



„Safe Social“

Kinder schützen. Digitale Souveränität stärken. Soziale Medien neu denken.

Ben Scott, Pencho Kuzev

- › Die EU sollte Kinderschutz im Netz und digitale Souveränität gemeinsam denken. Ein europäischer „Safe Social“-Ansatz kann breit unterstützte Kinderschutzpolitik mit einer industrie- und wettbewerbspolitischen Strategie verbinden.
- › Altersbeschränkungen für unter 16-Jährige sind als Übergangslösung gerechtfertigt. Ein Social-Media-Verbot allein reicht jedoch nicht aus.
- › Die EU sollte verbindliche Zertifizierungsstandards für „Safe Social“-Produkte schaffen – mit einem Schutzanspruch, wie er auch bei Spielzeug, Elektronik und anderen Produkten für Kinder selbstverständlich ist. Jedes Produkt, das als sicher zertifiziert wird, kann eine Ausnahme vom Verbot erhalten und für unter 16-Jährige zugelassen werden.
- › Damit der neue Markt nicht erneut von marktbeherrschenden Plattformen kontrolliert wird, sollten alle Anbieter einfache Interoperabilitätsstandards erfüllen.
- › Die Kombination aus Schutzstandards, Zertifizierung und Interoperabilität kann den Verkauf gefährlicher Produkte an Kinder beenden. Zugleich entsteht ein neuer Markt für „Safe Social“. Davon profitieren europäische Familien und digitale Souveränität wird dort greifbar, wo sie für Bürgerinnen und Bürger besonders konkret ist: im digitalen Alltag ihrer Kinder.

Einleitung

Digitale Souveränität wird häufig vor allem als geopolitische Herausforderung diskutiert. Im Mittelpunkt stehen dabei Fragen der Cloud-Infrastruktur, der Halbleiterversorgung oder der Industriepolitik. Diese Themen sind zweifellos wichtig. Für die meisten Bürgerinnen und Bürger bleiben sie jedoch abstrakt. Zu wenig Beachtung findet bislang der digitale Raum, in dem Europas Kinder und Jugendliche aufwachsen.

Für Eltern und Lehrkräfte sind die damit verbundenen Herausforderungen jedoch weder abstrakt noch theoretisch. Sie reichen von übermäßiger Bildschirmzeit und ungeeigneten Inhalten bis hin zu manipulativen Designelementen und Mechanismen, die eine problematische oder sogar abhängige Nutzung fördern. Das beeinträchtigt das Wohlbefinden, den Lernerfolg und die gesunde Entwicklung von Kindern und Jugendlichen. Wenn digitale Souveränität breite gesellschaftliche Unterstützung gewinnen soll, muss sie diese Sorgen direkt aufgreifen.

Digitale Souveränität
und der Schutz von
Kindern im Internet

Auch wenn einzelne Studien hinsichtlich ihrer Methodik und Ergebnisse variieren, zeichnet die internationale sozialwissenschaftliche Forschung ein zunehmend eindeutiges Bild: Problematische Formen der Nutzung sozialer Medien gehen insbesondere bei jungen Menschen mit erhöhten Risiken für die psychische Gesundheit und das allgemeine Wohlbefinden einher.¹ Viele Studien zeigen: Bestimmte Designmerkmale und Funktionen können für Minderjährige riskant sein. Sie können dazu führen, dass Kinder und Jugendliche schädliche Inhalte sehen, Plattformen zu lange nutzen oder anderen Gefahren ausgesetzt sind.² Tragische Fälle, in denen Kinder und Jugendliche im Zusammenhang mit sozialen Medien verletzt werden oder sogar ihr Leben verlieren, treten mit besorgniserregender Regelmäßigkeit auf.³

Hinzu kommt eine Alltagserfahrung, die für viele Jugendliche inzwischen normal geworden ist: unerwünschte sexuelle Kontaktaufnahmen und pornografische Inhalte über digitale Kanäle.⁴ Gleichzeitig wächst die Sorge um die psychische Gesundheit von Kindern und Jugendlichen. Angststörungen, Depressionen und Selbstverletzung nehmen zu. Deshalb ist der Schutz von Kindern im Netz in vielen europäischen Ländern zu einem wichtigen politischen Thema geworden.

Daraus ergibt sich eine Grundsatzfrage für die Politik: Wenn Europa digitale Souveränität ernst meint, darf sich die Debatte dann allein auf Infrastruktur und technologische Leistungsfähigkeit konzentrieren? Oder muss sie vor allem jene digitalen Produkte und Dienste in den Blick nehmen, die den Alltag von Millionen europäischer Kinder prägen? Digitale Souveränität erfordert beides: Dringende gesellschaftliche Anliegen müssen aufgegriffen und zugleich Märkte so gestaltet werden, dass Europas technologische Unabhängigkeit gestärkt wird. Genau dazu soll dieses Papier einen Beitrag leisten.

Social-Media-Verbot als Übergangsmaßnahme

Laut dem ifo-Bildungsbarometer 2025 befürwortet in Deutschland eine überwältigende Mehrheit der Bevölkerung von 85 Prozent ein Mindestalter von 16 Jahren für die Nutzung sozialer Medien.⁵ Zu ähnlichen Ergebnissen kommen weitere repräsentative Umfragen von Forsa⁶ und Appinio⁷. Die breite Unterstützung in Europa für ein Social-Media-Mindestalter von 16 Jahren zeigt, wie groß der wahrgenommene Handlungsdruck ist.⁸ Sie ist auch eine Reaktion auf jahrelange, weitgehend erfolglose Versuche, das Verhalten einiger weniger marktbeherrschender, überwiegend amerikanischer Technologieunternehmen wirksam zu begrenzen.

