Deutscher Bundestag **Drucksache 21/2046**

21. Wahlperiode 07.10.2025

Antrag

der Abgeordneten Donata Vogtschmidt, Clara Bünger, Dr. Michael Arndt, Anne-Mieke Bremer, Mandy Eißing, Katrin Fey, Nicole Gohlke, Ates Gürpinar, Dr. Gregor Gysi, Mareike Hermeier, Luke Hoß, Maren Kaminski, Ferat Koçak, Jan Köstering, Sonja Lemke, Sören Pellmann, Bodo Ramelow, David Schliesing, Evelyn Schötz, Julia-Christina Stange, Aaron Valent, Christin Willnat und der Fraktion Die Linke

zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern
KOM(2022) 209 endg.; Ratsdok. 9068/22

hier: Stellungnahme gegenüber der Bundesregierung gemäß Artikel 23 Absatz 3 des Grundgesetzes

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Sexualisierte Gewalt an Kindern zählt zu den niederträchtigsten Formen der Kriminalität, mit oft schweren Langzeitfolgen für die jungen Betroffenen. Verbunden damit sind häufig Darstellungen sexualisierter Gewalt an Kindern, die Online verbreitet werden. In Deutschland gab es laut polizeilicher Kriminalstatistik 42.854 ausermittelte Fälle von Missbrauchsdarstellungen an Kindern im Jahr 2024, das Dunkelfeld wird als weitaus größer angenommen. Ein Drittel der 12 bis 19-Jährigen in Deutschland hat sexualisierte Gewalt im Netz bereits erlebt, weltweit ist laut internationalen Studien etwa jedes zwölfte Kind von digitaler sexualisierter Gewalt betroffen (https://beauftragte-missbrauch.de/fileadmin/Content/pdf/Zahlen_und_Fakten/Zahlen_und_Fakten_Sexualisierte_Gewalt_gg._Kinder_und_Jugendliche_UBSKM_21.08.2025.pdf). Es ist daher dringend geboten, Kinder vor sexualisierter Gewalt besser als bisher zu schützen und auch Darstellungen dessen im Internet wirksamer als bisher zu bekämpfen. Dazu werden derzeit unterschiedliche Methoden angestrebt, die in sehr unterschiedlichem Ausmaß wirksam sind und teilweise auch zu unverhältnismäßigen Verletzungen der Privatsphäre von Kindern und Erwachsenen sowie zur allgemeinen Gefährdung der IT-Sicherheit führen können.

Am 11. Mai 2022 legte die EU-Kommission den Entwurf einer Verordnung für Regeln zur Prävention und Bekämpfung der Darstellung sexueller Gewalt an Kindern (KOM(2022)209) vor, die auch als Child Sexual Abuse (CSA)-Verordnung und unter dem Schlagwort „Chatkontrolle“ bekannt wurde. Gegenstand sind Verpflichtungen von Dienste-Anbietern, unter anderem von Kommunikationsdienstleistern, zum nicht-anlassbezogenen Scannen von Inhalten auf Darstellungen sexualisierter Gewalt an Kindern. Weiterhin beinhaltet die Verordnung unter anderem Szenarien für Verpflichtungen zu Netzsperren und zur verpflichtenden Altersverifizierung.

Kritisiert wird die geplante CSA-Verordnung als das größte Überwachungspaket, das es in der EU je gegeben habe und sie sei zudem auch nicht geeignet, um Kinder besser vor sexualisierter Gewalt zu schützen (siehe Begründung). Das Überwachen privater Kommunikation in diesem Ausmaß wäre auch mit der E-Privacy-Richtlinie (2002/58/EG) nicht vereinbar gewesen. Bereits im Juli 2021 wurde eine inzwischen auf April 2026 fristverlängerte Ausnahmeregelung (https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32021R1232&qid=1689261989495) verabschiedet, die es den Kommunikationsdienstleistern seither gestattet, auf freiwilliger Basis derart weitreichende Überwachungsmaßnahmen durchzuführen. Ein Beispiel ist das unter anderem von Microsoft, Google und Facebook eingesetzte Werkzeug „PhotoDNA“. Aus der bisherigen Freiwilligkeit soll mit dem CSA-Verordnungsentwurf eine Verpflichtung werden. Diese soll auch nicht-anlassbezogen für Ende-zu-Ende-verschlüsselte Kommunikationsinhalte gelten, was neben dem weitreichenden Eingriff in die Privatsphäre zahlloser Unschuldiger eine technische Schwächung sicherer, verschlüsselter Kommunikation zufolge hätte und die IT-Sicherheit insgesamt gefährdet.

