BAND 21
Materialien zur Konsumforschung

Fabian Fischer
Anna Pauls
(Institut für Technikfolgen-Abschätzung, ÖAW)

Louise Beltzung
(AK Wien)

ALTERSFESTSTELLUNG IM DIGITALEN RAUM

Ansätze und Auswirkungen auf Konsument:innen sowie Abwägungen zwischen Schutz der Privatsphäre und Kinderschutz

Endbericht

ÖAW ÖSTERREICHISCHE AKADEMIE DER WISSENSCHAFTEN
ITA INSTITUT FÜR TECHNIKFOLGEN ABSCHÄTZUNG
AK WIEN

BAND 21
Materialien zur Konsumforschung

Fabian Fischer
(Autor, Projektleitung)

Anna Pauls
(Autorin)

Louise Beltzung
(Hrsg.)

ALTERSFESTSTELLUNG IM DIGITALEN RAUM

Ansätze und Auswirkungen auf Konsument:innen sowie Abwägungen zwischen Schutz der Privatsphäre und Kinderschutz

Endbericht

Verlag Arbeiterkammer Wien
Februar 2026

INHALT

KURZFASSUNG 6
ABSTRACT 7
EINLEITUNG 8
1 ANWENDUNGSFELDER 13
1.1 FESTSTELLUNG DER ZUSTIMMUNGSFÄHIGKEIT 13
1.2 ZUGANGSBESCHRÄNKUNG ZU GEFÄHRDENDEN INHALTEN UND GÜTERN 13
1.2.1 Pornografische Inhalte 14
1.2.2 Gewaltvolle Inhalte 14
1.2.3 Radikalisierung 15
1.2.4 Süchtigmachende Angebote 16
1.2.5 Social Media 16
1.2.6 KI-Chatbots 16
1.2.7 Andere gefährliche Interaktionsmöglichkeiten 17
2 RECHTLICHE GRUNDLAGEN 18
2.1 NATIONALE REGELUNGEN WELTWEIT 18
2.2 EU-EBENE 19
2.3 ÖSTERREICHISCHE EBENE 20
3 TECHNISCHE GRUNDLAGEN 22
3.1 EBENEN DER ALTERSFESTSTELLUNG 22
3.1.1 Geräteebene 23
3.1.2 App Stores 23
3.1.3 Auf Ebene der App bzw. Plattform 24
3.1.4 Beschränkung einzelner Inhalte und Funktionen 24
3.2 METHODEN DER ALTERSFESTSTELLUNG 25
3.2.1 Selbstauskunft 25
3.2.2 Festlegung des Alters durch Bezugspersonen 26
3.2.3 Biometrische Methoden 26
3.2.4 Verhaltensanalyse 28
3.2.5 Authentifizierungsmethoden 29
3.3 VERFAHRENSUNABHÄNGIGE UMGEHUNGSMÖGLICHKEITEN 33
4 DATENSCHUTZ 34
4.1 DATENSCHUTZ UND -SICHERHEIT 34
4.2 ÜBERWACHUNG UND ZENSUR 37
5 AUSWIRKUNGEN AUF KONSUMENT:INNEN UND GESELLSCHAFT 38
5.1 INDIVIDUELLE FOLGEN 38
5.2 GESELLSCHAFTLICHE AUSWIRKUNGEN 40
5.3 FOLGEN FÜR KINDER UND JUGENDLICHE 40
6 AUSBLICK UND HANDLUNGSOPTIONEN 43
LITERATUR 46
ABKÜRZUNGSVERZEICHNIS 49

ABBILDUNGSVERZEICHNIS

Abbildung 1: Ebenen der Altersfeststellung nach oben hin steigender Granularität 22
Abbildung 2: Selbstauskunft durch Klicken auf einen Button (hier am Beispiel von Pornhub) 25
Abbildung 3: Implizite Selbstauskunft durch die Zustimmung zu den Nutzungsbedingungen (hier am Beispiel von TikTok) 25
Abbildung 4: Abgleich von Selfie und Lichtbildausweis, hier am Beispiel des Dienstleisters persona 28

TABELLENVERZEICHNIS

Tabelle 1: Überblick über aktuelle Bestrebungen für Altersbeschränkungen 19
Tabelle 2: Überblick über Methoden zur Altersfeststellung, deren Effektivität und Datenschutz-Aspekte 34
Tabelle 3: Überblick über Daten, die bei verschiedenen Methoden verarbeitet werden 35

VERZEICHNIS DER BOXEN

Box 1: Das Collingridge-Dilemma der Technikfolgenabschätzung 9
Box 2: Die UN-Kinderrechtskonvention 11
Box 3: Datenleck bei Discord 36

KURZFASSUNG

Studie untersucht Technologien zur Altersfeststellung im Internet

Angestoßen durch Berichte über die Gefährdung von Kindern und Jugendlichen durch die exzessive Nutzung von Sozialen Medien bzw. Smartphones sowie Online-Radikalisierungen wurden in den letzten Monaten intensive Debatten darüber geführt, im digitalen Raum Altersbeschränkungen einzuführen. Argumentiert wird dies überwiegend mit dem Schutz der betroffenen Minderjährigen. Ende 2025 hat Australien mit einem Social-Media-Verbot für Unter-16-Jährige in diesem Bereich eine Vorreiterrolle eingenommen. Die vorliegende Studie untersucht Altersfeststellungstechnologien. Dabei werden die Technikfolgen im Hinblick auf Datenschutz, Konsument:innenschutz und Kinderrechte betrachtet.

Dringender Handlungsbedarf

Es besteht ein dringender Handlungsbedarf, da Kinder und Jugendliche immer leichter Zugang zu gefährdenden Inhalten, Funktionen und Interaktionsmöglichkeiten haben. Von Pornografie, über gewaltvolle Inhalte, durch Algorithmen befeuerte Radikalisierung, süchtigmachende Interaktionsmuster bis hin zu neuen Gefahren durch KI-Chatbots existieren im digitalen Raum vielerlei problematische Angebote.

Altersüberprüfungen ineffektiv, überschießend und risikobehaftet

Altersbeschränkungen versprechen eine einfache Lösung. Bei näherer Betrachtung sind Altersbeschränkungen und die dafür notwendigen technischen Altersüberprüfungen aber sowohl ineffektiv als auch überschießend und risikobehaftet: Die meisten Methoden können leicht umgangen werden, insbesondere wenn die Altersbeschränkungen nur regional umgesetzt werden. Darüber hinaus ist es äußerst fraglich, ob eine flächendeckende Durchsetzung realistisch ist. Was droht, ist, dass Kinder und Jugendliche auf noch riskantere (weil schlecht moderierte) Plattformen ausweichen.

Hohe Datenschutzrisiken

Für Personen, die Schritte der Altersschätzung oder -verifizierung durchlaufen, entstehen hohe Datenschutzrisiken. Denn bei den meisten Methoden werden hochsensible Daten verarbeitet: Gesichtsaufnahmen, Lichtbildausweise, Online-Verhalten, Kreditkarte oder die Daten der ID Austria (Name, Geburtsdatum etc.).

EU-Lösungen datensparsam, aber beschränkt einsetzbar

In Entwicklung befindliche Methoden wie die europäische Altersfeststellungs-App und die Europäische Brieftasche für die Digitale Identität (die sog. EUDI-Wallet) sind demgegenüber datensparsam gestaltet. Sie sind aber auf Android- und Apple-Smartphones beschränkt – was wiederum die Abhängigkeit von Smartphones verstärkt.

Handlungsoptionen:

Plattformen in die Pflicht nehmen

Kompetenzen der Nutzer:innen entwickeln

Gesellschaftliche Debatte notwendig

Folgende Handlungsoptionen leiten sich davon ab: Erstens stellen Altersbeschränkungen eine Verschiebung der Verantwortung von Plattform zur Verbraucher:in dar. Stattdessen sollten Online-Plattformen verpflichtet werden, problematische Inhalte konsequent zu moderieren und süchtigmachende Muster zu unterbinden – wovon alle Konsument:innen profitieren würden. Zweitens müssen Medien-, KI- und Plattform-Kompetenzen insbesondere unter Bezugspersonen ausgebaut werden. Drittens braucht es eine breitere gesellschaftliche Debatte unter Einbeziehung z. B. der Bundesjugendvertretung darüber, wie Minderjährige schrittweise – analog zum Straßenverkehr – zur selbstbestimmten Nutzung des Internets befähigt werden. Das wäre auch besser geeignet, um die variierenden Entwicklungsgeschwindigkeit von Kindern zu berücksichtigen und diese Debatte ist mit Kinderrechten auf Informationsfreiheit, Schutz der Privatsphäre und Beteiligung am kulturellen Leben vereinbar. Parallel dazu müssen Angebote für Kinder und Jugendliche in Krisensituationen ausgebaut werden.

ABSTRACT

Triggered by reports of minors being harmed by excessive use of social media and smartphones, as well as online radicalisation, there has been intense debate in recent months about introducing age restrictions in the digital space. The primary rationale is to protect minors. At the end of 2025, Australia took a pioneering role in this area by imposing a social media ban for minors under 16. This technology assessment examines age verification and age estimation technologies with respect to data protection, consumer protection and children's rights, and relates these to the dangers they are intended to protect children and youths from.

The study explores technologies to verify the age on the internet

It should be noted that there is indeed an urgent need for action, as minors have increasingly easy access to harmful content, functions and interactions: from pornography and violent content to algorithm-driven radicalisation, addictive interaction patterns and new dangers posed by AI chatbots, there are many problematic types of content in the digital realm.

Need for urgent action

Against this backdrop, age restrictions promise a simple solution. On closer inspection, however, age restrictions and required age checks are ineffective, excessive, and risky: Most methods can be easily circumvented, especially when age restrictions are only implemented regionally. Furthermore, it is highly questionable whether a comprehensive enforcement is realistic. It appears likely that children and teens will resort to even riskier, poorly moderated platforms.

Age assessment is ineffective, excessive and risky

People who undergo age estimation or verification processes face significant data protection risks. This is because most methods involve the processing of highly sensitive data, such as facial images, photo IDs, behavioural data, credit card information or ID Austria data (name, date of birth, etc.). In contrast, methods currently under development, such as the European age verification app and the European Digital Identity Wallet, are designed to require minimal data. However, they are limited to Android and Apple devices, thereby increasing dependence on smartphones.

Significant data protection risks

EU solutions data-efficient but smartphone-dependent

This leads to the following options for action: Firstly, age restrictions shift responsibility from platforms to the consumer. Instead, online platforms should be required to moderate problematic content more vigilantly and prevent harmful interaction patterns – this would benefit all consumers, not only minors. Secondly, media, AI and platform skills must be developed, especially among caregivers of children and young people. Thirdly, there needs to be a social debate, involving different relevant actors, for example, the Federal Youth Council, on how minors can be gradually empowered to use the internet independently, similar to road traffic. This approach is also more adequate with regard to the varying rate at which children's maturity develops, and more compatible with children's rights (e.g., the rights to freedom of information, protection of privacy and participation in cultural life). At the same time, support for children and young people in crisis must be expanded.

Options for action:

Hold platforms accountable

Develop user skills

Societal debate necessary

EINLEITUNG

Internet wird als Gefahr für Kinder und Jugendliche diskutiert

Das Internet wird zunehmend als Gefahrenquelle für Kinder und Jugendliche wahrgenommen: Viele gesundheitliche und gesellschaftliche Probleme werden mit intensiver Internet- und vor allem Smartphone-Nutzung in Zusammenhang gebracht. Vor diesem Hintergrund wurden in letzter Zeit verstärkt Diskussionen zur Altersbeschränkung vieler Plattformen und zu einem eingeschränkten Zugang zu Inhalten im Internet geführt. In Österreich wurde dieses Thema nach dem Amoklauf an einer Grazer Schule im Juni 2025 drängend. Aber auch international und auf EU-Ebene ist das Thema in den letzten Jahren zunehmend ins Zentrum gerückt. Das weitreichendste und bekannteste Beispiel ist wohl das Social-Media-Verbot in Australien für Unter-16-Jährige.

Altersbeschränkungen werden ohne eindeutige Evidenz als effektiv angenommen

All diese Debatten bauen implizit auf der Annahme auf, dass Altersbeschränkungen effektiv und rechtskonform durchführbar und durchsetzbar sind. Bei näherer Betrachtung zeigt sich allerdings, dass es hier eine Vielzahl an Problemstellungen gibt. Die vorliegende Studie untersucht daher die Möglichkeiten und Herausforderungen der Altersüberprüfung im digitalen Raum (Internet, Apps etc.) aus Sicht der Technikfolgenabschätzung und des Konsument:innenschutzes. Damit soll ein wichtiger Beitrag zur Versachlichung der Debatte geliefert werden. Denn nur, wenn geklärt ist, wie und unter welchen Bedingungen das Alter online festgestellt werden kann, können die Vor- und Nachteile von Altersbeschränkungen fundiert abgewogen werden.

Kinder und Jugendliche leiden unter psychischer Belastung

Eine zentrale Motivation dafür, den Zugang im Internet für Kinder und Jugendliche einzuschränken, ist die wachsende Evidenz, dass wir aktuell eine „globale Krise der psychischen Gesundheit junger Menschen“ (Brailovskaia et al., 2025, S. 4) erleben. Ein Tiefpunkt der psychischen Gesundheit von Kindern und Jugendlichen war dabei die Corona-Pandemie. Seither hat sich ihre Situation zwar wieder gebessert, ist aber weiterhin deutlich schlechter als vor der Pandemie, wie eine Längsschnittstudie in Deutschland ergab (Kaman et al., 2025). Dabei zeigt sich, dass nach der Corona-Pandemie vor allem Sorgen aufgrund von Krieg, Terror, Wirtschafts- und Klimakrise vorherrschend waren: All diese Krisen sind für Kinder und Jugendliche heute aufgrund der weiten Verbreitung von Smartphones mit Kameras und sog. Sozialen Medien niederschwellig erlebbar.

Negative Folgen exzessiver Nutzung von Smartphones und Sozialen Medien

Weitere Bedenken gibt es in Bezug darauf, dass Kinder und Jugendliche zu viel Zeit mit Smartphones und Sozialen Medien verbringen. Mögliche Folgen exzessiver Nutzung digitaler Technologien und damit langer Bildschirmzeiten sind zum Beispiel reduzierte Schlafquantität und -qualität und verringerte körperliche Aktivität bis hin zu gesteigertem Risiko von Adipositas (OECD, 2025b). Während viele dieser Risiken auch auf Erwachsene zutreffen, sind Kinder und Jugendliche besonders gefährdet, da ihr Gehirn noch eine hohe Plastizität aufweist und ihr Verhalten somit leichter beeinflusst werden kann. Dennoch ist die Evidenzlage, wie besonders Soziale Medien sich auf das entwickelnde Gehirn auswirken, in den Neurowissenschaften relativ gering (Brailovskaia et al., 2025). Grund dafür ist unter anderem, dass die Betreiber der großen Plattformen einerseits interne Studien zurückhalten, andererseits zum Teil systematisch unabhängige Forschung unterminieren (Orben & Matias, 2025). Das lässt sich dadurch erklären, dass sich die Anbieter größtenteils über Werbeeinnahmen finanzieren und damit ein geschäftliches Interesse haben, dass Nutzer:innen möglichst viel Zeit auf ihren

Schlechte Evidenzlage, wie genau sich das Digitale auf Kinder auswirkt

Plattformen verbringen – und dabei möglichst viel Werbung sehen, um die Werbeeinnahmen zu steigern. Da Kinder und Jugendliche Schätzungen zufolge etwa ein Drittel aller Internetnutzer:innen darstellen (Livingstone et al., 2015), sind sie eine attraktive Zielgruppe für Werbung mit z.T. als manipulativ eingestuften Praktiken. Kinder und Jugendliche sind dabei sowohl als primäre Konsument:innen als auch als sekundäre Konsument:innen, die Bezugspersonen zu Kaufentscheidungen bewegen, relevant (Dopona, o. J.). Für Influencer:innen sind sie eine wichtige Zielgruppe, wie der Einbruch des generierten Einkommens mit australischen Teenagern als Zielgruppe mit Einführung des dortigen Social-Media-Verbot illustriert.[1] Sie als Nutzer:innen zu halten, liegt folglich im geschäftlichen Interesse der Plattformen.

Kinder beginnen früh, Smartphones und Social Media zu nutzen

Trotz der nicht eindeutigen Evidenzlage über genaue Zusammenhänge verdichten sich die Anzeichen für eine problematische Gemengelage – dies auch besonders vor dem Hintergrund, dass das Alter, in dem Kinder beginnen, sich online zu bewegen, zunehmend sinkt (Brailovskaia et al., 2025). Im Alter von zehn Jahren besitzen bereits ca. 70 % der Kinder in OECD-Ländern ein eigenes Smartphone und über die Hälfte der 15-Jährigen nutzen mehr als 30 Stunden pro Woche Smartphones – eine signifikante Minderheit sogar über 60 Stunden (OECD, 2025b). Es gibt also eindeutige Anzeichen, dass sich hier ein starker Wandel vollzieht. Auch wenn die Evidenzlage zu verschiedenen Kausalitäten noch nicht eindeutig ist, ist im Sinne des Vorsorgeprinzips ein Abwarten auf gesicherte Erkenntnisse fragwürdig, besonders da die Pubertät relativ kurz andauert und bei weiterem untätigem Zuwarten potentiell viele Personen von negativen Auswirkungen betroffen wären.

Box 1: Das Collingridge-Dilemma der Technikfolgenabschätzung

Das nach dem Autor David Collingridge benannte und auch als Steuerungs- oder Kontrolldilemma[2] bezeichnete Problem besagt, dass es eine inhärente Spannung zwischen Gestaltungsmöglichkeiten und verlässlichem Folgenwissen gibt (Grunwald, 2022, S. 211). Das zugespitzte Problem liegt darin, dass zu Beginn einer Entwicklung wenig (Folge-)Wissen vorhanden ist – dafür könnte die Entwicklung noch aktiv (mit)gestaltet werden. Zu einem späteren Zeitpunkt ist mehr gesichertes Wissen vorhanden, aber die Technologie bereits so fortgeschritten und verfestigt, dass man kaum noch gestaltend in deren Entwicklung eingreifen kann. Tatsächlich ist dieser Widerspruch selten so drastisch. Mit dem Vorsorgeprinzip[3] gibt es außerdem ein aus den Gentechnikdebatten stammendes Prinzip, wonach bereits bei berechtigtem Grund zur Besorgnis Vorsorgemaßnahmen ergriffen werden sollten/müssen. Das muss aber immer in Abwägung der zumutbaren Lasten und unter Berücksichtigung der Qualität der Informationslage geschehen.

---

1 *reuters.com/business/media-telecom/australias-teen-social-media-ban-pushes-content-creators-look-abroad-2025-11-24/*. **Dieser und alle folgenden URLs wurden zuletzt am 19.12.2025 kontrolliert.**

2 *de.wikipedia.org/wiki/Collingridge-Dilemma*.

3 *de.wikipedia.org/wiki/Vorsorgeprinzip*.

Better Internet for Kids: Strategie der Europäischen Kommission

Vor diesem Hintergrund wurden in den letzten Jahren verschiedene Initiativen auf politischer Ebene ins Leben gerufen. Im europäischen Kontext sind die Better Internet for Kids-Strategien BIK (aus 2012) und BIK+ (aus 2022) der Europäischen Kommission[4] hervorzuheben, die das Ziel verfolgen, ein zugänglicheres, altersgerechteres und informativeres Internet im Sinne der Interessen der Kinder voranzutreiben, unter anderem durch entsprechende Gesetzgebung. Eine der drei Säulen der BIK+-Strategie ist, das Internet für Kinder und Jugendliche sicherer zu machen. Eine erste Evaluierung dieser Strategie wurde 2025 veröffentlicht (Verdoodt et al., 2025).

Australien als Vorreiter bei Social-Media-Verbot

International hat vor allem das geplante Social-Media-Verbot in Australien große Aufmerksamkeit erfahren: Ende 2025 wurde der Zugang zu Sozialen Medien für Kinder und Jugendliche unter 16 verboten. Dieses Verbot genießt breite Unterstützung, widerspricht aber den Empfehlungen eines im Mai 2024 gestarteten Joint Parliamentary Select Committee, das die Auswirkungen Sozialer Medien auf Australier:innen untersucht hat. Die Kritik am Verbot ist vielfältig. Vor allem wird bemängelt, dass es das Problem grob vereinfachend angeht – während eine systemische Regulierung dem komplexen Phänomen angemessener wäre (Fardouly, 2025).

