



Chaos Computer Club

Mündliche Anhörung Landtag SH - Sozialausschuss

Sicheren und kompetenten Umgang mit sozialen Medien stärken

Elina Eickstädt

1. März 2026

Einordnung

Das derzeit diskutierte Verbot von sozialen Medien für Kinder und Jugendliche sowie die bereits vorhandenen Vorstöße in Australien und Großbritannien verfolgen grundsätzlich ein wichtiges Ziel. Der bessere Schutz von Kindern und Jugendlichen im digitalen Raum sowohl vor Missbrauch als auch vor süchtig machenden Gestaltungsformen von Plattformen. Die diskutierten Maßnahmen verfehlen jedoch das Ziel, Plattformanbieter mehr in die Pflicht zu nehmen und für eine echte Veränderung der Geschäftspraktiken zu sorgen. Stattdessen wird ein digitaler Zaun aufgestellt, dessen Auswirkungen sowohl auf das Internet als Infrastruktur als auch im Hinblick auf Schäden für ohnehin schon marginalisierte Gruppen völlig unterbetrachtet bleiben. Es ist gefährlich anzunehmen, dass Plattformen mit Alterskontrollen zu sichereren Orten werden. Und dass Jugendliche mit 16 automatisch die Medienkompetenzen haben, um mit den entsprechend problematischen Geschäftsmodellen von Plattformen umzugehen. Der CCC als größter Hackerverband Europas kann im Rahmen dieser Anhörung primär auf die technischen Aspekte und Implikationen eines Verbots eingehen. Empfehlungen zu Suchtprävention und sozialpädagogischen Aspekten liegen nicht in unserem Expertisebereich. Im Kern des Problems sind aber die Geschäftsmodelle großer Technologieplattformen zu sehen. Deren Praktiken nicht nur darin bestehen, möglichst viele Daten zu sammeln, sondern auch darin, ihre Nutzer:innen möglichst lange auf ihren Plattformen zu halten. Grundsätzlich möchten wir darauf aufmerksam machen, dass mit dem Digitale-Dienste-Gesetz (DSA) bereits ein rechtlicher Rahmen geschaffen wurde, der diverse Maßnahmen zum besseren Schutz von Kindern online vorsieht. Eine konsequente Umsetzung des DSA könnte bereits einen großen Anteil der in den Anträgen umschriebenen Probleme lösen.

Altersnachweise

Ein Mindestalter für soziale Medien, setzt den Einsatz von Altersnachweisen auf betroffenen Plattformen voraus. Grundsätzlich betreffen diese nicht nur Kinder und Jugendliche, sondern alle Nutzer:innen der Plattformen. Unabhängig von der gewählten technischen Durchführung stellen Altersnachweise eine Gefahr für anonyme und pseudonyme Internetnutzung dar. Wie der CCC bereits mehrfach hervorgehoben hat, ist das Recht auf Anonymität eine unabdingbare Voraussetzung für die Wahrnehmung wesentlicher Grundrechte.

Weiter würde eine solche Infrastruktur zu einer Zwangszentralisierung diverser Dienste führen und für die Stärkung von Monopolpositionen sorgen, anstatt Plattformen tatsächlich zu regulieren. Aufgrund der ausführlichen Studienlage im Hinblick auf technische Konzepte der Implementierung fokussiert sich diese Stellungnahme primär auf die Auswirkungen, die ein Verbot von sozialen Medien auf den digitalen Raum hätte. Für eine ausführliche Analyse der bestehenden Technologien für Altersnachweise verweisen wir auf die kürzlich veröffentlichte Studie des Knight-Georgetown Institutes¹. Unabhängig davon möchten wir darauf aufmerksam machen, dass es grundsätzlich an Forschung und Evidenz im Hinblick auf technische Auswirkungen von Verboten sozialer Medien fehlt. Der CCC schließt sich der Forderung², nach einem Moratorium für das Ausrollen einer noch nicht vorhandenen Altersnachweisinfrastruktur, von über 331 internationalen Wissenschaftler:innen aus dem Bereich IT-Sicherheit an.

