

Don't judge me – Systeme zur Altersverifikation aus feministischer Perspektive

Elisa Lindinger und Elina Eickstädt



Altersverifikationssysteme (AVS) kommen zum Einsatz, um Kinder und Jugendliche von Webseiten mit vermeintlich jugendgefährdenden Inhalten fernzuhalten. Erwachsene müssen ihr Alter nachweisen, um auf solche Webseiten zuzugreifen. Zunehmend werden Forderungen laut, dass auch Kinder ihr Alter verifizieren sollen, um sie vor Kontaktaufnahmen durch Erwachsene zu schützen und den Funktionsumfang einer Anwendung einzuschränken, oder um Erwachsene von digitalen Plattformen fernzuhalten, die Kindern und geschultem Personal vorbehalten sind.

Die technischen Lösungen für AVS sind vielfältig: Einige Systeme greifen auf offizielle Ausweisdokumente zurück, die von externen Instanzen entweder technisch (z. B. die „Online-Ausweisfunktion“ in Deutschland) oder menschlich (z. B. PostIdent-Verfahren der Deutschen Post AG) geprüft werden. Andere bedienen sich Verfahren wie Biometrie und Künstlicher Intelligenz, um das Alter der Nutzer*innen zu schätzen. Beide Ansätze werden [von Digital-Rights-Organisationen grundsätzlich kritisiert](#).

Soziale Annahmen und Probleme von technischer Altersverifikation

Die Idee von Altersverifikation in der virtuellen Welt basiert auf einer festen Definition dessen, welche digitalen Räume und Dienste wem in welchem Umfang zur Verfügung stehen sollen. In der physischen Welt dagegen sind die wenigsten Räume rechtlich kategorisch für Kinder und Jugendliche verschlossen. Hier obliegt es meist den Eltern oder Erziehungsberechtigten, entsprechend des Entwicklungsstandes des Kindes individuelle Entscheidungen zu treffen, was es in welchem Umfang darf und was nicht.

Diese Form elterlicher Einwilligung wird teilweise auch im Digitalen nachvollzogen (z. B. bei der Installation von Apps auf einem Endgerät), ist jedoch unter Umständen mit hohen Dateneingriffen [bis hin zur Abklärung von Familienregistern](#) verbunden. Häufiger als nuancierte Ansätze, die individueller Entwicklung Rechnung tragen, sind jedoch feste Altersgrenzen, die technisch durchgesetzt werden. Das birgt Probleme und Risiken.

So basiert die Altersverifikation per Ausweisdokument auf der Annahme, dass Kinder, Jugendliche und Erwachsene stets Zugriff auf ihre Dokumente haben und diese die deutschen Anforderungen an optische Sicherheitsmerkmale erfüllen. Sie schließt außerdem strukturell Erwachsene ohne Ausweis oder mit Ausweisen anderer Nationalitäten, die nicht den Vorgaben entsprechen, aus.

Die algorithmische Altersschätzung wiederum beruht auf dem Vorhandensein bestimmter technischer Hilfsmittel – beispielsweise einer funktionierenden Kamera. Wie alle KI-Verfahren funktioniert sie mit geringer Fehlerquote in dem als „normal“ definierten Bereich der Daten, jedoch deutlich schlechter für Daten, die diesem Bereich nicht angehören – und damit für die Menschen hinter diesen Daten. [Weit verbreitete AVS tendieren dazu](#), Frauen als zu jung einordnen, und schätzen auch das Alter von Menschen mit Down-Syndrom häufig falsch ein. Ein diskriminierender Ausschluss von Menschen mit Krankheiten oder Behinderungen, die sich auf die Gesichtszüge auswirken, ist deshalb viel wahrscheinlicher.

Eine flächendeckende, algorithmische biometrische Altersschätzung normalisiert nicht nur den Zwang, sich ständig und überall auszuweisen. Sie normalisiert auch einen ubiquitären Einsatz von Risikotechnologien im Bereich der privaten Internetnutzung. Sie schafft ein technisches System, das über Zugänge entscheidet – und gegen das Kinder, Jugendliche und Erwachsene im Fall einer falschen Ablehnung ihr Recht kaum durchzusetzen können.

Die sozialen Auswirkungen der digitalen Altersverifikation sind offensichtlich: Strukturelle Benachteiligung oder Diskriminierung erschweren auch hier den Zugang, was potenziell soziale Ungleichheiten verschärft. Der pauschale Einsatz von algorithmischen Systemen im Kontext einer diversen Bevölkerung steht dem Grundsatz „from the margins to the center“ diametral entgegen. Er kollidiert zudem mit individuellen, vertrauensvollen familiären Aushandlungsprozessen darüber, in welche Räume Jugendliche hineinwachsen können dürfen – und lässt gerade in der für die persönliche Entwicklung kritischen Phase kein Wachstum und kein Ausprobieren zu.

