Sachstand

Genese und Inhalt des Vorschlags der EU-Kommission zur „Chatkontrolle“

Genese und Inhalt des Vorschlags der EU-Kommission zur „Chatkontrolle“

Aktenzeichen:	WD 10 – 3000 – 021/22
Abschluss der Arbeit:	21. Mai 2022
Fachbereich:	WD 10: Kultur, Medien und Sport

Inhaltsverzeichnis

1. Vorbemerkung

Diese Arbeit gibt auftragsgemäß einen Überblick über Genese und Inhalt des Vorschlags der EU-Kommission für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Verhütung und Bekämpfung des sexuellen Missbrauchs von Kindern.[1]

2. Nomenklatur

Im Interesse der besseren Lesbarkeit und mangels einer amtlichen Übersetzung werden in dieser Arbeit bestimmte Begriffe verkürzt dargestellt. Diese seien hier erläutert. Legaldefinitionen finden sich in Art. 2 des Vorschlags für die Verordnung

- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down rules to prevent and combat child sexual abuse

  Vorschlag für die Verordnung

- REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down rules to prevent and combat child sexual abuse

  die Verordnung

- child sexual abuse material

  kinderpornografisches Material

- solicitation of children

  Grooming

  Unter Grooming (im deutschen Sprachraum eher als Cybergrooming bekannt) versteht man das gezielte Ansprechen von Kindern im Internet mit dem Zielt der Anbahnung sexueller Kontakte.[2]

---

1 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down rules to prevent and combat child sexual abuse vom 11. Mai 2022 – COM/2022/209 final. Abrufbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472. Zuletzt abgerufen – wie alle URL in dieser Arbeit – am 20. Juni 2022.

2 Bundesministerium für Justiz und Verbraucherschutz. Abrufbar unter: https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/DE/Cybergrooming.html.

Grooming ist nach Art. 2 Nr. 1 des Vorschlags für die Verordnung *„jede vorsätzliche Handlung, die eine Straftat im Sinne von Artikel 6 der Richtlinie 2011/93/EU[3] darstellt“* – also die *„Kontaktaufnahme zu Kindern für sexuelle Zwecke“.*

- Hosting services / interpersonal communications services

  Diensteanbieter

  Gemäß Art. 2 lit. f) Abschnitt 3 des Vorschlags für den Digital Services Act[4] ist unter einem Hosting-Anbieter ein Vermittlungsdienst zu verstehen, dessen „Hosting“-Leistung darin besteht, von einem Nutzer bereitgestellte Informationen in dessen Auftrag zu speichern.

  Ein nummernunabhängiger interpersoneller Kommunikationsdienst ist nach Art. 2 Nr. 5 RL 2018/1972/EU[5] ein gewöhnlich gegen Entgelt erbrachter Dienst, der einen direkten interpersonellen und interaktiven Informationsaustausch über elektronische Kommunikationsnetze zwischen einer endlichen Zahl von Personen ermöglicht, wobei die Empfänger von den Personen bestimmt werden, die die Kommunikation veranlassen oder daran beteiligt sind; dazu zählen keine Dienste, die eine interpersonelle und interaktive Kommunikation lediglich als untrennbar mit einem anderen Dienst verbundene untergeordnete Nebenfunktion ermöglichen.

- EU Centre on Child Sexual Abuse as a decentralised agency to enable the implementation of the new Regulation

---

3 Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates. Amtsblatt L 335/1 vom 17. Dezember 2011. Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32011L0093&from=DE.

4 Vorschlag für eine Verordnung des europäischen Parlaments und des Rates über einen Binnenmarkt für digitale Dienste (Gesetz über digitale Dienste) und zur Änderung der Richtlinie 2000/31/EG. COM(2020) 825 final vom 15.12.2020. Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52020PC0825.

5 Richtlinie des Europäischen Parlaments und des Rates über den europäischen Kodex für elektronische Kommunikation. Amtsblatt L 321/36 vom 11. Dezember 2018. Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32018L1972.

EU-Zentralbehörde[6]

Die EU charakterisiert diese Zentralbehörde folgendermaßen:

> *„Anordnungen zur Aufdeckung von Inhalten werden von Gerichten oder unabhängigen nationalen Behörden erlassen. Um die Gefahr der Falscherkennung und Falschmeldung so gering wie möglich zu halten, werden Meldungen von mutmaßlichem sexuellem Kindesmissbrauch vom EU-Zentrum überprüft, bevor sie an die Strafverfolgungsbehörden und an Europol weitergeleitet werden. Sowohl Anbieter als auch Nutzer haben das Recht, jede sie betreffende Maßnahme vor Gericht anzufechten.*[7]

Ein wenig später wird von der Kommission erläutert, wie hilfreich die in einem gemeinsamen Gebäude mit Europol untergebrachte EU-Zentralbehörde sein soll. Sie

> *„die Anbieter von Online-Diensten insbesondere dabei, ihre neuen Verpflichtungen zur Durchführung von Risikobewertungen sowie zur Aufdeckung, Meldung, Entfernung und Sperrung von Kindesmissbrauchsinhalten zu erfüllen, indem es Indikatoren für die Aufdeckung von sexuellem Kindesmissbrauch bereitstellt und die Meldungen der Anbieter entgegennimmt;*
>
> *die nationalen Strafverfolgungsbehörden und Europol, indem es die Meldungen der Anbieter überprüft, um sicherzustellen, dass es sich nicht um Falschmeldungen handelt, und indem es sie schnell an die Strafverfolgungsbehörden weiterleitet. Dies wird dazu beitragen, dass Kinder vor Missbrauchssituationen bewahrt und die Täter der Justiz zugeführt werden;*
>
> *die Mitgliedstaaten, indem es als Wissenszentrum für bewährte Praktiken im Bereich der Prävention und Opferhilfe dient und einen evidenzbasierten Ansatz fördert;*

---

6 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation. Amtsblatt L 201 vom 31. Juli 2002 S. 4. Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32002L0058.

„The EU-Center should work closesly with Europol. It will receive the reports from providers, check them to avoid reporting obvious false positives and forward them to Europol as well asto national law enforcement authorities. A representative from Europol will be part of the management board of the EU Centre. In turn, a representative from the EU Centre could be part of the management board of Europol, to further ensure effective cooperation and coordination.“

Die Einzelheiten werden in den Art. 40 – 82 des Vorschlags für die Verordnung geregelt.

7 Europäische Kommission: Kampf gegen Kindesmissbrauch: Kommission präsentiert Gesetzesvorschlag zum Schutz von Kindern. Vom 11. Mai 2022. Abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/de/ip_22_2976.

die Opfer, indem es ihnen dabei hilft, dass die betreffenden Missbrauchsdarstellungen entfernt werden.“[8]

Zusammengefasst bedeutet dies, dass

- die nationale Koordinierungsbehörde dann eine entsprechende Anordnung des Gerichts oder der unabhängigen Verwaltungsbehörde im Mitgliedsland auf Ausleitung erwirkt,
- die Diensteanbieter daraufhin alle verdächtigen Nachrichten an die EU-Zentralbehörde übermitteln müssen,
- die EU-Zentralbehörde dann die von ihr geprüften Nachrichten an die Strafverfolgungsbehörden der Mitgliedstaaten übermittelt,
- die EU-Zentralbehörde Unternehmen bei der Erfüllung ihrer Verpflichtungen unterstützen wird. Sie *„wird die Indikatoren zur Erkennung von sexuellem Missbrauch festlegen und dadurch den Anbietern Gewissheit darüber geben, welche Inhalte in der EU illegal sind. Das Zentrum wird die Erkennungstechnologie und die Tools für die menschliche Überprüfung aller Meldungen kostenlos bereitstellen. Dadurch werden insbesondere kleinere Anbieter entlastet.“*[9]

- Coordination Authority of establishment

  Koordinierungsbehörde[10]

  Eine solche nationale Behörde muss in jedem Mitgliedsland eingerichtet werden. Sie beantragt bei den zuständigen Justizbehörden oder unabhängigen Verwaltungsbehörden die *„detection order“*.