Online-Radikalisierung als Problemfeld in österreichischer Debatte

Wie bereits erwähnt, gibt es auch in Österreich aktuell eine Debatte darüber, ob für Soziale Medien eine Altersgrenze festgelegt werden soll. In Österreich war der Amoklauf an einer Grazer Schule und die mögliche Rolle von Social Media bei der Online-Radikalisierung junger Menschen ein Beweggrund, das Thema der Online-Altersbeschränkungen zu diskutieren. Im Juni 2025 hat Vizekanzler und Medienminister Andreas Babler für ein Verbot Sozialer Medien bis 15 Jahre plädiert; Bundeskanzler Christian Stocker hat dieses Alterslimit ebenfalls als eine Möglichkeit in Erwägung gezogen.[5] Seit 3. Juli läuft auch ein Volksbegehren, das ein Social-Media-Verbot für Unter-16-Jährige fordert.[6]

Debatten über Social-Media-Verbot auf EU-Ebene

Auch auf EU-Ebene gibt es entsprechende Debatten. Im Oktober 2025 haben die Staats- und Regierungschefs der EU-Staaten in einer Erklärung ein Mindestalter für Soziale Medien gefordert;[7] ebenso der Ausschuss für Binnenmarkt und Verbraucherschutz des Europäischen Parlaments, der ein EU-weites Mindestalter von 16 Jahren für Soziale Medien vorschlug (European Parliament, 2025).

Handyverbot an Schulen

Neben der Social-Media-Nutzung ist die Smartphone-Nutzung im Allgemeinen ein großes Thema. Beispielhaft sei hier auf das per 1. Mai 2025 in Österreich in Kraft getretene Handynutzungsverbot an Schulen bis einschließlich der 8. Schulstufe verwiesen. Das Nutzungsverbot wird damit begründet, dass Smartphones (und ähnliche Geräte wie Smartwatches) „Konzentrationskiller" seien. Hier geht es also in erster Linie um die Eliminierung eines Störfaktors im Unterricht. Darüber hinaus werden aber auch Drohungen, Mobbing und andere gefährliche Handlungen und Inhalte als Begründung aufgeführt.

---

4 *better-internet-for-kids.europa.eu/en/bik-plus-strategy* und *better-internet-for-kids.europa.eu/en/bik/old-bik-strategy*.

5 *derstandard.at/story/3000000274685/amoklauf-in-graz-babler-will-eu-l246sung-f252r-social-media-altersgrenze*.

6 *bmi.gv.at/411/files/registrierte_Volksbegehren/BF_Text_Social_Media_Verbot_fuer_Unter_16_Jaehrige_03072025.pdf*.

7 *tagesschau.de/ausland/europa/eu-fuer-mindestalter-in-sozialen-netzen-100.html*.

Altersbeschränkungen als Lösungsweg …

… benötigen eine Altersfeststellung

Zusammengefasst ergibt sich somit das Bild, dass es begründete Sorge gibt, dass digitale Erfahrungen für Kinder und Jugendliche teilweise schädliche Folgen haben können. Die Debatte konzentriert sich auf Soziale Medien und Smartphonenutzung. Quer durch die verschiedenen Debattenstränge werden Altersbeschränkungen häufig als möglicher Lösungsansatz aufgeworfen. Altersbeschränkungen bedürfen wiederum zwingend einer Altersfeststellung der Nutzer:innen. Was in einer Trafik oder einem Kino mit etablierten Mitteln einfach durchführbar ist, und wo auch dann, wenn Jugendliche die analoge Art der Altersfeststellung unterminieren – etwa durch Weitergabe des Schüler:innenausweises – grobe Abweichungen von der Altersgrenze auffallen, ist online diffiziler: Online ist es nicht offensichtlich, welche Nutzer:innen Kinder oder Jugendliche und welche Erwachsene sind (Livingstone et al., 2024). Daher untersucht die vorliegende Studie die Möglichkeiten der Umsetzung von Altersfeststellung im digitalen Raum. Sie wird von den folgenden Fragen geleitet:

Welche Ansätze zur Altersfeststellung im Internet werden aktuell diskutiert, verfolgt und entwickelt?

Welche Auswirkungen haben diese auf Konsument:innen, individuell und kollektiv als Gesellschaft?

Welche Bestrebungen gibt es diesbezüglich auf regulativer Ebene?

Welche Abwägungen, etwa zwischen dem Schutz der Privatsphäre und dem Kinderschutz, sind in diesem Kontext zu treffen?

Konsument:innenschutz, Datenschutz und Kinderrechte als Bezugspunkte

Normativ stehen Konsument:innenschutz, Privatsphäre/Datenschutz, Kinderrechte sowie Kinderschutz im Zentrum. Wie bereits der untenstehende Auszug aus der Kinderrechtskonvention erkennen lässt, können sogar Kinderrechte untereinander in gewissem Maße in einem Spannungsverhältnis stehen. Hervorzuheben ist auch der Unterschied zwischen Kinderschutz und Kinderrechten: Während Kinderschutz primär auf negative Freiheiten („Freiheit von“) im Sinne von Gewalt, Misshandlung etc. fokussiert, hebt der Begriff Kinderrechte auch positive Freiheiten („Freiheit zu“) im Sinne von Teilhabe, Informationsfreiheit usw. hervor.

Box 2: Die UN-Kinderrechtskonvention

Die UN-Kinderrechtskonvention von 1989 hält in 54 Artikeln umfassende Rechte für Kinder und Jugendliche fest. Diese besagt, dass „das Kind wegen seiner mangelnden körperlichen und geistigen Reife besonderen Schutz[es] und besonderer Fürsorge“ bedarf. Im Zusammenhang mit dem Thema dieser Studie seien exemplarisch das Recht des Kindes auf sein Wohl (Art. 3), Recht auf Meinungs- und Informationsfreiheit (Art. 13), Schutz der Privatsphäre und Ehre (Art.16), Recht auf Zugang zu Informationen, Medien, Kinder- und Jugendschutz (Art. 17), Schutz vor Gewaltanwendung, Misshandlung, Vernachlässigung (Art. 19) und das Recht auf Freizeit sowie auf volle Beteiligung am kulturellem und künstlerischem Leben und die staatliche Achtung und Förderung derselbigen (Art. 31) genannt.

Aufbau der Studie

Die Studie ist wie folgt aufgebaut: Im ersten Kapitel werden die wichtigsten Anwendungsfelder der Altersfeststellung vertiefend dargestellt. Kapitel 2 widmet sich den geltenden rechtlichen Rahmenbedingungen auf europäischer und

nationaler Ebene. Kapitel 3 analysiert die technischen Grundlagen, die eine Altersfeststellung im digitalen Raum ermöglichen. Die datenschutzrelevanten Aspekte der unterschiedlichen Methoden werden in Kapitel 4 erörtert. Kapitel 5 untersucht die möglichen Auswirkungen auf die Gesellschaft und Konsument:innen. Kapitel 6 bietet einen Ausblick und Handlungsempfehlungen.

1 ANWENDUNGSFELDER

Internet als gefährlicher Raum

Wie einleitend beschrieben, wird in den aktuellen Debatten rund um Altersbeschränkungen die Gefährlichkeit des Internets als primärer Beweggrund genannt. In diesem Zusammenhang werden regelmäßig Pornografie, Darstellungen von Gewalt, Mobbing, Spiel- und Social-Media-Sucht sowie Radikalisierung genannt.[8] Aber auch Glücksspiel und der Kauf von Alkohol und Tabakwaren durch Minderjährige sind teilweise ein Thema (Livingstone et al., 2024). Daneben stellt sich auch die Frage, wie Dienstanbieter sicherstellen können, dass die Nutzer:innen tatsächlich geschäftsfähig sind. In diesem Kapitel wird ein Überblick über mögliche Anwendungsfelder für die Altersfeststellung gegeben.

1.1 FESTSTELLUNG DER ZUSTIMMUNGSFÄHIGKEIT

Zustimmung zu Nutzungsbedingungen

Viele Aktivitäten im Internet setzen Zustimmung voraus oder beinhalten Vertragsabschlüsse: Um einen Dienst in Anspruch nehmen zu können, muss in der Regel den Nutzungsbedingungen (Terms of Service) zugestimmt werden. Ebenso können unzählige Transaktionen durchgeführt werden: Abonnements für Dienste (Spotify, Netflix usw.) können abgeschlossen, Güter bestellt und Apps gekauft bzw. in Apps (z.B. Spielen) Erweiterungen bzw. der Zugang zu bestimmten Funktionen erstanden werden.

Einwilligungsfähigkeit bei Minderjährigen

Wie in Abschnitt 2.2 näher ausgeführt wird, sieht die Datenschutz-Grundverordnung vor, dass bei Kindern unter 16 Jahren die Einwilligung durch die Eltern oder deren Zustimmung erforderlich ist (Kunz & Waldmann, 2025). Aber auch mündige Minderjährige (14-18 Jahre) sind nur eingeschränkt geschäftsfähig. In beiden Fällen könnte daher eine wirksame Altersbeschränkung notwendig sein, da sonst die Einwilligungsfähigkeit oder Geschäftsfähigkeit der Nutzer:in nicht gegeben sein könnte und somit die Zustimmung zu den Nutzungsbedingungen bzw. der Vertragsabschluss keine Wirksamkeit hätte (Kunz & Waldmann, 2025).

Online-Käufe als finanzielles Risiko

Besonders In-App-Käufe, Minikredite und sog. Lootboxen (Überraschungsboxen) scheinen ein ernsthaftes Problem zu sein, da Kinder auf diesem Wege teilweise beträchtliche Summen ausgeben, ohne dass ihre Eltern hier sinnvoll eingreifen können.[9] Besonders Lootboxen sind in der Kritik, Suchtpotential zu haben (siehe Abschnitt 1.2.4).

1.2 ZUGANGSBESCHRÄNKUNG ZU GEFÄHRDENDEN INHALTEN UND GÜTERN

Die Debatte um Altersbeschränkungen wird dominiert von dem Bedenken, dass viele Online-Angebote eine Gefährdung für Kinder und Jugendliche darstellen.

---

8 *Einen guten Überblick über die Argumente in dieser Richtung bietet z.B. burgenland.orf.at/stories/3314744/.*

9 *better-internet-for-kids.europa.eu/en/news/we-only-trust-those-well-designed-online-content-results-youth-participation-digital-youth.*

Mittels Zugangsbeschränkungen soll ihnen daher der Zugang erst ab einem gewissen Alter ermöglicht werden.

1.2.1 PORNOGRAFISCHE INHALTE

Früher Kontakt mit Pornografie

Pornografie ist über das Internet niederschwellig verfügbar und ausgesprochen populär (Döring, 2024). Dabei hat Pornografie viele Spielarten und, wo genau sie beginnt, ist nicht immer einfach zu beantworten. Auch Kinder und Jugendliche sind heute bereits früh mit pornografischen Inhalten im Internet konfrontiert: In Großbritannien und Australien findet durchschnittlich mit 13 Jahren erstmals Kontakt mit Pornografie statt (OECD, 2025a).

Neue Formen der Pornografie durch KI

Neben herkömmlichen pornografischen Angeboten wie PornHub, xHamster und XVideos, die primär filmische Darstellungen von Pornografie anbieten, gibt es seit dem Boom der generativen KI neue Spielarten wie KI-generierte Pornografie nach Wunsch der Nutzer:innen. Doch auch rund um Chatbots entstehen zunehmend erotische bis pornografische Angebote. Exemplarisch sei hier erwähnt, dass OpenAI plant, in Zukunft auch die Erstellung erotischer Inhalte zu erlauben. Dies soll jedoch nur verifizierten Volljährigen erlaubt sein.[10]

Porno-Angebote mit schwacher Alterskontrolle

Viele Pornografie-Webseiten haben sehr schwache Alterskontrollen: Bei den meisten reicht es aus, einen Button zu klicken, mit dem man bestätigt „über 18“ zu sein. Bei anderen steht gar nur, man solle unverzüglich die Webseite verlassen, wenn man nicht volljährig sei. Beides sind Formen der Selbstauskunft (siehe Abschnitt 3.2.1) und damit sehr schwache Hürden.

1.2.2 GEWALTVOLLE INHALTE

Vielfältige gewaltvolle Inhalte

Im digitalen Raum können gewaltvolle Inhalte vielfältige Formen annehmen. Relativ offensichtlich sind Bilder, Videos und detaillierte Beschreibungen von Gewaltverbrechen, wie sie z.B. aus Kriegsregionen verbreitet werden. Je nach Moderationspraxis digitaler Plattformen stoßen Nutzer:innen schnell auf solche Inhalte. Darüber hinaus gibt es auch Überschneidungen mit dem Thema Pornografie, wenn gewalttätige Sexszenen dargestellt werden.

Sexualisierte Gewalt

Ein großes Themenfeld ist daher auch sexualisierte Gewalt, die unter Kindern und Jugendlichen ein Problem ist (Maierl, 2023). Besonders dann, wenn zuvor private Informationen oder intime Aufnahmen geteilt wurden (absichtlich, unabsichtlich oder durch Manipulation), können diese im Rahmen sog. Sextortion zur Erpressung verwendet werden, indem gedroht wird, sensible (evtl. als peinlich wahrgenommene) Informationen zu veröffentlichen. Teilweise wird dies auch genutzt, um weiteres kompromittierendes Material zu erpressen.[11] Weiters gibt es Dienste, die per generativer KI Nacktbilder anhand von Fotos bekleideter Personen erstellen lassen (OECD, 2025a). Auch diese Bilder können für Sextortion und zur Erniedrigung eingesetzt werden.

Darunter Cybergrooming

Ein weiteres Problem ist Cybergrooming: Dabei geben sich Erwachsene als Kinder oder Jugendliche aus, um sich das Vertrauen von Minderjährigen zu erschleichen. Ist Vertrauen aufgebaut, werden die Kinder bzw. Jugendlichen zu persönlichen Treffen eingeladen, um sie dann sexualisierter Gewalt auszusetzen

---

10 *bbc.com/news/articles/cpd2qv58yl5o.*

11 *kinderschutz.ch/themen/sexualisierte-gewalt/sexuelle-entwicklung-und-digitale-sexualisierte-gewalt/digitale-sexualisierte-gewalt/sextortion.*

(Maierl, 2023). Täter:innen suchen dafür oft gezielt Plattformen auf, die sich an Kinder und Jugendliche richten, da dort die Dichte an potentiellen Opfern hoch ist und Kinder und Jugendliche vielleicht denken, dass nur andere Minderjährige unter den Nutzer:innen sind.

Moderationsanstrengungen werden reduziert

Bei den meisten Plattformen werden gewaltvolle Inhalte offiziell nicht geduldet. Allerdings gibt es aktuell einen Trend bei Sozialen Medien, die Anstrengungen zur Inhaltsmoderation zu reduzieren.[12] Damit ist die Wahrscheinlichkeit hoch, dass gewaltvolle Inhalte länger im Umlauf bleiben, wodurch auch Kinder und Jugendliche leichter darauf stoßen. In privaten Messengern und Chats hingegen wird in der Regel nicht moderiert (bzw. ist dies technisch aufgrund von Ende-zu-Ende-Verschlüsselung oft gar nicht möglich).

1.2.3 RADIKALISIERUNG

Mangelnde Moderation und verstärkende Algorithmen

Im Bereich der Radikalisierung bereitet die Kombination aus mangelhafter Moderation und verstärkenden Algorithmen die größten Sorgen. Diese Kombination ist auch eine der Hauptargumente für ein allgemeines Social-Media-Verbot. Attentäter:innen gelten zunehmend als „online radikalisiert“: Es wurde etwa berichtet, dass sich der Attentäter von Villach binnen weniger Monate online islamistisch radikalisiert habe.[13] Islamistische und rechtsextreme terroristischen Gruppen nutzen auch Grooming-Strategien, um gezielt Kämpfer und „Bräute“ zu rekrutiert. Dazu werden Hashtags und Inhalte produziert, die gezielt Junge ansprechen sollen, um sie für extremistische Sphären zu ködern (Scheuble & Oezmen, 2022).

Minderjährige als Täter und Opfer

Auch der Fall eines schwulenfeindlichen Terrornetzwerks, das ihre Opfer über Dating-Plattformen in Fallen gelockt und anschließend schwer misshandelt hat, ist ein mahnendes Beispiel dafür, wie sich Radikalisierte über das Internet organisieren und zu immer brutaleren Übergriffen aufstacheln.[14] Die Täter:innen aus dem rechtsextremen bis neonazistischen Milieu waren zwischen 14 und 26 Jahre alt und damit teilweise noch minderjährig.[15]

Nihilistische Gewalt

Unter dem Begriff Nihilistische Gewalt (nihilistic violence) werden Online-Communities beschrieben, die sich rund um Gewaltverherrlichung und Menschenfeindlichkeit sammeln (Gill, 2025; Institute for Strategic Dialogue, 2025). Was diese Subkulturen ausmacht, ist die untergeordnete Rolle von Ideologie (es gibt jedoch Überschneidungen mit ideologischen gewaltverherrlichenden Gruppierungen). Statt ideologischer Rechtfertigung ihrer Gewaltverherrlichung sind Ästhetik und Anerkennung zentrale Treiber. Manche dieser Gruppen praktizieren auch Sextortion (s.o.) und einige Attentäter der jüngeren Vergangenheit werden dieser Subkultur zugeordnet.

Rekrutierung von Minderjährigen für kriminelle Netzwerke

Neben politisch motivierten Tätergruppen rekrutieren auch wirtschaftlich motivierte kriminelle Netzwerke zunehmend gezielt Minderjährige über Soziale Medien und Messengerdienste (Europol, 2024). Teilweise bieten sogar Minderjährige Auftragsgewalt aktiv an (Brombacher & Scaturro, 2025; EUCPN, 2024).

---

12 *bbc.com/news/articles/cly74mpy8klo.*

13 *oeaw.ac.at/news/werden-jugendliche-durch-tiktok-radikalisiert.*

14 *wienerzeitung.at/a/schwulenfeindlicher-terror-und-fahrlaessige-berichterstattung.*

15 *derstandard.at/story/3000000262292/mehrere-festnahmen-nach-razzien-in-sieben-bundeslaendern.*

1.2.4 SÜCHTIGMACHENDE ANGEBOTE

Handy- und Social-Media-Sucht …

Viele Kinder und Jugendliche nehmen ihr Online-Verhalten selber als suchtgetrieben wahr: Sie bereuen oft, Zeit zu verschwenden, berichten von Erschöpfung und dem Hängenbleiben beim Scrollen durch Social Media & Co. (auch Doomscrolling genannt) (Verdoodt et al., 2025). Wie bereits in der Einleitung erwähnt, sind viele Online-Angebote auf hohe Verweildauer hin designt, da dies im Interesse der Betreiber:innen ist. Diese Interaktionsmuster werden auch süchtigmachendes Design (addictive design) genannt: Jugendliche sind in der Pubertät besonders anfällig für Sucht, und hier spielen Interaktionsmöglichkeiten wie „Likes" auf Sozialen Medien, Lootboxen (siehe auch Abschnitt 1.1.) und schnelle Kurzvideos eine entscheidende Rolle, da sie zur fortgesetzten Nutzung verleiten (Hutton et al., 2024; Verdoodt et al., 2025). Dieses Problem betrifft aber nicht nur Kinder und Jugendliche: Auch ältere Menschen leiden zunehmend unter Handysucht, besonders nach dem Erwerbsleben.[16]

… durch Addictive Design …

… betrifft nicht nur Minderjährige

1.2.5 SOCIAL MEDIA

Pauschales Social-Media-Verbot

Häufig wird nicht spezifisch eine Beschränkung der bisher genannten Angebote gefordert oder umgesetzt, sondern ein pauschales Social-Media-Verbot gefordert oder beschlossen (siehe dazu auch Kapitel 2). Dabei stellt sich unweigerlich die Frage, wie Soziale Medien zu definieren und legistisch greifbar zu machen sind. Denn die Übergänge zu anderen Plattformen sind fließend: Messengerdienste (wie WhatsApp und Telegram) sind in manchen Definitionen inkludiert, andere wiederum lassen sie außen vor, obwohl über sie oft Videos und andere, potentiell problematische, Inhalte geteilt werden.