¹ <https://kgi.georgetown.edu/research-and-commentary/age-assurance-online/>

² <https://csa-scientist-open-letter.org/ageverif-Feb2026>

Wirksamkeit und Erfolg

Im Hinblick auf die Wirksamkeit eines Verbots von sozialen Medien sollte zuallererst einmal das Ziel festgestellt werden. In der aktuellen Diskussion heißt es häufig, es würde zum besseren Schutz von Kindern und Jugendlichen dienen. Hier stellt sich aber erneut die Frage: Was ist das Ziel?

Grundsätzlich sollte das Ziel nicht sein, Kinder und Jugendliche vom digitalen Leben auszuschließen, sondern das Digitale in einer Form zu gestalten, die sich nicht negativ auf Kinder und Jugendliche auswirkt. Diese Form der Gestaltung kann aber kaum durch das Implementieren von Altersnachweisen erreicht werden. Das Verbot von sozialen Medien in Australien zeigt eindrucksvoll, dass der einzig zu verzeichnende Erfolg die Zahl der Jugendlichen ist, die von Plattformen ausgeschlossen wurde. In Australien zeigen sich jedoch auch die Misserfolge; erste Recherchen belegen, dass ein ganz neues Geschäft rund um das Umgehen von Altersnachweisen entstanden ist. Und dass sogar Eltern ihren Kindern dabei helfen, entsprechende Schranken zu umgehen³. Auch das technische Umgehen von Technologien, die das Alter von Nutzenden schätzen, wird bereits in sehr einfacher Form für Nutzende bereitgestellt⁴.

Dies zeigt: Technologien für Altersnachweise sind leicht zu umgehen, sei es technisch oder durch gezielte Täuschung. Eine 100% technische Durchsetzbarkeit kann nicht erreicht werden.

Weiter ist davor zu warnen, dass Kinder und Jugendliche auf unregulierte und unsichere Plattformen ausweichen werden. Auf diesen Plattformen ist nicht nur mit ummoderierten Inhalten zu rechnen sondern auch mit erhöhten Risiken von Betrug, Malware und Datendiebstahl.

Implikation für die Privatsphäre und Schadensszenarien

Das Ausrollen einer weitreichenden Altersverifikationsinfrastruktur birgt diverse Gefahren, sowohl für Grundrechte als auch für die Resilienz technischer Systeme in einer Zeit politischer Herausforderungen.

Anonymität Online

Anonymität ist ein wichtiges Gut, sowohl in der realen Welt als auch im Internet. Für die politische Willensbildung ist es wichtig, dass Bürgerinnen sich informieren und diskutieren können, ohne sich beobachtet oder verfolgt zu fühlen. Authentizität im Internet darf nicht zulasten der Anonymität gehen und nicht durch erkennungsdienstliche Behandlung erkaufte werden. Betreiberinnen anonymer Kommunikationsmöglichkeiten wie Tor oder VPNs dürfen nicht weiter Verfolgung und Repressalien ausgesetzt werden. Dazu muss eindeutig gesetzlich geklärt werden, dass sie grundsätzlich nicht für über ihre Dienste getätigte Äußerungen belangt werden dürfen.

Privatsphäre

Auch wenn es technische Lösungen gibt, die in der Theorie besonders datensparsam sind, werden wesentliche Vorbehalte im Hinblick auf die Privatsphäre nicht gelöst. Im

³ <https://www.abc.net.au/news/2026-02-05/social-media-ban-do-under-16s-think-it-is-working/106304064>

⁴ <https://age-verifier.kibty.town/>

andauernden technischen Diskurs hat sich mittlerweile sehr deutlich gezeigt, dass eine Form des Altersnachweises nicht robust genug sein wird, um Umgehung zu verhindern bzw. keine Nutzerinnen zu benachteiligen⁵. Dies gilt jedoch nicht nur aus technischer Perspektive, sondern auch aus europarechtlicher Perspektive. So ist in der eIDAS Verordnung klar geregelt, dass Bürger:innen bei nicht Nutzung von digitalen Identitäten kein Nachteil entstehen darf (Art.5, 5a)⁶.