Öffentliche Unterstützung
für eine Altersgrenze
bei sozialen Medien

Die Menschen erwarten Veränderung. Nicht zuletzt wegen dieser breiten öffentlichen Unterstützung ist der Schutz Minderjähriger seit Langem ein wichtiges politisches Ziel der EU. Er findet sich unter anderem im Digital Services Act (DSA) wieder. Der DSA adressiert systemische Risiken und verpflichtet Onlineplattformen zu besonderen Schutzmaßnahmen. Dazu gehört, ihre Benutzeroberflächen so zu gestalten, dass ein Höchstmaß an Datenschutz, Nutzerschutz und IT-Sicherheit gewährleistet ist. Anbieter müssen zudem Risiken begrenzen, die aus der Gestaltung ihrer Dienste entstehen. Das gilt besonders dann, wenn diese Gestaltung die Unerfahrenheit und Verletzlichkeit Minderjähriger ausnutzt. Trotz dieser klaren Verpflichtungen zeigt sich zunehmend, dass viele große digitale Plattformen weiterhin Praktiken anwenden, die weder dem Geist noch den konkreten Anforderungen des europäischen Regulierungsrahmens entsprechen. Die wichtigsten Geschäftsmodelle großer Social-Media-Plattformen haben sich kaum verändert. Auch viele Designanreize zielen weiter darauf ab, Nutzerinnen und Nutzer möglichst lange auf der Plattform zu halten. Rechtsverstöße bleiben häufig folgenlos.

Die zuständigen Aufsichtsbehörden stehen vor großen Herausforderungen und verfügen oft nur über begrenzte Mittel. Die bestehenden Aufsichts- und Durchsetzungsmechanismen sind auf einen Markt ausgelegt, in dem Rechtsverstöße die Ausnahme sind. Sie greifen jedoch zu kurz in einem Markt, in dem Kinder regelmäßig durch schädliche Praktiken gefährdet werden. Hinzu kommt: Die großen Konzerne setzen enorme Summen für Lobbyarbeit und Gerichtsverfahren ein, um regulatorische Eingriffe abzuwehren oder zu verzögern.

Plattformen missachten
EU-Vorschriften

Viele Funktionen, die mit exzessiver und schädlicher Social-Media-Nutzung verbunden sind, prägen deshalb weiterhin den digitalen Alltag von Kindern und Jugendlichen. Dazu gehören endloses Scrollen, algorithmische Verstärkung, Mechanismen sozialer Bestätigung sowie hochpersonalisierte Empfehlungssysteme.⁹ Gerichtsentscheidungen in den USA zeigen, wie groß das Problem ist. Dort wurden Plattformen haftbar gemacht, weil sie bewusst suchtfördernde Nutzungsformen bei jungen Menschen begünstigt haben sollen. Das macht deutlich: Veränderung ist notwendig. Social Media erlebt seinen „Tobacco Moment“¹⁰. Jetzt braucht es entschlossenes Handeln. Die bestehenden Regeln sind wichtig, aber sie reichen nicht aus.

Von Grund auf unsicher

Europa steht mit diesem Problem nicht allein. Australien hat bereits neue Regeln zum Schutz von Kindern im Netz beschlossen. Auch im Vereinigten Königreich und in Kanada liegen entsprechende Vorschläge vor. Sowohl die EU als auch die Bundesregierung haben Expertengremien eingesetzt, um politische Handlungsempfehlungen zu entwickeln. Mehrere Mitgliedstaaten – darunter Frankreich, Spanien, Dänemark und Griechenland – haben gesetzgeberische Prozesse eingeleitet, um jungen Menschen den Zugang zu sozialen Medien zu beschränken.¹¹ Die Zuständigkeit für klare Regeln im Binnenmarkt liegt jedoch in Brüssel. Die EU muss daher zügig handeln. Sie muss das Problem adressieren, regulatorische Fragmen-

tierung vermeiden und Rechtssicherheit schaffen – für Verbraucherinnen und Verbraucher ebenso wie für Anbieter.

In allen Staaten, die derzeit um besseren Schutz von Kindern im Netz ringen, fällt ein Punkt besonders auf: Die betroffenen Unternehmen sind in der Regel keine heimischen Anbieter. Mit Ausnahme von TikTok und Telegram handelt es sich überwiegend um US-Konzerne. Sie agieren in einem engen Oligopol, das neuen Wettbewerbern kaum Raum lässt. Viele politische Entscheidungsträgerinnen und Entscheidungsträger kommen deshalb zu dem Schluss: Wäre der Markt vielfältiger und gäbe es mehr lokale Wettbewerber, könnten Unternehmen stärker auf gesetzliche Vorgaben reagieren und sensibler für Schäden in den eigenen Gesellschaften sein. Fragen digitaler Souveränität sind daher für die Debatte über Kinderschutz unmittelbar relevant. Sie schaffen mehr Verantwortlichkeit und können zugleich Märkte öffnen, die für europäische Unternehmen lange verschlossen waren.

Die EU sollte deshalb Kinderschutz im Netz und digitale Souveränität stärker zusammendenken. Sie sollte die öffentliche Nachfrage nach Beschränkungen für gefährliche Social-Media-Produkte aufgreifen und in einen neuen Regulierungsansatz übersetzen.