---

8 Europäische Kommission: Kampf gegen Kindesmissbrauch: Kommission präsentiert Gesetzesvorschlag zum Schutz von Kindern. Vom 11. Mai 2022. Abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/de/ip_22_2976.

9 Europäische Kommission: Fragen und Antworten - neue Vorschriften zur Bekämpfung des sexuellen Missbrauchs von Kindern. Werden Dienstanbieter bei der Erfüllung dieser neuen Verpflichtungen unterstützt? Abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/de/qanda_22_2977.

10 Erwägungsgrund 44 des Vorschlags für die Verordnung:

„*In order to provide clarity and enable effective, efficient and consistent coordinationand cooperation both at national and at Union level, where a Member State designatesmore than one competent authority to apply and enforce this Regulation, it should designate one lead authority as the Coordinating Authority, whilst the designated authority should automatically be considered the Coordinating Authority where a Member State designates only one authority. For those reasons, the Coordinating Authority should act as the single contact point with regard to all matters related to the application of this Regulation, without prejudice to the enforcement powers of other national authorities.*“

Die Einzelheiten werden in den Art. 25 – 99 des Vorschlags für die Verordnung geregelt

3. Entwicklung

Die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation – e-Privacy-Richtlinie)[11] schützt in Art. 5 Abs. 1 und Art. 6 Abs. 1 die Vertraulichkeit der Kommunikation und der Verkehrsdaten.

In der Verordnung (EU) 2021/1232 des Europäischen Parlaments und des Rates vom 14. Juli 2021 über eine vorübergehende Ausnahme von bestimmten Vorschriften der Richtlinie 2002/58/EG hinsichtlich der Verwendung von Technologien durch Anbieter nummernunabhängiger interpersoneller Kommunikationsdienste zur Verarbeitung personenbezogener und anderer Daten zwecks Bekämpfung des sexuellen Missbrauchs von Kindern im Internet[12] wird von diesem umfassenden Schutz der Privatsphäre eine Ausnahme gemacht.[13]

Die – bis zum 3. August 2024 befristete – Verordnung erlaubt die

> *„freiwillige Nutzung von Technologien zur Verarbeitung personenbezogener und anderer Daten durch Anbieter in dem Umfang, der erforderlich ist, um sexuellen Missbrauch von*

11 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation. Amtsblatt L 201 vom 31. Juli 2002 S. 37 – 47. Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32002L0058.

12 Verordnung (EU) 2021/1232 des Europäischen Parlaments und des Rates vom 14. Juli 2021 über eine vorübergehende Ausnahme von bestimmten Vorschriften der Richtlinie 2002/58/EG hin-sichtlich der Verwendung von Technologien durch Anbieter nummernunabhängiger interpersoneller Kommunikationsdienste zur Verarbeitung personenbezogener und anderer Daten zwecks Bekämpfung des sexuellen Missbrauchs von Kindern im Internet. Amtsblatt L 274/41 vom 30. Juli 2021. Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32021R1232.

13 Genau genommen handelt es sich dabei um die Wiederherstellung einer schon früher bestehenden Ausnahme. Erwägungsgrund 9 der Verordnung (EU) 2021/1232 erläutert dies:

„Die Verarbeitung personenbezogener Daten durch Anbieter durch freiwillige Maßnahmen zur Aufdeckung sexuellen Missbrauchs von Kindern im Internet in ihren Diensten und der Meldung desselben und zur Entfernung von Online- Material über sexuellen Missbrauch von Kindern aus ihren Diensten unterlag bis zum 20. Dezember 2020 nur der Verordnung (EU) 2016/679. Die Richtlinie (EU) 2018/1972, die bis zum 20. Dezember 2020 umgesetzt werden musste, bewirkte, dass die Anbieter in den Anwendungsbereich der Richtlinie 2002/58/EG fallen. Um solche freiwilligen Maßnahmen nach dem 20. Dezember 2020weiterhin nutzen zu können, sollten die Anbieter die in der vorliegenden Verordnung festgelegten Bedingungen erfüllen. Die Verordnung (EU) 2016/679 wird weiterhin für die Verarbeitung personenbezogener Daten gelten, die mittels solcher freiwilligen Maßnahmen erfolgt.“

Kindern im Internet in ihren Diensten aufzudecken und zu melden und Online-Material über sexuellen Missbrauch von Kindern aus ihren Diensten zu entfernen."[14]

Dies bedeutet, dass Anbieter von Webmail und Messaging freiwillig im Kampf gegen Kinderpornographie Bilder und Textnachrichten der Nutzer unter diesem Aspekt durchsuchen dürfen.

Dies betrifft nur transportverschlüsselte Nachrichten, bei denen ein *„provider of hosting services or a provider of interpersonal communications services"* Zugriff auf den unverschlüsselten Inhalt der Bilder und Textnachrichten der Nutzer hat.

Zusammenfassend ist festzustellen, dass

- die inhaltliche Überprüfung eine freiwillige Angelegenheit des Diensteanbieters ist und
- nur transportverschlüsselte (s. dazu 7.1. auf S. 16) Nachrichten betrifft.

Um auch nach Ablauf der Befristung der Verordnung – nach Auffassung der Kommission – effektive Maßnahmen zur Verhinderung und Vorbeugung auf diesem Gebiet ergreifen zu können, hat die Kommission einen Vorschlag für die Verordnung vorgelegt.

Dieser Vorschlag unterscheidet sich grundsätzlich von der bisherigen Regelung dadurch, dass,

- die inhaltliche Überprüfung unter bestimmten Voraussetzungen eine Pflicht des Diensteanbieters ist,
- der Diensteanbieter eine Ausleitungspflicht an die zu schaffende EU-Zentralstelle hat und
- dies transportverschlüsselte und Ende-zu Ende-verschlüsselte Nachrichten (s. dazu 7.2. auf S. 18) gleichermaßen betrifft.

4. Stand der Gesetzgebung

Die Initiative der Kommission ist der erste Schritt in dem Gesetzgebungsverfahren nach Art. 294 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV[15] – s. Anhang S. 26).

---

14 Erwägungsgrund 12 der Verordnung (EU) 2021/1232 des Europäischen Parlaments und des Rates vom 14. Juli 2021 über eine vorübergehende Ausnahme von bestimmten Vorschriften der Richtlinie 2002/58/EG hin-sichtlich der Verwendung von Technologien durch Anbieter nummernunabhängiger interpersoneller Kommunikationsdienste zur Verarbeitung personenbezogener und anderer Daten zwecks Bekämpfung des sexuellen Missbrauchs von Kindern im Internet. Amtsblatt L 274/41 vom 30. Juli 2021. Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32021R1232.

15 Vertrag über die Arbeitsweise der Europäischen Union (konsolidierte Fassung). Amtsblatt C 326/47 vom sechsten 20. Oktober 2012. Abrufbar unter: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:de:PDF.

5. Motivation

In dem Vorschlag für die Verordnung wird betont[16], dass der Schutz von Kindern – sowohl offline als auch online – eine Priorität der Europäischen Union sei. Dabei wird hervorgehoben, dass im Übereinkommen der Vereinten Nationen über die Rechte des Kindes (UN-KRK)[17] und in Art. 24 Abs. 2 der Charta der Grundrechte der Europäischen Union[18] der Schutz und die Wahrung des Wohls und der Interessen von Kindern als Rechte verankert sind. Außerdem wird darauf verwiesen, dass 2021 der Ausschuss der Vereinten Nationen für die Rechte des Kindes sich dafür ausgesprochen habe, dass diese Rechte auch im digitalen Umfeld geschützt werden müssen.[19]

Außerdem wird auf die Richtlinie über den sexuellen Missbrauch von Kindern[20], die EU-Kinderrechtsstrategie[21] und die EU-Strategie für eine wirksamere Bekämpfung des sexuellen Kindesmissbrauchs[22] Bezug genommen.

Freiwillige Maßnahmen einiger weniger Diensteanbieter hätten bisher nicht den gewünschten Erfolg gehabt, sodass einige Mitgliedstaaten nationale Regelungen entweder planten oder schon

---

16 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down rules to prevent and combat child sexual abuse from the 11th Mai 2022 – COM/2022/209 final, S. 1-8. Abrufbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472.

