Deutscher Bundestag
Ausschuss für Digitales

Ausschussdrucksache
zu 20(23)137

10.03.2023

Schriftliche Antworten auf Fragen des Bundestages im Vorfeld der Anhörung am 1. März

Ella Jakubowska, Senior Policy Advisor, European Digital Rights (EDRi)

27. Februar 2023

EDRi ist eine dynamische und resiliente Vereinigung von Nichtregierungsorganisationen, Experten, Anwälten und Akademikern, die sich der Verteidigung und Förderung digitaler Rechte auf dem gesamten Kontinent widmen. Sie ist seit fast zwei Jahrzehnten das Rückgrat der Bewegung für digitale Rechte in Europa.

1. Der Vorschlag der EU-Kommission zur CSA-Verordnung, auch bekannt als Chatkontrolle, hat seit seiner Veröffentlichung im Mai 2022 für viele Diskussionen gesorgt. Bitte erläutern Sie die technischen, juristischen, grundrechtlichen, datenschutzrechtlichen, sozialen und/oder gesellschaftlichen Implikationen des Vorschlags.

Nach Einschätzung von EDRi hat die Europäische Kommission einen Vorschlag vorgelegt, der im Falle seiner Verabschiedung wohl gegen verschiedene Rechte nach der Charta der Grundrechte der Europäischen Union, gegen das kürzlich verabschiedete Gesetz über digitale Dienste, die Datenschutzgrundverordnung (DSGVO) und das Verbot allgemeiner Überwachungspflichten verstoßen würde, das vom Gerichtshof der Europäischen Union (EuGH) wiederholt bestätigt wurde. Wir halten fest, dass der kommissionsinterne „Ausschuss für Regulierungskontrolle“ mehrere Vorbehalte gegen den Vorschlag geäußert hat, darunter auch Bedenken, der Vorschlag erkläre nicht ausreichend, wie das Verbot der allgemeinen Überwachung einzuhalten sei.[1] Auch der Menschenrechtskommissar der Vereinten Nationen äußerte dieselben Bedenken bezüglich allgemeiner Überwachung.[2]

Dieser Gesetzesentwurf würde zu einem in einer demokratischen Gesellschaft noch nie dagewesenen Ausmaß an allgemeiner staatlicher Überwachung der Internetaktivitäten von Menschen (ebenso durch private Akteure im Auftrag von Staaten) führen. Er würde Unternehmen dazu zwingen, Nutzer ihrer Dienste massenhaft zu durchsuchen, und zwar auf der Grundlage einer Bewertung des allgemeinen Risikoprofils einer Plattform oder eines Dienstes und nicht auf der Grundlage eines begründeten, individualisierten Verdachts gemäß rechtsstaatlichen Grundsätzen.[3]

---

[1] Die Stellungnahme des Ausschusses für Regulierungskontrolle der Kommission ist im Jahr 2022 nach außen gedrungen und führt mehrere Bedenken gegen den Vorschlag innerhalb der Kommission auf. EDRi, „Leaked opinion of the Commission sets off alarm bellings for mass surveillance of private communications“, 23. März 2022, verfügbar unter: https://edri.org/our-work/leaked-opinion-of-the-commission-sets-off-alarm-bells-for-mass-surveillance-of-private-communications/.

[2] UN Office for the High Commissioner for Human Rights, „Spyware and surveillance: Threats to privacy and human rights growing, UN report warnings“, 16. September 2022, verfügbar unter: https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report.

[3] Wir legen dar, wie grundrechts- und rechtsstaatskonforme Ermittlungen gegen sexuellen Kindesmissbrauch aussehen können. EDRi, „10 principles to defend children in the digital age“, 09. Februar 2022, verfügbar unter: https://edri.org/our-work/chat-control-10-principles-to-defend-children-in-the-digital-age/. [In deutscher Sprache unter: https://digitalegesellschaft.de/wp-content/uploads/2022/02/Chatkontrolle-10-Prinzipien.pdf]

Ferner wären im Falle verschlüsselter Dienste oder Plattformen diese gezwungen, Scantechnologien einzusetzen, die einer Spionage-Software gleichkommen. Darüber hinaus würden sich Ermittlungen in Fällen sexuellen Kindesmissbrauchs wohl eher verzögern und weniger wahrscheinlich zu Verurteilungen führen, und es bestünde ein hohes Risiko, dass sexuelle Ausdrucksformen Jugendlicher und LGBTQI+-Personen kriminalisiert werden, was auch das Recht auf freie Meinungsäußerung und Nichtdiskriminierung verletzen würde (siehe Antwort auf Frage 3).

Vertieft man die Kernfrage der Grundrechte, muss gemäß Artikel 52 der Charta der Grundrechte der Europäischen Union jede Grundrechtseinschränkung nachweislich notwendig und verhältnismäßig sein sowie ausreichende Garantien bieten. Verdächtigt die Polizei beispielsweise jemanden begründet des sexuellen Kindesmissbrauchs, ist es legitim, die Privatsphäre, den Datenschutz und bestimmte andere Rechte der verdächtigten Person einzuschränken, solange man ein ordnungsgemäßes Verfahren einhält.

Die Europäische Kommission bestreitet nicht, dass die vorgeschlagene EU-Verordnung gegen sexuellen Kindesmissbrauch einschneidende Maßnahmen vorsieht, die einen Eingriff in die Grundrechte darstellen würden, einschließlich des Rechts auf Privatsphäre, Datenschutz und freie Meinungsäußerung der Internetnutzer. Die Schlüsselfrage ist somit, ob das vorgeschlagene Ausmaß dieser Grundrechtseingriffe zu rechtfertigen ist. Die Schwere des Straftatbestands des sexuellen Kindesmissbrauchs und die Verpflichtung zum Schutz von Kindern sind sehr wichtig, jedoch bedeuten selbst schwere Straftaten gemäß EU-Recht nicht, dass ein Staat jede Maßnahme um jeden Preis ergreifen kann.