Ein gezieltes Verbot für
sicherere soziale Medien

Dafür braucht es ein „intelligentes Verbot“. Gemeint ist keine bloße pauschale Sperre sozialer Medien für Kinder. Vielmehr geht es um neue Marktregeln, die Sicherheit verbindlich machen und zugleich Marktkräfte für dieses Ziel nutzen. Dieser Ansatz trägt der politischen Realität Rechnung. Die Öffentlichkeit unterstützt Social-Media-Beschränkungen zwar deutlich, zugleich besteht Skepsis, ob ein Verbot allein tatsächlich wirksam wäre. Ein pauschales Nutzungsverbot für Kinder hätte erhebliche Nachteile. Es könnte Fragen der Meinungs- und Informationsfreiheit aufwerfen und Plattformen Anreize geben, Altersverifikationen zu umgehen oder Überwachung auszuweiten. Und es könnte Kinder in weniger regulierte digitale Räume verdrängen.

Zudem adressiert ein pauschales Verbot nicht die Designmerkmale, die Schäden verursachen. Es schafft auch keine zusätzlichen Pflichten für große Plattformen, die ihre Dienste weiterhin faktisch an Minderjährige vermarkten könnten. Diese Risiken erklären sowohl den Widerstand gegen solche Maßnahmen als auch die Skepsis vieler Menschen, selbst unter den Befürworterinnen und Befürwortern.

Altersbeschränkungen sollten deshalb nicht als Ziel an sich verstanden werden. Sie sind eine Notmaßnahme und ein Übergangsinstrument. Sie müssen Teil eines breiteren Rahmens für sichere, wettbewerbliche und kindgerechte digitale Dienste sein.

Wir schlagen daher die Schaffung eines europäischen „Safe Social“-Marktes vor. Er soll Kindern sichere digitale Angebote bieten und zugleich den Wettbewerb stärken sowie europäische technologische Alternativen fördern.

Aufbau eines
sicheren europäischen
Social-Media-Marktes

Der politische Ansatz muss zwei Ziele erreichen. Erstens dürfen Unternehmen nicht länger von Schäden an Kindern profitieren. Zweitens braucht es einen klaren Weg zu sichereren und hochwertigeren digitalen Produkten für junge Menschen – Produkten, denen Eltern tatsächlich vertrauen können.

Digitale Souveränität und „Safe Social“

Die Entwicklung sozialer Medien der vergangenen Jahre führt zu zwei zentralen Schlussfolgerungen. *Erstens* braucht Europa einen kindgerechten Markt für soziale Medien, der Sicherheit konsequent in den Mittelpunkt stellt. Erforderlich ist ein „Safe Social“-Ökosystem. Es sollte Kurznachrichtendienste, Bildplattformen, Kurzvideo-Angebote und KI-kuratierte Feeds umfassen. *Zweitens* wächst in Europa das Misstrauen gegenüber großen amerikanischen Technologieunternehmen. Viele dieser Unternehmen haben über Jahre Geschäftsmodelle verfolgt, die auf der kommerziellen Verwertung der Aufmerksamkeit und Daten von Kindern beruhen. Gleichzeitig steigt die Nachfrage nach sicheren und vertrauenswürdigen Alternativen. Dass es solche Alternativen bislang kaum gibt, liegt vor allem an Netzwerkeffekten. Wer eine bestehende Plattform verlässt, verliert nicht nur ein Produkt. Er verliert auch den Zugang zu sozialen Kontakten, relevanten Inhalten und bestehender Interaktion. Viele Nutzerinnen und Nutzer bleiben deshalb auf Plattformen, obwohl sie mit deren Qualität und Risiken unzufrieden sind.¹²

Ein neuer Markt für Kinder und Jugendliche muss daher zwei Probleme gleichzeitig lösen: das *Sicherheits-* und das *Netzwerkeffektproblem*. Andernfalls würden neue Standards lediglich auf einem Markt eingeführt, der erneut von denselben Diensten dominiert wird. Die Folge wäre dieselbe Abwärtsspirale wie heute – mit denselben Fehlanreizen.

Der praktische Ausgangspunkt ist die gegenwärtige politische Lage. Mehrere Mitgliedstaaten arbeiten derzeit an Beschränkungen sozialer Medien für unter 16-Jährige. Wenn diese Regelungen umgesetzt werden, werden einige Familien bestehende Plattformen verlassen. Andere werden sichere Alternativen suchen.

Konvergierende
Modelle für sicherere
soziale Medien

Damit entsteht eine Nachfrage nach „Safe Social“. Zugleich eröffnet sich die Gelegenheit, Produktstandards und Wettbewerbsdynamiken neu zu gestalten. Diese Chance muss bewusst genutzt werden. Die Regeln müssen zukunftsfähig sein und auch neuen technologischen Entwicklungen standhalten. Und sie müssen die richtigen Anreize für die Entwicklung sicherer Produkte nach hohen Standards setzen.

