWIRKUNGEN DES DIGITALEN AUSWEISZWANGS UND DER ZUGANGSBESCHRÄNKUNG

Der Entwurf wirkt grundrechtlich in zwei Richtungen. Minderjährigen unter 14 Jahren kann der Zugang zu den erfassten Diensten verwehrt werden, während die übrige Nutzer:innenschaft eine Altersverifikation durchlaufen muss. Beide Eingriffe sind eigenständig zu betrachten und anschließend gemeinsam auf ihre Verhältnismäßigkeit zu prüfen:

3.1 Privatsphäre und Datenschutz

Altersverifikation setzt voraus, dass eine für den Zugang maßgebliche persönliche Eigenschaft verlässlich festgestellt und gegenüber dem jeweiligen Dienst bestätigt wird. Die dafür erforderliche Verifikation betrifft nicht nur Minderjährige unter 14 Jahren, sondern grundsätzlich alle Nutzer:innen, die Zugang zu den erfassten Diensten erhalten wollen. Auch Personen, welche die Altersgrenze längst

10 https://www.npr.org/2026/03/25/nx-s1-5746125/meta-youtube-social-media-trial-verdict
11 https://www.ethikrat.org/presse/mitteilungen/kein-pauschales-social-media-verbot/
12 https://5rightsfoundation.com/eu-says-tech-firms-must-prove-safety-before-accessing-children/

überschritten haben, müssen nachweisen können, dass sie zum Zugang berechtigt sind. **Damit berührt die Regelung unmittelbar das Recht auf Privatleben nach Art. 8 EMRK und das Grundrecht auf Datenschutz nach § 1 DSG sämtlicher Nutzer:innen der betroffenen Dienste.** Wird ein solches Verfahren für einen großen Teil der Bevölkerung zur Voraussetzung für die Nutzung verbreiteter digitaler Dienste, entsteht eine entsprechend umfangreiche Infrastruktur zur Verarbeitung und Bestätigung solcher Informationen.

Je nach eingesetztem Verfahren kann dafür die Verarbeitung besonders sensibler Informationen erforderlich werden, etwa von Ausweisdaten oder biometrischen Merkmalen. Der Entwurf versucht die damit verbundenen Risiken durch Anforderungen an Datenminimierung, Nichtverfolgbarkeit und die Trennung der beteiligten Stellen zu begrenzen. Plattformen sollen insbesondere keine Kenntnis von der Identität der Nutzer:innen erhalten und unterschiedliche Verifikationsvorgänge nicht miteinander verknüpfen können.

Ob diese Garantien auch in der praktischen Umsetzung zuverlässig funktionieren, ist für die Intensität des Grundrechtseingriffs von wesentlicher Bedeutung. Zugleich entstehen mit der großflächigen Nutzung von Altersverifikationsverfahren neue Daten- und Sicherheitsrisiken. Die technischen Anforderungen, Schutzmechanismen und Risiken der vorgesehenen Altersverifikation werden in Kapitel 4 näher behandelt.

Über die konkrete Datenverarbeitung hinaus ist auch die Etablierung einer solchen **Überwachungsinfrastruktur** grundrechtlich relevant. Wird der Zugang zu verbreiteten digitalen Diensten von der vorherigen Feststellung eines persönlichen Merkmals abhängig gemacht, entsteht eine technische Infrastruktur, die grundsätzlich eine Verknüpfung von Identitäts- und Nutzungsdaten ermöglichen kann. Gerade deshalb müssen Zweckbindung, Nichtverfolgbarkeit und technische Grenzen gegen eine solche Verknüpfung besonders strikt ausgestaltet sein. Wie aktuell dieses Ausweitungspotenzial ist, zeigt die erst jüngst erhobene politische Forderung, Altersverifikation mit einer Klarnamenpflicht zu verbinden.[13] Eine Klarnamenpflicht ist zwar nicht Gegenstand des vorliegenden Entwurfs, die enge Zweckbindung bietet jedoch keinen dauerhaften Schutz vor schleichender Ausweitung. In den USA wurden staatliche DNA-Datenbanken ursprünglich streng reguliert und ausschließlich zur Aufklärung schwerer Straftaten eingesetzt, im Zeitverlauf jedoch schrittweise ausgedehnt.[14] Wird die technische Grundlage für eine flächendeckende Altersverifikationsinfrastruktur einmal geschaffen, besteht die Gefahr, dass diese einem vergleichbaren Ausdehnungsdruck ausgesetzt wird. Die Debatte verdeutlicht jedoch, wie wichtig es ist, die technische und rechtliche Trennung zwischen Altersnachweis, Identität und konkreter Nutzung dauerhaft abzusichern.

Wie schwer diese Bedenken wiegen können, zeigt die französische Rechtsprechung. Der Conseil constitutionnel erklärte im August 2026 eine zentrale Bestimmung der französischen Regelung zu Altersbeschränkungen in sozialen Netzwerken wegen unzureichender Garantien für das Recht auf Achtung des Privatlebens für verfassungswidrig. Dabei war für den Conseil constitutionnel insbesondere von Bedeutung, dass zur Durchsetzung des digitalen Ausweiszwangs auch Erwachsene ihr Alter nachweisen müssen.[15]

13 https://www.krone.at/4085378
14 https://www.sciencedirect.com/science/article/pii/S1872497324000917
15 https://www.eff.org/deeplinks/2026/08/french-top-court-gets-it-right-strikes-down-social-media-ban-youths

3.2 Gefühl der Überwachung und Meinungsfreiheit

Die Auswirkungen des digitalen Ausweiszwangs beschränken sich nicht auf Privatsphäre und Datenschutz. Wird der Zugang zu digitalen Kommunikationsdiensten von einem vorherigen Altersnachweis abhängig gemacht, kann dies auch beeinflussen, wie frei Menschen diese Dienste nutzen. Die Meinungs-, Informations- und Kommunikationsfreiheit kann daher bereits durch die vorgeschaltete Nachweispflicht berührt werden und nicht erst dann, wenn einer Person der Zugang tatsächlich verweigert wird.

Von besonderer Bedeutung ist dabei das vom Verfassungsgerichtshof in anderem Zusammenhang thematisierte „*Gefühl der Überwachung*“[16]. Bereits die Verpflichtung, vor dem Zugang zu einem digitalen Kommunikationsraum einen digitalen Ausweis vorweisen zu müssen, kann bei Nutzer:innen den Eindruck erzeugen, identifizierbar oder kontrollierbar zu sein. Eine tatsächliche Verknüpfung der Identität mit der späteren Nutzung ist dafür nicht erforderlich. Menschen können dadurch davon Abstand nehmen, bestimmte Informationen abzurufen, sensible Angebote zu nutzen oder bestimmte Meinungen zu äußern. Dieser als „Chilling Effect“[17] bezeichnete Abschreckungseffekt kann dazu führen, dass Menschen aus Sorge vor Beobachtung, Kontrolle oder einer Verknüpfung ihrer Online-Aktivitäten mit der eigenen Identität ihre Kommunikation einschränken. Gerade bei digitalen Diensten, die wesentliche Entfaltungsmöglichkeiten für Information, gesellschaftliche Kommunikation und politische Teilhabe darstellen, kann ein solcher Effekt erhebliche Bedeutung haben.

