GESELLSCHAFT FÜR FREIHEITSRECHTE

Deutscher Bundestag
Ausschuss für Digitales

Ausschussdrucksache
20(23)132

22.02.2023

22. FEBRUAR 2023 | STELLUNGNAHME AN DEN AUSSCHUSS FÜR DIGITALES

CHAT-KONTROLLE

DER VERORDNUNGSENTWURF DER EU-KOMMISSION UND SEINE UNVEREINBARKEIT MIT DER EUROPÄISCHEN GRUNDRECHTECHARTA

INHALT

EINLEITUNG

Der Verordnungsentwurf der EU-Kommission zur Chatkontrolle[1] wirft erhebliche grundrechtliche Bedenken auf. Der Entwurf verfolgt mit der Bekämpfung sexueller Gewalt gegen Kinder ein Ziel, das für den Schutz von Kindern und ihrer Rechte essenziell ist und Grundrechtseingriffe rechtfertigen kann. An der Geeignetheit, Effektivität und Verhältnismäßigkeit der vorgeschlagenen Maßnahmen bestehen jedoch erhebliche Zweifel. Wir sind davon überzeugt, dass der Entwurf in entscheidenden Punkten gegen die EU-Grundrechtecharta verstößt. **Die fünf wichtigsten grundrechtlichen Einwände gegen den Vorschlag zur Chatkontrolle sind in dieser Stellungnahme zusammengefasst.**

Der Vorschlag der EU-Kommission stützt sich auf Art. 114 AEUV[2], die Harmonisierung des Europäischen Binnenmarktes. Durch die Wahl dieser Rechtsgrundlage legt sich die EU-Kommission darauf fest, der sexuellen Gewalt gegen Kinder mit dem Mittel der Wirtschaftsregulierung zu begegnen. Der Entwurf sieht einen Katalog an Pflichten für bestimmte Online-Dienste wie **interpersonelle Kommunikationsdienste**, **Hosting-Dienste**, **App-Stores** und **Internetzugangsanbieter** vor. Diese Kategorien sind dabei denkbar weit definiert, sodass eine große Anzahl von Diensteanbietern zu grundrechtlich sensiblen Maßnahmen verpflichtet werden soll:

Interpersonelle Kommunikationsdienste sind beispielsweise **E-Mail-Dienste wie Gmail** oder **Instant Messaging-Dienste wie WhatsApp**. Diese ermöglichen private Kommunikation über das Internet, zahlreiche Dienste bieten dabei Ende-zu-Ende-Verschlüsselung an. Die Pflichten für interpersonelle Kommunikationsdienste nach dem Chatkontrolle-Entwurf sollen auch für solche verschlüsselten Dienste gelten, bei denen der Anbieter die Inhalte der Kommunikation nicht einsehen kann. Zu den Hostingdiensten gehören alle Dienste, die im Auftrag ihrer Nutzer*innen Inhalte speichern. Das betrifft sowohl solche, die Inhalte Dritter für die Allgemeinheit öffentlich zugänglich machen (**Plattformen wie YouTube, Hostingdienste öffentlicher Webseiten**) als auch solche, die ihren Kund*innen einen privaten Cloudspeicher anbieten (**Dropbox, iCloud Drive**). Auch Mischformen zählen dazu, bei denen Inhalte nur einem bestimmten geschlossenen Personenkreis zugänglich sind (**private Accounts auf Twitter, geschlossene Gruppen auf Facebook, Hoster zugangsbeschränkter Organisationswebseiten**). App-Stores sind Diensteanbieter, die beim Download von Apps zwischen Entwickler*innen und Nutzer*innen vermitteln. Für die Installation von Apps auf modernen Smartphones ist in aller Regel ein App-Store notwendig. Die Regeln des Chatkontrolle-Vorschlags gelten nicht nur für die marktmächtigen **App-Stores von Google und Apple**, die auf Android-Geräten bzw. iPhones vorinstalliert sind, sondern auch für **Open-Source-Alternativen wie f-droid**.

Die Verbreitung von Darstellungen sexueller Gewalt gegen Kinder über Wirtschaftsakteure im Internet bzw. der Missbrauch dieser Online-Dienste zur Ausübung sexueller Gewalt gegen Kinder ist nur eine Facette eines schwerwiegenden Problems, das einer ganzheitlichen gesellschaftlichen Antwort bedarf. Rund drei Viertel der Fälle spielen sich im sozialen Nahfeld oder der Familie des Kindes ab[3]. Im letzten Abschnitt dieser Stellungnahme weisen wir deshalb auf **alternative, grundrechtlich weniger bedenkliche und effektivere Ansätze** hin, mit denen der Gesetzgeber seiner Pflicht zum Schutz von Kindern vor sexueller Gewalt nachkommen sollte. Ohne eine Änderung der Rechtsgrundlage Art. 114 AEUV und eine vollständig neue

[1] **Europäische Kommission**, Vorschlag für eine Verordnung des Europäischen Parlamentes und des Rates zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern, 2022, COM(2022) 209, 2022/0155/COD.
[2] Vertrag über die Arbeitsweise der Europäischen Union.
[3] **Bundesministerium für Familie, Senioren, Frauen und Jugend**, „Schieb den Gedanken nicht weg!" Kampagne für ein Umdenken bei sexueller Gewalt gegen Kinder gestartet, 17.11.2022.