Die EU kann einen europäischen „Safe Social“-Markt durch einen neuen Rechtsrahmen schaffen. Im Kern stünde ein grundsätzliches Verbot sozialer Medien für unter 16-Jährige. Anbieter könnten jedoch eine Ausnahme erhalten, wenn sie nachweislich hohe und verbindliche Schutzstandards erfüllen. Viele dieser Standards sind bereits in den Leitlinien zum Schutz Minderjähriger nach Artikel 28 des Digital Services Act angelegt:

Gestaltung eines
digitalen Marktes für
unter 16-Jährige

- › **Altersverifikation:** Altersnachweise müssen zuverlässig, datensparsam und schwer zu umgehen sein. Dies ist möglich, ohne neue Überwachungsstrukturen zu schaffen. Die neue europäische Altersverifikationslösung und die European Digital Identity Wallet bieten hierfür ein Modell.¹³ Weder der Dienst noch der Staat müssten mehr erfahren als die Information, dass die Altersanforderung erfüllt ist. Gleichwertige Verfahren mit demselben Maß an Datensparsamkeit sollten ebenfalls zulässig sein.

- › **Beschränkung suchtfördernder Designmerkmale:** Funktionen wie Infinite Scrolling, Autoplay, Likes, Streaks, Lesebestätigungen und Push-Benachrichtigungen sollten für Kinder und Jugendliche ausgeschlossen werden.
- › **Kontrolle über Algorithmen:** Nutzerinnen und Nutzer müssen selbst entscheiden, welche Themen und Inhalte ihnen angezeigt werden und in welcher Reihenfolge. Diese Kontrolle darf nicht nur eine Voreinstellung sein. Sie muss die einzige zulässige Option sein.
- › **Altersgerechte Inhaltsbeschränkungen:** Für Inhalte wie Pornografie, Glücksspiel, Drogen, Selbstverletzung sowie weitere für Minderjährige unzulässige oder entwicklungsgefährdende Themen braucht es strenge Moderationspflichten.
- › **Datenschutz:** Verhaltensdaten dürfen nicht genutzt werden. Standortfreigaben, Kontaktsynchronisierung sowie Kamera- und Mikrofonzugriffe sollten standardmäßig deaktiviert sein. Kontakte zwischen Minderjährigen und fremden Erwachsenen müssen wirksam begrenzt werden. Ausnahmen sollten nur für Familie und bekannte Kontakte gelten.
- › **Schutzvorgaben für KI:** Dienste mit KI-Funktionen müssen vor dem Start und regelmäßig danach geprüft werden. Dabei muss sichergestellt werden, dass kindgerechte Schutzmechanismen wirksam greifen. Eine gemeinsame Produkthaftung für Unternehmen, die rechtswidriges Verhalten ermöglichen, kann zusätzliche Anreize für hohe Standards schaffen.
- › **Interoperabilität:** Alle „Safe Social“-Dienste müssen technisch miteinander kommunizieren können. Nutzerinnen und Nutzer sollten Beiträge auf jedem zertifizierten Dienst lesen und veröffentlichen können. Das stärkt den Wettbewerb und verhindert neue Abhängigkeiten.

Ein Regelungsansatz mit verbindlichen Vorgaben und klar definierten Ausnahmen ist keine bloße Theorie. Kanada hat im Juni 2026 mit dem Safe Social Media Act (Bill C-34) ein entsprechendes Modell vorgelegt. Der Gesetzentwurf sieht ein Mindestalter von 16 Jahren für Social-Media-Konten vor.¹⁴ Zugleich können Dienste eine Ausnahme erhalten, wenn sie gegenüber den zuständigen Aufsichtsbehörden nachweisen, dass sie wirksame Schutzmaßnahmen für Kinder umgesetzt haben und dauerhaft einhalten. Auch die von der deutschen Bundesregierung eingesetzte Expertinnen- und Expertenkommission fordert in einer ihrer zentralen Empfehlungen einen stärkeren Kinder- und Jugendschutz in sozialen Medien. Im Mittelpunkt stehen Safety by Design und Safety by Default. Dazu gehören altersgerechte Voreinstellungen und verbindliche Designvorgaben für Jugendkonten. Die Schutzmaßnahmen sollten nach Altersgruppen ausgestaltet werden. Besonders relevant sind die Gruppen „13 bis 16 Jahre“ und „16 bis 18 Jahre“. Einschränkungen für Empfehlungssysteme, Dark Patterns und andere Hochrisikofunktionen sollten standardmäßig gelten. Junge Nutzerinnen und Nutzer sollten dafür nicht selbst aktiv werden müssen. Der zentrale Vorteil dieses Ansatzes ist ein Perspektivwechsel. Schutz wird nicht mehr vor allem zur individuellen Verantwortung von Eltern, Schulen oder jungen Menschen gemacht. Stattdessen werden strukturelle Schutzmechanismen in die Dienste selbst eingebaut. Hochriskante Funktionen werden standardmäßig deaktiviert oder begrenzt.¹⁵

Auch Australien verfolgt inzwischen einen ähnlichen Weg. Die dortige Mindestalter-Regelung für Social-Media-Konten unter 16 Jahren knüpft nicht allein an das Alter der Nutzerinnen und Nutzer an, sondern auch an bestimmte Plattformmerkmale. Erfasst werden insbesondere Dienste mit algorithmischen Empfehlungssystemen, Endlos-Feeds, Feedbackfunktionen

wie Likes sowie zeitlich begrenzte Formate wie Storys, die nach kurzer Zeit verschwinden. Dienste, die solche Funktionen nicht anbieten oder unter ausdrücklich ausgenommene Kategorien fallen, können außerhalb des Anwendungsbereichs der Regelung liegen.¹⁶

Die Annäherung dreier vergleichbarer demokratischer Staaten an ein Modell aus Verbot und zertifizierten Ausnahmen zeigt, dass ein ähnlicher europäischer Rahmen weder ein Sonderweg noch ein Bruch mit internationaler Regulierungspraxis wäre.

