CSA-Verordnung: Ein feministischer Blick auf die „Chatkontrolle“

Elina Eickstädt und Elisa Lindinger

Der Entwurf der EU-Kommission „Zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern“, auch bekannt als CSA-Verordnung oder Chatkontrolle, steht seit Mai 2022 massiv in der Kritik der Zivilgesellschaft. Die Debatte macht häufige Leerstellen und Fehlannahmen digitalpolitischer Gesetzgebungen sichtbar.

Die Grenzen des Tech-Solutionismus

Klar ist: Die Erstellung und die Verbreitung von Kindesmissbrauchsdarstellungen (*child sexual abuse material, CSAM*) müssen aktiv bekämpft werden. Doch die CSA-Verordnung greift dafür zu kurz. Denn sie sieht lediglich eine Reihe an technischen Lösungen vor. Das ist insofern problematisch, als dass auf nicht genau definierte, noch zu erfindende Technologien gesetzt wird, anstatt bestehende, erfolgreiche Strukturen des Kinderschutzes und deren Ausbau in den Blick zu nehmen. So werden technische Innovationen gegenüber sozialer Intervention, Unterstützung und Empowerment priorisiert.

Ein solches Vorgehen kann und muss als Tech-Solutionismus kritisiert werden. Tech-Solutionismus bezeichnet die Annahme, dass jedes Problem mithilfe technischer Neuerungen gelöst werden kann. Doch diese Ansicht ist nicht nur verkürzt. Sie blendet zudem aus, dass durch die Einführung komplexer neuer technischer Systeme auch neue Probleme entstehen. Besonders deutlich wird das am Beispiel algorithmischer Entscheidungssysteme: Die CSA-Verordnung sieht vor, dass auf diesem Weg automatisiert rechtswidrige Inhalte erkannt und an Strafverfolgungsbehörden weitergeleitet werden. Wie genau jedoch die Erkennung technisch erfolgen soll, darüber schweigt sich der Entwurf aus – er bleibt „technologieneutral“. Dabei ist das automatisierte Melden von Inhalten ein komplexeres Problem, als man vielleicht von außen annehmen würde. Schon heute zeigen andere Anwendungsfälle, dass solche Algorithmen bei der Kommunikation unterrepräsentierter Gruppen überdurchschnittlich häufig anschlagen, und das ohne inhaltliche Grundlage. Die technische Lösung setzt letztendlich also gesellschaftliche Diskriminierung fort, macht sie aber gleichzeitig scheinbar objektiv und damit weniger angreifbar. Naiver Tech-Solutionismus blendet aus, dass technische Lösungen immer

nur so neutral sein können, wie die Gruppe, die sie schafft, und die Daten, auf denen sie basiert.

Auch ignoriert die Rede von einfachen und sauberen technischen Lösungen, dass häufig dennoch ein hohes Maß an menschlicher Intervention nötig ist. Auch wenn die CSA-Verordnung hier Melde- und Prüfstrukturen in Form eines EU-Centers vorsieht, ist es wahrscheinlich, dass große Tech-Konzerne zunächst auf bestehende Content-Moderationsstrukturen zurückgreifen und Meldungen intern überprüfen, bevor sie Verdachtsfälle an das EU-Center melden. Content-Moderator*innen arbeiten unter hohem, zeitlichem Druck und sind täglich psychisch extrem belastenden Inhalten ausgesetzt. Die CSA-Verordnung wird für einen massiven Ausbau dieses hochproblematischen Berufsfeldes sorgen, ohne jedoch die notwendigen Arbeitsschutzmaßnahmen mitzudefinieren. Dabei existieren bereits Vorschläge, wie die Arbeitsbedingungen verbessert werden müssten.

Der Bruch von verschlüsselter Kommunikation ist keine Option

Die CSA-Verordnung sieht vor, jegliche interpersonelle Kommunikation zu scannen. Das betrifft alle möglichen digitalen Kommunikationskanäle – Messenger ebenso wie Chats auf Spieleplattformen, in Lern-Apps oder Ähnliches. Auch Anwendungen, die die Kommunikation zwischen den Gesprächsteilnehmenden verschlüsseln und daher als besonders sicher gelten, sind nicht ausgenommen. Das heißt: Eine wirklich Ende-zu-Ende verschlüsselte Kommunikation wäre nicht mehr möglich. Denn die Prüfung fände nicht nur im konkreten Verdachtsfall statt, sondern ständig und überall. Denn Verschlüsselung ist binär: Sie ist entweder intakt und von keiner Instanz ohne weiteres auszuhebeln, oder sie ist unterbrochen und damit von allen Seiten angreifbar.

