Die Empfehlung einer Expertenkommission veranlasst das Bundesfamilienministerium, ein Social-Media-Verbot für Kinder einzufordern. **Jens Berger** argumentiert in seinem Beitrag, dass der Kinderschutz nur ein Vorwand ist, um „das Ende der Anonymität im Internet“ einzuläuten. Australien, das „vor gut einem halben Jahr ein Social-Media-Verbot für Kinder unter 16 Jahren einführte“, scheiterte mit diesem Versuch, da entsprechende Maßnahmen wie z.B. Gesichtserkennung technisch leicht zu umgehen sind. Zugleich werden durch biometrische Daten oder Ausweisprüfungen erhebliche Datenschutzrisiken geschaffen, da dadurch „Datenkraken aus den USA die Möglichkeit [gegeben wird], die Ausweisdaten aller Nutzer abzufischen“. Das wird auch „von staatlichen Akteuren ge- oder besser missbraucht“ unter dem Vorwand der „Terrorabwehr“, „Kampf gegen „russische Desinformation““ und anderen sicherheitspolitischen Bedenken. Als Alternative schlägt unser Autor einen technischen Jugendschutz durch Elternkontrollen vor, der ohne Massenüberwachung auskommt. Wir danken unseren Leserinnen und Lesern, die sich nicht von den sommerlichen Temperaturen abhalten ließen, uns zu schreiben. Die Leserbriefe hat **Ala Goldbrunner** für Sie zusammengestellt.

---

1. Leserbrief

Sehr geehrte Redaktion,

Jens Berger trifft den entscheidenden Punkt: Es geht bei dieser Debatte nicht nur um Kinder- und Jugendschutz. Es geht um die Frage, ob unter dem Deckmantel des Kinderschutzes eine allgemeine Identifikationspflicht im Internet eingeführt werden soll.

Diese Tendenz ist seit Jahrzehnten sichtbar. Immer wieder werden emotionale Themen vorgeschoben, um Eingriffe in Freiheitsrechte technisch, politisch und gesellschaftlich akzeptabel zu machen. Früher waren es Netzsperren, Vorratsdatenspeicherung oder der Bundestrojaner, heute ist es der Schutz von Kindern vor sozialen Medien. Das Muster bleibt gleich: Wer dagegen ist, muss sich erst einmal rechtfertigen, obwohl eigentlich diejenigen in der Pflicht wären, die eine Infrastruktur zur Kontrolle aller Nutzer schaffen wollen.

Besonders problematisch ist dabei, dass Kindern offenbar nicht einmal ansatzweise Selbstverantwortung zugetraut werden soll. Natürlich brauchen Kinder Schutz, Begleitung und Grenzen. Aber sie brauchen eben auch Medienkompetenz, Vertrauen und schrittweise Eigenverantwortung. Wer alles über Verbote, Identifikation und technische Zugangskontrollen lösen will, erzieht keine mündigen Menschen, sondern gewöhnt die

Gesellschaft an Überwachung.

Der Wunsch, dass Eltern entsprechende Schutzmechanismen einrichten sollen, ist völlig richtig. Genau dafür gibt es längst technische Möglichkeiten. Auf Rechnern, Smartphones und auch in vielen Routern lassen sich Zeitlimits, Filter, App-Sperren und Jugendschutzprofile einrichten. Wer Kinder schützen möchte, kann das heute bereits tun. Eine allgemeine Pflicht zur Alters- oder Identitätsprüfung aller Nutzer ist deshalb nicht nur unverhältnismäßig, sondern politisch durchsichtig.

Noch heikler wird es, wenn solche Funktionen auf Betriebssystemebene verpflichtend eingebaut werden sollen. Dann betrifft es nicht nur Haushalte mit Kindern, sondern jeden Rechner, jedes Smartphone und jeden Nutzer. Damit wäre eine Infrastruktur geschaffen, mit der sich das Alter, später vielleicht auch die Identität, zentral oder halbzentral verifizieren lässt. Wer glaubt, eine solche Struktur werde niemals zweckentfremdet, hat aus den letzten Jahrzehnten wenig gelernt.