Unklare Definition

Ebenso stellt sich die Frage, ob Online-Spiele davon erfasst werden, die teilweise auch ähnliche Funktionalitäten wie Soziale Medien anbieten. Und letztlich zeigt das Beispiel Australien, wie heikel diese Definition ist: Dort wurde YouTube ursprünglich nicht vom Verbot erfasst; ein Umstand, der nach Protesten (von anderen Plattformen und Eltern) im Sommer 2025 geändert wurde.[17]

Online-Spiele betroffen?

Daneben gibt es aber auch unzählige kleinere Plattformen, die teilweise ebenso intensiv von Kindern und Jugendlichen genutzt werden und die einer breiten Öffentlichkeit (und damit auch den Gesetzgebern) aber unbekannt sind (z. B. MeowChat, Omegle und MeetMe) – doch gerade Kinder probieren bekanntlich schnell neue Angebote aus (Livingstone, 2025). Auch viele pornografische Webseiten, Streaming-Plattformen (z.B. Spotify) und Online-Spiele werden in der Regel nicht als Soziale Medien eingestuft, obwohl sie teilweise ähnliche Funktionalitäten haben. Hier stellt sich die Frage, inwiefern auch diese Plattformen von gesetzlichen Social-Media-Verboten erfasst oder doch weiterhin zugänglich wären.

Kinder nutzen oft auch kleinere Plattformen …

… die teilweise nicht reguliert werden

1.2.6 KI-CHATBOTS

Chatbots mit neuen Gefahren

Neben Sozialen Medien, Messengerdiensten und anderen etablierten Teilen des Internets spielen Chatbots seit der Verfügbarkeit von ChatGPT Ende 2022 eine immer größere Rolle. Einerseits entstehen neue Angebote, andererseits werden

---

16 *orf.at/stories/3410793/.*

17 *reuters.com/legal/litigation/australia-widens-teen-social-media-ban-youtube-scraps-exemption-2025-07-29/.*

Chatbots zunehmend in verschiedene Apps integriert. Dies war etwa bei Snapchat der Fall, wo der Chatbot My AI als „Teilnehmer" in Gruppenchats integriert war, es sei denn, man bezahlte dafür, dass dieser abgestellt wurde – Kinder und Jugendliche fungieren hier gerne ohne aktive Einwilligung als Testpublikum (Teknologirådet, 2024). Manche der Chatbots können auch Bilder generieren, andere nur Texte. Wie bereits in Abschnitt 1.2.1 dargestellt, plant OpenAI, in ChatGPT zukünftig auch erotische Inhalte zuzulassen, sofern Nutzer:innen sich als volljährig verifizieren lassen.

Chatbots mit schädlichen Inhalten und Interaktionen

Doch bereits jetzt ist es bei vielen Chatbots möglich, dass diese gewaltverherrlichende, sexualisierte, rassistische und hasserfüllte Inhalte ausgeben. In einer Untersuchung wurden Forschende, die mit Accounts von Kindern mit Character.AI kommunizierten, binnen kurzer Zeit mit Inhalten wie Grooming, sexueller Ausbeutung, emotionaler Manipulation, Gewalt, Drogenmissbrauch, psychischen Gesundheitsrisiken und Rassismus und Hassrede konfrontiert (ParentsTogether Action & Heat Initiative, 2025). Character.AI wird auch die Mitschuld an Suiziden gegeben, aktuell laufen einige Klagen gegen die Betreiberfirma. Infolgedessen teilte Character.AI im Oktober 2025 mit, den Dienst ab 25. November 2025 für Minderjährige zu beschränken.[18]

1.2.7 ANDERE GEFÄHRLICHE INTERAKTIONSMÖGLICHKEITEN

Neben den bisher aufgeführten Gefahren bietet der digitale Raum noch weitere risikobehaftete Interaktionsmöglichkeiten. Eine umfassende Darstellung ist im Rahmen dieser Studie nicht möglich. Daher seien nur ein paar ausgewählte weitere Aspekte erwähnt, ohne Anspruch auf Vollständigkeit.

Bestellung von Alkohol etc.

Die Bestellung von für Minderjährige verbotenen Gütern (wie Alkohol, Tabak) oder allgemein stark reglementierten bis verbotenen Gütern (Drogen, Waffen etc.) ist ein Risiko, das (auch) Kinder und Jugendliche über das Internet prinzipiell betrifft. Diese Fälle werden aber in der Regel selten im Diskurs um Altersbeschränkungen und Social-Media-Verbote erwähnt.

Sexting, Mobbing, Dick Picks auch unter Gleichaltrigen

Andere Gefahren gehen von Sexting, Mobbing und dem unaufgeforderten Zusenden von Intimaufnahmen („Dick Picks" – seit 2025 in Österreich strafbar[19]) aus. Diese Phänomene weisen teils fließende Übergänge zu den oben ausgeführten Gefahren auf. Teilweise finden diese Interaktionen aber auch unter Gleichaltrigen statt und sind dann durch Altersbeschränkungen nicht zu unterbinden.

---

18 *orf.at/stories/3410086/*.

19 *parlament.gv.at/aktuelles/pk/jahr_2025/pk0721*.

2 RECHTLICHE GRUNDLAGEN

Altersbeschränkungen existieren bereits

Auf verschiedenen Ebenen werden aktuell Debatten geführt, ob und wie das Internet kinder- und jugendgerechter reguliert werden soll bzw. kann. Doch bereits jetzt gibt es eine Reihe an Rechtsnormen, die Implikationen für Altersfeststellungen im Internet haben, vom Digital Services Act (DSA) über die Datenschutz-Grundverordnung bis zum Jugendschutzgesetz. Darüber hinaus gibt es international bereits einige Beispiele für verschärfte Altersbeschränkungen. Dieses Kapitel gibt einen Überblick über den rechtlichen Kontext, in dem sich die aktuelle Debatte in Österreich bewegt.

2.1 NATIONALE REGELUNGEN WELTWEIT

In diesem Abschnitt geben wir einen kursorischen Überblick über einschlägige Regelungen, die in einzelnen Staaten getroffen wurden. Tabelle 1 gibt einen Überblick über diese Entwicklungen.

Australien als internationaler Vorreiter

Prominentestes Beispiel ist zweifellos Australien, das in Sachen Social-Media-Verbot eine Vorreiterrolle einnimmt: Kinder und Jugendliche unter 16 Jahren dürfen seit Ende 2025 kein Konto auf Sozialen Medien mehr besitzen (Fardouly, 2025). Aber auch Kalifornien ist bestrebt, die Gefahr Sozialer Medien für Minderjährige zu reduzieren, etwa indem süchtig machende Feeds und Benachrichtigungen zwischen Mitternacht und 6 Uhr früh sowie 8 Uhr morgens bis 15 Uhr nachmittags für Minderjährige verboten werden.[20] Texas hingegen verlangt von Webseiten, deren Inhalt mehr als ein Drittel Pornografie umfasst, dass sie eine Altersüberprüfung durchführen müssen.[21]

Entwicklungen in den EU-Mitgliedstaaten

In der EU planen einige Mitgliedsstaaten, nationale Regelungen einzuführen. Dänemark plant etwa ein Social-Media-Verbot für Unter-15-Jährige. Kinder zwischen 13 und 15 sollen mit Erlaubnis der Eltern Soziale Medien nutzen dürfen. Dabei ist noch unklar, welche Plattformen genau betroffen sein sollen.[22] Eine Untersuchungskommission des französischen Parlaments fordert in ihrem Abschlussbericht vom 4. September 2025, Soziale Medien für Minderjährige unter 15 zu verbieten und für 15-18-Jährige eine Social-Media-Sperrstunde zwischen 22 und 8 Uhr einzuführen (Delaporte & Miller, 2025). Auch in Norwegen gibt es aktive Diskussionen. Doch am schnellsten ist Griechenland: Bereits Ende Oktober 2025 trat in Griechenland ein Social-Media-Verbot für Unter-16-Jährige in Kraft.[23]

Online Safety Act in Großbritannien

In Großbritannien trat im Juli 2025 unter dem Online Safety Act ein Bündel an Verpflichtungen für Online-Plattformen in Kraft. Unter anderem müssen Pornografie-Webseiten eine robuste Altersverifikation durchführen. Einfache Selbstauskunft (siehe Abschnitt 3.2.1) ist dafür nicht ausreichend, ebenso wenig wie die

---

[20] *edition.cnn.com/2024/09/21/politics/california-social-media-bill-gavin-newsom/index.html.*

[21] *calawyers.org/privacy-law/supreme-court-upholds-texas-age-verification-law-in-major-free-speech-decision/.*

[22] *heise.de/news/Daenemarks-Regierung-plaediert-fuer-Social-Media-Verbot-fuer-Kinder-unter-15-Jahren-10733906.html.*

[23] *derstandard.at/story/3000000290093/griechenland-verbietet-social-media-nutzung-unter-16-jahren.*

Verifizierung über Zahlungsdienstleister, die auch für Unter-18-Jährige zugänglich sind.[24] Aber auch Inhalte über Suizid, selbstverletzendes Verhalten und Essstörungen werden streng reguliert und sollen Minderjährigen nicht zugänglich gemacht werden. Bei hasserfüllten, beleidigenden oder gewalttätigen Inhalten müssen je nach Alter abgestufte Vorkehrungen getroffen werden (Ofcom, 2025).

Tabelle 1: Überblick über aktuelle Bestrebungen für Altersbeschränkungen

Land	Altersbeschränkung	Status
Europäische Union	Einwilligung ab 16. Lebensjahr	Seit 2018 in Kraft
Österreich	Einwilligung ab 14. Lebensjahr	Seit 2018 in Kraft
Griechenland	Social-Media-Verbot bis 16	Seit November 2025 in Kraft
Frankreich	Social-Media-Verbot bis 15	Im September 2025 gefordert
Dänemark	Social-Media-Verbot bis 15	In Vorbereitung
Norwegen	Social-Media-Verbot bis 15	Gesetzesvorschlag, Konsultationsrunde im Oktober 2025 beendet
Großbritannien	Teilverbot von Pornografie und Inhalten über Suizid, Selbstverletzung und Essstörungen	Seit Juli 2025 in Kraft
Australien	Social-Media-Verbot bis 16	Seit Ende 2025 in Kraft
Texas (USA)	Pornografie-Verbot für Minderjährige	Im Juni 2023 beschlossen
Kalifornien (USA)	Verbot gewisser Interaktionsmuster; Benachrichtigungsverbot in der Nacht und während der Schulzeit	Ab Jänner 2027 in Kraft

2.2 EU-EBENE

Mehrere EU-Verordnungen berühren das Thema Minderjährige im digitalen Raum: Sowohl die Datenschutzgrundverordnung (DSGVO/GDPR) als auch der Digital Services Act sind hier zu erwähnen, ebenso wie die KI-Verordnung (AI Act).

[24] *ofcom.org.uk/online-safety/protecting-children/age-checks-to-protect-children-online.*

DSGVO regelt einwilligungsfähiges Alter …

… mit maximal 16 Jahren

Im Zentrum der DSGVO steht der Umgang mit personenbezogenen Daten. Da sowohl Soziale Netzwerke als auch Messengerdienste, viele Spiele usw. persönliche Daten verarbeiten, gilt auch für sie die DSGVO (Kunz & Waldmann, 2025). Um personenbezogene Daten verarbeiten zu dürfen, bedarf es in diesem Kontext i.d.R. der Einwilligung. Art. 8 Abs. 1 DSGVO regelt, dass Kinder erst ab vollendetem 16. Lebensjahr einwilligen können. Mitgliedsstaaten können dieses Alter aber auch niedriger ansetzen – bis zu einer Altersgrenze von 13 Jahren. Haben Nutzer:innen dieses Alter noch nicht erreicht, bedarf es der Zustimmung der Eltern. Daher ist die Frage, ob Nutzer:innen zustimmungsfähig sind, abhängig von ihrem Alter (siehe Abschnitt 1.1). Bei nicht verifizierten Altersangaben könnte Art. 7 Abs. 1 der DSGVO verletzt sein, der Verantwortliche verpflichtet, nachweisen zu können, dass betroffene Personen wirksam zur Datenverarbeitung eingewilligt haben (Kunz & Waldmann, 2025).

Digital Services Act verpflichtet Anbieter zum Schutz von Kindern und Jugendlichen

Art. 28 des DSA regelt den Online-Schutz Minderjähriger: Er besagt, dass Anbieter von für Minderjährige zugänglichen Online-Plattformen „geeignete und verhältnismäßige Maßnahmen ergreifen“ müssen, um ein hohes Maß an Privatsphäre und Sicherheit von Kindern und Jugendlichen zu gewährleisten (Abs. 2). Ebenso dürfen sie keine maßgeschneiderte Werbung schalten, wenn sie davon ausgehen können, dass der bzw. die Nutzer:in minderjährig ist (Abs. 2). Explizit sind die Betreiber aber *nicht* angehalten, zusätzliche personenbezogene Daten zu sammeln, um diesen Vorkehrungen umsetzen zu können (Abs. 3). Die Nutzung für Minderjährige in den Nutzungsvereinbarungen einfach zu verbieten enthebt die Betreiber nicht von diesen Pflichten, wenn nicht weitere wirkungsvolle Maßnahmen ergriffen werden, wodurch die Nutzung durch Minderjährige verhindert werden kann (Directorate-General For Communication Networks, Content And Technology, 2025).

AI Act verbietet Ausnutzen der Vulnerabilität junger Menschen

Der AI Act verbietet in Art. 5 Abs. 1b die Ausnutzung der altersbedingten Verwundbarkeit von Personen durch KI-Systeme. In den Richtlinien zu diesen verbotenen Praktiken spezifiziert die Europäische Kommission, dass insbesondere die kognitive Unreife von Kindern nicht zur schädlichen Beeinflussung, Manipulation und Ausbeutung missbraucht werden darf (European Commission, 2025). Als Beispiele werden die Verleitung von Kindern zu zunehmend riskanten Herausforderungen („Challenges“), um digitale Anerkennung zu erhalten (wie das Erklimmen von Möbeln, Würgen oder Hantieren mit scharfen Gegenständen), genannt, sowie KI, die auf einzelne Kinder zugeschnittene Anreize schafft, um sie zu längerer Nutzung zu ermuntern.

2.3 ÖSTERREICHISCHE EBENE

Auf Ebene nationaler Gesetzgebung sind grob drei Themenbereiche relevant: Spezifizierungen zur DSGVO, die Frage der Geschäftsfähigkeit und Jugendschutzgesetze.

Österreich legt die DSGVO liberal aus …

… Einwilligung ab 14 möglich

Wie im vorigen Abschnitt erwähnt, erlaubt die DSGVO den Mitgliedsstaaten, eine andere Altersschwelle für die Zustimmungsfähigkeit zur Verarbeitung personenbezogener Daten zu setzen. Österreich hat diese Möglichkeit wahrgenommen und legt im Datenschutzgesetz (DSG) Art. 2 § 4 Abs. 4 fest, dass Kinder per vollendetem vierzehnten Lebensjahr einwilligen können. Damit gilt – wenn keine Zustimmung der Eltern gegeben ist – ein Social-Media-Verbot in Österreich bis

zum 14. Geburtstag,[25] da in Sozialen Medien davon auszugehen ist, dass personenbezogene Daten verarbeitet werden (s.o.).

Eingeschränkte Geschäftsfähigkeit von Minderjährigen …

In Österreich sind Kinder zwischen sieben und 13 Jahren beschränkt geschäftsfähig und dürfen nur kleine Geschäfte des alltäglichen Lebens abschließen („Taschengeldgeschäfte"). Online getätigte Geschäfte zählen nicht darunter.[26] 14- bis 18-Jährige sind mündig, aber weiterhin nur beschränkt geschäftsfähig: Sie können frei über Einkommen aus eigenem Erwerb verfügen, solange die Befriedigung ihrer Lebensbedürfnisse nicht gefährdet ist. Das heißt, dass Geschäfte, die über Taschengeldgeschäfte hinausgehen, ohne Zustimmung der Eltern „schwebend unwirksam" sind: Sie können durch die Zustimmung der gesetzlichen Vertreter:innen (i.d.R. die Eltern) nachträglich noch gültig werden.[27]

… macht Online-Verträge oft (schwebend) unwirksam

Selbstregulierung der Medienbranche

Seit 2019 ist in Österreich der Jugendschutz (eigentlich im Zuständigkeitsbereich der Bundesländer) großteils bundesweit harmonisiert. Er regelt u.a. den Zugang zu Alkohol und Tabak sowie den Medienschutz. Seit 2021 ist dieser neu geregelt und basiert überwiegend auf einer Selbstregulierung der Medienbranche.[28]

„potentiell entwicklungsbeeinträchtigende Inhalte"

Die Regeln des Medienschutzes sehen vor, dass „potentiell entwicklungsbeeinträchtigende Inhalte" durch die Wahl der Sendezeit üblicherweise von Minderjährigen nicht gesehen werden. Abrufdienste (d.h. Online-Portale) müssen anderweitig ein ähnliches Schutzniveau sicherstellen. „Besonders schädliche Inhalte" wie Hardcore-Pornografie erfordern „Maßnahmen wie Altersverifikationssysteme oder vergleichbare Maßnahmen der Zugangskontrolle" (Verein zur Selbstkontrolle audiovisueller Medienangebote zum Schutz von Minderjährigen, 2021). Anzumerken ist an dieser Stelle, dass Video-Portale wie Netflix und YouTube nicht in der Liste der diesen Richtlinien verpflichteten Akteure aufscheinen.[29]

Netflix & Co. nicht erfasst

---

25 *saferinternet.at/news-detail/mindestalter-ab-wann-duerfen-kinder-soziale-netzwerke-nutzen.*

26 *onlinesicherheit.gv.at/Themen/Gefahren-im-Netz/Kinder-im-Internet/Kinder-und-Vertraege.html.*

27 *oesterreich.gv.at/de/themen/gesetze_und_recht/gerichtsorganisation_der_justiz/zivilrecht/8/Seite.1740386.*

28 *jugendmedienschutz.at.*

29 *jugendmedienschutz.at/wp-content/uploads/2025/10/Liste_Jugendschutzerklaerungen_2025-10.pdf.*

3 TECHNISCHE GRUNDLAGEN

Es gibt verschiedene Verfahren, die Altersbeschränkungen zugrunde liegen können. Dabei gibt es zwei Möglichkeiten, diese Verfahren zu systematisieren. Erstens können sie an unterschiedlichen Ebenen greifen: Wie in Abschnitt 3.1 ausgeführt wird, kann dies auf Ebene des Geräts stattfinden, vor der Installation von Anwendungen, innerhalb einer Anwendung oder Plattform oder bei einzelnen Inhalten.

Präzise Altersfeststellung vs. Schätzung

Zweitens können Methoden grob in Altersfeststellung im engeren Sinne und Altersabschätzung gegliedert werden: Bei ersterer soll das präzise Alter festgestellt werden (etwa durch Dokumente oder Selbstauskunft), bei letzterer wird das Alter grob geschätzt (etwa durch Gesichtsanalyse). In Abschnitt 3.2 werden die verschiedenen methodischen Ansätze genauer erläutert: Selbstauskunft, biometrische Methoden, Verhaltensanalyse und verschiedene Formen der Authentifizierung.

3.1 EBENEN DER ALTERSFESTSTELLUNG

Altersfeststellung kann auf verschiedenen Ebenen stattfinden …

Die Altersfeststellung kann auf mehreren Ebenen greifen. Dabei werden aktuell primär vier Ebenen diskutiert: Die Beschränkung einzelner Inhalte und Funktionen, die Beschränkung ganzer Plattformen und Apps, die Altersfeststellung in App Stores und schließlich auf Geräte-Ebene. Relativ selten wird die Beschränkung auf Internet-Provider-Ebene in den aktuellen Debatten diskutiert, obwohl Provider etwa bei Copyright-Fragen relativ stark in die Pflicht genommen wurden, um den Zugang zu bestimmten Webseiten zu unterbinden.

… mit variierender Granularität

Abbildung 1 zeigt die vier zentral diskutierten Ebenen schematisch: Während die Sperre von spezifischen Inhalten und Funktionen sehr feingliedrig ist, sind Beschränkungen auf Geräte- und App-Store-Ebene relativ grobschlächtig. Darüber hinaus geht mit der Ebene auch die Zuständigkeit einher: Während es nur wenige App Stores und Betriebssystem-Anbieter gibt, sieht die Sache bei Plattformen (inkl. Webseiten), Inhalten und Funktionen anders aus: Hier sind unzählige Akteure involviert, besonders dann, wenn auch durch Nutzer:innen erstellte Inhalte angeboten werden.

