# Chatkontrolle

Was ist es und welche Kritik gibt es?

Lars Noack

29. Juni 2022

# Inhaltsverzeichnis

# 1 Vorbemerkung

Apple plante 2021 eine mithilfe einer künstlichen Intelligenz iPhones nach kinderpornografischen Inhalten zu scannen, und diese dann automatisch einer Dienststelle zu melden. Da dies aber immense Kritik von unter anderem IT-Experten und Datenschützern gab, ruderte Apple im August 2021 zurück.[ntv, 03.09.2021] Jedoch wird dies jetzt in Form von Chat Control 2, einem Gesetzespaket der EU-Kommission zurückkehren. Und das verpflichtend für alle Messenger Dienste.

Bevor ich aber zu Chat Control komme, erläutere ich grob die Strategie der EU-Kommission, um zu zeigen, dass diese es sehr wohl ernst mit dem Kinderschutz meint.

# 2 Bisherige Strategie zum Kinderschutz

In der 2020 veröffentlichten Strategie gegen Kindesmissbrauch der EU-Kommision[eu lex, 24.07.2020] ist unter anderem die Rede davon, dass die EU-Mitgliedstaaten in der Umsetzung der 2011 beschlossenen Präventivprogrammen im Rückzug sind. Dagegen solle etwas unternommen werden.
*S. 12 "Einige der Artikel der Richtlinie zur Bekämpfung des sexuellen Missbrauchs von Kindern, bei denen die Mitgliedstaaten mit der vollständigen Umsetzung mehr in Rückstand geraten, sind solche, die die Einführung von Präventionsprogrammen erfordern, an denen verschiedene Akteure aktiv beteiligt sind."*

## 2.1 Präventionsnetz

Daher wird die EU-Kommission an der Einrichtung eines Präventionsnetzes von renomierten Praktikern und Forschern unterstützt. Dies soll gemacht werden, da das Thema "Täter werden" im Bezug auf Kindesmissbrauch schlecht erforscht ist. Dieses Netz soll sowol die Umsetzung in die Praxis der Staaten mit der Wissenschaft verbinden,
*S. 13 "einen Erfolgszyklus zwischen Praxis und Forschung sowie zwischen Forschung und Praxis ermöglichen:"*
als auch die Mitgliedsstaaten mit Medienkampagnen und Schulungsmaterial unterstützen.
*S. 14 "Unterstützung der Mitgliedstaaten bei ihrer Sensibilisierungsarbeit durch gezielte Medienkampagnen und Schulungsmaterial"*

## 2.2 Ein Europäisches Zentrum gegen Kindesmisbrauchs

Zusätzlich will der EU-Kongress *S. 16: "Ein Europäische Zentrum zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern"* einrichten.

Die Grundidee bei diesem Zentrum ist, dass es die verschiedenen Instanzen und Maßnahmen verbindet. Zum Beispiel könnte das Zentrum sowohl mit Strafverfolgungsbehörden in EU-Staaten, als auch in Drittstaaten zusammenarbeiten, um das Miteinander zu stärken.
*S. 17 "[...] könnte das Zentrum mit den Strafverfolgungsbehörden in der EU und in Drittländern zusammenarbeiten, um sicherzustellen, [...]."*
Auch soll das Zentrum die Koordination der Präventionsmaßnahmen erleichtern, Doppelarbeit vermeiden und die Maßnahmen der Mitgliedsstaaten bewerten.
*S. 17: "[...] könnte das Zentrum die Mitgliedstaaten dabei unterstützen, nutzbare, einer strengen Bewertung unterzogene [...] Präventionsmaßnahmen einzuführen [...]. Es könnte die Koordinierung erleichtern, um die effizienteste Nutzung der investierten Ressourcen und des verfügbaren Fachwissens im Bereich Prävention EU-weit zu unterstützen und Doppelarbeit zu vermeiden. [...]"*
Zuletzt solle das Zentrum auch Opfern helfen und betreuen.
*S. 17: "Das Zentrum könnte eng mit nationalen Behörden und internationalen Experten zusammenarbeiten, um sicherzustellen, dass die Opfer eine angemessene, umfassende Betreuung erhalten, [...]"*

## 2.3 generell

Dies waren nicht alle Punkte der Strategie, sondern nur zwei, dennoch ist vor allem das EU-Zentrum ein sehr wichtiger Teil der Strategie. Tatsächlich wurde das EU-Zentrum wirklich in die Tat umgesetzt, und das ziemlich zügig [EU Zentrum]. Dieses Beispiel zeigt, dass in diesem Bereich auf jeden Fall Maßnahmen geplant werden, und das diese auch teilweise in die Tat umgesetzt werden.

Trotzdem wurde dem EU-Kongress für "Chat Control 2", eine Maßnahmen die zum Kinderschutz beitragen soll, viel Kritik erteilt. Aber was ist das jetzt genau?

# 3 Überblick über Chat Control 2

Der Begriff "Chat Control 2" bzw. "Chatkontrolle"[1] wurde von dem EU-Parlamentarier Patrik Breyer (Piratenpartei) geprägt.[Spiegel, 14.05.2022] Es bezeichnet den 134-Seitigen, stark kritisierten Gesetzesentwurf der EU-Kommission [Gesetzesentwurf, 11.05.2022].

In diesem Gesetzesentwurf geht es darum, Messenger Dienste **verpflichtend** mit einer von der EU-Kommission entwickelten künstlichen Intelligenz die Geräte auf der Clientseite nach Kinderpornografie durchsuchen zu lassen. Wenn etwas gefunden wird soll es an eine unabhängige Prüfungsstelle geschickt werden, die den Fall prüft und ggf. Anzeige erstattet. Da solche künstlichen Intelligenzen mit Wahrscheinlichkeiten rechnen, haben jene auch eine recht hohe Fehlerquote.

Das grundlegende Prinzip dahinter ist aber auf keinen Fall etwas neues.

# 4 "Chat Control 1"

Der "Vorgänger" existiert nähmlich schon seit 2020 in Form einer Schnittstelle, mit der Firmen Straftaten bezüglich Kindesmissbrauch melden können. Diese Schnittstelle ist für z.B. Unternehmen aus der USA das National Center for Missing and Exploited Children (**NCMEC**).
"*Note on reporting to appropriate authorities [...] For companies based in the United States of America, reporting is mandated via the National Center for Missing and Exploited Children (NCMEC). [...]*" [gov.uk, 24.04.2022]

Die einheitlichen Prinzipen, was gemeldet wird und was nicht werden auch festgelegt [gov.uk, 24.04.2022]. Jedoch gibt es hier entscheidende Unterschiede zu dem neuen Gesetzesentwurf.

## 4.1 Unterschiede zu Chat Control 2

Die wichtigsten Unterschiede sieht man schon in der Überschrift: "*Voluntary Principles*" [gov.uk, 24.04.2022]

- "*Voluntary*" legt nahe, dass dies alles **freiwillig** ist.
- "*Principles*" sagt, dass die technische Umsetztung komplett den Firmen überlassen ist.

## 4.2 Optionen der technischen Umsetzung

Für die technische Umsetzung davon gibt es mehrere Möglichkeiten.