Die im Entwurf vorgesehenen Anforderungen an Nichtverfolgbarkeit und die Trennung der beteiligten Stellen können dieses Risiko zwar begrenzen, **sie beseitigen jedoch nicht den vorgelagerten Umstand, dass der Zugang selbst von einem Altersnachweis abhängig gemacht wird.** Für die Meinungs-, Informations- und Kommunikationsfreiheit ist deshalb nicht nur entscheidend, welche Daten technisch miteinander verknüpft werden können, sondern bereits, welche Wirkung eine verpflichtende Identifikation als Zugangsvoraussetzung auf die unbefangene Nutzung digitaler Kommunikationsräume entfaltet.

3.3 Kinder als Träger von Grund- und Menschenrechten

Für Minderjährige unter 14 Jahren kommt zu diesen allgemeinen Auswirkungen ein weiterer Grundrechtseingriff hinzu. Ihnen kann der Zugang zu den erfassten Plattformen beziehungsweise Funktionen überhaupt verwehrt werden. Eine grundrechtliche Bewertung darf Kinder dabei nicht bloß auf ihre Schutzbedürftigkeit reduzieren. Sie sind selbst Träger:innen von Grund- und Menschenrechten. Schutzinteressen müssen daher mit ihren eigenen Rechten auf Information, Meinungsäußerung, gesellschaftliche Teilhabe und persönliche Entfaltung in Einklang gebracht werden.

Soziale Medien können Kindern und Jugendlichen Kommunikation mit Gleichaltrigen, den Aufbau sozialer Beziehungen, den Zugang zu Informationen und Lerninhalten sowie die Teilnahme an digitalen Gemeinschaften ermöglichen. Ein Ausschluss betrifft damit nicht lediglich die Freizeitgestaltung, sondern kann auch Möglichkeiten gesellschaftlicher Teilhabe und Persönlichkeitsentwicklung beschränken. [18]

16 G 72-74/2019 , Seite 65

17 https://www.ohchr.org/en/documents/studies-and-research/pushed-shadows-evidencing-digital-surveillance-chilling-effects-and

18 https://www.oecd.org/en/publications/how-s-life-for-children-in-the-digital-age_0854b900-en/full-report/the-impact-of-digital-activities-on-children-s-lives_4df70664.html?utm_source=chatgpt.com

Dies wird auch durch das Bundesverfassungsgesetz über die Rechte von Kindern (BVG Kinderrechte) verdeutlicht. Nach Art. 4 BVG über die Rechte von Kindern hat jedes Kind das Recht auf angemessene Beteiligung und Berücksichtigung seiner Meinung in allen das Kind betreffenden Angelegenheiten. Diese Bestimmung ist für die digitale Lebenswelt von besonderer Bedeutung, da soziale Medien mittlerweile einen wesentlichen Raum für gesellschaftliche Kommunikation, Artikulation eigener Interesse und politischer Meinungsbildung darstellen.[19] Im Unterschied zu Zugangsbeschränkungen bei Suchtmitteln wie Alkohol oder Tabak, bei denen kein grundrechtlich geschütztes Interesse Minderjähriger am Zugang besteht, ist die Nutzung sozialer Medien unmittelbar mit der Wahrnehmung kinder- und grundrechtlich geschützter Positionen verknüpft.

Besondere Bedeutung können solche Räume für Jugendliche haben, die auf niedrigschwellige Möglichkeiten zum Austausch oder zur Suche nach Unterstützung angewiesen sind. Dazu zählen etwa LGBTQ+-Jugendliche[20] und Angehörige gesellschaftlicher Minderheiten[21]. Zugangsbeschränkungen und verpflichtende Verifikationsverfahren können gerade für jene zusätzliche Hürden schaffen, die auf solche digitalen Unterstützungs- und Entfaltungsräume besonders angewiesen sind.

Auch eine starre Altersgrenze kann die unterschiedliche Entwicklung von Kindern nur begrenzt abbilden. Mit zunehmendem Alter wachsen Kompetenzen, Verständnis und eigenständige Handlungsfähigkeit. Ein grundrechtsorientierter Kinder- und Jugendschutz muss dieser Entwicklung Rechnung tragen und Schutz mit wachsender Selbstständigkeit verbinden. Die verpflichtende Altersverifikation bewirkt eine Einschränkung des elterlichen Erziehungsrechts indem sie die autonome Entscheidung der Erziehungsberechtigten über die Mediennutzung ihrer Kinder durch staatliche Regulierung ersetzt. Studien zeigen, dass aktive elterliche Mediation wie Gespräche und gemeinsame Internetnutzung nachhaltigere Erfolge erzielen als Verbote.[22]

Besonders deutlich wird die Schwäche einer starren Zugangsschranke an der Altersgrenze von 14 Jahren. Mit Vollendung des 14. Lebensjahres verschwinden weder die beschriebenen Risiken noch der Bedarf an altersgerechtem Schutz. Gleichzeitig gewinnen Selbstständigkeit und Rechte der Jugendlichen mit zunehmendem Alter an Gewicht. Ein tragfähiges Schutzkonzept kann deshalb nicht darin bestehen, bis zu einem bestimmten Geburtstag den Zugang zu sperren und danach die problematischen Plattformfunktionen grundsätzlich wieder freizugeben. Es braucht abgestufte Schutzinstrumente, die Kinder und Jugendliche entsprechend ihrer Entwicklung unterstützen.

3.4 Verhältnismäßigkeit mit Maß statt Maximum

Grundrechtseingriffe müssen dem Grundsatz der Verhältnismäßigkeit entsprechen. Auch ein legitimes Ziel rechtfertigt nicht jeden Grundrechtseingriff. Eine Maßnahme muss geeignet und erforderlich sein und darf die Betroffenen nicht stärker belasten, als es ihr tatsächlicher Nutzen rechtfertigt.[23] Entscheidend ist daher, ob die vorgesehene Zugangsbeschränkung einen Schutzgewinn erzielt, der die Breite der damit verbundenen Grundrechtseingriffe rechtfertigen kann.

