26. Mai 2026

DIGITALE GESELLSCHAFT

MACHT PLATTFORMEN BESSER, STATT EXKLUSIV!

POSITION ZU ALTERS- UND IDENTITÄTSVERIFIKATION AUF SOCIAL-MEDIA-PLATTFORMEN

Fachgruppe Plattformregulierung der Digitalen Gesellschaft

DIGITALE GESELLSCHAFT / CH-4000 BASEL
OFFICE@DIGITALE-GESELLSCHAFT.CH / DIGITALE-GESELLSCHAFT.CH

1 MANAGEMENT SUMMARY

Die Digitale Gesellschaft erachtet Social-Media-Verbote für Jugendliche als nicht zweckmässig. Social Media sind für Jugendliche heute Lebenswelt, Lernort, Ausdrucksraum – und trotz hunderter Studien gibt es keine eindeutige Evidenz für einen kausalen Zusammenhang zwischen Social-Media-Nutzung und psychischen Problemen. Im Februar 2026 hat die Digitale Gesellschaft deshalb Position gegen ein Social-Media-Verbot unter 16 Jahren bezogen. Das vorliegende Positionspapier vertieft die gesellschaftlichen und technischen Risiken der Altersverifikation, zeigt aber gleichzeitig Alternativen für Jugendschutz sowie bessere Plattformen für alle auf. Und es beleuchtet, was die kommende E-ID in dieser Fragestellung leisten kann und was nicht.

Altersverifikation führt zu einer noch grösseren Datensammlung durch die Plattformen und damit unweigerlich zu mehr Überwachung und einem höheren Missbrauchsrisiko. Das (von allen) notwendige «Vorzeigen» eines Ausweises für die Teilnahme an Debatten der digitalen Öffentlichkeit entspricht nicht der Kultur des freien und demokratischen Internets. Insbesondere für vulnerable Gruppen, Minderheiten oder Whistleblower:innen und Oppositionelle sind diese Entwicklungen gravierend.

Da der digitale Austausch für Jugendliche ein zentrales Grundbedürfnis darstellt, bewirken Altersschranken oft das Gegenteil des intendierten Schutzes: Sie werden entweder technisch umgangen oder drängen Jugendliche systematisch in unregulierte, unsichere Online-Räume. Nicht zuletzt führt das Ausschliessen der Jugendlichen von grossen Social-Media-Plattformen dazu, dass Big-Tech-Konzerne weniger in der Verantwortung sind, die Probleme zu lösen, welche die ganze Gesellschaft betreffen (Hassrede, manipulative Algorithmen oder ausländische Beeinflussung der Demokratie).

Eine griffige Plattformregulierung führt dazu, dass digitale Austausch- und Debattenräume zu sichereren, vielfältigeren und informativeren Orten werden – für alle Nutzer:innen, unabhängig von ihrem Alter. Insbesondere im Bereich Empfehlungssysteme (Feed-Gestaltung) sowie manipulative (Dark Patterns) und süchtig machende Designs gibt es zahlreiche Hebel, welche Politik, Justiz und Gesellschaft von Plattformen einfordern sollten, um negative Auswirkungen zu minimieren: Vom Ausschalten von Push-Benachrichtigungen in der Nacht über entschleunigtes Scrollen bis hin zum Verzicht auf FOMO-Elemente.

Die kommende E-ID ist ein datensparsames und sicheres Instrument zur Altersverifikation, das die Digitale Gesellschaft mitausgearbeitet hat und das sie als Lösung für beispielsweise Online-Alkoholkäufe unterstützt. Für Social-Media-Altersverifikationen ist die E-ID aber noch nicht genügend tragfähig, da relevante Bevölkerungsgruppen (noch) nicht über die E-ID verfügen können oder wollen – und da Plattformen noch nicht gezwungen sind, die E-ID als Verifikationsinstrument zu akzeptieren.

