Stellungnahme an den Ausschuss für Digitales zur CSA-Verordnung (“Chatkontrolle”)

Elina Eickstädt

Chaos Computer Club

23. Februar 2023

Contents

Vorbemerkung

Der Gesetzesvorschlag der EU-Kommission zur Bekämpfung von Kindesmissbrauch verfolgt grundsätzlich ein wichtiges Ziel. Zweifelsohne muss den Betroffenen von Kindesmissbrauch besser geholfen werden und die Verbreitung von dokumentiertem Kindesmissbrauch unterbunden werden. Der Gesetzesvorschlag sieht jedoch Maßnahmen vor, die eine Überwachung aller Kommunikationsinhalte bedeuten würden und fundamentale Prinzipien von vertraulicher, sicherer digitaler Kommunikation untergraben. In ihrer derzeitigen Form würde die Verordnung eine nie da gewesene Überwachungsinfrastruktur schaffen, die weder grundrechtskonform noch technisch realisierbar ist. Der Verordnungsentwurf ist ungeeignet, das erklärte Ziel zu erreichen, und würde in der Praxis neue Probleme für die Strafverfolgung aufwerfen, statt zielgerichtet und effektiv schwerwiegende Straftaten zu bekämpfen. Technologie kann stets nur ein unterstützendes Werkzeug für die Lösung komplexer gesellschaftlicher Probleme sein. Diese Stellungnahme geht zunächst die technischen Grundlagen für die Umsetzung der von der Verordnung geforderten Aufdeckungsanordnungen ein. Des Weiteren werden Konsequenzen für die Privatsphäre aller Bürgerinnen sowie die Gefahren der vorgeschlagenen Altersverifikation aufgezeigt. Im letzten Abschnitt wird die technisch unrealistische Umsetzung von Netzsperren, sowie die problematische Rolle des geplanten EU-Centers beschrieben. Grundsätzlich machen wir darauf aufmerksam, dass mit dem Digitale-Dienste-Gesetz (DSA) bereits ein rechtlicher Rahmen besteht, der diverse Maßnahmen zum besseren Schutz von Kindern vorsieht. Eine konsequente Umsetzung des DSA könnte bereits einen großen Anteil der von der Kommission genannten Probleme lösen.

Vorgesehene Maßnahmen und technische Umsetzung

Im Kern zielt die Verordnung darauf ab, alle Inhalte interpersoneller Kommunikation (soziale Medien, Chatdienste, aber auch Hosting und Cloud-Anbieterinnen) zu scannen, unabhängig von einem konkreten Verdacht. Insbesondere sieht der Gesetzesvorschlag Pflichten zur Aufdeckung von bekanntem Material, unbekanntem Material, das Kindesmissbrauch dokumentiert sowie Anbahnungsversuchen, dem sogenannten Grooming, vor.

Aufdeckung von bekanntem Material

Das Erkennen von bekanntem Material erfolgt durch sogenanntes *Perceptual Hashing*. Es gibt bereits unterschiedliche Implementationen dieser Technologie, z. B. das von Microsoft entwickelte *PhotoDNA*. Meta nutzt die *PDQ-Hash*-Funktion und Apple die *NeuralHash*-Funktion. Den *„Hash"* eines Bildes kann man sich vorstellen wie einen Fingerabdruck. Es wird ein Bild in den Algorithmus eingespeist. Dieser berechnet auf Basis unterschiedlicher Merkmale eine bildspezifische Prüfsumme. Da die *Hashes* basierend auf unterschiedlichen Merkmalen des Bildes erstellt werden, wird auch bei kleinen Änderungen der gleiche *Hash* erzeugt, so dass relevantes Bildmaterial relativ zuverlässig gefunden werden kann. Der Abgleich von kurzen Fingerabdrücken ist weniger aufwendig

als der Abgleich gegen ein vollständiges Bild. Außerdem muss so keine zentrale Datenbank von CSAM vorgehalten werden, sondern lediglich die *Hashes*, dies reduziert mögliches Missbrauchspotential.

