Digitale Silver Bullets

Grundrechtswidrige Regulierungsvorhaben statt wirksamer Kinder- und Jugendschutz

Jürgen Bering & Svea Windwehr

30.08.2024 doi: 10.59704/56dd28505f6a47b2

Chatkontrolle, KI-gestützte Altersverifizierung und Zwangsfilter auf Betriebssystemen bilden die letzten Beispiele einer langen Reihe von Regulierungsvorhaben, die im Namen des Kinder- und Jugendmedienschutzes Grundrechtseingriffe als alternativlos darstellen. Dabei verkauft die Politik die noch nicht-existenten Techniken als *silver bullets*, also als simple Lösung zu einem komplexen Problem. Das ist fatal, weil die Vorhaben die Grundrechte aller Nutzer*innen unterminieren, nicht nur jene der vereinzelten Täter. Außerdem lassen die Vorhaben Kinder und Jugendliche die sich im Netz bewegen, mit ihren komplexen und vielschichtigen Bedürfnissen und Risikoprofilen im Stich. Anstatt evidenzbasierte Alternativkonzepte zu entwickeln und in wirksame, holistische Ansätze für Kinder- und Jugendmedienschutz zu investieren, werden auch ihre Grundrechte auf informationelle Selbstbestimmung, Privatsphäre und Autonomie eingeschränkt.

Chatkontrolle noch nicht vom Tisch

Die Chatkontrolle ist zwar vorerst gescheitert, allerdings ist sie damit nur aufgeschoben, nicht aufgehoben: Auch nach intensivem Ringen hat es die belgische Präsidentschaft des Rats der Europäischen Union nicht geschafft, eine qualifizierte Mehrheit der Mitgliedsstaaten hinter ihrem Verordnungsentwurf zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (CSA-Verordnung) zu versammeln. So konnten massive Eingriffe in die Grundrechte aller europäischer Nutzer*innen zwar vorerst abgewandt werden. Trotz des erneuten Scheiterns des Rats, sich auf eine gemeinsame Position zu einigen, ist aber klar, dass Vorschläge wie das Client-Side-Scanning noch nicht vom Tisch sind, und auch in Zukunft die Europäische Kommission und Mitgliedstaaten wie Spanien und Irland das Projekt Chatkontrolle weiterhin mit Eifer verfolgen werden.

Außerdem ist in der Debatte um Altersverifizierungen im Netz mit neuen Vorstößen zu rechnen. Es häufen sich etwa Aussagen von Spitzenpolitiker*innen, nach denen die Nutzung von sozialen Netzwerken eingeschränkt und auf über 15-Jährige limitiert werden oder gar die Funktionsweisen von Endgeräten massiv beschnitten werden sollen. Zeitgleich wird im Rahmen der Novellierung des Jugendmedienschutzstaatsvertrags für Zwangsfilter auf Betriebssystemebene als ultimative technische Lösung für den Jugendschutz geworben. Dabei sollte spätestens nach dem Scheitern der Chatkontrolle klar sein, dass es ein „weiter so“ nicht geben darf, und es höchste Zeit ist, effektiven Kinder- und Jugendmedienschutz und Grundrechte zusammen zu denken.

Keine Privatsphäre ist auch keine Lösung

Das grundlegende Ziel, das die CSA-Verordnung verfolgt, ist ein sehr wichtiges und berechtigtes: den Missbrauch von Kindern über das Internet und die Verbreitung von Missbrauchsdarstellungen zu verhindern. Dafür setzt der Verordnungsentwurf der Kommission auf eine Reihe von Maßnahmen wie Netzsperren und Altersverifikationen. Im Kern ist das Ziel aber, Dienste dazu zu verpflichten, Inhalte nach unbekannten und bekannten Missbrauchsdarstellungen zu durchsuchen. Diese Verpflichtungen sind insbesondere an Dienste gerichtet, die ein erhebliches Risiko aufweisen, für den Austausch kindesmissbräuchlicher Inhalte verwendet zu werden (unabhängig vom tatsächlichen Ausmaß dessen). Qua Definition sind damit alle Dienste betroffen, die den Austausch von Nachrichten, Bildern oder Videos ermöglichen, auch solche, die Ende-zu-Ende Verschlüsselung einsetzen und momen-

tan nicht in der Lage sind, auf die Inhalte ihrer Nutzer*innen zuzugreifen. Gleichzeitig wird die direkte Aussage, dass Verschlüsselung aufgebrochen werden soll, weitgehend vermieden. Die vermeintliche Lösung soll das sogenannte Client-Side-Scanning bieten, also ein Scannen von Inhalten, bevor diese verschlüsselt werden. Dabei handelt es sich aber im Kern um einen Taschenspielertrick: Entweder Inhalte können verschlüsselt und privat versendet werden – einschließlich auf dem eigenen Endgerät – oder eben nicht.