Das heißt, für eine erfolgreiche Durchsetzung von Altersnachweisen müssten alle drei Möglichkeiten (Altersverifikation, Altersschätzung, Altersbestimmung durch zusätzliche Informationen (Kreditkarten o. Ä.)) zur Anwendung kommen. Altersverifikationssysteme setzen ganz grundsätzlich auf Ausweisdokumente. Hier geben Nutzer:innen also bereits mehr Daten preis, als sie es normalerweise tun würden. Während Altersschätzungen mithilfe biometrischer Daten durchgeführt werden. Bei beiden Kategorien stellt sich die Frage, wie die Daten sicher gespeichert werden. Enorme Datenleaks wie zuletzt bei Discord zeigen, wie gefährlich es ist, Ausweisdokumente in die Hände digitaler Dienste zu legen⁷.

Der größte Punkt ist jedoch die Frage, welche Entität die Daten schlussendlich verarbeitet. Das kann entweder die Plattform selbst sein oder ein weiterer Anbieter, der den Nachweis für die Plattform durchführt. Dieser Entität muss die Nutzer:in gezwungenermaßen vertrauen, um Zugang zu einer Plattform zu erlangen. Nutzer:innen, die dieser Entität nicht trauen, sind vollkommen von allen sozialen Medien und somit jeglicher digitaler Partizipation ausgeschlossen. Weiterhin ist darauf hinzuweisen, dass es immer Personengruppen gibt, für die keine der drei Nachweisarten funktioniert, aufgrund fehlender Ausweisdokumente, falscher Klassifikation und fehlender Information. Dies würde zu einem per se Ausschluss der genannten Personengruppe führen.

⁵ <https://datatracker.ietf.org/doc/html/draft-iab-agews-report#name-more-than-one-approach-will>

⁶ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014R0910-20240520>

⁷ <https://arstechnica.com/security/2025/10/discord-says-hackers-stole-government-ids-of-70000-users/>

Gefahr von Zentralisierung und Gatekeeping

Auswirkung auf das Open-Source Ökosystem

Das Einführen einer flächendeckenden Altersverifikation würde die Open-Source Community besonders hart treffen. Die Infrastruktur von Open-Source-Distributionen sieht in der Regel ähnlich aus wie bei der Distribution Arch Linux. Diese Linux Distribution legt ein besonderes Augenmerk darauf, möglichst wenig Daten über die Nutzer:innen zu sammeln. Sowohl die Distribution selbst als auch die Packages (Software Applikationen) können von einer Vielzahl sogenannter Mirrors heruntergeladen werden. Ein Mirror (zu Deutsch: Spiegel) beschreibt einen gespiegelten Speicherort von Dateien, die damit an mehreren Orten im Internet verfügbar sind.

Die Mirrors sind wiederum in drei sogenannte Tiers (zu Deutsch: Stufen) eingeteilt: Mirrors des Tiers 0 enthalten die vom Arch-Team selbst erstellten Softwarepakete. Mirrors des Tiers 1 sind Kopien von Tier 0, Mirrors von Tier 2 entsprechend Kopien von Tier 1. Diese dezentrale Verteilung der Software verhindert auch, dass Entwickler:innen an zentraler Stelle Informationen über ihre Nutzer:innen sammeln können. Gleiches gilt auch für das Tracken der Downloads von Software-Paketen. Um eine Altersverifikation zu gewährleisten, müssten sich Distributionen, aber auch Open-Source App-Stores wie F-Droid von diesem datensparsamen, dezentralen Modell verabschieden.

