SEPTEMBER 2022

Zum Schutz der Kinder vor sexuellem Missbrauch

Thorns Sicht auf den zukunftsweisenden Vorschlag der EU-Kommission

THORN

EINLEITUNG

Wir sind Thorn - eine Nonprofit-Organisation, die Technologien und Software entwickelt, um Kinder vor sexuellem Missbrauch zu schützen. Unser Bestreben ist es, unsere Erfahrungen und unser technisches Fachwissen allen relevanten Stakeholdern zur Verfügung zu stellen, insbesondere denjenigen, die beim Schutz von Kindern im Internet an vorderster Front stehen.

Der Vorschlag der EU-Kommission für eine Verordnung des Europäischen Parlaments und des Rates mit Vorschriften zur Prävention und Bekämpfung des sexuellen Kindesmissbrauchs ist bahnbrechend für den Kinderschutz. Er verspricht nicht nur, die bisherige Rechtslage in diesem Problemfeld zu verbessern, sondern auch die Bemühungen im Kampf gegen den sexuellen Kindesmissbrauch im Internet zu unterstützen. Dieser Vorschlag ist ein wichtiger Schritt in Richtung mehr Kindersicherheit weltweit.

Die Verbreitung von Missbrauchsmaterial im Internet hat in den letzten Jahren drastisch zugenommen und wächst weiterhin. Viele Stakeholder im digitalen Bereich **bemühen sich bereits freiwillig um die Eindämmung des Problems**. Die fehlende Rechtssicherheit ist jedoch ein zentrales Hindernis für Fortschritte im weltweiten Kampf gegen die Verbreitung von sexuellem Kindesmissbrauchsmaterial (Engl. “child sexual abuse material”, oder CSAM) im Internet und sorgt für gravierende Aufdeckungslücken. Wir müssen eine wirksame Rechtsgrundlage schaffen, damit das Internet ein sicherer Raum für Kinder wird.

Wir bei Thorn wissen, dass die Verbreitung von CSAM im Internet nur durch gemeinsames Handeln gestoppt werden kann. Es bedarf deswegen einer Zusammenarbeit von Bürger:innen, Institutionen, politischen Entscheidungsträger:innen, Technologieunternehmen und gemeinnütziger Organisationen gleichermaßen.

Wir stellen auch fest, dass zahlreiche Technologieunternehmen bereits bedeutende Vorkehrungen getroffen haben, um der Verbreitung von CSAM auf ihren Plattformen entgegenzuwirken. Der Vorschlag gibt den Unternehmen weitere Impulse und setzt den Schwerpunkt auf Prävention und Safety by Design. Indem die Verordnung Technologieunternehmen mit der Durchführung von Risikobewertungen betraut, sorgt sie für **mehr Transparenz** bei den Maßnahmen zur Bekämpfung der Verbreitung von CSAM im Internet und regt zu konkretem Handeln an. Der Vorschlag trägt auch zur höheren **Rechtssicherheit** für Unternehmen bei, indem er ihre Pflichten in Bezug auf CSAM präzisiert.

Mit den vorgeschlagenen Aufdeckungsanordnungen und der Einrichtung eines EU-Zentrums leitet die Verordnung der Kommission einen maßgeblichen politischen Wandel in der EU ein. Nachfolgend gibt Thorn seine Ansichten und Empfehlungen zu diesen beiden zentralen politischen Entwicklungen wieder.

Während wir die Einführung von Aufdeckungspflichten begrüßen, unterstreicht Kapitel I die Bedeutung der freiwilligen Bemühungen von Technologieunternehmen zur Aufdeckung von CSAM. Wir fordern die EU-Politiker:innen auf, **proaktive freiwillige Bemühungen zur Aufdeckung als unerlässlich für die Risikominderung anzuerkennen**.

In Kapitel II wird die Frage erörtert, inwieweit das EU-Zentrum als kontinentales Forschungszentrum

fungieren kann. Dies **erfordert adäquate finanzielle, technische und materielle Ressourcen**, ergänzt durch strenge Datenschutz- und Sicherheitsvorkehrungen und eine Einbettung des EU-Zentrums in das bestehende Kinderschutzsystem.

Wir bei Thorn glauben, dass die Aufdeckung von CSAM im Internet ein unabdingbarer Bestandteil der globalen Anstrengungen zugunsten des Kinderschutzes ist. Dies ist jedoch nur ein Teil einer ganzheitlichen Lösung. Wir begrüßen alle im Vorschlag enthaltenen Vorschriften, die die Beseitigung von CSAM sicherstellen und die Hilfestellung für die Opfer fördern sollen. Wenn wir gemeinsam an einem Strang ziehen und die von der Europäischen Kommission vorgeschlagenen Maßnahmen umsetzen, können wir einen echten Wandel herbeiführen und das Internet für Kinder sicherer machen, jetzt und für kommende Generationen.

I

Argumente für eine sichere und verhältnismäßige proaktive Aufdeckung von CSAM im Internet

Wir bei Thorn begrüßen und schätzen alle Bemühungen, die zum besseren Schutz von Kindern in digitalen Räumen unternommen werden. Da die Fälle von CSAM im Internet weiterhin in alarmierendem Maße zunehmen, besteht für das digitale Ökosystem nun das Momentum zu einer koordinierten Anstrengung, um deren Verbreitung im Internet zu beenden.