Marktanreize und digitale Souveränität

Ein System zertifizierter Ausnahmen vom Verbot würde neue Marktdynamiken schaffen. Anbieter dürften den Markt für unter 16-Jährige nur betreten, wenn sie die verbindlichen Sicherheitsstandards bereits vor dem Produktstart erfüllen. Die Kriterien für eine Ausnahme sollten von einer Regulierungsbehörde festgelegt und überwacht werden. Das Prüfverfahren sollte beschleunigt erfolgen, damit sichere Innovationen nicht unnötig verzögert werden. Für alle Anbieter sollten dieselben Standards gelten. Für etablierte Plattformen mit einer Vorgeschichte von Verstößen gegen Kinder- und Jugendschutzpflichten sollte die Aufsicht jedoch strenger ausfallen. Vor der Erteilung einer Ausnahme sollten für diese Anbieter strengere Prüfmaßstäbe gelten.

Um eine übermäßig komplexe Vorabprüfung der Einhaltung regulatorischer Vorgaben zu vermeiden, könnte die Kommission ein einfacheres Verfahren zur Selbsterklärung in Betracht ziehen. Dessen Verlässlichkeit könnte durch stichprobenartige Kontrollen und Tests sichergestellt werden. Ein solches Modell funktioniert jedoch nur, wenn Verstöße mit sehr hohen Sanktionen belegt werden, die eine tatsächlich abschreckende Wirkung entfalten.

Zertifizierung als
Zugangsvoraussetzung

Beschwerden und Untersuchungen bei Verstößen können grundsätzlich auf den bestehenden Verfahren des Digital Services Act aufbauen. Sie müssen jedoch schneller greifen. Ziel ist es, unmittelbare Schäden zu verhindern und Sanktionen zu verhängen, die das Verhalten der Anbieter tatsächlich verändern.

Der Unterschied zur allgemeinen DSA-Durchsetzung ist einfach, aber entscheidend. Liegt eine glaubhafte Beschwerde mit Belegen für einen Verstoß gegen „Safe Social“-Standards vor und hält die Kommission diese Beschwerde in einer ersten Prüfung für wahrscheinlich begründet, sollte der Dienst im betroffenen Mitgliedstaat vorübergehend vom Markt genommen werden können. Die Aussetzung bleibt bestehen, bis der Verstoß behoben ist und sich nicht wiederholt.

Der Kern dieses Ansatzes liegt nicht nur in hohen Standards und ihrer konsequenten Durchsetzung. Entscheidend ist vielmehr, Marktkräfte so zu nutzen, dass sich sichere und verantwortungsvolle Angebote auch wirtschaftlich durchsetzen. Wenn Unternehmen dauerhafte Ermittlungen und Bußgelder lediglich als Kosten ihres Geschäftsmodells einkalkulieren können, ist die Regulierung gescheitert. Erfolgreich ist sie erst dann, wenn Sicherheit nicht nur Voraussetzung für den Marktzugang ist, sondern auch zu einem Wettbewerbsmerkmal wird. Sichere Produkte müssen für Verbraucherinnen und Verbraucher attraktiver sein.

Sicherheit, Wettbewerb
und Interoperabilität

Ohne Interoperabilität würde dieses Potenzial jedoch durch Netzwerkeffekte zunichtegemacht. Nutzerinnen und Nutzer würden weiterhin bei weniger sicheren Diensten bleiben, um ihre bestehenden Kontakte und Inhalte nicht zu verlieren. Deshalb ist Interoperabilität ein zentrales Kriterium für „Safe Social“. Wenn die Netzwerkeffekte der heutigen Plattformen aufgebrochen werden, können europäische Unternehmen leichter in einen neuen Markt ein-

treten. Dieser Markt wäre nicht länger von wenigen Oligopolisten kontrolliert. Europäische Anbieter könnten zudem von einer wachsenden Nachfrage nach vertrauenswürdigen heimischen Produkten profitieren.

Gleichzeitig verhindert Interoperabilität, dass neue Monopole entstehen. Kein Anbieter kann das frühere Geschäftsmodell aus Marktmacht und Ausbeutung einfach wiederholen. Der Wechsel zwischen Diensten wird deutlich einfacher. Der Wettbewerb würde sich dann auf das richten, was Verbraucherinnen und Verbraucher tatsächlich erwarten: hohe Sicherheitsstandards und ein attraktives Nutzererlebnis.

Auch das technische Argument gegen Interoperabilität verliert an Gewicht. In der Vergangenheit scheiterten ähnliche Ansätze oft daran, bestehende Plattformen nachträglich interoperabel zu machen. Bei neuen Anbietern stellt sich dieses Problem nicht. Für sie können klare Anforderungen von Beginn an gelten. Zusätzlich verändert der schnelle Fortschritt bei KI-Agenten die Ausgangslage. Es braucht nicht zwingend ein einheitliches technisches Protokoll für den gesamten Markt, eine maschinenlesbare Datenschnittstelle oder API kann ausreichen.

Damit wird europäische digitale Souveränität für Bürgerinnen und Bürger konkret erfahrbar. Europa könnte zugleich ein neues Modell für digitale Dienste entwickeln.