2 WAS SIND SOCIAL MEDIA?

Definition gemäss deutschsprachiger Wikipedia:

> «Soziale Medien oder englisch Social Media sind digitale Medien bzw. Plattformen, die es Nutzenden ermöglichen, sich im Internet zu vernetzen, sich also untereinander auszutauschen und mediale Inhalte einzeln, in einer definierten Gemeinschaft oder offen in der Gesellschaft zu erstellen, zu diskutieren und weiterzugeben.
>
> Soziale Medien lassen sich in zwei Kategorien einteilen:
>
> - in soziale Medien mit dem vorherrschenden Ziel der Kommunikation
> - in soziale Medien, die auch zur Kommunikation eingesetzt werden, deren Fokus jedoch außerdem auf dem Inhalt liegt, welchen die Nutzer generieren, bearbeiten und miteinander austauschen»

Zur ersten Gruppe gehören Dienste wie Facebook, Snapchat, LinkedIn, X, Bluesky und Mastodon. Im Vordergrund steht die Kommunikation zwischen Nutzer:innen, wobei plattform-spezifische Algorithmen teilweise eine Vorselektion oder Priorisierung der gezeigten Inhalte vornehmen.

Zur zweiten Gruppe gehören primär auf Konsum ausgerichtete Plattformen wie YouTube, TikTok und Instagram, sowie Plattformen mit pornografischen Inhalten wie Pornhub oder Youporn. Auch bei diesen Plattformen sind zwar Kommunikationsmöglichkeiten (Chats) vorhanden. Sie stehen aber nicht im Vordergrund.

Messenger wie WhatsApp (in der klassischen Chat-Funktion), Signal oder Threema ermöglichen ebenfalls die Vernetzung und den Austausch von Nachrichten und Inhalten. Sie haben aber traditionellerweise einen abgeschlossenen Charakter (Kommunikation findet zwischen zwei Nutzer:innen oder in kleinen Gruppen statt) und sind daher nicht direkt mit Socia-Media-Plattformen im eigentlichen Sinne zu vergleichen.

3 WIE FUNKTIONIERT HEUTE ALTERSVERIFIKATION? IST ES DAS GLEICHE WIE IDENTIFIKATION?

Identifikation und *Altersverifikation* werden teilweise als Synonyme verwendet, bezeichnen im Grunde genommen aber unterschiedliche Dinge. Gemeinsam ist den beiden in der analogen Welt, dass ein amtlicher Ausweis zum Einsatz kommt. Dessen Nutzung ist allerdings unterschiedlich:

- Bei der *Identifikation* geht es darum, die Identität einer Person auf Basis eines amtlichen Ausweises zu ermitteln. Ein Beispiel dazu ist das Abholen eines eingeschriebenen Briefs in einer Poststelle: Das Schreiben wird nur gegen Vorweisen eines amtlichen Ausweises an die Person übergeben, an die es adressiert ist.
- Bei der *Altersverifikation* steht die Verifikation des Alters im Vordergrund und die Identität einer Person ist nur insofern relevant, als dass das Altersnachweis-Dokument glaubhaft zur Person passen muss (diese Kontrolle erfolgt meist über einen optischen Abgleich von Foto und Gesicht). Beispiele dafür sind der Kauf von Alkohol durch junge Erwachsene oder der Zutritt zu einem Ü16-/Ü18-Club. Zwar erfolgt die Altersverifikation meist ebenfalls mittels amtlichem Ausweis, aber der darin enthaltene Name ist für den eigentlichen Vorgang irrelevant.