Die eine Möglichkeit ist **Serverside Scanning**. Dort werden alle Daten die auf dem Server[2] nach illegalen Inhalten wie Grooming oder Kinderpornografie gescannt. Die andere Möglichkeit ist **Clientside Scanning**. Dort werden die Daten auf dem Client[3] gescannt.

Beim Scanning gibt es wieder mehrere Optionen[4]. Zum einen kann man den **Hasch Wert**[5] eines Bildes mit den Hash Werten von Bildern, die schon als Kinderpornografie erkannt worden sind vergleichen. Dies hat den Nachteil, das keine neuen Bilder erkannt werden können. Die andere Option sind **Künstliche Intelligenzen**. Diese können auch neue Bilder erkennen, aber arbeiten mit Warscheinlichkeiten. Das heißt, die Fehlerrate wird ziemlich hoch sein.

Wichtig ist, dass bei Ende-zu-Ende-Verschlüsselung der Server weder Bilder noch Textnachrichten lesen kann und somit Serverside Scanning keine Option ist.

## 4.3 Welche Firmen Scannen schon wie?

Viele große Firmen haben schon 2020 die "Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse" unterzeichnet. In diesem gesammten Abschnitt beziehe ich mich auf [Netzpolitik.org, 30.05.2022].

[1] Ich werde beide Bezeichnungen austauschbar verwenden.
[2] Der Computer der Firma auf dem alle Accountdaten, Chatverläufe, Bilder, etc. liegen.
[3] Endgeräte wie Handys oder Computer die mit dem Server kommunizieren.
[4] Um Grooming zu erkennen könnte man höchstens "sentient-text-analysis" verwenden, darauf gehe ich aber hier nicht ein.
[5] Sehr vereinfacht ist ein Hash-Wert der digitale Fingerabdruck eines Bildes.

**Google** Google wendet **Serverside Scanning** unter anderem bei Diensten wie YouTube, Gmail und Google Drive an. Das wird von Google sowohl mit Hash Werten, als auch mit **Künstlicher Intelligenz** gemacht. Die Daten, welche von der KI[6] erkannt werden, werden aber vorher von Mitarbeitern kontrolliert.

**Facebook** Facebook hat über 22 Millionen Meldungen dem NCMEC geschickt. Die Firma verschweigt aber, welche Technologie sie verwendet. Da Facebook jedoch ankündigt immer mehr ihrer Dienste E2E-Verschlüsseln[7] zu wollen, liegt die Vermutung nahe, dass Clientside-Scanning verwendet wird. Das ist aber lediglich Spekulation.

**Apple** Apple macht dies zwar nicht mehr, aber hat Scanning mit Clientside-Scanning versucht. Die Firma ruderte dann aber wie schon in der Vorbemerkung gesagt wurde wieder zurück.

**Microsoft** Microsoft entwickelte schon 2009 zusammen mit dem Forscher Hany Farid an [Microsoft-PhotoDNA]. PhotoDNA nutzt Serverside-Scanning, aber funktioniert auch mit Clientside-Scanning. Die Technologie basiert auf den Hashwerten. Microsoft verwendet PhotoDNA auf Bing und den File-Hosting Diensten. Außerdem kann man sich bei Microsoft einfach bewerben, um PhotoDNA zu nutzen. Genutzt wird der Dienst beispielsweise von den Firmen:

- Google
- Twitter
- Facebook
- Reddit
- Discord

# 5 Der Gesetzesentwurf der EU-Kommission

Obwohl viele riesige Unternehmen einiges freiwillig tun, durchleuchtet keines massenweise die gesamte Kommunikation der Kunden, wie es der EU-Kongress will [Netzpolitik.org, 30.05.2022].

Laut Artikel 7 des [Gesetzesentwurf, 11.05.2022]s, können die Gerichte **jeden** Internethoster und **jeden** Messengerdienst, unabhängig von deren Größe, dazu zwingen, mit dem Scanning anzufangen.
*S. 47, Artikle 7 1.: "The Coordinating Authority of establishment shall have the power to request the competent judicial authority of the Member State that designated it or another independent administrative authority of that Member State to issue a detection order requiring a provider of hosting services or a provider of interpersonal communications services under the jurisdiction of that Member State to take the measures specified in Article 10 to detect online child sexual abuse on a specific service."*

## 5.1 Was bedeutet Scanning?

Aber wie sieht das Scanning jetzt aus? Das [EU Zentrum] stellt laut Artikel 50, Absatz 1
*S. 83: "The EU Centre shall make available technologies that providers of hosting services and providers of interpersonal communications services may acquire, install and operate, free of charge [...]."*
den Firmen kostenlos eine Technologie zur Verfügung. Jedoch ist auch wichtig, dass die Provider laut Artikel 10 Absatz 2 diese nicht nutzen muss, solange die Bedingungen der EU-Kommission erfüllt sind.
*S. 51: "[...] The provider shall not be required to use any specific technology, including those made available by the EU Centre, as long as the requirements set out in this Article are met. [...]"*
Trotzdem sind kleinere Provider, wie [Signal] dazu verpflichtet diese Technologie zu nutzen, da sie nicht die Mittel haben eine eigene zu entwickeln, welche gut genug wäre.

[6] kurz für Künstliche Inteligenz
[7] kurz für Ende-zu-Ende-Verschlüsselung

## 5.2 Bedingungen des Scannings und technologische Optionen

Welche Bedingungen von Firmen entwickelte Technologien erfüllen müssen, um genutzt zu werden, steht größtenteils in Artikel 10 des [Gesetzesentwurf, 11.05.2022]s.

Die Technologie soll laut Absatz 3a wirksam sein in der Aufdeckung der Verbreitung von Material sexuellen Kindesmissbrauchs. Dieses Material **muss** aber auch Unbekanntes beinhalten.
*S. 84: "effective in detecting the dissemination of known or new child sexual abuse material or the solicitation of children, as applicable;"*
Das bedeutet, die Option des Abgleichens von Hash Werten als einzige genutzte Technologie ist nicht möglich. Also **müssen** Firmen Künstliche Intelligenz zusätzlich einsetzen.

**Datenbanken von Indikatoren** Die Künstliche Intelligenz reicht aber nicht, da es auch noch eine Datenbank von Indikatoren gibt, die laut Artikel 10 Paragraph 3.b alleinig verwendet werden sollen.
*S. 52: "not be able to extract any other information from the relevant communications than the information strictly necessary to detect, using the indicators [...]"*
Diese Datenbanken von Indikatoren werden in Artikel 40 näher erläutert. Es gibt drei Arten von Indikatoren.

1. Indikatoren für schon bekanntes Material zu sexuellem Kindesmissbrauchs.
2. Indikatoren für noch unbekanntes Material zu sexuellem Kindesmissbrauchs.
3. Indikatoren um grooming zu erkennen.

Wie diese Indikatoren technisch aussehen, wird nicht erläutert, aber für das schon bekannte Material wäre eine Datenbank mit Hash-Werten denkbar wie bei [Microsoft-PhotoDNA]. Für das Erkennen neuer Inhalte wäre eine Implementation einer Künstlichen Inteligenz wie [GitHub-NudeNet] denkbar. [GitHub-NudeNet] erkennt zwar nur Nacktheit, und keinen Kindesmissbrauch, ist dabei aber ziemlich akkurat, wenn auch nicht perfekt. Kindesmissbrauch zu erkennen wäre technisch jedoch um einiges schwerer und fehleranfälliger. Sicher grooming erkennen zu können ist noch schwerer.