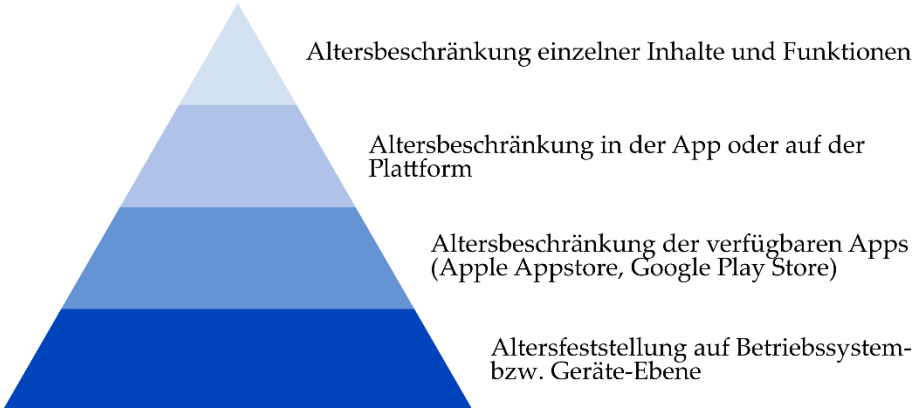

Abbildung 1: Ebenen der Altersfeststellung nach oben hin steigender Granularität

3.1.1 GERÄTEEBENE

Kinder-Konten auf Smartphones

Viele Betriebssysteme bieten die Möglichkeit an, Kinder-Accounts einzurichten. Häufig geht das einher mit Management-Funktionen für Eltern. Bei Android können dann etwa mittels Family Link Zeitbeschränkungen eingestellt und bestimmte Apps oder Webseiten blockiert werden.[30] Außerdem wird automatisch die Google-Suche gefiltert und gewisse Einstellungen können für das Kind gesperrt werden.

Griechenland: Kids Wallet blockiert Social Media

Auf Gerätebene greift auch die Umsetzung des Social-Media-Verbots in Griechenland: Wird auf einem Smartphone die staatliche App „Kids Wallet" installiert, unterbindet diese automatisch die Nutzung von Plattformen wie Facebook, Instagram, X und TikTok.[31] Was hier zu bedenken ist, ist der Fokus auf Smartphones, Tablets und anderen „smarten" Geräten (wie Fernseher): Es ist unklar, ob bzw. wie eine ähnliche Beschränkung auf Laptops und Desktop-PCs, wo viele Inhalte nicht über Apps, sondern über Web-Browser abgerufen werden, umgesetzt werden soll. Dass auch diese Geräte ein Thema sind, zeigt die Umsetzung von Filtern auf Schüler:innenlaptops durch das Bildungsministerium.[32]

Vorschlag von epicenter.works

Ein im Dezember 2025 veröffentlichtes Konzept der Datenschutz-NGO epicenter.works setzt ebenfalls auf der Geräte-Ebene an.[33] Der Vorschlag ist, dass auf Geräten Konten für Minderjährige eingerichtet werden können, in denen Bezugspersonen das Alter festlegen, um in weitere Folge an Apps und Webseiten kommuniziert zu werden (Details dazu in Abschnitt 3.2.2). Wie epicenter.works herausstreicht, fehlt für diese Form der Umsetzung noch der technische Standard – sowohl zur Umsetzung von Minderjährigen-Accounts auf verschiedenen Plattformen als auch zur Übermittlung der Information an Webseiten und Apps – hier könnte die EU eine führende Rolle einnehmen.

3.1.2 APP STORES

Apps werden häufig über App Stores bezogen

App Stores sind ein zentraler Angelpunkt vieler Betriebssysteme: Besonders dominant sind sie unter den zentralen Smartphone- und Tablet-Betriebssystemen Android und iOS/iPad OS sowie „smarten" Geräten (Uhren, Fernseher): Es ist teilweise schwer bis unmöglich, auf anderem Weg Anwendungen zu beziehen. Aber auch unter Windows und Mac OS kommt App Stores eine zunehmende wichtige Rolle zu.

Kuratierung von Apps durch Store-Betreiber

App Stores bieten einerseits eine Infrastruktur zur Monetarisierung für Software-Anbieter und -Updates, andererseits dienen sie auch der Qualitätskontrolle: Heute werden die darin angebotenen Apps in vielerlei Hinsicht kuratiert und gegebenenfalls auch aus dem Katalog genommen. Hier reicht die Bandbreite von Scans auf Schadsoftware bzw. schädliche Funktionen, Zugriffsrechte, aber auch darauf, ob Inhalte und Funktionen den App-Store-Richtlinien widersprechen.

---

30 *support.google.com/families/answer/7158477?hl=de.*

31 *derstandard.at/story/3000000290093/griechenland-verbietet-social-media-nutzung-unter-16-jahren.*

32 *orf.at/stories/3406830/.*

33 *epicenter.works/content/altersverifikation-neu-gedacht-ein-moeglicher-loesungsansatz.*

Kategorisierung der Apps nach Altersgerechtigkeit

Ein Teil dieser Richtlinien ist sowohl bei Googles Play Store als auch bei Apples App Store die Einstufung von Apps nach Alter (OECD, 2025a): Sie sollen darstellen, für welche Altersgruppe eine App geeignet ist. Darauf aufbauend gibt es auch eine an Kinder gerichtete App-Auswahl. Dennoch bekommen sogar Accounts von Kindern teilweise unpassende Apps als Empfehlung – die Umsetzung scheint somit mangelhaft (OECD, 2025a). Für Online-Spiele gibt es eine Erweiterung des Pan European Game Information Systems (PEGI) zur Klassifikation von Spielen inkl. Alterskennzeichnungen mit einer Lizenz zur Darstellung des Logos für Spiele, welche die Kriterien erfüllen.[34]

Mindestalter für App Stores

Doch auch die Nutzung der App Stores selbst unterliegt einem Mindestalter: Dies ist bei den gängigen App Stores (von Google, Apple und Huawei) grundsätzlich mit 13 Jahren festgelegt, in manchen Regionen gelten jedoch höhere Altersschranken bis zu 16 Jahren (OECD, 2025a).

3.1.3 AUF EBENE DER APP BZW. PLATTFORM

Altersbeschränkung durch App/Plattform geregelt …

Anbieter von Apps und Online-Plattformen können, unabhängig von vorgelagerten Beschränkungen (s.o.), die Nutzung erst ab einem gewissen Alter erlauben. Das ist bereits jetzt vielfach der Fall: Viele Nutzungsbedingungen sehen ein Mindestalter vor. WhatsApp, Instagram, Facebook, TikTok, Threads, ChatGPT und X sind nur einige der Plattformen, die grundsätzlich ein Mindestalter von 13 Jahren voraussetzen. Häufig wird dieses Mindestalter in den Nutzungsbedingungen um den Hinweis ergänzt, dass je nach lokaler Gesetzgebung auch ein höheres Mindestalter einzuhalten ist – hier wird die Verantwortung, die geltenden Gesetze zu kennen, auf die Verbraucher:innen übertragen.

… durch Nutzungsbedingungen

Zustimmung der Eltern

Manche Dienste wie beispielsweise YouTube schreiben zusätzlich zum Mindestalter vor, dass Minderjährige über dieser Altersgrenze (14 bei YouTube) die Zustimmung der Eltern brauchen. In diesem Fall sollten Eltern gemeinsam mit den Minderjährigen die Nutzungsbedingungen durchlesen.

Umgehungsmöglichkeit per Webbrowser

Da viele Plattformen in Webbrowsern ohne Registrierung nutzbar sind, ist fraglich, wie effektiv die Nutzung durch Kinder und Jugendliche verhindert werden kann, wenn das Alter nur bei der Installation von Apps oder beim Anlegen eines Kontos überprüft wird.

3.1.4 BESCHRÄNKUNG EINZELNER INHALTE UND FUNKTIONEN

Einzelne Inhalte und Funktionen beschränken …

Die granularste Ebene der Beschränkung ist, die Nutzung eines Dienstes per se allen zu erlauben, aber den Zugang zu bestimmten Inhalten und Funktionen zu beschränken. Dies ist etwa bei der Nutzung von YouTube der Fall: Manche Inhalte können ohne Login nicht betrachtet werden. Bei der Kontoerstellung ist die Altersfeststellung durchzuführen (bei YouTube bzw. Google durch Selbstauskunft).

… braucht deren Kuratierung

Wie bei App Stores (s.o.) ist auch hier eine Vorbedingung, dass die Inhalte kuratiert werden: Es müssen somit Moderationsinfrastruktur und -richtlinien existieren. Wie bereits in Abschnitt 1.2.2 erwähnt, erfolgt derzeit jedoch ein Rückbau von Moderationsbestrebungen: So hat Facebook Anfang 2025 in den USA seine Fact-Checking-Abteilung durch Nutzer:innen-basierte Faktenchecks ersetzt – und

[34] *pegi.info/de/node/51.*

das in einer Zeit, in der generative KI das Verbreiten von Desinformation erleichtert.[35]

Grenze zur Zensur fließend

Die Auswahl, welche Inhalte als adäquat für welche Altersgruppe gelten, kann durchaus zu kontroversen Einschätzungen führen und liegt bei dieser Umsetzung von Altersbeschränkungen in der Hand der Plattform-Betreiber. Ungarns Verbot von LGBTIQ-Inhalten in Medien, die sich an Kinder richten, zeigt, dass hier keine Einigkeit in der EU angenommen werden kann.

3.2 METHODEN DER ALTERSFESTSTELLUNG

Es gibt eine Vielzahl konkreter Methoden, wie das Alter festgestellt werden kann. Manche werden bereits heute breit genutzt, andere sind noch in Entwicklung und werden erst in Monaten bis Jahren einsatzfähig sein. Die Verfahren sind sehr unterschiedlich ausgestaltet und haben jeweils viele Vor- und Nachteile.

3.2.1 SELBSTAUSKUNFT

Selbstauskunft durch Klicken eines Buttons …

Die heute wohl geläufigste Variante, das Alter von Nutzer:innen festzustellen, ist die Selbstauskunft: Einerseits gibt es die Form, ausdrücklich zu bestätigen, über einem bestimmten Alter zu sein (etwa älter als 18 Jahre). Das wird in der Regel durch das einfache Anklicken einer Schaltfläche realisiert, wie es beispielsweise viele pornografische Webseiten aktuell einsetzen (siehe **Fehler! Verweisquelle konnte nicht gefunden werden.**).

Abbildung 2: Selbstauskunft durch Klicken auf einen Button[36]

4.3 Mindestalter

Sie können die Plattform nur nutzen, wenn Sie 13 Jahre oder älter sind, obwohl Sie für einige Funktionen älter sein müssen (wir werden Sie darüber informieren, wenn dies der Fall ist). Wir überwachen die Nutzung durch Minderjährige und werden Ihr Konto sperren (während wir Nachforschungen anstellen) oder kündigen, wenn wir den begründeten Verdacht haben, dass Sie minderjährig sind oder einer Person unter 13 Jahren die Nutzung Ihres Kontos erlauben. Gegen eine Kündigung Ihres Kontos können Sie Einspruch einlegen, wenn Sie glauben, dass wir uns geirrt haben.

Kurz gesagt: Sie müssen 13 Jahre oder älter sein, um unsere Plattform nutzen zu können.

Abbildung 3: Implizite Selbstauskunft durch die Zustimmung zu den Nutzungsbedingungen[37]

… oder implizit durch Akzeptieren der Nutzungsbedingungen

Andererseits findet dies aber auch durch das Akzeptieren der Nutzungsbedingungen (Terms of Service) einer Plattform oder App statt: Häufig wird in diesen ein Mindestalter festgehalten, unter welchem Nutzer:innen die Plattform nicht

[35] *msutoday.msu.edu/news/2025/01/ask-the-expert-what-meta-new-fact-checking-policies-mean-for-misinformation-and-hate-speech.*

[36] Screenshot von *pornhub.com* vom 4.9.2025.

[37] Screenshot von *tiktok.com/legal/page/eea/terms-of-service/de* vom 29.7.2025.

benutzen dürfen (siehe Abbildung 3). Wird den Nutzungsbedingungen zugestimmt, wird somit bestätigt, über dem darin festgehaltenen Alter zu sein (auf die in diesem Fall schlagend werdende Problematik dieser Zustimmung bzw. Nichtzustimmung durch Kinder wurde bereits in Abschnitt 1.1 hingewiesen).

3.2.2 FESTLEGUNG DES ALTERS DURCH BEZUGSPERSONEN

Bezugspersonen legen Alter auf Gerätebene fest

Die Festlegung des Alters von Kindern und Jugendlichen durch Bezugspersonen (Eltern, Lehrer:innen und andere Aufsichtspersonen) auf Geräteebene ist eine Variante, die durch die Zivilrechts-NGO epicenter.works (siehe auch Abschnitt 3.1.1) Ende 2025 vorgeschlagen wurde. Bei diesem Ansatz liegt die Verantwortung der korrekten Angabe bei diesen Bezugspersonen. Inwiefern ein derartiger Ansatz durch Minderjährige umgangen werden kann, liegt in erster Linie an der konkreten Umsetzung – sowie den Kompetenzen der Bezugspersonen.

Information über Alter wird datensparsam mit Apps und Webseiten geteilt

Der klare Vorteil dieses Ansatzes ist, dass dem Prinzip der Datenminimierung gefolgt würde. Ein Ausweis oder ähnliches würde weder für die Bezugsperson noch die minderjährige Person benötigt. In weiterer Folge würde dieses Alter bzw. die Information, über einer bestimmten Altersschwelle zu sein, sowohl an Apps als auch an Webseiten übermittelt werden. Diese Übermittlung kann datensparsam umgesetzt werden, ähnlich den Attributsbescheinigungen der EUDI-Wallet (siehe Abschnitt 3.2.5.3). Dieser Ansatz ist aber zum Zeitpunkt dieser Studie im Konzeptstadium; aktuell ist daher nicht absehbar, ob er tatsächlich praktische Verwendung finden wird.

3.2.3 BIOMETRISCHE METHODEN

Schätzung des Alters anhand körperlicher Eigenschaften

Biometrische Methoden, also die Analyse körperlicher Eigenschaften, stellen einen anderen Ansatz dar. Dabei wird das Alter der Nutzer:innen geschätzt. In der Regel werden hierfür die Gesichter der Nutzer:innen analysiert. Zum Einsatz kommen Maschinelle Lernverfahren (Machine Learning), also eine Spielart von Künstlicher Intelligenz. Ein anderer Einsatz biometrischer Methoden ist, zu überprüfen, ob die Person vor dem Laptop, Smartphone oder Tablet auch tatsächlich die Person auf einem Lichtbildausweis ist.

3.2.3.1 SCHÄTZUNG DES ALTERS DURCH GESICHTSANALYSE

Fotos oder Videos des Gesichts

Wird nur das Gesicht ohne Ausweisdokument analysiert, handelt es sich um eine reine Schätzung des Alters anhand körperlicher Merkmale. Dabei können sowohl Fotos als auch (Live-)Videoaufnahmen analysiert werden. Letztere erlauben es, das Gesicht aus mehreren Blickwinkeln zu betrachten, indem die Nutzer:innen den Kopf drehen. Dank der mittlerweile omnipräsenten Kameras für Videotelefonie und Selfies in den gängigen Endgeräten braucht es dazu keine aufwändige zusätzliche Infrastruktur und die Nutzung ist oft ausgesprochen niederschwellig (European Commission. Directorate General for Communications Networks, Content and Technology. et al., 2024).

Roblox schätzt das Alter durch Gesicht

Eine Plattform, die diesen Ansatz verfolgt, ist die Spieleplattform Roblox.[38] Basierend auf dem geschätzten Alter werden verschiedene Einstellungen

[38] *en.help.roblox.com/hc/de/articles/42295385001236-Wie-sch%C3%A4tze-ich-mein-Alter-auf-Roblox.*

vorgenommen: Wird das Alter unter 13 geschätzt, werden etwa bestimmte personenbezogene Daten wie E-Mail und Telefonnummer gelöscht. Andere Funktionen werden nur für ältere Kinder und Jugendliche aktiviert. Ergänzend nutzt Roblox aber auch in manchen Situationen die Altersverifizierung mittels Lichtbildausweis.[39]

Schätzung relativ ungenau …

Allerdings kann in diesem Fall das Alter der Nutzer:in nur *geschätzt* werden. Das heißt, diese Methode ist relativ ungenau und damit als unzuverlässig einzuschätzen (Kunz & Waldmann, 2025). Aufgrund des gestiegenen Interesses an dieser Technologie untersucht das US-amerikanische National Institute of Standards and Technology (NIST) seit 2024 regelmäßig die Ergebnisse dieser Methode in Hinblick auf deren Zuverlässigkeit. Im Durchschnitt war die Abweichung zum tatsächlichen Alter 3,1 Jahre. Dabei variiert die Qualität jedoch nach Geschlecht, Geburtsort und Alter, insbesondere waren die Fehlerraten bei weiblichen Gesichtern fast durchgängig höher als bei männlichen (Grother et al., 2024).

… und nicht für alle gleich gut

Umgehungs-möglichkeiten

Zu dieser Unzuverlässigkeit kommt noch hinzu, dass frei verfügbare KI-Angebote zum künstlichen Altern einer Person auf einem Foto genutzt werden können, um die Altersfeststellung zu manipulieren. Es hat sich auch gezeigt, dass Videospielcharaktere zur Umgehung der Alterssperre eingesetzt werden können.[40]

Für manche funktioniert Gesichtserkennung nicht

Es gibt aber auch zahlreiche Berichte darüber, dass die Software Gesichter nicht als solche erkennt, wenn bestimmte Merkmale stark vom Durchschnitt abweichen.[41] Auch hier stellt somit das Problem des Bias von Algorithmen, Machine-Learning bzw. KI basierenden Technologien eine anhaltende Herausforderung dar.

3.2.3.2 ABGLEICH VON GESICHT UND LICHTBILDAUSWEIS

Ist die Person vor Smartphone die gleiche wie am Ausweis?

Ein anderer Einsatz der Gesichtsbiometrie ist der automatische Abgleich eines Lichtbildausweises mit einer Live-Aufnahme der Nutzer:in.[42] Hier wird also nicht das Alter der Nutzer:in geschätzt, sondern es soll sichergestellt werden, dass ein Ausweisdokument tatsächlich auch der Nutzer:in vor dem Gerät gehört – und nicht etwa einem Elternteil. Dazu wird in der Regel mit der Webcam (Laptop) bzw. der Selfie-Kamera (Smartphone, Tablet) ein Foto oder Video aufgenommen, in dem die Nutzer:in das Dokument und das eigene Gesicht gleichzeitig aufnimmt. Üblicherweise wird gleichzeitig das Geburtsdatum vom Dokument abgelesen und digitalisiert (siehe Abbildung 4).