17 Übereinkommen über die Rechte des Kindes. Bundesgesetzblatt II, S. 990 vom 10. Juli 1992, Abrufbar unter: https://www.bmfsfj.de/resource/blob/93140/78b9572c1bffdda3345d8d393acbbfe8/uebereinkommen-ueber-die-rechte-des-kindes-data.pdf.

18 Charta der Grundrechte der Europäischen Union. Amtsblatt C 202/389 vom 7. Juni 2016. Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:12016P/TXT&from=LT.

19 Allgemeine Bemerkung Nr. 25 (2021) des Ausschusses für die Rechte des Kindes der Vereinten Nationen über die Rechte der Kinder im digitalen Umfeld. Vereinte Nationen CRC/C/GC/25 vom 24. März 2021. Abrufbar unter: https://www.dkhw.de/fileadmin/Redaktion/1_Unsere_Arbeit/1_Schwerpunkte/2_Kinderrechte/2.14_Koordinierungsstelle_Kinderrechte/2.14.1_Kinderrechte_in_der_digitalen_Welt/Allgemeine_Bemerkung_25_final_09_11_2021_so6.pdf.

20 Richtlinie 2011/92/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates. Amtsblatt L 335/1 vom 17. Dezember 2011. Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32011L0093.

21 EU-Kinderrechtsstrategie. Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Nationen vom 24. März 2021. Abrufbar unter: https://ec.europa.eu/info/sites/default/files/1_de_act_part1_v2_1.pdf.

22 EU-Strategie für eine wirksame Bekämpfung des sexuellen Missbrauchs von Kindern. Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Nationen vom 24. Juli 2020. Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020DC0607&from=EN.

verabschiedet hätten. Dadurch drohe eine Fragmentierung des Kampfes gegen Kinderpornographie einerseits und nach dem Bericht über die Folgenabschätzung[23] zu dem Vorschlag der Kommission für die Verordnung eine stärkere Fragmentierung des digitalen Binnenmarktes für Dienstleistungen andererseits.

Der Vorschlag für die Verordnung hebt die Bedeutung und Notwendigkeit der Abwägung zwischen den zu treffenden Maßnahmen und den Grundrechten der Beteiligten hervor:

> *„It is therefore particularly important to establish a fair balance between measures to protect child victims of sexual abuse and their fundamental rights and thus to achieve important objectives of general societal interest, and the fundamental rights of other users and of the providers.“*[24]

6. Inhalt

Der Vorschlag der Kommission statuiert unter der Voraussetzung einer mehrstufigen Risikoabwägung eine Pflicht der Diensteanbieter, Material über sexuellen Missbrauch von Kindern und Grooming zu erkennen, zu melden, zu sperren und aus ihren Diensten zu entfernen. Dadurch soll eine bessere Aufdeckung, Untersuchung und Verfolgung von Straftaten ermöglicht werden.

Der Inhalt des ungefähr 140-seitigen Vorschlags der Kommission sei hier in den Grundzügen dargestellt:

6.1. Verpflichtete

Art. 1 Nr. 1 des Vorschlags für die Verordnung statuiert:

> *„(a) obligations on providers of relevant information society services to minimise the risk that their services are misused for online child sexual abuse;*
> *(b) obligations on providers of hosting services and providers of interpersonal communication services to detect and report online child sexual abuse;*
> *(c) obligations on providers of hosting services to remove or disable access to child sexual abuse material on their services;*

---

23 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down rules to prevent and combat child sexual abuse from the 11th Mai 2022 – COM/2022/209 final, S. 8-15. Abrufbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472.

24 Ebd., S. 4.

(d) obligations on providers of internet access services to disable access to child sexual abuse material;“[25]

Die genauen Definitionen der Begriffe finden sich in Art. 2 des Vorschlags für die Verordnung[26]. Im Folgenden werden lediglich die Verpflichtungen der Anbieter von Hosting-Diensten und von Diensten der interpersonellen Kommunikation (Diensteanbieter) dargestellt. Die Verpflichtungen betreffen dabei Diensteanbieter aller Größenordnungen.

6.2. Voraussetzungen für die Verpflichtung

Nach Art. 3 des Vorschlags für die Verordnung[27] müssen die Diensteanbieter eine Risikobewertung unter den in Abs. 2 genannten Aspekten vornehmen und das Risiko der Nutzung des Dienstes zum Zwecke des sexuellen Missbrauchs von Kindern im Internet ermitteln, analysieren und bewerten.

Nach Abs. 3 können die Diensteanbieter auch das EU Centre (EU-Zentralbehörde) bitten, eine Analyse von Daten Stichproben durchzuführen und so die Risikobewertung zu unterstützen. Die dabei entstehenden Kosten sollen die Diensteanbieter tragen.

Abs. 4 sieht vor, dass die Diensteanbieter diese Risikobewertung aus gegebenem Anlass, mindestens aber alle drei Jahre vornehmen.

Art. 4 des Vorschlags für die Verordnung[28] befasst sich mit der Minimierung des in der Risikobewertung festgestellten Risikos und den dafür erforderlichen Maßnahmen. In Abs. 1 wird dazu festgelegt:

> *„Providers of hosting services and providers of interpersonal communications services shall take reasonable mitigation measures, tailored to the risk identified pursuant to Article 3, to minimise that risk…“*

Im Text des Vorschlags für die Verordnung werden keine exakten Kriterien für die Risikobewertung genannt. Diese sollen von der EU-Zentralbehörde festgelegt werden. Die Art der zu ergreifenden Maßnahmen durch die Diensteanbieter wird durch unbestimmten Rechtsbegriffe beschrieben.

---

25 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down rules to prevent and combat child sexual abuse from the 11th Mai 2022 – COM/2022/209 final S. 38. Abrufbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472.

26 Ebd., S. 39.

27 Ebd., S. 42f.

28 Ebd., S. 43f.

Die Art und der Umfang der ergriffenen Maßnahmen ist innerhalb von drei Monaten nach Art. 5 des Vorschlags für die Verordnung[29] der Coordinating Authority of establishment (Koordinierungsbehörde [für die Niederlassung]) zu melden. Auch der EU-Zentralstelle soll dies gemeldet werden.

Wenn *„there is evidence of a significant risk of the service being used for the purpose of online child sexual abuse, there is evidence of a significant risk of the service being used for the purpose of online child sexual abuse“* und die Grundrechtsabwägung ergeben hat, dass *„the reasons for issuing the detection order outweigh negative consequences for the rights and legitimate interests of all parties affected, having regard in particular to the need to ensure a fair balance between the fundamental rights“* (Art. 7 Abs. 4 des Vorschlags für die Verordnung[30]), kann eine die Diensteanbieter verpflichtende „detection order“ ergehen.

6.3. Verpflichtende Stelle

Die Koordinierungsbehörde fordert nach Art. 7 Abs. 1 des Vorschlags für die Verordnung[31] die Justizbehörden des Mitgliedstaats oder eine andere unabhängige Verwaltungsbehörde dazu auf, eine *„detection order“* gegenüber den Diensteanbietern zu erlassen, wenn Maßnahmen der Diensteanbieter das Risiko nicht oder nur unzureichend minimieren.

Die Koordinierungsbehörde legt dabei den Justizbehörden oder der unabhängigen Verwaltungsbehörde den Antrag auf Erteilung der *„detection order“* zusammen mit dem – unzureichenden – Abhilfeplan der Diensteanbieter sowie den Einschätzungen der EU-Zentralbehörde und der Datenschutzbehörde vor (Art. 7 Abs. 3 des Vorschlags für die Verordnung[32]).

6.4. Inhalt der Verpflichtung der Diensteanbieter

Nach Erhalt der „*detection order*“ müssen die Diensteanbieter nach Art. 10 Abs. 1 des Vorschlags für die Verordnung[33] Technologien installieren und betreiben, um neues und bekanntes kinderpornografisches Material oder Grooming zu erkennen.

---

29 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down rules to prevent and combat child sexual abuse from the 11th Mai 2022 – COM/2022/209 final S. 44f. Abrufbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472.