Auf eine Anfrage, wie genau diese Indikatoren aussehen würden, reagierte die EU-Kommission (Stand: 25. Juni 2022) nicht.

**Voratsdatenspeicherung vom Material Kindesmissbrauchs** In Artikel 44 Absatz 4 ist eine wichtige Sache versteckt:
'" *The EU Centre shall keep records of the submissions and of the process applied to generate the indicators and compile the list referred to in the first and second subparagraphs. It shall keep those records for as long as the indicators, including the uniform resource locators, to which they correspond are contained in the databases of indicators referred to in paragraph 1.*'"
In diesem Absatz findet man zwei wichtige Punkte:

1. Die Indikatoren werden mit Material von Kindesmissbrauch erstellt.
2. Die Materialien von Kindesmissbrauch werden gespeichert, bis die Indikatoren nicht mehr verwendet werden.

Da die Indikatoren mit Material aus Kindesmissbrauch erstellt werden, ist dies die einzige Möglichkeit solche Materialien zu erkennen. Sowohl wenn Hash Werte verwendet werden, als auch wenn künstliche Intelligenzen verwendet werden. Bei beiden Möglichkeiten ist es jedoch nicht möglich die ursprünglichen Materialien wieder zu bekommen.

Jedoch sollen die Materialien gespeichert werden, bis die Indikatoren nicht mehr verwendet werden. Das Problem dabei ist, dass es kein rationalen Grund gibt, nach einer Weile bestimmte Indikatoren zu verwenden. Bei Hash Werten können die nicht mehr verwendeten Werte nähmlich nicht mehr erkannt werden, bei Künstlichen Intelligentzen fließen alle Materialien von Kindesmissbrauch ein. Und das ohne die Möglichkeit, einzelne Elemente entfernen zu können. Das heißt, dass diese Materialien aus Kindesmissbrauch, unter die auch Kinderpornografie fällt, in einer zentralisierten Datenbank gespeichert werden.

Damit gibt es sehr große Probleme. Zum Beispiel gab es selbst bei der cia [CNN, 06.16.2020] leaks von cyber Waffen. Die Vergangenheit zeigt somit mit diesem und ähnlichen Fällen, dass **alle** Daten geleakt und gehackt werden können. Das wäre bei einer solchen Datenbank schlimm. Es würde die Opfer solcher Taten nicht schützen und die Verbreitung verhindern, sondern die schlimmsten Momente deren Lebens öffentlich in einem Leak zeigen.

Aber man muss diesem Absatz zu gute halten, dass nur eine einzige Person diese Daten verarbeiten kann und darf. Das senkt das Missbrauchsrisiko immens, auch wenn es immer noch da ist.

Dieser Absatz 4 läuft sehr auf eine Vorratsdatenspeicherung für Kinderpornografie hinaus. Das wird wichtig, wenn man bedenkt, dass der EuGH[8] Vorratsdatenspeicherung schon 2020 verboten hat [Tagesschau, 06.10.2020]. Ausnahmen gibt es zur Bekämpfung schwerer Kriminalität und ein konkreter Fall einer Bedrohung der nationalen Sicherheit. Natürlich handelt es sich bei Kindesmissbrauch bzw. Missbrauch generell um schwere Kriminalität, aber es handelt sich auch um die schlimmsten Momente im Leben von Opfern die gespeichert werden sollen.

Einen unangenehmen Beigeschmack hat das alles, wenn man bedenkt, das dieser Abschnitt in 123 Seiten lediglich 5 Zeilen bekommen hat, und sehr schemenhaft formuliert ist. Dies könnte Absicht sein, das die EU-Kommission nicht viel Aufmerksamkeit darauf ziehen wollte. Aber egal ob mit Absicht oder nicht, es hat funktioniert da diese Vorratsdatenspeicherung nirgends erwähnt wurde[9]. Trotzdem findet man viele Artikel und Kritik dazu von unterschiedlichsten Organisationen. Der einzige Weg davon zu erfahren ist es wirklich den ganzen Gesetzesentwurf genau zu lesen. Dieser Punkt sollte aber auf jeden Fall kritisch betrachtet werden, da es auch einfach Zufall sein kann.

# 6 Kritik an der Chatkontrolle

Es gibt viele namhafte Kritiker der Chatkontrolle. Diese Kritiker reichen von Datenschutzorganisationen bis zu Kinderschutzorganisationen.

## 6.1 die Zeit

Eine der bekanntesten Zeitschriften im deutschen Raum, die sich dazu geäußert haben ist '"Die Zeit'". In dem Artikel "Es trifft die Falschen" [DIE ZEIT, 18.05.2022] wird zuerst gesagt, dass Kindesmissbrauch ein großes Problem ist. Dannach wird Chat Control zusammengefasst und ein Überblick gegeben, wie ich es ausführlich schon in den oberen Abschnitten getan habe.

Der folgende zentrale Kritikpunkt der Zeit begründet, warum das Gesetz nichts bringen würde. Die Ämter sind überflutet. So spührte die Polizei 2021 40.000 Fälle auf, aber es haben die Ressourcen gefehlt, um diese Fälle richtig zu bearbeiten. Diese Ressourcen werden mit Chat Control nicht erhöht.

"*Das Problem der Ermittler [...] ist nicht [...], dass die Täter im Verborgenen agieren. 2021 spürte die Polizei in Deutschland knapp 40.000 Fälle von "Verbreitung, Erwerb, Besitz oder Herstellung sogenannter kinderpornografischer Schriftenäuf, mehr als doppelt so viele wie 2020. Doch die Ermittler kommen kaum hinterher, die gigantischen Datenmengen zu durchforsten, die dabei anfallen. Trotz neuer Taskforces fehlt es noch immer an Personal. Wer den Kampf gegen sexuelle Gewalt an Kindern vorantreiben will, muss daran als Erstes etwas ändern.*"

Im folgenden Text spricht die Zeit auch über einen Kollateralschaden, der die Gefahr einer Überwachung aller Bürger sei.

## 6.2 Chaos-Computer-Club

Der Chaos-Computer-Club[10] kritisierte in dem letzten Abschnitt seines Onlineartikel [CCC, 09.05.2022] das gleiche wie DIE ZEIT, fügt aber Wichtiges hinzu. DIE ZEIT redet davon, dass die Behörden mit zusätzlichem echtem Material von Kindesmisbrauch überfordert wären und das man dort ansetzten solle. Jedoch werden aber allein in Deutschland mehr als eine halbe Milliarde Nachrichten pro Tag versendet [statista, 21.10.2015]. Dadurch werden aufgrund der Fehlerrate jeder Künstlichen Intelligenz, mehrere tausende Nachrichten **pro Tag**, die nicht Material von Kindesmissbrauchs erhalten, an zuständige Behörden geschickt.