Nebenbei würde eine solche Lösung auch noch ein zweites Problem für große Konzerne lösen: Sie stärkt die Kontrolle von Microsoft, Apple und Google über die digitale Grundinfrastruktur. Für freie Systeme wie Linux könnte das schnell zu einem massiven Problem werden, wenn bestimmte Dienste nur noch über offiziell zertifizierte Alters- oder Identitätsmechanismen erreichbar wären. Was als Kinderschutz verkauft wird, könnte am Ende auch ein weiterer Schlag gegen offene, freie und unabhängige Betriebssysteme sein.

Kinderschutz ist wichtig. Aber er darf nicht als trojanisches Pferd für die Abschaffung anonymer Internetnutzung missbraucht werden. Die richtige Antwort wäre Aufklärung, Medienkompetenz, elterliche Verantwortung und freiwillig nutzbare technische Schutzmaßnahmen — nicht eine Identifikationsarchitektur für alle.

Mit freundlichen Grüßen
Niki Beckmann

---

2. Leserbrief

Liebe NachDenkSeiten-Redaktion, lieber Jens Berger,

es stimmt, der Datenschutz darf für den Kinderschutz nicht über Bord geworfen werden. Es gäbe jedoch Alternativen, z.B. hardwarebasierte Lösungen, die ganz ohne Daten auskämen,

doch an denen hat die Tech-Industrie selbstverständlich kein Interesse.

In meinem Leserbrief vom 24. Februar 2026 habe ich schon einmal deutlich gemacht, warum die Klarnamenpflicht nicht die Lösung für Kinder- und Jugendschutz im Internet sein sollte und welche Alternativen es gäbe. Auch die EUDI-Wallet sollte nicht zum Einsatz kommen.

Dennoch braucht es Kinder- und Jugendschutz vor Social Media. Denn so, wie es im Moment läuft, ist es bewusst tolerierte Kindeswohlgefährdung und unterlassene Hilfeleistung, weil wir der Tech-Industrie hörig sind.

Gestern ist ein Interview mit mir zu den Empfehlungen der Expertenkommission erschienen. Vielleicht mögen Sie auch auf Ihrer Seite darauf hinweisen.

noz.de/deutschland-welt/politik/artikel/kein-social-media-verbot-fuer-kinder-diese-mutter-ist-verzweifelt-50827886

Datenschutz und Kinderschutz müssen Hand in Hand gehen und sollten sich nicht gegenseitig blockieren.

Viele Grüße

Jeannette Deckers (Lehrerin, Mutter zweier Kinder, *Petentin [Anm. A.G.: weibliche Person, die eine Petition einreicht]* der Petition “Kein Zugang zu Sozialen Medien für Kinder und Jugendliche unter 16 Jahren” und Autorin von “Schutzlos digital”, das im September erscheint)

---

3. Leserbrief

Sehr geehrter Herr Berger,

zu Ihrem letzten Absatz in Ihrem Artikel hätte ich für Sie die Information, dass diese Jugendschutzfunktionen von der Firma Apple in der nächsten großen Aktualisierung des Betriebssystems iOS umgesetzt werden.

Wenn Sie sich das selbst gerne anschauen möchten, hier die Verknüpfung zum Video der Eröffnung der Entwicklerkonferenz aus diesem Jahr:
developer.apple.com/videos/play/wwdc2026/101/

Der Teil zur Sicherheit beginnt ab Minute 17:00.

Mein Tipp: Schalten Sie den Ton aus, blenden die deutschen Untertitel ein und lesen Sie nur diese. Das ist deutlich angenehmer.

Also in Bezug auf Ihren Artikel ein kleiner Lichtblick.

Freundliche Lesergrüße
P. W. S.

---

4. Leserbrief

Sehr geehrter Herr Berger,

am Ende ihres Artikels schreiben sie:

> “Warum verpflichtet die EU die Anbieter von Betriebssystemen von Smartphones und Computern nicht einfach, einen „Jugendschutzmodus“ einzurichten? In diesem Modus könnten Erziehungsberechtigte dann bestimmte Apps und Angebote nach eigenem Gutdünken für ihre Kinder blockieren oder auch freigeben.”