Konzeption des Entwurfs kann der europäische Gesetzgeber diese wichtigen Impulse jedoch nicht aufnehmen, soweit sie über die Wirtschaftsregulierung hinausgehen. Die Chatkontrolle-Verordnung droht dem Kinderschutz somit einen Bärendienst zu erweisen, da sie die politische Debatte auf Überwachungs- und Sperrverpflichtungen verengt, die wegen eklatanter Verstöße gegen die EU-Grundrechtecharta vor Gericht keinen Bestand hätten.

1. DIE CHATKONTROLLE VERLETZT DAS RECHT AUF PRIVATSPHÄRE

Mit „Chatkontrolle" wird oftmals umgangssprachlich der gesamte Verordnungsentwurf der EU-Kommission bezeichnet. Bei Chatkontrolle im engeren Sinne handelt es sich um den Teil des Gesetzesentwurfs, wonach **Behörden Anbieter*innen von Kommunikationsdiensten wie WhatsApp oder Signal zur Überwachung privater Kommunikation verpflichten** können. Dabei handelt es sich um einen besonders schwerwiegenden Eingriff in das Recht auf Privatsphäre und auf den Schutz personenbezogener Daten (Art. 7 und 8 der EU-Grundrechtecharta): Die Überwachung findet anlasslos statt und umfasst den Inhalt der privaten Chatnachrichten – anders als die ebenfalls grundrechtswidrige Vorratsdatenspeicherung. Diese ist auf Metadaten beschränkt – also auf Informationen darüber, wer zu welchem Zeitpunkt mit wem kommuniziert hat.

Behörden können sogenannte „Aufdeckungsanordnungen" gegen Anbieter von interpersonellen Kommunikationsdiensten verhängen. Darunter versteht man, dass Behörden z.B. Messenger-Dienste dazu verpflichten können, die **Kommunikation all ihrer Nutzer*innen zu überwachen**. Dafür reicht aus, dass die Behörde ein erhebliches Risiko festgestellt hat, dass der betroffene Dienst für die Verbreitung sexueller Gewaltdarstellungen genutzt wird. **Aufdeckungsanordnungen sind nicht zielgerichtet**, sie müssen sich nicht auf die Überwachung der Kommunikation bestimmter Nutzer*innen beschränken, die konkret unter Verdacht stehen. Stattdessen können Behörden anordnen, dass alle Kommunikationsinhalte aller Nutzer*innen des Dienstes präventiv überwacht werden. Es handelt sich also um anlasslose Massenüberwachung.[4]

Eine solche behördliche Anordnung kann Diensteanbieter dazu verpflichten, Inhalte nach bekannten sowie unbekannten Darstellungen sexueller Gewalt gegen Kinder zu filtern. Darüber hinaus sollen Anbahnungsversuche Erwachsener gegenüber Minderjährigen (Grooming) automatisch erkannt werden. Auf diese Weise ermittelte Inhalte müssen die Diensteanbieter an ein neu zu schaffendes EU-Zentrum ausleiten, das die Informationen nach einer Plausibilitätsprüfung an die Strafverfolgungsbehörden der Mitgliedstaaten weitergibt. Schon an der Geeignetheit dieser Maßnahme, der Verbreitung von Darstellungen sexueller Gewalt gegen Kinder im Internet wirksam zu begegnen, gibt es erhebliche Zweifel. Ermittlungserfolge deutscher Strafverfolgungsbehörden in der Vergangenheit haben gezeigt, dass Kriminelle oftmals über interpersonelle Kommunikationsdienste lediglich die Schlüssel zu Dateien austauschen, die in verschlüsselter Form auf Hosting-Anbietern gespeichert sind. Die Links zu diesen Dateien werden wiederum in Darknet-Foren ausgetauscht. Bei einer derartigen Vorgehensweise der Kriminellen, wie beispielsweise im Falle „Boystown"[5], würde die Chatkontrolle vollständig ins Leere laufen, weil weder die automatische Filterung von interpersonellen Kommunikationsdiensten noch von Hostingdiensten die so ausgetauschten Inhalte auffinden könnte.

[4] Vgl. **Bäcker/Burmeyer**, My spy is always with me: Comments on the planned obligations of Internet service providers to combat sexualized violence against children (so-called "chat control" regulation), Verfassungsblog 2022.
[5] Vgl. **Der Spiegel**, Mutmaßliche »Boystown«-Administratoren: Vier Männer stehen wegen Missbrauchsseite vor Gericht, 14.09.2022.

Auch wenn den Diensteanbietern freigestellt wird, welche Technologien sie einsetzen, um der behördlichen Anordnung nachzukommen, müssen diese Technologien in jedem Fall in der Lage sein, die Kommunikationsinhalte zu analysieren. Damit einher geht das inhärente Risiko, dass auch legale intime Kommunikationsinhalte durch Mitarbeiter*innen der Technologiefirmen eingesehen, an Behörden ausgeleitet und schlimmstenfalls sogar durch Datenlecks an Kriminelle weitergeleitet werden. Wenn im Kontext der Chatkontrolle-Verordnung von Technologieneutralität die Rede ist, führt das in die Irre, weil keine Technologien vorhanden und auch nicht denkbar sind, die einerseits die Vorgaben des Verordnungsentwurfs erfüllen, andererseits aber die Vertraulichkeit legaler Kommunikation garantieren können.