Der Schutz von Kindern und Jugendlichen vor schädlichen Inhalten, suchtfördernden Designmechanismen und anderen Risiken digitaler Plattformen ist zweifellos ein gewichtiges öffentliches Interesse. Für die Verhältnismäßigkeitsprüfung ist zunächst entscheidend, in welchem Ausmaß die vorgesehene Maßnahme überhaupt geeignet ist, dieses Ziel zu erreichen. Der

19 https://www.bpb.de/shop/zeitschriften/izpb/medienkompetenz-355/523579/jugend-und-soziale-medien/
20 https://www.jmir.org/2022/9/e38449/
21 https://pmc.ncbi.nlm.nih.gov/articles/PMC13139868/
22 https://www.mdpi.com/2076-0760/14/11/627
23 Vgl. Berka/Binder/Kneihs, *Die Grundrechte – Grund- und Menschenrechte in Österreich* (2019), S. 199.

vorgesehene Schutzmechanismus bleibt in seiner Reichweite jedoch begrenzt. Wie bereits in Kapitel 2 dargestellt, verändert die Zugangsbeschränkung die vom Gesetzgeber selbst als problematisch identifizierten Plattformfunktionen nicht. Sie bleiben für minderjährige Nutzer:innen ab 14 Jahren bestehen und stehen auch unter 14-Jährigen weiterhin zur Verfügung, wenn die Altersbeschränkung umgangen wird.

Gerade diese Umgehbarkeit ist für die grundrechtliche Bewertung relevant. Die Erfahrungen aus Australien zeigen, dass formale Zugangsbeschränkungen die tatsächliche Nutzung nur begrenzt verhindern. Eine Untersuchung der Molly Rose Foundation aus dem Frühjahr 2026 ergab, dass drei von fünf 12- bis 15-Jährigen weiterhin Zugang zu einem Social-Media-Konto hatten.[24] Eine weitere Untersuchung kam wenige Monate später zu dem Ergebnis, dass mehr als 85 Prozent der unter 16-Jährigen weiterhin soziale Medien nutzten.[25] Die vorgesehenen Sperren lassen sich insbesondere durch die Nutzung von Virtual Private Network Diensten (VPN) mit geringem Aufwand umgehen, durch die vorgetäuscht wird, dass sich die betreffende Person in einem Land ohne Alterskontrollen befindet. Ein Viertel der britischen Kinder nutzt bereits einen VPN.[26] Die Umgehung von Altersbeschränkungen ist mit erheblichen Sicherheits- und Datenschutzrisiken verbunden. Insbesondere kostenlose VPN-Dienste weisen häufig intransparente Geschäfts- und Datenschutzpraktiken auf, setzen unzureichende Sicherheitsmechanismen ein oder können darüber hinaus die Verbreitung von Schadsoftware begünstigen. Eine Zugangsbeschränkung muss nicht vollkommen unumgehbar sein, um einen Beitrag zum Jugendschutz zu leisten. Je leichter und verbreiteter eine Umgehung jedoch möglich ist, desto geringer fällt der zusätzliche Schutzgewinn aus, der den damit verbundenen Grundrechtseingriffen gegenübersteht.

Hinzu kommt die Gefahr einer Problemverlagerung. Werden etablierte und stärker regulierte Plattformen schwerer zugänglich, können Minderjährige auf kleinere, weniger regulierte oder schlechter moderierte Angebote ausweichen. Dadurch werden die zugrunde liegenden Risiken nicht beseitigt, sondern können in Bereiche verlagert werden, in denen Moderations-, Melde- und Unterstützungsmechanismen schwächer ausgeprägt sind. Eine technische Zugangsschranke darf daher nicht mit tatsächlichem Schutz gleichgesetzt werden. Ein wirksamer Kinder- und Jugendschutz wird nicht durch eine einzelne technische Zugangsschranke erreicht. UNICEF weist darauf hin, dass Altersbeschränkungen allein Kinder im Internet nicht ausreichend schützen können.[27] Eine gemeinsame Studie der Arbeiterkammer Wien und der Österreichischen Akademie der Wissenschaften sieht digitale Alterszwänge nicht als alleinige Lösung, sondern fordert ein mehrschichtiges Schutzkonzept aus datenschutzkonformer Regulierung, wirksamer Plattformkontrolle, Transparenz- und Aufsichtspflichten sowie Maßnahmen zur Förderung von Medienkompetenz zu ergänzen, da technische Zugangsschranken allein die komplexen Risiken der digitalen Nutzung Minderjähriger nicht hinreichend erfassen.[28]

Nachdem die Geeignetheit der Maßnahme geprüft wurde, ist im nächsten Schritt der Verhältnismäßigkeitsprüfung ihre Erforderlichkeit zu beurteilen. Eine staatliche Maßnahme ist nur dann erforderlich, wenn kein anderes, gleich wirksames, aber das Grundrecht weniger beeinträchtigendes Mittel zur Erreichung des legitimen Zwecks zur Verfügung steht. **Solche gelinderen Mittel kommen hier in Betracht.**

24 https://mollyrosefoundation.org/wp-content/uploads/2026/04/MRF_Australia-Social-Media-Ban-Research_Briefing-April-26.pdf
25 https://www.bmj.com/content/393/bmj-2026-363695
26 https://www.gov.uk/government/publications/childrens-circumvention-behaviours-online/childrens-circumvention-behaviours-online
27 https://www.unicef.org/press-releases/age-restrictions-alone-wont-keep-children-safe-online
28 https://wien.arbeiterkammer.at/beratung/konsumentenschutz/handyundinternet/internet/Studie_Altersfeststellung_2026.pdf

Eine unmittelbare Regulierung der problematischen Plattformmechanismen setzt dort an, wo die Gefährdung entsteht, ohne den Zugang zu digitalen Kommunikationsräumen für die gesamte Nutzer:innenschaft von einem Altersnachweis abhängig zu machen. Sie kann zugleich ältere Jugendliche und Erwachsene vor denselben problematischen Mechanismen schützen. **Vor diesem Hintergrund ist zweifelhaft, ob ein breit wirkender Altersnachweis erforderlich ist, wenn gleich geeignete, weniger eingriffsintensive Maßnahmen unmittelbar an den beschriebenen Gefahrenquellen ansetzen können.**

Auch wenn für bestimmte Angebote eine altersbezogene Differenzierung als notwendig angesehen wird, folgt daraus nicht, dass dafür die gesamte Nutzer:innenschaft einen individuellen Altersnachweis erbringen muss. Auch innerhalb eines solchen Schutzmodells kommen weniger eingriffsintensive technische Lösungen in Betracht

Der Deutsche Ethikrat empfiehlt insbesondere technische Möglichkeiten zur altersgerechten Beschränkung von Apps, Funktionen, Inhalten und Nutzungszeiten, die auch für weniger technikaffine Eltern einfach und sicher anwendbar sind.[29] **Einen konkreten Ansatz in diese Richtung haben wir bereits 2025 mit einem gerätebasierten Modell vorgeschlagen**.[30] Die Grundidee besteht darin, nicht die Online-Interaktionen sämtlicher Nutzer:innen an ihre Identität zu binden. Stattdessen können Geräte oder Benutzerkonten von Kindern einer Altersgruppe zugeordnet werden. Betriebssystem oder Browser übermitteln anschließend lediglich ein entsprechendes Alterssignal an Apps und Websites.