Gezielte Erkennung und Aufdeckung ist eines der wirkungsvollsten Instrumente, die wir einsetzen können, um Kinder in großem Umfang zu schützen. Dies umfasst alle Technologien, die dazu dienen, die Existenz und/oder die Verbreitung von (un)bekanntem CSAM oder die gezielte Kontaktaufnahme zu Minderjährigen in Missbrauchsabsicht erkennen. Diese sind mitunter bekannt als *„Hashing and Matching"* (bekanntes Material), *„Classifiers"* (unbekanntes Material) und *„Anti-Grooming-Tools"*.

Mit der Einführung von Aufdeckungsanordnungen erkennt die Kommission die entscheidende Bedeutung von Erkennungstechnologien zur Bekämpfung und Beseitigung von CSAM im Internet an. Die Kommission möchte auch die Transparenz von Erkennungstechnologie erhöhen, indem sie die Anbieter auffordert, ihre Nutzer über den Einsatz solcher Technologien zur Bekämpfung von CSAM zu informieren und deren Funktionsweise zu erklären (Art. 10, 5a). Wir schätzen diese Anerkennung und Verpflichtung zur Transparenz und rufen die europäischen Gesetzgeber dazu auf, die Technologie bestmöglich zu nutzen, um digitale Plattformen im Kampf für den Schutz von Kindern im Internet zu stärken.

Obwohl das Potenzial von Erkennungstechnologien erkannt wird, erlaubt die aktuelle Version des Vorschlags den Anbietern nicht, CSAM freiwillig oder proaktiv zu erkennen und zu melden. Nach den vorgeschlagenen Regeln müssten die Anbieter von Online-Diensten auf eine Aufdeckungsanordnung warten, um solche Technologien nutzen zu können. Die Kommission weist zu Recht darauf hin, dass freiwillige Maßnahmen allein das wachsende Problem von CSAM nicht lösen werden, weshalb wir die Einführung von Aufdeckungsanordnungen begrüßen.

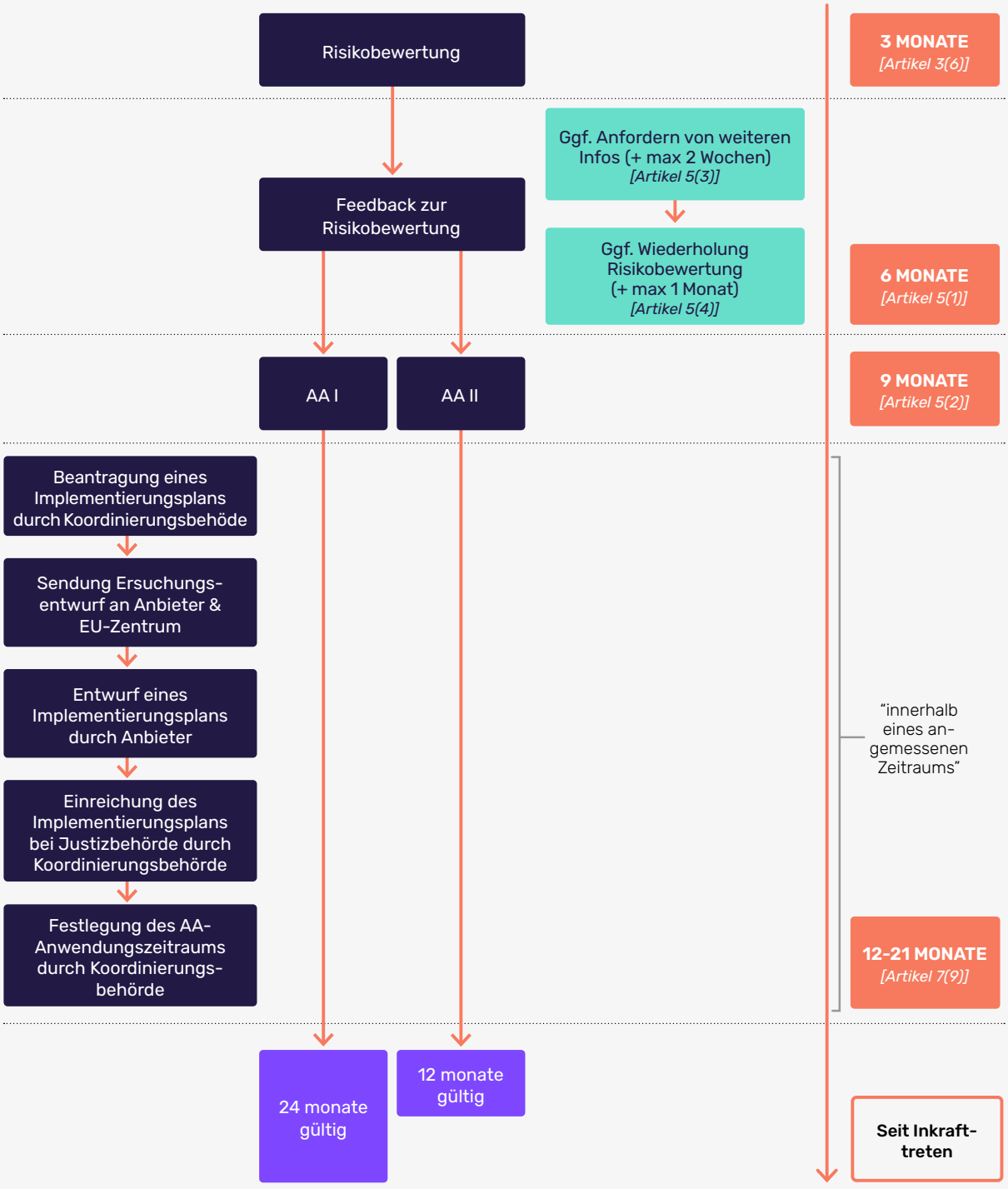
Nicht alle Anbieter von Online-Diensten sind bereit, Aufdeckungsmaßnahmen zu ergreifen. **Es ist jedoch von entscheidender Bedeutung, dass die proaktive Erkennung auch ohne das Vorliegen einer vorherigen Aufdeckungsanordnung eine Option für diejenigen Anbieter bleibt, die freiwillig zu einer Eindämmung der Verbreitung von CSAM bereit und in der Lage sind**. Wir glauben, dass jeder Anbieter in der Lage sein sollte, sicherzustellen, dass seine Plattform frei von CSAM ist. Denn ein sicheres Internet wird nicht nur von den Nutzern erwartet, sondern ist auch notwendig, damit Überlebende von sexuellem Kindesmissbrauch den Teufelskreis der Reviktimisierung durchbrechen können. Wenn diese Regelung beibehalten wird, wird sie zu einer Unterbrechung bestehender Prozesse führen, was erhebliche negative Auswirkungen auf den weltweiten Kampf gegen CSAM im Internet haben wird. Die freiwillige und die obligatorische Aufdeckung ergänzen sich und können beide, bei einer richtigen Ausgestaltung, den gleichen rechtlichen Garantien unterliegen.