Auch wenn diese Technologie grundsätzlich als sehr zuverlässig betrachtet werden kann, gibt es zwei wesentliche Nachteile, die bedacht werden müssen. Zum einen ist eine Datenbank nötig, die zentralisiert gepflegt werden muss. Die Verwalterin der Datenbank hat die Entscheidungsgewalt darüber, welche Bilder erkannt und ausgeleitet werden. Dies bietet Missbrauchspotential. Zusätzlich ist die *Perceptual-Hashing*-Methode nicht vollkommen fehlerfrei. Harmlose Bilder können so manipuliert werden, dass sie einem als "illegal" markierten Bild entsprechen. Dies ermöglicht es Angreiferinnen, für eine Ausleitung von Bildern zu sorgen, ohne Kontrolle über die Datenbank zu haben.[1]

Aufdeckung von unbekanntem Material

Die Verordnung ist zwar vermeintlich technologieneutral gehalten, aus dem mit der Verordnung veröffentlichen *Impact Assessment* geht aber sehr klar hervor, dass auf sog. künstlicher Intelligenz (KI) basierende Systeme zum Einsatz kommen sollen. Für das Erkennen von unbekanntem Material werden Filtersysteme vorgeschlagen, die auf KI oder Machine Learning (ML) basieren. Hierfür wird ein sogenanntes Machine-Learning-Modell mit bereits bekanntem Material "trainiert". Dieses Modell kann dann mit einer bestimmten Gewissheit neues Material erkennen. Für das Training dieser Modelle ist eine große Menge an Daten notwendig, sowohl von bestätigtem illegalen Material als auch legalem Material. Es ist davon auszugehen, dass die Ressourcen für die Entwicklung solcher Modelle nur bei großen Konzernen vorhanden sind. Gerade im Bereich der Inhaltsmoderation führt dies immer wieder zu Intransparenz, da große Unternehmen die entwickelten Modelle als Geschäftsgeheimnis einstufen. Dieses Vorgehen würde also die Vormachtstellung der großen Tech-Konzerne weiter stärken. Für Nutzerinnen ist nicht ersichtlich, auf welcher Basis Entscheidungen getroffen werden. Auch hier haben wir es mit einer Technologie zu tun, deren Fehlerrate im einstelligen Prozentbereich liegt. Bei 1 Million geprüften Bildern und mit einer niedrig angesetzten Fehlerquote von 1% würden bereits 10.000 Falschmeldungen zu tun, diese müssten dann entsprechend durch Anbieter oder das EU-Center gesichtet werden. Um dafür zu sorgen, dass es nicht zu diversen zehn- oder hunderttausenden Falschmeldungen pro Tag kommt, setzen große Unternehmen bereits jetzt Content-Moderatorinnen zum Vorsortieren ein. Somit würden private, vertrauliche Bilder zunächst durch viele Hände gehen, auch wenn sie zu Unrecht vom Algorithmus identifiziert und gemeldet wurden. Der Einsatz von KI im Zusammenhang mit hoch vertraulicher Kommunikation bringt mehr Risiken mit sich, als dass er das eigentliche Problem löst.

[1] Adversarial Detection Avoidance Attacks: Evaluating the robustness of perceptual hashing-based client-side scanning - https://arxiv.org/abs/2106.09820

Aufdeckung von Anbahnungsversuchen (Grooming)

Zum Aufdecken von Grooming ist eine detaillierte Analyse aller Texte in Chats notwendig. Das bedeutet: Jede einzelne Nachricht muss vor oder während des Versands auf verdächtige Muster geprüft werden. Der Versuch z.B. mithilfe von Schlagwörtern Hassrede oder Extremismus auf sozialen Plattformen zu moderieren, führt regelmäßig dazu, dass Inhalte zu Unrecht blockiert werden. Denn Schlagwörter nehmen noch längst keine kontextuelle Einordnung vor. Anders als beim Erkennen von bereits bekanntem Bildmaterial ist das Erkennen von Grooming weitaus komplexer. Bei der Inhaltsmoderation von Texten ist eine kontextuelle Einordnung unerlässlich, um eine grundrechtskonforme Umsetzung zu gewährleisten.