Um bekannte Darstellungen sexueller Gewalt gegen Kinder aufzudecken, genügt womöglich noch ein automatisierter Abgleich von versendeten Mediendateien mit einer Referenzdatenbank. Um **unbekannte Darstellungen sexueller Gewalt und Grooming zu erkennen, muss maschinelles Lernen zum Einsatz** kommen, das die Kommunikationsinhalte analysiert. Diese Verfahren sind besonders fehleranfällig: Sie geben anhand von Mustern in der analysierten Kommunikation lediglich eine Schätzung darüber ab, um was für einen Inhalt es sich handeln könnte – ohne den Inhalt oder den Gesprächskontext tatsächlich zu verstehen. Es sind keine Technologien bekannt, die dazu in der Lage sind, solche unbekannten illegalen Inhalte zuverlässig von legaler Kommunikation zu unterscheiden.

Der Europäische Gerichtshof hat in seiner Rechtsprechung zur Vorratsdatenspeicherung darauf hingewiesen, dass eine anlasslose Massenüberwachung von Kommunikationsinhalten den Wesensgehalt des Rechts auf Privatsphäre verletzen würde.[6] **Anlasslose Massenüberwachung ist mit dem Schutz von Privatsphäre und Datenschutz nach der EU-Charta unvereinbar**, egal ob es um verschlüsselte oder unverschlüsselte Kommunikation geht. Im Zentrum der öffentlichen Kritik an der Chatkontrolle steht jedoch, dass diese keine Ausnahme für Kommunikationsdienste vorsieht, die eine Ende-zu-Ende-Verschlüsselung anbieten. Diese Dienste zeichnen sich dadurch aus, dass ausschließlich die an einer privaten Unterhaltung beteiligten Personen die Kommunikationsinhalte lesen können. Immer mehr Menschen greifen gezielt auf Ende-zu-Ende-verschlüsselte Messenger zurück, um sich zu schützen. Erhält der Anbieter eines solchen Messengers eine behördliche Anordnung, kann er diese nicht mit der Begründung zurückweisen, dass er die Kommunikationsinhalte gar nicht mitlesen kann. Verschlüsselung sei zwar wichtig, heißt es in dem Entwurf der EU-Kommission lapidar, die Diensteanbieter dürften aber nur zwischen solchen Technologien wählen, die ihnen erlauben, die illegalen Inhalte aufzuspüren. Mit anderen Worten: Diensteanbieter, die Ende-zu-Ende-Verschlüsselung ohne Hintertüren anbieten, können behördliche Anordnungen nicht umsetzen und kommen so in Konflikt mit dem Gesetz. Die **Aufhebung von Ende-zu-Ende-Verschlüsselung verstärkt die Intensität der Grundrechtseingriffe**, die von der anlasslosen Massenüberwachung ausgehen.

[6] „Zum Wesensgehalt des Grundrechts auf Achtung des Privatlebens und der übrigen in Art. 7 der Charta verankerten Rechte ist festzustellen, dass die nach der Richtlinie 2006/24 vorgeschriebene Vorratsspeicherung von Daten zwar einen besonders schwerwiegenden Eingriff in diese Rechte darstellt, ***doch nicht geeignet ist, ihren Wesensgehalt anzutasten, da die Richtlinie***, wie sich aus ihrem Art. 1 Abs. 2 ergibt, ***die Kenntnisnahme des Inhalts elektronischer Kommunikation als solchen nicht gestattet***", Gerichtshof der Europäischen Union, Urteil vom 8. April 2014, *Digital Rights Ireland*, verbundene Rechtssachen C-293/12 und C-594/12, Rn. 39, Hervorhebung durch den Autor. Siehe auch **Tuchtfeld**„ "Vielen Dank, Ihre Post ist unbedenklich"- Wie die Europäische Kommission das digitale Briefgeheimnis abschaffen möchte, Verfassungsblog 2022.

2. ES DROHEN CHILLING EFFECTS FÜR DIE KOMMUNIKATIONSGRUNDRECHTE

Bereits mehrfach hat der Europäische Gerichtshof angemahnt, dass eine **anlasslose Massenüberwachung sich mittelbar negativ auf die Meinungsfreiheit** (Art. 11 EU-Grundrechtecharta) auswirkt: Kommunikationsteilnehmer*innen werden darin gebremst, ihre Meinung frei zu äußern, wenn sie sich der Vertraulichkeit ihrer Kommunikation nicht sicher sein können.[7] Das trifft insbesondere Berufsgeheimnisträger*innen wie Journalist*innen bei der Kommunikation mit ihren Quellen, Whistleblower*innen, Oppositionelle oder Menschen in Kriegsgebieten. In der Ukraine etwa nahm die Zahl der Downloads der Messenger-App Signal in den zwei Monaten nach Beginn des Angriffskriegs Russlands um über 1000 Prozent gegenüber den Vormonaten zu.[8] Die Gefahr sogenannter **„Chilling Effects", also einer Abschreckungswirkung für die Ausübung der Kommunikationsgrundrechte,** wird verstärkt, wenn **die Chatkontrolle-Verordnung, wie von der EU-Kommission vorgeschlagen, die Ende-zu-Ende-Verschlüsselung von Messenger-Diensten angreift**. Die genannten Personenkreise greifen aus gutem Grund auf solche Messenger zurück. Wird ihnen diese Möglichkeit genommen, weil Diensteanbieter die Verschlüsselung umgehen müssen, ist mit erheblichen Chilling Effects, zu rechnen.
Dieser Effekt tritt unabhängig davon ein, ob Diensteanbieter*innen private Kommunikationsinhalte durch eine Hintertür in der Verschlüsselungstechnik überwachen oder durch eine der Verschlüsselung vorgeschaltete Ausleuchtung der Inhalte auf dem Endgerät der Nutzer*innen realisieren (Client-Side Scanning). Die Kommunikationsteilnehmer*innen erwarten, dass ihre Kommunikation vertraulich bleibt – und zwar schon in dem Moment, in dem sie eine Nachricht in das Chatprogramm auf ihrem Handy eingeben – nicht erst in dem Moment, in dem diese Nachricht an deren Adressat*in zugestellt wird. Entscheidend ist, dass die **Erwartung in die Vertraulichkeit und Integrität des Kommunikationsprozesses derart erschüttert** ist, dass die Betroffenen sich gezwungen sehen, die Ausübung ihrer Kommunikationsfreiheiten selbst einzuschränken.