Eltern, Erziehungsberechtigte oder Schulen können ein Kindergerät, beziehungsweise ein Kinderkonto, altersgerecht konfigurieren. Damit erhalten sie ein einfaches Instrument, um die Nutzung entsprechend dem Alter und der Entwicklung des Kindes zu begleiten. Zugleich verbleibt die Verantwortung für die konkrete Gestaltung und Sicherheit der Dienste bei den jeweiligen Anbietern. Diese müssen das übermittelte Alterssignal berücksichtigen und die geltenden Jugendschutzvorgaben umsetzen.

Ein solcher Ansatz kann altersgerechten Schutz mit einer deutlich geringeren Eingriffsintensität verbinden. Insbesondere müsste nicht die gesamte Nutzer:innenschaft gegenüber jedem erfassten Dienst ihr Alter nachweisen. Ein gerätebasiertes Modell ist daher im Rahmen der Erforderlichkeitsprüfung als mögliches gelinderes Mittel zum digitalen Ausweiszwang zu berücksichtigen.

Das EuGH-Urteil C-188/24, auf das sich die Erläuterungen zur Zulässigkeit der Altersverifikation stützen, ist auf den vorliegenden Entwurf nicht übertragbar.[31] Die beiden Maßnahmen unterscheiden sich hinsichtlich ihrer grundrechtlichen Eingriffsintensität grundlegend. Während Altersbeschränkungen für pornografische Angebote lediglich den Zugang zu Inhalten regulieren, deren Verbreitung gegenüber Minderjährigen bereits rechtlich eingeschränkt ist, schließen Altersverifikationssysteme für soziale Medien eine gesamte Altersgruppe von einem wesentlichen Kommunikations-, Informations- und Sozialisationsraum aus. Der damit verbundene Eingriff in die Meinungs- und Informationsfreiheit ist daher qualitativ schwerwiegender.

Schließlich müssen im Rahmen der Angemessenheitsprüfung der tatsächliche Schutzgewinn und die Schwere der Grundrechtseingriffe gegeneinander abgewogen werden. Auf der einen Seite steht ein

29 https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/kinder-und-jugendliche-in-der-digitalen-welt.pdf, Seite 71

30 https://epicenter.works/content/altersverifikation-neu-gedacht-ein-moeglicher-loesungsansatz

31 Siehe Erläuterungen des Entwurfs insb Seite 2-3

Schutzmechanismus, der die problematischen Plattformfunktionen selbst nicht verändert, dessen Wirkung durch Umgehungsmöglichkeiten begrenzt wird und bei dem eine Verlagerung auf weniger regulierte Angebote möglich ist. Auf der anderen Seite wird Minderjährigen der Zugang zu relevanten digitalen Kommunikationsräumen beschränkt und die Nutzung der erfassten Dienste für die übrige Nutzer:innenschaft von einem Altersnachweis abhängig gemacht.

Beim vorliegenden Entwurf steht damit einer breit wirkenden Altersverifikationspflicht ein Schutzmechanismus gegenüber, der die zugrunde liegenden problematischen Plattformfunktionen nicht verändert und nur einen begrenzten zusätzlichen Schutz verspricht. **Ein grundrechtsorientierter Regulierungsansatz sollte die Verantwortung daher vorrangig dort verorten, wo die Risiken entstehen, bei der Gestaltung und Funktionsweise der Plattformen.**

4. TECHNISCHE AUSGESTALTUNG DER ALTERSVERIFIKATION

Die technische Umsetzung der Altersverifikation hat unmittelbare Auswirkungen auf die Intensität des Grundrechtseingriffs. Datenminimierung, Nichtverfolgbarkeit, Unverknüpfbarkeit und die Trennung der beteiligten Stellen sind deshalb nicht lediglich technische Qualitätsmerkmale, sondern zentrale Voraussetzungen dafür, die mit der Altersverifikation verbundenen Eingriffe möglichst zu begrenzen.

Der Begutachtungsentwurf stellt entsprechend hohe Anforderungen an die technische Ausgestaltung.[32] Für den Altersnachweis soll die nach dem Stand der Technik datensparsamste verfügbare Methode eingesetzt werden. Die Plattform soll lediglich erfahren, ob die erforderliche Altersschwelle erreicht ist, nicht jedoch Namen, Geburtsdatum oder andere unmittelbar identifizierende Informationen. Umgekehrt soll der Anbieter der Altersverifikation nicht erfahren können, gegenüber welcher konkreten Plattform eine Person den Altersnachweis verwendet. Dieses Double-Blind-Prinzip soll verhindern, dass Identitäts- und Nutzungsdaten miteinander verknüpft werden können.[33] Diese Zielsetzung ist zu begrüßen. Im Detail sind jedoch noch folgende Überlegungen zu berücksichtigen:

4.1 ID Austria und zertifizierte Drittanbieter

Für die praktische Altersverifikation kommen nach dem Entwurf ID Austria sowie zertifizierte Drittanbieter in Betracht. Laut den für Digitalisierung und die ID Austria zuständigen Minister:innen und Staatssekretär:innen seit 2020 soll die Nutzung von ID Austria weiterhin freiwillig bleiben. Diese Freiwilligkeit ist bereits einfachgesetzlich mit dem Widerspruchsrecht verankert[34] und wird mit der ab 24. Dezember 2026 verpflichtenden Umstellung auf die eIDAS 2 Verordnung mit einer auf die Privatwirtschaft ausgedehnten Freiwilligkeit und einem Schutz vor Schlechterstellung beim Widerspruch abgesichert[35]. Voraussetzung für die praktische Funktionsfähigkeit des Systems ist daher, dass neben der ID Austria auch tatsächlich geeignete alternative Verifikationsverfahren zur Verfügung stehen. Es bleibt jedoch unklar mit welcher Motivation und welchem Geschäftsmodell alternative Anbieter einer Altersnachweisfunktion den Anforderungen dieses Gesetzes folgen sollten.