Diese Maßnahmen kann man unterschiedlich bewerten. Erstens: Um nachzuweisen, dass das vorgeschlagene Gesetz notwendig und verhältnismäßig ist, darf es keinen weniger tiefen Eingriff geben. Wie ich in meiner Antwort auf Frage 3 erläutern werde, gibt es zahlreiche weniger einschneidende Optionen, die die EU verfolgen könnte. Zweitens sind Wirksamkeit und Effizienz dieser Maßnahmen durch objektive Beweise zu untermauern, was in der Folgenabschätzung der Kommission nicht der Fall ist.

Drittens muss die Abwägung der Grundrechte zeigen, dass der Eingriff in diese Rechte verhältnismäßig und nicht übermäßig schädlich ist. Die Analyse der EDRi zeigt, dass der Vorschlag einen schwerwiegenden Eingriff in die Grundrechte potenziell aller Internetnutzer bilden würde, indem er ihnen die unerlässliche digitale Sicherheit und Privatsphäre vorenthält, die zur Verwirklichung eines breiten Spektrums ihrer wirtschaftlichen, sozialen, kulturellen und politischen Rechte unabdingbar ist. Dies gilt unabhängig davon, ob sie der Kontaktaufnahme zu Kindern mit Missbrauchsabsicht („Grooming“) oder der Verbreitung von Darstellungen sexuellen Kindesmissbrauchs (CSAM) verdächtigt werden, oder ob sie das Internet lediglich aus legitimen und rechtmäßigen Gründen nutzen (wie die meisten Internetnutzer). Das liegt daran, dass es keine Möglichkeit gibt, Aufdeckungsanordnungen wirklich gezielt zu erlassen.

Daher hat sich die Kommission ihrer Beweislast nicht entledigt, die Notwendigkeit und Verhältnismäßigkeit der Grundrechtseinschränkungen durch die vorgeschlagene CSA-Verordnung zu begründen. Dieser Nachweis ist wesentlicher Teil der EU-Gesetzgebung, und es beschädigt unsere gemeinsamen EU-Werte, wenn die Kommission einen Vorschlag vorlegt, der in dieser Hinsicht so lückenhaft ist. Dies unterstreicht die Forderung der EDRi an die gesetzgebenden Organe, den Vorschlag abzulehnen und die Europäische Kommission aufzufordern, einen Gesetzesentwurf vorzulegen, der mit EU-Recht vereinbar ist und der Bedeutung der Bekämpfung sexuellen Kindesmissbrauchs gerecht wird. Unsere Empfehlung an die Kommission, das Gesetz zurückzuziehen, wird von 123 weiteren zivilgesellschaftlichen Gruppen mitgetragen, darunter Organisationen für digitale Rechte von Kindern, für die Stärkung von Frauen und Mädchen, für die Unterstützung von

Opfern, ferner Rechtsanwälte, Befürworter quelloffener Software und Medienfreiheit sowie Organisationen für digitale Rechte.[4]

2. Der Vorschlag der Kommission sieht vor, dass Aufdeckungsanordnungen ergehen sollen, die dazu führen, dass Anbieter*innen von Kommunikationsdiensten oder Geräten verdeckt Informationen ausleiten müssen, sofern der Verdacht besteht, dass über diese Dienste oder Geräte Missbrauchsmaterial ausgetauscht wird oder auf diesen Grooming stattfindet. Welche Dienste und Geräte sind aus Ihrer Sicht davon potenziell und in welcher Reichweite betroffen und welche Auswirkungen hat dies auf deren Nutzer*innen?

Anbieter im Sinne der Aufdeckungsanordnungen sind alle „Anbieter von Hostingdiensten" oder „interpersonellen Kommunikationsdiensten", die in der EU tätig sind (Artikel 7 Absatz 1). Diese weit gefassten Begriffe schließen Social-Media-Plattformen, Online-Foren/Chatseiten, Spiele-Websites mit Chat-Funktionen, Anbieter von Cloud-Diensten, File-Sharing-Dienste, Messaging-Apps, Dating-Apps und so weiter ein. Aufgrund des weiten Geltungsbereichs wären nur Einzelpersonen ausgenommen, die einen Dienst vollständig selbst hosten und betreiben (z. B. eine Person mit eigenem E-Mail-Dienst und -Server für rein private Zwecke), während eine Person, die einen E-Mail-Server und -Dienst für ihre Arbeit oder als kostenloses Open-Source-Projekt hostet, unter diese Vorschriften fallen würde. Wir gehen davon aus, dass kleinere Anbieter sowie Anbieter kostenloser und quelloffener Software (manchmal auch als FOSS / FLOSS bezeichnet) sehr stark betroffen wären, da von ihnen erwartet wird, dass sie die gleichen Regeln einhalten wie große Unternehmen. Dies könnte zu einer weiteren Machtkonzentration bei den großen Technologiekonzernen führen, die Vorschriften leichter einhalten können, was zudem die Schaffung und Nutzung von FOSS/FLOSS erschweren könnte.

Die Auswirkungen auf Nutzer wären sehr weitreichend, aber um ein Beispiel zu nennen: Ein verschlüsselter Nachrichtendienst könnte gemäß Artikel 7-11 (Aufdeckungsanordnungen) gezwungen werden, entweder die Nachrichten seiner Nutzer zu durchsuchen (was unweigerlich den Einsatz von Client-Side-Scanning, CSS, bedeuten würde), die Verschlüsselung aufzugeben, die er seinen Nutzern versprochen hat, oder den EU-Markt zu verlassen. WhatsApp und Signal haben beide zu Protokoll gegeben, sich aus Ländern zurückziehen zu wollen, wo ihre Verschlüsselung gefährdet wäre. Im Ergebnis könnten die Europäer keinen Zugang zu sicheren und privaten Messaging Services mehr haben – was für Journalisten, Whistleblower, Menschenrechtsaktivisten, Politiker, Menschen auf der Suche nach medizinischer Versorgung, religiöse Gemeinschaften, LGBTQI+-Personen, Opfer häuslicher Gewalt/von Gewalt in der Partnerschaft (einschließlich Stalking mit häufig digitaler Komponente) und Angehörige von Minderheiten ein besonderes Risiko birgt.