Bekannte Methoden zur digitalen Altersverifikation sind unter anderem

- Selbstdeklaration: Anklicken beispielsweise eines Buttons, dass man ein bestimmtes Alter erreicht hat – diese Methode ist aber wirkungslos, da keine Verifikation erfolgt
- Hinterlegen einer Kreditkarte: Basiert auf der Annahme, dass nur Erwachsene Kreditkarten erhalten. In der Praxis ist das überholt, da Banken seit einigen Jahren auch Kreditkarten für Jugendliche anbieten.
- Passkopie: Eine Person kopiert ID oder Pass und schickt diese per Briefpost oder E-Mail an die anfordernde Stelle. Wird in der Schweiz zum Beispiel für Behördenauskünfte oder für Anfragen über von einem Unternehmen gehaltene Personendaten verwendet.
- Videoident: Videocall, bei dem ein offizielles/staatliches Ausweisdokument (ID, Pass) gezeigt/gescannt wird und die Verifikationsstelle das dort vorhandene Bild mit dem Aussehen der Person vergleicht. Wird heutzutage in der Schweiz typischerweise von Banken eingesetzt, im Ausland über Drittanbieter wie Personas auch in Ländern wie Grossbritannien, die eine Altersverifikation bereits gesetzlich fordern.
- KI-basierte Verifikation aufgrund des Nutzungsverhaltens: Online-Verhalten auf einer Social-Media-Plattform wird von KI-Algorithmen ausgewertet, daraus wird ein vermutetes Alter abgeleitet. Aufgrund der Unsicherheit aber nicht geeignet für «harte» (gesetzliche) Alterslimiten.

Die schweizerische E-ID sieht eine Verwendung rein für die Altersverifikation vor, bei der ausser dem Alter (bzw. U16/U18/erwachsen) keine Informationen an den Anbieter fliessen. Offen ist, ob ausländische Plattformen die E-ID nutzen werden oder ob sie (im Sinne einer globalen Einheitlichkeit) generell auf eine der obigen Methoden setzen.

4 WESHALB WIR ALTERS- UND IDENTITÄTSVERIFIKATION AUF SOCIAL MEDIA ABLEHNEN

4.1 Datensammlung, Datensicherheit und Überwachung

Die verpflichtende Altersverifikation im Internet führt zwangsläufig zu einer massiven Ausweitung der Datensammlung durch Plattformen und Drittanbieter. Dies betrifft Erwachsene genauso, da ja auch sie nachweisen müssen, ein bestimmtes Alter erreicht zu haben.

Bereits heute gilt: Jedes Datenattribut, das Nutzer:innen preisgeben, dient der Profilbildung und zum Ausspielen zielgerichteter Werbung. Es ist unrealistisch, anzunehmen, dass ausgerechnet Altersdaten davon ausgenommen wären. Selbst wenn die Nutzung von Alters- und Identitätsdaten gesetzlich verboten ist: Missbrauch ist praktisch nicht nachweisbar. Vielmehr ist zu erwarten, dass die Unternehmen sämtliche im Rahmen der Verifikation erhobenen Informationen – etwa Geburtsdatum, Ausweisbilder oder Namen – in bestehende Datenprofile integrieren.

Besonders problematisch ist, dass viele Systeme die vollständige Übermittlung von Ausweisdokumenten verlangen. Teilweise bereits für die Altersverifikation, sicher aber für die Identifikation. Selbst wenn Anbieter beteuern, diese Daten unmittelbar zu löschen, ist davon auszugehen, dass sie diese zumindest temporär speichern, zu Testzwecken nutzen oder als Nachweis aufbewahren. Diese Ausweisdaten sind qualitativ hochwertig, «amtlich bestätigt» und daher besonders attraktiv – sowohl für Unternehmen als auch für kriminelle Akteure. Sicherheitsvorfälle sind keine Ausnahme: So wissen wir, dass bei der von vielen Jugendlichen genutzten Plattform Discord über 70’000 Identitätsdokumente bei einem Altersverifikations-Drittanbieter gestohlen wurden. Solche Vorfälle werden sich mit wachsender Datensammlung häufen.

Darüber hinaus entsteht ein strukturelles Überwachungsrisiko. Einmal erhobene Alters- und Identitätsdaten stehen auch Strafermittlungsbehörden und Geheimdiensten zur Verfügung. So teilt beispielsweise der Altersverifikationsdienst «Persona» alle seine Daten mit der US-Regierung. Datensparsame Lösungen wie die E-ID können dieses Risiko mindern; jedoch ist die E-ID berechtigterweise freiwillig (es werden deshalb vermutlich weitere Verifikations-Optionen angeboten) und Anbieter:innen sind derzeit nicht verpflichtet, die E-ID als Nachweis zu akzeptieren (siehe Ausführungen unten).