32 Siehe insb § 54e Abs 3 a
33 Siehe Erläuterungen des Entwurfs insb Seite 8
34 Siehe insb §4a E-GovG
35 Siehe Artikel 5a paragrah 15 Verordnung (EU) 2024/1183

Die bestehende Altersnachweisfunktion der ID Austria ist noch sehr weit vom vorgesehenen Anwendungsfall entfernt. **Sie erfüllt nach der vom Ministerium beauftragten Datenschutz-Folgenabschätzung[36] die im Entwurf vorgeschriebenen Datenschutzvoraussetzungen nicht** und ist auch nicht für eine Online-Fernüberprüfung ausgelegt, sondern nur für eine Überprüfung in physischer Nähe (Bluetooth). Die für vier Millionen Euro über zwei Jahre entwickelte Altersverifikationslösung der EU-Kommission[37] wurde kurz nach ihrer Veröffentlichung in wenigen Stunden gehackt[38]. Vor diesem Hintergrund ist von signifikantem Entwicklungsaufwand in Österreich auszugehen, bis eine den Anforderungen entsprechende Lösung realistisch vorliegen dürfte.

Eine Softwarelösung zum Altersnachweis hat die Notwendigkeit von größtmöglichen Teilen der Bevölkerung als vertrauenswürdig eingestuft zu werden, da diese auch bei nicht vertrauenswürdigen Diensten im Internet (Soziale Netzwerke, Pornographie, etc.) zum Einsatz kommen soll. Es fehlt im Gesetzestext jegliche Vorgabe, wie dieses Vertrauensniveau zu erreichen und nachzuprüfen wäre. Lediglich in den Erläuterungen[39] werden Vorschläge dafür gemacht, die jedoch weit unter dem liegen, was für die Wallet- und Trust-Infrastruktur der EU als Vorgaben gilt[40]. Die Vorgaben der Erläuterungen erlauben einen Nachweis der Einhaltung der Datenschutzstandards lediglich durch das Vorlegen von interner Dokumentation[41]. Eine unabhängige Prüfung oder eine verpflichtende Veröffentlichung des Programmcodes der Altersverifikationsmethode ist nicht vorgeschrieben. **Es wird daher dringend angeraten eine verpflichtende Open Source Veröffentlichung und Zertifizierung aller zugelassenen Altersverifikationsmethoden (inkl. der ID-Austria-Komponenten) gesetzlich vorzuschreiben.** Da die ID Austria derzeit nicht dem Datenschutzniveau der eIDAS 2 Verordnung entspricht und dem Vernehmen nach dieses auch 2027 nicht erreichen wird, erscheint eine Zertifizierung und unabhängige Prüfung von zumindest den Komponenten zur Altersprüfung unumgänglich. Ebenso sollten Drittanbieter einer Zertifizierung unterliegen, welche die Einhaltung der gesetzlichen Anforderungen an Datenminimierung, Nichtbeobachtbarkeit, Nichtverknüpfbarkeit und Sicherheit gewährleistet.

Weiters hat die mit der Durchsetzung dieses Entwurfs betraute KommAustria keinen Zugriff auf jene Abteilungen der RTR GmbH, welche mit Vertrauensdiensten und der Umsetzung der eIDAS-Vorgaben betraut sind, da diese derzeit nur der TKK zugewiesenen ist. Es fehlt der KommAustria also die notwendige Fachexpertise für die behördeninterne Bewertung von Altersverifikationsmethoden.

4.2 Hohe Anforderungen an die praktische Umsetzung

Das Gesetz formuliert technisch ein anspruchsvolles Ideal. Ob dieses unter realen Bedingungen gleichzeitig sicher, datensparsam und zuverlässig erreicht werden kann, ist jedoch eine bisher unbeantwortete Frage. **Ohne taugliche technische Werkzeuge droht die geplante Altersbeschränkung breite Teile der Bevölkerung von Internetdiensten auszuschließen.**

Die praktische Umsetzung ist anspruchsvoll.[42] Es muss verhindert werden, dass dauerhafte Identifikatoren entstehen, unterschiedliche Verifikationsvorgänge derselben Person miteinander

36 Siehe insb Seite 17-19 und 84 der DSFA des ID Austria Altersnachweis https://www.id-austria.gv.at/dam/jcr:a6d5aef2-166a-499d-9264-860952285494/DSFA-Digitaler_Altersnachweis-20230825.pdf

37 https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/tender-details/ae950883-112f-4139-989e-1c8d794bb77a-CN

38 https://www.derstandard.at/story/3000000317238/eu-app-zur-alterspruefung-von-experten-in-weniger-als-zwei-minuten-geknackt

39 Siehe Seite 8 bis 13 der Erläuterungen

40 Siehe insb Artikel 5c gemeinsam mit Artikel 5a von Verordnung (EU) 2024/1183

41 Siehe Seite 10 Erläuterungen „Zu weiteren Aspekten der Anordnung in Abs. 3a"

42 https://www.internetsociety.org/resources/policybriefs/2025/age-restrictions-and-online-safety/

verknüpft werden oder der Anbieter des Altersnachweises nachvollziehen kann, welche Dienste eine Person nutzt. Gleichzeitig muss der Nachweis zuverlässig genug sein, damit Plattformen auf seine Richtigkeit vertrauen können. Dafür sind insbesondere Prinzipien wie Zero Knowledge[43], Unlinkability[44] und Unobservability[45] relevant. Je stärker die Verifikation gegen Umgehungsversuche abgesichert wird, desto größer kann der Bedarf an zusätzlichen technischen Prüfungen und Identitätsmerkmalen werden.[46]

Beim flächendeckenden Einsatz reicht es nicht, dass ein System unter kontrollierten Bedingungen einen Altersnachweis erzeugen kann. Entscheidend ist, wie es sich bei Millionen von Nutzer:innen, unterschiedlichen Geräten und Plattformen sowie gegenüber Manipulations- und Umgehungsversuchen verhält. Zwischen einem technischen Konzept und einer ausreichend erprobten Infrastruktur für den Masseneinsatz besteht ein erheblicher Unterschied.

Die technische Absicherung gegen Umgehung darf dabei nicht dazu führen, dass immer weitergehende Identitätsinformationen erhoben werden. Je größer der Druck wird, Altersbeschränkungen möglichst unumgehbar zu machen, desto größer kann der Anreiz werden, zusätzliche Datenpunkte und Kontrollmechanismen einzusetzen. Der gesetzlich vorgesehene Grundsatz der Datenminimierung muss deshalb auch dann gelten, wenn eine vollkommen lückenlose Alterskontrolle technisch nicht erreichbar ist.

Eine Altersverifikation kann ihren Zweck nur erfüllen, wenn sie für unterschiedliche Nutzer:innen praktisch zugänglich ist. Digitale Altersnachweise müssen trotzdem zugänglich und inklusiv sein. Insbesondere Personen, die über keinen geeigneten amtlichen Identitätsnachweis verfügen, könnten faktisch vom Zugang zu den betroffenen digitalen Angeboten ausgeschlossen werden. Dies betrifft Personen ohne gültige Ausweisdokumente, Geflüchtete, Personen mit ungeklärtem Aufenthaltsstatus und Menschen ohne festen Wohnsitz. Darüber hinaus können Personen benachteiligt werden, die nicht über die erforderlichen digitalen Kompetenzen oder ein geeignetes Smartphone verfügen oder keine entsprechende digitale Identitätslösung nutzen können oder wollen.