3. Wieso ist der Kommissionsvorschlag Ihrer Meinung nach geeignet oder nicht geeignet, Kinder effektiv vor (sexuellen) Übergriffen und der Verbreitung von Missbrauchsmaterial zu schützen und wo sehen Sie konkreten Handlungsbedarf?

Bedauerlicherweise ist der Vorschlag der Kommission aus mehreren Gründen nicht geeignet, Kinder vor sexuellem Missbrauch zu schützen, und könnte die Bekämpfung von CSAM sogar noch erschweren:

1. Derzeit werden mehr als 90 % des CSAM von Kinderschutz-Hotlines (die deutsche Hotline heißt eco-Beschwerdestelle) innerhalb weniger Tage aus dem Internet entfernt. Kinderrechts- und Kinderschutzgruppen sind sich einig, dass die zügige Entfernung von CSAM aus dem Internet unmittelbar nach der Identifizierung oberste Priorität für den Schutz der Überlebenden hat. Die

[4] EDRi, „European Commission must uphold privacy, security and free expression by withdrawing new law, say civil society", 08. Juni 2022, verfügbar unter: https://edri.org/our-work/european-commission-must-uphold-privacy-security-and-free-expression-by-withdrawing-new-law/.

vorgeschlagene CSA-Verordnung sieht allerdings ein kompliziertes und bürokratisches Melde- und Reaktionssystem vor, bei dem es mehrerer Monate bedarf, um mit der Entfernung von Inhalten oder auf den Verdacht auf Grooming zu reagieren. Dieser lange Zeitraum bedeutet nicht nur, dass die Opfer warten müssen und gefährdet sind, sondern auch, dass, wenn dann endlich auf Meldungen reagiert wird, die Originaldaten aufgrund der Vorschriften zur Vorratsdatenspeicherung wohl schon gelöscht wurden. Dadurch wird es wahrscheinlich schwieriger, Verurteilungen der Täter zu erwirken.

2. Zudem weist der Vorschlag den Hotlines, die derzeit wichtige Kinderschutzarbeit leisten, keine formale Rolle zu, obwohl sie bislang nur unsicher finanziert und in vielen Mitgliedstaaten mit nur wenigen Mitarbeitern ausgestattet sind. Wie ich in verschiedenen nachfolgenden Antworten erläutern werde, scheint die vorgeschlagene Rolle des EU-Zentrums die wesentliche Funktion dieser Meldestellen zu überschatten, anstatt ihre wichtige Arbeit zu unterstützen.

3. Wie in meiner Antwort auf Frage 4 näher erläutert, ist damit zu rechnen, dass Falschmeldungen das gesamte System verstopfen (das macht es zur Suche nach der Nadel im Heuhaufen), dass heißt, es gibt weniger Aufmerksamkeit und Ressourcen für echte CSA-Fälle, und es wird viel Zeit für die Untersuchung von Falschmeldungen verschwendet.

4. Wir sind ferner besorgt, dass die sexuelle Selbstdarstellung Jugendlicher durch den Vorschlag kriminalisiert wird. In sechs EU-Mitgliedstaaten ist es für Jugendliche ab einem bestimmten Alter rechtlich zulässig, einvernehmlich intimes Material (z. B. Nackt-Selfies, „Sexts“) zu teilen. Gemäß CSA-Verordnung würden solche Inhalte jedoch – wenngleich auf nationaler Ebene rechtmäßig – als CSAM gelten. Von einem Anbieter gemeldet, müssten sie von einem Moderator geprüft, dann an das EU-Zentrum und anschließend an die nationalen Strafverfolgungsbehörden zu Ermittlungen weitergeleitet werden. Dies bedeutet: Einvernehmliche und rechtmäßige intime Bilder Jugendlicher könnten zwar routinemäßig mit mehreren Personen geteilt werden, doch könnte gegen junge Menschen ermittelt werden, nur weil sie ihre sexuelle Identität erkunden. Das Risiko ist speziell für LGBTQI+-Jugendliche hoch, die sich oft besonders auf digitale Hilfsmittel verlassen, um ihre sexuelle Identität auszudrücken. In Ländern mit systematischer LGBTQI+-Diskriminierung können die Risiken für queere Menschen durch die Offenlegung ihrer sexuellen Aktivität und ihrer sexuellen Selbstdarstellung eine Frage der physischen Sicherheit sein.

5. Wie in der Antwort zu Frage 9 näher erläutert, kann die allgemeine Überwachung der digitalen Aktivitäten junger Menschen ihre Entwicklung und freie Meinungsäußerung sehr beeinträchtigen und ihnen sichere Online-Räume und sogar Möglichkeiten vorenthalten, bei Missbrauch Hilfe zu suchen.

6. Auch die Sexualerziehung ist wohl von der angestrebten Grooming-Erkennung betroffen. Die schwedische Hilfsorganisation für Sexualaufklärung und reproduktive Rechte (RFSU) berichtete uns, dass es üblich ist, wichtige Informationen zur sexuellen Gesundheit über verschlüsselte Nachrichten auszutauschen, insbesondere wenn junge Menschen keinen leichten Zugang zu solcher Aufklärung haben. Die in der CSA-Verordnung vorgeschlagene Erkennung von Grooming würde wohl jeden Erwachsenen, der einem Jugendlichen Sexualerziehung oder Informationen über LGBTQI+-Themen anbietet, zum CSA-Täter machen, was für Sexualerziehung eine starke Abschreckungswirkung hätte.