30 Ebd., S. 47.

31 Ebd., S. 46.

32 Ebd., S. 46.

33 Ebd., S. 51.

Gem. Art. 12 und 13 des Vorschlags für eine Verordnung[34] müssen die Diensteanbieter Informationen über einen möglichen Kindesmissbrauch an die EU-Zentralbehörde ausleiten. Dabei müssen u.a. auch alle Inhaltsdaten – Bilder Videos und Text – ausgeleitet werden.

Art. 10 Abs. 2 des Vorschlags für die Verordnung räumt den Diensteanbietern das Recht ein, entsprechende Technologien zu diesem Zweck kostenlos von der EU-Zentralbehörde zu erhalten.

Diese Technologie sollen nach Abs. 3 dem jeweiligen Stand der Technik entsprechen und nur die unbedingt erforderlichen Informationen mit einer möglichst geringen Fehlerquote zu extrahieren.

Zur Vermeidung von *„false positive“* Meldungen müssen die Diensteanbieter nach Abs. 4 eine Vielzahl von Maßnahmen treffen. U.a. müssen sie eine *„regular human oversight as necessary to ensure that the technologies operate in a sufficiently reliable manner and, where necessary, in particular when potential errors and potential solicitation of children are detected, human intervention“* gewährleisten.

Abs. 5 schreibt den Diensteanbietern vor, die Nutzer über den Einsatz dieser Technologien klar, verständlich und an hervorgehobener Position zu informieren. Dies gilt auch für den Umstand, dass verdächtige Informationen an die EU-Zentralbehörde ausgeleitet werden.

6.5. Weiterleitung der Informationen durch die EU-Zentralbehörde

Nach Art. 48 Abs. 3 des Vorschlags für die Verordnung leitet die EU-Zentralbehörde bei einem nicht völlig unbegründeten Verdacht die Nachricht an die Strafverfolgungsbehörden des Mitgliedslands weiter.

6.6. Lösch- und Blockieranordnungen

Gemäß Art. 14 des Vorschlags für die Verordnung[35] ersucht die Koordinierungsbehörde die zuständige Justizbehörde des Mitgliedstaats oder eine andere unabhängige Verwaltungsbehörde des Mitgliedstaats, eine Anordnung zu erlassen, die Diensteanbieter unter der Jurisdiktion eines Mitgliedstaats dazu verpflichtet, kinderpornografisches Material entweder zu entfernen oder den Zugang dazu in allen Mitgliedstaaten zu sperren. Dies muss grundsätzlich innerhalb von 24 Stunden geschehen.

Art. 16 des Vorschlags für die Verordnung[36] sieht in diesen Fällen ein ähnliches Verfahren vor, durch das die Internetprovider oder Zugangsanbieter durch eine Blockieranordnung verpflichtet werden, *„to take reasonable measures to prevent users from accessing known child sexual abuse*

---

34 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down rules to prevent and combat child sexual abuse from the 11th Mai 2022 – COM/2022/209 final S. 53ff. Abrufbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472.

35 Ebd., S. 54f.

36 Ebd., S. 54f.

material indicated by all uniform resource locators on the list of uniform resource locators included in the database of indicators, in accordance with Article 44(2), point (b) and provided by the EU Centre.“

7. Technische Hintergründe

Der Vorschlag der Kommission für die Verordnung sieht beim Vorliegen eines konkreten Risikos einer Nutzung des Dienstes für Kindesmissbrauch bzw. Grooming eine Verpflichtung der Anbieter vor, diese zu „erkennen“ und „zu melden“. Welche Technologie hierfür einzusetzen ist, sieht der Vorschlag dagegen nicht vor; daher seien hier die technischen Möglichkeiten skizziert.

Hinsichtlich des technischen Hintergrundes der Dienste ist dabei zwischen unverschlüsselter bzw. transportverschlüsselter (auch Punkt-zu-Punkt-verschlüsselte Kommunikation genannt) und Ende-zu-Ende verschlüsselter Kommunikation zu unterscheiden.

7.1. Transportverschlüsselung

Bei der Transportverschlüsselung (z.B. E-Mail-Programme, Facebook-Messenger, Instagram-Nachrichten) wird zwischen dem Nutzer und dem Server des Diensteanbieters eine verschlüsselte Verbindung aufgebaut. Der Inhalt der Dateien wird nicht verschlüsselt.

In einem weiteren Schritt werden die unverschlüsselten Daten dann über eine durch Verschlüsselung gesicherte Verbindung an den Server des Diensteanbieters des Empfängers weitergeleitet.

Die Weiterleitung der unverschlüsselten Daten vom Server des Diensteanbieters des Empfängers über eine ebenfalls durch Verschlüsselung gesicherte Verbindung an diesen ist der letzte Schritt.

Die Daten werden nur zwischen den Knotenpunkten durch eine verschlüsselte Verbindung gesichert – an den Knotenpunkten wie z.B. dem Server des Diensteanbieters sind die Daten kurzzeitig unverschlüsselt und daher lesbar. Deshalb wird die Transportverschlüsselung auch als Punkt-zu-Punkt-Verschlüsselung bezeichnet. Der Diensteanbieter hat also in diesem Moment Zugriff auf den unverschlüsselten Inhalt der Nachrichten.[37] Er kann also in diesem Moment – sowohl durch Künstliche Intelligenz (KI) als auch durch Menschen – den Inhalt der Nachrichten[38] kontrollieren.

7.1.1. Textnachrichten

Textnachrichten können ohne besondere Schwierigkeiten nach Stichwörtern durchsucht werden. In Anbetracht des aktuellen Erkenntnisstandes kann keine definitive Aussage getroffen werden,

---

37 Bundesamt für Sicherheit in der Informationstechnik: Verschlüsselt kommunizieren im Internet. Transportverschlüsselung. Abrufbar unter: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Verschluesselt-kommunizieren/verschluesselt-kommunizieren_node.html.

38 Nachrichten in diesem Sinne sind Textnachrichten, Sprachnachrichten und Bilder/Videos.

inwieweit und mit welcher Fehlerquote KI den Sinn von Sprache erfassen kann, was beispielsweise für die Unterscheidung von Grooming und unproblematischer Kommunikation relevant ist.

7.1.2. Bilder

Bei Bildern und Videos ist zu unterscheiden zwischen solchen, die – z.B. aufgrund der Durchsuchung von Festplatten der Computer von Kriminellen – den Ermittlungsbehörden als kinderpornographisches Material bekannt sind, und solchen, die ihnen noch nicht bekannt sind.

7.1.2.1. Den Ermittlungsbehörden bekannte Bilder

Bilder, die den Ermittlungsbehörden bekannt sind, können durch einen Hashing-Algorithmus gekennzeichnet werden. Durch das Hashing werden die Daten der Bilder in kleine Teile zerlegt und in einer bestimmten Struktur geordnet. Prüfsummen „digitale Fingerabdrücke“, werden erzeugt. Diese Hashwerte ermöglichen es, bestimmte Bilder schnell zu finden, weil nicht der gesamte Datensatz analysiert werden muss.

Insofern können Diensteanbieter Bilder, die den Ermittlungsbehörden bekannt sind und deren Hashwert den Diensteanbietern übermittelt worden ist, unproblematisch erkennen und automatisch ausleiten.

7.1.2.2. Veränderungen an Bildern, die den Ermittlungsbehörden bekannt sind

Veränderungen an Bildern – z.B. das Ändern auch nur eines einzigen Pixels – verändern den Hashwert, sodass sie nicht mehr automatisch erkannt werden können. In dieser Arbeit kann nicht darauf eingegangen werden, inwieweit KI in der Lage ist, veränderte bekannte Bilder mit welcher Fehlerquote zu identifizieren.

7.1.2.3. Bilder, die den Ermittlungsbehörden noch nicht bekannt sind

Von Bildern, die den Ermittlungsbehörden noch nicht bekannt sind, liegen keine Hashwerte vor, sodass sie nicht automatisiert abgeglichen werden können. Insofern müssen diese Bilder durch KI überprüft werden. Inwieweit und mit welcher Fehlerquote KI in der Lage ist, harmlose Familienbilder wie z.B. ein am Strand spielendes nacktes Kleinkind von fotografischen Dokumentationen krimineller Handlungen zu unterscheiden, kann hier nicht dargestellt werden.