Häufig verwendete Methode

Lösungen dieser Art werden etwa durch X (ehemals Twitter) zur Verifizierung der Identität genutzt – was Vorbedingung ist, um manche Möglichkeiten der Plattform zu nutzen (z. B. der Markierung als verifizierter Account, prioritärer Support-Zugang und Monetarisierung).[43] Konkret werden in diesem Fall etwa

---

39 *en.help.roblox.com/hc/en-us/articles/39143693116052-Understanding-Age-Checks-on-Roblox.*

40 *ia.acs.org.au/article/2025/unbelievably-easy-online-age-checks-tricked-in-uk.html.*

41 *forbes.com/sites/gusalexiou/2025/02/27/disfigurement-charity-exposes-rampant-exclusion-by-ai-facial-recognition-tools/.*

42 In manchen Kontexten, z. B. bei Banken, wird dieser Abgleich auch in Videocalls von Menschen durchgeführt.

43 *help.x.com/en/rules-and-policies/verification-policy; help.x.com/en/rules-and-policies/age-assurance.*

Au10tix,[44] Persona[45] und Stripe[46] genutzt, wobei X auch an einer eigenen Lösung arbeiten dürfte.[47]

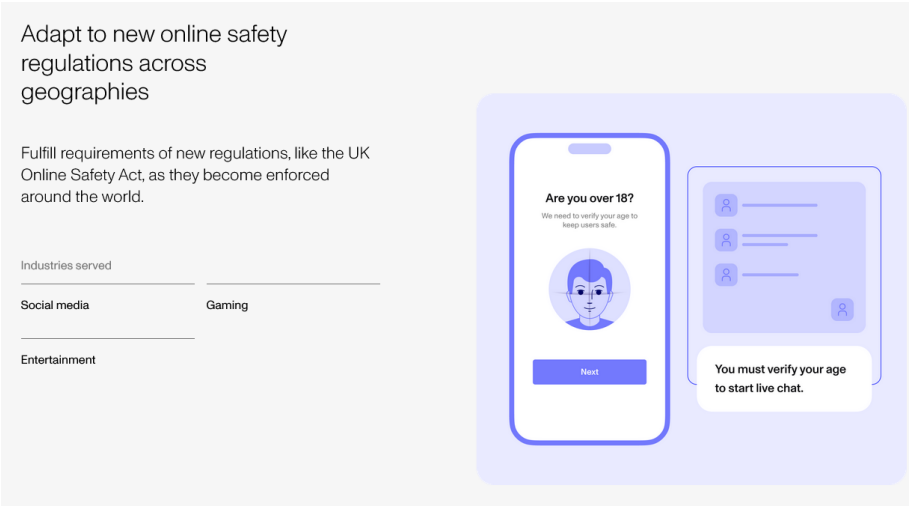

Abbildung 4: Abgleich von Selfie und Lichtbildausweis, hier am Beispiel des Dienstleisters persona[48]

3.2.4 VERHALTENSANALYSE

Wie sich Nutzer:innen im Internet bewegen, wie und welche Inhalte sie konsumieren oder ob und welche Einkäufe sie online tätigen, sind mächtige Informationen für das Anlegen von Profilen. Derartige Profile können auch dazu genutzt werden, das Alter abzuschätzen.

Nutzungsverhalten gibt Aufschluss über Alter

Einige Plattformen geben an, derartige Ansätze zu verfolgen, um minderjährige Nutzer:innen zu identifizieren: YouTube analysiert in den USA etwa, wonach Nutzer:innen auf YouTube suchen, welche Videos sie in der Vergangenheit angesehen haben und wie lange der Account bereits existiert.[49] Wird jemand auf diese Weise als unter 18 eingestuft, werden automatisch die Einstellungen für Unter-18-Jährige aktiviert, was unter anderem bedeutet, dass der Zugang zu manchen Inhalten beschränkt wird. Um die Inhalte trotzdem anzuzeigen, müssen sich Nutzer:innen mit einer Kreditkarte (siehe Abschnitt 3.2.4.1) oder einem Lichtbildausweis verifizieren (siehe Abschnitt 3.2.2).

Ähnliche Ansätze dürften etwa auch TikTok und X verfolgen: TikTok gibt an, dass bei „begründetem Verdacht“ auf ein zu junges Alter das Nutzer:innenkonto gesperrt werden kann. X gibt an, dass verschiedene „Signale“ und die Daten der

---

44 *au10tix.com.*

45 *withpersona.com/use-case/compliance/age-assurance.*

46 *stripe.com.*

47 Vgl. „ID verification: Users can submit a government-issued ID, which will be used to estimate their age by our artificial intelligence systems. These measures should be made available in the following weeks. We will update this page in due course.“ *help.x.com/en/rules-and-policies/age-assurance.*

48 Screenshot von *withpersona.com/use-case/compliance/age-assurance* vom 4.9.2025.

49 *blog.youtube/news-and-events/extending-our-built-in-protections-to-more-teens-on-youtube/.*

Nutzer:innen genutzt werden können, um das Alter zu schätzen. Wie in Abschnitt 1.2.5 bereits ausgeführt, haben diese Plattformen keinen Anreiz, dem Verdacht auf Minderjährigkeit konsequent nachzugehen und Einschränkungen vorzunehmen.

Fehlerhaft und baut auf Tracking von Nutzer:innen auf

Ein relativ offensichtliches Problem dieses Ansatzes ist, dass er einerseits recht fehlerhaft ist – und dann möglicherweise noch eine weitere Verifizierungsmethode herangezogen werden muss, um die Einschätzung zu verbessern. Andererseits ist er aber auch ein bequemes Argument, um das Profiling von Nutzer:innen voranzutreiben und zu legitimieren.

3.2.5 AUTHENTIFIZIERUNGSMETHODEN

Authentifizierung genauer als Schätzung

Die bisher vorgestellten Methoden sind in der Regel relativ unzuverlässig: Die Schätzung des Alters mittels Gesichts- oder Verhaltensanalyse ist relativ ungenau. Ebenso ist eine falsche Selbstauskunft einfach zu bewerkstelligen. Die im Abschnitt 3.2.2.2 vorgestellte Methode, ein Selfie mit einem Lichtbildausweis abzugleichen, steht und fällt mit der Qualität der Gesichtserkennung, kann aber auch als Authentifizierung gelten, da hier das Geburtsdatum am Lichtbildausweis entscheidend ist – und nicht das Aussehen an sich.

Die im nun folgenden Abschnitt vorgestellten Methoden dienen nicht der Schätzung des Alters, sondern sollen verlässliche Auskunft geben, ob ein Gegenüber tatsächlich volljährig ist – oder, je nach Technologie, über bzw. unter einer Altersschwelle ist.

3.2.5.1 KREDITKARTE

Kreditkarten nur für Volljährige verfügbar

Eine etablierte Praxis ist, Nutzer:innenkonten mit Kreditkartendaten zu verknüpfen. In erster Linie dienen diese Informationen der Bezahlung von Abonnements oder Käufen. Oft wird damit aber auch angenommen, dass die Nutzer:in auch die Inhaber:in der Kreditkarte ist. Da Kreditkarten nur Volljährigen zur Verfügung stehen, wird daraus gefolgert, dass die Nutzer:in volljährig ist.

Kreditkartendaten können leicht weitergegeben werden …

… und haben nicht alle zur Verfügung

Diese Annahme ist aber zu hinterfragen: So ist es gut möglich, dass auch Konten von Kindern mit den Kreditkarten der Eltern oder von Bekannten verknüpft werden, um zum Beispiel In-App-Käufe zu tätigen. Je nachdem, wie sorgfältig die Daten verifiziert werden (etwa per 2-Faktor-Authentifizierung), könnten auch findige Kinder und Jugendliche ohne Wissen der Karteninhaber:innen die Daten eingeben. Und schließlich haben nicht alle Erwachsenen eine Kreditkarte, etwa weil ihre Kreditwürdigkeit zu gering ist. Sie könnten auf diesem Wege von Angeboten ausgeschlossen werden (Kunz & Waldmann, 2025).

3.2.5.2 ID AUSTRIA

ID Austria zur Umsetzung von Altersbeschränkungen erwähnt

Mit der ID Austria gibt es seit Ende 2023 eine Möglichkeit, die eigene Identität gegenüber Onlinediensten nachzuweisen. Sie hat im Dezember 2023 endgültig die Handysignatur abgelöst und ist zunehmend Voraussetzung für den Login bei vielen staatliche digitalen Diensten. Im Zuge gefährdender Inhalte im Internet wurde immer wieder eine Registrierungspflicht für Soziale Medien in die Diskussion eingebracht. Zuletzt hat dies etwa im Juni 2025 Digitalisierungs-Staatsekretär Alexander Pröll öffentlich überlegt: So solle es möglich sein, den Zugang erst ab

einem gewissen Alter zu ermöglichen. Als technische Lösung wurde die ID Austria genannt.[50]

Überidentifikation würde drohen

Anders als die EUDI-Wallet (siehe unten, Abschnitt 3.2.5.3) würde die ID Austria es aber weder erlauben, sich mit Pseudonymen auszuweisen, noch unterstützt die ID Austria das Teilen einzelner Eigenschaften (wie das Alter) – letzteres soll hingegen die Europäische Altersfeststellungs- (siehe unten, Abschnitt 3.2.5.4) erlauben. Somit wäre die Identifikation von Nutzer:innen ohne Probleme möglich – angesichts des Ansinnens, das Alter zu überprüfen, freilich in Widerspruch zum Grundsatz der Datenminimierung. Dadurch wäre Tracking einfach, auch über Plattformen hinweg.

3.2.5.3 EUROPÄISCHE BRIEFTASCHE FÜR DIE DIGITALE IDENTITÄT (EUDI-WALLET)

EUDI-Wallet ab Ende 2026 EU-weit verfügbar

Im Mai 2024 trat die sogenannte eIDAS 2.0-Verordnung in Kraft, die einen europäischen Rahmen für eine digitale Identität schafft.[51] Artikel 5a dieser Verordnung definiert die rechtlichen Grundlagen für die Europäische Brieftasche für die digitale Identität (European Digital Identity Wallet/EUDI-Wallet). Bis Ende 2026 sollen alle EU-Mitgliedsstaaten eine EUDI-Wallet anbieten.

Teilen von einzelnen Attributen und Authentifizierung per Pseudonym

Die EUDI-Wallet soll Nutzer:innen unter anderem ermöglichen, sich gegenüber Online-Plattformen zu authentifizieren oder ausgewählte Eigenschaften zu teilen (sog. Attributsbescheinigungen). Da die Online-Plattformen auf die Authentifizierung durch die EUDI-Wallet vertrauen werden sie als sog. vertrauende Beteiligte (relying parties) bezeichnet. Die Authentifizierung kann dabei auch per Pseudonym stattfinden, sofern die (amtliche) Identifizierung der Nutzer:innen nicht anderweitig vorgeschrieben ist.

Volle Kontrolle bei Nutzer:innen

Dabei ist ein zentrales Ziel der Verordnung, dass Nutzer:innen stets volle Kontrolle über die Daten und deren Weitergabe behalten. Neben anderen Funktionen wäre es also möglich, dass je nach Anwendungsfall nur das Alter oder auch nur die Überschreitung eines gewissen Alters übermittelt wird. Weitere Funktionen der EUDI-Wallet wie das Validieren im physischen Raum (etwa bei Verkehrskontrollen) und das qualifizierte Signieren von Dokumenten sind für das Thema der vorliegenden Studie von untergeordneter Bedeutung und werden daher in Folge nicht näher betrachtet.[52]

Einfaches Online-Login

Was heißt die Einführung der EUDI-Wallet konkret für Verbraucher:innen, gerade im Zusammenhang mit Altersbeschränkungen? Erstens sollte es damit in Zukunft ähnlich einfach sein, sich (auch per Pseudonym) bei verschiedenen Online-Diensten mit der EUDI-Wallet einzuloggen, wie es bereits bei vielen Plattformen beispielsweise mit einem Google- oder Amazon-Konto ist, ohne ein dezidiertes Nutzer:innenkonto (mit zugehörigem Passwort usw.) zu eröffnen.

Gezieltes Teilen einzelner Attribute wie „über 18“

Zweitens wird beim gezielten Teilen von einzelnen Eigenschaften (Attributen) konsequent das Prinzip der Datenminimierung angewandt. Das heißt, wenn eine Plattform verifizieren möchte, dass ein:e Nutzer:in volljährig ist, dann wird nur die Information „Ich bin über 18“ geteilt. Dabei ist es egal, ob die Nutzer:in den

---

50 *derstandard.de/story/3000000274542/regierung-will-mit-registrierungspflicht-die-anonymitaet-im-netz-abschaffen.*

51 *eur-lex.europa.eu/eli/reg/2024/1183/oj.*

52 Siehe (Verordnung (EU) 2024/1183 des Europäischen Parlaments und des Rates vom 11. April 2024 zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung des europäischen Rahmens für eine digitale Identität, 2024).

Nachweis am 18. Geburtstag erbringt oder bereits im gehobenen Alter ist: Es werden weder das Geburtsdatum noch das absolute Alter und insbesondere nicht der Name und andere für den Zweck nicht benötigte Daten geteilt.

Drittens soll die Lösung explizit nutzer:innenfreundlich sein. Sie soll also so komfortabel nutzbar sein, wie es derzeit Wallet-Apps von Banken, Google und Apple am Smartphone sind.

Starker Datenschutz vorgesehen, wie …

Viertens sieht die Verordnung Vorkehrungen für einen starken Datenschutz für das Teilen von Attributen vor: Denn weder Online-Dienste, mit denen man Attribute teilt, noch die ausstellende Stelle (d.h. der Staat) sollen in der Lage sein, nachzuvollziehen, wann, wo (und im Falle des Staates: gegenüber wem) die EUDI-Wallet genutzt wurde (unlinkability). Und sogar in Zusammenarbeit zwischen Staat und Online-Plattformen soll dies unmöglich bleiben (untraceability) (Baum et al., 2024). Es soll, anders gesagt, nicht möglich sein zu wissen, dass ein und dieselbe Nutzer:in sich auf Plattform A als volljährig ausgewiesen hat und ebenso auf Plattform B. Es soll für Plattformbetreiber aber auch nicht möglich sein, zu wissen, dass dieselbe Nutzer:in sich gestern und heute als volljährig ausgewiesen hat. Und für alle Nutzungen der EUDI-Wallet soll es der ausstellenden Stelle (i.d.R. dem Staat) nicht möglich sein, nachzuvollziehen, wann, wie oft und in welchem Kontext die EUDI-Wallet genutzt wird (unobservability).

… Unlinkability, …

… Untraceability …

… und Unobservability

Open Source

Fünftens müssen alle EUDI-Wallets – zumindest jener Teil, der auf einem Smartphone oder anderem Endgerät der Nutzer:innen installiert wird – vollständig Open Source sein, d.h. der Quelltext muss offen einsehbar sein. Damit kann er auch von unabhängigen Akteuren (z. B. aus der Wissenschaft und Zivilgesellschaft) überprüft werden.

Datensparsame Lösung

Für Alterskontrollen im Internet verspricht die EUDI-Wallet damit eine datensparsame und nutzer:innenfreundliche Lösung. Das Deutsche Bundesinnenministerium etwa entwickelt eine Implementierung, bei der Attributsbescheinigungen für 12, 14, 16, 18, 21 und 65 Jahre oder (jeweils) älter geplant sind (Kunz & Waldmann, 2025). Damit würde sich folglich eine abgestufte Altersabfrage umsetzen lassen.

Konkrete Umsetzung entscheidet, ob hohe Standards eingehalten werden

Trotz der robusten Verordnung gibt es einige Kritikpunkte und offene Fragen, die sich erst im Laufe der Umsetzung endgültig klären lassen werden. Erstens enthält die Verordnung selbst keine Details zur technischen Umsetzung. Diese ist im Architektur- und Referenzrahmenwerk (Architecture and Reference Framework, ARF) spezifiziert.[53] Hier wurde von Expert:innen aus Wissenschaft und Zivilgesellschaft kritisiert, dass die oben genannten strengen Privatsphäre-Vorgaben des ARF nicht umgesetzt werden. Anders gesagt: Die geplante technische Umsetzung würde de facto der Verordnung widersprechen – obwohl es etablierte technische Möglichkeiten gäbe, das korrekt umzusetzen (Baum et al., 2024; Eichacker et al., 2024).

Verknüpfen mit Plattform-Konten nur durch Einwilligung erlaubt

Zweitens ist es zwar prinzipiell verboten, die Daten in der EUDI-Wallet mit Plattform-Konten zu verknüpfen. Allerdings besteht die Möglichkeit, dieses Verbot auf expliziten Wunsch der Nutzer:in zu umgehen. Hier besteht also das Risiko, dass durch Interaktionsmuster (Nudging) Nutzer:innen ohne Notwendigkeit diese explizite Zustimmung erteilen (Eichacker et al., 2024).

---

[53] *eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.4.0/arf/.*

Umsetzung mit Smartphone problematisch …

Drittens ist die Umsetzung aktuell auf Smartphones geplant (Eichacker et al., 2024). Das heißt, ein Smartphone würde zur Notwendigkeit, um Attribute wie das Alter zu teilen. In Bezug auf Kinder und Jugendliche stellt sich damit die Frage, ob dadurch der Druck weiter steigt, ein persönliches Smartphone zu besitzen, um sich gerade für kinder- und jugendgerechte Angebote (z. B. ab 12 oder 14 Jahren) auszuweisen. Das ist einerseits aus sozio-ökonomischer Perspektive (Leistbarkeit) zu hinterfragen, andererseits werden Smartphones selbst, wie in der Einleitung ausgeführt, zunehmend als für Kinder und Jugendliche problematisch angesehen.

… Smartphone-freies Leben zunehmend schwierig

Auch für Erwachsene ist die zunehmende Notwendigkeit, ein Smartphone zu besitzen und bei sich zu haben, problematisch. Denn je mehr sensible Aktivitäten über Smartphones durchgeführt werden (müssen), desto wichtiger ist, dass diese gut abgesichert sind (Eichacker et al., 2024). Das ist vor dem Hintergrund, dass nach wie vor viele Geräte (und hier vor allem leistbare) nur für kurze Zeit Sicherheitsupdates erhalten, ein Problem. Weiters ist auch fehlende Kompetenz im Umgang mit Sicherheitseinstellungen und die Gefahr, wichtige Tätigkeiten nicht verrichten zu können, sollte das Smartphone einen leeren Akku haben, defekt sein oder verloren bzw. gestohlen sein, als heikel anzusehen.[54] Schließlich erschwert die ständige Notwendigkeit des Zurückgreifens auf ein Smartphone Versuche, dieses beispielsweise für längere Zeitperioden wegzulegen, um so einen gesunden Umgang damit zu pflegen.

3.2.5.4 EUROPÄISCHE ALTERSFESTSTELLUNGS-APP

Übergangslösung bis zur EUDI-Wallet

Weil die EUDI-Wallet erst ab Ende 2026 flächendeckend eingeführt werden wird, arbeitet die Europäische Kommission derzeit an einer Übergangslösung: Eine eigene Alterskontroll-App wird derzeit entwickelt.[55] Ein erster Prototyp wurde im Juli 2025 quelloffen verfügbar gemacht.[56]

Erlaubt das Ausweisen als volljährig

In einem ersten Schritt soll die App es erlauben, dass Nutzer:innen sich als volljährig ausweisen, um etwa pornografische Inhalte abzurufen oder online Alkohol kaufen zu können. Da es sich nur um einen Prototyp handelt, können EU-Mitgliedsstaaten aber auch entscheiden, ein anderes Alterslimit zu konfigurieren.

Technologie ähnelt der geplanten EUDI-Wallet

Die technologische Basis gleicht dabei der geplanten EUDI-Wallet (s.o.). Nutzer:innen können auf zwei Wegen ihre Identität in der App speichern: erstens über eine nationale eID – in Österreich wäre das die ID Austria – zweitens über das Ablesen der Daten von einem Pass oder Personalausweis. Bei Pässen wird zuerst ein Foto des Passes gemacht, anschließend werden die biometrischen Daten per Near Field Communication (NFC) des Smartphones ausgelesen und mit einem Selfie-Video abgeglichen. Obwohl in beiden Prozessen viele Daten ausgelesen werden, soll in der Altersverifikations-App nur die Information, über einer Altersschwelle zu sein, gespeichert werden.

Da die technischen Grundlagen der EUDI-Wallet gleichen, ist die Altersverifikations-App mit der EUDI-Wallet kompatibel und wird wohl schlussendlich in dieser aufgehen. Daher wird sie auch mini-Wallet genannt.

---

54 Zur zunehmenden Schwierigkeit, ein Leben ohne Smartphone zu leben siehe z. B. auch *help.orf.at/stories/3232635/.*

55 *digital-strategy.ec.europa.eu/en/policies/eu-age-verification; digital-strategy.ec.europa.eu/en/factpages/blueprint-age-verification-solution-help-protect-minors-online.*

56 *ageverification.dev/Setup/*.

3.3 VERFAHRENSUNABHÄNGIGE UMGEHUNGSMÖGLICHKEITEN

Während es je nach Verfahren zur Altersabschätzung und -verifizierung spezielle Möglichkeiten zur Umgehung gibt, gibt es auch verfahrensunabhängige Möglichkeiten, diese zu umgehen.

Umgehungsmöglichkeit per VPN

In Fällen, in denen Online-Dienste und Apps regional ausdifferenzierte Zugänge zur Altersbeschränkung umsetzen, ist die Netzwerkebene eine der wichtigsten Möglichkeiten, um diese zu umgehen. Führt ein Dienst zum Beispiel nur in der EU eine Altersfeststellung durch, tut dies aber in anderen Regionen nicht (oder mit anderen Grenzwerten), dann ist die Umgehung per Virtuellem Privaten Netzwerk (VPN) eine einfache Möglichkeit, die Beschränkung auszuhebeln: Mittels VPNs ist es möglich, den Internetverkehr über andere Länder umzuleiten.[57]

Beschränkung von VPNs als Folge?