Die Chatkontrolle-Verordnung droht Chilling Effects weit über die Grenzen der Europäischen Union hinaus zu entfalten. Einmal eingebaute Sicherheitslücken können von Geheimdiensten oder Kriminellen auf der ganzen Welt ausgenutzt werden. Wenn Anbieter in der EU Anpassungen an ihren interpersonellen Kommunikationsdiensten vornehmen müssen, um die Verschlüsselung zu schwächen, besteht außerdem eine hohe Wahrscheinlichkeit, dass sie diese Veränderungen global ausrollen – sei es aus unternehmerischen Erwägungen oder auf Druck von Drittstaaten. Gerade autoritäre Regime können sich hier den **„Brussels Effect"** zunutze machen, also die Wirkung europäischer Regulierung als globaler Standard. Sie müssen mit weniger Kritik für repressive Gesetze auf dem internationalen Parkett rechnen, wenn die EU mit Maßnahmen zur Überwachung vorausgeprescht ist.

Auch Kinder, zu deren Schutz die EU-Kommission die Chatkontrolle-Verordnung auf den Weg bringen will, haben ein Recht auf Privatsphäre und könnten von diesen Chilling Effects besonders betroffen sein. Mit zunehmendem Alter spielt bei Minderjährigen die private Internetnutzung eine immer wichtigere Rolle bei der Entfaltung ihrer Persönlichkeit. Wenn Kinder und Jugendliche in ihrem persönlichen Umfeld von

[7] Gerichtshof der Europäischen Union, Urteil vom 6. Oktober 2020, *La Quadrature du Net u.a.*, C-511/18, ECLI:EU:C:2020:791.
[8] **Report of the Office of the United Nations High Commissioner for Human Rights**, The Right to Privacy in the Digital Age, 04.08.2022.

sexueller Gewalt betroffen sind, kann die vertrauliche Kommunikation über das Internet ein Weg sein, Hilfsangebote in Anspruch zu nehmen. Die Erwartung, dass private Kommunikationsinhalte überwacht werden, kann Betroffene deshalb von der Inanspruchnahme solcher Hilfsangebote abhalten.

3. DE-FACTO-FILTERPFLICHT FÜR HOSTINGANBIETER OHNE VERFAHRENSRECHTLICHE GARANTIEN

Die geplanten Pflichten für Messenger stehen unter dem Schlagwort „Chatkontrolle" im Zentrum der öffentlichen Kritik an dem Verordnungsentwurf. Doch auch die geplanten Auflagen für Hostingdienste, die im Auftrag ihrer Nutzer*innen fremde Inhalte speichern, halten einer grundrechtlichen Prüfung nicht stand. Soweit sich die geplanten Pflichten für Hostinganbieter auf nichtöffentliche Inhalte beziehen, ist die unter 1. und 2. beschriebene **Gefährdung der Privatsphäre und der Meinungsfreiheit auch für die Hostingdienste einschlägig**. Hinzu kommen spezifische Probleme: Viele der vorgesehenen verfahrensrechtlichen Hürden für Aufdeckungsanordnungen können bei Hostingdiensten ins Leere laufen. Das liegt an den unterschiedlichen Privatsphäre-Regeln für Kommunikation auf Messengern und Hostingdiensten.

Hostingdienste (einschließlich privater Cloudspeicher-Anbieter wie Google oder Dropbox) können nicht nur nach der Chatkontrolle-Verordnung zum Scannen privater Inhalte verpflichtet werden, sie können Inhalte auch freiwillig durchsuchen. Die Chatkontrolle-Verordnung sieht vor, dass alle Diensteanbieter zunächst eine eigene Risikoanalyse vornehmen müssen, ob ihre Dienste das Risiko bergen, für sexuelle Gewalt gegen Kinder missbraucht zu werden. Nur wenn ein Diensteanbieter aus Sicht der Behörden auf diese Risikoanalyse mit unzureichenden Maßnahmen reagiert, verhängen sie eine Aufdeckungsanordnung. Die Hostingdienste ergreifen die Maßnahmen also nicht freiwillig, sondern um einer behördlichen Anordnung zu entgehen. Indem sie den Hostingdiensten aber nur vage Vorgaben macht, wie diese Maßnahmen auszusehen haben, hebelt die EU-Kommission jedoch einen effektiven Grundrechtsschutz aus: Im Rahmen dieser selbst gewählten Maßnahmen kann es dazu kommen, dass **Anbieter von Hostingdiensten auf fehleranfällige Filter zur Überwachung privater Kommunikation zurückgreifen**, ohne dass die für behördliche Aufdeckungsanordnungen vorgesehenen verfahrensrechtlichen Garantien zum Tragen kommen.