Dieser Wandel ist neu und folgenreich. Die Interoperabilitätsstudie der Europäischen Kommission aus dem Jahr 2026 kommt zu dem Schluss, dass Interoperabilität in sozialen Medien grundsätzlich technisch machbar ist. Sie warnt jedoch davor, ein einziges gemeinsames Protokoll für Plattformen mit unterschiedlichen Architekturen auszuhandeln.¹⁷ Ein solches Verfahren wäre langsam, konfliktträchtig und könnte veraltete technische Entscheidungen im Recht festschreiben. Dieses Argument verliert an Überzeugungskraft, wenn KI-Agenten unterschiedliche Dienste nahtlos verbinden können. Diese technische Möglichkeit wurde in der Studie nicht berücksichtigt, weil KI diese Fähigkeit erst seit Kurzem erreicht hat.

Bestehende System-
grenzen mit KI-Agenten
überwinden

Regulierer müssen daher nicht ein gemeinsames Protokoll unterhalb des gesamten Marktes vorschreiben. Es genügt, dass jedes zertifizierte Produkt eine einfache API (maschinenlesbare Lese- und Schreibschnittstelle) bereitstellt. Die Integration findet dann auf Anwendungsebene statt. Zertifizierte Apps können mithilfe agentischer KI Inhalte aus anderen Diensten lesen und dort veröffentlichen – jeweils nur in dem Umfang, den Nutzerinnen und Nutzer autorisiert haben. Erste Prototypen solcher Anwendungen existieren bereits. Die Verantwortung für die Inhaltsmoderation liegt weiterhin bei der Plattform, auf der ein Beitrag ursprünglich veröffentlicht wird. Andere Dienste können auf dieser Grundlage zusätzliche Sicherheitsfilter und Nutzerkontrollen anbieten.

Ein API-basierter Interoperabilitätsstandard hält die Verpflichtung schlank und überprüfbar. Die technische Integrationsschicht kann sich mit der Technologie weiterentwickeln, ohne im Gesetz festgeschrieben zu werden. Zugleich behalten Regulierungsbehörden die entscheidenden Hebel: Marktzugang, Prüfung gleichwertiger API-Funktionalität und Durchsetzung gegen Diskriminierung. Da diese Pflicht nur für neue Anbieter gilt, die eine Zertifizierung anstreben, müssen die technischen Altlasten bestehender Plattformen nicht gelöst werden.

Recht und Politik: Ein stufenweiser Ansatz

Um das Ziel eines „Safe Social“-Marktes zu erreichen, braucht es neue gesetzliche Standards und eine wirksame Aufsicht. Die EU muss jedoch nicht bei null beginnen. Der Schutz von Kindern im Netz ist bereits im europäischen Recht verankert. Bestehende Grundsätze, Schutzpflichten, Aufsichtsstrukturen und Durchsetzungsverfahren können als Grundlage dienen.

Die EU könnte diese Änderungen im Rahmen einer gezielten Überprüfung des Digital Services Act und des Digital Markets Act voranbringen. Möglich wäre auch ein neues Gesetzgebungsinstrument, etwa im Rahmen des Digital Fairness Act.

Gleichzeitig muss klar sein: Ein solcher Rahmen entsteht nicht über Nacht. Die Festlegung der Kriterien für zertifizierte Ausnahmen und Interoperabilität wird Zeit brauchen. Sie kann Monate oder Jahre in Anspruch nehmen. Dennoch darf Europa nicht abwarten. Ein Notverbot darf aber auch kein dauerhaftes Vakuum schaffen, das Kinder und Plattformen gleichermaßen dazu drängt, das Recht zu umgehen.

Deshalb braucht es ein stufenweises Vorgehen. Wahrscheinlich werden mehrere Mitgliedstaaten in den kommenden Monaten Verbote oder Zugangsbeschränkungen für heutige Social-Media-Produkte für unter 16-jährige einführen. Parallel dazu sollte die EU mit der Entwicklung der „Safe Social“-Standards beginnen.

Eine stufenweise
Regulierungsstrategie

In der Übergangsphase zwischen Verboten und der Öffnung eines neuen Marktes können klare Mindestregeln für sichere soziale Dienste formuliert werden. So können Unternehmen frühzeitig mit der Entwicklung neuer Angebote beginnen. Zugleich bleibt Raum für spätere Anpassungen durch Regulierung und technische Weiterentwicklung.

Fazit

In vielen EU-Mitgliedstaaten gibt es starken politischen Druck, soziale Medien für Kinder unter 16 Jahren schnell mit Altersbeschränkungen zu versehen. Angesichts der bestehenden Fehlentwicklungen und der damit verbundenen Risiken für Kinder und Jugendliche ist diese Reaktion nachvollziehbar.

Über Alterskontrollen
hinaus: Sichere soziale
Medien gestalten

Eine Altersgrenze darf jedoch kein Selbstzweck sein. Wenn sie alleinsteht, nimmt sie Kindern die Chance, die Vorteile digitaler Technologien zu nutzen. Das wäre der falsche Ansatz, denn das eigentliche Versagen liegt bei den etablierten Technologieunternehmen. Sie stellen unter den heutigen Marktregeln keine sicheren Produkte für Kinder bereit.

Europa kann es besser machen. Europa kann Kinder besser schützen, neue Wettbewerber ermöglichen und digitale Souveränität dort greifbar machen, wo sie für Bürgerinnen und Bürger am unmittelbarsten spürbar ist: im digitalen Alltag ihrer Kinder. Erforderlich ist eine „Safe Social“-Politik, die Sicherheit verbindlich vorschreibt und Marktanreize so setzt, dass sich verantwortungsvolles Handeln auch wirtschaftlich lohnt.