Inzwischen sind die Technologien zur Inhaltsmoderation wesentlich weiterentwickelt, bergen aber ähnliche Gefahren. Zum Erkennen von illegalen Inhalten kommt sogenanntes Natural Language Processing zum Einsatz. Auch hier kommt Machine Learning zum Einsatz. Diesmal wird das Modell nicht mit bekannten Bildern trainiert, sondern mit bekannten Posts, Nachrichten oder Sprachmustern, die häufig in Groomingfällen Anwendung finden. Aber auch hier sind die Fehlerraten enorm, bei rein textbasierten Analysen liegen sie bei 5-10%. [2] Am Tag werden ungefähr 10 Mrd. Textnachrichten in der EU versendet, das bedeutet, wir hätten es mit bis zu 1 Mrd. Chats zu tun, die fälschlich ausgeleitet werden.[3] Auch hier müsste es wieder eine menschliche Intervention geben und private, nicht strafbare Inhalte würden durch viele Hände gehen, bevor sie als unbedenklich markiert werden würden.

Alle drei Methoden sind nicht vollkommen fehlerfrei [4][5]. Nutzerinnen würden dauerhaft mit dem Wissen leben, dass alle geteilten Inhalte, egal ob Text oder Bild, eventuell bei Moderatorinnen oder Strafverfolgungsbehörden landen. Das Wissen darüber, ständig unter Beobachtung zu stehen, hat enorme Auswirkungen darauf, wie man sich als Nutzerin äußert – bis hin zur Selbstzensur (*Chilling-effect*). Aktuelle Fälle zeigen, dass, selbst wenn sich das Material als fälschlich markiert herausstellt, Anbieterinnen betroffene Accounts häufig dauerhaft sperren bzw. das Wiederherstellen von Accounts häufig sehr lange dauert und mit großen Anstrengungen verbunden ist. [6]

Gefahren für private, vertrauliche Kommunikation

Die oben genannten technischen Werkzeuge beziehen sich lediglich auf die Detektion von Material im Allgemeinen. Der Gesetzesentwurf sieht eine Aufdeckung

[2] ExtremeBB: Enabling Large-Scale Research into Extremism, the Manosphere and Their Correlation by Online Forum Data - https://arxiv.org/pdf/2111.04479.pdf

[3] Chat Control or Child Protection? - https://arxiv.org/abs/2210.08958

[4] Analyse Zuverlässigkeit Perceptual Hashing - https://www.hackerfactor.com/blog/index.php?/archives/2022/10/03.html

[5] ExtremeBB: Enabling Large-Scale Research into Extremism, the Manosphere and Their Correlation by Online Forum Data - https://arxiv.org/pdf/2111.04479.pdf

[6] Fälschlicherweise verdächtigter Vater verliert zugriff auf Google Konten - https://www.nytimes.com/2022/08/21/technology/google-surveillance-toddler-photo.html

in jeglicher interpersoneller Kommunikation und Hosting-Diensten vor. Dies umfasst öffentlich einsehbare Plattformen, private und geschäftliche Cloud-Speicher, aber auch für private und vertrauliche Kommunikation genutzte Chatdienste wie z. B. Signal, WhatsApp, Threema oder E-Mail. Diensteanbieter, die Ende-zu-Ende-Verschlüsselung anbieten, könnten dazu gezwungen werden, Technologien anzuwenden, die die Verschlüsselung brechen oder unterwandern. Es ist festzuhalten, dass folgende Bedingungen zu erfüllen sind, wenn wir vertrauenswürdige Kommunikation gewährleisten wollen:

- Das eigene Gerät muss integer sein und darf Inhalte nicht an Dritte ausleiten.
- Die Verschlüsselung muss sicher sein, sodass wir dem Netz, gemeint sind hier Internet-Abieter und ähnliche Akteure, nicht vertrauen müssen.

In der mit dem Gesetzesvorschlag veröffentlichten Folgeabschätzung [7] zeigt sich, welche Technologien für die Umsetzung angedacht sind. Es wird vorgeschlagen, das "Prüfen von Material mittels vollständigen *Hashing* auf dem Gerät mit Abgleich auf dem Server" vorzunehmen. Das *Hashing* wird mit den oben genannten beschriebenen Methoden durchgeführt. Für das Prüfen von Material in verschlüsselter Kommunikation wird das so genanntes Client-Side-Scanning genannt.