"*Eine „künstliche Intelligenz", die auf Missbrauchsinhalte untersucht, wird auch Inhalte fälschlicherweise als illegal markieren. Auch kleinste Fehlerquoten würden zu massiven Mengen an fälschlicherweise ërkannteründ ausgeleiteter Nachrichten führen: Allein in Deutschland werden weit mehr als eine halbe Milliarde Nachrichten pro Tag versendet. Auch enorm "guteËrkennungsraten würden zur Ausleitung mehrerer Tausend Nachrichten pro Tag führen.*"

[8] EuGH: Europhäischer Gerichtshof

[9] Ich habe nichts gefunden

[10] "Der Chaos Computer Club e. V. (CCC) ist die größte europäische Hackervereinigung und seit über dreißig Jahren Vermittler im Spannungsfeld technischer und sozialer Entwicklungen. Die Aktivitäten des Clubs reichen von technischer Forschung und Erkundung am Rande des Technologieuniversums über Kampagnen, Veranstaltungen, Politikberatung, Pressemitteilungen und Publikationen bis zum Betrieb von Anonymisierungsdiensten und Kommunikationsmitteln."

Aufgrund dieses Fakts, würde Chat Control den Behörden nicht helfen, sondern die Ermittlungen erschweren, da die Behörden sich alles Material ansehen müssen.

Laut des Artikels des CCC[11] [CCC, 09.05.2022] wird auch erwähnt, dass das Material von Kindesmissbrauch zum Großteil über öffentliche Hoster verteilt wird und nicht über Messanger Dienste [Tagesschau, 02.12.2021]. Wichtig zu erwähnen ist aber, dass der Gesetzesentwurf auch diese öffentliche Hoster einschließt.

Der Zentrale Kritikpunkt des Chaos-Computer-Club ist jedoch der, dass Chatkontrolle zwei fundamentale Grundrechte außer Kraft setzten würde.

1. Das Fernmeldegeheimnis. [Wikipedia-Fernmeldegeheimnis] Das Fernmeldegeheimnis ist ein festgelegtes Grundrecht in der Verfassung Deutschlands, Österreichs und der Schweiz. In Deutschland ist das Fernmeldegeheimnis in Artikel 10 zu finden [Grundgesetz]. Dies besagt, dass selbst die Polizei nicht Nachrichten abhören dürfe [bpb]. "*Ohne Erlaubnis darf niemand private elektronische Nachrichten lesen oder hören. Der Interner Link:Staat muss dafür sorgen, dass die Nachrichten geheim bleiben. Auch die Polizei darf Nachrichten nicht lesen oder abhören.*"

2. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[12] [Wikipedia-IT-Grundrecht]. Dies ist ein in der Bundesrepublik Deutschland geltendes Grundrecht, welches zum Schutz der persöhnlichen Daten dient, jedoch nicht im [Grundgesetz] eigens genannt ist. Es wurde 2008 vom Bundesverfassungsgericht definiert.

## 6.3 Offener Brief

In einem offenen Brief zu diesem Thema unterschrieb nicht nur der Chaos-Computer-Club, sondern ganze 52 Organisationen [EDRI, 17.03.2022]. Zusammengefasst fordern diese Organisationen 3 Punkte.

1. Keine Massenüberwachung. Mit Massenüberwachung wird das generalisierende und automatisierte Scanning von Privater Kommunikation gemeint.

2. Eingriffe in die private Kommunikation darf nur auf individuelle Verdachtsfälle geschehen. Das schließt sich dem ersten Punkt an.

3. Die Maßnahmen müssen die sein, die die Privatsphäre am wenigsten verletzen, und dürfen sich nur auf CSAM[13] beschränken. Das heißt keine Maßnahmen wie CSS[14], die Verschlüsselung brechen oder unterwandern. Auch keine Künstliche Intelligenzen, da diese eine hohe Fehlerquote haben.

Die Organisationen, die Unterschrieben haben sind größtenteils Datenschutz- und Bürgerrechts-Organisationen. Hier ist eine Aufzählung aller Organisationen: European Digital Rights (EDRi) (International) ApTI (Romania), ARTICLE 19 (International), Associação Portuguesa para a Promoção da Segurança da Informação (Portugal), Big Brother Watch (UK), Bits of Freedom (The Netherlands), Centre for Democracy & Technology (CDT) (International), Chaos Computer Club (CCC) (Germany), Committee to Protect Journalists (CPJ) (International), Cryptoparty Köln-Bonn (Germany), Data Rights (The Netherlands / European), dataskydd.net (Sweden), Defend Digital Me (UK), Derechos Digitales (International), Deutscher Anwaltverein (DAV) (Germany), Deutsche Vereinigung für Datenschutz (DVD) (Germany), DieDatenschützerRheinMain (Germany), Digitalcourage (Germany), Digitale Gesellschaft (Germany), Državljan D/Citizen D (Slovenia), EURAFRI Networking (International), European Federation of Journalists (European), Electronic Frontier Foundation (EFF) (International), Electronic Frontier Finland (Effi), Electronic Frontier Norway (EFN), Electronic Privacy Information Center (EPIC) (United States), Entropia (Germany), European Center for Not-for-Profit Law (ECNL), European Sex Workers' Rights Alliance (ESWA), Foundation for Information Policy Research (FIPR) (UK / European), Global Voices (the Netherlands / International), Global Forum for Media Development (International), Giordano Bruno Foundation (Germany), Homo Digitalis (Greece), Internet Society Catalan Chapter (ISOC-CAT) (European), Irish Council for Civil Liberties (ICCL) (Ireland), ISOC Brazil – Brazil Chapter of the Internet Society (Brazil), IT-Pol Denmark, LGBT Technology Partnership (International), Ligue des droits humains (Belgium), Mnemonic (Germany / International), Open Governance Network for Europe, Open Rights Group (ORG) (UK), pEp Foundation (Switzerland), Privacy and Access Council of Canada, Privacy International (PI), Ranking Digital Rights (International), SaveTheInternet (Germany), StopACTA2 (Poland), Tech for Good Asia, TOPIO – public space for privacy (Germany) und Vrijschrift.org (The Netherlands).

[11] kurz: Chaos-Computer-Club
[12] auch IT-Grundrecht
[13] CSAM: Child-Sex-Abuse-Material
[14] CSS: Client-Side-Scanning

## 6.4 Kinderschutzorganisationen

Zu den Organisationen die Fachwissen bezüglich des Themas haben, zählen nicht nur Datenschutz- und IT-Organisationen. Dazu zählen auch Kinderschutz-Organisationen. Manche übten auch Kritik an der Chatkontrolle [Netzpolitik.org, 20.05.2022].

**Deutscher Kinderverein** Einer dieser Kinderschutz-Organisationen ist der Deutsche Kinderverein. Die Organisation ist ein "Impulsgeber und Kinderschutz-Lobbyist auf Grundlage der UN-Kinderrechtskonventionen" [Deutscher Kinderverein]. Der Geschäftsführer Rainer Rettinger bezeichnet den Gesetzesentwurf gegenüber netzpolitik.org als "*massiver Eingriff in rechtsstaatliche Grundsätze*" [Netzpolitik.org, 20.05.2022]. Als Begründung verweist er auf die schon bestehenden Defizite im Kinderschutz. Einer dieser Defizite ist, dass entdecktes Material von Kindesmissbrauch, trotz der technischen Machbarkeit, nicht gelöscht wird [Netzpolitik.org, 21.03.2022].