- 1 WHO Regional Office for Europe & Health Behaviour in School-aged Children (HBSC), A Focus on Adolescent Social Media Use and Gaming in Europe, Central Asia and Canada (Sept. 2024) (Die problematische Nutzung sozialer Medien bei 11- bis 15-Jährigen stieg in 44 Ländern und Regionen von 7 % im Jahr 2018 auf 11 % im Jahr 2022.), <https://www.who.int/europe/news/item/25-09-2024-teens--screens-and-mental-health> (letzter Abruf: 14.7.2026); Office of the U.S. Surgeon General, Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory (2023), <https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf> (letzter Abruf: 14.7.2026).
- 2 Jonathan Haidt, Jean Twenge & Zach Rausch, Social Media and Mental Health: A Collaborative Review (laufendes, unveröffentlichtes Manuskript, New York University), abrufbar unter <https://jonathanhaidt.com/social-media/> (letzter Abruf: 14.7.2026). Hierbei handelt es sich um ein fortlaufend aktualisiertes Dokument, das korrelative, Längsschnitt- und experimentelle Studien zusammenfasst.
- 3 Rechtsstreitigkeiten im Zusammenhang mit dem Tod von Kindern in Verbindung mit der TikTok-„Blackout-Challenge“, darunter Anderson gegen TikTok, Inc., Nr. 22-3061 (3. Cir., 27. August 2024) sowie Klagen britischer Familien im Namen von Kindern, die im Jahr 2022 starben: Grieving Mum suing TikTok says hearing was 'painful', 17. Januar 2026, <https://www.bbc.co.uk/news/articles/c20gvp3pzwpo> (letzter Abruf: 14.7.2026).
- 4 Children's Commissioner for England, "A lot of it is actually just abuse": Young People and Pornography (2023), <https://www.childrenscommissioner.gov.uk/resource/a-lot-of-it-is-actually-just-abuse-young-people-and-pornography/> (letzter Abruf: 14.7.2026); Thorn, Sexual Extortion & Young People: Navigating Threats in Digital Environments (Juni 2025), <https://www.thorn.org/research/library/sexual-extortion-young-people/> (letzter Abruf: 14.7.2026).
- 5 Ifo-Umfrage: <https://www.ifo.de/publikationen/2025/aufsatz-zeitschrift/zwischen-likes-und-lernen> (letzter Abruf: 14.7.2026).
- 6 Forsa-Umfrage: <https://www.rtl.de/news/kommt-jetzt-ein-social-media-verbot-fuer-kinder-in-deutschland-umfrage-zu-tiktok-instagram-und-co-id31006119.html> (letzter Abruf: 14.7.2026).
- 7 Appinio: <https://research.appinio.com/#/de/survey/public/eWF0ZeBS> (letzter Abruf: 14.7.2026). Siehe auch: Deutsches Schulportal: <https://deutsches-schulportal.de/schule-im-umfeld/social-media-gesetz-australien-umfrage-sollten-soziale-medien-fuer-kinder-unter-16-auch-in-deutschland-verboden-sein/> (letzter Abruf: 14.7.2026).
- 8 YouGov, Most Europeans in six countries support banning social media for under-16s, Feldforschung 6.–24. März 2026 (veröffentlicht: Juni 2026), <https://yougov.com/en-gb/articles/54429-most-europeans-in-six-countries-support-banning-social-media-for-under-16s> (letzter Abruf: 14.7.2026).
- 9 Im März 2026 befand eine Jury des Obersten Gerichtshofs von Los Angeles in der Rechtssache K.G.M. gegen Meta Platforms, Inc. (Social Media Cases, JCCP Nr. 5255) Meta und YouTube auf der Grundlage der Produkthaftung und der Theorie des „süchtig machenden Designs“ für die Schäden eines jugendlichen Klägers haftbar; und in der Rechtssache Staat New Mexico gegen Meta Platforms, Inc., Nr. D-101-CV-2023-02838 (1. Bezirksgericht, Santa Fe County) befand eine Jury Meta gemäß dem Unfair Practices Act des Bundesstaates für haftbar und sprach eine Entschädigung in Höhe von 375 Millionen US-Dollar zu.
- 10 Über Jahrzehnte war Rauchen gesellschaftlich akzeptiert und wurde aktiv beworben. Erst als die gesundheitlichen Schäden wissenschaftlich bewiesen wurden, reagierten Staaten mit Warnhinweisen und Rauchverboten. Dieser politische Wendepunkt wird heute oft als „Tobacco Moment“ bezeichnet.
- 11 Siehe z. B.: Frankreich (Gesetzesentwurf zum Verbot der Nutzung sozialer Medien durch Kinder unter 15 Jahren, der im Januar 2026 vom Nationalrat verabschiedet wurde und nun dem Senat zur Beratung vorliegt); Spanien (Gesetzesentwurf zur Festlegung eines Mindestalters von 16 Jahren mit obligatorischer Altersüberprüfung, angekündigt für 2026); Dänemark (Regierungsbeschluss zum Verbot für unter 15-Jährige, mit der Möglichkeit für Eltern, diese Regelung für 13- und 14-Jährige außer Kraft zu setzen); und Griechenland (Pilotprojekt zur Altersbeschränkung für unter 15-Jährige und zur Altersüberprüfung mittels App). Für eine Übersicht siehe Euronews, Which European countries are considering banning social media for children under 16? (2025), <https://www.euronews.com/next/2025/12/23/which-european-countries-are-considering-banning-social-media-for-children> (letzter Abruf: 14.7.2026).
- 12 Leonardo Burszty, Benjamin Handel, Rafael Jiménez-Durán & Christopher Roth, When Product Markets Become Collective Traps: The Case of Social Media, American Economic Review 115(12): 4105–36 (2025) (auch NBER Working Paper Nr. 31771), <https://www.nber.org/papers/w31771> (letzter Abruf: 14.7.2026), mit der Feststellung, dass viele Nutzerinnen und Nutzer in einer Produkt-Markt-Falle gefangen sind – sie würden es zwar vorziehen, wenn Plattformen wie TikTok und Instagram nicht existierten, nutzen sie aber dennoch weiter, aufgrund von Netzwerkeffekten und aus Angst, etwas zu verpassen.