Darin unterscheiden sich Hostingdienste von Messenger-Diensten: Messenger- und Mail-Programme wie WhatsApp, Signal und Proton Mail fallen unter die e-Privacy-Richtlinie, die diesen Diensteanbietern grundsätzlich verbietet, private Kommunikationsinhalte ihrer Nutzer*innen zu überwachen. Eine bislang geltende temporäre Ausnahme von diesem Verbot, die ihrerseits schwerwiegenden grundrechtlichen Bedenken begegnet,[9] soll durch die Chatkontrolle-Verordnung ersetzt werden. Nach Inkrafttreten der Chatkontrolle-Verordnung dürfen Messenger und Mail-Programme nur noch auf Grundlage einer behördlichen Anordnung auf private Kommunikationsinhalte zugreifen. Für Hostinganbieter wie

[9] **Colneric,** Legal opinion commissioned by MEP Patrick Breyer, The Greens/EFA Group in the European Parliament, 2021.

beispielsweise private Cloudspeicher gilt die e-Privacy-Richtlinie mit dem Verbot der Überwachung privater Kommunikation dagegen nicht.

Für Hostinganbieter wird es regelmäßig attraktiv sein, durch „freiwillige" Maßnahmen einer behördlichen Anordnung zu entgehen. Auf diese Weise behalten die Unternehmen mehr Kontrolle – auch über die Kosten. Denn der **Anreiz ist groß, auf kostspielige Maßnahmen zum Schutz der Nutzer*innen-Grundrechte zu verzichten**.

Eine Behörde muss vor der Verhängung einer Anordnung das von dem Dienst ausgehende Risiko mit dem Eingriff in die Kommunikations-Grundrechte der Nutzer*innen abwägen. Der Europäische Gerichtshof hat diesbezüglich enge Grenzen für den verpflichtenden Einsatz von Filtersystemen definiert.[10] Diese sind nur dann mit dem Verbot allgemeiner Überwachungspflichten vereinbar, wenn die Filter so fehlerfrei funktionieren, dass die Diensteanbieter die Inhalte nicht "eigenständig inhaltlich beurteilen müssen". Zumindest **im Fall von unbekanntem Material und der Kontaktanbahnung mit Kindern (Grooming) sind die Filtersysteme hierzu nicht in der Lage**. Wenn ein Hostingdienst „freiwillig" im Rahmen seiner Pflicht zur Risikominimierung Inhalte filtert, findet eine staatliche Abwägung, **ob die Filtersysteme überhaupt den grundrechtlichen Anforderungen genügen**, nicht statt.

Die Folge wäre, dass große Mengen privater Inhalte wie beispielsweise einvernehmlich erstellte intime Fotos auf den Smartphones Erwachsener, die automatisch in der Cloud abgespeichert werden, von den Unternehmen automatisch identifiziert und gesammelt werden. Durch Datenlecks oder unzuverlässige Mitarbeiter*innen, die im Auftrag der Unternehmen die Daten sichten, können diese Informationen an die Öffentlichkeit geraten. Auch können auf solche „false positives" unzulässige Accountsperrungen oder falsche Meldungen an Strafverfolgungsbehörden folgen, wie bereits mehrfach geschehen.[11] Betroffene können dann plötzlich nicht mehr auf ihre Dateien zugreifen und werden nicht entschädigt, wenn sie dadurch in ihrer Berufsausübung oder anderen Lebensbereichen eingeschränkt werden.

4. GEPLANTE NETZSPERREN ERFORDERN ÜBERWACHUNG DES SURFVERHALTENS

Der Verordnungsentwurf sieht Sperrverpflichtungen für Internetzugangsanbieter vor, die sich auf einzelne Webseiten (URLs) beziehen. Vor Erlass einer Sperranordnung sollen Internetzugangsanbieter den Behörden Informationen über den Zugriff von Nutzer*innen auf die betreffende URL übermitteln. Um die nötigen Informationen über den Aufruf einzelner URLs erheben und an Behörden ausleiten zu können, **müssten Internetzugangsanbieter das Surfverhalten all ihrer Kund*innen präventiv und flächendeckend überwachen**. Das wäre aber mit dem **Verbot allgemeiner Überwachungspflichten und mit dem Grundrecht auf Privatsphäre unvereinbar**. Diese Informationen sind für die Internetzugangsanbieter obendrein technisch unzugänglich, wenn die URL durch die Verwendung des https-Protokolls in verschlüsselter Form aufgerufen wird. Inzwischen verwenden fast alle Webseiten https, um sicherzustellen,

[10] Gerichtshof der Europäischen Union, Urteil vom 26. April 2022, *Republik Polen/Europäisches Parlament und Rat der Europäischen Union*, C-401/19, ECLI:EU:C:2022:297.
[11] **The New York Times**, A Dad Took Photos of His Naked Toddler for the Doctor. Google Flagged Him as a Criminal, 21.08.2022.

dass beispielsweise Adress- oder Kreditkartendaten, die Nutzer*innen in Webformulare eingeben, verschlüsselt übertragen werden. Der flächendeckende Einsatz von https wird vom Bundesamt für Sicherheit in der Informationstechnik empfohlen.[12]

Auch eine gezielte Sperrung von einzelnen URLs ist den Internetzugangsanbietern ohne eine Aufgabe der https-Verschlüsselung[13] und die Überwachung der Kommunikationsinhalte nicht möglich. DNS-Sperren sind für die geplante Sperrung einzelner URLs nicht geeignet, denn sie betreffen stets ganze Domains. Eine DNS-Sperre, die gegen eine Missbrauchsdarstellung auf einer Sharehosting-Plattform gerichtet ist, würde auch alle anderen Inhalte des Sharehosters betreffen und damit den Anforderungen des Europäischen Gerichtshofs an die Zielgerichtetheit von Netzsperren nicht entsprechen.[14] In der Praxis besteht also eine **erhebliche Gefahr, dass Internetzugangsanbieter die Sperranordnungen entweder zulasten der Meinungs- und Informationsfreiheit übererfüllen**, indem sie eine ganze Domain mittels DNS sperren. Oder sie müssen beim Versuch einer zielgenauen Sperrung die Sicherheit der Onlinekommunikation mittels https aufgeben und das Surfverhalten ihrer Kund*innen überwachen.