**Der Deutsche Kinderschutzbund** Der Deutsche Kinderschutzbund [Der Deutsche Kinderschutzbund] kritisierte Chatkontrolle ähnlich wie der Deutsche Kinderverein. Die Argumente des Bundesvorstands Joachim Türk waren, dass verschlüsselte Kommunikation bei der Verbreitung von Missbrauchsdarstellungen kaum eine Rolle spiele. Deshalb hält er "*anlasslose Scans von verschlüsselter Kommunikation für unverhältnismäßig und nicht zielführend.*"

**Netzwerk Kinderrechte** Netzwerk Kinderrechte[15] [Netzwek Kinderrechte] begrüßte gegenüber netzpolitik.org den Gesetzesentwurf der EU-Kommission. Die Begründung ist hierbei, dass es das erste Mal sei, dass ein Gesetzesentwurf der EU einen grundsätzlich kinderrechtlichen Ansatz verfolge und den Vorrang des Kindeswohls in den Fokus rücke.

Jedoch meinte sie auch, dass der Entwurf schwerwiegend in Grundrechte und Persönlichkeitsrechte eingreife, und es sich nicht absehen lässt, ob die Mechanismen um dies zu verhindern ausreichen.

**Innocence in Danger** Der Vorstand von Innocence in Danger [Innocence in Danger] Julia von Weiler äußerte sich gegenüber netzpolitik.org uneingeschränkt positiv zu Chatkontrolle. Sie meinte, dass aufgrund der Verdopplung von Missbrauchstaten im Netz [DIE ZEIT, 05.04.2022] Kinder und Jugendliche online mit dem Gesetz viel besser geschützt wären.

**Zusammengefasst** Zusammengefasst kann man sagen, dass die Meinungen vieler Kinderschutzorganisationen zu diesem Thema unterschiedlich und nicht einheitlich sind.

## 6.5 Deutschland

Deutschland ist in der EU ein sehr wichtiger Staat. Deshalb ist Kritik von Deutschlands Regierung sehr bedeutend. Natürlich hat nicht Deutschland als ganzes Kritik geübt, sondern diverse Abgeordnete als auch das Bundesministerium für Digitales und Verkehr.

**Nancy Faeser (Innenmenisterin)** Nancy Faeser ist seit 2019 Vorsitzende der SPD Hessen, und seit 2021 Bundesministerin für Inneres und Heimat. Das heißt, dass sie eine sehr starke Stimme ist. In einem Interview kritisierte sie Chatkontrolle, und lehnte einen Eingriff in die verschlüsselte Privatkommunikation ab [Tagesschau, 22.05.2022]. Auch meinte sie in selbigem Interview, das Ermitlungsbehörden auf "Darknet" Plattformen verstärkt tätig werden sollen. Die Chatkontrolle sei so laut Faeser "Nicht vereinbar mit Freiheitsrechten".

**Abgeordnete des EU-Parlaments** Nicht nur Frau Faeser sondern auch mehrere Abgeordnete des Europäischen Parlaments äußerten sich kritisch zu der geplanten Chatkontrolle.

- Einer davon ist Tiemo Wölken[16]. In einem Twitter-Thread [Tiemo Wölken] sagte er, es sei nicht möglich mit diesem Gesetztesentwuf Datenschutz und Privatsphäre zu achten.
  "*Gleichzeitig sollen sie strikt limitiert werden, den Datenschutz & Privatheit der Kommunikation beachten (haha!). Und das alles ohne Fehler.*"
  Zusätzlich bezeichnete er die geplanten Filter als "#Horrorfilter". Am Ende ist sein Fazit, dass mit

[15] Jutta Croll Vorstandsmitglied
[16] Abgeordneter der SPD

diesem Gesetzesentwurf es kein Datenschutz und keine Privatsphäre mehr geben würde. Auserdem stellt er die Anschuldigung in den Raum, dass der Gesetzesentwurf absichtlich undurchdringbar und verwirrend verfasst wurde.
"*Klar ist: Datenschutz & Privatsphäre gibt es nicht, wenn unsere private Kommunikation durchleuchtet wird. Die 135 Seiten Verordnung zur #Chatkontrolle aber versuchen vorzugaukeln, dass beides garantiert wird. Der Text ist zudem undurchdringbar & verwirrend verfasst. Absicht?*"

- Auch Alexandra Geese[17] kritisierte in einem Tweet [Alexandra Geese] Chatkontrolle. Sie sagt, dass Chatkontrolle das Grundrecht auf vertrauliche Kommunikation verletze und Kindern nichts bringe. Laut ihr werden Kinder eher duch mehr Personal für Ermittler und Jugendschutz geschützt.
"*#Chatkontrolle verletzt das Grundrecht auf vertrauliche Kommunikation und ist ein gefährlicher Tabubruch. Kinder werden durch mehr Personal für Ermittler*innen und Jugendschutz geschützt, nicht durch systematisches Ausspionieren.*"

**Bundesministerium für Digitales und Verkehr** In einem weiteren Tweet twitterte das Bundesministerium für Digitales und Verkehr [BMDV], dass der Schutz von Kindern im Netz wichtig sei, und sie daran arbeiten. Jedoch wurde im selben Tweet erwähnt, dass das Bundesministerium für Digitales und Verkehr Chatkontrolle als Werkzeug ablehnt.
"*#Kinder müssen wirksam vor #Missbrauch im Netz geschützt werden. Gleichzeitig darf es nicht zu einer anlasslosen Kontrolle privater Kommunikation kommen. Das @bmdv_bund wird darauf hinwirken, deutlich zielgerichteter vorzugehen.* "

Dies waren die relevantesten Institutionen und Politiker, jedoch wurde Chatkontrolle auch von Sabine Leutheusser-Schnarrenberger[18] in einem Tweet [Sabine Leutheusser] und von Dr. Konstantin von Notzs[19] auf Abgeordnetenwatch [Abgeordnetenwatch-06.04.2022] kritisiert. Kristian von Notzs ist trotzdem hervorzuheben, da er seit März 2022 Vorsitzender des Parlamentarischen Kontrollgremiums zur Kontrolle der Nachrichtendienste des Bundes ist.

## 6.6 Die Kritik zusammengefasst

Zusammengefasst wird die sogenanne "Chatkontrolle" von allen Seiten kritisiert. Die stärksten Kritiker sind Datenschutz und Bürgerrechtsorganisationen. Kritisiert wird der Gesetzesentwurf aber auch von Kinderschutzorganisaionen, deutschen Politikern und dem BMDV. Die Datenschutz und Bürgerrechtsorganisationen haben zusammen einen offenen Brief verfasst, der von über 50 Organisationen unterschrieben wurde.

Die wichtigsten Kritikpunkte sind:

- Die Bearbeitungsstellen haben schon jetzt nicht die Ressourcen, gemeldetes Material Kindesmissbrauchs einwandfrei nachzuverfolgen. Das wird mit Chatkontrolle schlimmer werden.
- Bevor man die Integrität von Ende zu Ende verschlüsselten Messenger verletzt, sollte man an anderen Stellen ansetzen, wie daran gemeldetes Material von Servern zu löschen.
- Die Privatsphäre wird stark verletzt werden mit CSS[20] und mit KI's mit zwangsläufig hoher Fehlerrate.