Angesichts der Schwere und des Ausmaßes dieser Risiken für die CSA-Bekämpfung und der Schäden für Jugendliche und Erwachsene kommt EDRi zu dem Schluss, dass Änderungen nicht ausreichen, um diesen Vorschlag a. wirksam und b. grundrechtskonform zu machen. Den Mitgliedstaaten empfehlen wir nachdrücklich, die vielfältigen alternativen Optionen zu verfolgen, die ihnen bereits zur Verfügung stehen und in vielen Fällen sehr viel schneller umsetzbar sind als beispielsweise die vorgeschlagenen Rechtsvorschriften:

- Die Umsetzung des kürzlich verabschiedeten Gesetzes über digitale Dienste, auf das sich die europäischen gesetzgebenden Organe geeinigt haben, um gegen alle Formen von illegalem Material im Internet wie CSAM vorzugehen. Insbesondere der neue Mechanismus für Meldungen und Maßnahmen sowie das System der vertrauenswürdigen Hinweisgeber werden sich günstig auf die Entfernung von CSAM aus dem Internet auswirken
- Die Reform der EU-Richtlinie zur Bekämpfung des sexuellen Missbrauchs von Kindern aus dem Jahr 2011 – eine Rechtsvorschrift zur Bekämpfung des sexuellen Kindesmissbrauchs in den EU-Mitgliedstaaten, deren Umsetzung so mangelhaft war, dass die Europäische Kommission gegen mehrere nicht-konforme Mitgliedstaaten ein Vertragsverletzungsverfahren einleiten musste.
- Investitionen in die nationalen Hotlines, wie hier bereits angesprochen
- Gewährleistung, dass sämtliche Plattformen und Dienste in der EU eine klare, zugängliche und kinderfreundliche Möglichkeit bieten, mutmaßliche CSAM zu melden, und dass die Notdienste über ausreichende Ressourcen für rasche und wirksame Reaktionen verfügen.
- Verfolgung ehrgeiziger sozialer Reformen, meist auf nationaler Ebene, u. a. in den Bereichen sozialstaatliche Maßnahmen, Armutsbekämpfung, soziale Dienste, Polizeireform und Justizreform
- Auseinandersetzung mit den gesellschaftlichen Faktoren, die CSA begünstigen, einschließlich schädlicher Geschlechternormen in Bezug auf Frauen und Mädchen und allgemeiner Fragen sozialer Ungleichheit
- Gewährleistung einer einheitlichen Überprüfung des Strafregisters, Schulung und Sensibilisierung für Anzeichen von CSA für alle, die mit Kindern und Jugendlichen arbeiten
- Aufstockung der Forschungsmittel und -kapazitäten für die Prävention sowie zügige Umsetzung von Präventionsmethoden, um Verbrechen im Zusammenhang mit CSA zu verhindern, bevor Kinder Schaden nehmen. Die US-amerikanischen *Centers for Disease Control and Prevention* (CDC) erklären, dass zahlreiche wirksame oder zumindest vielversprechende Präventionsstrategien zwar bekannt sind, weltweit jedoch kaum erprobt oder umgesetzt werden.[5]

4. Wie schätzen Sie die Gefahr ein, dass unbescholtene Bürger*innen durch falsch-positive automatisierte Erkennung unter Verdacht geraten, und was würden solche Falsch-Positiv-Meldungen für Auswirkungen sowohl auf die Verdächtigten als auch die Ermittlungsbehörden haben?

Falsche Warnmeldungen und ihre Folgen sind höchst schädlich. Laut einer Untersuchung der EDRi-Mitglieder ICCL und DRI in Irland handelte es sich bei mindestens 10 % der bei der irischen Polizei eingegangenen CSAM-Meldungen um Falschmeldungen, wobei die tatsächliche Zahl wohl viel, viel höher ist.[6] Bei Hunderten dieser Meldungen stellte sich heraus, dass es sich um legitime Aktivitäten handelte: darunter von Erwachsenen ausgetauschte einvernehmliche intime Inhalte, und Familien, die am Strand oder in der Badewanne spielten.

Die irische Polizei bestätigte zwar die Unschuld der Betroffenen, behielt deren personenbezogenen Daten jedoch ein. Dies wird derzeit noch untersucht, aber es dürfte sich als unrechtmäßige Datenspeicherung erweisen. Die Folgen von Falschmeldungen können vom Ausschluss vom digitalen Leben (etwa dem dauerhaften Verlust von Zugriffsmöglichkeiten auf alle Fotos und E-Mail-Konten)

[5] CDC, „Fast Facts: Preventing Child Sexual Abuse“, 6. April 2022, verfügbar unter: https://www.cdc.gov/violenceprevention/childsexualabuse/fastfact.html.
[6] EDRi, „A Safe Internet for All“, Oktober 2022, verfügbar unter: https://edri.org/wp-content/uploads/2022/10/EDRi-Position-Paper-CSAR.pdf, Seite 53.

über ungerechtfertigte polizeiliche Ermittlungen bis hin zum Verlust von Kindern, Arbeitsplätzen und dem Tod von Menschen reichen.

Der Vorschlag stützt sich auf bestimmte auf künstlicher Intelligenz (KI) gründende „Indikatoren" zur Erkennung neuer CSAM- und Grooming-Fälle, Indikatoren, die zwar mit einem gewissen Grad an Genauigkeit Merkmale wie nackte Haut oder eine geschätzte Altersgruppe einer Person erkennen lassen, was aber nicht dasselbe ist wie die Erkennung von CSAM. So sind beispielsweise sehr viele online ausgetauschte Fotos und Videos mit nackter Haut rechtmäßig und legitim. KI-Systeme haben keinen gesunden Menschenverstand – sie werden nie zuverlässig zwischen rechtmäßigen Inhalten und CSAM unterscheiden können. Somit ist eine sehr große Anzahl von Fehlalarmen unvermeidlich.

Mit dem durch die CSA-Verordnung geschaffenen System würden jedoch alle Warnmeldungen zunächst an das EU-Zentrum und dann an die nationalen Strafverfolgungsbehörden weitergeleitet, es sei denn, sie wären als CSAM „offensichtlich unbegründet" (z. B. ein falsches Bild eines Hundes, das niemand als CSAM ansehen würde). In einigen Mitgliedstaaten ist die Polizei verpflichtet, diesen Meldungen nachzugehen – wobei die bereits unterfinanzierten Polizeibehörden in Deutschland und den Niederlanden erklären, nicht in der Lage zu sein, die große Menge an Falschmeldungen zu bearbeiten, die nach diesem Vorschlag eingehen würden.[7]

5. Anbieter von Hosting-Diensten und Anbieter interpersoneller Kommunikationsdienste, die eine Aufdeckungsanordnung erhalten haben, sollen laut Artikel 10 CSAM-E Technologien installieren und betreiben, die die Kontaktaufnahme zu Kindern mit Missbrauchsabsicht („Grooming") erkennen. Sind Ihnen Technologien bekannt, die verlässlich zwischen unbedenklicher, sexuell oder romantisch aufgeladener Kommunikation und Grooming unterscheiden können?