Die wichtige Rolle von VPNs im Zuge von Online-Altersbeschränkungen verdeutlicht die Situation in Großbritannien: Als im Juli 2025 im Zuge des Online Safety Acts viele Plattformen Altersverifikation einführten (darunter sowohl pornografische Webseiten wie auch soziale Medien), stieg die Nachfrage nach VPN-Apps sprunghaft an: Unter den Top-10-Apps in Apples iOS App Store befanden sich fünf VPN-Apps.[58] Dabei ist wichtig festzuhalten, dass die Nachfrage vermutlich großteils nicht von Kindern und Jugendlichen ausgeht, sondern wahrscheinlich auch zu einem signifikanten Teil von Volljährigen, die nicht bereit sind, sich mit biometrischen Methoden auszuweisen oder Finanzinformationen zur Verifizierung zu teilen.[59] In Folge dieser Entwicklung wird in Großbritannien aktuell diskutiert, den Zugang zu VPNs ebenfalls zu beschränken (Children's Commissioner, 2025).

Weitergabe gefährlicher Inhalte über Messenger, Bluetooth & Co.

Eine weitere allgemeine Umgehungsmöglichkeit stellt die Weitergabe von Inhalten zwischen Einzelpersonen oder in Gruppen dar. Solange Kinder und Jugendliche Zugang zu Messengerdiensten haben, können sie auch über diese Inhalte erlangen, auf die sie direkt über Soziale Netzwerke keinen Zugriff hätten. Aber auch die direkte Weitergabe in räumlicher Nähe über Bluetooth, Speicherkarten und -Sticks oder AirDrop sind Möglichkeiten, wie Material weitergegeben kann und wird.

Umgehung mit Hilfe Volljähriger

Schließlich gibt es auch bei allen Methoden die Möglichkeit, diese durch ältere Freunde, Geschwister, Bekannte und auch Eltern durchführen zu lassen und somit auszuhebeln. Eine Ausnahme könnte die Altersfestlegung durch Bezugspersonen sein – hier könnte nur mit Administratorrechten oder mit besonderen Kompetenzen ein neues Konto angelegt werden bei dem ein höheres als das tatsächliche Alter eingetragen würde. Bei allen Methoden gibt es die Möglichkeit, über Geräte anderer (älterer) Personen, eigentlich für jüngere beschränkte Inhalte abzurufen. In diesen Situationen besteht die Gefahr, neue Abhängigkeiten zu schaffen (mehr dazu in Abschnitt 5.3).

---

[57] Andere Nutzen für VPNs sind insbesondere, in unsicheren Netzwerken den eigenen Internetverkehr zu sichern, die Verbindung zu Unternehmens- oder Universitätsnetzwerken herzustellen oder lokale Zensur zu umgehen (z.B. durch Dissident:innen).

[58] *bbc.com/news/articles/cn72ydj70g5o*.

[59] *theverge.com/tech/827435/uk-vpn-restrictions-ban-online-safety-act.*

4 DATENSCHUTZ

Unterschiede zwischen Methoden bezüglich des Datenschutzes

Verfahren zur Altersfeststellung und -schätzung sind zum überwiegenden Teil sehr datenintensiv: Häufig werden umfangreiche persönliche Daten geteilt, teils biometrischer Natur. Dennoch gibt es Unterschiede zwischen den im vorigen Kapitel vorgestellten Ansätzen in Hinblick auf Datenschutz, aber auch in ihrer Eignung zur Überwachung und Zensur.

Tabelle 2 bietet einen Überblick darüber, wie einzelne Methoden grob einzuschätzen sind – in Hinblick auf Effektivität (Genauigkeit, Einfachheit der Umgehung und Aufwand zur Verifizierung bzw. Schätzung für Nutzer:innen) und Datenschutz (Datensparsamkeit, Überwachungspotential und Sensitivität der Daten).

Tabelle 2: Überblick über Methoden zur Altersfeststellung, deren Effektivität und Datenschutz-Aspekte

Methode	Effektivität			Datenschutz		
	GENAUIG-KEIT	UMGEHUNG	AUFWAND	DATEN-SPARSAMKEIT	ÜBERWACHUNGS-POTENTIAL	SENSITIVITÄT DER DATEN
Selbstauskunft	niedrig	einfach	minimal	gut	minimal bis mittel	minimal
Altersfestlegung durch Bezugspersonen	hoch	mittel	minimal	gut	minimal	minimal
Gesichtsanalyse	mittel	mittel	mittel	schlecht	hoch	hoch
Lichtbildausweis	hoch	einfach	mittel	schlecht	sehr hoch	hoch
Lichtbildausweis mit Gesichtsvergleich	hoch	schwer	hoch	sehr schlecht	sehr hoch	sehr hoch
Verhaltensanalyse	niedrig	mittel	minimal	schlecht	hoch	mittel bis hoch
Kreditkarte	hoch	mittel	mittel	schlecht	hoch	hoch
ID Austria	hoch	schwer	mittel	schlecht	sehr hoch	sehr hoch
EUDI-Wallet	hoch	schwer	mittel	gut	minimal	minimal
EU-Alters-feststellungs-App	hoch	schwer	mittel	gut	minimal	minimal

4.1 DATENSCHUTZ UND -SICHERHEIT

Viele Methoden verletzen Prinzip der Datenminimierung

Ein Hauptproblem vieler Ansätze der Altersüberprüfung ist die Verletzung des Grundsatzes der Datensparsamkeit bzw. -minimierung. Der eigentliche Zweck ist schließlich nur, festzustellen, ob das Alter der Nutzer:innen unter oder über einer bestimmten Schwelle ist. Daher wird bereits bei Übermittlung des exakten Geburtsdatums oder sogar des Geburtsjahres mehr Information entgegengenommen, als strikt notwendig wäre. Tabelle 3 gibt einen Überblick, welche Daten über den eigentlichen Zweck hinaus weitergegeben werden müssen. Wie daraus erkenntlich wird, gibt es viele (besonders derzeit gängige) Methoden, die viele sensible Informationen verarbeiten, wohingegen datensparsame Methoden erst in Entwicklung sind.

Hochsensible Daten betroffen

Die Weitergabe derart sensibler Informationen ist mit hohem Risiko behaftet: Gesichtsaufnahmen können in Zeiten von Deep Fakes (d.h. per KI generierte Darstellungen von realen Personen) in den falschen Händen für weitreichenden Schäden führen (Mobbing, Erpressung, Herstellung nicht-konsensualer sexueller Inhalte usw.). Darüber hinaus könnten Plattformanbieter in Versuchung geraten, die Daten für das Training von KI zu nutzen, da dafür große Datenbestände benötigt werden, oder aus diesen herausgelesene Nutzer:inneneigenschaften in ihre (u.U. an Dritte weitergegebenen) Analysen des Nutzer:innenverhaltens miteinzuschließen. Auch die Wiedererkennung von Personen auf anderen Fotos und Videos wäre Plattformen mit diesen Daten prinzipiell möglich (und wohl mitbeabsichtigt).

Identitätsdiebstahl kann drohen

Fotos von Lichtbildausweisen und die darin enthalten Informationen sind in höchstem Maß geeignet für Identitätsdiebstahl und allen damit verbundenen finanziellen, rechtlichen und emotionalen Konsequenzen[60]. Wird kein Abgleich mit einem Live-Video oder Selfie (siehe Abschnitt 3.2.3.2) durchgeführt, kann außerdem nicht nachgewiesen werden, dass die Ausweisinhaber:in eingewilligt hat und tatsächlich anwesend ist (Kunz & Waldmann, 2025).

Tabelle 3: Überblick über Daten, die bei verschiedenen Methoden verarbeitet werden

Methode	Weitergegebene Daten
Selbstauskunft	Über X Jahre. Eventuell zusätzliche Daten bei der verlangten Einrichtung eines Kontos
Altersfestlegung durch Bezugspersonen	Über X Jahre oder X Jahre, sonst keine
Schätzung des Alters durch Gesichtsanalyse	Aussehen, eventuell Hintergrund
Abgleich von Gesicht und Lichtbildausweis	Aussehen, sämtliche auf dem Lichtbildausweis vermerkte Daten (je nach Ausweis sind das Ausweisnummer, Geburtsdatum, Name, Nationalität, Körpergröße, Adresse, Ausstellungsort und -datum etc.)
Verhaltensanalyse	Surfverhalten, inhaltliche Präferenzen (mit Möglichkeit, sexuelle Orientierung, politische Präferenzen, gesundheitliche Situation usw. einzuschätzen)
Kreditkarte	Kreditkarten-Informationen, Name, Ausstellungsland (bei manchen Anbietern)
ID Austria	Eindeutige Identität (i.d.R. Name, Geburtsdatum, möglicherweise auch Lichtbild, Meldedaten etc.)
EUDI-Wallet	Über X Jahre, sonst keine[61]
EU-Altersfeststellungs-App	Über X Jahre, sonst keine

[60] Siehe hierzu auch die Studie „Identitätsdiebstahl. Die Folgen für Betroffene und wie ihnen geholfen werden kann“ im Auftrag der Arbeiterkammer: *arbeiterkammer.at/beratung/konsument/Datenschutz/Identitaetsdiebstahl.pdf*

[61] Hier gehen wir davon aus, dass die EUDI-Wallet tatsächlich so umgesetzt wird, dass sie möglichst datensparsam ist und Dienste-Anbieter keine überschießenden Daten abfragen dürfen. Siehe dazu Abschnitt 3.2.5.3 für Details.

Daten als attraktives Ziel für Kriminelle

Verbraucher:innen sind dazu genötigt, den Plattform-Betreibern zu vertrauen, dass diese ihre Daten nicht speichern. Selbst wenn die Daten gut abgesichert sind, kann eine hundertprozentige Sicherheit nie gewährleistet werden. Dazu kommt, dass Sammlungen von Tausenden bis zu Millionen Ausweisdaten oder Gesichtsaufnahmen ein besonders attraktives Ziel für Kriminelle darstellen (Goldman, 2025). Meta etwa gibt an, dass Aufnahmen zur Altersschätzung für Instagram nach der Schätzung gelöscht würden.[62] Allerdings gibt es keine effektive Möglichkeit, die Löschung zu überprüfen. Das aktuelle Beispiel der Plattform Discord (siehe Box unten) zeigt, dass die Möglichkeit der Kompromittierung mitgedacht werden muss und Bedenken des Datenschutzes nicht rein theoretischer Natur sind.

Löschung nach Altersüberprüfung nicht überprüfbar

Box 3: Datenleck bei Discord

Die Brisanz der Datensicherheit hat ein Vorfall der besonders unter Gamer:innen (darunter mutmaßlich viele Kinder und Jugendliche) beliebten Plattform Discord im Oktober 2025 verdeutlicht: Ein externer Dienstleister wurde zur Verifizierung des Alters von Nutzer:innen betraut. Dieser wurde kompromittiert und infolge dessen sind Lichtbildausweise von 70.000 Nutzer:innen abgeflossen.[63]

Tracking von Nutzer:innen erlaubt tiefe Einblicke

Verfahren der Verhaltensanalyse benötigen als Grundlage das Anlegen von Nutzer:innenprofilen und das Tracken ihres Verhaltens. Diese Daten sind nicht so offensichtlich bedenklich wie das Verarbeiten von Lichtbildausweisen und Gesichtsfotos, erlauben aber auch Rückschlüsse auf z.B. sexuelle Orientierung, soziale Kontakte, politische Einstellung usw., da die Interaktion mit Inhalten und anderen Personen auf einer Plattform und teilweise auch über Plattformen hinweg gespeichert wird. Über den Umweg der Altersschätzung mit dieser Methode könnte einer problematischen Praxis, welche häufig für gezielte Werbung (Targeting) eingesetzt wird, neue Legitimation verleihen.

Missbrauch von Kreditkartendaten

Kreditkartendaten wiederum sind insofern sensibel, als sie in den falschen Händen zu ökonomischem Schaden führen können; im schlimmsten Fall können die Karteninhaber:innen sogar in rechtliche Schwierigkeiten kommen, wenn ihre Daten für illegale Tätigkeiten missbraucht werden. Die Feststellung der Einwilligung der Karteninhaber:in zur Nutzung der Daten ist in diesem Fall an das Kreditkarteninstitut ausgelagert – und je nach deren Umsetzung (etwa durch Zwei-Faktor-Authentifizierung) mehr oder weniger robust oder offen für Missbrauch (etwa durch die eigenen Kinder ohne Wissen der Eltern).

ID Austria übermittelt zu viele sensible Daten

Bei einer Authentifizierung über ID Austria besteht ebenfalls die Möglichkeit, hochsensible Daten zu teilen – vom Foto eines aktuellen Lichtbildausweises, über Meldedaten und natürlich Name und Geburtsdatum. Gegenüber Sozialen Medien etwa muss man diese Daten bisher nicht teilen. Eine Umsetzung mit ID Austria käme quasi einer Klarnamenpflicht gleich – zumindest die Plattformbetreiber

---

62 *about.instagram.com/de-de/blog/announcements/new-ways-to-verify-age-on-instagram.*

63 *discord.com/press-releases/update-on-security-incident-involving-third-party-customer-service.*

wüssten dann genau, welche Identität hinter User:innenkonten (die oft mit Pseudonymen geführt werden) steckt.

EUDI-Wallet und Altersfeststellungs-App sehr sparsam

Sowohl die EUDI-Wallet als auch die EU-Altersfeststellungs-App, sofern sie korrekt umgesetzt sind, folgen hingegen dem Prinzip der Datenminimierung: Beide Lösungen erlauben es, nur die Information über einem Schwellenalter (14, 16 etc.) zu sein, zu teilen. Weder Name noch Geburtsdatum noch weitere Informationen werden weitergegeben. Aus Datenschutzsicht sind diese Lösungen folglich ein großer Fortschritt. Ebenso verhält es sich bei der Festlegung des Alters auf Geräteebene.

4.2 ÜBERWACHUNG UND ZENSUR

Eindeutige Identifizierung erleichtert Überwachung

Altersfeststellungsmethoden ermöglichen die Überwachung von Nutzer:innen, wenn sie eine eindeutige Identifizierung erlauben – sei es per Name, per Foto oder über eindeutige Attribute, die über einen längeren Zeitraum hinweg und möglicherweise auch über Plattformen hinweg gleich bleiben. Grundsätzlich muss man dabei zwischen kommerzieller (Nutzer:innenverhalten) und staatlicher Überwachung unterscheiden. Über Anfragen von Strafverfolgungsbehörden kann es aber zu einer Vermischung kommen.

Dienstleister als Überwachungs-knotenpunkt

Die Verknüpfung von eindeutiger Identifikation (sei es über Lichtbildausweis oder ID Austria) mit anderen Daten ermöglicht es Plattformen, besonders aussagekräftige Profile anzulegen. Dienstleister, die Altersfeststellung für mehrere Plattformen durchführen, können darüber hinaus zu regelrechten Überwachungs-Knotenpunkten werden: Sie wissen, welche Personen sich gegenüber welchen Plattformen ausweisen.

Nutzung der ID Austria nachvollziehbar

Das trifft auch auf die Nutzung der ID Austria zu: Jede Nutzung der ID Austria wird protokolliert, weshalb es im Fall der Fälle möglich wäre, nachzuvollziehen, wo sich Individuen im Internet bewegen und welche Dienste sie wann in Anspruch nehmen. Hier würden somit sowohl für den Staat umfangreiche Daten anfallen, als auch sensible Daten mit den Plattformen geteilt werden.

Robuste Umsetzung kann Überwachung bei EUDI-Wallet verhindern

Bei der EUDI-Wallet ist aktuell noch unklar, ob sie so robust umgesetzt wird, dass eine Überwachung (in dem Sinne, dass mehrere Authentifizierungen derselben Person verknüpft werden können) ausgeschlossen ist (Details dazu in Abschnitt 3.2.5.3).

Möglichkeit zur Zensur über Kinder- und Jugendschutz

Altersfeststellungen können unter gewissen Bedingungen auch als Instrument der Zensur dienen: Einerseits können über die Steuerung, was für Minderjährige als unpassend gilt, gewisse Inhalte schwerer zugänglich gemacht werden. Als Beispiel sei hier etwa die Frage genannt, welche Informationen zu Verhütung und Sexualität als altersgerecht eingeschätzt werden. Ein Blick nach Russland, in die USA und auch nach Ungarn zeigt, dass hier keineswegs breiter Konsens angenommen werden kann.

5 AUSWIRKUNGEN AUF KONSUMENT:INNEN UND GESELLSCHAFT

Weitreichende Auswirkungen …

… auch wenn nicht flächendeckend umgesetzt

Altersbeschränkungen und die dafür notwendige Altersschätzung oder -verifizierung haben eine Reihe möglicher Auswirkungen, die über das eigentliche Ziel hinausgehen. Das gilt sowohl für den Fall, dass eine flächendeckende Altersbeschränkung erfolgreich und effektiv umgesetzt werden kann, als auch für den Fall, dass dies nur lückenhaft möglich ist. Dabei kann zwischen Folgen für Einzelpersonen und jenen auf gesellschaftlicher Ebene unterschieden werden. Schließlich nimmt dieses Kapitel dezidiert mögliche Folgen für Kinder und Jugendliche in den Blick: Immerhin ist deren Schutz die Motivation, überhaupt Altersbeschränkungen einzuführen.

5.1 INDIVIDUELLE FOLGEN

Auf individueller Ebene entstehen durch Altersbeschränkungen verschiedene Risiken. Neben den bereits in Kapitel 4 ausgeführten Datenschutzrisiken, die direkt mit manchen der Verfahren einhergehen, gibt es auch nachgelagerte Risiken.

Ausschluss einzelner, falls Altersfeststellung scheitert

In einem Internet mit flächendeckender Altersbeschränkung kann ein Ausschluss Einzelner aus Bereichen des Internets erfolgen, wenn sie – aus welchem Grund auch immer – nicht die Möglichkeit haben, sich entsprechend zu authentifizieren, die Risiken, welche mit der jeweiligen Feststellungsmethode nicht eingehen wollen, oder die Altersschätzung scheitert: Das kann zum Beispiel das Fehlen einer (funktionierenden) Webcam sein, um Selfies oder Live-Videos aufzunehmen. Es kann aber auch eine Vielzahl an Gründen geben, weshalb Personen weder Kreditkarte noch Lichtbildausweis zur Verfügung haben. Besonders Kreditkarten stehen ökonomisch Benachteiligten nicht immer zur Verfügung (Sperre aufgrund von Zahlungsverzug, Kreditkartengebühren etc.). Auch Passgebühren können für manche Menschen eine Hürde darstellen. Schließlich können derlei Dokumente gestohlen, verloren oder anderweitig (vorübergehend) nicht zugänglich sein. Es ist auch fraglich, wie der Zugang zu wichtigen Informationen für Menschen, die sich nur vorübergehend oder erst kurze Zeit im Land aufhalten, gewährleistet werden kann, wenn diese nicht für die im jeweiligen Land für bestimmte Angebote geltende Feststellungsmethoden eingerichtet sind.

Teilen hochsensibler Daten wird Routine

Ein weiterer Effekt jener Methoden, die auf Selfies, Videoaufnahmen, Kreditkarten oder Lichtbildausweisen basieren, ist, dass Konsument:innen damit daran gewöhnt werden, hochsensible Daten mit einer Vielzahl von Plattformen zu teilen, deren Zweck primär keine dieser Daten erfordert. Die Gefahr dabei ist, dass ein solcher Gewöhnungseffekt dazu führen kann, diese Daten auch leichtfertiger mit Kriminellen zu teilen. So erscheint es plausibel, dass Kriminelle Webseiten und Plattformen, welche persönliche Daten und Kreditkarteninformationen

sammeln (z. B. Fakeshops, oder Imitationen von Behördenseiten)[64] aufbauen, um unter dem Vorwand der Altersfeststellung weitere Daten wie Lichtbildausweise und Aufnahmen von Personen sammeln. Es kommt somit zu einer enormen Verantwortung seitens der Verbraucher:innen, die einschätzen müssen, ob ein Dienst vertrauenswürdig ist oder nicht.