Deshalb wurden bereits erhebliche Zweifel geäußert (s. etwa hier, hier und hier), ob die Vorschläge zu einer Chatkontrolle überhaupt grundrechtskonform sein könnten. Insbesondere wird nach überwiegender Auffassung davon ausgegangen, dass es sich um einen unverhältnismäßigen Eingriff in Grundrechte darstellt. Konkret betroffen sind unter anderem das Recht auf Privatsphäre (Art. 7 Charta der Grundrechte der EU, i.F. GRCh) und das Recht auf Schutz personenbezogener Daten (Art. 8 GrCh). Dabei kann man zunächst bezweifeln, inwiefern das Scannen von privaten Nachrichten ein geeignetes Ziel für mehr Kinder- und Jugendschutz ist und kritisch darauf hinweisen, dass die vorgeschlagenen Technologien hohe Fehlerquoten aufweisen. Selbst wenn man annehmen würde, dass die Chatkontrolle ein geeignetes Mittel wäre, um die Ziele der Verordnung durchzusetzen, liegt es nahe, dass dies eine anlasslose und umfassende Überwachung privater Kommunikation – einschließlich der Durchbrechung von Ende-zu-Ende-Verschlüsselung – nicht rechtfertigen würde.

Den rechtlichen Ausgangspunkt für diesbezügliche Zweifel bildet die Rechtsprechung des EuGH in den Sachen La Quadrature du Net und Digital Rights, nach denen Überwachungsmöglichkeiten unter anderem dadurch Grenzen aufgezeigt sind, dass diese verhältnismäßig sein müssen und es auch Kontrollmöglichkeiten bedarf. Darüber hinaus muss der Wesensgehalt der entsprechenden Grundrechte erhalten bleiben. In Bezug auf die Vorratsdatenspeicherung sah das Gericht keine Verletzung des Wesensgehalts, da es sich lediglich um Metadaten handelte, also kein Zugriff auf die tatsächliche Kommunikation vorlag. Das ist bei der Chatkontrolle anders. Auch wenn mit der Entscheidung La Quadrature du Net II Anzeichen dafür vorliegen, dass der EuGH seine Anforderungen abgesenkt haben könnte, ist im Kern weiter davon auszugehen, dass eine allgemeine, anlasslose und unkontrollierte Überwachung der Kommunikation zumindest einen unverhältnismäßig intensiven Eingriff darstellt.

Hinzu kommt die faktische Verpflichtung gegenüber Unternehmen, Verschlüsselungstechnik durch Client-Side-Scanning abzuschwächen. Der Europäische Gerichtshof für Menschenrechte hatte erst vor Kurzem entschieden, dass Ende-zu-Ende-Verschlüsselung eine grundrechtliche Bedeutung zukommt und es rechtswidrig ist, diesen Schutz präventiv aufzubrechen.

Auch wenn derzeit unklar ist, wie es mit dem Vorhaben weitergeht, erfolgen die oben beschriebenen Grundrechtseingriffe übrigens schon heute. Denn die EU hat bereits im Jahr 2021 eine Verordnung verabschiedet – und diese nun bis 2026 verlängert –, die es Anbieter*innen von Messengern und E-Mail-Diensten ermöglichen soll, auf freiwilliger Basis Nachrichten nach Missbrauchsdarstellungen zu durchsuchen, wovon viele Dienste wie Gmail oder Messenger von sozialen Netzwerken wie X und Facebook Gebrauch machen. Denn, auch wenn derzeit noch keine Verpflichtung zum Scannen besteht, gibt es doch hinreichend politischen Druck, die Maßnahme schon jetzt durchzuführen.