Vor der im Impact Assessment der Verordnung vorgeschlagenen Technologie des Client-Side-Scanning warnen sogar internationale IT-Sicherheitsexpert*innen und der Hohe Kommissar der Vereinten Nationen für Menschenrechte. Denn bei diesem Verfahren werden Dateien vor der eigentlichen Verschlüsselung auf dem Gerät der Nutzer*innen auf illegales Material untersucht und bei Verdacht ausgeleitet. Nutzer*innen verlieren damit jegliche Kontrolle über die Vertraulichkeit ihrer Kommunikation. Aber Privatsphäre ist ein Grundrecht. Das deutsche Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme schützt unsere persönlichen Daten und unsere privaten Kommunikationen, die digital gespeichert oder verarbeitet werden. Präventive Eingriffe in diesen Schutzraum sind mit hohen Hürden verbunden und immer nur anlassbezogen, also bei konkretem Verdacht, zulässig.

Die CSA-Regulierung führt dazu, dass solche Schutzräume faktisch nicht mehr existieren dürfen und kontinuierlicher maschineller und menschlicher Überwachung unterzogen werden.
Dabei ist das Recht auf Privatsphäre gerade für ältere Kinder und Jugendliche essenziell. Ab dem Alter von rund 10 Jahren fordern Kinder und Jugendliche mehr Privatsphäre ein, während sie gleichzeitig risikofreudiger werden – online wie offline. Eigene Erfahrungen zu sammeln und sich von Autoritäten abzunabeln ist ein zentraler Entwicklungsschritt im Erwachsenwerden, der älteren Kindern und Jugendlichen nicht vorenthalten werden darf (vgl. Wisniewski et al. 2022). Privatsphäre zu untergraben und Verschlüsselung technisch unmöglich zu machen, sendet ein fatales Signal: "On one hand, adults tell teens that they need to care about their online privacy to stay safe; on the other hand, as designers and parents, we develop and use surveillance technologies that take teens' privacy away for the sake of their online safety." (Wisniewski et al. 2022, 319)

Doch nicht nur Kinder und Jugendliche haben ein Recht auf Privatsphäre – auch durch Verschlüsselung –, das es zu schützen gilt. Angehörige benachteiligter Gruppen, Journalist*innen, Whistleblower*innen und Anwälte
sind am meisten von Überwachung und Machtmissbrauch durch staatliche und andere Kontrollstellen betroffen und deshalb besonders auf intakte Verschlüsselung ihrer Kommunikation angewiesen. Ist diese erst einmal ausgehebelt, sind der Repression Tür und Tor geöffnet. In ganz Deutschland wurden über in Polizeidienststellen über Jahre hinweg illegal personenbezogene Daten abgerufen, ohne dass dies aufgefallen wäre. Wenn nun eine technische Möglichkeit geschaffen wird, Kommunikationsinhalte automatisiert zu durchsuchen und auszuleiten, kann das auch für völlig andere Zwecke genutzt und missbraucht werden.
Die CSA-Verordnung priorisiert das Recht auf Schutz vor Gewalt (UN-Kinderrechtskonvention Artikel 19) gegenüber dem Recht auf Privatsphäre. Diese zentralen Rechtsgüter gegeneinander abzuwägen, die eigentlich zusammen gedacht und umgesetzt werden müssen, sorgt lediglich für plakative Forderungen und verhärtete Fronten.

Nicht nur für die CSA-Regulierung gilt, dass neue Policy-Vorschläge, Verordnungen und Richtlinien Grundrechte schützen müssen, statt sie auszuhebeln. Der Koalitionsvertrag der Bundesregierung sieht vor, ein Recht auf Verschlüsselung einzuführen. Ein solches Recht steht in direktem Widerspruch zum durch das Impact Assessment der CSA-Verordnung vorgesehenen Client-side Scanning. Um einen effektiven Schutz von verschlüsselter Kommunikation zu gewährleisten, müsste Technologien wie Client-side Scanning verboten werden.
Diese verschlüsselte Kommunikation de facto global auszuhebeln, ist ein Dammbruch im Bereich der Kommunikationssicherheit, dessen Folgen nicht mehr rückgängig gemacht werden können.

Nicht vorhandene Technologien sind keine gute Basis für Gesetze

Die CSA-Verordnung macht keine klaren Vorgaben dazu, mit welchen konkreten Technologien die Maßnahmen umgesetzt werden sollen. Die Verantwortung für deren Auswahl und Entwicklung wird stattdessen auf die Plattform-Betreiberfirmen abgewälzt. Was dort technologisch geleistet werden soll, ist jedoch umfangreich und komplex. Zum einen sind einige Tatbestände noch gar nicht ausreichend definiert, um tatsächlich zielführende technologische Erkennungsverfahren entwickeln zu können (zum Beispiel die Kontaktaufnahme mit Missbrauchsabsicht zu Kindern und Jugendlichen, das sogenannte Gooming). Zum anderen weisen bereits bestehende algorithmische Erkennungsverfahren, beispielsweise für Hate Speech, deutliche Schwächen auf, Kontext zu erkennen und richtig zu bewerten. Die CSA-Verordnung setzt also auf nicht vorhandene Technologien, um ihre Vorgaben umzusetzen.