Nein, mir sind keine Technologien bekannt, die dies zuverlässig leisten könnten. Grooming ist für erfahrene Sozialarbeiter und Polizeibeamte nur schwer zu erkennen, und es gibt nur wenige Verurteilungen wegen Grooming, weil es schwierig ist, Grooming nachzuweisen.

6. Welche technischen Ansätze halten Sie für effektive und grundrechtlich unbedenkliche Alternativen zu den im Verordnungsentwurf vorgesehenen Maßnahmen?

Von Entwicklern und Anwendern der Technologien hören wir oft, dass ihre Systeme oder Methoden die Antwort auf komplexe gesellschaftliche Probleme sein können. Natürlich ist die Realität viel differenzierter, und technologische Lösungsansätze werden bestenfalls ein kleines Puzzleteil einer viel größeren Gesamtheit von Ansätzen sein können, die sich auf Bildungs-, Gesellschafts-, Polizei- und Justizreformen richten.

Dort, wo Technologie eine unterstützende Rolle spielen kann, sind die einfacheren Alternativen allgemein folgende: Wie zu Frage 3 erörtert, etwa die Verpflichtung der Anbieter, einen leicht erreichbaren und kinderfreundlichen Melde-Button einzurichten – eine einfache, aber wirkungsvolle Lösung.

Man kann auch andere Ideen rund um die Befähigung und Teilhabe der Benutzer*innen verfolgen, was der Empfehlung des *Child Rights International Network* (CRIN) entsprechen würde, dass die beste Möglichkeit, die online-Sicherheit junger Menschen zu gewährleisten, darin bestehe, dafür zu sorgen, dass sie angemessen ausgebildet sind, dass sie ihre Wirkmächtigkeit in Online-Räumen erleben (anstatt überwacht zu werden oder sich zu fürchten, was vernünftigem Verhalten abträglich

[7] Tweede Kamer, „Europese Verordening ter voorkoming en bestrijding van seksueel kindermisbruik", 04. Oktober 2022, verfügbar unter: https://debatgemist.tweedekamer.nl/node/29579, und Deutschland Funk, „Sexueller Kindesmissbrauch: Wie Ermittler im Internet vorgehen", 20. Oktober 2022, verfügbar unter: https://www.deutschlandfunk.de/strafverfolgung-sexueller-kindesmissbrauch-datenschutz-100.html.

ist) und dass sie vertrauenswürdige Erwachsene haben, an die sie sich wenden können, wenn sie etwas für nicht in Ordnung halten.

Es gibt ferner vielversprechende Untersuchungen zu Methoden des Kinderschutzes ohne Massenüberwachung in Online-Umfeldern, etwa das Projekt *Fortnite Undercover Avatar* der Kinderschutzgruppe *L'Enfant Bleu* in Zusammenarbeit mit der französischen Polizei.[8] Dabei wurden kreative Methoden eingesetzt, um „herkömmliche" polizeiliche Ermittlungsarbeit und Kinderpsychologen in digitalen Räumen zusammen zu bringen, und es gelang, 1200 gefährdeten Kindern in weniger als zwei Monaten zu helfen. Bei 400 dieser Kinder wurde anschließend festgestellt, dass sie „akut" von Missbrauch bedroht waren. Wegen fehlender Mittel wurde das Projekt eingestellt, aber es zeigt, was erreicht werden kann, wenn wir Zeit und Mittel an den richtigen Stellen aufwenden.

7. Der Vorschlag der Kommission enthält u.a. die Forderung nach einer verpflichtenden Altersverifikation. Wo genau und unter welchen Voraussetzungen müssten Internetnutzer*innen nach diesem Vorschlag ihr Alter verifizieren und welche technischen Ansatzpunkte gibt es oder werden gerade erforscht, um eine Altersverifikation grundrechtskonform unter Wahrung der Anonymität der Nutzer*innen im Internet umzusetzen?

In den Artikeln 3 und 4 wird eine Altersüberprüfung für Anbieter von sozialen Medien, von Cloud-, E-Mail-, Chat-/Nachrichten- und anderen Hosting- und Diensten zur interpersonellen Kommunikation vorgeschrieben, die ein Grooming-Risiko auf ihren Plattformen festgestellt haben. Bei dieser Formulierung des Vorschlags dürfte jeder Anbieter, der keine Altersüberprüfung vornimmt, als risikobehaftet gelten, da der Vorschlag eine umfassende Altersüberprüfung vorschreibt. Können Anbieter nicht nachweisen, dass sie das Risiko auf nahezu Null gesenkt haben, könnten sie mit einer Aufdeckungsanordnung und anschließend mit einer Geldstrafe von bis zu 6 % des Umsatzes belegt werden.

Uns sind keine Methoden zur Altersverifizierung bekannt, mit denen die Anonymität der Nutzer gewahrt würde und die rechtskonform wären. Alle uns derzeit bekannten Methoden sind mit Risiken für Privatsphäre und Datenschutz verbunden und stellen ein besonderes Risiko für Menschen dar, deren Arbeit, Sicherheit und/oder Teilhabe am demokratischen Leben von der Anonymität im Internet abhängt. Verschiedene bekannte Methoden bergen zudem ein hohes Risiko, die digitale Ausgrenzung bereits schutzloser Bevölkerungsgruppen zu verschärfen, insbesondere von Menschen ohne Papiere, Roma und Sinti sowie älteren Menschen, da sie ihnen den Zugang zu digitalen Diensten effektiv verwehren.

8. Der Vorschlag der Kommission würde es ermöglichen, private Kommunikationsdienste zu Aufdeckungsanordnungen zu verpflichten, u.a. um Inhalte aus privaten und verschlüsselten Chats zu erlangen (u.a. Client-Side-Scanning), um Grooming zu erkennen oder das Alter zu verifizieren; als Folge des technologieneutralen Ansatzes sind potenziell auch Netzsperren denkbar. Welche internationalen Konsequenzen würden solche Möglichkeiten, das Nutzer*innenverhalten zu analysieren, oder den Zugang zu Online-Inhalten und sicheren Räumen zu beschränken, zeitigen – insbesondere im Hinblick auf eine höhere Gefahr rechtswidriger Eingriffe (Hacking) in die Privatsphäre europäischer Bürger*innen aus dem Ausland und im Hinblick darauf, dass autoritäre Staaten die EU-Regeln als Blaupause für illegitime Überwachungsmaßnahmen ohne rechtsstaatliche Einhegung nutzen?