Diskriminierung bei biometrischen Methoden

Biometrische Methoden sind, wie in Abschnitt 3.2.3 ausgeführt, von Verzerrungen (sog. „Biases“) gekennzeichnet. Das heißt insbesondere, dass gewisse Personengruppen bei diesen Ansätzen von manchen Diensten ausgeschlossen werden können, sei es, weil die Altersschätzung bei ihnen fehleranfälliger ist (sie z.B. jünger schätzt) oder gänzlich versagt (z.B. infolge von Verletzungen).

Alternativen zu Android und iOS geschwächt

Ansätze, die ein Smartphone mit einer speziellen App voraussetzen, sind teilweise deutlich datenschutzfreundlicher. Allerdings deutet derzeit alles darauf hin, dass ein Smartphone mit Google Play Store oder Apple App Store Voraussetzung ist, um die EU-Altersfeststellungs-App nutzen zu können:[65] Für Verbraucher:innen bedeutet dies, dass Smartphones mit alternativen Betriebssystemen oder App Stores für diesen Zweck nicht brauchbar sein könnten. Insbesondere Huawei-Smartphones bieten keinen Zugriff auf den Google Play Store, sind aber teilweise relativ günstig erhältlich. Überhaupt ist die Voraussetzung, ein Smartphone zu nutzen, problematisch, da es den Entscheidungsspielraum, ein Smartphone-freies Leben zu führen, einschränkt.

Offener Standard für Altersfestlegung begrüßenswert

Im Falle der Altersfestlegung am Endgerät durch Bezugspersonen ist die Mitwirkung der Betriebssystem- bzw. Gerätehersteller essentiell. Sollte dafür ein offener Standard entwickelt werden, wäre es zumindest möglich, diesen Ansatz auch auf alternativen Betriebssystemen jenseits von Apple, Android und Windows umzusetzen.

Einschränkung, welche Daten von EUDI-Wallet abgefragt werden können

Im Falle der EUDI-Wallet stellt sich vor allem die Frage, wie sichergestellt wird, dass Daten nur im minimal notwendigen Umfang geteilt werden: Wenn Anbieter selbst entscheiden können, welche Daten sie abfragen, kann das Prinzip der Datenminimierung schnell unterlaufen werden, indem etwa das Geburtsdatum abgefragt wird, obwohl etwa nur ein Beleg, über 16 Jahre alt zu sein, ausreichend wäre. Hier wird somit viel von der konkreten Umsetzung abhängen, insbesondere, ob es ein behördliches Register geben wird, das ganz klar festhält, wozu einzelne Anbieter berechtigt sind.

Wie oft muss Altersfeststellung durchlaufen werden?

Die genannten Risiken sind besonders gravierend, wenn die Altersfeststellung nicht nur bei der Erstellung eines Nutzer:innenkontos notwendig ist, sondern häufiger. Sollte sie nur beim Erstellen des Kontos durchgeführt werden, müssen die notwendigen Verfahren immerhin nicht ständig durchlaufen werden und Dokumente nicht ständig in Griffweite sein. Gleichzeitig bedeutet das, dass man zunehmend dazu verleitet wird, auf Plattformen Konten anzulegen, wo man es ohne die Altersbeschränkung nicht getan hätte. Somit wären Nutzer:innen dem Tracking auf diesen Plattformen stärker ausgesetzt als bisher.

---

64 Z.B. *watchlist-internet.at/unserioese-webseiten/.*

65 *netzpolitik.org/2025/prototyp-vorgestellt-eu-will-alterskontroll-app-an-google-binden/.*

5.2 GESELLSCHAFTLICHE AUSWIRKUNGEN

Woher kommen Daten für Altersschätzungen?

Viele der Folgen auf individueller Ebene haben auch gesamtgesellschaftliche Auswirkungen. Bei biometrischen Methoden bedarf es etwa einer Datensammlung an Fotos und Videos von Menschen, um die dahinterliegenden Machine-Learning-Modelle zu trainieren. Hier stellt sich die Frage, auf welchem Wege diese Sammlungen zustande kommen – und ob man als Gesellschaft derartige Sammlungen begünstigen oder doch eher hintanhalten möchte.

Struktur des Internets könnte sich umfassend ändern

Neue Digital Divide

Sollten Altersbeschränkungen auch jenseits der großen Plattformen umgesetzt werden, droht sich das Internet als solches deutlich zu verändern. Bereits heute droht das „freie Internet" immer kleiner zu werden: Zunehmend sind Inhalte nur noch nach Logins auf Online-Plattformen oder hinter Bezahlschranken zugänglich. Besonders Letzteres droht zu einer neuen Digital Divide, also einer digitalen Spaltung der Bevölkerung, zu führen, da viele Inhalte finanzschwachen Haushalten verborgen bleiben. Müssten auch kleinere Plattformen je nach Inhalt den Zugang beschränken, könnten diese Tendenzen verstärkt werden: Altersverifizierungen können mit Kosten für Betreiber:innen verbunden sein, und für Nutzer:innen könnte es bequemer sein, Plattformen zu besuchen, bei welchen man das Alter bereits verifiziert hat. Beides würde die Eintrittshemmnisse für neu in den Markt eintretende Firmen verstärken. Dies verringert den Wettbewerb, mit den negativen Folgen hoher Marktkonzentration für Konsument:innen. Im Allgemeinen drohen häufige Altersbeschränkungen, welche die anonyme Nutzung des Internets zu erschweren.

Marktmacht von Google und Apple verstärkt

Die zentrale und damit limitierende Rolle, die Smartphones in manchen Ansätzen zukommt, ist ebenso bedenklich, insbesondere da der Markt für Smartphone-Betriebssysteme de-facto ein Duopol ist: Jenseits von Apple iOS und Google Android gibt es in der EU keine ernsthafte Alternative mit nennenswerter Marktdurchdringung. Sind Smartphone-Lösungen so gestaltet, dass entweder ein Apple-Gerät oder ein Gerät mit Android notwendig ist (s.o.), dann trägt dies zur weiteren Festigung der Marktmacht dieser Anbieter bei.

5.3 FOLGEN FÜR KINDER UND JUGENDLICHE

Verantwortung von Plattformen zu Nutzer:innen verschoben

Für Kinder und Jugendliche, deren Schutz das Ziel von Altersbeschränkungen ja ist, ergeben sich einige spezifische Folgen. Im Allgemeinen ist festzuhalten, dass die aktuelle Debatte den Fokus von der Verantwortlichkeit der Plattformen für deren kindgerechte Ausgestaltung hin zu Kindern, Jugendlichen und deren Eltern verschiebt, die nun die Hauptlast tragen, in einem nicht kindgerechten Internet sicher unterwegs zu sein (Livingstone et al., 2024).

Kinder und Jugendliche oft erste Nutzer:innen neuer Plattformen

Kinder und Jugendliche gelten als Early Adopters, d.h. sie sind oft unter den Ersten, die neue Plattformen ausprobieren und nutzen (Livingstone, 2025). Gerade neue Plattformen haben mit höherer Wahrscheinlichkeit keine geeigneten Vorkehrungen, um schädliche Inhalte effektiv zu moderieren, und/oder sie haben noch keine Altersbeschränkung umgesetzt. Gleichzeitig ist anzunehmen, dass Regulierungsbehörden relativ langsam reagieren würden, um etwaige Gesetze des Kinder- und Jugendschutzes effektiv durchzusetzen. In Großbritannien gelten beispielsweise für kleine Plattformen weniger strikte Regelungen, was angesichts des Nutzungsverhaltens von Kindern und Jugendlichen fragwürdig ist

Droht zu langsame Reaktion der Behörden?

(Livingstone, 2025) und eventuell sogar zu Klagen auf Basis internationalen Rechts bezüglich Benachteiligung konkurrierender Plattformen führen könnte.[66]

Mangelhafte Rechtsdurchsetzung im digitalen Raum

Da bereits derzeit im digitalen Raum die Rechtsdurchsetzung mangelhaft ist, kann davon ausgegangen werden, dass eine flächendeckende Umsetzung von Altersbeschränkungen nicht durchsetzbar sein wird. Was droht, ist eine Verdrängung von Kindern und Jugendlichen auf völlig unregulierte Plattformen, insbesondere wenn sie auf der Suche nach riskanten Inhalten sind. Auf diesen sind sie verstärkt Gefahren ausgesetzt wie gewaltvollen Inhalten, Grooming und Radikalisierung (Goldman, 2025).

Alter hat mangelhafte Aussagekraft über Entwicklungsstand von Kindern & Jugendlichen

Ein grundsätzliches Problem von Altersbeschränkungen besteht darin, dass Kinder und Jugendliche sich in ihrer Entwicklungsgeschwindigkeit unterscheiden. Das bedeutet in weiterer Folge, dass eine Altersgrenze für manche gerade zu ihrem Entwicklungsstand (z.B. in Bezug auf psychische, soziale und emotionale Kompetenz) passt. Für andere könnten die Regelungen aber zu restriktiv sein (d.h. ihnen ist der Zugang zu Informationen, die ihren Fähigkeiten angemessen sind, verwehrt) oder zu freizügig sein (d.h. sie sind noch nicht fähig, mit gewissen ihnen bereits zugängigen Inhalten adäquat umzugehen). Eindeutige Altersgrenzen stellen somit zwar klare Lösungen dar, führen aber auch zu Asymmetrien und Ungerechtigkeiten (Livingstone & Sylwander, 2025).

Positive Aspekte des Digitalen nicht übersehen

Smartphones, Soziale Medien und andere digitale Angebote stellen aber nicht nur eine Gefahr für Kinder und Jugendliche dar, im Gegenteil: Sie können wichtige Informationsangebote (auch für die Bildung) sein, bieten Gelegenheiten, sich mit anderen zu vernetzen, sich auszudrücken, eine Identität auszubilden, sich gesellschaftlich zu engagieren und vieles mehr (Goldman, 2025; Livingstone et al., 2025). Gerade vulnerable Kinder und Jugendliche finden online oft wichtige Ressourcen und Gemeinschaft.

Stärkere Abhängigkeit von Erwachsenen möglich

Besteht – aus welchem Grund auch immer – der Bedarf nach Zugang zu beschränkten Angeboten, so können Kinder und Jugendliche in stärkere Abhängigkeit von Erwachsenen geraten: Dies können die eigenen Eltern sein, die ihnen dann Zugang zu gewissen Diensten und Inhalten ermöglichen (oder auch verbieten), es könnten aber auch andere Volljährige sein – und somit ein Einfallstor für Manipulation, Machtmissbrauch und Grooming.

Digitale Kompetenz von Kindern und Erziehungsberechtigten unzureichend

Eine rezente Studie führte Fokusgruppen mit Kindern und Befragungen von Eltern in 15 EU-Ländern (Österreich war nicht darunter) und mehreren südamerikanischen und asiatischen Ländern durch (ECPAT International Project et al., 2024). Es zeigte sich eine große Diskrepanz zwischen dem Grad, in welchem Erziehungsberechtigte das Onlineverhalten ihrer Kinder zu kennen glaubten und dem Grad, in dem sie es der Erfahrung ihrer Kinder nach kannten. Außerdem scheinen Jugendliche ihre Fähigkeiten im Umgang mit Onlinerisiken zu überschätzten, während sie sowohl in der Schule als auch von Erziehungsberechtigten kompetenten und differenzierten Rat dazu vermissten. Erziehungsberechtigte selbst gaben vor allem abstrakte und verallgemeinernde Warnhinweise.

Wahlrecht ab 16 vs. Bevormundung online

Abschließend sei auch darauf hingewiesen, dass Jugendliche in Österreich bereits mit 16 Jahren das aktive Wahlrecht haben. Sollte der Zugang zu Informationen oder ganzen Plattformen (wie Sozialen Medien) vor dem 16. Lebensjahr beschränkt sein, haben diese Jugendlichen weniger Möglichkeiten, sich online

---

[66] Im Rahmen sog. Investor-State Dispute Settlements wurden bereits EU-Staaten geklagt, vgl. ***europarl.europa.eu/RegData/etudes/BRIE/2015/545736/EPRS_BRI%282015%29545736_EN.pdf.***

politisch zu informieren und eine Meinung zu bilden – das ist problematisch, denn immerhin ist das Internet für die Meinungsbildung zunehmend zentral. Hier besteht somit eine offensichtliche Diskrepanz zwischen ihrer Mündigkeit als Wähler:inen und einer Bevormundung bei der Nutzung digitaler Angebote.

6 AUSBLICK UND HANDLUNGSOPTIONEN

Hoher Handlungsdruck

Die Bestandsaufnahme, dass Kinder und Jugendliche aktuell unter vielen Aspekten der Digitalisierung leiden, drängt zu raschem Handeln: Es verdichten sich die Hinweise, dass im Zusammenhang mit digitalen Technologien neue Problemlagen entstehen oder bestehende Probleme verstärkt werden. Der Ansatz, Schutz durch Altersbeschränkungen einzuführen, erscheint bei eingehender Betrachtung allerdings als gleichzeitig überschießend, wenig effektiv und risikobehaftet. Altersbeschränkungen werden als relativ klare, insbesondere legistisch einfach umsetzbare Lösung dargestellt. Dabei ist die Hoffnung groß, damit die einleitend dargestellten Problemfelder, die insbesondere Kinder und Jugendliche belasten, in den Griff zu bekommen.

Altersbeschränkungen wenig effektiv und risikobehaftet

Altersbeschränkungen alleine keine Lösung

Eine Altersbeschränkung ersetzt entgegen dieser Hoffnung aber nicht andere Maßnahmen, allen voran den Aufbau von Medien- und Digitalisierungskompetenzen bei Kindern, Jugendlichen, Eltern und Lehrkräften: Früher oder später werden Heranwachsende auch in einem altersbeschränkten Internet auf problematische Inhalte stoßen und müssen erlernen, damit umzugehen. Auch ist eine lückenlose Durchsetzung von Altersbeschränkungen unrealistisch, weshalb möglicherweise Kinder und Jugendliche auf der Suche nach Verbotenem – was einen eigenen Reiz ausübt – auf besonders unregulierte und damit gefährliche Plattformen ausweichen. Es müssen daher dringend andere, effektivere Wege gefunden werden, um Kinder und Jugendliche effektiv vor verstörenden und nicht altersgerechten Inhalten zu schützen.

Umgang mit problematischen Inhalten muss erlernt werden

Abwägung mit verschiedener Kinderrechte wichtig

Die mangelhafte Effektivität von Altersbeschränkungen geht einher mit verschiedenen Risiken. Je nach Umsetzung entstehen hohe Gefahren insbesondere im Bereich Datenschutz und Datensicherheit. Doch auch Kinderrechte wie das Recht auf Meinungs- und Informationsfreiheit, Recht auf Zugang zu Informationen und Medien sowie das Recht auf Beteiligung an Freizeit, kulturellem und künstlerischem Leben drohen durch Altersbeschränkungen beschnitten zu werden: Viele Kinder und Jugendliche leiden unter Sozialen Medien, gleichzeitig bieten diese auch Möglichkeiten, Anschluss, Austausch und wichtige Informationen zu finden, und ihre minderjährigen Nutzer:innen profitieren vom Zugang dazu.

Verarbeitung hochsensibler Daten

Datensparsame Methoden sind in Entwicklung

Unter den aktuell praktizierten und diskutierten Methoden der Altersfeststellung gibt es einige, die aus Sicht des Datenschutzes hohe Risiken bergen und sensible Daten weit über die Altersfeststellung hinaus verarbeiten und möglicherweise auch speichern. Demgegenüber sind insbesondere die geplante Altersfeststellungs-App der EU und die European Digital Identity Wallet datensparsam. Dennoch gibt es auch bei diesen noch offene Fragen, einerseits inwiefern die praktische Umsetzung den hohen rechtlichen Vorgaben gerecht wird und andererseits, ob die Notwendigkeit eines Smartphones nicht kontraproduktiv ist.

Das Internet könnte zum Nachteil von Konsument:innen verändert werden

Allen Altersbeschränkungen wohnt gleichsam die Möglichkeit inne, die Architektur des Internets – sofern sie flächendeckend umgesetzt werden – umfassend zu verändern, und zwar für alle Verbraucher:innen sowie für Anbieter:innen (insbesondere Online-Medien jeder Art). Dadurch können Effekte zweiter Ordnung entstehen, die letztlich insbesondere für Verbraucher:innen nachteilig sein können: Verminderter Medienpluralismus, schlechterer Zugang zu Informationen, Zunahme von Bezahlschranken und möglicherweise intensiviertes User:innen-Tracking. Doch sind genau dieses User:innen-Tracking und darauf

aufbauende Personalisierungen ein Teil des Problems, das zu adressieren versucht wird, insbesondere auf Social-Media-Plattformen (Livingstone et al., 2025).

Handlungsoptionen:

Aus den Ergebnissen dieser Studie lassen sich einige Vorschläge für den Umgang mit der Herausforderung der Altersfeststellung im digitalen Raum ableiten:

Plattformen in die Pflicht nehmen …

… und schädliche Designs vermeiden

1. Die aktuellen Debatten um Altersbeschränkungen können als Verschiebung der Verantwortung von Plattform-Betreibern zu Verbraucher:innen eingeordnet werden. Dem könnte entgegengewirkt werden: Plattformen könnten verpflichtet werden, viele der schädlichen Eigenschaften auf Designebene zu vermeiden. Plattformen, die keine süchtig machende Interaktionsmuster nutzen, die Radikalisierung befeuernde Algorithmen verhindern und gewaltvolle Inhalte effektiv moderieren, wären für alle Internetnutzer:innen ein Gewinn, nicht nur für Kinder und Jugendliche. Entsprechende Anreize könnten gesetzt werden.

Kompetenzaufbau dringend notwendig …

… besonders bei Bezugspersonen

2. Der breite Kompetenzaufbau über alle Altersgruppen ist dringlich und umfasst sowohl Medien- als auch KI-Kompetenz,[67] aber auch sogenannte Plattform-Kompetenzen, also das Verständnis, wie Daten, Algorithmen und Geschäftsmodelle Online-Plattformen formen (Livingstone et al., 2025). Hier sind Eltern und andere erwachsene Bezugspersonen besonders gefordert, oft aber auch überfordert. Zielgruppenspezifische Konzepte und Angebote scheinen noch ausbaufähig. Kinder und Jugendliche sind vergleichsweise leicht über den Unterricht zu erreichen – dies setzt jedoch entsprechend geschultes Lehrpersonal und damit eine kritische Inhaltsgestaltung und zeitgemäße Vermittlung voraus.

Debatte sollte Kinder und Jugendliche einbinden

3. Eine gesellschaftliche Debatte, wie Kinder und Jugendliche stufenweise an den teils risikobehafteten digitalen Raum herangeführt werden können, erscheint notwendig. Dabei sollten unbedingt Kinder und Jugendliche mit einbezogen werden, etwa über die Bundesjugendvertretung, Schulsprecher:innen und ähnliche Institutionen.

   Schrittweises Heranführen an digitalen Raum

   In diesem Kontext wird oft die Parallele zum Straßenverkehr gezogen: Im Straßenverkehr drohen ständig Unfallgefahren, dennoch haben sich Prozesse etabliert, wie Kinder schrittweise lernen, sich in diesem Raum zu bewegen – anfangs mit enger Begleitung, um sich schließlich selbständig und die Gefahren erkennend im Straßenverkehr bewegen zu können. Umgelegt auf den digitalen Raum könnte dies z. B. anfangs ein Familien-Tablet sein, das ältere Kinder unter Aufsicht nutzen, und erst zu einem späteren Zeitpunkt der Besitz eines eigenen Smartphones.[68]

Prozessorientierung kompatibel mit Kinderrechten

4. Solche prozessorientierten Ansätze könnten ein zentraler Lösungsansatz sein, denn sie sind gut mit verschiedenen Kinderrechten vereinbar, da sie flexibler auf die individuelle Entwicklung einzelner Kinder und Jugendlicher eingehen können. Denn das Alter allein ist eine schlechte Orientierung für die Fähigkeit, mit belastenden Inhalten, Situationen und Funktionen umgehen zu können. Es kommt auf deren individuellen Entwicklungsstand, aber auch auf die Begleitung durch kompetente Erwachsene, denen Kinder vertrauen, an.