EFFEKTIVE PROZESSE NOTWENDIG

Der Vorschlag stellt einen bedeutenden politischen Wandel dar. Er ersetzt ein System, das sich ausschließlich auf die freiwilligen Bemühungen der Anbieter zur Aufdeckung, Meldung und Beseitigung von CSAM stützt, durch ein System,

das auf Aufdeckungsanordnungen für einzelne Anbieter ausgerichtet ist. Die Anbieter dürfen nämlich nur dann Erkennungstechnologien einsetzen, wenn sie dazu verpflichtet sind. Bestimmten Anbietern würden in einem langen bürokratischen und schwerfälligen Verfahren „Aufdeckungsanordnungen" erteilt. **Grafik 1** veranschaulicht den Prozess, den die Anbieter durchlaufen müssten, bis eine Aufdeckungsanordnung erteilt werden kann.

GRAFIK 1 | Aufdeckungsanordungen (AA)



Beginn der Risikobewertung 3 Monate nach dem Inkrafttreten der Verordnung oder 3 Monate nachdem der Anbieter den Dienst in der EU begonnen hat anzubieten [Artikel 3(6)]

Wiederholung der Bewertung mind. 1x alle 3 Jahre oder bei Bedarf und mind. 2 Monate vor Ablauf der Geltungsdauer der AA [Artikel 3(6)]

AA I = betreffen Verbreitung (un-)bekannter CSAM [Artikel 7(9)]

AA II = betreffen die Anwerbung von Kindern ("Grooming") [Artikel 7(9)]

Das Hauptproblem des Verfahrens zur Erteilung von Aufdeckungsanordnungen ist der potenzielle **Engpass**, der entstehen könnte, wenn Anbieter nicht die Möglichkeit haben, proaktiv freiwillige Aufdeckungsmaßnahmen zu ergreifen.

Dieses Verfahren könnte zu einer Verzögerung von ein bis zwei Jahren zwischen dem Inkrafttreten der Rechtsvorschriften und dem Erlass der ersten Aufdeckungsanordnungen führen. In dieser Schätzung ist zudem die Zeit zwischen der Beantragung auf Erlass einer Aufdeckungsanordnung und der Zulassung des Antrags durch eine Justizbehörde nicht enthalten; diese Zeitspanne ist nicht genau spezifiziert, wird aber mit Sicherheit einige zusätzliche Monate in Anspruch nehmen.

ENTSTEHUNG SCHÄDLICHER AUFDECKUNGSLÜCKEN VERHINDERN

Eine unmittelbare Folge des von der Kommission vorgeschlagenen Systems der Aufdeckungsanordnungen ist die Entstehung von schädlichen Aufdeckungslücken.

In der Vergangenheit haben Rechtslücken in der EU die negativen Auswirkungen von Aufdeckungslücken auf den Kinderschutz aufgezeigt: Als Anbieter aufgrund der Rechtsunsicherheit im Zusammenhang mit der EU-Datenschutzrichtlinie für elektronische Kommunikation die Aufdeckung und Meldung von CSAM in der EU für den Großteil des Jahres 2021 einstellten, ging die Zahl der Meldungen von CSAM aus der EU laut NCMEC um 58% zurück.[1]

Das im Vorschlag skizzierte System wird zu noch größeren Aufdeckungslücken führen, da es keine Überbrückungslösung vorsieht, die eine kontinuierliche Aufdeckung durch die Anbieter zwischen dem Auslaufen der vorläufigen Ausnahmeregelung und dem Inkrafttreten der neuen Rechtsvorschriften gewährleistet. Anbieter, die derzeit auf freiwilliger Basis ermitteln, werden gezwungen sein, ihre Tätigkeit einzustellen und jahrelang zu warten, bis eine Aufdeckungsanordnung erlassen wird. In der Zwischenzeit wird CSAM zweifellos frei im Internet zirkulieren und den Strafverfolgungsbehörden werden Informationen fehlen, die für ihre Ermittlungen wichtig sind.

AUSSCHLUSS FREIWILLIGER AUFDECKUNGSMASSNAHMEN UNTERGRÄBT RISIKOBEWERTUNGEN DER ANBIETER

Der Vorschlag sieht den Erlass einer Aufdeckungsanordnung nur als letztes Mittel vor. Die vorangehenden Schritte bestehen in der Durchführung einer Risikobewertung und, basierend auf dem Ergebnis der Bewertung, in der Anwendung freiwilliger Maßnahmen zur Risikominderung.