7.1.3. Sprachnachrichten

Auch hinsichtlich der technischen Möglichkeiten und Voraussetzungen der automatischen Analyse, Bewertung und Ausleitung von Sprachnachrichten durch KI bedarf es einer gesonderten Prüfung.

7.2. Ende-zu-Ende-Verschlüsselung

Bei der Ende-zu-Ende-Verschlüsselung (z.B. bei WhatsApp, Threema, Signal) ist die Nachricht[39] auf dem gesamten Weg von der Absendung durch den Nutzer bis zum Empfänger permanent durch Verschlüsselung geschützt: Die Nachricht *„wird vor dem Versand mit dem öffentlichen Schlüssel des Adressaten verschlüsselt und wird erst beim Empfang durch dessen zweiten passenden und geheimen Schlüssel geöffnet.“*[40] Dadurch kann der Inhalt der Nachricht weder durch den Diensteanbieter des Absenders auf seinem Server noch an den Knotenpunkten oder auf dem Server des Diensteanbieters des Empfängers ermittelt werden.

Das Bundesamt für die Sicherheit in der Informationstechnik (BSI) erläutert die Funktionsweise folgendermaßen:

> *„Der Absender oder die Absenderin kann eine Prüfsumme, auch Hashwert genannt, aus der versandfertigen E-Mail berechnen und diese mit dem eigenen geheimen Schlüssel kodieren. Das ist dann eine digitale Signatur, die einem Fingerabdruck oder Stempel entspricht und an die E-Mail angehängt werden kann. Der Adressat berechnet einerseits ebenfalls die Prüfsumme der empfangenen E-Mail und entschlüsselt andererseits mit dem öffentlichen Schlüssel des Absenders dessen angehängte Signatur, wodurch er die vom Absender errechnete Prüfsumme erhält. Stimmen beide Prüfsummen überein, weiß der Empfänger, dass die Mail nicht verändert wurde, also die Integrität gegeben ist.*
>
> *Ferner kann er oder sie verifizieren, dass die Mail wirklich vom Besitzer des passenden geheimen Schlüssels stammt und damit die Authentizität stimmt. Das asymmetrische Schlüsselpaar des Absenders oder der Absenderin kann so die Integrität und Authentizität der E-Mail garantieren.“*[41]

Das BSI kommt zu dem Schluss:

> *„Nur die Ende-zu-Ende-Verschlüsselung garantiert daher einen Komplettschutz der übertragenden Datenpakete und erfüllt drei wichtige Ziele der Verschlüsselung im Internet:*
>
> > ***Schutz der Vertraulichkeit:*** *Die Nachrichten oder Daten sind nur für denjenigen im Klartext zu lesen oder deutlich zu hören, für den sie bestimmt ist.*
> >
> > ***Schutz der Authentizität:*** *Die Echtheit des Absenders wird verifiziert. Der Absender ist wirklich die Person, die als Absender angegeben wird.*

---

39 Nachrichten in diesem Sinne sind Textnachrichten, Sprachnachrichten und Bilder/Videos.

40 Bundesamt für Sicherheit in der Informationstechnik: Verschlüsselt kommunizieren im Internet. Ende-zu-Ende-Verschlüsselung. Abrufbar unter: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Verschluesselt-kommunizieren/verschluesselt-kommunizieren_node.html.

41 Ebd.

> ***Schutz der Integrität:*** *Die Nachricht kann auf dem Weg vom Absender zum Empfänger nicht unbemerkt durch Dritte verändert werden.“*[42]

Dies führt dazu, dass der Diensteanbieter selbst bei einer entsprechenden staatlichen Verpflichtung technisch keine Möglichkeit hat, nach der Absendung auf den Inhalt der Nachrichten zuzugreifen. Dies gilt auch für den Diensteanbieter des Empfängers.

Deshalb ist bei der Ende-zu-Ende-Verschlüsselung ein Zugriff auf die Inhalte eher durch eine auf den Geräten der Nutzer zu installierende Software möglich, die die Daten auf den Geräten der Nutzer vor oder nach deren Verschlüsselung scannt, das sog. „Client Side Scanning“ (CSS).

7.3. Scan-Software auf dem Gerät der Nutzer – „Client Side Scanning“ (CSS)

Client-Side-Scanning (CSS) erfolgt durch eine Software auf dem Gerät des Nutzers. Eingehende Nachrichten[43] werden gescannt und daraufhin analysiert, ob sie kinderpornographische Inhalte beinhalten oder Grooming sind. Wie genau dieser Abgleich technisch realisiert wird, kann im Rahmen dieser Arbeit nicht dargestellt werden.[44]

Die unter 7.1.1. bis 7.1.3. angesprochenen Probleme der Identifikation und Analyse der übermittelten Inhalte bestehen auch bei diesem Verfahren.

7.4. Verwendung von Meta-Daten

Darüber hinaus wird noch diskutiert, die bei den Diensteanbietern vorliegenden Meta-Daten der Nutzer mit dem vermeintlichen Nutzerverhalten der Kriminellen zu vergleichen. Diese Theorie geht davon aus, dass Menschen, die Kinderpornographie konsumieren oder kommerzialisieren, ein bestimmtes Nutzungsverhalten haben, z.B. viele Fotos innerhalb von Chat-Gruppen verteilen.

Fraglich ist, inwieweit diese Ansicht durch Tatsachen gestützt werden kann und inwieweit sie zu falschen Positiv-Meldungen führt.

7.5. Leistungsfähigkeit der Künstlichen Intelligenz

Ebenfalls fraglich ist, inwieweit KI in der Lage ist, strafbare Beiträge von (noch) legalen Inhalten zu unterscheiden – s. dazu 6.1.1. bis 6.1.3.

---

42 Bundesamt für Sicherheit in der Informationstechnik: Verschlüsselt kommunizieren im Internet. Ende-zu-Ende-Verschlüsselung. Abrufbar unter: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Verschluesselt-kommunizieren/verschluesselt-kommunizieren_node.html.

43 Nachrichten in diesem Sinne sind Textnachrichten, Sprachnachrichten und Bilder/Videos.

44 Eine gute Zusammenfassung findet sich in: Breithut, Jörg: Kampf gegen Kindesmissbrauch. Bürgerrechtler wehren sich gegen ein europäisches Chat-Überwachungsgesetz. In: spiegel.de vom 19. März 2022.

7.6. Zwischenfazit

In technischer Hinsicht gibt es noch erheblichen Klärungsbedarf, ob und inwieweit die in der Verordnung definierten Ziele der Kommission und damit verbundene technischen Abläufe realisiert werden können.

8. Kritikpunkte in der öffentlichen Diskussion – aktuelle Rezeption

> *„Ich halte unseren Plan für bahnbrechend, denn wir schützen sowohl die Privatsphäre der Internet-Nutzer als auch die Kinder und uns ist es gelungen, beides unter einen Hut zu bringen.“*[45]

Diese Ansicht wird von vielen nicht geteilt. In der öffentlichen Diskussion der letzten Wochen sind eine Vielzahl von Aspekten angesprochen worden, von denen zumindest einige hier genannt werden sollen:

8.1. Verstoß gegen elementare Grundrechte

Der Medienrechtler Stephan Dreyer zeigte im „Deutschlandfunk“ das Spannungsfeld auf: *„Die Freiheit unserer digitalen Kommunikation auf der einen Seite, die Sicherheit von Kindern und Jugendlichen im Netz auf der anderen.“*

Er sieht in der Überwachung von Nachrichten durch die Diensteanbieter eine *„systematische Überwachung von Privatkommunikation“*.

Er kommt zu dem Schluss, dass eine solche Überwachung einer gerichtlichen Prüfung nicht standhalten werde, da die grundrechtlich geschützte Kommunikation zwischen Individuen angegriffen werde.