[8] Europol, „Europol Excellence Award in Innovation", undatiert, verfügbar unter: https://www.europol.europa.eu/media-press/newsroom/news/europol-excellence-award-in-innovation.

Ich würde meinen, dass der Vorschlag der Kommission nicht technologieneutral ist; es ist ganz klar absehbar, dass er sich auf die Verschlüsselung auswirken wird, und dass den Anbietern keine andere Wahl bleibt, als *Client-Side-Scanning* (CSS) zu nutzen. Denn um auf den Inhalt einer verschlüsselten Nachricht zugreifen zu können, muss eine Art Eintrag in die Nachricht gemacht werden.

Der Einsatz von CSS gelang noch nie in großem Maßstab, und die mit der Bewertung verschiedener CSS-Methoden beauftragte Expertengruppe der Europäischen Kommission kam zu dem Schluss, dass selbst bei den drei besten CSS-Methoden die Durchführbarkeit, der Schutz der Privatsphäre und die Sicherheit gering bzw. mittelmäßig sind (so die Folgenabschätzung). Da die Folgenabschätzung die Wirksamkeit des Vorschlags belegen soll, ist es sehr bedenklich, dass ihre Schlussfolgerungen wiederholt falsch dargestellt wurden.

Hinzu kommt der Aufschrei von Cybersicherheits-, Technologie- und Datenschutz-Fachleuten weltweit, die alle bestätigen, dass CSS weder sicher noch auf eine Weise realisierbar ist, die die Grundrechte respektiert.

Und ist CSS erst einmal auf dem Gerät einer Person installiert, ist es wie eine Hintertür, durch die jeder eindringen kann: Stalker, böswillige Staaten, Hacker, Kinderschänder oder andere böswillige Akteure. Es wäre gelinde gesagt grotesk, würde der Block, der die Datenschutz-Grundverordnung (DSGVO) geschaffen hat und derzeit Regeln zur Verbesserung der Cybersicherheit entwickelt, ein noch nie dagewesenes Massenüberwachungsgesetz auf den Weg bringen, das die Privatsphäre und die Sicherheit der gesamten Internet-Welt schwächen würde.

9. Zuletzt hat das „Child Rights International Network“ in einer Studie die Bedeutung unterstrichen, „das Framing von Privatsphäre versus Kinderschutz hinter uns [zu] lassen, um die Rechte aller Kinder zu schützen“ (Berichterstattung bei netzpolitik.org vom 02.02.2023). Wie verhält sich der aktuelle EU-Kommissionsvorschlag zu dem Recht von Kindern und Jugendlichen auf Privatsphäre und sichere IT-Systeme und welche kurzfristigen und langfristigen Konsequenzen hätte der Kommissionsvorschlag im Hinblick darauf?

Der Kommissionsvorschlag analysiert gründlich das Recht von Kindern, von sexuellem Missbrauch und Ausbeutung unbehelligt zu sein, doch weder berücksichtigt noch bewertet er ihre Rechte auf Selbstdarstellung, informationelle Selbstbestimmung (Zugang zu Informationen) oder Autonomie im Internet. Dem Kommissionsvorschlag zufolge wäre das Internet ein sehr gefährlicher Ort für Minderjährige, und das bedeutet: Die von der Kommission in der Folgenabschätzung vorgenommene Grundrechtsabwägung ist unzureichend. Das Europäische Parlament hat diese Unzulänglichkeit erkannt und einen unabhängigen Berater beauftragt, Teile der Folgenabschätzung der Kommission neu zu erstellen, um allen Gefahren für die Grundrechte besser Rechnung zu tragen.

In dem Vorschlag werden weder junge Menschen als legitime Internetnutzer anerkannt, noch der Wert digitaler Kommunikation und Communities für die Suche nach Unterstützung (insbesondere für Opfer und psychische Gesundheit) und für die Entwicklung ihrer Autonomie. Sowohl UNICEF als auch die UN betonen die Bedeutung digitaler Räume für junge Menschen und warnen vor Maßnahmen, die eine allgemeine Überwachung ihrer Internetnutzung darstellen würden.[9] Und wie Alexander Hanff, Opfer und Überlebender von Missbrauch, erklärt, kann die Überwachung der Gespräche von

[9] United Nations, „General comment No. 25 (2021) on children’s rights in relation to the digitial environment“, 2021, verfügbar unter: https://digitallibrary.un.org/record/3906061?ln=en und UNICEF, „Children’s online privacy and freedom of expression toolkit“, Mai 2018, verfügbar unter: https://sites.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf.

Überlebenden diese demoralisieren und sie letztlich davon abhalten, sich zu melden und ihren Missbrauch anzuzeigen.[10]

10. Welches politische Maßnahmenpaket ist aus Ihrer Sicht ganzheitlich erfolgversprechend, um wirksam, effektiv und grundrechtskonform gegen sexualisierte Gewalt an Kindern vorzugehen – wo besteht Nachsteuerungs- und Verbesserungspotenzial im Bereich der Prävention und bei der Bekämpfung von sexualisierter Gewalt und deren Darstellung im Internet?