Die technische Lösung muss damit mehrere anspruchsvolle Anforderungen gleichzeitig erfüllen. Sie muss zuverlässig und sicher funktionieren, möglichst wenig personenbezogene Daten verarbeiten, eine Nachverfolgung verhindern und zugleich für einen möglichst breiten Kreis von Menschen praktisch nutzbar bleiben. Ob dies im vorgesehenen Umsetzungsrahmen gewährleistet werden kann, ist für die Bewertung des Systems von zentraler Bedeutung.

4.3 Hacks und Datenlecks

Besondere Aufmerksamkeit erfordern die Sicherheitsrisiken einer flächendeckenden Altersverifikationsinfrastruktur. Je mehr Personen und Dienste auf dieselben oder ähnliche Verifikationsanbieter zurückgreifen, desto attraktiver werden diese Systeme als Angriffsziel. Eine einzelne Schwachstelle kann dadurch große Mengen sensibler Identitäts- und Verifikationsdaten betreffen.

Dass dieses Risiko praktisch relevant ist, zeigt ein im September 2026 bekannt gewordener Fall besonders deutlich.[47] Auf einer Plattform für Identitätsdiebstahl wurden mehr als 150 Millionen

43 https://app.notion.com/p/dpi-privacy/Zero-Knowledge-Proofs-241b205f82488045aea5ee380713578e
44 https://app.notion.com/p/dpi-privacy/Unlinkability-241b205f8248803399dfea676208842a
45 https://app.notion.com/p/dpi-privacy/Unobservability-240b205f82488079ac8aff9e7e432cea
46 https://netzpolitik.org/2026/alterskontrollen-der-pudding-wird-uns-auf-die-fuesse-fallen/
47 https://www.derstandard.at/story/3000000338691/fuehrerschein-scans-von-altersueberpruefungs-dienst-landeten-ueber-ein-jahr-kontinuierlich-im-darknet?ref=rss

Führerschein-Scans von Personen aus den USA und Kanada angeboten. Die angebotenen Bilder waren von IDScan.net gesammelt worden, einem Unternehmen, das unter anderem Identitäts- und Altersüberprüfungen durchführt. Die Betreiber der Plattform behaupteten, seit mehr als einem Jahr laufend neue Datensätze aus einem aktiven Datenleck bei einem großen Identitätsprüfungsunternehmen abgegriffen zu haben. Das FBI leitete eine Untersuchung zur Herkunft der Daten ein.

Auch bei der Firma AU10TIX zeigte sich das Risiko externer Identitätsprüfungsdienste.[48] Dort waren über längere Zeit administrative Zugangsdaten öffentlich zugänglich, wodurch sensible Identitätsdaten potenziell abrufbar waren. Bereits solche Vorfälle verdeutlichen, welche Folgen entstehen können, wenn besonders sensible Datenbestände bei spezialisierten Verifikationsanbietern konzentriert werden.

Die Folgen solcher Datenlecks unterscheiden sich wesentlich von gewöhnlichen Account-Kompromittierungen. Ein Passwort kann geändert werden. Geburtsdaten, Ausweisdokumente oder biometrische Merkmale lassen sich dagegen nicht ohne Weiteres ersetzen. Gelangen solche Informationen in falsche Hände, können die Folgen langfristig bestehen bleiben.

Gerade deshalb sollte ein Altersverifikationssystem vermeiden, dass Ausweiskopien oder vergleichbare Identitätsdaten für einzelne Nachweise erneut übertragen oder dauerhaft gespeichert werden. Je konsequenter die technische Architektur verhindert, dass solche Daten überhaupt anfallen, desto geringer ist das Schadenspotenzial eines späteren Sicherheitsvorfalls.

Der Entwurf setzt mit seinen Anforderungen an Datenminimierung, Nichtverfolgbarkeit und die Trennung der beteiligten Akteure grundsätzlich an der richtigen Stelle an. Entscheidend ist jedoch, dass diese Vorgaben nicht bloße Zielbestimmungen bleiben. Sie müssen in überprüfbare technische und organisatorische Mindeststandards übersetzt werden, deren Einhaltung vor einer Zertifizierung nachgewiesen und anschließend durch Offenlegung des Programmiercodes regelmäßig unabhängig kontrolliert wird.

Bei einer Infrastruktur, deren Nutzung gesetzlich zur Voraussetzung für den Zugang zu verbreiteten digitalen Diensten gemacht wird, können Nutzer:innen das damit verbundene Sicherheitsrisiko nicht ohne Weiteres vermeiden. Umso höher müssen die Anforderungen an Datenschutz durch Technikgestaltung, Datensparsamkeit, IT-Sicherheit, unabhängige Auditierbarkeit und die Begrenzung möglicher Datenbestände sein. **Der Schutz Minderjähriger darf nicht mit neuen, vermeidbaren Risiken für die Identitäts- und Nutzungsdaten der gesamten Bevölkerung erkauft werden.**

5. UNIONSRECHTLICHE UND LEGISTISCHE BEDENKEN

Neben den grundrechtlichen und technischen Fragen stellt sich auch die Frage, ob der Entwurf unionsrechtlich auf einer tragfähigen Grundlage steht und hinreichend bestimmt gefasst ist. Dabei sind zwei unionsrechtliche Ebenen zu unterscheiden. Zum einen ist fraglich, ob Art. 28b AVMD-RL die vorgesehene Zugangsbeschränkung überhaupt trägt. Zum anderen stellt sich die Frage, ob Österreich in den durch den DSA harmonisierten Bereichen zusätzliche Pflichten für Plattformanbieter vorsehen darf. Hinzu kommen erhebliche Unklarheiten darüber, welche Dienste und Funktionen von der Regelung tatsächlich erfasst werden.