Sein Fazit: *„Eine bevölkerungsweite, anlasslose Überwachung von Individualkommunikation ist aus meiner Sicht weder national noch auf EU-Ebene mit den geltenden Menschenrechtsrahmen vereinbar. Das haben die europäischen Gerichte mehrfach deutlich gemacht, dass das so nicht funktionierte. Insofern bin ich etwas schockiert über die Nonchalance, mit der hier auf entsprechende grundrechtliche Verbürgungen heruntergesehen wird.“* [46]

Die ehemalige Thüringer Justizministerin und jetzige MdEP Marion Walsmann vertritt dagegen die Auffassung, dass auch das Recht auf private Kommunikation in verhältnismäßigen Rahmen

---

45 EU-Kommissarin Ylva Johannson. Zitiert nach: Umstrittene ChatkKontrolle. Werden Sie jetzt zur Zensur-Ylva, Frau Kommissarin? Interview mit Ylva Johannson. Spiegel.de vom 13. Mai 2022.

46 Deutschlandfunk. EU-Gesetz gegen Kindesmissbrauchsinhalte. Chatkontrolle „nicht mit Menschenrechten vereinbar“. Gespräch zwischen Sören Brinkmann und dem Medienrecht nach Stephan Dreyer vom 11. Mai 2022. Abrufbar unter: https://www.deutschlandfunk.de/chatkontrolle-eu-messenger-kindesmissbrauch-scanning-durchsuchung-kommission-gesetzentwurf-100.html.

eingeschränkt werden könne, wenn der Schutz eines Kindes vor grausamer Gewalt auf dem Spiel stehe: *„Datenschutz darf nicht zum Täterschutz werden.“*[47]

8.2. Kein konkreter Richtervorbehalt bei der Übermittlung der Daten an die EU-Zentralbehörde

Die EU-Zentralbehörde kann aufgrund ihrer Macht hinsichtlich der Risikoeinschätzung bei den Diensteanbietern den Koordinationsbehörden der Mitgliedsländer vorschreiben, bei den Justizbehörden oder anderen unabhängigen Behörden eine Anordnung zu beantragen. Diese sieht vor, dass eine Vielzahl von Nachrichten bei einem entsprechenden Verdacht – also nicht bei einem entsprechenden Nachweis – an die EU-Zentralbehörde ausgeleitet werden müssen.

Die Kritik richtet sich dagegen, dass hier Grundrechte nicht etwa aufgrund eines konkreten Anlasses, sondern aufgrund einer abstrakten – und dazu noch nicht einmal transparenten – Risikoabwägung aufgehoben werden.[48]

8.3. Mögliche Ausdehnung über den Bereich der Kinderpornographie hinaus

Tom Jennigsen vom Verein Digitale Gesellschaft befürchtet eine Ausdehnung der dann vorhandenen Überwachungstechnologien auch auf andere Felder: „*Seien es weitere Kriminalitätsfelder, sei es Aktivismus, politische Opposition oder whistleblower: Gerade autoritäre Regime weltweit würden sich über die Vorlage der EU und die Etablierung entsprechender Technologien freuen.“*[49]

8.4. Geringe Benutzung von Messaging-Diensten für die Verbreitung kinderpornographischer Inhalte

Der Chaos Computer Club zieht bereits den Ansatz der Kommission – und damit die Geeignetheit des Mittels zur Erreichung des Zwecks – in Zweifel: *„Zweifellos muss den Betroffenen von Kindesmissbrauch besser geholfen werden, die Chatkontrolle ist allerdings ein überbordender Ansatz, leicht zu umgehen und setzt an der völlig falschen Stelle an. Ohne erwartbaren Erfolg im Sinne des eigentlichen Ziels soll ein nie dagewesenes Überwachungswerkzeug eingeführt werden.“*[50]

---

47 Zitiert nach: Mayntz, Gregor: Wie die EU sexuellen Kindermissbrauch im Netz bekämpfen will. In: Saarbrücker Zeitung vom 12. Mai 2022.

48 MMR-Aktuell 2022, 448870, ZD-Aktuell 2022, 01173, Heise, c't, Holger Bleich: Massenüberwachung durch die Hintertür. Abrufbar unter: https://www.heise.de/select/ct/2022/13/2213311415464909776.

49 Zitiert nach: Schmidt, Joel: Härteres Durchgreifen im Netz. In: Neues Deutschland vom 4. Juni 2022, S. 7.

So auch: Deutschlandfunk: EU-Gesetz gegen Kindesmissbrauchsinhalte. Chatkontrolle „nicht mit Menschenrechten vereinbar“. Gespräch zwischen Sören Brinkmann und dem Medienrecht nach Stephan Dreyer vom 11. Mai 2022. Abrufbar unter: https://www.deutschlandfunk.de/chatkontrolle-eu-messenger-kindesmissbrauch-scanning-durchsuchung-kommission-gesetzentwurf-100.html.

50 Chaos Computer Club: EU-Kommission will alle Chatnachrichten durchleuchten. Vom 9. Mai 2022. Abrufbar unter:https://www.ccc.de/de/updates/2022/eu-kommission-will-alle-chatnachrichten-durchleuchten.

Hintergrund ist, dass das eigentliche kinderpornographische Material verschlüsselt bei den üblichen webhostern gespeichert wird. Die erforderlichen Schlüssel werden dann im Darknet und nicht über Messenger-Dienste ausgetauscht: *„Die Täter*innen nutzen statt den von der Kommission ins Visier genommenen Messengern öffentliche Hoster – nicht zuletzt, weil Messenger zum Tauschen großer Dateisammlungen völlig ungeeignet sind. Vor dem Tausch verschlüsseln sie die Daten zudem zusätzlich.“*[51]

Patrick Beyer, MdEP bekräftigt dies:

> *„Die Chat-Kontrolle hilft dabei gar nicht. Kinderporno-Ringe tauschen sich nicht über den Facebook-Messenger oder Gmail aus.“*

Sogar in den Fällen, in denen tatsächlich ein Austausch über die genannten Dienste stattfände, hülfe diese Technik nicht, da die Dateien auch hier in der Regel verschlüsselt seien.[52]

Allein schon deshalb werde – so der Chaos Computer Club – die geplante Überwachung die Weiterverbreitung von Missbrauchsabbildungen nicht verhindern.[53]

8.5. Scan-Software auf dem Gerät der Nutzer – „Client Side Scanning“ (CSS)

Das bei der von Ende-zu-Ende-Verschlüsselung anzuwendende Verfahren der Überwachung durch Scan-Software auf dem Gerät der Nutzer (s. dazu 7.3. auf S. 19) beinhalte – so Dreyer – die Gefahr, *„dass hier ein Generalschlüssel für verschlüsselte Kommunikation mit drin steckt.“*[54]

Umfassender nimmt dazu der Chaos Computer Club Stellung:

> *„Nicht nur Journalist*innen und Whistleblower*innen sind auf vertrauenswürdige Kommunikation angewiesen – sie ist ein Grundrecht und wichtiger Eckpfeiler unser aller IT-Sicherheit. Damit Kommunikation tatsächlich vertrauenswürdig ist, müssen zwei Bedingungen erfüllt sein:*
>
> - *Das eigene Gerät muss integer sein und darf Inhalte nicht an Dritte ausleiten.*

---

51 Chaos Computer Club: EU-Kommission will alle Chatnachrichten durchleuchten. Vom 9. Mai 2022. Abrufbar unter:https://www.ccc.de/de/updates/2022/eu-kommission-will-alle-chatnachrichten-durchleuchten.

52 Breithut, Jörg: Kampf gegen Kindesmissbrauch. Bürgerrechtler wehren sich gegen ein europäisches Chat-Überwachungsgesetz. In: spiegel.de vom 19. März 2022.

53 Chaos Computer Club: EU-Kommission will alle Chatnachrichten durchleuchten. Vom 9. Mai 2022. Abrufbar unter:https://www.ccc.de/de/updates/2022/eu-kommission-will-alle-chatnachrichten-durchleuchten.

54 Deutschlandfunk. EU-Gesetz gegen Kindesmissbrauchsinhalte. Chatkontrolle „nicht mit Menschenrechten vereinbar“. Gespräch zwischen Sören Brinkmann und dem Medienrecht nach Stephan Dreyer vom 11. Mai 2022. Abrufbar unter: https://www.deutschlandfunk.de/chatkontrolle-eu-messenger-kindesmissbrauch-scanning-durchsuchung-kommission-gesetzentwurf-100.html.

