D64
Zentrum für
Digitalen Fortschritt

# Check-Liste für Gespräche zur Chatkontrolle bzw. CSA-Verordnung

Die Bundesregierung lehnt – wohl auch in Reaktion auf den massiven öffentlichen Druck durch die Zivilgesellschaft – die Einführung der "Chatkontrolle" ab. Nun geht es also erneut in Verhandlungen zur Ressortabstimmung für die Positionierung Deutschlands auf EU-Ebene. Über die "Chatkontrolle", also die Überwachung privater Nachrichten hinaus, finden sich im Entwurf der CSA (Child Sexual Abuse) Verordnung auch noch andere problematische Vorschläge, wie Altersverifikationen und Netzsperren.

Diese Handreichung soll dabei unterstützen, der inhaltlichen Entleerung etablierter Konzepte im politischen Diskurs entgegenzuwirken. So ist uns aufgefallen, dass sich beispielsweise Vertreterinnen und Vertreter aus dem Sicherheitsbereich gegen "anlasslose" Überwachung aussprechen, den "Anlass" aber soweit fassen, dass ihm keine eigenständige Bedeutung mehr zukommt. Das widerspricht dem bisherigen Verständnis, welches insbesondere auch von der einschlägigen (verfassungsgerichtlichen) Rechtsprechung geteilt wird. Wir regen an, dass in diesen Fällen kritisch nachgefragt wird.

Im Folgenden stellen wir beispielhaft Äußerungen dar, bei denen sich unserer Erfahrung nach kritische Nachfragen lohnen. Die Äußerungen sind thematisch nach den wichtigsten Konzepten in der Debatte um die CSA-Verordnung geordnet.



Fehlen Begriffe? Gibt es noch Fragen? Wir stehen gerne für ein Hintergrundgespräch zur Klärung von Einzelheiten zur Verfügung und sind jederzeit unter info@d-64.org erreichbar.

D64 – Zentrum für digitalen Fortschritt e. V. setzt sich in Deutschland und Europa für eine Digitalpolitik ein, in der die Grundwerte Freiheit, Gerechtigkeit und Solidarität verwirklicht werden. Mit rund 800 Mitgliedern gehört D64 zu den größten digitalpolitischen Vereinen in der DACH-Region.

D64 ist Teil des Bündnisses Chatkontrolle STOPPEN!.

## Flächendeckende Überwachung

***Selbstverständlich bin ich gegen flächendeckende Überwachung!***

- Einige Akteure aus dem Sicherheitsbereich vertreten die Ansicht, dass Überwachung nicht "flächendeckend" sei, wenn nur einige Anbieter überwacht werden. Dabei kann es jedoch völlig genügen, einzelne, große Anbieter zu verpflichten, um die Kommunikation (nahezu) aller Menschen in Europa zu erfassen. So nutzen zum Beispiel rund 80 % der Deutschen Whatsapp. Es muss also nicht jeder Anbieter verpflichtet werden, damit (fast) alle überwacht werden.
- Der Europäische Gerichtshof hat in seiner Rechtsprechung betont, dass Überwachungsmaßnahmen immer dann besonders bedenklich sind, wenn sie "pauschal sämtliche Personen [erfasst], die elektronische Kommunikationsdienste nutzen, ohne dass sich diese Personen auch nur mittelbar in einer Lage befinden, die Anlass zur Strafverfolgung geben könnte", also auch für Personen gilt "bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit dem Ziel der Bekämpfung schwerer Straftaten stehen könnte" (ständige Rechtsprechung, vgl. bspw. *La Quadrature du Net*, 2020, Rn. 143)

## Anlasslose Überwachung

***Ich spreche mich entschieden gegen anlasslose Überwachung aus!***

- Auch hier wird teilweise versucht, das Konzept des "Anlasses" weit über die bisherigen Grenzen auszudehnen. Als "Anlass" kann aber nicht ausreichen, dass die Überwachungsmaßnahme ein legitimes Ziel verfolgt (wie bspw. die Bekämpfung von Kindesmissbrauch), es muss in Bezug auf die Betroffenen einen konkreten Anlass geben, warum eben diese Personen überwacht werden sollten.
- Das Bundesverfassungsgericht hat in seiner Rechtsprechung mehrfach betont, dass der "Anlass" für derart intensive Überwachungsmaßnahmen hinreichend konkret im Einzelfall vorliegen muss. So heißt es bspw. in der *Entscheidung zum BKA-Gesetz* aus 2016: "Der Zugriff auf informationstechnische Systeme und die Wohnraumüberwachung dürfen sich unmittelbar nur gegen diejenigen als Zielperson richten, die für die drohende oder dringende Gefahr verantwortlich sind [...]. Ihre Erstreckung auf Dritte steht unter strengen Verhältnismäßigkeitsanforderungen und setzt eine spezifische individuelle Nähe der Betroffenen zu der aufzuklärenden Gefahr oder Straftat voraus." (Rn. 115, 116)
- Im Koalitionsvertrag wird betont, "dass Daten rechtssicher anlassbezogen und durch richterlichen Beschluss gespeichert werden können."