Die Bundesregierung hatte sich nach längerem Zögern im April 2023 gegen Maßnahmen positioniert, die Anbieter zum Aufdecken verschlüsselter privater Kommunikation verpflichten können oder Ende-zu-Ende-verschlüsselte Kommunikation anderweitig schwächen (https://netzpolitik.org/2023/bundesregierung-innenministerium-setzt-sich-bei-chatkontrolle-durch/#2023-04-05_Bundesregierung_Positionspapier_CSA-VO; https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2024/stellungnahme-bfdi-32taetigkeitsbericht2023.pdf?__blob=publicationFile&v=1). Im Rat der EU konnte bis heute keine Einigung erzielt werden, zusammen mit Deutschland ergab sich eine Sperrminorität gegen Vorhaben, derartige Maßnahmen einzuführen.

Die derzeitige dänische Ratspräsidentschaft strebt nun für den 14. Oktober 2025 eine Einigung an, wobei es sich bei dem derzeitigen Entwurf der CSA-Verordnung vom 24.07.2025 (https://data.consilium.europa.eu/doc/document/ST-11596-2025-INIT/en/pdf) um eine Variante nahe am Ursprungsentwurf handelt, die unter anderem das verpflichtende Scannen auch verschlüsselter privater Kommunikation einschließt (https://netzpolitik.org/2025/internes-protokoll-daenemark-will-chatkontrolle-durchdruecken/). Die amtierende Bundesregierung hat sich bisher auf keine gemeinsame Position zur CSA-Verordnung festgelegt (vgl. Drucksache 21/1089, Frage 51). Dabei hängt die Sperrminorität im Rat der EU entscheidend von der Position Deutschlands ab. Sollte die Bundesregierung die Position der vorherigen Bundesregierung in dieser Frage nicht übernehmen, wäre eine Ausrichtung der EU auf das Scannen auch verschlüsselter privater Kommunikation wahrscheinlich.

Maßnahmen, die geeigneter, angemessener und wirksamer sind als im Entwurf der CSA-Verordnung, finden sich hingegen im Entwurf einer neuen Kinderschutz-Richtlinie (https://data.consilium.europa.eu/doc/document/ST-6241-2024-INIT/de/pdf), die seit dem Jahr 2024 parallel zur CSA-Verordnung verhan-

delt wird. Anforderungen für den besseren Schutz von Kindern auch vor sexualisierter Gewalt ergeben sich weiterhin aus Artikel 28 des Digital Services Act, zu dessen Umsetzung im Juli 2025 eine Leitlinie veröffentlicht wurde (https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors).

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

1. sich in Verhandlungen auf EU-Ebene und proaktiv in Gesprächen mit anderen Mitgliedstaaten klar und unmissverständlich gegen die geplante CSA-Verordnung einzusetzen;
2. sich in den Verhandlungen auf EU-Ebene für ein klares Verbot von Client-Side-Scanning (i.S.v. Durchsuchung und ggf. Ausleitung von Kommunikationsinhalten auf den Endgeräten von Nutzenden) und anderweitiger Schwächung Ende-zu-Ende-verschlüsselte Kommunikation einzusetzen;
3. sich in Verhandlungen auf EU-Ebene im Rahmen der derzeit ebenfalls beratenen EU-Kinderschutzrichtlinie KOM(2024)60 für ein zügiges Vorankommen wirksamer und verhältnismäßiger Maßnahmen für mehr Schutz von Kindern vor sexualisierter Gewalt einzusetzen, unter anderem konsequentes Löschen von CSA-Material, mehr Schutz vor sexueller Ausbeutung von Kindern per Livestream, klare Straftatbestände für Cybergrooming und CSA-Deepfakes, bessere Opferhilfe durch Opferschutz und Meldesysteme, Ausbau der Angebote kindergerechter digitaler Teilhabe, umfassend verbesserte digitale Bildung, gezielte Ermittlungswerkzeuge wie Quick-Freeze von Verkehrsdaten, Login-Fallen und „Honeypots“, sowie bessere europäische Zusammenarbeit und Kompetenzaufbau;
4. sich in Verhandlungen auf EU-Ebene dafür einzusetzen, dass Anforderungen des Kinderschutzes an Onlineplattformen gemäß Artikel 28 des Digital Services Act nach Maßgabe dazugehöriger Leitlinien konsequenter als bisher durchgesetzt werden können, insbesondere hinsichtlich Eindämmung suchtauslösender Elemente, sichere Voreinstellungen für Schutz vor Cybergrooming sowie gut und kindergerecht zugängliche Meldesysteme.