-
- 13 Im April 2026 veröffentlichte die Europäische Kommission eine Lösung zur Altersüberprüfung unter Wahrung des Datenschutzes, die für die Integration in die nationalen EUDI-Wallets (European Digital Identity) konzipiert ist. Sie nutzt Zero-Knowledge-Proofs, um zu bestätigen, dass ein Nutzer eine Altersgrenze erreicht hat, ohne dabei das Geburtsdatum, eine Ausweisnummer oder andere personenbezogene Daten preiszugeben. Siehe European Commission, The EU approach to age verification, <https://digital-strategy.ec.europa.eu/en/policies/eu-age-verification> (letzter Abruf: 14.7.2026).
 - 14 Parliament of Canada, Bill C-34 (45-1), <https://www.parl.ca/DocumentViewer/en/45-1/bill/C-34/first-reading>; Government of Canada, Bill C-34, the Safe Social Media Act, <https://www.canada.ca/en/canadian-heritage/services/safe-social-media-act.html> (letzter Abruf: 14.7.2026).
 - 15 HE 37, <https://www.bmbfsfj.bund.de/resource/blob/290236/32c7a742b1ee00b498fca42c37784c99/20260624-handlungsempfehlungen-expertenkommission-kinder-und-jugendmedienschutz-data.pdf> (letzter Abruf: 14.7.2026).
 - 16 Online Safety (Age-Restricted Social Media Platforms) Amendment Rules 2026 (Cth), Federal Register of Legislation No. F2026L00370, <https://www.legislation.gov.au/F2026L00370/asmade/text> (letzter Abruf: 14.7.2026); siehe auch Australian Government Department of Infrastructure, Transport, Regional Development, Communications and the Arts, Updates to social media minimum age rules.
 - 17 European Commission, Directorate-General for Communications Networks, Content and Technology, Study of interoperability tools in the digital single market (Publications Office of the European Union, 2026), <https://op.europa.eu/en/publication-detail/-/publication/7ed3fe8e-42a7-11f1-8095-01aa75ed71a1/language-en> (letzter Abruf: 14.7.2026).

Impressum

Die Autoren

Dr. Ben Scott ist CEO von Reset, einer globalen Initiative, die sich für demokratische Werte in der digitalen Welt einsetzt und mit Regierungen, Stiftungen sowie der Zivilgesellschaft an der Gestaltung zukunftsfähiger Technologiemarkte arbeitet. Zuvor war er Politikberater für Innovation der damaligen US-Außenministerin Hillary Clinton und koordinierte die technologisch-politische Beratergruppe ihres Präsidentschaftswahlkampfes 2016.

Dr. Pencho Kuzev ist Policy Advisor für Daten- und Wettbewerbspolitik bei der Konrad-Adenauer-Stiftung in Berlin. Er entwickelt Konzepte, wie Europa digitale Regulierung wirksam durchsetzen und zugleich seine technologischen Fähigkeiten stärken kann. Zudem ist er Initiator und Veranstalter des European Data Summit.

Herausgeberin: Konrad-Adenauer-Stiftung e. V., 2026, Berlin

Kontakt:

Pencho Kuzev

Daten- und Wettbewerbspolitik

Analyse und Beratung

Pencho.Kuzev@kas.de

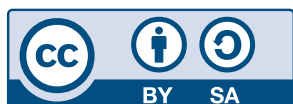
Tel. +49 30 26996-3247

Bildnachweis Titelseite: Rawpixel/smarterpix.com, mit KI bearbeitet

Gestaltung und Satz: Konrad-Adenauer-Stiftung e. V.

Hergestellt mit finanzieller Unterstützung der Bundesrepublik Deutschland.

Diese Veröffentlichung der Konrad-Adenauer-Stiftung e. V. dient ausschließlich der Information. Sie darf weder von Parteien noch von Wahlwerbenden oder -helfenden zum Zwecke der Wahlwerbung verwendet werden. Dies gilt für Bundestags-, Landtags- und Kommunalwahlen sowie für Wahlen zum Europäischen Parlament.



Der Text dieses Werkes ist lizenziert unter den Bedingungen von „Creative Commons Namensnennung-Weitergabe unter gleichen Bedingungen 4.0 international“, CC BY-SA 4.0 (abrufbar unter: <https://creativecommons.org/licenses/by-sa/4.0/legalcode.de>).

ISBN 978-3-98574-365-0