Ende-zu-Ende verschlüsselte Kommunikation ist zwar von der sogenannten Interims-Verordnung ausgenommen, allerdings gelangt ein Gutachten der Grünen/Europäischen Freien Allianz und der Europäischen Piratenpartei zu dem Ergebnis, dass die freiwilligen Maßnahmen unter der Interims-Verordnung nichtsdestotrotz EU-Grundrechte verletzen. Neben der bereits angesprochenen Unverhältnismäßigkeit der Eingriffe, die sich bei jeder Form anlassloser massenhafter Überwachung auftun, bringen die freiwilligen Maßnahmen der Anbieter*innen eigene Probleme mit sich. So werden an staatliche Überwachungsmaßnahmen strenge Anforderungen gestellt, was die Kontrolle und die Durchführung der Maßnahmen angeht, die für

Unternehmen nicht gelten. Auch können sich Nutzer*innen gegen staatliche Maßnahmen einfacher gerichtlich zur Wehr setzen. Sobald Private aber einen Freischein erhalten, zu überwachen, greifen viele dieser Absicherungen nicht mehr oder nur eingeschränkt. So entscheidet kein Gericht darüber, wie es bei staatlichen Überwachungsmaßnahmen in der Regel der Fall ist, wann Inhalte gescannt werden. Auch hat ein deutsches Gericht bereits entschieden, dass für eine Klage eines deutschen Nutzers gegen die Scanpraxis irische Gerichte zuständig sind, auch wenn die Daten schlussendlich beim deutschen Bundeskriminalamt landen. Dies wurde mit den europäischen Zuständigkeitsregeln in grenzüberschreitenden Fällen begründet. Das ist aber problematisch, weil Nutzer*innen davon absehen werden ihre Rechte in einem Gerichtsverfahren im Ausland durchzusetzen. Das liegt nicht zuletzt am sehr hohen finanziellen Risiko eines solchen Verfahrens.

Das falsche Versprechen der Altersverifizierung

Während die (freiwillige) anlasslose Massenüberwachung von privater Kommunikation durch private Anbieter*innen andauert, weil die EU die Interims-Verordnung verlängert hat, und verschiedene Akteure die verpflichtende Chatkontrolle rechtspolitische weiter verfolgen, wird in den Mitgliedsländern um eine weitere Maßnahme zum Kinderschutz gerungen: die Altersverifizierung. Der Begriff der Altersverifizierung beschreibt verschiedene Ansätze zur Ermittlung des Alters von Nutzer*innen im Netz. Dabei lässt sich grob zwischen zwei verschiedenen Herangehensweisen unterscheiden: die Verifizierung des Alters durch einen Datenabgleich, und das Schätzen des Alters aufgrund biometrischer Daten oder Einblicke in das Nutzer*innenverhalten.

Die Altersverifizierung ist im Rahmen der CSA-Verordnung für Dienste vorgesehen, die das Risiko tragen, für die Erstellung und Verbreitung von kindesmissbräuchlichen Materialien genutzt zu werden. Sie ist aber auch im Rahmen der Kinder- und Jugendmedienschutz-Regeln des Digital Services Act im Gespräch, wo sie als eine mögliche Maßnahme aufgeführt wird, um spezifische Risiken für Minderjährige zu mindern. Auch in den Mitgliedsstaaten ist die Altersverifizierung im Gespräch: Frankreichs und Dänemarks Staatsoberhäupter haben sich unlängst dafür ausgesprochen, den Zugang zu Online-Plattformen wie TikTok mittels Altersverifizierung auf Über-15-Jährige zu beschränken. Die spanische Regierung hat derweil angekündigt, einen Prototyp zur Altersverifizierung ab Ende Sommer 2024 zur Verfügung zu stellen. Und auch das deutsche Bundesfamilienministerium hat die Entwicklung eines Prototyps beauftragt, um ihre Vision einer angeblich datensparsamen und anonymen Methode zur Altersverifizierung vorzustellen.

Doch eine grundrechtskonforme Methode der Altersverifizierung umzusetzen, scheint der Quadratur des Kreises gleichzukommen. Alle bekannten Ansätze zeigen schwerwiegende Unzulänglichkeiten auf und bergen ernsthafte Risiken für die Kommunikationsfreiheit. Die Feststellung bzw. Verifizierung des Alters über Ausweispapiere oder elektronischen ID-Lösungen kann einem de facto Verbot der anonymen Nutzung von Internet-Diensten gleichkommen. Einige Personengruppen wie Geflüchtete oder auch Kinder besitzen nicht einmal gültige Ausweispapiere, die sie zur nutzen könnten, um ihr Alter zu verifizieren. Auch für Trans-Personen kann eine Verpflichtung, das eigene Alter mithilfe eines Ausweisdokuments, das mit dem geführten Namen nicht übereinstimmt, eine massive Zugangsbeschränkung zu Inhalten und Diensten bedeuten. Hinzu kommen Risiken für die Sicherheit und des Missbrauchs der so abgefragten und gesammelten Daten, zumal solche Identitätsprüfungen regelmäßig auf externe Dienstleister ausgelagert werden.