Berlin, den 7. Oktober 2025

Heidi Reichinnek, Sören Pellmann und Fraktion

Begründung

Sexualisierte Gewalt an Kindern ist ein besonders schwerwiegendes Verbrechen und jeder einzelne Vorfall wie auch die Verbreitung von entsprechenden Darstellungen müssen konsequent geahndet und verfolgt werden. Zwar sind die vom BKA erfassten Fälle 2024 nicht mehr weiter angestiegen, sie verharren jedoch auf hohem Niveau (https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/SexualdelikteNvKindernuJugendlichen/BLBSexualdeliktezNvKindernuJugendlichen2024.pdf)

Die in der CSA-Verordnung vorgeschlagenen Maßnahmen gegen sexualisierte Gewalt an Kindern sind nicht nur ineffektiv und voller problematischer Nebenwirkungen, sondern sogar geradezu schädlich für das angestrebte Ziel. Das gilt in besonderem Maße für die geplanten Aufdeckungsanordnungen, die sogenannte Chatkontrolle.

Denn insbesondere Minderjährige würden damit einem höheren Risiko als bisher ausgesetzt. Sowohl bei der automatisierten Erkennung von bisher unbekannten Darstellungen sexualisierter Gewalt an Kindern als auch bei der Erkennung sogenannter Anbahnungsversuche Erwachsener an Kinder („Grooming“) rechnen Expert*innen mit Fehlerraten, die zu einer große Anzahl Falschpositiver Meldungen führen (https://www.bundestag.de/resource/blob/983096/WD-10-038-23-pdf.pdf). Dies führt nicht nur dazu, dass in zehntausenden Fällen Unschuldige einem unerträglichen Verdacht ausgesetzt würden. Es bewirkt auch, dass legitime, aber sensible private Kommunikationsinhalte von Minderjährigen (wie im Familienchat geteilte Fotos vom Strandurlaub oder gewaltfreie Inhalte der alterstypischen Sexualentwicklung von Teenagern) massenhaft bei Polizeidienststellen landen, was die Privatsphäre Minderjähriger enorm verletzt. Der Verordnungsentwurf greift somit explizit die Privatsphäre und informationelle Selbstbestimmung ausgerechnet von Kindern und Jugendlichen an, anstatt diese zu verbessern. Deshalb kritisierte sowohl der Deutsche Kinderverein als auch unter anderem Joachim Türk vom Deutschen Kinderschutzbund den Verordnungsentwurf als „unverhältnismäßig“ und „nicht zielführend“ (https://www.bundestag.de/resource/blob/935798/Stellungnahme-Tuerk.pdf). Die zu erwartende hohe Anzahl falschpositiver Befunde würde dazu führen, dass Polizeikräfte weniger Zeit zur Verfügung hätten, tatsächliche Fälle zu verfolgen, was eine Verschlechterung der aktuellen Situation bedeuten würde. Schon heute sind nur etwa die Hälfte der beim BKA eingehenden Fälle strafrechtlich relevant, und etwa die Hälfte der Tatverdächtigen sind selber minderjährig. Zu den Ursachen hebt das BKA hervor, dass den Minderjährigen die strafrechtliche Relevanz oft nicht bewusst sei, beispielsweise wenn sie sich selber filmen oder derartiges Material mit Personen ihrer Altersgruppe teilen (https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2025/08/SexualdeliktezNvKindernuJugendlichen2024.html). Hier wäre viel mehr Aufklärung und Medienbildung wichtig, beides fehlt jedoch im CSA-Verordnungsentwurf.