48 https://www.eff.org/deeplinks/2024/06/hack-age-verification-company-shows-privacy-danger-social-media-laws

5.1 AMD-G und AVMD-RL als taugliche Rechtsgrundlage?

Das AMD-G setzt im Bereich der Video-Sharing-Plattformen die Vorgaben der Richtlinie über audiovisuelle Mediendienste um.[49] Art. 28b AVMD-RL verpflichtet Video-Sharing-Plattformen zu Maßnahmen zum Schutz Minderjähriger und nennt dabei ausdrücklich auch Alterskontrollsysteme. Damit besteht grundsätzlich eine unionsrechtliche Grundlage für Alterskontrollen auf Video-Sharing-Plattformen. **Fraglich ist jedoch, ob diese Grundlage auch die wesentlich weitergehende Zugangsbeschränkung des Begutachtungsentwurfs trägt.**

Die Alterskontrolle nach Art. 28b AVMD-RL steht im Zusammenhang mit dem Schutz Minderjähriger vor Inhalten, die ihre *„körperliche, geistige oder sittliche Entwicklung"*[50] beeinträchtigen können. Sie dient damit grundsätzlich der Frage, ob eine Person alt genug ist, um bestimmte Inhalte abrufen oder angezeigt bekommen zu können. Der vorliegende Entwurf geht darüber hinaus. Die Zugangsbeschränkung knüpft nicht an die Schädlichkeit eines konkreten Inhalts an, sondern an bestimmte Funktionen der Plattform und kann dazu führen, dass Minderjährige unter 14 Jahren einen Dienst insgesamt nicht nutzen können.

Damit verschiebt sich der Regelungsgegenstand vom Schutz vor bestimmten Inhalten zur Zulässigkeit des Zugangs zu einem Kommunikationsdienst. Auch vollkommen unbedenkliche Inhalte und Nutzungsmöglichkeiten können von der Zugangsbeschränkung erfasst werden, wenn die Plattform die im Gesetz genannten Funktionen anbietet und keinen davon getrennten Bereich zur Verfügung stellt. Dass Empfehlungssysteme oder suchtfördernde Gestaltungsmechanismen ihrerseits Risiken für Minderjährige begründen können, bedeutet noch nicht, dass Art. 28b AVMD-RL die Mitgliedstaaten dazu ermächtigt, den Zugang zu einem gesamten Dienst unabhängig von dessen konkreten Inhalten zu untersagen.[51]

Hinzu kommt, dass Art. 28b Abs. 2 AVMD-RL verlangt, dass die von Video-Sharing-Plattformen zu ergreifenden Maßnahmen durchführbar und verhältnismäßig sind und unter anderem der Größe des jeweiligen Dienstes sowie der Art der angebotenen Dienste Rechnung tragen. Die Richtlinie geht damit von einer am jeweiligen Dienst und den von ihm ausgehenden Risiken orientierten Betrachtung aus. Eine starre Altersgrenze, die bei Vorliegen bestimmter Funktionen unabhängig von der konkreten Ausgestaltung und Nutzung des Dienstes greift, steht mit diesem differenzierenden Ansatz zumindest in einem Spannungsverhältnis.

Ein weiteres Problem ergibt sich aus dem sachlichen Anwendungsbereich der AVMD-RL. Nicht jedes soziale Netzwerk ist eine Video-Sharing-Plattform im unionsrechtlichen Sinn. Dienste, deren Angebot wesentlich auf Bildern, Fotografien oder Text beruht, werden nicht allein dadurch zu Video-Sharing-Plattformen, dass sie Empfehlungssysteme oder vergleichbare Funktionen einsetzen.[52] **Die Zugangsbeschränkung wird damit zwar mit den Risiken bestimmter Plattformfunktionen begründet, ihre rechtliche Reichweite hängt jedoch zugleich davon ab, ob ein Dienst überhaupt als Video-Sharing-Plattform einzustufen ist.** Vergleichbare problematische Funktionen können daher auf Diensten außerhalb des Anwendungsbereichs verbleiben, während auf erfassten Plattformen auch unproblematische Nutzungsmöglichkeiten von der Altersgrenze betroffen sein können.

49 Siehe Erläuterungen zum Entwurf, Seite 1
50 Erläuterungen zur Regierungsvorlage 462 BlgNR XXVII. GP zur Umsetzung der AVMD-RL, Link: https://www.parlament.gv.at/dokument/XXVII/I/462/fnameorig_848562.html
51 https://leibniz-hbi.de/die-huerden-eines-social-media-verbots-in-deutschland/, Seiten 16-17
52 https://www.weizenbaum-institut.de/media/Publikationen/Weizenbaum_Discussion_Paper/Weizenbaum_Discussion_Paper_54.pdf

Vor diesem Hintergrund bestehen erhebliche Zweifel, ob Art. 28b AVMD-RL eine taugliche Rechtsgrundlage für die vorgesehene Zugangsbeschränkung darstellt. Insbesondere lässt sich ein allgemeines Mindestalter für soziale Medien nur eingeschränkt auf Art. 28b AVMD-RL stützen.[53]

5.2 Grenzen nationaler Plattformregulierung

Mit dem Digital Services Act (DSA) hat der Unionsgesetzgeber bereits einen umfassenden Rechtsrahmen für digitale Dienste geschaffen. Ziel der Verordnung ist es, ein sicheres, transparentes und vertrauenswürdiges digitales Umfeld sowie einheitliche Regeln für digitale Dienste innerhalb der Europäischen Union zu schaffen.[54] Für die vom DSA harmonisierten Bereiche bedeutet dies zugleich, dass den Mitgliedstaaten grundsätzlich kein eigener Spielraum verbleibt, zusätzliche Anforderungen an Plattformanbieter zu erlassen. Dies wird auch expressis verbis in Erwägungsgrund 9 DSA festgehalten, wonach Mitgliedstaaten keine zusätzlichen nationalen Anforderungen in Bezug auf die vom DSA erfassten Bereiche erlassen oder beibehalten sollen. Zugleich enthält der DSA bereits Verpflichtungen zum Schutz Minderjähriger. Art. 28 DSA verpflichtet Plattformanbieter, ein hohes Maß an Privatsphäre, Sicherheit und Schutz Minderjähriger zu gewährleisten. Art. 34 und 35 DSA sehen für sehr große Online-Plattformen darüber hinaus Risikoanalysen und Maßnahmen zur Risikominderung vor.[55]

Damit stellt sich für den österreichischen Entwurf die Frage, ob und inwieweit für die vorgesehenen zusätzlichen Pflichten gegenüber Plattformanbietern überhaupt noch ein nationaler Regelungsspielraum besteht. Die französische Debatte zeigt, dass dabei zwischen der nationalen Festlegung einer Altersgrenze und zusätzlichen nationalen Verpflichtungen für Plattformanbieter unterschieden werden muss.