Client-Side-Scanning Beim Client-Side-Scanning (CSS) handelt es sich um eine neue Technologie, die es Strafverfolgungsbehörden und Sicherheitsbehörden ermöglicht, Verschlüsselung zu umgehen. Anders als bei früher vorgeschlagenen Lösungen erhalten die Behörden keinen Schlüssel für eine Hintertür. CSS findet direkt auf dem Gerät statt und führt eine Analyse aller Inhalte vor der Verschlüsselung durch.[8] Verdächtiges Material wird dann direkt an Dritte, z.B. Content-Moderatorinnen oder Strafverfolgungsbehörden, ausgeleitet. CSS bricht nicht nur den Grundsatz von ende-zu-ende-verschlüsselter Kommunikation, nämlich dass die Nutzerin bestimmen kann, wer Zugriff auf die von ihr versandten Inhalte hat, sondern bedeutet auch, dass Überwachungssoftware auf den eigenen Geräten gehostet wird. Dies kann unter anderem dafür sorgen, dass das Gerät anfälliger für sogenannte "Zero-Day-Exploits" wird, die von Angreiferinnen ausgenutzt werden können. Dies kann nicht nur eine abstrakte Angreiferin sein, sondern auch Personen im sozialen Nahfeld. Insbesondere für Betroffene von Missbrauch jeglicher Art ist ein sicheres Gerät zur Kommunikation besonders wichtig. Nicht ohne Grund hat Apple einen entsprechenden Vorschlag aus dem Jahr 2021 zurückgezogen[9]. CSS schafft von Natur aus ernsthafte Sicherheits- und Datenschutzrisiken für die gesamte Gesellschaft, während die Unterstützung, die es den Strafverfolgungsbehörden bieten kann, aufgrund der hohen Fehlerquote und fehlender Transparenz hochgradig problematisch ist. Zusätzlich ist festzuhal-

[7] Folgeabschätzung - https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12726-Fighting-child-sexual-abuse-detection-removal-and-reporting-of-illegal-content-online_en

[8] Bugs in our Pockets: The Risks of Client-Side Scanning - https://arxiv.org/abs/2110.07450

[9] Apple zieht Client-Side-Scanning zurück: https://netzpolitik.org/2022/chatkontrolle-apple-macht-rueckzieher-beim-client-side-scanning/

ten, dass es zu einer möglichen Monopolbildung, bei der zur Verfügungstellung von Technologie kommen kann. Die Verordnung sieht auch kleine und mittelständische Unternehmen in der Pflicht Aufdeckungsanordnungen umzusetzen. Diese werden aber kaum die Ressourcen haben, um Technologien selbst zu entwickeln. Auch das in der Verordnung angeführte EU-Center wird dieses Problem kaum lösen können, es soll zwar Empfehlungen für die Umsetzung von Aufdeckungsanordnungen geben, dies umfasst aber lediglich eine Liste an geeigneten Technologien (Art. 50 Abs.1). Zusätzlich schafft die Verordnung einen Anreiz, weitere auf CSS basierende Überwachungstechnologien zu entwickeln. Dies ist gerade vor dem Hintergrund des Überwachungsskandals rund um die Spyware Pegasus und ihren Hersteller NSO-Group hochgradig fragwürdig.

Insgesamt setzt der Gesetzesvorschlag gleich zwei Grundrechte außer Kraft: das Fernmeldegeheimnis [10] und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme [11]. Er verkehrt sie sogar in ihr Gegenteil: aus dem Schutz vor Überwachung wird eine Verpflichtung zur Überwachung ohne jeden Verdacht oder konkrete Gefahr. Nutzerinnen verlieren die Kontrolle darüber, welche Daten sie wie mit wem teilen und somit das Grundvertrauen in das eigene Gerät.