Um die Anzahl falschpositiver Treffer bei automatisierten Scans privater Kommunikation zu senken, befinden sich deshalb die auch seitens des BMI in der nichtöffentlichen Sitzung des Digitalausschusses vom 12.09.2025 (https://www.bundestag.de/presse/hib/kurzmeldungen-1108356) geäußerten Vorschläge in Diskussion, die Aufdeckungsanordnungen als Kompromissüberlegung nur noch auf bereits bekanntes CSA-Material zu beschränken. Dieses könnte mithilfe entsprechender Datenbanken anhand von generierten Hash-Werten erkannt werden. Davon abgesehen, dass der aktuelle dänische Vorschlag das Scannen unbekannten Materials weiterhin umfasst (Erwägungsgründe 13, 61 und Artikel 5 Nr. 2a (nicht jedoch das Scannen auf Cybergrooming; Erwägungsgrund 77a)), würde der Verzicht darauf nichts an der Tatsache ändern, dass eine allgemeine technische Schwächung und inhaltliche Analyse der verschlüsselten privaten Kommunikationsinhalte erfolgt. Dies kommt einer faktischen Aufhebung des elektronischen Briefgeheimnisses gleich und ist daher völlig inakzeptabel. Kernproblem bleibt auch hier die fehlende Anlassbezogenheit der Scans. Die dänische Ratspräsidentschaft versucht auf das Problem in ihrem aktuellen Entwurf einerseits mit einer Eingrenzung der Detektion auf visuelle Inhalte und URLs (Erwägungsgrund 23a) zu reagieren, sowie mit einem Risikoklassenmodell (Erwägungsgrund 18a), das die Scans auf bestimmte risikoreiche Dienste eingrenzen soll. Allerdings war zumindest nach bisherigen Entwürfen der belgischen Ratspräsidentschaft ausgerechnet die Tatsache, dass eine sichere, verschlüsselte Kommunikation vorliegt, der Anlass, von einem hohen Risiko und damit nötigen Aufdeckungsanordnungen auszugehen – eben weil sich das Risiko aufgrund der Verschlüsselung nicht bewerten lässt (https://netzpolitik.org/2024/chatkontrolle-verschluesselte-dienste-sollen-als-erstes-durchleuchtet-werden/). In dem Fall könnten ausgerechnet Messenger mit einem hohen Schutzniveau der Privatsphäre wie Wire, Threema, Signal oder Messenger auf Basis des Matrix-Protokolls gezwungen werden, den technischen Schutz der Kommunikationsinhalte ihrer Nutzenden aufzugeben. Das gleiche gilt für Hosting-Services, die ebenfalls von Aufdeckungsanordnungen erfasst wären. Im dänischen CSA-Verordnungsentwurf ist angedacht, die Risikoklassifizierung in späteren delegierten Rechtsakten zu präzisieren (Artikel 5 Nr. 2a). Sind die technischen Voraussetzungen für die Überwachung auch verschlüsselter Kommunikationsinhalte einmal geschaffen, ist stark davon auszugehen, dass dies weitreichendere Begehrlichkeiten der Informationsgewinnung weckt. Die dänische Ratspräsidentschaft schlägt deshalb in ihrem aktuellen Entwurf (Artikel 7, Punkt 8) Ausnahmen vor, um die Vertraulichkeit der Kommunikation von Sicherheitsbehörden und den militärischen Sektor nicht zu untergraben. Für den Schutz der öffentlichen Hand im weiteren Sinne, von Journalist*innen, von vertraulicher Kommunikation mit Ärzt*innen, von Menschen vor politischer Verfolgung usw. ist dies jedoch keine Lösung. Dazu schlägt die dänische Ratspräsidentschaft vor, dass verschlüsselte Kommunikation auch ohne Aufdeckungsanordnungen weiterhin geschützt bleiben soll, wenn der Anbieter sicherstellt, dass keine visuellen Inhalte oder URLs verschickt werden können (Erwägungsgrund 26a). Wie dies praktisch umsetzbar sein soll, ohne die Nachrichteninhalte eben doch zu kontrollieren, bleibt unklar. Zudem sind Verharmlosungen der Aufdeckungsanordnung, indem die Scans der Kommunikationsinhalte mit herkömmlichen Spam-

Filtern verglichen werden, aus mehreren Gründen sachlich falsch und abzulehnen (https://chat-kontrolle.eu/wp-content/uploads/2023/10/Hintergrundpapier-Spam-Malware-Filter-Chatkontrolle.pdf). Weiterhin gibt es außerhalb des Entwurfs der dänischen Ratspräsidentschaft Kompromiss-Vorstellungen dahingehend, dass die Analysen der Kommunikationsinhalte lediglich dem Anbieter der betreffenden Software gemeldet werden und eine Ausleitung an Behörden unterbleibt. Doch auch in diesem Szenario müsste der technische Schutz Ende-zu-Ende-verschlüsselter Kommunikation zerstört werden und es bliebe ebenso zweifelhaft, welcher Beitrag zum Kinderschutz damit erreicht werden soll.