4.2 Einfluss auf Online-Kultur und digitale Teilhabe

Eine verpflichtende Altersverifikation (und erst Recht eine Identifizierungspflicht) verändert die Kultur des Internets grundlegend. Wenn für die Teilnahme an digitalen Debatten ein Ausweis erforderlich ist, entsteht der Eindruck, dass Kommunikation einer Erlaubnis bedarf. Dies entspricht nicht unserer Vorstellung einer freien und demokratischen Öffentlichkeit. Und es verschiebt das Machtverhältnis zwischen Zivilgesellschaft, Plattformen und Staat zugunsten der letzteren beiden.

Zudem fragmentiert Altersverifikation den digitalen Raum in getrennte Sphären. Während eine Trennung nach Alter in bestimmten Kontexten sinnvoll sein kann (Schutz vor Übergriffen), ist es für gesellschaftliche und politische Diskussionen problematisch. Die digitale Teilhabe wäre massiv erschwert. Insbesondere junge Menschen nutzen Social Media nicht nur zur Unterhaltung, sondern auch für Bildung, Austausch, Gaming und Identitätsfindung. Der oft zitierte Vergleich mit Alkohol ist verfehlt: Es handelt sich um komplexe Kommunikationsräume, in denen viele Aspekte für viele Jugendliche positiv sind. Nur ein Teil davon ist schädlich. Die wissenschaftliche Evidenz ist uneindeutig und differenziert. Ein pauschaler Ausschluss wirkt daher unverhältnismässig. Wir schliessen einen Jugend-Treff auch nicht per se, nur weil dort einmal Partydrogen-

Dealer aufgetaucht sind. Sondern setzen alles daran, die Dealer fernzuhalten und den Treff wieder zu einem besseren Ort zu machen.

4.3 Kollateralschäden und «chilling effect» auf vulnerable Gruppen und Aktivismus

Die Pflicht zur Alters- oder Identitätsverifikation oder der Ausschluss von bestimmten Gruppen haben erhebliche Auswirkungen auf besonders schutzbedürftige Menschen. Für Whistleblower:innen, politische Aktivist:innen oder Angehörige diskriminierter Minderheiten ist der Zugang zu anonymen (oder mindestens pseudonymen) Räumen im Netz oft essenziell. Diese Räume ermöglichen es, Missstände aufzudecken, sich auszutauschen oder Unterstützung zu finden, ohne Repressionen befürchten zu müssen. Das betrifft mehr Menschen als gedacht und nicht nur «Datenschutz-Nerds»: Es geht um ausgewanderte Oppositionelle, queere Jugendliche auf dem Land, Menschen mit psychischen Problemen oder auch einfach Personen, die andere Ansichten als die gesellschaftliche Mehrheit in ihrem Umfeld haben (siehe auch: 16 Beispiele, warum Pseudonymität im Netz unverzichtbar ist – netzpolitik.org). Diese Personen müssten im Falle einer Verifikation mit (öffentlicher) Identifizierung entweder mit Konsequenzen für ihre Äusserungen leben – oder unterliegen einem «chilling effect», indem sie auf legitime Meinungsäusserung aus Angst vor Konsequenzen verzichten.

Alle Verifikationssysteme diskriminieren zudem Personen, welche über keinen «Ausweis» verfügen: Geflüchtete und Sans-Papiers, aber auch Personen ohne Smartphone oder ohne digitale Kompetenzen für die nötigen Verifikationsprozesse. Zudem: Altersverifikationen, die auf biometrischer Gesichtserkennung beruhen, haben die bereits bekannten diskriminierenden Effekte auf Frauen und Menschen dunkler Hautfarbe.