Altersverifikation

Der Gesetzesvorschlag sieht Altersverifikation als Werkzeug vor, dass immer dann zur Anwendung kommen soll wenn ein eventuelles Risiko besteht dass die Anwendung zur Verbreitung von CSAM oder Grooming genutzt werden kann. Des Weiteren sieht er eine Verpflichtung zur Altersverifikation für App-Store-Anbieterinnen (Art. 6 Abs. 1) vor, die sicherstellen soll, dass Minderjährige keinen Zugriff auf solche Applikationen haben. Dies bedeutet nichts weiter als eine breit Angelegte Pflicht zur Altersverifikation, da ein Restrisiko nie ausgeschlossen werden kann. Wird die im Gesetzesvorschlag angedachte, flächendeckende Altersverifikation umgesetzt, dann schafft die EU unter deutscher Mitwirkung die Grundlage dafür, Anonymität im Netz weitgehend abzuschaffen. Der CCC hat bereits mehrfach hervorgehoben, dass das Recht auf Anonymität unabdingbare Voraussetzung für die Wahrnehmung wesentliche Grundrechte ist.

Recht auf Anonymität [12]
Anonymität ist ein wichtiges Gut, sowohl in der realen Welt als auch im Internet. Für die politische Willensbildung ist es wichtig, dass Bürgerinnen sich informieren und diskutieren können, ohne sich beobachtet oder verfolgt zu fühlen. Authentizität im Internet darf nicht zu Lasten der Anonymität gehen und nicht durch erkennungsdienstliche Behandlung erkauft werden. Betreiberinnen anonymer

[10] Fernmeldegeheimnis - https://www.bfdi.bund.de/DE/Buerger/Inhalte/Telefon-Internet/TelekommunikationAllg/Fernmeldegeheimnis.html

[11] Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme - https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html

[12] CCC veröffentlicht Formulierungshilfe für Digitales im neuen Regierungsprogramm - https://www.ccc.de/de/updates/2021/ccc-formulierungshilfe-regierungsprogram

Kommunikationsmöglichkeiten wie etwa Tor oder VPNs dürfen nicht weiter Verfolgung und Repressalien ausgesetzt werden. Dazu muss eindeutig gesetzlich geklärt werden, dass sie grundsätzlich nicht für über ihre Dienste getätigte Äußerungen belangt werden dürfen.

Zusätzlich zur Altersverifikation mithilfe von Ausweisdokumenten wird häufig Altersverifikation mithilfe von biometrischen Daten als mögliche Lösung angeführt. Biometrische Daten sind hochsensibel (DSGVO Art. 9.1), der Einsatz eines solchen Systems würde zu einer systematischen Verarbeitung und Sammlung von biometrischen Daten von Kindern und Jugendlichen führen, die als solche besonders schützenswert sind. Das Problem bei biometrischen Daten ist, dass diese nur schwer änderbar sind und somit dazu dienen können, Personen für immer eindeutig zu identifizieren. Im letzten Jahr gelang es Mitgliedern des CCC, Geräte zum Erfassen von biometrischen Daten von Ortskräften in Afghanistan auf eBay zu ersteigern. Auf den Geräten wurden 2600 hochsensible Datensätze gefunden, die in den falschen Händen das Leben dieser Menschen massiv in Gefahr gebracht hätten. Dies zeigt, welche dramatischen Konsequenzen der unverantwortliche Umgang mit biometrischen Daten hat. [13]

Eine grundrechtskonforme Altersverifikation, die das Recht auf Anonymität nicht untergräbt, gibt es nicht. Dies wurde bereits im DSA anerkannt (vgl. Erwägungsgrund 71). Die im DSA genannten Lösungsvorschläge zur Risikominderung ohne Altersverifikation sollten in Erwägung gezogen werden.

Fehlendes Verständnis für Open-Source-Software

Weiterhin würde die Pflicht zur Altersverifikation die Open-Source-Community besonders hart treffen. Erneut zeigt sich hier das Unverständnis der Gesetzgeberin für Open-Source-Software, die sie eigentlich als ein wichtiges gesellschaftliches Gut ansieht.