Technologien im Netz zu etablieren, kann nie nur national gedacht werden

Das Internet ist ein globales Netzwerk. Gesetzliche Vorschriften, die sich von Land zu Land unterscheiden, werden von den Betreibern digitaler Services auf unterschiedliche Weise umgesetzt: Bei Zugriffen auf Webseiten erfolgt die Zuweisung der entsprechenden nationalen Rechtsordnung häufig anhand der IP-Adresse der Nutzer*in. Eine IP-Adresse lässt sich jedoch mit einfachen technischen Hilfsmitteln wie einem VPN oder dem Tor-Netzwerk – legalen und essenziellen Hilfsmitteln u. a. für Menschenrechtsaktivist*innen – ändern, um nationale Beschränkungen zu umgehen. In den USA nutzen [laut einer Studie](#) 41 Prozent der befragte Kinder zwischen 11 und 14 Jahren einen VPN.

Werden technische AVS rein national gedacht, sind sie zumindest per Browser leicht umgehbar. Gleichzeitig droht der Ansatz der digitalen Zugangskontrolle international Schule zu machen: Erkennbar ist die Tendenz, den Einsatz dieser Technologien auch auf andere Kontexte auszuweiten und so den freien Zugang zu Informationen, beispielsweise über Sexualität oder reproduktive Rechte, massiv einzuschränken. Das

ist höchst problematisch – insbesondere für Jugendliche mit Marginalisierungserfahrung, die auf entsprechende Angebote besonders angewiesen sind. Der rechtliche Ausschluss einer solchen Ausdehnung ist dabei nicht mehr als ein Lippenbekenntnis, denn technisch ist eine Zugriffsbeschränkung nicht auf einen bestimmten Anwendungsfall begrenzt. Wir bauen damit Zensurwerkzeuge für die ganze Welt.

Weitere technische Maßnahmen der Zugriffskontrolle, wie das Blockieren oder Filtern von Inhalten auf Netzwerkebene, kommen vor allem in illiberalen und autoritären Staaten zum Einsatz. Solche Eingriffe führen zum „Splinternet“, einem Internet, das in seinen Grundfunktionalitäten nicht mehr global ist. Nicht zuletzt wegen des hohen Missbrauchspotenzials [sprach sich Bundeskanzler Olaf Scholz explizit gegen diese Entwicklung aus.](#)

Im Fall von Apps auf Smartphones ist Altersverifikation über die Einstellungen für elterliche Kontrolle („parental control“) ohnehin möglich, ohne dass es AVS für einzelne Plattformen und Anwendungen bedarf. Sie lassen granulare – der individuellen Entwicklung des Kindes angepasste – Regeln zu.

Systemische Dimensionen: Welche Welt bauen wir mit technisierter Altersverifikation?

Manche Räume, ob on- oder offline, sollen entweder Kindern oder Erwachsenen vorbehalten sein. Schutzräume für Kinder und Jugendliche dürfen aber nicht durch einen massiven Einsatz von Überwachungs- und Kontrolltechnologien geschaffen werden, denn Fürsorge lässt sich nicht technisieren. Im Gegenteil: Technische Lösungen, auch wenn sie fürsorglich motiviert sind, werden besonders denen nicht gerecht, die sie am meisten brauchen.

Technische Lösungen machen die individuelle Einschätzung der Erziehungsberechtigten und einen Aushandlungsprozess mit Kindern und Jugendlichen darüber, welche Rechte ihnen eingeräumt werden, faktisch unmöglich. Stattdessen schreiben sie staatliche Macht in einen Bereich ein, der von Lernen, Wachsen, Vertrauen und Ausprobieren geprägt sein sollte. Diese Grundprinzipien verantwortungsvoller Erziehung vertragen sich nicht mit einem durchtechnisierten System nicht verhandelbarer One-size-fits-all-Lösungen. Auch, weil diese oft keine oder zumindest keine einfachen Optionen beinhalten, falsche Entscheidungen der Technik zu korrigieren.

Der Wunsch nach harten technischen Lösungen entspringt der realen Überforderung vieler Eltern und Lehrkräfte. Halbtechnische und individuell anpassbare Lösungen für elterliche Kontrolle, zum Beispiel die Einstellungen für „parental control“ auf gängigen Smartphones, sind ein wichtiger Ansatzpunkt dafür, Kinder und Jugendliche online zu schützen. Sie sind aber derzeit für viele Eltern schwer zu bedienen. Mehr Aufklärung

und Austausch über Möglichkeiten dieser Funktionen und eine bessere, leichter handhabbare Gestaltung sind dringend notwendig.

Hier liegt ein zentraler Ansatzpunkt: Welche Angebote brauchen wir, um Eltern, Lehrer*innen und Erzieher*innen, Kinder und Jugendliche in einen Austausch darüber zu bringen, was junge Menschen online erleben wollen und dürfen und wie sie ihre Rechte durchsetzen können? Und zwar ohne die Angst, dass die einzige Antwort darin besteht, ihre digitalen Möglichkeiten einzuschränken.

Veröffentlicht auf feministtechpolicy.org/



Ein Projekt von
SUPERRR Lab
Oranienstr. 58A
10969 Berlin
superrr.net

Ansprechpartnerin: Elisa Lindinger

elisa@superrr.net