Tatsächlich gibt es solche Möglichkeiten bereits, nur halt nicht verpflichtend. Für Android-Geräte gibt es beispielsweise die App “Family Link” von Google. Apple hat einen entsprechenden Jugendschutzmodus direkt im iOS integriert. Für PCs gibt es ebenfalls entsprechende Möglichkeiten. Fast alle Anbieter von Virenschutz bieten auch derartige Programme an.

Mit freundlichen Grüßen
Daniel Rische

---

5. Leserbrief

Sehr geehrter Herr Berger,

Es geht ja nicht nur um die Identifikationspflicht.

Langsam aber sicher wird der Bürger in eine digitale Zwangsjacke / Gefängnis gesteckt:

Identifikationspflicht

EU- ID Wallet

Digitaler Euro (Abschaffung cash)

Erweiterte Befugnisse für Sicherheitskräfte.

Der wichtigste Punkt dabei ist, dass jede Maßnahme zum Guten oder Bösen angewendet werden kann.

Wir verfügen bereits heute über Beweise, dass die EU und in Verlängerung davon die einzelnen Regierungen den Rechtsstaat ausgehebelt haben: die Sanktionen gegen Jacques Baud und weitere EU Bürger erweitert auf ihre Familien sprechen für sich.

Bedeutet konkret mit an Sicherheit grenzender Wahrscheinlichkeit, dass den Bürgern übel mitgespielt werden wird im digitalen Kontroll-Universum.

Mit freundlichem Gruß
Patrick Janssens

---

6. Leserbrief

Lieber Herr Berger,

sie fragen in ihrem Artikel “Social-Media-Verbot für Kinder? Falsch – es geht um eine Identifikationspflicht für alle”, warum nicht einfach Anbieter von Betriebssystemen verpflichtet würden, einen Jugendschutzmodus einzuführen. Diese Pflicht wurde bereits vor 1,5 Jahren durch Neufassung des Jugendmedienschutzstaatsvertrag eingeführt:

(13.12.2024):

> *“Bundesländer beschließen Porno-Filter für Betriebssysteme – Auch*

> *Betriebssysteme müssen laut dem reformierten Jugendmedienschutz-Staatsvertrag bald sicherstellen, dass sie eine “Jugendschutzvorrichtung” haben. Die Regierungschefs der Länder haben am Donnerstag bei der Ministerpräsidentenkonferenz in Berlin eine erneute Reform des Jugendmedienschutz-Staatsvertrags (JMStV) beschlossen. Damit sollen Pornofilter schon auf der elementaren Ebene von PCs, Laptops und Smartphones installiert und eine Alterskennzeichnung für Webseiten und Apps eingeführt werden. Laut dem überarbeiteten Paragraf 12 müssen Anbieter von Betriebssystemen künftig sicherstellen, dass diese über eine “Jugendschutzvorrichtung” verfügen. Eine solches Filtersystem, heißt es weiter, “muss in einfacher, leicht zugänglicher und abgesicherter Weise aktiviert, deaktiviert und angepasst werden können”.”*

Im neuen Jugendmedienschutzstaatsvertrag wurden auch einige weitere Kontrollfunktionen der Landesmedienanstalten über das Internet und dessen Content-Anbieter eingeführt:

> *“3. § 2…„Maßnahmen gegen Anbieter von Telemedien oder Betriebssystemen mit Sitz in einem anderen Mitgliedstaat sind auf Grundlage dieses Staatsvertrages zulässig, wenn die Maßnahme*
> *1.zum Schutz*
> *a) der öffentlichen Sicherheit und Ordnung, einschließlich des Jugendschutzes, insbesondere im Hinblick auf*
> *aa) die Verhütung, Ermittlung, Aufklärung, Verfolgung und Vollstreckung von Straftaten und Ordnungswidrigkeiten,*
> *bb) die Bekämpfung der Verunglimpfung aus Gründen der Rasse, des Geschlechts, des Glaubens oder der Nationalität,*
> *cc) Verletzungen der Menschenwürde einzelner Personen oder*
> *dd) **die Wahrung nationaler Sicherheits- und Verteidigungsinteressen**,*
> *b) **der öffentlichen Gesundheit** oder*
> *c)der Interessen der Verbraucher und der **Interessen von Anlegern** erforderlich ist,*
> *…*
> *19. § 20 wird wie folgt geändert:*
> *„Darüber hinaus kann die zuständige Landesmedienanstalt den am Zahlungsverkehr Beteiligten, **insbesondere den Kredit- und Finanzdienstleistungsunternehmen**, nach vorheriger Nennung unzulässiger Angebote im Sinne des § 4 Abs. 1 und 2 die Mitwirkung an Zahlungen für diese*