Die Infrastruktur von Open-Source Distributionen sieht in der Regel ähnlich aus wie bei der Distribution Arch Linux. Diese Linux Distribution legt ein besonderes Augenmerk darauf, möglichst wenig Daten über die Nutzerinnen zu sammeln. Sowohl die Distribution selbst als auch die Packages (Software Applikationen) können von einer Vielzahl sogenannter Mirrors heruntergeladen werden. Ein Mirror (zu Deutsch: Spiegel) beschreibt einen gespiegelten Speicherort von Dateien, die damit an mehreren Orten im Internet verfügbar sind. Die Mirrors sind wiederum in drei sogenannte Tiers (zu Deutsch: Stufen) eingeteilt: Mirrors des Tiers 0 enthalten die vom Arch-Team selbst erstellten Softwarepakete. Mirrors des Tier 1 sind Kopien von Tier 0, Mirrors von Tier 2 entsprechend Kopien von Tier 1. Diese dezentrale Verteilung der Software verhindert auch, dass Entwicklerinnen an zentraler Stelle Informationen über ihre Nutzerinnen sammeln können. Gleiches gilt auch für das Tracken der Downloads von Software-Paketen.

Um eine Altersverifikation zu gewährleisten, müssten sich Distributionen aber

[13] Biometrische Daten, tickende Zeitbombe - https://www.ccc.de/de/updates/2022/afghanistan-biometrie

auch Open-Source App-Stores wie F-Droid von diesem Datensparsamen dezentralen Modell verabschieden. Des Weiteren könnte die Altersverifikation trotzdem leicht umgangen werden, denn die Quellen aller Software-Pakete (git Repositories) sind öffentlich einsehbar. Das eigenständige Kompilieren von Programmen ist eine zentrale Voraussetzung für die Transparenz offener Software. Um die Verordnung einzuhalten, müssten die Anbieterinnen und Nutzerinnen offener Software jedoch darauf verzichten. So hat etwa Levente Polyák von der Distribution ArchLinux darauf hingewiesen, dass eine Implementierung von Altersverifikationen eine Zentralisierung erfordern würde, die der Entwicklung freier Software wesensfremd ist und unmöglich umzusetzen wäre. [14]

Sperren von URLs ist technisch nicht möglich

Die Verordnung sieht das Sperren von Webseiten durch Internetzugangsanbieter (ISP) vor, allerdings nicht wie derzeit auf Basis von Domains, sondern basierend auf URLs (Uniform Ressource Locators). In der Verordnung wird das Sperren in zwei Schritte aufgeteilt. Zunächst soll der ISP feststellen, ob die URL überhaupt von Nutzerinnen aufgerufen wird, anschließend soll die URL gesperrt werden. Dieses Vorgehen ist technisch aus mehreren Gründen nicht möglich. Zum einen hat der ISP aufgrund moderner Transportverschlüsselung, https, keine Informationen darüber, welche spezifischen URLs von Nutzerinnen aufgerufen werden. Zum anderen ist ein gezieltes Sperren von URLs ohne das Aufbrechen von sicherer Transportverschlüsselung nicht möglich, hier müssten weitere Überwachungswerkzeuge wie z.B. Deep Packet Inspection eingesetzt werden. Ein Aufbrechen der https-Verschlüsselung in jeglicher Form ist grundsätzlich abzulehnen, da diese essenziell für die Sicherheit jeglicher Onlinetransaktionen wie z.B. Online-Banking ist. Sperren auf Basis von Domains sind grundsätzlich wenig zielgerichtet und führen beispielsweise dazu, dass die Sperre, die gegen eine Sharehosting-Plattform gerichtet ist, auch alle anderen Inhalte des Sharehosters betrifft.[15] In Österreich haben solche Sperren bereits dazu geführt, dass weite Teile des Internets nicht mehr erreichbar waren.[16]

Rolle des EU-Centers

Die Schaffung einer europäischen Version des NCMEC *(National Center for Missing and Exploited Children)*, welches in den USA für die Verwaltung einer zentralen Datenbank von Missbrauchsdarstellung sowie die Koordinierung von Meldungen zuständig ist, ist ein zentraler Punkt der Verordnung. Allerdings wird der Aufgabenbereich dieses EU-Centers sehr viel weiter gefasst. So soll die Behörde nicht nur für die Verwaltung der Bilddatenbank zuständig sein,

[14] Chatkontrolle akute Gefahr für offene Software - https://netzpolitik.org/2022/chatkontrolle-akute-gefahr-fuer-offene-software/

[15] Protect the Stack: Die Inhaltskontrolle ist nicht Aufgabe von Infrastrukturanbietern - https://protectthestack.org/de/