Die derzeitige Fassung des Vorschlags sieht keine freiwilligen Aufdeckungsmaßnahmen in der Risikobewertung vor – auch nicht den gezielten Einsatz spezieller Aufdeckungstechnologien zur Identifizierung von CSAM. Dieser Ausschluss stellt eine Entscheidung dar, die den beabsichtigten Zweck einer solchen Anordnung erheblich unterminiert.

In der Realität wissen viele Unternehmen nicht, dass ihre Plattformen für die Verbreitung von CSAM missbraucht werden, während andere zwar davon wissen, aber keine Maßnahmen ergreifen. Ohne die Erlaubnis zum Einsatz von notwendigen Aufdeckungstechnologien, werden die **Anbieter nicht in der Lage sein, die mit CSAM verbundenen Risiken** auf ihren Plattformen gründlich zu bewerten und sie werden über das Ausmaß dieses Verbrechens auf ihren Plattformen im Unklaren bleiben. Der Ansatz der Kommission zur Risikobewertung ist daher fehlerhaft.

Dies stellt einen blinden Fleck im gesamten Aufdeckungsprozess dar, der ja darauf ausgelegt ist, die Aufdeckung von CSAM-Risiken zu ermöglichen, die Anbieter aber daran hindert, CSAM-Aufdeckungstechnologien zu verwenden. Es ist von entscheidender Bedeutung, dass die Anbieter bei der Durchführung ihrer Risikobewertung über angemessene Technologien

1 CyberTipline Data (missingkids.org)

und Informationen verfügen.

Unsere Erfahrung im Bereich der digitalen Kindersicherheit zeigt uns, dass für eine wirksame Risikobewertung mehr nötig ist als die drei im Vorschlag vorgesehene Maßnahmen zur Risikobewertung (Altersüberprüfung, Kennzeichnung der Nutzer und Auslagerung der Bewertung an das EU-Zentrum).

Die Altersüberprüfung ist zwar ein wichtiges Präventivinstrument, insbesondere zum Schutz von Kindern vor Grooming, aber sie allein kann die Verbreitung von CSAM nicht verhindern. Die Kennzeichnung und Meldung von Nutzern sollte eine eingebaute und vereinfachte Funktion eines jeden Dienstes sein. Diese Praxis hat jedoch offensichtliche Grenzen, da die Verfahren nicht immer einfach zu verfolgen oder zu aufwändig sind.

Bei der dritten Option, der Auslagerung der Risikobewertung an das EU-Zentrum, können die Anbieter das EU-Zentrum bitten, auf eigene Kosten eine „repräsentative Stichprobe" auf das Risiko von CSAM zu analysieren. Dies wirft die Frage auf, wie und von wem die Daten solcher Stichproben ausgewählt würden. Die Anbieter sollten sich nicht ihrer Verantwortung entziehen können, indem sie Daten nach ihrem Belieben aussuchen und weitergeben.

EINSCHRÄNKUNG DES EINSATZES WIRKSAMER RISIKOMINDERUNGSMASSNAHMEN

Sobald ein Anbieter seine Risikobewertungen durchgeführt hat, wird er aufgefordert, diese **Risiken ohne den Einsatz von Aufdeckungstechnologien zu mindern**. Dadurch werden den Anbietern die Instrumente zur wirksamen Bekämpfung einer Straftat vorenthalten. Die Anbieter sollen stattdessen „geeignete technische und operative Maßnahmen und Personalausstattung" (Art. 4) einsetzen, was Maßnahmen wie Altersüberprüfung und die Anpassung der Empfehlungssysteme beinhalten kann – beides ist eindeutig unzureichend, wenn bereits Fälle von CSAM bestätigt wurden. **Die Bestimmung über geeignete Maßnahmen ist vage, insbesondere in Bezug darauf, welche Technologien in den Bereich der Risikominderung fallen und welche eine Aufdeckungsanordnung erfordern würden**. Dies schafft Rechtsunsicherheit für die Anbieter, weshalb diese zögern werden, neue Technologien ohne vorherige Zulassung durch das EU-Zentrum einzusetzen und zu entwickeln.

INNOVATIONEN NICHT ERSTICKEN

In den letzten zehn Jahren waren die freiwilligen Aufdeckungsbemühungen der Anbieter entscheidend für die Förderung von Innovationen im weltweiten Kampf gegen CSAM im Internet. **Die Fähigkeit zur Innovation und ständigen Verbesserung von Aufdeckungstechnologien bildet das Rückgrat dieses Kampfes**. Thorn begrüßt daher, dass die Kommission in ihrem Vorschlag einen grundsätzlich innovationsfreundlichen Ansatz verfolgt.

Durch den Ausschluss der proaktiven, freiwilligen Erkennung wird jedoch ungewollt eine der wichtigsten Triebkräfte für Innovationen in diesem Bereich neutralisiert. Die Anbieter kennen ihre Plattformen und wissen, welche Lösungen für diese Probleme in Frage kommen. Wo es keine Lösungen gibt, müssen sie entwickelt werden, und zahlreiche Anbieter haben bewiesen, dass sie dabei äußerst erfolgreich sind. Indem der Vorschlag den Spielraum für proaktive Bemühungen einschränkt und vorschreibt, welche Technologien bei Aufdeckungsanordnungen eingesetzt werden können, gibt er den Anbietern wenig Anreiz, neue Lösungen zu entwickeln oder bestehende zu verbessern. Sinnvoll ist eine Lösung, die dezentrale und proaktive Innovationen durch die Anbieter besser fördert.