4.4 Ausweichen auf unsichere Räume ohne Moderation

Insbesondere queere Jugendliche, ethnische Minderheiten, Hilfesuchende (beispielsweise für Selbsthilfegruppen) oder Menschen in repressiven Umfeldern sind auf Online-Austauschräume angewiesen. Für viele von ihnen sind digitale Räume die einzigen Orte, an denen sie Gemeinschaft und Unterstützung erfahren. Werden diese Personen aufgrund einer Altersschranke ausgeschlossen oder verfügen sie nicht über die nötigen Ausweise für die Verifikation, verlagert sich der Austausch unter diesen Nutzer:innen in weniger regulierte Räume. Das Bedürfnis nach Austausch bleibt und es erfolgt eine Migration ganzer Communities auf andere Plattformen. Diese sind oft schlechter moderiert und anfälliger für Betrug, Extremismus oder Schadsoftware. Dokumentiert ist auch das Ausweichen auf informelle Austauschmöglichkeiten – etwa unmoderierte Foren oder improvisierte Lösungen wie gemeinsam genutzte Google-Dokumente mit Chat-Funktion. Damit gehen bestehende Schutzmechanismen verloren, ohne dass die zugrundeliegenden Probleme gelöst werden.

4.5 Reduzierte Verantwortung der Plattformen für Inhalte und Algorithmen

Altersschranken wie unter 14, 16 oder 18 Jahre verschieben die Verantwortung für problematische Inhalte und algorithmische Effekte weg von den Plattformen selbst. Indem eine Gesellschaft Jugendliche als vulnerable Gruppe von den Plattformen ausschliesst, reduziert sie die Verantwortung und die Kosten (für Moderation und Infrastruktur) der Plattformen, um die Systeme insgesamt (das heisst für alle) sicherer zu gestalten. Diese Entwicklung ist politisch kontraproduktiv. Sie untergräbt Bemühungen, Plattformen stärker in die Pflicht zu nehmen für Auswirkungen, welche für alle Menschen und/oder die gesamte Gesellschaft schädlich sind. Etwa Hassrede, manipulative Algorithmen oder ausländische Beeinflussung der Demokratie. Altersschranken sind ein taktisches Eigentor im Hinblick auf das Ziel, Plattformen zu mehr Verantwortung für die Gesellschaft zu verpflichten.

Gleichzeitig werden private Plattformen durch Alters- oder gar Identitätsverifikation zu machtvollen Gatekeepern zum digitalen öffentlichen Raum, auch für Erwachsene. Sie können missliebige Personen durch den Verifikationsprozess fernhalten, allenfalls auch auf Druck der (US-)Regierung.

4.6 Massives Lobbying durch Tech-Konzerne

Angesichts dessen ist es nicht verwunderlich, dass Big-Tech-Konzerne für Altersschranken lobbyieren: Diese kommen ihnen in vielfacher Hinsicht entgegen. Mark Zuckerbergs Meta (der Mutterkonzern von Facebook und Instagram) gab zu diesem Zweck allein 2025 über 26 Millionen US-Dollar für Lobbyarbeit in den USA aus und unterstützte indirekt Organisationen wie die «Digital Childhood Alliance», die Alterskontrollen fordern. Einige Konzerne fordern, dass die Alterskontrolle bereits auf Betriebssystem-Ebene (Google Play Store oder App Store von Apple) erfolgt – dies hätte aber gravierende Konsequenzen für die Internet-Architektur insgesamt, würde von Google/Apple unabhängige Smartphone-Betriebssysteme vor grosse Probleme stellen und würde Desktop-Anwendungen nicht abdecken.

4.7 Technisch leicht zu umgehen

Altersschranken sind in den meisten Formen technisch ineffektiv. Jugendliche finden zahlreiche Wege, die Verifikation zu umgehen: Durch VPNs, die Nutzung fremder Identitäten oder einfache Tricks bei biometrischen Verfahren (beispielsweise durch Freund:innen, Gesichtsmasken oder die Nutzung eines aufgemalten Schnauzbartes für die Bildaufnahme). Erfahrungen aus Ländern wie Australien zeigen, dass ein erheblicher Teil der Jugendlichen weiterhin Zugang zu Plattformen hat – trotz gesetzlicher Verbote. Im Fall Australien: Aktiv umgangen haben die Kontrollen rund ein Viertel der Jugendlichen, beim grössten Teil haben die Plattformen schlichtweg nichts unternommen und gar nicht erst eine Altersverifikation durchgeführt.