- *Die Verschlüsselung muss sicher sein, sodass wir dem Netz nicht vertrauen müssen.*

*Mit dem Fernmeldegeheimnis und dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme setzt die Chatkontrolle gleich zwei fundamentale Grundrechte außer Kraft. Nutzer*innen verlieren die Kontrolle darüber, welche Daten sie wie mit wem teilen. Sie verlieren das Grundvertrauen in ihre eigenen Geräte.*

Bisher ist nicht klar, wer die Erkennungsalgorithmen und -datenbanken definieren und kontrollieren soll. Ein derart intransparentes System kann und wird nach seiner Einführung leicht erweitert werden. So ist schon heute absehbar, dass sich die Rechteverwertungsindustrie für das System ebenso brennend interessieren wird wie demokratiefeindliche Regierungen. Umso erschreckender ist, mit welcher Arglosigkeit es nun eingeführt werden soll.“[55]

Der Vorschlag für die Verordnung ist aber auch für andere, zurzeit noch nicht bekannte Möglichkeiten offen, das *„ist eine Möglichkeit unter mehreren. Unser Gesetzesvorschlag beschränkt sich nicht auf ein konkretes Verfahren. Ich will verhindern, dass unser Plan wegen des rasanten technischen Fortschritts schon obsolet ist, bis wir das Gesetz finalisiert haben.“*[56]

8.6. Entwicklung von Erkennungssoftware durch EU-Zentralbehörde

Es wird bezweifelt, dass die EU-Zentralbehörde dazu in der Lage sein wird, eine Erkennungssoftware mit geringer Fehlerquote zu entwickeln und den Diensteanbietern zur Verfügung zu stellen.

8.7. Anzahl der „false positive“-Meldungen

Es gibt derzeit keine validen Zahlen darüber, wie viele (in absoluten Zahlen) Nachrichten von den Diensteanbietern an die EU-Zentralbehörde ausgeleitet werden und wie viele davon „false positive“ sein werden. Ebenso wenig gibt es Annahmen darüber, wie viele Menschen in der EU-Zentralbehörde die ausgeleiteten Nachrichten überprüfen werden. Auch hinsichtlich der Fähigkeiten der KI scheint es noch keine gesicherten Erkenntnisse zu geben, *„das ist einer der Gründe, warum ich so großen Wert darauf lege, unseren Vorschlag Technologie neutral zu halten – denn die Anwendung der künstlichen Intelligenz beispielsweise entwickelt sich rasend schnell weiter , und ich hoffe, sie werden besser und präziser.“*[57]

Der Chaos Computer Club fasst zusammen:

> *„Eine ‚künstliche Intelligenz‘, die auf Missbrauchsinhalte untersucht, wird auch Inhalte fälschlicherweise als illegal markieren. Auch kleinste Fehlerquoten würden zu massiven Mengen an fälschlicherweise ‚erkannter‘ und ausgeleiteter Nachrichten führen: Allein in*

---

55 Chaos Computer Club: EU-Kommission will alle Chatnachrichten durchleuchten. Vom 9. Mai 2022. Abrufbar unter:https://www.ccc.de/de/updates/2022/eu-kommission-will-alle-chatnachrichten-durchleuchten.

56 EU-Kommissarin Ylva Johannson. Zitiert nach: Umstrittene ChatkKontrolle. Werden Sie jetzt zur Zensur-Ylva, Frau Kommissarin? Interview mit Ylva Johannson. Spiegel.de vom 13. Mai 2022.

57 Ebd.

Deutschland werden weit mehr als eine halbe Milliarde Nachrichten pro Tag versendet. Auch enorm ‚gute' Erkennungsraten würden zur Ausleitung mehrerer Tausend Nachrichten pro Tag führen."[58]

8.8. Abgrenzungsprobleme

Problematisch ist die Abgrenzung zwischen kinderpornographischem Material und legalen Bildern. Es spricht viel dafür, dass diese Abgrenzung bis auf weiteres nur durch menschliche Einsichtnahme in die ausgeleiteten Nachrichten vorgenommen werden kann. Der Chaos Computer Club zieht folgendes Resümee:

„Die Wahrscheinlichkeit der Ausleitung steigt natürlich bei privatem, völlig legalem und konsensuellen Bildertausch unter Erwachsenen und Jugendlichen. Junge Erwachsene dürfen sich schon jetzt auf die Schätzung ihres Alters durch die Kontrollstellen freuen. Die dumpfe Sorge darüber, ob unsere Nachrichten ausgeleitet werden, wer sie betrachtet und wie sicher sie dort wiederum vor Missbrauch sind, wird uns alle betreffen."[59]

8.9. Auswirkungen auf die Arbeit der Ermittlungsbehörden

Patrick Beyer, MdEP skizziert die seiner Meinung nach eintretenden Auswirkungen auf die Arbeit der Ermittlungsbehörden drastisch:

„Das ist so, als würde die Post alle Briefe öffnen und Polizisten Millionen von Wohnungen durchsuchen… Ohnehin überlastete Strafverfolgungsbehörden werden unnötig damit belastet, die sind millionenfach gemeldeten Müll zu durchforsten."[60]

Auch der Chaos Computer Club sorgt sich um die Einsatzfähigkeit der Ermittlungsbehörden:

*„Gleichzeitig werden sich bei den Kontrollstellen Berge an irrelevantem Material häufen und die Beamt*innen von wichtiger Ermittlungsarbeit abhalten. Bereits mit den heute anfallenden Daten sind Ermittlungsbehörden überlastet. Ermittlungserfolge bleiben aus, und gefundene Materialien werden noch nicht einmal gelöscht. Diese Defizite wirkungsvoll zu beseitigen, wäre das wichtigste Ziel im Kampf gegen Kindesmissbrauch. Stattdessen will die Kommission auf Massenüberwachung und die Heilsversprechen ‚künstlicher Intelligenz' setzen."*[61]

---

58 Chaos Computer Club: EU-Kommission will alle Chatnachrichten durchleuchten. Vom 9. Mai 2022. Abrufbar unter:https://www.ccc.de/de/updates/2022/eu-kommission-will-alle-chatnachrichten-durchleuchten.

59 Ebd.

60 Zitiert nach: Breithut, Jörg: Kampf gegen Kindesmissbrauch. Bürgerrechtler wehren sich gegen ein europäisches Chat-Überwachungsgesetz. In: spiegel.de vom 19. März 2022.

61 Chaos Computer Club: EU-Kommission will alle Chatnachrichten durchleuchten. Vom 9. Mai 2022. Abrufbar unter: https://www.ccc.de/de/updates/2022/eu-kommission-will-alle-chatnachrichten-durchleuchten.

9. Fragenkatalog Bundesregierung

Zu dem Vorschlag für die Verordnung der Europäischen Kommission berichtet Netzpolitik.org über einen langen Fragenkatalog mit insgesamt 61 Fragen, den die Bundesregierung an die Europäische Kommission gerichtet habe[62] – siehe dazu Anhang .

Das Auskunftsersuchen der Bundesregierung beinhaltet beispielsweise die Frage, welche Technologien die Ende-zu-Ende-Verschlüsselung nicht aushebeln, die Endgeräte schützen und dennoch Kinderpornographien und Grooming aufdecken können.[63]

In einer weiteren Frage erkundigt sich demnach die Bundesregierung, wie ausgereift die modernen Technologien zur Vermeidung *„false-positive“* Treffer sind und welcher Anteil an *„false-positive“* Treffern zu erwarten ist, wenn Technologien zur Aufdeckung von Grooming eingesetzt werden.[64]

10. Fazit

Eine endgültige Beurteilung dieses sowohl inhaltlich wie auch vom Umfang her extrem komplexen Vorhabens ist nicht Gegenstand dieser Arbeit.

Schon jetzt ist aber davon auszugehen, dass die Einsicht/Durchsuchung von Nachrichten durch den Diensteanbieter, die aufgrund eines gesetzlich nicht näher definierten Risikos durch einen gerichtlichen Beschluss ermöglicht werden soll, auch wenn die konkrete Nachricht dazu keinen Anlass gibt, einer intensiven juristischen und politischen Diskussion bedarf.