---

[67] Siehe dazu z. B. das Projekt Critical AI Literacy: *oeaw.ac.at/ita/projekte/cail-critical-ai-literacy.*

[68] Siehe dazu z. B. die Initiative Smarter Start ab 14: *smarterstartab14.de/smarter-startab14.de.*

5. Die Verfügbarkeit spezialisierter Unterstützung von Kindern und Jugendlichen zu verbessern, sollten sie mit dem digitalen Raum überfordert sein, wäre eine weitere wichtige Handlungsoption. Hier wäre es wichtig, dass ihnen nicht wertend begegnet wird: Es müsste ihnen Raum geben zu lernen, Fehler zu begehen und diese produktiv zu verarbeiten (Livingstone et al., 2025). Ein Ausbau der Kinder- und Jugendpsychiatrie sowie mehr präventive Initiativen sind als Sicherheitsnetz besonders wichtig.

Spezialisierte Unterstützung für belastete Kinder und Jugendliche ausbauen

6. Für jene Fälle, in denen eine Altersbeschränkung für Dienste, Inhalte und Funktionen sinnvoll erscheint, sind datensparsame Methoden (EU-Altersfeststellungs-App, EUDI-Wallet und Altersfestlegung am Gerät durch Bezugspersonen) in Entwicklung. Solche Methoden müssen gemäß Datenschutzrecht anderen Methoden vorgezogen werden. Dabei muss darauf geachtet werden, dass alle Möglichkeiten zu starkem Datenschutz ausgeschöpft werden, wie zum Beispiel die Führung eines Registers, das Plattformen klar vorschreibt, welche Attribute sie abfragen dürfen (z.B. nur „über 18“).

Datensparsame Methoden vorziehen

7. Das Fördern von analogem Erleben für Kinder und Jugendliche und das Sichern des Weiterbestehens nicht-digitaler Kanäle sollte auch für Kinder und Jugendliche die positiven Aspekte der Sozialen Medien erlebbarer machen, indem Zugehörigkeit, Selbstwirksamkeit und Austausch nicht nur online erfahren wird.

Analoges Erleben ist wichtig für Minderjährige

LITERATUR

Baum, C., Blazy, O., Camenisch, J., Hoepman, J.-H., Lee, E., Lehmann, A., Lysyanskaya, A., Mayrhofer, R., Montgomery, H., Nguyen, N. K., Preneel, B., shelat, a., Slamanig, D., Tessaro, S., Thomsen, S. E., & Troncoso, C. (2024). *Cryptographers' Feedback on the EU Digital Identity's ARF*.

Brailovskaia, J., Buchmann, J., Hertwig, R., Metzinger, T., Montag, C., Sadeghi, A.-R., Schneider, S., Spiecker gen. Döhmann, I., & Waldherr, A. (2025). Soziale Medien und die psychische Gesundheit von Kindern und Jugendlichen. In *Diskussion* (Bd. Bd. 40). MyCoRe Community. ***https://doi.org/10.26164/LEOPOLDINA_03_01307***

Brombacher, D., & Scaturro, R. (2025, Juni 26). Child soldiers of Europe: Why is organized crime increasingly recruiting minors? *Global Initiative Against Transnational Organized Crime*. ***https://globalinitiative.net/analysis/child-soldiers-of-europe-why-is-organized-crime-increasingly-recruiting-minors/***

Children's Commissioner. (2025). *„Sex is kind of broken now": Children and pornography* (S. 44). Children's Commissioner. ***https://assets.childrenscommissioner.gov.uk/wpuploads/2025/08/Embargoed-Sex-is-kind-of-broken-now-Children-and-Pornography.pdf***

Delaporte, M. A., & Miller, L. (2025). *Rapport fait au nom de la commission d'enquête sur les effets psychologiques de TikTok sur les mineurs* (S. 324). Assemblée Nationale. ***https://www.assemblee-nationale.fr/dyn/17/rapports/cetiktok/l17b1770-ti_rapport-enquete.pdf***

Directorate-General For Communication Networks, Content And Technology. (2025). *Commission guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28(4) of Regulation (EU) 2022/2065. For Public Consultation 13 May—10 June 2025* [Communication from the Commission]. European Commission.

Dopona, V. (o. J.). Research report: Manipulative digital marketing practices targeted at children and youth online. *Research Report*.

Döring, N. (2024). Digitale Pornografie. In P. Grimm, K. E. Trost, & O. Zöllner (Hrsg.), *Digitale Ethik* (S. 357–368). Nomos Verlagsgesellschaft mbH & Co. KG. ***https://doi.org/10.5771/9783748942399-357***

ECPAT International Project, Eurochild, & Terre des Hommes Netherlands. (2024). *Speaking Up for Change: Children's and caregivers' voices for safer online experiences*. ***https://ecpat.org/wp-content/uploads/2024/04/VOICE_Report.pdf***

Eichacker, M., Hajric, A., Moll, T., Möllers, F., & Vogelgesang, S. (2024). *Report on the Architecture of the EUDI-Wallet* (Nos. 2024–0393; S. 57). Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V.

EUCPN. (2024). *Preventing youth recruitment into organised crime: Insights from a multinational perspective* [Recommendation paper]. EUCPN. ***https://eucpn.org/sites/default/files/document/files/2502_ENG_PAPER_Youth%20recruitment_LR.pdf***

European Commission. (2025). *Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)* (Communication from the Commission No. C(2025) 5052 final). ***https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act***

European Commission. Directorate General for Communications Networks, Content and Technology., LLM., & Center for Law and Digital Technologies (eLaw). (2024). *Mapping age assurance typologies and requirements: Research report.* Publications Office. ***https://data.europa.eu/doi/10.2759/455338***

European Parliament. (2025, Oktober 16). *New EU measures needed to make online services safer for minors*. ***https://www.europarl.europa.eu/news/en/press-room/20251013IPR30892/new-eu-measures-needed-to-make-online-services-safer-for-minors***

Europol. (2024). *The recruitment of young perpetrators for criminal networks* (Intelligence Notification Nos. 2024–033; Europol PUBLIC Information, S. 3). Europol. ***https://www.europol.europa.eu/cms/sites/default/files/documents/IN_The-recruitment-of-young-perpetrators-for-criminal-networks.pdf***

Fardouly, J. (2025). Potential effects of the social media age ban in Australia for children younger than 16 years. *The Lancet Digital Health*, *7*(4), e235–e236. ***https://doi.org/10.1016/j.landig.2025.01.016***

Gill, G. (2025, Juli 18). Meaning Through Its Opposite: Significance Quest Theory and Nihilistic Violent Extremism. *Global Network on Extremism & Technology*. ***https://gnet-research.org/2025/07/18/meaning-through-its-opposite-significance-quest-theory-and-nihilistic-violent-extremism/***

Goldman, E. (2025). *The "Segregate-and-Suppress" Approach to Regulating Child Safety Online*.

Grother, P. J., Ngan, M. L., Yang, J., Quinn, G. W., & Hom, A. (2024). *Face analysis technology evaluation: Age estimation and verification* (No. NIST IR 8525; S. NIST IR 8525). National Institute of Standards and Technology (U.S.). ***https://doi.org/10.6028/NIST.IR.8525***

Grunwald, A. (2022). *Technikfolgenabschätzung: Einführung*. Nomos Verlagsgesellschaft mbH & Co. KG. ***https://doi.org/10.5771/9783748928775***

Hutton, J. S., Piotrowski, J. T., Bagot, K., Blumberg, F., Canli, T., Chein, J., Christakis, D. A., Grafman, J., Griffin, J. A., Hummer, T., Kuss, D. J., Lerner, M., Marcovitch, S., Paulus, M. P., Perlman, G., Romeo, R., Thomason, M. E., Turel, O., Weinstein, A., … Potenza, M. N. (2024). Digital Media and Developing Brains: Concerns and Opportunities. *Current Addiction Reports*, *11*(2), 287–298. ***https://doi.org/10.1007/s40429-024-00545-3***

Institute for Strategic Dialogue. (2025, Mai 8). Terror without ideology? The rise of nihilistic violence – An ISD Investigation. *Digital Dispatches*. ***https://www.isdglobal.org/digital_dispatches/terror-without-ideology-the-rise-of-nihilistic-violence-an-isd-investigation/***

Kaman, A., Devine, J., Erhart, M., Napp, A.-K., Reiss, F., Moeller, S., Zoellner, F., Behn, S., & Ravens-Sieberer, U. (2025). Youth Mental Health in Times of Global Crises: Evidence From the German Longitudinal COVID-19 and Psychological Health Study. *Journal of Adolescent Health*, S1054139X25001983. ***https://doi.org/10.1016/j.jadohealth.2025.05.010***

Kunz, T., & Waldmann, U. (2025). Online-Altersverifikation zur Gewährleistung des Minderjährigenschutzes. *Datenschutz und Datensicherheit - DuD*, *49*(6), 384–389. ***https://doi.org/10.1007/s11623-025-2108-1***

Livingstone, S. (2025, Januar 15). Child online safety – next steps for regulation, policy and practice. *London School of Economics: British Politics and Policy*. ***https://blogs.lse.ac.uk/politicsandpolicy/child-online-safety-next-steps-for-regulation-policy-and-practice/***

Livingstone, S., Carr, J., & Byrne, J. (2015). *One in Three: Internet Governance and Children's Rights* (No. 22). Global Commission on Internet Governance.

Livingstone, S., Jessen, R. S., Stoilova, M., Stänicke, L. I., Graham, R., Staksrud, E., & Jensen, T. (2025). Can platform literacy protect vulnerable young people against the risky affordances of social media platforms? *Information, Communication & Society*, 1–18. ***https://doi.org/10.1080/1369118X.2025.2518254***

Livingstone, S., Nair, A., Stoilova, M., Van Der Hof, S., & Caglar, C. (2024). Children's Rights and Online Age Assurance Systems: The Way Forward. *The International Journal of Children's Rights*, *32*(3), 721–747. ***https://doi.org/10.1163/15718182-32030001***

Livingstone, S., & Sylwander, K. R. (2025). There is no right age! The search for age-appropriate ways to support children's digital lives and rights. *Journal of Children and Media*, *19*(1), 6–12. ***https://doi.org/10.1080/17482798.2024.2435015***

Maierl, K. (2023, Februar). *Sexualität und digitale Medien – Online-Prävention sexualisierter Gewalt*. Gewaltinfo.at. ***http://www.gewaltinfo.at/themen/gewalt-an-kindern/sexualitaet-und-digitale-medien.html***

OECD. (2025a). *Age assurance practices of 50 online services used by children*. OECD Publishing. ***https://doi.org/10.1787/a19853ab-en***

OECD. (2025b). *How's Life for Children in the Digital Age?* OECD Publishing. ***https://doi.org/10.1787/0854b900-en***

Ofcom. (2025). *Protecting Children from Harms Online: Guidance on Content Harmful to Children*. Ofcom.

Orben, A., & Matias, J. N. (2025). Fixing the science of digital technology harms. *Science*, *388*(6743), 152–155. ***https://doi.org/10.1126/science.adt6807***

ParentsTogether Action, & Heat Initiative. (2025). *„Darling, Please Come Back Soon": Sexual Exploitation, Manipulation and Violence on Character AI Kids' Accounts*. ***https://parentstogetheraction.org/wp-content/uploads/2025/09/HEAT_REPORT_CharacterAI_DO_28_09_25.pdf***

Scheuble, S., & Oezmen, F. (2022). *Extremists' Targeting of Young Women on Social Media and Lessons for P/CVE* (Radicalisation Awareness Network (RAN) Practitioners). European Commission. ***https://home-affairs.ec.europa.eu/system/files/2022-03/ad_hoc_young_women_social_media_Lessons-p-cve_022022_en.pdf***

Teknologirådet. (2024, Oktober 7). *Innspill fra Teknologirådet vedrørende forslag til lov om aldersgrenser for bruk av sosiale medier*. ***https://media.wpd.digital/teknologiradet/uploads/2025/10/Horingsinnspill-aldersgrenser-fra-Teknologiradet.pdf***

Verdoodt, V., Lievens, E., O'Neill, B., & Dopona, V. (2025). *First evaluation of the European strategy for a better internet for kids (BIK+): A summary of consultations with children, young people, expert stakeholders, teachers, and parents*. European Schoolnet, prepared for the European Commission. ***https://better-internet-for-kids.europa.eu/sites/default/files/2025-04/BIK-plus-strategy-evaluation-report-May-2025.pdf***

Verein zur Selbstkontrolle audiovisueller Medienangebote zum Schutz von Minderjährigen. (2021, August). *Verhaltensrichtlinien*. JugendMedienSchutz. ***https://www.jugendmedienschutz.at/verhaltensrichtlinien/***

Verordnung (EU) 2024/1183 des Europäischen Parlaments und des Rates vom 11. April 2024 zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung des europäischen Rahmens für eine digitale Identität (2024). ***https://eur-lex.europa.eu/eli/reg/2024/1183/oj***

ABKÜRZUNGSVERZEICHNIS

Abs. .....Absatz
AI.....Artificial Intelligence
App .....Application
ARF .....Architecture and Reference Framework (EU)
Art. .....Artikel
BIK .....Better Internet for Kids
d.h. .....das heißt
DSA.....Digital Services Act (der EU)
DSG.....Datenschutzgesetz (Österreichs)
DSGVO.....Datenschutz-Grundverordnung (der EU)
eID.....elektronische Identität
eIDAS.....Electronic IDentification, Authentication and trust Services (EU-Verordnung)
et al.....und andere
etc. .....et cetera
EU .....Europäische Union
EUDI .....Europäische Digitale Identität (EU)
GDPR.....General Data Protection Regulation (siehe DSGVO)
i.d.R.....in der Regel
ID.....Identität
iOS.....[Apple-Betriebssystem]
KI.....Künstliche Intelligenz
LGBTIQ .....Lesbian, Gay, Bisexual, Transgender, Intersex, and Queer
NFC.....Near Field Communication
NIST.....National Institute of Standards and Technology (USA)
o.J.....ohne Jahr
ÖAW.....Österreichische Akademie der Wissenschaften
OECD.....Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OS.....Operating System
PC.....Personal Computer
s.o. .....siehe oben
UN.....United Nations
US(A) .....United States (of America)
usw.....und so weiter
VPN .....Virtual Private Network
X .....[vormals Twitter, eine Social-Media-Plattform]
z. B.....zum Beispiel

KURZBIOGRAFIEN

Dipl.-Ing. FABIAN FISCHER, BSc MA

Projektleitung, Institut für Technikfolgen-Abschätzung, Österreichische Akademie der Wissenschaften

Fabian Fischer forscht an der Schnittstelle von Wissenschafts- und Technikforschung sowie Informatik an den Wechselwirkungen zwischen digitalen Technologien und Gesellschaft. Forschungsschwerpunkt ist sind dabei datengetriebene algorithmische Systeme und „KI“.
https://www.oeaw.ac.at/ita/fischer

Mag. Dr. ANNA PAULS

Academy Scientist, Institut für Technikfolgen-Abschätzung, Österreichische Akademie der Wissenschaften

Anna Pauls wendet im Bereich Technikfolgenabschätzung ihren Hintergrund in Verhaltensökonomie, politischer Ökonomie und ökologischer Ökonomie an. Teil ihrer Forschungsinteressen sind Anreize durch digitale Lösungen und deren gesellschaftspolitische Auswirkungen, zum Beispiel auf Machtgefüge.
https://www.oeaw.ac.at/ita/pauls

MAG.ª LOUISE BELTZUNG

Referentin Abteilung Konsument:innenpolitik, AK Wien

Louise Beltzung befasst sich mit den Auswirkungen von Digitalisierung auf Verbraucher:innen. Ihre Expertise umfasst soziale Plattformen, algorithmische Preisgestaltung, Internetbetrug, Dark Patterns und Künstliche Intelligenz.
https://www.linkedin.com/in/louisebeltzung/

ZUR REIHE „MATERIALIEN ZUR KONSUMFORSCHUNG“

In der Reihe „Materialien zur Konsumforschung“ werden aktuelle und relevante Themen zu Konsum und damit im Zusammenhang stehende gesellschaftliche Entwicklungsprozesse diskutiert. Expert:innen aus verschiedensten Bereichen wie der Wissenschaft/Forschung, Bildung, Politik, NGOs oder Praxis sind eingeladen, empirische oder theoretische Beiträge zu liefern und so zu einem breiten Diskurs beizutragen. Diese Beiträge können Basis für weiterführende Diskussionen oder Anknüpfungspunkte an gesellschaftliche Entwicklungsprozesse sein und durchaus kontroversielle Perspektiven einnehmen. Die hier vertretenen Meinungen sind unabhängig von der Meinung der Herausgeberin. Die Reihe erscheint in unregelmäßigen Abständen.

ZULETZT IN DER REIHE „MATERIALIEN ZUR KONSUMFORSCHUNG“ ERSCHIENEN

Wiesböck, Laura, Wang, Nuoyi, Reitzer, Pauline, Bănoiu, Irina, Beltzung, Louise und Lehner, Petra (2026): ADDICT. Reihe Materialien zur Konsumforschung, Nr. 20
https://emedien.arbeiterkammer.at/resolver?urn=urn:nbn:at:at-akw:g-7306832

Prantner, Christian und Rupprecht, Benedikta (2025): Wie stehen Konsument:innen zum digitalen Bezahlen? Reihe Materialien zur Konsumforschung, Nr. 19
https://emedien.arbeiterkammer.at/resolver?urn=urn:nbn:at:at-akw:g-7223822

Birkner-Tröger, Nina (2025): AK-Spielzeugstudie: Mehr Qualität, weniger Quantität. Reihe Materialien zur Konsumforschung, Nr. 18
https://emedien.arbeiterkammer.at/resolver?urn=urn:nbn:at:at-akw:g-7128993

Birkner-Tröger, Nina (2024): Kaufsucht in Österreich 2023. Reihe Materialien zur Konsumforschung, Nr. 17
https://emedien.arbeiterkammer.at/resolver?urn=urn:nbn:at:at-akw:g-6699376

Meixner, Oliver, Pichlbauer, Manfred, Haddu, Inès Nahéma und Birkner-Tröger, Nina (2024): „Krisen & Konsum“. Reihe Materialien zur Konsumforschung, Nr. 16
https://emedien.arbeiterkammer.at/resolver?urn=urn:nbn:at:at-akw:g-6617988

FOTOCREDITS
Porträtfotos Fabian Fischer & Anna Pauls: ITA/Bayer
Porträtfoto Louise Beltzung: © Jacqueline Godany

DER DIREKTE WEG ZU UNSEREN PUBLIKATIONEN
https://wissenschaft.arbeiterkammer.at/
https://emedien.arbeiterkammer.at/
https://emedien.arbeiterkammer.at/resolver?urn=urn:nbn:at:at-akw:g-1052860

ZITIERFÄHIGER LINK ZUR STUDIE
https://emedien.arbeiterkammer.at/resolver?urn=urn:nbn:at:at-akw:g-7309490

CREATIVE COMMONS CC BY-SA
Sofern nicht anders ausgewiesen, steht der Inhalt dieses Werks unter der Creative Commons Lizenz CC BY-SA 4.0 zur Verfügung: https://creativecommons.org/licenses/by-sa/4.0/deed.de

Bei Verwendung von Textteilen wird um Zusendung eines Belegexemplars an die AK Wien / Abteilung Konsument:innenpolitik ersucht.

IMPRESSUM
Medieninhaberin: Kammer für Arbeiter und Angestellte für Wien,
Prinz-Eugen-Straße 20–22, 1040 Wien, Telefon: (01) 501 65 0
Offenlegung gem. § 25 MedienG: siehe wien.arbeiterkammer.at/impressum
Auftraggeberin: AK Wien / Abt. Konsument:innenpolitik
Rückfragen an: Louise Beltzung (Louise.Beltzung@akwien.at)
Gestaltung: Alexander Ullrich | A SQUARED
Verlags- und Herstellungsort: Wien
Druck: AK Wien
ISBN: 978-3-7063-1190-8
© 2026 AK Wien

DIE AK – SO NAH

Sie wollen mit uns reden?
Unsere Videos sehen? Oder uns in den sozialen Medien besser kennenlernen? Auch auf unserer Homepage können Sie sich wie zuhause fühlen oder Sie machen es sich in der AK Bibliothek gemütlich.
Wir sind für Sie da – und immer in Ihrer Nähe.

wien.arbeiterkammer.at/immernah

AK WIEN
GERECHTIGKEIT MUSS SEIN

© Westend61 - Adobe Stock

ALTERSFESTSTELLUNG IM DIGITALEN RAUM

Ansätze und Auswirkungen auf Konsument:innen sowie Abwägungen zwischen Schutz der Privatsphäre und Kinderschutz

Endbericht

(Materialien zur Konsumforschung 21)

Februar 2026

9 783706 311908