Die wichtigsten Empfehlungen von Thorn

Thorn empfiehlt, dass der Vorschlag **es Anbietern erlaubt, proaktive Aufdeckungstechnologien im Rahmen ihrer Risikobewertung und freiwilligen Risikominderung einzusetzen**. Wir sind der Meinung, dass ein Systemwechsel notwendig ist, weg von einem System, welches sich ausschließlich auf obligatorische Aufdeckungsanordnungen stützt, die auf einem unvollständigen Bild beruhen, hin zu einem System, welches es den Anbietern ermöglicht, auf ihren Plattformen freiwillig CSAM zu erkennen.

Diejenigen Anbieter, die die freiwillige Erkennung von CSAM im Rahmen ihrer Risikobewertung oder ihrer Maßnahmen zur Risikominderung nutzen möchten, sollten in der Lage sein, dies zu tun. Dabei sollten sie die zuständigen Behörden über ihre Aktivitäten, die von ihnen verwendete Technologie und die damit erzielten Ergebnisse informieren. Somit würden Anbieter denselben Prozess durchlaufen wie diejenigen, die den regulären Aufdeckungsprozess durchlaufen, und würden daher auch denselben rechtlichen Bestimmungen unterliegen. In der Zwischenzeit hätten diese Anbieter jedoch die Möglichkeit, CSAM zu bekämpfen.

Sollte die Überprüfung durch die Behörden ergeben, dass die Technologie und das Verfahren eines Anbieters nicht den Standards des EU-Zentrums entsprechen – oder dass der Einsatz von Aufdeckungstechnologie angesichts der vom Anbieter festgestellten Risiken nicht gerechtfertigt ist –, könnten die Behörden die Maßnahmen des Anbieters ändern oder nachbessern.

Diese Empfehlung würde verhindern, dass der Prozess der Aufdeckungsanordnungen zu Aufdeckungslücken führt, und gleichzeitig die Kontrollen und Abwägungen aufrechterhalten, die sicherstellen, dass die Aufdeckungstechnologien gezielt eingesetzt werden und den höchsten Standards entsprechen.

Kapitel I Empfehlungen

ARTIKEL 3 - RISIKOBEWERTUNG

- Anbieter sollten die Möglichkeit haben, Erkennungstechnologien proaktiv als Teil ihrer Risikobewertung einzusetzen.
- Anbieter, die im Rahmen ihrer Risikobewertung freiwillig CSAM aufdecken wollen, sollten die zuständigen Behörden darüber benachrichtigen.
- Es müssen zusätzliche Sicherheitsvorkehrungen getroffen werden, um zu überprüfen, ob die Daten, die die Anbieter dem EU-Zentrum zur Analyse übermitteln, repräsentativ sind und nicht dazu dienen, sich ihrer Verantwortung zu entziehen.

ARTIKEL 4 - RISIKOMINDERUNG

- Der proaktive Einsatz von Aufdeckungstechnologien sollte zu den Maßnahmen gehören, die Anbieter zur Minderung des Risikos von CSAM ergreifen können.
- Anbieter, die bereit sind, CSAM im Rahmen ihrer Risikominderungsmaßnahmen proaktiv aufzudecken, sollten die zuständigen Behörden entsprechend benachrichtigen.

ARTIKEL 7 - ERLASS VON AUFDECKUNGSANORDNUNGEN

- Eine Ermöglichung der Zulassung von proaktiven Aufdeckungstätigkeiten der Anbieter innerhalb des Verfahrens zur Erteilung von Aufdeckungsanordnungen.

II

Errichtung eines kompetenten EU-Zentrums

Thorn unterstützt die vorgeschlagene Einrichtung eines **EU-Zentrums, das eine wichtige Säule im globalen Kampf gegen CSAM sein wird**. Ähnliche Zentren gibt es bereits in verschiedenen Ländern. Sie haben sich dabei bewährt, aufgedecktes Material zentral zu erfassen, als Bindeglied zwischen Aufsichtsbehörden und Anbieten zu fungieren und Opfern die nötigen Hilfeleistungen zu erbringen.

Mit der Gründung des EU-Zentrums ergibt sich für die EU die Chance, ihre Strategie auf die Vielzahl aktueller und künftiger Herausforderungen im Bereich der CSAM-Bekämpfung zuzuschneiden und damit einen internationalen Standard für die kommenden Jahrzehnte zu setzen. Die Einrichtung, Pflege und der Betrieb von Datenbanken mit CSAM-Indikatoren in einer unabhängigen europäischen Einrichtung ist ein großer Schritt nach vorn. Die zentralisierte Erfassung ist unerlässlich, da sonst Datensilos entstünden, die den Schutz von Kindern erheblich beeinträchtigten.

Als Organisation, die Technologien entwickelt, begrüßt Thorn die Fähigkeit des EU-Zentrums, als kontinentales Forschungszentrum zu fungieren, und wir sehen einer möglichen Zusammenarbeit in diesem Bereich erwartungsvoll entgegen. Die Wahrnehmung einer so anspruchsvollen und zugleich sensiblen Aufgabe setzt **angemessene finanzielle, technische und materielle Ressourcen voraus, wobei gleichzeitig strenge Datenschutz- und Sicherheitsvorkehrungen eingehalten werden müssen**. Das EU-Zentrum muss daher ein hohes Maß an Autonomie gegenüber Politik und Strafverfolgung bewahren und über eigene finanzielle und personelle Ressourcen verfügen. Um den weltweiten Bemühungen im Kampf gegen CSAM den Rücken zu stärken, muss auch die Grundlage für die Kooperation zwischen dem EU-Zentrum und bereits bestehenden Strukturen genauer festgelegt werden.