Vom Eingriff in die Privatsphäre Minderjähriger und aller anderen Menschen abgesehen schwächen die Aufdeckungsanordnungen die IT-Sicherheit generell, weil sich die zu schaffenden Schnittstellen auf den Endgeräten zur Ausleitung von Informationen auch von Kriminellen ausnutzen lassen. Selbst bei bestmöglicher Umsetzung entstehend dabei unweigerlich zusätzliche IT-Schwachstellen. Im aktuellen Verordnungs-Entwurf findet sich außerdem keine Antwort auf die Frage, wie gegen systematisch agierende Täter vorgegangen werden könnte, die CSA-Darstellungen besonders häufig über veränderliche URLs zu verschlüsselt gespeicherten Inhalten austauschen – eine Praxis, die mit den angestrebten automatisierten Scans mit Hashwert-Abgleichen kaum aufgedeckt werden könnte.

Im Entwurf der CSA-Verordnung ist auch das geplante EU-Zentrum abzulehnen. Vorgeblich dient es der Prävention, damit ist im Kern aber die Weitergabe aufgedeckter Verdachtsfälle an die Polizei, und die praktische Umsetzung von Aufdeckungsanordnungen gemeint, darunter auch die Zertifizierung von Technologie zum Scannen verschlüsselter Kommunikation. CSA-Material muss schnellstmöglich gelöscht anstatt massenhaft gesammelt werden. Auch deshalb ist die Idee des KI-Trainings mithilfe dieser Inhalte eine absurde Fehlentwicklung. In Erwägungsgrund 39 versucht die dänische Ratspräsidentschaft Grenzen einzuziehen, ohne jedoch zu negieren, dass das Ansammeln von CSA-Material für die technische Umsetzung der Aufdeckungsanordnungen erforderlich ist. Hinzu kommt, dass für Außenstehende keine Möglichkeit besteht zu überprüfen, nach welchen hinterlegten Inhalten tatsächlich gescannt wird (Erwägungsgrund 64).

Die vorgesehenen verpflichtenden Alterskontrollen stellen einen unverhältnismäßigen Eingriff in das Recht auf Internetnutzung Minderjähriger dar und wären mit dem Recht auf anonyme Internetnutzung nicht vereinbar (https://www.bundestag.de/resource/blob/935250/7ecae89c214ef74dc6e40bd922c854e9/Stellungnahme-Reda-data.pdf). Sie sind außerdem bei Open-Source-Software nicht durchsetzbar, ohne dabei das Open-Source-Ökosystem insgesamt zu zerstören. Auch der DSA fordert deshalb keine Verpflichtung zu Alterskontrollen, ebenso wenig wie die im Juli 2025 gefassten Leitlinien der EU dazu (https://netzpolitik.org/2025/jugendschutz-leitlinien-eu-kommission-gibt-klares-jein-zu-alterskontrollen/#netzpolitik-pw). Auch hier geht der Entwurf der CSA-Verordnung über ein geeignetes Maß hinaus. Viel sinnvoller wäre es, Artikel 28 des DSA auch im Sinne von mehr Kinderschutz vor sexualisierter Gewalt konsequenter als bisher durchzusetzen. Die in den Leitlinien genannten Maßnahmen zur Eindämmung suchtauslösender Elemente, für mehr Schutz vor Cybergrooming und für wirksame und kindergerechte Meldewege sind sinnvoll. Sie könnten erhebliche Verbesserungen bringen und die Plattformkonzerne stärker in die Haftung nehmen, wenn sie denn auch entschlossen durchgesetzt würden. Indem die Bundesregierung bis heute nicht genug Personal beim nationalen Digitale Dienste Koordinator (DSC-Coordinator) eingeplant hat, spart sie hier wieder einmal genau an der falschen Stelle. Nach wie vor sind nicht einmal die Hälfte der im Erfüllungsaufwand des Digitale Dienste Gesetz vorgesehenen Stellen geschaffen, geschweige denn besetzt.