Im französischen TRIS-Notifikationsverfahren[56] wurde diese Frage konkret beantwortet. Die EU-Kommission stellte öffentlich klar, dass nationale Rechtsvorschriften grundsätzlich ein Mindestalter für den Zugang zu bestimmten Online-Diensten festlegen können, sofern sie mit dem Unionsrecht vereinbar sind.[57] Die ausführliche Stellungnahme der Kommission im Notifikationsverfahren wurde jedoch nicht amtlich veröffentlicht. Nach einer veröffentlichten Analyse dieser Stellungnahme richteten sich die unionsrechtlichen Bedenken insbesondere gegen zusätzliche Pflichten für Plattformanbieter, darunter auch Verpflichtungen zur Altersverifikation oder zur Einholung elterlicher Zustimmung.[58]

Für den österreichischen Entwurf ist daher entscheidend, zwischen der Festlegung einer Altersgrenze und zusätzlichen Pflichten für Plattformanbieter zu unterscheiden. § 54e AMD-G beschränkt sich nicht auf eine Altersgrenze, sondern verpflichtet die erfassten Plattformanbieter, den Zugang Minderjähriger unter 14 Jahren zu beschränken und dafür ein wirksames Altersverifikationssystem einzusetzen. Hinzu kommen gesetzliche Anforderungen an dessen technische Ausgestaltung und behördliche Durchsetzungsmechanismen. Damit werden gegenüber den Plattformanbietern zusätzliche Handlungspflichten geschaffen.

Zwar unterscheidet sich das österreichische Modell in einzelnen Punkten vom französischen Regelungsversuch. **Der zentrale unionsrechtliche Konflikt ist jedoch derselbe. Österreich versucht, Plattformanbietern zusätzliche Pflichten aufzuerlegen, obwohl dieser Bereich**

53 https://www.bundestag.de/resource/blob/1104862/WD-7-036-25.pdf, Seite 8
54 https://www.rtr.at/medien/was_wir_tun/DigitaleDienste/DSA/DSA.de.html
55 Denk/Mischensky, Der Digital Services Act und das Kommunikationsplattformen-Gesetz, Medien und Recht 2023, 128.
56 https://technical-regulation-information-system.ec.europa.eu/en/notification/27828
57 https://audiovisual.ec.europa.eu/en/media/video/I-292518 , ab Minute 1:32
58 https://www.leclubdesjuristes.com/societe/numerique/majorite-numerique-bruxelles-met-un-coup-darret-au-parlement-francais-16906/

durch den DSA unionsweit harmonisiert ist. Vor diesem Hintergrund spricht vieles dafür, dass der Entwurf unionsrechtlich erheblichen Bedenken ausgesetzt ist.

5.3 Unklarer Anwendungsbereich und Bestimmtheit

Unabhängig von den unionsrechtlichen Fragen muss bei einer grundrechtsrelevanten Zugangsbeschränkung hinreichend klar und vorhersehbar sein, welche Dienste und Funktionen tatsächlich erfasst werden. Gerade hier lässt der Entwurf wesentliche Fragen offen.

Bereits die Einordnung einzelner sozialer Netzwerke als Video-Sharing-Plattform kann Schwierigkeiten bereiten. Bei Diensten, die audiovisuelle, bildbasierte und textbasierte Elemente kombinieren, ist nicht immer eindeutig, ob Videos eine wesentliche Funktion im Sinne des AMD-G darstellen. Als Grenzfälle kommen etwa Pinterest oder Reddit in Betracht. Damit ist nicht ohne Weiteres vorhersehbar, welche Dienste letztlich der Zugangsbeschränkung unterliegen.

Zusätzliche Unklarheiten entstehen durch die tatbestandsauslösenden Funktionen selbst. Bei Empfehlungssystemen soll die Zugangsbeschränkung unter anderem dann greifen, wenn mehr als ein Drittel der vorgeschlagenen oder angezeigten Inhalte nicht von Kontakten der Nutzer:innen stammt. Die Erläuterungen nennen zwar verschiedene Möglichkeiten, wie die Regulierungsbehörde das Vorliegen dieser Voraussetzung in der Praxis prüfen kann.[59] Offen bleibt jedoch, auf welcher Grundlage dieser Anteil zu bestimmen ist, ob auf Ebene der Plattform insgesamt, eines einzelnen Accounts, eines bestimmten Zeitraums oder einer konkreten Nutzungssitzung. Empfehlungssysteme sind dynamisch. Ihre Ergebnisse können sich laufend und zwischen einzelnen Nutzer:innen unterscheiden.

Darüber hinaus ist nicht nachvollziehbar, weshalb gerade ein Anteil von einem Drittel die gesetzliche Schwelle bildet. Der Entwurf muss nicht nur erkennen lassen, wie diese Grenze praktisch zu berechnen ist, sondern auch, weshalb gerade bei Überschreiten dieses Werts jene Gefährdung angenommen wird, die eine Zugangsbeschränkung für eine gesamte Altersgruppe rechtfertigen soll. Sowohl die praktische Reichweite der Regelung als auch die sachliche Grundlage der gewählten Schwelle bleiben damit klärungsbedürftig.

Hinzu kommt, dass die in § 54e Abs. 3 Z 5 AMD-G genannten Funktionen nach den Erläuterungen nicht abschließend sein sollen. Gerade bei einer Regelung, deren Anwendung darüber entscheidet, ob Minderjährige einen Dienst nutzen dürfen und ob die übrigen Nutzer:innen zuvor eine Altersverifikation durchführen müssen, ist ein offener Tatbestand besonders problematisch. Für Plattformanbieter und Nutzer:innen muss vorhersehbar sein, welche konkrete Gestaltung eines Dienstes die gesetzliche Zugangsbeschränkung auslöst.

Diese Unklarheiten sind nicht nur eine Frage guter Legistik. Aus dem rechtsstaatlichen Bestimmtheitsgebot folgt, dass gesetzliche Eingriffe in Grundrechte hinreichend klar und vorhersehbar ausgestaltet sein müssen.[60] Für die Betroffenen muss grundsätzlich erkennbar sein, unter welchen Voraussetzungen eine bestimmte Nutzungsmöglichkeit beschränkt wird. Je weitreichender die Folgen einer gesetzlichen Einordnung sind, desto weniger kann die Bestimmung des tatsächlichen Anwendungsbereichs erst der späteren Interpretation oder behördlichen Vollziehung überlassen werden.

59 Erläuterungen zum Entwurf, Seite 6f

60 Vgl. Berka/Binder/Kneihs, Die Grundrechte – Grund- und Menschenrechte in Österreich, 2019, S. 188.

Der Entwurf sollte deshalb den Anwendungsbereich und die tatbestandsauslösenden Funktionen wesentlich präziser fassen. Insbesondere bedarf es klarer Kriterien dafür, wann ein Dienst als erfasste Video-Sharing-Plattform gilt, wie quantitative Schwellen bei Empfehlungssystemen zu berechnen sind, worauf die gewählten Grenzwerte sachlich beruhen und welche weiteren, nicht ausdrücklich genannten Funktionen eine Zugangsbeschränkung auslösen können.

Bei einer Regelung, die über den Zugang zu gesellschaftlich- und grundrechtlich relevanten Plattformen **entscheidet und zugleich eine Altersverifikation für die übrige Nutzer:innenschaft auslöst, darf ihre tatsächliche Reichweite nicht erst im Vollzug geklärt werden.**