Das EU-Zentrum und sein Technologieausschuss werden auch eine maßgebende Rolle bei der Prüfung neuer Technologien spielen. Dabei wird von zentraler Bedeutung sein, dass **das EU-Zentrum fundierte und rechtzeitige Empfehlungen erteilen kann, um sicherzustellen, dass die Technologien wirksam sind und Datenschutzstandards erfüllen**. Nur so kann ein schnelles Innovationstempo erzielt werden, das für die Eindämmung dieses sich ständig weiterentwickelnden Verbrechens notwendig ist.

AUTONOMIE DES EU-ZENTRUMS

Eine enge Koordinierung zwischen dem EU-Zentrum und Europol ist für eine wirksame Bekämpfung von CSAM eine Voraussetzung. Das EU-Zentrum wird als Bindeglied zwischen den privaten Anbietern und den Strafverfolgungsbehörden dienen: Es wird Reports von Anbietern entgegennehmen und bewerten und, wenn ein Report CSAM enthält, diesen an Europol weiterleiten. Die **unabhängige** Ausübung dieser Vermittlerrolle wird zur Effizienz des Ablaufs und zum Vertrauen der Bürger:innen in die EU bei der Bekämpfung von CSAM beitragen. Das EU-Zentrum wird außerdem sicherstellen, dass die Mitteilungen an die Strafverfolgungsbehörden korrekt sind und dass die relevanten Hinweise zügig und unkompliziert bei den zuständigen Instanzen ankommen. Die Sensibilität der Aufgaben des EU-Zentrums erfordert es, dass seine Arbeitsbereiche von den Strafverfolgungsbehörden komplett isoliert sind.

Der derzeitige Entwurf des Kommissionsvorschlags sieht eine solche Autonomie nicht vor. Gemäß Artikel 53 des Verordnungsvorschlags soll das EU-Zentrum auf Unterstützungsdienste (in den Bereichen Personal, IT einschließlich Cybersicherheit, Kommunikation) von Europol angewiesen sein, was dessen Autonomie von Europol einschränkt. Dies kann zwar zu einer gewissen Kosteneffizienz verhelfen, birgt aber die Gefahr, dass solche gemeinsamen Verwaltungsbereiche die und Vertrauen in das EU-Zentrums können.

Die wichtigsten Empfehlungen von Thorn

Thorn empfiehlt, dass **der Anspruch auf Unabhängigkeit des EU-Zentrums sich auch in seiner Finanzierung und Struktur wiederfindet**. Zu diesem Zweck sollte das EU-Zentrum über einen eigenen Haushalt, eigene Verwaltungsstrukturen, eigenes Personal und eigene Sicherheitssysteme verfügen. Dies steht einer gegenseitigen Vertretung von Europol- und EU-Zentrumsbeamten in den Verwaltungsräten nicht entgegen, sofern diese unabhängig agieren können.

EINBINDUNG DES EU-ZENTRUMS IN DAS GLOBALE UMFELD

Der weltweite Kampf gegen CSAM erfordert ein sorgfältig koordiniertes Vorgehen. Um bewährte Verfahren zu festigen, muss sich das EU-Zentrum nahtlos in das globale Umfeld einfügen. Die Zusammenarbeit mit den bereits vorhandenen und künftigen regionalen Beobachtungsstellen ist ein wichtiger Aspekt, der in dem Vorschlag jedoch nicht näher erläutert wird. Es müssen Kanäle zwischen den verschiedenen Meldestellen geschaffen werden, die einen reibungslosen Informationsaustausch gewährleisten. Diese Stellen identifizieren Missstände oft als erste, und schnelles Eingreifen ist entscheidend, damit betroffene Kinder schnellsten gefunden werden können. Daher würden wir weitere Präzisierungen begrüßen, wie die verschiedenen Einrichtungen unter Wahrung der Privatsphäre und der personenbezogenen Daten kooperieren würden.

ENTWICKLUNG, VERBREITUNG UND EINSATZ NEUER ERKENNUNGSTECHNOLOGIEN

Als Forschungs- und Innovationszentrum birgt das EU-Zentrum das Potenzial, als Katalysator für den Fortschritt im Kampf gegen CSAM zu fungieren. In dieser Hinsicht ist es äußerst wichtig, dass das Zentrum über die dafür notwendigen Kapazitäten, Finanzmittel und Instrumente verfügt, um diese Funktion auszuüben. Da sich die Täter in einem dynamischen digitalen Umfeld bewegen, kommt es darauf an, dass das Zentrum ebenso schnell reagieren kann. **Zu diesem Zweck sind reibungslose und effiziente Verfahren zur Entwicklung, Verbreitung, Einsatz und Optimierung von Erkennungstechnologien für das EU-Zentrum von entscheidender Bedeutung.**

Der Technologieausschuss des EU-Zentrums wird dabei eine zentrale Rolle spielen und trägt daher eine besondere Verantwortung für das gesamte technologische und sozialpolitische Umfeld. Wir begrüßen die Einrichtung dieses Ausschusses und sind überzeugt, dass er das Vertrauen der Öffentlichkeit in diese Technologie fördern wird. Die Befugnis des Technologieausschusses, Gutachten zu bereits existierenden und neuen Erkennungstechnologien zu verfassen, verleiht diesem Gremium ein neues Maß an Transparenz und setzt Anreize für mehr Innovationen in diesem Bereich.