Maßnahmen, die sexualisierte Gewalt gegen Kinder generell verhindern (und nicht erst die Verbreitung der Darstellungen davon begrenzen), müssen viel stärker angewendet und weiterentwickelt werden, denn das ist der effektivste Opferschutz. Soziale Ursachen, wie autoritär geprägte Beziehungen zu Kindern, die ungleichen globalen Besitzverhältnisse der kapitalistisch geprägten Weltordnung mit Folgen der Armutsmigration wie Prostitution von Minderjährigen und sexueller Gewalt gegen diese – seit einigen Jahren auch global vernetzt durch sexuelle Ausbeutung per Livestream – werden in der geplanten Verordnung gar nicht adressiert. Dazu fehlen beispielsweise Maßnahmen zur stärkeren Kontrolle auffälliger Finanztransaktionen, die auf kommerzielle sexuelle Ausbeutung von Kindern hindeuten (zum Beispiel Livestream Exploitation). Obwohl es dafür typische Transaktionsmuster gibt (https://www.nottingham.ac.uk/research/beacons-of-excellence/rights-lab/resources/reports-and-briefings/2023/october/payment-methods-and-investigation-of-financial-transactions-in-online-sexual-exploitation-of-children-cases.pdf), bleiben Geldinstitute lediglich zur Erkennung von Terrorismus, Geldwäsche und Betrug gesetzlich angehalten. Klar muss dabei auch werden, was Tätermotive sind, wofür mehr Forschung nötig ist. Die Missbrauchsbeauftragte der Bundesregierung Kerstin Claus stellte klar, dass das Motiv der Täter und auch Täte-

rinnen keineswegs nur Pädophilie als sexuelle Neigung sei, sondern vor allem die Auslebung von Macht, Machtmissbrauch, Dominanz und Verfügungsgewalt. Der „Lolita-Express“ von Jeffrey Epstein und Sextortion von „White Tiger“ sind nur zwei Beispiele dafür.

Die im Entwurf der CSA-Verordnung enthaltenen Netzsperren führen aufgrund der allgemein verbreiteten https-Verschlüsselung schnell zu Overblocking und gelten außerdem als unwirksam, um kriminell agierende Netzwerke zu bekämpfen. Deshalb hatte sich als bessere Alternative das Prinzip „Löschen statt Sperren“ eigentlich durchgesetzt. Das wiederholte Posting von CSAM-Material lässt sich durch Kontaktieren betreffender Server-Betreiber erreichen, auf denen diese Inhalte gespeichert sind. Dies ist relativ einfach möglich, weil die Inhalte in der Regel nicht im Darknet, sondern im Deep-Web gespeichert sind. Da die Inhalte passwortgeschützt abgelegt werden, sind sie dem Server-Betreiber meistens nicht bekannt. Der Betreiber nimmt Hinweise daher oft dankend an und löscht die CSA-Inhalte. Recherchen des NDR und des Spiegels zeigten die Wirksamkeit dieser Vorgehensweise bereits im Dezember 2021 auf (https://play.funk.net/channel/strgf-11384/paedoforen-warum-loescht-niemand-die-aufnahmen-strgf-1778317). Bis heute jedoch sucht das BKA proaktiv aber nicht nach CSAM-Material und nutzt die Möglichkeit der Löschaufforderung nicht (https://www.ndr.de/fernsehen/sendungen/panorama/aktuell/Kindesmissbrauch-Innenminister-lassen-weiter-nicht-aktiv-loeschen,imkmissbrauch100.html). Das zeigt auf, wie groß die ungenutzten Möglichkeiten sind, belastetes Material zu entfernen und die Täternetzwerke zu stören. Das geplante EU-Zentrum im CSA-Verordnungsentwurf soll Provider zum Löschen auffordern, ebenso wie zuständige Behörden (Erwägungsgrund 66). Das ist sinnvoll, aber dafür bedarf es des EU-Zentrums nicht, denn bei CSA-Material im Netz besteht kein Erkenntnis- sondern vor allem ein Vollzugsproblem.