Angenommen wir würden sämtliche Bedenken gegen die vorgeschlagene CSA-Verordnung beiseiteschieben, selbst dann wäre eine „perfekt funktionierende" CSA-Verordnung immer noch kein ausreichendes Mittel gegen sexuellen Kindesmissbrauch. Denn der Vorschlag versucht, nur ein Symptom des abscheulichen Verbrechens von Kindesmissbrauch zu bekämpfen (in diesem Fall die Rolle von Online-Vermittlern bei der Verbreitung von CSAM und Grooming), jedoch ohne die üblen gesellschaftlichen Wurzeln des Problems anzugehen – deshalb besteht die einzige wirklich wirksame Maßnahme in der Prävention; nur so lässt sich verhindern, dass Kinder überhaupt geschädigt werden. In den meisten Fällen würde die CSA-Verordnung erst dann greifen, wenn Missbrauch bereits stattgefunden hat. Dies hängt auch mit dem Problem der Rechtsgrundlage der vorgeschlagenen CSA-Verordnung zusammen, genauer gesagt der Harmonisierung des Binnenmarktes: Auf eben dieser Grundlage präsentiert die EU die Lösung für die Verbreitung von CSAM als wirtschaftliches und unternehmerisches Problem – und nicht als ein gesellschaftliches.

Wir haben die Literatur über Empfehlungen zur Prävention von Kindesmissbrauch, die die Grundlage für die Empfehlungen in der Antwort zu Frage 3 bildet, umfassend recherchiert. Aus Platzgründen sind die vollständigen Referenzen und Ergebnisse des Literaturüberblicks auf Anfrage erhältlich.

11. Erfasst der Vorschlag der EU-Kommission alle Plattformen im Internet, auf denen kinderpornographisches Material verbreitet werden kann, zielgerecht, oder in welcher Form besteht möglicherweise Nachbesserungsbedarf mit Blick auf den Geltungsbereich?

Im Gegenteil, der Geltungsbereich des Vorschlags ist sehr weit gefasst – er schließt nicht nur die typischen Social-Media-Unternehmen und -Apps ein, an die man denken mag, sondern auch E-Mails, Cloud-Infrastruktur-Anbieter, Anbieter von Telefon- und SMS-Diensten und sogar Einzelpersonen, die einen kleinen Server betreiben, etwa im Auftrag von Arbeitskollegen. Bei angemessenen Verpflichtungen der Anbieter wäre dieser breite Geltungsbereich vielleicht kein Problem (es wäre vernünftig, von allen Anbietern zu erwarten, dass sie vertretbare Schritte und Maßnahmen ergreifen, um das Missbrauchsrisiko auf ihren Plattformen oder Diensten zu verringern). Doch sind die vorgeschlagenen Maßnahmen nicht zumutbar, was bedeutet, dass der breite Geltungsbereich sehr problematisch ist.

12. Sind Instrumente zur besseren Strafverfolgung und Rechtsdurchsetzung hinreichend im Vorschlag der EU-Kommission gewürdigt worden, wo besteht möglicherweise Verbesserungsbedarf und welche Instrumente wären dazu notwendig?

Nein, das ist nicht der Fall – es gibt dringenden Verbesserungsbedarf bei Strafverfolgung und Strafvollzug, was eher auf der Mitgliedstaatenebene in Angriff genommen werden sollte. Insbesondere ist eine Justiz- und Polizeireform notwendig, die in Kenntnis der Traumaproblematik und aus der Perspektive der Überlebenden realisiert werden sollte. Das heißt: Man sollte von der Sicht der Überlebenden darauf ausgehen, wie Gerechtigkeit aussieht und wie sie hergestellt werden

[10] Alexander Hanff, „Why I don't support privacy invasive measures to tackle child abuse", 11. November 2020, verfügbar unter: https://www.linkedin.com/pulse/why-i-dont-support-privacy-invasive-measures-tackle-child-hanff.

kann, einschließlich der Konsultation Überlebender sowie aller anderen einschlägigen Akteure entsprechend ihrer Expertise. Siehe Antwort zu Frage 3 für weitere Informationen über das Gesetz über digitale Dienste und die Richtlinie zur Bekämpfung des sexuellen Missbrauchs von Kindern von 2011, die die nationalen Bemühungen stützen können.

13. Wird das neue EU-Zentrum die nationalen Strafverfolgungsbehörden und Europol, laut der aktuellen Planungen, angemessen unterstützen können, und welche Ausstattung würde es dazu benötigen?

Ich glaube nicht, dass das EU-Zentrum in der Lage wäre, die nationalen Strafverfolgungsbehörden in angemessener Weise zu unterstützen. Ein EU-Zentrum ist zwar prinzipiell kein Problem, aber sein Aufgabenbereich sollte drastisch beschränkt und auf Aufklärung, Prävention und die Unterstützung von Meldestellen für die Arbeit an vorderster Front ausgerichtet werden (siehe Antwort auf Frage 3). Und es müsste völlig unabhängig von Europol sein.

14. Umfasst der Vorschlag der EU-Kommission aus Ihrer Sicht alle technischen Ansätze, mit denen das Ziel, dem Schutz von Kindern gerecht zu werden, erreicht werden kann, und welche weiteren technischen Ansätze wären aus Ihrer Sicht erforderlich?

Technologischen Ansätzen sind immer Grenzen gesetzt. Ich empfehle, „einfache“ technische Maßnahmen (z. B. verbindliche Buttons für Meldungen, Kontrollfunktionen für Anwender) zu pfüfen, bevor stärker eingreifende Technologien in Betracht gezogen werden, und gesellschaftlichen – insbesondere präventiven – Maßnahmen stets Vorrang einzuräumen. Da Kinderschutzgruppen zufolge 80-90 % der Missbrauchsfälle von jemandem begangen werden, der den Opfern bekannt ist, liegen die Vorteile systematischer Überprüfungen des Strafregisters, früheren polizeilichen Eingreifens (z. B. dass Überlebenden geglaubt wird, wenn sie sich melden, was sich als strukturelles Problem erwiesen hat) und anderer nicht-technischer Maßnahmen auf der Hand.

15. Der Verordnungsentwurf sieht auch die Möglichkeit von Netzsperren einzelner URLs vor, die im Zuge der bisherigen Entwurfsänderungen während der tschechischen Ratspräsidentschaft sogar noch ausgeweitet werden sollen. Halten Sie es angesichts der weit verbreiteten https-Verschlüsselung von URL-Abrufen für technisch möglich, einzelne URLs gezielt zu sperren, ohne auf die Sperrung ganzer Domains zurückzugreifen, wenn ja, auf welche Weise soll dies möglich sein und wenn nein, können Netzsperren auf diese Weise den Anforderungen des europäischen Gerichtshofs an die Zielgerichtetheit von Netzsperren genügen?