Hinzu kommt: Auch wenn theoretisch alle Kommunikationsanbieter*innen und Plattformbetreiber*innen eigene technische Lösungen für die Umsetzung der CSA-Verordnung entwickeln können, sind solche Vorhaben teuer und faktisch nur von den größten Firmen, wie Microsoft, Alphabet oder Apple oder durch Einbindung spezialisierter externer Firmen zu bewältigen. Das hat zwei konkrete Folgen, die in starkem Kontrast zu allen anderen Regulierungsansätzen der EU stehen:
Die Tech-Konzerne, deren Übermacht die EU mühsam versucht zu regulieren und einzugrenzen, erhalten einen völlig neuen Gestaltungsspielraum, – und zwar das offizielle Mandat, hochinvasive, grundrechtseinschränkende Technologien zu erschaffen und einzusetzen. Die Schieflage des digitalen Marktes wird weiter verstärkt, Big Tech baut seine Vormachtstellung weiter aus.
Bessere Lösungen als die von Big Tech haben kaum eine Möglichkeit, sich durchzusetzen. Hochspezialisierte Firmen, die Kommunikation überwachen, gehören zu den stärksten Befürwortern der CSA-Verordnung. Ihre Behauptungen, wie wirksam ihre Technik heute sei, finden sich (unüberprüft) in den politischen Entwürfen der EU wieder.

Feministische Digitalpolitik als Antwort

Der derzeitige Entwurf der CSA-Verordnung steht in vielfachem Konflikt mit intersektionalen feministischen Perspektiven. Sie verstärkt Machtungleichheiten, sie institutionalisiert paternalistisches Verhalten gegenüber Heranwachsenden, sie lässt die Bedürfnisse anderer bedrohter Gruppen in ihrer Betrachtung völlig außen vor.

Feministische Digitalpolitik hinterfragt kritisch, ob der Einsatz von Technologien tatsächlich zielführend ist, und sucht nach nachhaltigen Lösungen, um Probleme an der Wurzel zu fassen. Der Einsatz von Technologien als Mittel staatlicher und privatwirtschaftlicher Überwachung ist – selbst zu Schutzzwecken – ultimativ paternalistisch. Die CSA-Verordnung setzt darauf, Kinder und Jugendliche

maschinell abzuschirmen, statt sie mithilfe von Aufklärung und Empowerment zu stärken. Was im Übrigen – im Gegensatz zur CSA-Verordnung – auch im Hinblick auf Übergriffe im nahen Umfeld hilfreich wäre. Gesellschaftliche Probleme lassen sich nicht rein technisch lösen. Soziale Handlungsansätze müssen im Vordergrund stehen, um wirklich wirksam zu sein.

Zu einer feministischen digitalpolitischen Perspektive gehört auch die Nichtverhandelbarkeit von Grundrechten. Das Recht auf Privatsphäre, das von der Bundesregierung geplante Recht auf Verschlüsselung und das Recht auf Schutz vor Gewalt dürfen nicht gegeneinander ausgespielt werden. Sie alle sind essenziell für die gesellschaftliche und demokratische Teilhabe aller, insbesondere von unterrepräsentierten Gruppen und nicht zuletzt von Jugendlichen und Heranwachsenden selbst.

Damit der rechtlich vorgeschriebene Einsatz von Technologien bestehende Probleme nicht verschleiert oder neue Herausforderungen schafft, müssen Policy-Entwürfe einer kontextuellen, gesellschaftlichen Folgenabschätzung unterzogen werden. Die Vergangenheit zeigt, dass solche Folgenabschätzungen meist auf rechtlicher oder technischer Ebene enden. Um wirklich nachhaltige, ethisch vertretbare Lösungen zu schaffen, müssen aber auch gesellschaftliche und wirtschaftliche Faktoren einbezogen werden. Zudem muss die technische Implementierung kritisch begleitet und iterativ analysiert werden. Denn gerade bei technologieoffenen Verordnungen ist unklar, welche Lösungen entwickelt werden. Die Aufgabe des Gesetzgebers ist es deshalb umso mehr, eine Grundlage zu schaffen, die klare rote Linien für ethisch und juristisch hochproblematische Technologien festlegt.

Die CSA-Verordnung zeigt, in welchem komplexen Verhältnis gesellschaftliche Probleme und potenzielle digitale Lösungen zueinander stehen, und wie schnell Tech-Solutionismus unbeabsichtigte negative Folgen mit sich bringt. Es gehört zur Verantwortung von Gesetzgeber*innen, solche Komplexitäten zu erfassen und maßgeschneiderte, zielführende Lösungsansätze zu entwickeln, die negative Auswirkungen minimieren.

SUPERRR Lab
Oranienstr. 58 A
10969 Berlin
https://superrr.net/

Bald mehr auf https://feministtechpolicy.org/