Diese Umgehungsstrategien führen wiederum zu neuen Problemen. Diskussionen über VPN-Verbote zeigen, dass sich regulatorische Eingriffe schnell ausweiten. Gleichzeitig entstehen neue Datenschutzrisiken, da auch Umgehungstools Daten sammeln.

5 UND WAS IST MIT DER E-ID?

Wenn Altersverifikation, dann mit einem Instrument wie der kommenden Schweizer E-ID. Die Digitale Gesellschaft hat die Konzeption (als Self Sovereign Identity) und die gesetzliche Verankerung der E-ID in den letzten vier Jahren geprägt. Und die Vorlage in der Abstimmungskampagne entschieden unterstützt.

Mit der E-ID erfolgt die Altersverifikation datensparsam, das heisst auf das Notwendige beschränkt: Die binäre Information, ob das Alter einer Person über oder unter einer bestimmten Schwelle ist – ohne Speicherung des genauen Geburtsdatums oder weiterer Identitätsmerkmale. Das Ergebnis muss anonymisiert, nicht rückverfolgbar und ohne Tracking (über mehrere Zugriffe hinweg) übermittelt werden. Transparenz durch Open-Source-Code ist dabei zentral. Die E-ID erfüllt diese Anforderungen.

Es bestehen aber noch ungelöste Herausforderungen, welche derzeit verhindern, dass die E-ID eine tragfähige Lösung für Altersverifikation ist:

- Sie muss international funktionieren, was derzeit noch nicht der Fall ist.
- Plattformen (insbesondere internationale) müssen vom Gesetzgeber verpflichtet werden, die E-ID als Verifikationsmethode zu akzeptieren, und sie müssen eine entsprechende Infrastruktur bereitstellen.
- Derzeit ist nicht gesichert, dass die E-ID-App auf Smartphone-Betriebssystemen ausserhalb von Google oder Apple angeboten wird – somit wären besonders Nutzer:innen mit hoher Sensibilität für Unabhängigkeit von Big Tech von der E-ID ausgeschlossen. Auch Personen ohne Smartphone können keine E-ID haben, das sie (noch) nicht als Laptop-Anwendung angeboten wird.

Diese Herausforderungen sind noch nicht gelöst. Zudem ist die E-ID zurecht freiwillig. Deshalb stellt sich die Frage, wie mit dem nicht vernachlässigbaren Teil der Bevölkerung in der Schweiz umgegangen werden soll, die auch in Zukunft nicht über eine E-ID verfügen will oder kann. Diese Personen pauschal von Social-Media-Plattformen auszuschliessen, würde als E-ID-Zwängerei verstanden. Auch das Ausweichen auf andere, unsichere und übergriffige Verifikationsmethoden kann keine Lösung sein.

Aus diesen Gründen halten wir die E-ID momentan noch nicht für eine alleine genügend tragfähige Lösung für eine Altersverifikation auf grossen Social-Media-Plattformen, die heute die Funktion öffentlicher Debattenräume im Digitalen einnehmen.

Sinnvoll und angemessen kann eine Altersverifikation dort sein, wo der Inhalt klar auf Erwachsene ausgerichtet ist (und das heute schon gesetzlich verankert ist). Dazu gehört zum Beispiel der Zugriff auf Pornhub wie auch der Kauf von Alkoholika in einem Online-Store. Selbstverständlich gilt hier trotzdem, dass es sich um eine reine Verifikation handelt und keine Identitätsdaten an den jeweiligen Anbieter fliessen.