[16] Konsequenzen von Netzsperren - https://netzpolitik.org/2022/overblocking-netzsperren-klemmen-in-oesterreich-legale-webseiten-ab/

sondern auch eine wichtige Rolle bei der Weiterleitung von Daten an Europol und Ermittlungsbehörden spielen. Die Weiterleitung von Daten ist jedoch sehr weit gefasst: in Artikel 48 Abs. 3 heißt es, dass eine Meldung dann weitergeleitet werden soll, wenn sie "nicht offensichtlich unbegründet" ist. Basierend auf den zuvor evaluierten Technologien besteht hier ein großes Risiko der unrechtmäßigen Weiterleitung von sensiblen Daten an Strafverfolgungsbehörden. Eine Anfrage des *Irish Council of Civil Liberties (ICCL)* an irische Strafverfolgungsbehörden zeigt, dass bereits jetzt unverantwortlich mit den vom NCMEC erhaltenen Daten umgegangen wird. In diesem Fall wurden Daten von Nutzerinnen durch Strafverfolgungsbehörden auf Vorrat gespeichert, obwohl zuvor festgestellt wurde, dass es sich bei ihnen um Falschmeldungen handelte.[17]

Fazit

Der Verordnungsentwurf verfehlt grundsätzlich sein Ziel, der Verbreitung von Kindesmissbrauchsdarstellung entgegenzutreten. Sinnvolle Maßnahmen, wie eine Stärkung der Ermittlungskapazitäten sowie die angemessene Ausstattung von Institutionen, die sich aktiv für den Schutz von Kindern einsetzen, lässt der Vorschlag vollkommen außer Acht. In seiner jetzigen Ausgestaltung erzeugt er sogar das Gegenteil, da die enormen Mengen an Falschmeldungen, die sich aus der Verordnung zwangsläufig ergeben werden, die Meldestrukturen überlasten und damit die Ermittlungen gegen die Kriminellen noch schwieriger machen könnten. Dies machte auch die niederländische Polizei bei einer Anhörung durch das Parlament klar und wies auf die Überlastung durch die entstehenden Datenmengen hin [18]:

"[. . .] Bald werden wir ein neues Gesetz [in den Niederlanden] haben, das regelt, dass sexuelles Chatten mit Minderjährigen strafbar wird. Das wird also schon eine Herausforderung sein, damit umzugehen [. . .] Die aktuelle Masse an Meldungen ist jetzt schon schwer zu bearbeiten, eine weitere Regelung würde zur vollständigen Überlastung führen."

Die Berge an irrelevantem Material werden die Beamtinnen von wichtiger Ermittlungsarbeit abhalten. Ermittlungserfolge bleiben aus, und gefundene Materialien werden, wie mehrere Fälle sowie parlamentarische Anfragen zeigten, nicht einmal gelöscht [19]. Diese Defizite wirkungsvoll zu beseitigen wäre das wichtigste Ziel im Kampf gegen Kindesmissbrauch.

Jegliche technische Umsetzung der Verordnung würde den Aufbau einer noch nie dagewesenen Überwachungsinfrastruktur bedeuten, die tief in IT-sicherheitsrelevante Prinzipien eingreift und Nutzerinnen jegliche Kontrolle

[17] An Garda Síochána unlawfully retains files on innocent people who it has already cleared of producing or sharing of child sex abuse material - https://www.iccl.ie/news/an-garda-siochana-unlawfully-retains-files-on-innocent-people-who-it-has-already-cleared-of-producing-or-sharing-of-child-sex-abuse-material/

[18] Anhörung im niederländischen Parlament - https://debatgemist.tweedekamer.nl/node/29579

[19] Fehlende Rechtsgrundlage für das Löschen von Material - https://www.tagesschau.de/investigativ/panorama/kinderpornografie-loeschung-101.html

über ihre digitale Kommunikation nimmt. Der Verordnungsvorschlag ist grundlegend abzulehnen. Wollen wir betroffenen Kindern und Jugendlichen möglichst rasch helfen, wäre es sinnvoller, bessere Alternativen gemeinsam mit Kinderschutz- und Technologieexpertinnen zu entwickeln.