5. ALTERSVERIFIKATION BIRGT GEFAHREN FÜR KOMMUNIKATIONSFREIHEIT

Der Verordnungsentwurf sieht vor, dass alle Anbieter*innen von Messenger- und Mail-Programmen sowie alle Hosting-Anbieter*innen, die für Grooming in Betracht kommen, das **Alter ihrer Nutzer*innen verifizieren** müssen. Das festgestellte Risiko muss dabei nicht erheblich sein – die Verpflichtung zur Altersverifizierung würde also grundsätzlich für alle Mail- und Messengerdienste gelten, die Kommunikation zwischen Minderjährigen und Erwachsenen ermöglichen. Lediglich Diensteanbieter, die ein Grooming-Risiko vollständig ausschließen können, sind von der Pflicht zur Altersverifizierung ausgenommen. Um vollständig auszuschließen, dass Erwachsene über einen Dienst mit Kindern kommunizieren können, muss ein Diensteanbieter jedoch das Alter seiner Nutzer*innen kennen, de facto gilt die Pflicht zur Altersverifizierung also für alle Anbieter von interpersonellen Kommunikationsdiensten oder Hosting-Diensten.

Darüber hinaus trifft die Pflicht zur Altersverifizierung auch alle Anbieter von App-Stores. Diese müssen darüber hinaus verhindern, dass minderjährige Nutzer*innen Apps überhaupt herunterladen können, von denen ein erhebliches Risiko ausgeht, für Grooming genutzt zu werden. Durch diese Maßnahme werden die **Kommunikationsgrundrechte besonders von Jugendlichen empfindlich eingeschränkt**. App-Stores müssten ihnen kategorisch verweigern, bestimmte Apps zu installieren, ohne dass eine Abwägung ihrer Rechte auf Meinungs- und Informationsfreiheit gegen das von der App ausgehende Risiko für minderjährige Nutzer*innen stattgefunden hat. Selbstverständlich ist das Grooming-Risiko einer App dann am größten, wenn sie sich sowohl bei Jugendlichen als auch bei Erwachsenen großer Beliebtheit erfreut. Das könnte weit verbreitete **Messenger wie WhatsApp** betreffen, beliebte **Online-Spiele wie Fortnite** oder **soziale Netzwerke wie TikTok**. Unabhängig von ihrem individuellen Entwicklungsstand müssten im Falle eines hohen Grooming-Risikos alle Minderjährigen vollständig von diesen Apps ausgeschlossen werden.

[12] **Bundesamt für Sicherheit in der Informationstechnik**, Basistipps zur IT-Sicherheit.
[13] Vgl. **European Data Protection Board**, Proposal to combat child sexual abuse online presents serious risks for fundamental rights, 29.07.2022.
[14] Gerichtshof der Europäischen Union, Urteil vom 27. April 2014, *UPC Telekabel Wien*, C-314/12, ECLI:EU:C:2014:192.

Durch die starke Marktkonzentration in diesem Bereich[15] sind die Möglichkeiten zum Ausweichen auf einen alternativen App-Store begrenzt, wenn ein Marktführer einer bestimmten App ein erhebliches Grooming-Risiko zuschreibt und minderjährigen Nutzer*innen den Download ungerechtfertigterweise verweigert. Selbst die wenigen alternativen zu Apple und Google auf dem App-Store-Markt, wie das Open-Source-Projekt f-droid für Android-Geräte, sind von der Pflicht zur Altersverifikation betroffen[16]. Für diese alternativen Projekte ist die Chatkontrolle-Verordnung existenzgefährdend. Die dezentralisierte Open-Source-Community ist nicht in der Lage, ein zentralisiertes Altersverifikationssystem zu implementieren und damit den App-Store-Pflichten aus dem Verordnungsentwurf nachzukommen. Damit droht der Vorschlag genau die Marktkonzentration auf dem App-Store-Markt zu zementieren, die eine andere EU-Verordnung, der Digital Markets Act[17], gerade aufzubrechen versucht.

Zur Altersverifizierung wählen Diensteanbieter zwischen Verfahren zur Altersbeurteilung (beispielsweise KI-gestützte Gesichtsanalyse, wie sie Instagram bereits einsetzt)[18] und solchen zur Altersfeststellung (mittels eines Ausweisdokuments oder eines digitalen Identitätsnachweises). Beide **Verfahren sind für die Nutzer*innen äußerst eingriffsintensiv**.