> *Angebote untersagen, ohne dass es einer vorherigen Inanspruchnahme des Anbieters durch die Aufsicht bedarf.“”*

Die neue Macht der Landesmedienanstalten, Zahlungen an ausländische Content-Anbieter zu unterbinden, wurde zunächst an Porno-Portalen ausprobiert:

(7.8.2025):

> *“Die Landesmedienanstalten wollen Finanzdienstleister dazu zwingen, Zahlungen an Erotikportale wie Pornhub und Youporn abzulehnen – auch Zahlungen Erwachsener. Rechtsgrundlage ist der neue Jugendmedienschutz-Staatsvertrag (JMStV). Das hat der Vorsitzende der Kommission für Jugendmedienschutz (KJM), Marc Jan Eumann, dem Evangelischen Pressedienst (epd) erklärt.”*

Ich denke mir das so, dass unterschiedlichste Wege der Kontrolle des Internets in den vergangenen Jahren gesetzlich parallel eingeführt wurden. Die neue Identifikationspflicht im Internet wäre eine neue Facette. Je nach politischem Gegner und Zweck wird man auf unterschiedliche Gesetzesgrundlagen zurückgreifen können, die man für die Kontrolle des Internets einsetzen kann.

Mit freundlichen Grüßen
A.

---

7. Leserbrief

Moin,

Sie nennen das Kind beim Namen, Herr Berger, und das treffend pointiert bereits in der Überschrift. Vielen Dank dafür! Eine dringend notwendige Klarheit, die hoffentlich dafür sorgt, daß das Thema auf demokratischer Ebene diskutiert wird.

Das Problem betrifft nicht nur Deutschland, sondern wird weltweit ausgerollt. Deutschland ist, wie immer, quasi das Nesthäkchen der Digitalisierung. Ward es zunächst das mächtige Bundesdatenschutzgesetz, das übergriffigen Konzernen Riegel vorschob, wurde es mit der EU-europäischen DSGVO aufweichend ergänzt; aufweichend deswegen, weil insbesondere

Artikel 6 für die Rechtfertigung von allerlei Datensauereien herhalten muß, allen voran Buchstabe f) (das allein wäre ein Thema für sich): dsgvo-gesetz.de/art-6-dsgvo/

Das ist bei der Debatte nach Jugendschutz in Bezug auf soziale Medien besonders pikant, denn im letzten Teilabsatz heißt es ausdrücklich:

> “insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.”

Gemäß einschlägiger Datenschutzvorschriften ist das gesamte Vorhaben rechtlich auf wackelige Füße gestellt, denn man unterstellt einfach, daß das Persönlichkeitsrecht weniger wöge, und, wie in diesem Fall, das Recht des Kindes als Schutzbefohlenes, das per se höher als das eines Erwachsenen zu gewichten ist.

Auch Sanktionsmöglichkeiten wären denkbar: Wer in der EU-Liste steht, der kriegt keine Altersfreigabe und kann die damit verbundenen Dienste nicht nutzen.

Was bei der Debatte über Altersprüfungen sehr gerne unter den Tisch fällt, das sind Datenlecks. Da stehen sensible persönliche Daten, die zumindest auf dem Papier besonders zu schützen sind (insbesondere medizinische Daten), teilweise komplett ungeschützt, für Jedermann abrufbar, im Internet. Es wurden bereits mehrere solcher Fälle dokumentiert, in verschiedenen Ländern wie England, den USA oder Indien, mit Millionen von Datensätzen über natürliche Personen, inklusive besonders sensiblen und daher besonders zu schützenden medizinischen wie auch biometrische Daten.