Auch das Schätzen des Alters von Nutzenden über die Auswertung biometrischer Daten oder anderer Signale, wie beispielsweise die Browserhistorie, geht mit erheblichen Nachteilen einher. Bei besonders sensiblen biometrischen Daten wird Nutzer*innen viel Vertrauen abverlangt, diese in die Hände von privaten Unternehmen zu geben. Zudem ist bei der Auswertung von biometrischen Daten und anderer Ansätze, die mittels KI Daten auswerten und nach Mustern und Regelmäßigkeiten suchen, oft unklar, wie genau das Modell zu seiner Einschätzung gelangt ist. Das ist besonders problematisch, wenn auf Grundlage solcher

Technologien Fehleinschätzungen vorgenommen werden und besonders jung aussehende Erwachsene oder Personen mit ungewöhnlichem Nutzungsverhalten vom Zugang zu bestimmten Apps oder Webseiten ausgeschlossen werden.

Damit stellen gängige Altersverifizierungsansätze nicht nur eine Reihe von Risiken für Nutzer*innen und ihre Kommunikationsfreiheit dar, sie vermitteln außerdem ein falsches Gefühl der Sicherheit. Denn es liegt auf der Hand, dass technische Systeme nie perfekt sind und umgangen werden können. Insbesondere Erwachsene mit böswilligen Absichten, die sich Zugang zu nur für Kinder bestimmte Räume verschaffen wollen, werden Mittel und Wege finden, ihre Ziele zu erreichen.

Massenüberwachung aufgeben, Kinderschutz priorisieren

Zugleich ist klar, dass technische Schutzsysteme nicht ausreichen, solange unsere Gesellschaft nicht bereit ist, massiv in die notwendigen Fähigkeiten zu investieren, die Kinder, Jugendliche und Erwachsene benötigen, um sich selbstbestimmt und sicher durch die digitale Welt bewegen zu können. Dazu gehören signifikante Investitionen in die Ausbildung von Medienkompetenz in Betreuungseinrichtungen und Schulen, gleichzeitig aber auch die Aus- und Weiterbildung von Polizist*innen und Mitarbeiter*innen von Jugendämtern im Umgang mit sexualisierter Gewalt gegen Kinder. Beratungsstellen und zivilgesellschaftliche Angebote für die Begleitung und Unterstützung von Kindern und Jugendlichen müssen ausgebaut und nachhaltig finanziert werden.

Auf Seite der Strafverfolgungsbehörden müssen die Kapazitäten erhöht werden, um sicherzustellen, dass Missbrauchsdarstellungen konsequent verfolgt, aber auch gelöscht werden. Das bedeutet mehr und besser ausgebildetes Personal, und Investitionen in eine technische Infrastruktur, die Polizeibehörden dabei unterstützt, kollaborativ auch über Landesgrenzen hinaus zusammenzuarbeiten.

Innerhalb von Diensten und Apps, die Kinder nutzen, muss es möglich sein, rechtswidrige Inhalte direkt gegenüber den zuständigen Behörden anzuzeigen und Unterstützung von Eltern oder anderen Vertrauenspersonen hinzuzuziehen. Kinder, Jugendliche und ihre Bezugspersonen müssen in der Lage sein, leicht bedienbare, aber granulare Konfigurationen vorzunehmen, um Inhalte und Interaktionsmöglichkeiten altersgerecht zu beschränken. Denn Kinder und Jugendliche haben das Recht, sich sicher durch die digitale Welt bewegen zu können. Politik, Gesellschaft und Diensteanbieter müssen dafür sorgen, dass sie dies tun können, ohne ihre Rechte auf Privatsphäre, Datenschutz und den freien Zugang zu Wissen an der Schwelle abgeben zu müssen.

AUTOR*INNEN
Jürgen Bering
Jürgen Bering ist Leiter des Center for User Rights, Gesellschaft für Freiheitsrechte.
Svea Windwehr
Svea Windwehr ist Co-Vorsitzende von D64.

EMPFOHLENE ZITATION
Bering, Jürgen; Windwehr, Svea: Digitale Silver Bullets: Grundrechtswidrige Regulierungsvorhaben statt wirksamer Kinder- und Jugendschutz, Verfassungsblog, 30.08.2024, doi: 10.59704/56dd28505f6a47b2.

Lizensiert unter CC BY-SA 4.0.

Langzeitarchiviert bei IntRechtDok unter: doi.org/10.17176/20240830-143718-0.