# 7 Szenarios

Dies sind ernst zu nehmende Kritikpunkte. Folgende Szenarios von Alice und Bob zeigen das nochmal deutlicher.

[17] Abgeordnete der Grünen
[18] Mitglied der FDP und seit 2019 Mitglied des Bayerischen Verfassungsgerichthofes
[19] Abgeordneter im Bundestag der Grünen und Vorsitzender des Parlamentarischen Kontrollgremiums zur Kontrolle der Nachrichtendienste des Bundes
[20] Client Side Scanning

### 7.1 Einvernehmlicher Bildertausch

In dem ersten Szenario leben Alice und Bob in einer Fernbeziehung. Sie sind ein junges gleichaltriges Paar. Leider sieht Alice jünger aus, als sie ist, und Bob sieht älter aus, als er ist[21]. Da sie in einer Fernbeziehung leben, entscheiden sie, etwas sexting zu betreiben, und Nacktbilder auszutauschen. Dies ist komplett ok und legal, da sie beide älter [Polizei Beratung, 19.06.2020] sind. Unwissend erkennen die von der EU-bereitgestellten Indikatoren dieses erlaubte und einverständliche Sexting und Bilderaustausch als Material Kindesmissbrauchs. Folglich wird die ganze Unterhaltung mit Bildern an eine Stelle von Meta[22] zur weiteren Durchsuchung geschickt. Diese Stelle denkt auch, das dies Material von Kindesmissbrauchs sei und leitet dies an das EU-Zentrum weiter. Das EU-Zentrum ermittelt, und stellt fest, dass beide alt genug sind, und dies kein Missbrauch sei. Leider haben dem Meta Mitarbeiter die Bilder gefallen, woraufhin er diese gespeichert hat und nun mit seinen Kolegen tauscht. Das klingt zwar etwas weit her geholt, aber laut Edward Snowden ist sowas selbst im NSA passiert. [lessentiel, 18.07.2014] sollen private Nacktbilder getauscht haben. Unglücklicherweise bekommt diese Meta Mitarbeiter einen Virus, und alles wird geleakt, jetzt sind Alices Nacktbilder in dem öffentlichen Internet zu finden.

### 7.2 Online Therapie

Im zweiten Szenarie wurde Bob als Kind sexuell missbraucht. Deshalb will er in Therapie gehen. Er hat jedoch keine Zeit, weshalb er Onlinetherapie in Anspruch nehmen will. Diese Onlinetherapie nutzt für besonden Datenschutz [Signal]. Alice, Bobs Therapeutin hat selbstverständlich Schweigepflicht, und der Chat ist Ende zu Ende verschlüsselt. Das heißt nichts kann nach außen dringen. Auf Alice's bitte erzählt Bob Alice detailreich, wie er als Kind missbraucht wurde. Die Erzählung erkennt die Künstliche Inteligenz auf Bobs Gerät aber als Straftat und sendet diese Unterhaltung an die Server von [Signal]. Da Signal kaum Ressourcen hat, wird dies direkt an die Server der EU-Kommission gesendet. Da bei der Ermittlung ein Fehler passiert bekommt Bob ein Brief, der den Inhalt der Nachricht schildert und den Sachverhalt schildert. Kurz darauf kommt ein Entschuldigungsbrief, dass ein Fehler in der Ermittlung passiert ist, und Bob gar nicht schuldig ist.

Trotzdem wurde Bob's Privatsphäre aufs extreme verletzt[23].

## 8 Fazit und eigene Meinung

Chatkontrolle ist schlecht. Die ungenaue Formulierung des Gesetzesentwurfs bezüglich technischen Details machen ein ungutes Gefühl, die Kritiker sind manigfaltig, und die Szenarien führen einem vor Augen was das für echte Auswirkungen hat. Nichtsdestotrotz finde ich nur Teile von Chatkontrolle schlecht.

### 8.1 Hauptkritikpunkte

Aber ein Punkt der schlimm ist, ist **die Vorratsdatenspeicherung**. Diese schützt die Kinder nicht, sondern gefährdet sie aktiv. Auch muss die **Integrität von End to End Verschlüsselten Diensten bzw. Messengern** erhalten bleiben. Also darf Client Side Scanning keine Option sein. Die **Überlastung der Auswertung der Meldungen** wird auch ein riesiges Problem.

### 8.2 Positives

So schlecht das alles ist, gut ist dass Hoster Serverside Scanning betreiben müssen, und die Technologie von der EU Kommision gestellt bekommen. Jedoch sollte diese Technologie nur auf Hash Werten basieren und nicht auf Künstlichen Intelligenzen, um Überlastung im System zu verhindern. Dies hätte das Potenzial viel zu verhindern. Bei anderen Diensten die nicht Ende zu Ende verschlüsselt sind, wäre solch Server Side Scanning auch auch denkbar, da nicht die Integrität gebrochen werden würde. Wie vorhin schon erwähnt machen das tatsächlich schon ein paar Firmen. Deshalb muss der Gesetzesentwurf geändert werden.

[21] Der visuelle Altersunterschied spielt keine große Rolle, da das gleiche ohne den passieren könnte und wird
[22] die Firma hinter Whats-App
[23] selbst wenn Bob kein Brief bekommen hätte.

## Quellenverzeichnis


[ntv, 03.09.2021] ntv: Apple vertagt Kinderporno-Suche auf iPhone. Der US-Tech-Riese Apple stellt im August Pläne für die gezielte Suche nach Kinderpornografie auf seinen Geräten vor, nun rudert er zurück und vertagt das System. IT-Experten und Datenschützer sehen die Gefahr des Missbrauchs der Technik, etwa durch autokratische Regierungen., https://www.n-tv.de/technik/Apple-vertagt-Kinderporno-Suche-auf-iPhone-article22783832.html (Stand: 30.05.2022)

[eu lex, 24.07.2020] Eu Kommission: COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. EU strategy for a more effective fight against child sexual abuse. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0607&qid=1634899236324 (Stand: 30.05.2022)

[EU Zentrum] Eu Kommission: EU Centre of Expertise for Victims of Terrorism. EU Centre offers expertise, guidance and support to national authorities and victim support organisations on victims of terrorism. URL: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/protecting-victims-rights/eu-centre-expertise-victims-terrorism_en (Stand: 2. Juni 2022)

[Spiegel, 14.05.2022] Hoppenstedt, Max/Rosenbach, Marcel: Gutes Ziel, falscher Weg. DATENSCHUTZ Mit ihrem Vorstoß zur anlasslosen Kontrolle von Chatnachrichten bringt die EU-Kommission vom Chaos Computer Club bis zum Kinderschutzbund alle gegen sich auf. In: DER SPIEGEL, 14. Mai 2022, S. 70

[Gesetzesentwurf, 11.05.2022] EU-Kommission: REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. laying down rules to prevent and combat child sexual abuse. https://eur-lex.europa.eu/resource.html?uri=cellar:13e33abf-d209-11ec-a95f-01aa75ed71a1.0001.02/DOC_1&format=PDF (Stand: 31. März 2022)

[gov.uk, 24.04.2022] United Kingdom public sector: Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse: formal letter (accessible version). URL https://www.gov.uk/government/publications/voluntary-principles-to-counter-online-child-sexual-exploitation-and-abuse/voluntary-principles-to-counter-online-child-sexual-exploitation-and-abuse (Stand: 31. März 2022)