## Private, verschlüsselte Kommunikation

***Private, verschlüsselte Kommunikation möchten wir nicht überwachen!***

- Private und verschlüsselte Kommunikation wird oft synonym verwendet, es handelt sich aber nicht um das Gleiche. E-Mails sind bspw. in aller Regel privat, aber oft nicht (Ende-zu-Ende-) verschlüsselt. Zwar ist das Aufbrechen oder Umgehen von Ende-zu-Ende-Verschlüsselung ganz besonders problematisch (siehe hierzu auch den nächsten Punkt, "Client-Side-Scanning"), es ist aber jede Form der privaten Kommunikation grundrechtlich geschützt, egal, ob sie verschlüsselt ist oder nicht.
- Das Recht auf vertrauliche Kommunikation wird in der Europäischen Union insbesondere durch Art. 7 (Recht auf Privatsphäre) und Art. 8 (Recht auf Datenschutz) der Grundrechte-Charta gewährleistet. Die Bundesrepublik ist darüber hinaus durch die sich aus Art. 10 GG (Brief-, Post- und Fernmeldegeheimnis) ergebende Schutzpflicht aus verfassungsrechtlichen Gründen dazu aufgefordert, das Kommunikationsgeheimnis auch vor Eingriffen privater oder supra- bzw. internationaler Institutionen zu schützen.
- Auch die Rechtsprechung des EuGH macht die offenkundige Unvereinbarkeit des aktuellen Vorhabens mit den genannten Grundrechten deutlich. So hat der Gerichtshof mehrfach betont, dass ein genereller Zugriff auf Inhalte von Kommunikation den nach Art. 52 Abs. 1 S. 1 GrCh absolut geschützten Wesensgehalt des Rechts auf Achtung des Privatlebens verletzt (*Digital Rights*, 2014, Rn. 39; *Schrems I*, 2015, Rn. 94).
- Im Koalitionsvertrag heißt es diesbezüglich: "Allgemeine Überwachungspflichten, Maßnahmen zum Scannen privater Kommunikation und eine Identifizierungspflicht lehnen wir ab. […] Solange der Schutz des Kernbereichs privater Lebensgestaltung nicht sichergestellt ist, muss ihr Einsatz unterbleiben".

## Client-Side-Scanning

***Wir müssen uns Client-Side-Scanning annähern.***

- Client-Side-Scanning beschreibt das Durchsuchen von Nachrichten bevor diese verschlüsselt werden. Dabei wird der Inhalt von Nachrichten (Text, Bild, Audio oder Video) vor dem Versenden mithilfe von Künstlicher Intelligenz oder anderen Technologien analysiert.
- Man kann sich dem Client-Side-Scanning nicht "annähern", entweder nutzt man es, oder nicht. Client-Side-Scanning setzt vor der eigentlichen Verschlüsselung an und macht Ende-zu-Ende verschlüsselte Kommunikation damit obsolet. In der Sache handelt es sich um eine Überwachung von Telekommunikation auf dem jeweiligen Gerät. Als „Quellen-TKÜ" ist ein ähnliches Verfahren in Deutschland bereits möglich, rechtlich aber hoch umstritten und an hohe Anforderungen im Einzelfall geknüpft. Insbesondere werden hierbei aber auch nicht die Kommunikationsanbieter verpflichtet, Hintertüren zum Scannen von Inhalten in ihre Software zu bauen.
- Bereits im letzten Jahr warnten führenden Sicherheitsforscher*innen vor den Sicherheitsrisiken dieser Technologie.

- Der Hohe Kommissar für Menschenrechte der UN warnt vor einem gefährlichen Paradigmenwechsel durch Client-Side-Scanning, der mehr als nur das Recht auf Privatsphäre gefährden würde.
- Im Koalitionsvertrag heißt es dazu: „Wir führen ein Recht auf Verschlüsselung [...] ein".

## Vorhaben jenseits der Chatkontrolle

***Natürlich lehne ich die Chatkontrolle, also das Durchsuchen von Messengern, ab!***

- Der Entwurf der CSA-Verordnung umfasst noch deutlich mehr als Chatkontrolle. So beinhaltet er Vorschläge zur Einführung von Altersverifikation, Upload-Filter, Netzsperren sowie die Überwachung von Cloud-Anbietern, die ebenfalls problematisch sind.
- Eine Übersicht mit allen Vorschlägen inklusive einer Bewertung hat hat European Digital Rights (EDRi) hier erstellt.