Ein zweites für sich genommen sinnvolles Element im CSA-Verordnungsentwurf ist der geforderte Ausbau von Meldefunktionen bei CSA-Material. Dazu braucht aber keine neue Verordnung geschaffen werden, denn dies ist bereits im Digital Services Act (DSA) angelegt, der inzwischen in Kraft ist. Insbesondere zum Schutz vor Cyber-Grooming hält der DSA eine Anzahl Verpflichtungen der Plattformen etwa zu Meldesystemen und geschützten Umgebungen für Minderjährige bereit, die in der Praxis jedoch oft nicht eingehalten werden. Anstatt den DSA hinsichtlich des Kinderschutzes konsequent durchzusetzen, versäumt es die Bundesregierung, der Bundesnetzagentur die erforderlichen Personalstellen zur Aufsicht zuzuweisen. Im CSA-Verordnungsentwurf sind auch Maßnahmen zum besseren Erfahrungsaustausch und Vernetzung im Kampf gegen sexualisierte Gewalt beschrieben, diese könnten jedoch genauso auch von der parallel geplanten EU-Kinderschutzrichtlinie (siehe unten) umgesetzt werden, ebenso wie die von der dänischen Ratspräsidentschaft ergänzten Forderungen an Suchmaschinen, CSA-Material auszulisten. In der Summe können diese wenigen sinnvollen Elemente des CSA-Verordnungsentwurfs nicht ausreichen, um eine weitere Verfolgung dieses insgesamt hochgefährlichen Vorhabens weiter zu rechtfertigen.

Schon am 8. Juni 2022 haben sich mehr als 90 Grundrechtsorganisationen in einem offenen Brief an die EU-Kommission gewandt und darin gefordert, den Verordnungsentwurf in Gänze zurückzuziehen. Die Kritik aus Wissenschaft, Zivilgesellschaft, einigen Kinderschutzorganisationen reißt seither nicht ab. Auch die wissenschaftlichen Dienste des Bundestags kamen im Oktober 2022 zu der Einschätzung, dass die CSA-Verordnung weder geeignet, noch angemessen, erforderlich oder verhältnismäßig sei, und nicht mit den Grundrechten der EU-Grundrechtecharta vereinbar (https://www.bundestag.de/resource/blob/914580/WD-10-026-22-pdf.pdf). Besonders einhellig war dabei die Position der Sachverständigen bei der Anhörung zur CSA-Verordnung im Digitalausschuss des Bundestags am 1. März 2023 (https://www.bundestag.de/webarchiv/Ausschuesse/ausschuesse20/a23_digitales/Anhoerungen/932296-932296), wo selbst Markus Hartmann von der Stabsstelle Cybercrime Nordrhein-Westfalen umfassende Bedenken bezüglich des CSA-Verordnungsentwurfs äußerte (https://www.bundestag.de/resource/blob/935242/Stellungnahme-Hartmann.pdf). Zuletzt haben über 700 Wissenschaftler*innen (Stand September 2025) die geplante CSA-Verordnung in einem offenen Brief scharf kritisiert (https://netzpolitik.org/2025/offener-brief-hunderte-wissenschaftlerinnen-stellen-sich-gegen-chatkontrolle/). Die derzeitige Argumentation von Befürwortern der CSA-Verordnung, man brauche sie um wenigstens das freiwillige Scannen privater Kommunikation weiterhin zu erlauben, ist nicht plausibel. Sollte man der Auffassung sein, dies sei zielführend, könnte die dazugehörige Ausnahme-Verordnung von der e-Privacy-Richtlinie problemlos ein weiteres mal verlängert werden, zumal eine erneute Verlängerung ohnehin selbst dann geplant ist, wenn die CSA-Verordnung kommen sollte (Erwägungsgrund 78 des dänischen CSA-Verordnungsentwurfs). Ob das überhaupt sinnvoll wäre, ist nicht klar, da die EU-Kommission wiederholt daran scheiterte, die Verhältnismäßigkeit dieser Ausnahme zu belegen (https://netzpolitik.org/2023/bericht-eu-kommission-scheitert-verhaeltnismaessigkeit-der-freiwilligen-chatkontrolle-zu-belegen/). Das unsachliche Argumentationsniveau ist wenig überraschend, denn hinter der Einführung der CSA-Verordnung stehen auch ganz andere, rein ökonomische Interessen von potenziellen KI-

Anbietern verbunden mit Vertretern von Sicherheitsbehörden. Allein über die „Oak Foundation“ sollen mindestens 24 Mio € für Lobbyismus pro Chatkontrolle auf EU-Ebene investiert worden sein, wie Recherchen 2023 aufdeckten (https://netzpolitik.org/2023/anlasslose-massenueberwachung-recherchen-decken-netzwerk-der-chatkontrolle-lobby-auf/). Dass die Verletzung der e-Privacy-Richtlinie mit der CSA-Verordnung dauerhaft erlaubt werden soll (vgl. Artikel 1 Punkt 4), ist ohnehin als höchst fragwürdig anzusehen, und würde im übrigen die geplante e-Privacy-Verordnung verunmöglichen.