[Netzpolitik.org, 30.05.2022] Köver, Chris: Was Unternehmen schon freiwillig tun. Die EU-Kommission will Unternehmen dazu verpflichten, in privaten Nachrichten nach Darstellungen von Gewalt gegen Kinder zu suchen. Dabei machen viele das bereits freiwillig. Welche Technologien heute schon zum Einsatz kommen. URL https://netzpolitik.org/2022/chatkontrolle-was-unternehmen-schon-freiwillig-tun/ (Stand: 31. März 2022)

[Microsoft-PhotoDNA] Microsoft: Help stop the spread of child exploitation. In 2009, Microsoft partnered with Dartmouth College to develop PhotoDNA, a technology that aids in finding and removing known images of child exploitation. Today, PhotoDNA is used by organizations around the world and has assisted in the detection, disruption, and reporting of millions of child exploitation images. URL https://www.microsoft.com/en-us/photodna (Stand: 31. März 2022)

[Signal] Signal: Sprich offen. Freu dich auf eine neue Erfahrung beim Messaging: ein unerwarteter Fokus auf Privatsphäre, verbunden mit all den Features, die du erwartest. URL https://www.signal.org/de/ (Stand: 31. März 2022)

[GitHub-NudeNet] NudeNet: Neural Nets for Nudity Classification, Detection and selective censoring. URL: https://github.com/notAI-tech/NudeNet (Stand: 5. Juni 2022)

[CNN, 06.16.2020] Cohen, Cachary/ Marquardt, Alex: CIA cyber weapons stolen in historic breach due to 'woefully lax security', internal report says. Washington (CNN)The largest theft of data in CIA history happened because a specialized unit within the agency was so focused on building cyber weapons that an employee took advantage of "woefully laxßecurity and gave secret hacking tools to WikiLeaks, according to an internal report released on Tuesday. URL: https://edition.cnn.com/2020/06/16/politics/cia-wikileaks-vault-7-leak-report/index.html (Stand: 25. Juni 2022)

[Tagesschau, 06.10.2020] Tagesschau: Pauschale Vorratsdatenspeicherung unzulässig. Um die pauschale Speicherung von Kommunikationsdaten gibt es seit Langem Streit. Ein Urteil des höchsten europäischen Gerichts bestärkt nun Datenschützer. In Ausnahmen sei die Speicherung aber rechtens. URL: https://www.tagesschau.de/ausland/eugh-vorratsdatenspeicherung-101.html (Stand: 25. Juni 2022)

[DIE ZEIT, 18.05.2022] Nezik, Ann-Kathrin: Es trifft die Falschen . Die EU will WhatsApp und andere verpflichten, Chats nach Missbrauchsbildern zu durchsuchen. Ein tiefer Eingriff in die Privatsphäre – der wenig bringt. ln: DIE ZEIT, Ausgabe Nr. 21/2022, S. 70

[CCC, 09.05.2022] linus: EU-Kommission will alle Chatnachrichten durchleuchten. Am Mittwoch, dem 11. Mai 2022 veröffentlicht die EU-Kommission voraussichtlich den Gesetzesentwurf zur sogenannten Chatkontrolle. Geplant ist eine KI-basierte Prüfung aller Nachrichteninhalte und Bilder direkt auf unseren Geräten. Das so genannte Client-Side-Scanning wäre ein Angriff auf jegliche vertrauliche Kommunikation. URL: https://www.ccc.de/de/updates/2022/eu-kommission-will-alle-chatnachrichten-durchleuchten (Stand: 7. Juni 2022)

[statista, 21.10.2015] statista: Anzahl der verschickten SMS- und WhatsApp-Nachrichten in Deutschland von 1999 bis 2014 und Prognose für 2015. URL: https://de.statista.com/statistik/daten/studie/3624/umfrage/entwicklung-der-anzahl-gesendeter-sms-mms-nachrichten-seit-1999/ (Stand: 7. Juni 2022)

[Tagesschau, 02.12.2021] Ackermann, Lutz; Bongen, Robert; Güldenring, Benjamin; Moßbrucker, Daniel: Ermittler lassen Bilder nicht löschen. Zahlreiche Fotos und Videos, die schweren sexuellen Missbrauch von Kindern zeigen, bleiben oft jahrelang im Netz, obwohl Ermittlungsbehörden sie löschen könnten. Das zeigen Recherchen von NDR und SSpiegel". URL: https://www.tagesschau.de/investigativ/panorama/kinderpornografie-loeschung-101.html (Stand: 7. Juni 2022)

[Wikipedia-Fernmeldegeheimnis] Wikipedia: Fernmeldegeheimnis. Das Fernmeldegeheimnis ist ein in der Verfassung Deutschlands, Österreichs und der Schweiz geschütztes Grundrecht. Es wird meist ergänzt durch das Briefgeheimnis, in Deutschland außerdem durch das Postgeheimnis. Es wird mit Rücksicht auf die technische Entwicklung auch als Telekommunikationsgeheimnis bezeichnet. URL: https://de.wikipedia.org/wiki/Fernmeldegeheimnis (Stand: 7. Juni 2022)

[Grundgesetz] Bundeszentrale für politische Bildung: GRUNDGESETZ für die Bundesrepublik Deutschland, 2017

[bpb] BPB: Brief-, Post- und Fernmeldegeheimnis. Das Brief- Post- und Fernmeldegeheimnis schützt den Austausch von Nachrichten zwischen einem Sender und einem Empfänger. Das Brief- Post- und Fernmeldegeheimnis schützt schriftliche Nachrichten, Nachrichten über das Internet oder über das Telefon. Auch der Inhalt von Paketen und Päckchen ist geschützt. URL: https://www.bpb.de/kurz-knapp/lexika/lexikon-in-einfacher-sprache/249815/brief-post-und-fernmeldegeheimnis/ (Stand: 8. Juni 2022)

[Wikipedia-IT-Grundrecht] Wikipedia: Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (umgangssprachlich auch als IT-Grundrecht, Computer-Grundrecht oder Grundrecht auf digitale Intimsphäre bezeichnet[1]) ist ein in der Bundesrepublik Deutschland geltendes Grundrecht, welches vornehmlich dem Schutz von persönlichen Daten dient, die in informationstechnischen Systemen gespeichert oder verarbeitet werden. Dieses Recht wird im Grundgesetz nicht eigens genannt, sondern wurde als spezielle Ausprägung des allgemeinen Persönlichkeitsrechts 2008 durch das Bundesverfassungsgericht derart formuliert bzw. aus vorhandenen Grundrechtsbestimmungen abgeleitet. URL: https://de.wikipedia.org/wiki/Grundrecht_auf_Gew%C3%A4hrleistung_der_Vertraulichkeit_und_Integrit%C3%A4t_informationstechnischer_Systeme (Stand: 7. Juni 2022)

[EDRI, 17.03.2022] EDRI: Open letter: Protecting digital rights and freedoms in the Legislation to effectively tackle child abuse. EDRi is one of 52 civil society organisations jointly raising our voices to the European Commission to demand that the proposed EU Regulation on child sexual abuse complies with EU fundamental rights and freedoms. You can still add your voice now! URL: https://edri.org/our-work/protecting-digital-rights-and-freedoms-in-the-legislation-to-effectively-tackl (Stand: 10. Juni 2022)