Des Weiteren könnte die Altersverifikation trotzdem leicht umgangen werden, denn die Quellen aller Software-Pakete (Git Repositories) sind öffentlich einsehbar. Das eigenständige Kompilieren von Programmen ist eine zentrale Voraussetzung für die Transparenz offener Software. So hat etwa Levente Polyák von der Distribution Arch Linux darauf hingewiesen, dass eine Implementierung von Altersverifikationen eine Zentralisierung erfordern würde, die der Entwicklung freier Software wesensfremd ist und unmöglich umzusetzen wäre⁸.

Wenn Deutschland und auch die EU ihre Open Source Strategie weiterhin erfolgreich verfolgen wollen, dann müssen sie an dieser Stelle sehr genau über weitere Schritte nachdenken.

Mögliche Auswirkung auf generelle Funktionalität des Internets

Auch fundamentale Funktionsprinzipien des Internets könnten durch das Einführen einer zentralisierten Altersverifikationsinfrastruktur gefährdet werden. Wie bereits im vorherigen Abschnitt betont, setzt die Einführung von Altersverifikationslösungen eine Form der Zentralisierung voraus. Eine primäre Charaktereigenschaft des Internets ist jedoch Dezentralität. In einem Zeitalter, in dem sogenannte Internetshutdowns, sprich das Verhindern des Zugangs zum Internet durch repressive Staaten, zur Norm in der Unterdrückung von Protesten geworden sind. Es ist davor zu warnen, jegliche Form von Zentralisierung zu fördern, da diese Shutdowns enorm vereinfacht. Weiter würden solche Maßnahmen zur weiteren Fragmentierung des Internets⁹ beitragen, da sie den offenen Charakter des Internets gefährden.

⁸ <https://netzpolitik.org/2022/chatkontrolle-akute-gefahr-fuer-offene-software/>

⁹ <https://www.internetsociety.org/resources/internet-fragmentation/about-the-explainer/>

Weiter zeigt sich am Beispiel des Online Safety Bill in Großbritannien, dass ein solches Unterfangen nicht bei der Inpflichtnahme von Plattformen endet. Sondern dass für die Durchsetzung eines solchen Vorhabens schnell Umgehungsmöglichkeiten wie VPNs gezielt reguliert werden¹⁰. Hier zeigt sich erneut die große Gefahr für Betreiberinnen anonymer Kommunikationsmöglichkeiten, die gerade in politischen Ausnahmesituationen essenziell für demokratische Beteiligung und Widerstand sind.

Fazit

Grundsätzlich würde ein Verbot von sozialen Medien die weitreichende Einführung von Altersnachweisen bedeuten, während am problematischen Geschäftsmodell großer Plattformen kaum gerüttelt würde und Grundrechte wie das Recht auf Anonymität vollständig ausgehebelt würden. Deswegen lehnt der CCC jegliche Maßnahmen ab, die zum Ende von anonymer und pseudonymer Internetnutzung führen würden, sowie zusätzliche Hürden für den Zugang zu Partizipation online. Weiter sind die Auswirkungen auf die globale digitale Infrastruktur, kurz das Internet, unabsehbar. Diese Auswirkungen sollten entsprechend untersucht werden, um die Schäden, die eine solche Infrastruktur mit sich bringen würde, zu verstehen. Diese Forderung ist nicht aus der Luft gegriffen, sondern spiegelt sich auch in der Analyse des IAB/W3C sowie in dem heute Veröffentlichen Brief internationaler technischer Experten¹¹ wider. Wollen wir betroffenen Kindern und Jugendlichen möglichst rasch helfen, wäre es sinnvoller, bessere Alternativen gemeinsam mit Kinderschutz- und Technologieexpertinnen zu entwickeln.

¹⁰ <https://www.heise.de/en/news/British-House-of-Lords-wants-age-verification-for-VPNs-and-social-media-11154709.html>

¹¹ <https://csa-scientist-open-letter.org/ageverif-Feb2026>