Die wichtigsten Empfehlungen von Thorn

Angesichts dieser wichtigen Rolle sollte der Text **die Zusammensetzung und die Verwaltung des Technologieausschusses genauer darlegen**. Um die Technologie sachgerecht begutachten zu können, muss sich der Ausschuss aus technischen Expert:innen bilden, die unabhängig von den Anbietern agieren können, sowie aus Strafrechtsexpert:innen, die beurteilen können, ob die Erkennungstechnologie dem Umfang und der Schwere der Straftat angemessen ist. Darüber hinaus empfehlen wir, dass im Technologieausschuss die Zivilgesellschaft vertreten ist. Nur so kann ein ausgewogener Blick auf die Auswirkung der CSAM-Straftaten sowie der dagegen eingesetzten Instrumente auf den Einzelnen, die Gesellschaft und die Privatsphäre gewahrt werden.

DATENSPEICHERUNG UND DATENZUGANG

Damit die Strafverfolgungsbehörden wirksam gegen den sexuellen Kindesmissbrauch vorgehen und Kinder schützen können, muss der Zugang zu Daten gewährleistet sein. Das EU-Zentrum wird die Mitteilungen für die Strafverfolgungsbehörden überprüfen, aber diese benötigen oftmals zusätzliche Daten von den Anbietern. Artikel 22 des Vorschlags legt fest, dass Daten nicht länger als 12 Monate aufbewahrt werden dürfen, aber es wird keine Mindestaufbewahrungsfrist vorgeschrieben.

Ohne eine Mindestaufbewahrungsfrist könnten die Unternehmen einen Report an das EU-Zentrum übermitteln und damit zusammenhängende Daten dann unverzüglich löschen. In einem Bereich, in dem jedes Bild den Schauplatz eines Verbrechens darstellt, ist jedes Beweisstück wichtig. Wir plädieren für die Einführung einer begrenzten Mindestaufbewahrungsfrist für Unternehmen in Bezug auf alle Daten, die im Zusammenhang mit einem Report an das EU-Zentrum stehen.

Zugang zur Indikatoren-Datenbanken ist ebenso eine Voraussetzung dafür, dass Anbieter und Organisationen CSAM aufdecken und ihre Erkennungsinstrumente verbessern können. Gemäß Artikel 46 ist der Zugang von Anbietern zu diesen Indikatoren jedoch an das Ausführen einer Aufdeckungsanordnung geknüpft.

Da Thorn für die proaktive freiwillige Nutzung von Aufdeckungstechnologien plädiert, **sollte Anbietern der Zugang zu Indikatoren-Datenbanken nicht verwehrt werden, wenn sie derartige Anstrengungen freiwillig unternehmen**. Außerdem beschränkt Artikel 46 den Zugang zu diesen Datenbanken auf Internetanbieter und Strafverfolgungsbehörden und schließt damit eine Vielzahl von Organisationen aus, die im Kampf gegen CSAM involviert sind, sei es durch die Entwicklung von Aufdeckungstechnologien oder die Bereitstellung von Aufdeckungsdiensten. Wie unabdingbar die Einbeziehung verschiedener Stakeholder in die Bekämpfung von CSAM ist, hält Artikel 54 fest. Dem EU-Zentrum wird darin die Befugnis eingeräumt, Absichtserklärungen mit verschiedenen Partnerorganisationen zu unterzeichnen. Diese Absichtserklärungen eröffnen vielfältige Wege der Kooperation, zu denen auch die Möglichkeit gehören sollte, dass Partnerorganisationen Zugang zu den Datenbanken beantragen können. Die Zugangsbeschränkung auf Anbieter würde das Potential der Vielzahl anderweitig involvierter Organisationen nicht ausschöpfen.

Die wichtigsten Empfehlungen von Thorn

Um zu verhindern, dass Anbieter die Daten, die im Zusammenhang mit einem Report an das EU-Zentrum stehen, unverzüglich löschen, schlägt Thorn eine Mindestaufbewahrungsfrist von mindestens sechs Monaten vor. Dieser Zeitraum würde den Strafverfolgungsbehörden ausreichend Zeit lassen, um die für ihre Ermittlungen relevanten Daten zu untersuchen.

Darüber hinaus empfehlen wir, dass Partnerorganisationen, mit denen das EU-Zentrum Absichtserklärungen abgeschlossen hat, befugt sind, Zugang zu den Indikatoren-Datenbanken zu beantragen, wenn dies den Zielen des EU-Zentrums dienlich ist. Dieses Recht sollte in Artikel 46 verankert werden.

Kapitel II Empfehlungen

ARTIKEL 22 - INFORMATIONSBEWAHRUNG

- Die Anbieter bewahren die Daten, die im Zusammenhang mit einem Report an das EU-Zentrum stehen, mindestens sechs Monate ab dem Datum der Mitteilung oder der Löschung oder Sperrung des Zugangs auf, je nachdem, was zuerst eintritt.

ARTIKEL 40 - EINRICHTUNG UND TÄTIGKEITSBEREICH DES EU-ZENTRUMS; ARTIKEL 67 - AUFSTELLUNG UND AUSFÜHRUNG DES HAUSHALTSPLANS; ARTIKEL 69 - MITTELAUSSTATTUNG

- Der Anspruch auf Unabhängigkeit des EU-Zentrums sollte sich auch in seiner Finanzierung und Struktur wiederfinden.
- Es sollte über einen eigenen Haushalt, eigene Verwaltungsstrukturen, eigenes Personal und eigene Sicherheitssysteme verfügen und in diesen Belangen nicht auf die Unterstützung anderer Gremien angewiesen sein.