6 WIE KÖNNEN WIR JUGENDLICHE BEFÄHIGEN UND WO NÖTIG AUCH SCHÜTZEN?

Viele der Herausforderungen und Gefahren, mit denen Jugendliche bei der Nutzung von Social Media konfrontiert sind, betreffen grundsätzlich auch Erwachsene. Dazu gehören unter anderem Algorithmen, welche zum endlosen, zeitlich unbeschränkten Scrollen von Inhalten verleiten; Cybermobbing; eine Verzerrung der Wahrnehmung durch einseitig selektierende Inhalte; und die unbeabsichtigte (und oft auch unbemerkte) Preisgabe persönlicher Daten. Das beste Mittel gegen diese Probleme ist schlicht eine Regulierung, welche die Plattformen unabhängig vom Alter der Nutzer:innen verstärkt in die Pflicht nimmt und sie für die von ihnen eingesetzten Algorithmen und deren Folgen verantwortlich macht.

Die Digitale Gesellschaft hat zusammen mit weiteren zivilgesellschaftlichen Organisationen vertiefte Vorschläge zur Plattformregulierung gemacht. Mit diesen sollen Social Media *für alle* zu Räumen mit einer besseren Debattenkultur, einem selbstbestimmteren und weniger manipulierten Informationskonsum und einer freieren Meinungsbildung werden. Dazu gehören konkret:

- Die Aufnahme von negativen Auswirkungen auf Minderjährige in der Liste der systemischen Risiken sowie die Pflicht, diese Risiken auch zu minimieren;
- Ein Verbot des Ausspielens personalisierter Werbung an Minderjährige;
- Die Pflicht, Empfehlungssysteme anzubieten, die nicht auf Profiling und Interaktions- und Aufmerksamkeitsmaximierung basieren;
- Eine Einschränkung von Dark Patterns (manipulative Benutzer:innen-Führung) und das Verbot von «addictive designs».

Gerade bezüglich Design der Plattformen, das mit den beiden letzten Punkten angesprochen ist, sind diverse Mechanismen bekannt, die einfach (das heisst durch die Plattformen selbst) umsetzbar wären. Dazu gehören:

- Der Verzicht auf «FOMO»-Elemente: «Fear of missing out» durch beispielsweise verschwindende Storys
- Psychohygiene-Streak statt Snap-Streak: Belohnungen für gesundes Verhalten statt täglicher Nutzungszwang
- Benachrichtigungen nachts abschalten
- Eltern-Tools für Nutzungszeit: Eltern sollen Zeitlimits und Sperrzeiten einstellen können
- Keine Like-Zähler: Öffentliche Likes verbergen, um sozialen Druck zu reduzieren
- Standortfreigabe abschaffen: Kein ständiges Teilen des Standorts mit Kontakten
- Entschleunigtes Scrollen: Autoplay deaktivieren, Zwangspausen nach einer bestimmten Nutzungsdauer
- Wohlbefinden statt Engagement-Metriken: Optimierung der Plattform auf die Zufriedenheit der Nutzenden statt auf reine Bildschirmzeit oder Klicks.

Im März 2026 haben Gerichte in den USA Instagram/Meta und YouTube/Google aufgrund des süchtig machenden Designs der Plattformen schuldig gesprochen. Diese Urteile sind die Basis, um auf politischer Ebene Plattformen in die Pflicht zu nehmen, ihre Kommunikationsräume für alle besser zu machen, statt bestimmte Gruppen pauschal auszuschliessen.

Ebenfalls gefordert sind schlussendlich Eltern und Schulen. Selbst *mit* einer Altersverifikation (und dem Sperren von Plattformen bis zum Erreichen des 16. oder 18. Lebensjahres) entsteht Medienkompetenz nicht über Nacht, sondern muss vermittelt und geschult werden. Diese Vermittlung erfolgt am besten auf Basis der Plattformen selbst, indem Jugendliche durch Eltern und Schulen bei der Nutzung von Social Media begleitet und unterstützt werden. Das sieht auch die Eidgenössische Kommission für Kinder- und Jugendfragen EKKJ in ihrem Positionspapier so.

7 WEITERFÜHRENDE QUELLEN

Joint statement of security and privacy scientists and researchers on Age Assurance (February 2026, signed by more than 400 scientists): https://csa-scientist-open-letter.org/ageverif-Feb2026

Electronic Frontier Foundation, Dossier Age Verification: https://www.eff.org/issues/age-verification