Die Feststellung des Alters über Ausweispapiere kommt einem Verbot des Rechts auf anonymen Internetnutzung gleich, das die Bundesregierung laut Koalitionsvertrag garantieren will. Es ist auch nicht absehbar, dass die geplante europäische ID-Wallet eine datensparsame Abfrage der Volljährigkeit einer Person vorsehen wird. Weder der Verordnungsentwurf der EU-Kommission zur europäischen digitalen Identität[19] (EIDAS-Reform) noch das Verhandlungsmandat des Rates[20] verhindern, dass Unternehmen, die eine Volljährigkeitsabfrage mittels der digitalen Identität vornehmen, auf personenbezogene Daten wie das Geburtsdatum oder den Namen einer Person zugreifen können[21]. Es ist also keine technische Lösung zur Altersverifizierung in Aussicht, die eine anonyme Internetnutzung ermöglicht.

Die KI-gestützte Gesichtsanalyse wiederum wird von Diensteanbietern gerne auf externe Firmen ausgelagert, über deren Umgang mit diesen besonders sensiblen personenbezogenen Daten die Nutzer*innen kaum Kontrolle haben. Kommt die Technologie zu einer falschen Einschätzung, können außerdem auch **jung aussehende Erwachsene von der Nutzung bestimmter Apps ausgeschlossen werden**. Wer über keine Ausweispapiere verfügt oder seine biometrischen Daten keinem Unternehmen anvertrauen will, wird von elementarer Kommunikationstechnologie wie der Eröffnung eines Mail-Accounts oder der Nutzung eines App-Stores ausgeschlossen. Ein modernes Smartphone ohne App-Store zu nutzen ist kaum möglich. Auch ein Verzicht auf Messenger-Dienste ist gerade für Menschen, die aus gutem Grund besonderen Wert auf eine anonyme Internetnutzung legen (Whistleblower*innen, Betroffene von Stalking, politisch Verfolgte), unzumutbar. Im Gegensatz zu Diensteanbietern können Nutzer*innen außerdem **nicht immer zwischen verschiedenen Verfahren der Altersverifikation wählen**.

[15] Siehe **Gesellschaft für Freiheitsrechte e.V.**, Grundrechtsbindung von Digitalkonzernen, 2022.
[16] Vgl. **Elina Eickstädt, Netzpolitik**, Chatkontrolle: Akute Gefahr für offene Software, 2022.
[17] Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor.
[18] Siehe **Instagram**, Introducing New Ways to Verify Age on Instagram, 23.06.2022.
[19] **Europäische Kommission**. Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität. 2021. COM(2021) 281, 2021/0136/COD.
[20] **Rat der Europäischen Union**. Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität – Allgemeine Ausrichtung, 2022, 14959/22, 25.11.2022.
[21] Das Europäische Parlament hat sein Verhandlungsmandat noch nicht verabschiedet.

6. GRUNDRECHTLICH UNBEDENKLICHE ALTERNATIVEN

Durch die Wahl des Art. 114 AEUV als Rechtsgrundlage hat die EU-Kommission sich darauf festgelegt, der sexuellen Gewalt gegen Kinder mittels der Regulierung von Wirtschaftsakteuren begegnen zu wollen. Ihre Gesetzgebungskompetenz leitet die EU-Kommission daraus ab, dass „Hindernisse für den digitalen Binnenmarkt für Dienste entstanden" seien, „nachdem einige Mitgliedstaaten unterschiedliche nationale Vorschriften zur Prävention und Bekämpfung des sexuellen Kindesmissbrauchs im Internet eingeführt"[22] hätten. Der Verordnungsentwurf diene also dazu, diese Hindernisse für den Binnenmarkt zu beseitigen und die Entstehung neuer Hindernisse für die grenzübergreifende Erbringung von Onlinediensten zu beseitigen.

Diese Begründung vermag nicht zu überzeugen. Alle Dienste, die vom Entwurf für die Chatkontrolle erfasst sind, fallen ebenfalls in den Geltungsbereich des kürzlich in Kraft getretenen Digital Services Act. Der Digital Services Act hat die Pflichten dieser Diensteanbieter in Bezug auf die Bekämpfung der Verbreitung illegaler Inhalte durch ihre Nutzer*innen vollharmonisiert. Die von der EU-Kommission beschworene Gefahr, dass nationale Gesetzgebung zur Bekämpfung sexueller Gewalt gegen Kinder im Internet eine Fragmentierung des europäischen Binnenmarktes befördern würde, besteht also nicht.

Das bedeutet nicht, dass Online-Dienste keinerlei Verantwortung für den Kinderschutz tragen sollten. Bei derartigen Vorgaben sollten jedoch die Schutzpflichten des Staates für die Grundrechte aller Betroffenen im Vordergrund stehen, nicht die Harmonisierung des Europäischen Binnenmarktes. Tatsächlich ist die sexuelle Gewalt gegen Kinder auch im Internet ein schwerwiegendes Problem, dessen Bekämpfung für den Schutz von Kindern und ihrer Rechte essenziell ist. Die Verbreitung von Darstellungen sexueller Gewalt gegen Kinder über das Internet trägt zu einer ständigen Retraumatisierung der Betroffenen bei und auch die Nutzung von Online-Diensten durch Kriminelle zu Zwecken des Grooming bedarf geeigneter, effektiver und verhältnismäßiger Gegenmaßnahmen.