Viele sinnvolle Maßnahmen für mehr Schutz von Kindern vor sexualisierter Gewalt im Lichte der immer digitaleren Gesellschaft und KI-Nutzung finden sich hingegen in der geplanten EU-Richtlinie 2024/0035(COD) (https://data.consilium.europa.eu/doc/document/ST-6241-2024-INIT/de/pdf), die derzeit ebenfalls verhandelt wird. Dazu zählen an die technische Entwicklung angepasste Straftatbestände, die sich explizit auch gegen sexuelle Ausbeutung per Livestream, gegen Anleitungen zu Cybergrooming und gegen mit KI-Programmen generierte DeepFakes der sexualisierten Gewalt richten, bessere Opferhilfe durch Opferschutz und Meldesysteme, Präventionsprogramme für potenzielle Täter, bessere europäische Zusammenarbeit und auch verdeckte Ermittlungen durch die Polizei, etwa mittels sogenannter „Honeypots“. Auch diese Richtlinie muss entlang der Wahrung der Grundrechte verhandelt werden, sie bietet aber im Unterschied zum Entwurf der CSA-Verordnung einen geeigneten Rahmen, um besseren Schutz von Kindern vor sexualisierter Gewalt mit verhältnismäßigen Mitteln zu erreichen. Auf Bundesebene ist eine Umsetzung der geplanten EU-Kinderschutzrichtlinie unter anderem mit dem im Koalitionsvertrag angekündigten Digitale Gewaltschutzgesetz zu erwarten. Auch das im Januar 2025 vom Bundestag beschlossene Gesetz zur Stärkung der Strukturen gegen sexuelle Gewalt an Kindern und Jugendlichen (https://dip.bundestag.de/vorgang/gesetz-zur-st%C3%A4rkung-der-strukturen-gegen-sexuelle-gewalt-an-kindern/314885) war ein Schritt in die richtige Richtung und muss nun gut umgesetzt werden. Betroffenen Kindern kann nur geholfen werden, wenn ihre Probleme ernstgenommen werden und Eltern, Lehrkräfte und andere Beschäftigte mit Kontakt in soziale Nahfelder von Kindern für die Problematik sensibilisiert sind und gut damit umzugehen wissen – das ist gegenwärtig vielfach nicht ansatzweise der Fall. Anstatt auf gute Beratung und Hilfe, stoßen betroffene Kinder oft auf Misstrauen, Unwissen und Schuldzuweisungen. Neben Prävention braucht es auch eine Schwerpunktverlagerung der Polizeiarbeit auf diesen Bereich. Mit gezieltem Vorgehen kann es bei ausreichend zur Verfügung stehenden Ressourcen auch gelingen, ohne das technische Schwächen verschlüsselter Kommunikationsinhalte Täter zu identifizieren, die hinter Plattformen der sexualisierten Gewalt an Kindern stehen. Auf diese Weise konnten beispielsweise die Hintermänner der pädokriminellen Darknet-Plattform „Boystown“ identifiziert werden (https://netzpolitik.org/2025/ip-catching-die-ueberwachungs-massnahme-die-geheim-bleiben-soll/). Auch wenn die Rechtsgrundlagen beispielsweise für IP-Catching, Quick-Freeze und Login-Falle von IP-Adressen derzeit noch fehlen, könnten dies geeignete Maßnahmen sein, ebenso wie intelligente Analysen öffentlich zugänglicher Daten und Metadaten (Open Source Intelligence) und für besonders schwere Fälle auch der Einsatz verdeckter polizeilicher Ermittler*innen, das Einrichten von sogenannten Honeypots und sogenannte Timing-Analysen im Darknet. All diese Möglichkeiten der Strafverfolgung wären voraussichtlich wirksamer und dennoch weniger invasiv als die Chatkontrolle. Sie sind aber nicht Gegenstand der geplanten CSA-Verordnung. Auch deshalb ist diese als eine Fehlentwicklung zu bezeichnen und in Gänze abzulehnen.