ARTIKEL 46 - ZUGANG, SACHLICHE RICHTIGKEIT UND SICHERHEIT

- Anbieter sollten das Recht haben, bei einer proaktiven freiwilligen Nutzung von Aufdeckungstechnologien Zugang zu den Indikatoren-Datenbanken des EU-Zentrums zu beantragen.
- Partnerorganisationen, mit denen das EU-Zentrum Absichtserklärungen abgeschlossen hat, sollten befugt sein, Zugang zu den Indikatoren-Datenbanken zu beantragen, wenn dies den Zielen des EU-Zentrums dienlich ist.

ARTIKEL 54 - ZUSAMMENARBEIT MIT PARTNERORGANISATIONEN

- Es sollten weitere Präzisierungen darüber vorgenommen werden, wie die verschiedenen Einrichtungen unter Wahrung der Privatsphäre und der dem besonderen Schutz personenbezogener Daten kooperieren sollen.
- Es sollte näher erläutert werden, wie die Zivilgesellschaft mit dem EU-Zentrum zusammenarbeiten und weiterhin ihren unersetzlichen Mehrwert einbringen soll.

ARTIKEL 66 - EINSETZUNG UND AUFGABEN DES TECHNOLOGIEAUSSCHUSSES

- Die Zusammensetzung und die Verwaltung des Technologieausschusses sollten genauer dargelegt werden.
- Um die Technologie sachgerecht begutachten zu können, muss sich der Ausschuss aus technischen Expert:innen bilden, die unabhängig von den Anbietern agieren können, sowie aus Strafrechtsexpert:innen, die beurteilen können, ob die Erkennungstechnologie dem Umfang und der Schwere der Straftat angemessen ist.
- Im Technologieausschuss sollte die Zivilgesellschaft vertreten sein, damit ein ausgewogener Blick auf die Auswirkung der CSAM-Straftaten sowie der dagegen eingesetzten Instrumente auf den Einzelnen, die Gesellschaft und die Privatsphäre gewahrt wird.

III

Verschlüsselung

Thorn ist davon überzeugt, dass wir die Privatsphäre gewährleisten und gleichzeitig Kinder schützen können. Um eine Welt zu schaffen, in der jedes Kind das Internet sicher nutzen kann, müssen wir Sicherheit in unsere Technologie integrieren, auch in verschlüsselten Bereichen. Wir sind allerdings nicht dafür, dass Regierungen darin Hintertüren einbauen. **Wir unterstützen vielmehr verschlüsselte Räume, die den Schutz der Privatsphäre gewährleisten und in denen Unternehmen sowohl bekannte als auch unbekannte CSAM-Bilder und -Videos erkennen können.**

Verschlüsselte Bereiche sind unschätzbare technische Hilfsmittel, die die Privatsphäre der Nutzer schützen und eine sichere Übertragung von Daten und Informationen ermöglichen. Verschlüsselung gibt es in vielen Formen – von der Sicherung unserer Bankkonten über Transportverschlüsselung für E-Mails bis hin zu vollständig verschlüsselter Ende-zu-Ende-Kommunikation. **Wir bei Thorn wissen, dass eine starke Verschlüsselung eine Notwendigkeit ist, und glauben, dass es ausgewogene Ansätze gibt, die eine Erkennung von CSAM in verschlüsselten Bereichen ermöglichen.**

Im Vorschlag werden weder Verschlüsselung noch andere Technologien ausdrücklich genannt, da er technologieneutral sein soll, um mit der sich verändernden Technologielandschaft Schritt halten zu können. Wir begrüßen diese Bemühungen, da wir bei Thorn wissen, wie schnell sich die Technologie weiterentwickeln kann. Diese Gesetzgebung macht deutlich, dass eine Aufdeckungsanordnung nur dann erlassen werden kann, wenn es eine Technologie gibt, die eine Aufdeckung in dieser Umgebung ermöglicht. Dies ist eine wichtiger Schutzmechanismus, um sicherzustellen, dass gesicherte Bereiche sicher bleiben und jede Technologie, die zur Aufdeckung von CSAM eingesetzt wird, ausschließlich zu diesem Zweck verwendet wird.

Bei der Suche nach Lösungen, um alle digitalen Bereiche für Kinder sicherer zu machen, ist es wichtig, dass wir Kreativität, Aufdeckungsbereitschaft und die Entwicklung einer Vielzahl von potenziellen Lösungen fördern. Ein Umfeld, in dem ständige Innovation gefördert wird, ist der einzige Weg zur Lösung dieses komplexen Problems. Da sich die Technologie weiterentwickelt, muss Safety by Design in den Geschäftsvorhaben der Unternehmen verankert werden. Das Streben nach einem datenschutzfreundlichen, sicheren Bereich der Kommunikation sollte ein Grundprinzip des technologischen Fortschritts sein. Diese Gesetzgebung strebt gemäß heutigem Stand der Technik ein Gleichgewicht an und schafft eine sicherere digitale Welt. Es ist jetzt an der Zeit, diese Diskussion zu führen. Verschlüsselung ist ein wichtiger Bestandteil der Technologie, und wir können ein Gleichgewicht finden, das die Privatsphäre schützt und gleichzeitig nicht zulässt, dass Kinder ausgenutzt werden und CSAM unkontrolliert auf öffentlichen Plattformen verbreitet wird. Die Bekämpfung von CSAM in großem Maßstab erfordert einen ganzheitlichen Ansatz – dazu gehört die Betrachtung aller Arten von Technologie und aller Lösungen.

FÜR WEITERE INFORMATIONEN WENDEN SIE SICH BITTE AN:

Emily Slifer, Direktorin für Politik
emily.slifer@wearethorn.org

Dies ist eine Übersetzung des englischen Originaltextes. Nur die englische Fassung ist verbindlich.