Nein, unseres Erachtens bedeutet die weit verbreitete Verwendung von https, dass Internetdienstanbieter gezwungen wären, ganze Domains zu sperren, um eine Sperranordnung umzusetzen. Um zum Beispiel eine Wikipediaseite wegen des Verdachts auf CSAM zu sperren, müsste die gesamte Wikipedia gesperrt werden, was nicht den Anforderungen an eine gezielte Sperrung entspräche.

16. Wie bewerten Sie die Rolle und den Charakter des laut EU-Verordnungsentwurf geplanten EU-Zentrums einerseits mit Blick auf die Wahrnehmung primär präventiver Aufgaben und andererseits mit Blick auf Aufgaben, die die Entwicklung und den Einsatz technischer Überwachungswerkzeuge betreffen?

Es wird praktisch kaum über die präventiven Aufgaben des EU-Zentrums informiert, jedoch wird die gesamte CSA-Verordnung als präventive Rechtsvorschrift dargestellt – was nicht den Methoden und Modellen des Vorschlags entspricht. Entwicklung und Einsatz technischer Überwachungsinstrumente durch das EU-Zentrum sind im Zusammenhang mit einer Verordnung, die den Einsatz gefährlicher Instrumente fördert, immer problematisch. Soll eine koordinierte EU-Einrichtung zum Schutz von

Kindern eine Rolle bei der Nutzung von Kinderschutztechnologien spielen, wäre es wichtig, dass der Europäische Datenschutzausschuss sowie unabhängige Datenschutz- und Sicherheitsexperten die Aufsicht übernehmen. Außerdem wäre ein hohes Maß an Transparenz zu gewährleisten.

17. Wenn nicht die Endgeräte, sondern die mit ihnen mögliche Kommunikationen („Chats“) durchsucht würden, gälte das auch für eine Ende-zu-Ende-Verschlüsselung etwa von Messenger-Diensten. Auch hier gerieten ungezählte gesetzestreue Bürger ins Visier der Behörden, nur weil sie einen bestimmten Dienst mit entsprechender Software nutzen. Sind Ihnen Software-Lösungen bekannt, die das Echtzeit-Mitlesen oder zumindest das Knacken Ende-zu-Ende-verschlüsselter Kommunikation erlauben? Halten Sie es für vertretbar, die grundgesetzlich garantierte vertrauliche private Kommunikation durch Algorithmen aufzuheben?

Jede Software-„Lösung“ mit Echtzeit-Entschlüsseln oder -Auslesen verschlüsselter Kommunikation verstößt *per definitionem* gegen Grundprinzip und Wesen der Ende-zu-Ende-Verschlüsselung. Es ist so, als würde man in die Wohnung einer Person eindringen, ihr beim Schreiben eines Briefes über die Schulter schauen und behaupten, dies sei akzeptabel, weil man den Umschlag nicht geöffnet hat. Das ist nach wie vor eine nicht hinnehmbare Verletzung der Privatsphäre (außer bei begründetem, individuellem Verdacht gegen den Betreffenden), und daran kann keine noch so große technische Errungenschaft etwas ändern.

Ob durch Algorithmen oder andere Methoden: Der Bruch der Vertraulichkeit privater Kommunikation ist nur dann zu rechtfertigen, wenn ein begründeter Verdacht auf eine Straftat besteht, die schwer genug ist, um dieses Eindringen zu rechtfertigen. Dies ist nicht nur verfassungsrechtlich, sondern auch in der Charta der Grundrechte der Europäischen Union festgelegt und vom EuGH durchgesetzt.

18. Im Verordnungsentwurf heißt es, das zu gründende Zentrum für Fragen des sexuellen Kindesmissbrauchs in Den Haag solle verbindliche Indikatoren für Abbildungen sexuellen Missbrauchs liefern, die von den scannenden Unternehmen anzuwenden seien. Nun wissen erfahrene Ermittler, dass es keineswegs eindeutig zu definieren und im Einzelfall zu belegen ist, aufgrund welcher Kriterien was als Familienfoto, als selbstdokumentiertes Spiel unter Kindern und Jugendlichen, als Zufallsschnappschuss einer Sportveranstaltung oder eben als Kinderpornografie zu gelten hat. Gibt es bereits Erkenntnisse über das methodische Vorgehen des genannten EU-Zentrums? Und falls ja, kann dieses Vorgehen gegebenenfalls als verlässlich und geeignet eingeschätzt werden?

Ich stimme dem voll und ganz zu; siehe meine Antwort auf Frage 3 für weitere Hinweise zum Unvermögen KI-gestützter Tools, solche Unterscheidungen zu treffen. Es gibt kaum Informationen darüber, wie die Kommission dies vorsieht. Felix Redas auf die Informationsfreiheit gestützter Antrag von 2022 zeigte jedoch erneut, dass sich die Kommission auf ungeprüfte Behauptungen von Technologieanbietern über die Funktionsweise ihrer Technologien stützt.[11] Nach der dem Kommissionsvorschlag beigefügten Folgenabschätzung halte ich es für wahrscheinlich, dass die Kommission für das EU-Zentrum plant, Software von Thorn/Safer zu verwenden. Thorn ist eine Non-Profit-Organisation und stellt die kostenlose Scantechnologie des in den USA ansässigen

[11] Siehe *Ask The EU*, „Technologies for the detection of new CSAM referenced by Commissioner Johansson“, ab dem 08. August 2022, verfügbar unter: https://www.asktheeu.org/en/request/technologies_for_the_detection_o.

kommerziellen Unternehmens Safer zur Verfügung. Sowohl Thorn als auch Safer werden von Ashton Kutcher geleitet.[12]

Für weitere Informationen wenden Sie sich bitte an: Ella.Jakubowska@edri.org

[12] Netzpolitik.org, „Dude, where's my privacy? How a Hollywood star lobbies the EU for more surveillance", 12. Mai 2022, verfügbar unter: https://netzpolitik.org/2022/dude-wheres-my-privacy-how-a-hollywood-star-lobbies-the-eu-for-more-surveillance/.