Im Rahmen der von der EU-Kommission gewählten Rechtsgrundlage sind nur solche grundrechtsschondenden alternativen Maßnahmen denkbar, die sich an Online-Dienste richten. Diesen Rahmen sucht der Berichterstatter des mitberatenden Binnenmarktausschusses des Europäischen Parlaments auszuschöpfen. In seinem kürzlich veröffentlichten Berichtsentwurf[23] plant er, einige besonders schwerwiegenden Grundrechtseingriffe wie Client-Side Scanning, Altersverifikation und die automatische Erkennung unbekannter Darstellungen sexueller Gewalt oder von Grooming zu streichen. Stattdessen will er interpersonelle Kommunikationsdienste und Hosting-Dienste verpflichten, Kinder durch besonders privatsphärefreundliche Voreinstellungen (privacy by design and by default), leicht auffindbare und altersgerechte Informationen über Risiken des Dienstes und Beratungsangebote, sowie kinderfreundliche und beschleunigte Meldewege für verdächtige Inhalte zu schützen. Diese Vorschläge müssen zwar in Bezug auf den personellen Mehraufwand bei den betroffenen Diensten einer

[22] **Europäische Kommission**, Vorschlag für eine Verordnung des Europäischen Parlamentes und des Rates zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern, 2022, COM(2022) 209, 2022/0155/COD, Begründung. Rechtsgrundlage, Subsidiarität und Verhältnismäßigkeit, S. 7.

[23] **Europäisches Parlament**. Draft Opinion of the Committee on the Internal Market and Consumer Protection for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse. (COM(2022)0209 – C9-0174/2022 – 2022/0155(COD)), 08.02.2023.

Verhältnismäßigkeitsabwägung unterliegen, sind unserer Ansicht nach aber grundsätzlich besser geeignet als technische Scheinlösungen, einen Ausgleich der verschiedenen betroffenen Grundrechte zu gewährleisten.

Auch eine solch grundlegende Neuorientierung der Pflichten für Online-Dienste, wie sie im Binnenmarktausschuss des Europaparlaments diskutiert wird, greift für eine effektive Bekämpfung sexueller Gewalt gegen Kinder zu kurz, weil sie das Problemfeld allein aus der Perspektive der Wirtschaftsregulierung betrachtet. Wir begrüßen, dass die Bundesregierung durch Maßnahmen wie die Kampagne „Schieb den Gedanken nicht weg!" des Bundesministeriums für Familie, Senioren, Frauen und Jugend einen ganzheitlicheren Ansatz verfolgt und der besonderen Gefahr von sexueller Gewalt im Nahfeld von Kindern und Jugendlichen Rechnung trägt. Diese Erkenntnis schlägt sich jedoch noch nicht hinreichend in öffentlicher Unterstützung für Präventions- und Hilfsangebote nieder. Als illustratives Beispiel sei auf die unzulänglichen Telefonzeiten des Hilfe-Telefons Sexueller Missbrauch der Unabhängigen Beauftragten für Fragen des sexuellen Kindesmissbrauchs verwiesen.[24]

Wir hoffen darüber hinaus, dass die Debatte um die Chatkontrolle den Blick des Gesetzgebers auf die Unzulänglichkeiten der Strafverfolgung im Online-Bereich in der öffentlichen Verantwortung schärft. Grundlage von Empfehlungen zur Verbesserung der Strafverfolgung sollte eine Analyse der bisherigen erfolgreichen Ermittlungen gegen kriminelle Strukturen im Internet wie der Fall „Boystown" bilden. In diesen Fällen haben verdeckte Ermittler*innen eine zentrale Rolle gespielt. Diese gilt es durch Ausbildung und faire Arbeitsbedingungen angesichts dieser psychisch besonders belastenden Aufgaben zu unterstützen.

Der Vorschlag zur Chatkontrolle droht stattdessen Strafverfolgungsbehörden nicht nur mit zahlreichen Meldungen von false positives zu beschäftigen. Darüber hinaus besteht auch die Gefahr, dass sich die Meldungen von einvernehmlichem Sexting unter Jugendlichen häufen werden. Da solche Inhalte durchaus den Straftatbestand des § 184b StGB erfüllen können, sind die Behörden verpflichtet, solchen Hinweisen nachzugehen und die Jugendlichen strafrechtlich zu verfolgen. Diese Verfahren könnten dringend benötigte personelle Ressourcen von verdeckten Ermittlungen gegen erwachsene Täter*innen abzweigen. Eine Überprüfung von § 184b StGB mit Blick eine Korrektur des Strafrahmens, wie kürzlich von der 93. Konferenz der Justizministerinnen und Justizminister der Länder beschlossen, erscheint mit Blick auf eine bessere Priorisierung der begrenzten Ressourcen der Strafverfolgungsbehörden ebenfalls sinnvoll, um es Staatsanwaltschaften zu ermöglichen, in bestimmten Fällen von einer Strafverfolgung abzusehen.

Wir hoffen, dass diese Auswahl geeigneterer, grundrechtsschonender Alternativen zur Chatkontrolle illustriert, dass die Möglichkeiten des Gesetzgebers zur Prävention und effektiven Bekämpfung sexueller Gewalt gegen Kinder bei Weitem nicht ausgeschöpft sind. Eine Ablehnung des Verordnungsentwurfs zur Chatkontrolle sollte mit einem Maßnahmenpaket flankiert werden, das der besonderen Schwere dieser Verbrechen Rechnung trägt, ohne Kinderschutz und den Schutz vertraulicher Kommunikation gegeneinander auszuspielen.

[24] Mo, Mi & Fr 9–14 Uhr, Di & Do 15–20 Uhr, nicht an bundesweiten Feiertagen, am 24. oder 31.12. Vgl. **Hilfe-Portal Sexueller Missbrauch**. Ein Angebot der Unabhängigen Beauftragten für Fragen des sexuellen Kindesmissbrauchs.