Insbesondere der Diebstahl biometrischer Daten, beispielsweise Fingerabdrücke und Gesichtserkennung, ist irreversibel, denn die eigenen körperlichen Merkmale lassen sich nicht mal eben ändern wie ein Paßwort. Ein fiktives Beispiel wurde in einem der “Batman”-Filme gezeigt: Kriminelle erbeuteten die Fingerabdrücke von Bruce Wayne, um seine Firma über Börsengeschäfte zu ruinieren. Werden biometrische Daten entwendet, so kann man sich kaum eines digitalen Identitätsdiebstahles erwehren.

> “Ein solcher Datenpool weckt Begehrlichkeiten. Sei es die Terrorabwehr […] oder einfach nur eine so schwere Straftat wie das Bezeichnen eines Bundesministers als „Schwachkopf“ – wenn es diese Daten gibt, werden sie auch […] missbraucht.”

Abgesehen davon, daß diese Bezeichnung mitnichten eine schwere Straftat darstellt, sondern lediglich eine Bagatelle, die unter normalen demokratischen Maßstäben unter Berücksichtigung der Meinungsfreiheit überhaupt nichts ausgelöst hätte (schon gar keine Wohnungsdurchsuchung), so kann ich diese Tatsache mit einem prominenten Beispiel untermauern:

Während der “Corona”-PLANdemie waren Gastwirte gezwungen, Namen & Adressen inklusive Datums- & Zeitangaben ihrer Gäste festzuhalten. Nachdem Phantasienamen wie “Donald Duck” kursierten, weil den Menschen ihr eigener Datenschutz tatsächlich wichtig war, wurde dies unter Strafandrohung für die Wirte unterbunden. Diese, sodann “korrekt” gesammelten Daten, wurden dann später in manchen Bezirken tatsächlich von der Polizei verwendet, sogar bei kleineren Vergehen, obwohl es zuvor ausdrücklich und “hoch & heilig versprochen” hieß, daß sie ausschließlich für die Kontaktverfolgung im (irrationalen) “Infektionsfall” genutzt würde, um “Infektionsketten” erfolgreich nachverfolgen und angeblich unterbrechen zu können.

Wer sollte dem Staat nach solch einem vorsätzlichen Datenmißbrauch noch glauben, daß er mit ihnen sorgsam umginge? Ich tue das auf keinen Fall. Und wer garantierte, daß nicht auch Wirte mit diesen Daten sorgsam umgingen? Das weitet sich natürlich aus auf (Sub-)Unternehmen, die im staatlichen oder sonstigen Aufträgen sensible persönliche Daten verarbeiten sollen.

Die neueste Sau, die jetzt zur Zensur verwendet wird: der Mißbrauch von Verschlüsselungen: anti-spiegel.ru/2026/weitere-zensurmassnahmen-in-planung-wie-sie-den-anti-spiegel-auch-dann-weiter-lesen-koennen/

Sprich:

Wenn man sich denn erfolgreich als Ü16 oder Ü18 bei Behörden & Datenkraken präsentierte, dann entscheiden andere Faktoren darüber, was man lesen darf und was nicht. Technischer Hintergrund sind die Zertifikate, die von den großen Browsern wie Googles Chrome, Microsofts Edge, Firefox oder Apples Safari etc. genutzt werden: “westliche” Zertifizierungsstellen sanktionieren dann andere Länder, die selbst auf Nachfrage keine Zertifikate mehr kriegen: die Seite kann in diesen Browsern dann nicht mehr angezeigt werden. Prominentes Beispiel sind russische Seiten, allen voran die offiziellen behördlichen. Natürlich werden zeitgleich ältere oder andere, alternative Browser von großen Seiten wie YouTube rigoros ausgesperrt, sodaß der gemeine Internetnutzer gezwungen ist, eine aktuelle Version der “gängigen” Browser zu installieren.

Ich für meinen Teil nutzte noch nie die “sozialen Medien” wie Facebook oder TikTok und könnte mich als Nicht-Betroffener beruhigt zurücklehnen. Doch ich befürchte, daß die Altersverifikation langfristig auf noch viel mehr Felder ausgedehnt wird und das Internet, wie wir es einst kannten, dann gar nicht mehr ohne künstliche Barrieren genutzt werden kann. Da ich aber auch den Datenschutz sehr hoch halte, kann ich mich nur in die Liste der Warner einreihen, ein solches System gar nicht erst zuzulassen, denn sowohl der Mißbrauch dieses Instrumentes als auch Datenlecks werden meiner Einschätzung nach eintreten.