### Netzsperren

***Mit Netzsperren können wir die Verbreitung von Material verhindern!***

- Der Verordnungsentwurf sieht Sperrverpflichtungen für Internetzugangsanbieter vor, die sich auf einzelne Webseiten (URLs) beziehen. Vor Erlass einer Sperranordnung sollen Internetzugangsanbieter den Behörden Informationen über den Zugriff von Nutzer*innen auf die betreffende URL übermitteln. Diese Informationen liegen den Internetzugangsanbietern nicht vor, wenn die URL mittels SSL („https") in verschlüsselter Form aufgerufen wird. Der flächendeckende Einsatz von https ist aus Sicherheitsgründen erforderlich und wird vom Bundesamt für Sicherheit in der Informationstechnik empfohlen.
- Auch eine gezielte Sperrung von einzelnen URLs ist den Internetzugangsanbietern ohne eine Aufgabe der https-Verschlüsselung und die Überwachung der Kommunikationsinhalte mittels Deep Packet Inspection nicht möglich. DNS-Sperren sind für die geplante Sperrung einzelner URLs nicht geeignet, denn sie betreffen stets ganze Domains. Eine DNS-Sperre, die gegen eine Missbrauchsdarstellung auf einer Sharehosting-Plattform gerichtet ist, würde auch alle anderen Inhalte des Sharehosters betreffen und damit den Anforderungen des EuGH an Zielgerichtetheit von Netzsperren nicht entsprechen.
- Im Koalitionsvertrag heißt es dazu: „Wir führen ein Recht auf Verschlüsselung [...] ein".

### Altersverifikation

***Mit einer Altersverifikation erhöhen wir die Sicherheit für alle!***

- Eine Altersverifikation ohne allgemeine Offenlegung der Identität ist zum jetzigen Zeitpunkt schwer vorstellbar.
- Es gibt Überlegungen, den elektronischen Personalausweis dafür zu nutzen oder die eID (eIDAS) so zu gestalten, dass nur das Alter ohne Offenlegung der Identität geprüft werden kann. Einerseits können dadurch Menschen ohne Papiere von der Internetnutzung ausgeschlossen werden. Außerdem ist es sehr wahrscheinlich, dass die eID für Kinder auf

den Geräten der Eltern gespeichert werden. Somit haben Erwachsene die Möglichkeit, sich im Internet als Kinder auszugeben.

- Geheimheit und Anonymität sind grundsätzliche Voraussetzungen für Freiheit. Es ist deshalb essenziell, dass es möglich ist, sich im (digitalen) öffentlichen Raum im Schutze der Anonymität bewegen zu können. Dies gilt umso mehr, wenn der für die Demokratie konstitutive öffentliche Debattenraum betroffen ist, in dem Meinungen und Überzeugungen ausgetauscht, argumentiert und diskutiert werden.
- Eine allgemeine Identifikationspflicht wäre mit erheblichen *chilling effects* für die – auch in der EU durch Art. 11 grundrechtlich geschützten – Informations- und Meinungsfreiheit verbunden. Diese dürfte aber "durch die Hintertür" durch die geplante Altersverifikation für App-Stores oder Messenger (als Teil ihrer Risikominimierung) eingeführt werden. Bisher sind keine Maßnahmen bekannt, die eine solche Altersverifikation ohne eine allgemeine Offenlegung der Identität ermöglichen.
- Im Koalitionsvertrag heißt es dazu: "Anonyme und pseudonyme Online-Nutzung werden wir wahren".

**Künstliche Intelligenz / Uploadfilter**

***Mit künstlicher Intelligenz können wir das Material filtern!***

- Die bestehende Technologie hat eine sehr hohe Fehleranfälligkeit.
- Der Gesetzesentwurf sieht die Erkennung von unbekanntem Material und Anbahnungsversuchen sogenanntem Grooming vor. Auch wenn der Gesetzesentwurf technologieneutral gehalten ist, ist klar, dass hier Filtersysteme zum Einsatz kommen sollen, die auf künstlicher Intelligenz (KI) beruhen.
- Die Fehlerkennungsraten bereits existierender KI-Lösungen sowie die Prognosen im Hinblick auf zukünftige Entwicklungen liegen in einer Höhe, die zu falsch erkannten Material im Millionenbereich oder mehr, je nach Kommunikationsaufkommen, führen würden.
- Dies würde nicht nur für eine extreme Belastung der Ermittlungsbehörden sorgen, sondern auch Bürger:innen fälschlicherweise in den Fokus von Ermittlungen rücken.
- Der Einsatz von KI im Zusammenhang mit hochvertraulicher Kommunikation bringt mehr Risiken mit sich, als dass er das eigentliche Problem löst. Technologien wie KI sind nicht die magische Antwort auf komplexe gesellschaftliche Probleme. Eine entsprechende Ausstattung der Ermittlungsbehörden mit personellen Ressourcen ist weitaus weniger eingriffsintensiv und effizienter für den Schutz aller Bürger:innen.
- Im Koalitionsvertrag heißt es zu Filterpflichten: "Zum Schutz der Informations- und Meinungsfreiheit lehnen wir verpflichtende Uploadfilter ab" und zur Anwendung von künstlicher Intelligenz (KI): "Bei der Gestaltung von KI in der Arbeitswelt setzen wir auf einen menschenzentrierten Ansatz, soziale und wirtschaftliche Innovation ebenso wie Gemeinwohlorientierung. Wir unterstützen den risikobasierten EU-Ansatz."