[Netzpolitik.org, 20.05.2022] Meineck, Sebastion: Das sagen Kinderschutz-Organisationen zur Chatkontrolle. Neben dem Kinderschutzbund lehnt auch der Deutsche Kinderverein Chatkontrollen mit Nachdruck ab – als „massiven Eingriff in rechtsstaatliche Grundsätze“. Es gibt aber auch Fürsprache. URL: https://netzpolitik.org/2022/massenueberwachung-das-sagen-kinderschutz-organisationen-zur-chatkontrolle/ (Stand: 10. Juni 2022)

[Deutscher Kinderverein] Deutscher Kinderverein: GEGEN KINDESMISSHANDLUNG. FÜR DIE RECHTE VON KINDERN. URL: https://deutscher-kinderverein.de/ueber-uns/ (Stand: 10. Juni 2022)

[Netzpolitik.org, 21.03.2022] Reuter Markus: BKA soll nur finden, nicht löschen. Die Rekordzahlen bei Ermittlungen gegen Kindesmissbrauch im Internet führen nicht dazu, dass diese Materialien auch konsequent gelöscht werden. Die Bundesregierung sagt nun, dass das Bundeskriminalamt gar nicht für Löschmeldungen zuständig sei. URL: https://netzpolitik.org/2022/darstellungen-von-kindesmissbrauch-bka-soll-nur-finden-nicht-loeschen/ (Stand: 10. Juni 2022)

[Der Deutsche Kinderschutzbund] Der Deutsche Kinderschutzbund: URL: https://www.dksb.de/de/startseite/ (Stand: 10. Juni 2022)

[Netzwek Kinderrechte] Netzwek Kinderrechte: Für die Rechte der Kinder.„Bei allen Maßnahmen, die Kinder betreffen, [...] ist das Wohl des Kindes ein Gesichtspunkt, der vorrangig zu berücksichtigen ist.“ (Art. 3 UN-KRK). URL: https://netzwerk-kinderrechte.de/home/ueber-uns/ (Stand: 10. Juni 2022)

[Innocence in Danger] Innocence in Danger Warum die Arbeit von Innocence in Danger so wichtig ist. Ziel von Innocence in Danger ist der Schutz von Kindern vor sexuellem Missbrauch und pornografischer Ausbeutung im Internet. URL: https://innocenceindanger.de/ueber-uns/ (Stand: 10. Juni 2022)

[DIE ZEIT, 05.04.2022] Parth, Christian: “Wir konnten mehr Kinder aus dem Missbrauch befreien“. Die Kriminalität sinkt insgesamt, doch die Polizei registriert so viele Missbrauchsdarstellungen wie noch nie. Das sei eine gute Nachricht, sagt Ermittler Sven Schneider. URL: https://www.zeit.de/gesellschaft/2022-04/sexualisierte-gewalt-kinder-missbrauch-polizei-ermittlung (Stand: 10. Juni 2022)

[Tagesschau, 22.05.2022] Tagesschau: Mehr ermitteln, mehr Täter entdecken. Bilder und Videos sexualisierter Gewalt gegen Kinder kursieren oft in Foren und im Darknet. Innenministerin Faeser will die Ermittlungsbehörden deshalb verstärken. Einen Eingriff in die verschlüsselte Privatkommunikation lehnt sie ab. URL: https://www.tagesschau.de/inland/faeser-sexualisierte-gewalt-verfolgen-101.html (Stand: 7. Juni 2022)

[Tiemo Wölken] Wölken, Tiemo: Morgen veröffentlicht die @EU_Commission ihren Vorschlag zur Bekämpfung von Kindesmissbrauch #CSAM. Der geleakte Entwurf ist eine Katastrophe: #Chatkontrolle auch bei privater Kommunikation, #Netzsperren, #AgeVerification - alles was das Überwachungsherz begehrt. URL: https://twitter.com/woelken/status/1524068321955663873 (Stand: 7. Juni 2022)

[Alexandra Geese] Geese, Alexandra: #Chatkontrolle verletzt das Grundrecht auf vertrauliche Kommunikation und ist ein gefährlicher Tabubruch. Kinder werden durch mehr Personal für Ermittler*innen und Jugendschutz geschützt, nicht durch systematisches Ausspionieren. URL: https://twitter.com/AlexandraGeese/status/1524263829361864704 (Stand: 7. Juni 2022)

[BMDV] Bundesministerium für Digitales und Verkehr: #Kinder müssen wirksam vor #Missbrauch im Netz geschützt werden. Gleichzeitig darf es nicht zu einer anlasslosen Kontrolle privater Kommunikation kommen. Das @bmdv_bund wird darauf hinwirken, deutlich zielgerichteter vorzugehen. URL: https://twitter.com/BMDV_bund/status/1525737371844632576?t=VL8-gEFl1HnAOl2N9_llSQ (Stand: 7. Juni 2022)

[Sabine Leutheusser] Leutheusser-Schnarrenberger, Sabine: Der Kommissions-Entwurf zur Bekämpfung von Kindesmissbrauch im Netz überschreitet alle Vorstellungen. #Uploadfilter könnten in unvorstellbarem Ausmaß kommen, auch in Messengern. Das Recht auf #Verschlüsselung wird unmöglich gemacht. Das wäre mehr als #Chatkontrolle. URL: https://twitter.com/sls_fdp/status/1524354541386407936 (Stand: 7. Juni 2022)

[Abgeordnetenwatch-06.04.2022] Notzs, Konstantin: Sehr geehrter Herr K. vielen Dank für Ihre Frage zur „Chatkontrolle“ und ihr darin zum Ausdruck kommendes Interesse an meiner politischen Arbeit. Über beides habe ich mich sehr gefreut. URL: https://www.abgeordnetenwatch.de/profile/konstantin-von-notz/fragen-antworten/wie-stehen-sie-zur-sog-chatkontrolle (Stand: 7. Juni 2022)

[Polizei Beratung, 19.06.2020] Polizei Beratung: Sexting: Wann sind Nacktbilder strafbar?. Beim so genannten Sexting versenden Menschen freiwillig erotische Fotos, Videos oder Nachrichten über Mail oder Messenger an de Partner oder die Partnerin. Grundsätzlich das mit gegenseitigem Einverständnis auch erlaubt. Bei Minderjährigen kann es sich jedoch auch um Kinder- und Jugendpornografie handeln - und das ist strafbar. URL: https://www.polizei-beratung.de/startseite-und-aktionen/aktuelles/detailansicht/sexting-wann-sind-nacktbilder-strafbar/ (Stand: 5. Juni 2022)

[lessentiel, 18.07.2014] Lessentiel: NSA-Mitarbeiter tauschen Nacktbilder aus. Die Datensammelei der NSA hat angeblich eine weitere Nebenwirkung. Laut Edward Snowden tauschen Analysten abgefischte Nacktbilder untereinander aus. URL: https://www.lessentiel.lu/de/story/nsa-mitarbeiter-tauschen-nacktbilder-aus-564393357190 (Stand: 5. Juni 2022)