> “Denn um den Schutz der Kinder geht es ja offensichtlich nicht.”

Wer die Tragweite dieses Vorhabens erfaßt: völlig richtig, das ist nur der Öffner der Büchse der Pandora, moralisch hehr daher kommend, denn welcher Bürger würde die kindliche Unversehrtheit nicht wollen? Daß Diese damit nicht wirklich geschützt wird, verrät man natürlich nicht — sonst könnten Zweifel an dem Vorhaben aufkommen.

Mit freundlichen Grüßen,
Michael Schauberger

---

8. Leserbrief

In Zeiten der feixenden Staatsanwälte und Bademäntel wäre so eine Klarnamenpflicht im Internet ein Sargnagel für die Demokratie …

Ach Moment, ich lege ihn mal in meine Kiste mit den Sargnägeln…. Uuups, da liegen ja schon so viele!

- eine Demokratie, wo die Politik jahrzehntelang nicht den Willen der Bevölkerungsmehrheit tut – ist einfach keine
- eine Demokratie, wo die Politiker/Journalisten wie Muttis es ihren Kindern ‘nur noch besser vermitteln’ wollen, wenn die die Politikerweisheit nicht einsehen, und *nicht mal mehr auf die Idee kommen*, dass viellllleicht auch der Bürger Recht haben könnte – ist keine
- eine Demokratie, wo schwerste Grundrechtseingriffe aus der Coronazeit, deren Falschheit durch die RKI-Files belegt ist, nicht mal *untersucht* werden sollen – ist

hundertprozentig keine!

- eine Demokratie, wo es einfach egal ist, ob eine Partei bei einer Neuauszählung höchstwahrscheinlich ins Parlament (das Heiligtum der Demokratie!) reinkäme – ist eine Bananendemokratie

- eine Demokratie, in der Habeckwitze bald so schlimm sind wie Honeckerwitze – kann auch keine bleiben …

Jeder der hier aufgezählten Sargnägel reicht schon **ganz allein** aus zu zeigen, dass dieses Staatswesen wichtige Eigenschaften einer Demokratie nicht mehr hat.

Martin aus S

---

9. Leserbrief

Wer demnächst in Deutschland etwas im Internet lesen oder sagen will, muss erst seinen Perso vorlegen

Liebe NDS-Redaktion,

dem “braven Bürgersmann” muss doch seine eigene (Total)-Überwachung schmackhaft gemacht werden, denn er soll/muss die ja schließlich bezahlen. “Schutz der Kinder, Schutz vor Desinformation, Schutz vor Terror, Schutz vor Hass & Hetze…” – denn Bullerbü muss leben!

Wie weit das schon geht, kann man auch noch folgenden Artikeln entnehmen:

Unsichtbare digitale Ketten

(Tobias Augenbraun auf Free21)

Ende der freien Rede durch DSA

(Manfred Kölsch auf norberthaering.de)

Viele Grüße

Michael Wrazidlo

---

10. Leserbrief

Liebe NDS, Jens Berger

Danke für den Artikel. Hoffentlich denken die Menschen endlich mal nach…

Der letzte Absatz ist der wichtigste. Eltern sollten nicht vom Staat, der EU usw bevormundet werden. Sie tragen die Verantwortung für die Entwicklung ihrer Kinder in einer Demokratie.

So einfach kann Schutz gehen…
Grüße

Anmerkung zur Korrespondenz mit den NachDenkSeiten

Die NachDenkSeiten freuen sich über Ihre Zuschriften, am besten in einer angemessenen Länge und mit einem eindeutigen Betreff.

Es gibt die folgenden E-Mail-Adressen:

- leserbriefe(at)nachdenkseiten.de für Kommentare zum Inhalt von Beiträgen.
- hinweise(at)nachdenkseiten.de wenn Sie Links zu Beiträgen in anderen Medien haben.
- videohinweise(at)nachdenkseiten.de für die Verlinkung von interessanten Videos.
- redaktion(at)nachdenkseiten.de für Organisatorisches und Fragen an die Redaktion.

Weitere Details zu diesem Thema finden Sie in unserer „Gebrauchsanleitung“.