Ferner sollten auch die technischen Herausforderungen analysiert und diskutiert werden. Dies gilt insbesondere im Hinblick auf eine faktische Verdrängung von Ende-zu-Ende-Verschlüsselung durch die komplexen Herausforderungen.

---

62 Reuter, Markus/Meister, André: Chatkontrolle: Bundesregierung löchert EU-Kommission mit kritischen Fragen. In: NETZPOLITIK.ORG vom 17. Juni 2022. Abrufbar unter: https://netzpolitik.org/2022/chatkontrolle-bundesregierung-loechert-eu-kommission-mit-kritischen-fragen/.

63 Ebenda: “5. Could the COM please describe in detail on technology that does not break end-to-end-encryption, protect the terminal equipment and can still detect CSAM? Are there any technical or legal boundaries (existing or future) for using technologies to detect online child sexual abuse?”

64 Ebenda: “7. How mature are state-of-the-art technologies to avoid false positive hits? What proportion of false positive hits can be expected when technologies are used to detect grooming? In order to reduce false positive hits, does COM deem it necessary to stipulate that hits are only disclosed if the method meets certain parameters (e.g., a hit probability of 99.9% that the content in question is appropriate)?”

11. Anhang

- **Art. 294 AEUV**

Art. 294 AEUV

(ex-Artikel 251 EGV)

(1) Wird in den Verträgen hinsichtlich der Annahme eines Rechtsakts auf das ordentliche Gesetzgebungsverfahren Bezug genommen, so gilt das nachstehende Verfahren.

(2) Die Kommission unterbreitet dem Europäischen Parlament und dem Rat einen Vorschlag.

Erste Lesung

(3) Das Europäische Parlament legt seinen Standpunkt in erster Lesung fest und übermittelt ihn dem Rat.

(4) Billigt der Rat den Standpunkt des Europäischen Parlaments, so ist der betreffende Rechtsakt in der Fassung des Standpunkts des Europäischen Parlaments erlassen.

(5) Billigt der Rat den Standpunkt des Europäischen Parlaments nicht, so legt er seinen Standpunkt in erster Lesung fest und übermittelt ihn dem Europäischen Parlament.

(6) Der Rat unterrichtet das Europäische Parlament in allen Einzelheiten über die Gründe, aus denen er seinen Standpunkt in erster Lesung festgelegt hat. Die Kommission unterrichtet das Europäische Parlament in vollem Umfang über ihren Standpunkt.

Zweite Lesung

(7) Hat das Europäische Parlament binnen drei Monaten nach der Übermittlung

a) den Standpunkt des Rates in erster Lesung gebilligt oder sich nicht geäußert, so gilt der betreffende Rechtsakt als in der Fassung des Standpunkts des Rates erlassen;

b) den Standpunkt des Rates in erster Lesung mit der Mehrheit seiner Mitglieder abgelehnt, so gilt der vorgeschlagene Rechtsakt als nicht erlassen;

c) mit der Mehrheit seiner Mitglieder Abänderungen an dem Standpunkt des Rates in erster Lesung vorgeschlagen, so wird die abgeänderte Fassung dem Rat und der Kommission zugeleitet; die Kommission gibt eine Stellungnahme zu diesen Abänderungen ab.

(8) Hat der Rat binnen drei Monaten nach Eingang der Abänderungen des Europäischen Parlaments mit qualifizierter Mehrheit

a) alle diese Abänderungen gebilligt, so gilt der betreffende Rechtsakt als erlassen;

b) nicht alle Abänderungen gebilligt, so beruft der Präsident des Rates im Einvernehmen mit dem Präsidenten des Europäischen Parlaments binnen sechs Wochen den Vermittlungsausschuss ein.

(9) Über Abänderungen, zu denen die Kommission eine ablehnende Stellungnahme abgegeben hat, beschließt der Rat einstimmig.

Vermittlung

(10) Der Vermittlungsausschuss, der aus den Mitgliedern des Rates oder deren Vertretern und ebenso vielen das Europäische Parlament vertretenden Mitgliedern besteht, hat die Aufgabe, mit der qualifizierten Mehrheit der Mitglieder des Rates oder deren Vertretern und der Mehrheit der das Europäische Parlament vertretenden Mitglieder binnen sechs Wochen nach seiner Einberufung eine Einigung auf der Grundlage der Standpunkte des Europäischen Parlaments und des Rates in zweiter Lesung zu erzielen.

(11) Die Kommission nimmt an den Arbeiten des Vermittlungsausschusses teil und ergreift alle erforderlichen Initiativen, um auf eine Annäherung der Standpunkte des Europäischen Parlaments und des Rates hinzuwirken.

(12) Billigt der Vermittlungsausschuss binnen sechs Wochen nach seiner Einberufung keinen gemeinsamen Entwurf, so gilt der vorgeschlagene Rechtsakt als nicht erlassen.

Dritte Lesung

(13) Billigt der Vermittlungsausschuss innerhalb dieser Frist einen gemeinsamen Entwurf, so verfügen das Europäische Parlament und der Rat ab dieser Billigung über eine Frist von sechs Wochen, um den betreffenden Rechtsakt entsprechend diesem Entwurf zu erlassen, wobei im Europäischen Parlament die Mehrheit der abgegebenen Stimmen und im Rat die qualifizierte Mehrheit erforderlich ist. Andernfalls gilt der vorgeschlagene Rechtsakt als nicht erlassen.

(14) Die in diesem Artikel genannten Fristen von drei Monaten beziehungsweise sechs Wochen werden auf Initiative des Europäischen Parlaments oder des Rates um höchstens einen Monat beziehungsweise zwei Wochen verlängert.

Besondere Bestimmungen

(15) Wird in den in den Verträgen vorgesehenen Fällen ein Gesetzgebungsakt auf Initiative einer Gruppe von Mitgliedstaaten, auf Empfehlung der Europäischen Zentralbank oder auf Antrag des Gerichtshofs im ordentlichen Gesetzgebungsverfahren erlassen, so finden Absatz 2, Absatz 6 Satz 2 und Absatz 9 keine Anwendung.

In diesen Fällen übermitteln das Europäische Parlament und der Rat der Kommission den Entwurf des Rechtsakts sowie ihre jeweiligen Standpunkte in erster und zweiter Lesung. Das Europäische Parlament oder der Rat kann die Kommission während des gesamten Verfahrens um eine Stellungnahme bitten, die die Kommission auch von sich aus abgeben kann.

Sie kann auch nach Maßgabe des Absatzes 11 an dem Vermittlungsausschuss teilnehmen, sofern sie dies für erforderlich hält.

- Europäische Kommission: Kampf gegen Kindesmissbrauch: Kommission präsentiert Gesetzesvorschlag zum Schutz von Kindern. Vom 11. Mai 2022. Abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/de/ip_22_2976.

- Europäische Kommission: Fragen und Antworten - neue Vorschriften zur Bekämpfung des sexuellen Missbrauchs von Kindern. Abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/de/qanda_22_2977.

- Europäische Kommission: Factsheet: Sexueller Missbrauch von Kindern – eine reale und wachsende Gefahr. Abrufbar unter: file:///C:/Users/karst/AppData/Local/Temp/MicrosoftEdgeDownloads/f100bab0-1fe7-42a6-b6e9-fd4b0c824fe9/Sexueller_Kindesmissbrauch.pdf%20(5).pdf.

- Umstrittene „Chatkontrolle. Werden Sie jetzt zur Zensur-Ylva, Frau Kommissarin? Interview mit EU-Kommissarin Ylva Johansson. In spiegel.de vom 13. Mai 2022.

- Breithut, Jörg: Kampf gegen Kindesmissbrauch. Bürgerrechtler während sich gegen ein europäisches Chat-Überwachungsgesetz. In: spiegel.de vom 19. März 2022.

- Reuter, Markus/Meister, André: Chatkontrolle: Bundesregierung löchert EU-Kommission mit kritischen Fragen. In: NETZPOLITIK.ORG vom 17. Juni 2022. Abrufbar unter: https://netzpolitik.org/2022/chatkontrolle-bundesregierung-loechert-eu-kommission-mit-kritischen-fragen/.

***