

Anlasslose, biometrische Massenkontrolle

EU-Massenscanning-Strategie

Die Möglichkeit zur privaten Kommunikation soll abgeschafft werden

von Dr. Peter F. Mayer, Wien | tkp.at [3] – Der Blog für Science & Politik

Die EU-Kommission arbeitet seit einiger Zeit daran, das Briefgeheimnis abzuschaffen und vor allem private Chats anlasslos abzuhören und die Verschlüsselung zu durchbrechen. Diese EU-Pläne zur verpflichtenden Durchleuchtung privater Kommunikation und Aufhebung sicherer Verschlüsselung (Chatkontrolle 2.0) wurde mangels Mehrheit im EU-Rat vorerst auf Eis gelegt. Aber die Parlamentsberichterstatte~~r~~rin [Birgit Sippel](#) [4] (SPD) forciert eine Verlängerung der bestehenden freiwilligen verdachtslosen Chatkontrolle. Dagegen gibt es jedoch heftigen Widerstand.

Ein Konsortium von Technologieunternehmen hat einen dringenden Appell an Politiker in der gesamten Europäischen Union gerichtet. Darin wird eindringlich davor gewarnt, eine vorgeschlagene Verordnung zu unterstützen, die sich auf den sexuellen Missbrauch von Kindern konzentriert und als Vorwand dient, die Sicherheitsintegrität von Internetdiensten zu gefährden, die auf eine Ende-zu-Ende-Verschlüsselung basiert, wie RECLAIM THE NET [am 29.01.2024 berichtet](#) [5].

Insgesamt 18 Organisationen – überwiegend Anbieter von verschlüsselten E-Mail- und Messaging-Diensten – haben sich besorgt über die potenzielle experimentelle Verordnung der Europäischen Kommission geäußert und die „schädlichen“ Auswirkungen auf die Privatsphäre und Sicherheit von Kindern sowie die möglichen schlimmen Folgen für die Cybersicherheit hervorgehoben.

In einem offenen Brief, der am 22. Januar 2024 veröffentlicht wurde, wird argumentiert, dass der Entwurf der EU-Kommission, der unter dem Namen „Chat Control“ bekannt ist und das umfassende Scannen verschlüsselter Kommunikation vorschreibt, Schwachstellen im Internet schaffen kann, die Bürger und Unternehmen einem erhöhten Risiko aussetzen. Der Brief thematisiert auch die Pattsituation zwischen den Mitgliedsstaaten, der EU-Kommission und dem Europäischen Parlament, die ihre unterschiedlichen Ansichten über die Verhältnismäßigkeit und Durchführbarkeit der EU-Massenscanning-Strategie im Hinblick auf die Sicherheit von Kindern noch nicht in Einklang gebracht haben.

Zu den Unterzeichnern gehören Proton, ein verschlüsselter E-Mail-Dienst aus der Schweiz, Tuta Mail und NextCloud, die auf E-Mail bzw. Cloud-Speicher spezialisiert sind, sowie Element, ein Anbieter von verschlüsselten Kommunikations- und Kollaborationsdiensten. Gemeinsam fordern sie die Staats- und Regierungschefs der EU auf, eine ausgewogenere Version der Verordnung in Erwägung zu ziehen, wie sie vom Europäischen Parlament vorgeschlagen wurde und die nach Ansicht von Experten wirksamer und effizienter ist als das massenhafte Scannen verschlüsselter Dienste.

Die von der Europäischen Kommission vorgeschlagene Version der Verordnung drängt Technologieunternehmen dazu, „Hintertüren“ einzubauen oder „clientseitiges Scannen“ zu nutzen, um den Inhalt aller verschlüsselten Kommunikationen auf Hinweise auf sexuellen Kindesmissbrauch zu untersuchen. Diese Unternehmen sind jedoch der festen Überzeugung, dass der Mechanismus trotz seines Zwecks, die Cyberkriminalität zu bekämpfen, schnell von Straftätern genutzt werden könnte, was „die Sicherheit für alle gefährdet“.

Die Anwendung des clientseitigen Scannens – die Gegenüberstellung von „Hash-Werten“ verschlüsselter Nachrichten mit einer „Hash-Wert“-Datenbank rechtswidriger Inhalte, die sich auf persönlichen Geräten befinden – stößt in der Sicherheitsgemeinschaft auf heftige Kritik.

Trotz des positiven Standpunkts der EU zum Datenschutz, der den Weg für ethische, datenschutzfreundliche Technologieunternehmen auf dem europäischen Markt geebnet hat, glauben diese Technologieunternehmen, dass der Vorschlag der EU-Kommission anderen EU-Vorschriften wie dem [Cyber Resilience Act](#) [6] (CSA) und dem [Cybersecurity Act](#) [7] widersprechen könnte, die die Anwendung von Ende-zu-Ende-Verschlüsselung zur Bekämpfung von Cyberrisiken fördern.

Die Technologieunternehmen schlagen Alternativen zum obligatorischen Scannen vor, die ihrer Meinung nach effektiver sind und dem Datenschutz und der Sicherheit Vorrang einräumen. Sie argumentieren, dass ein Ansatz, der mit den Vorschlägen des Europäischen Parlaments übereinstimmt, einen soliden Rahmen für den Schutz von Kindern bietet. Darüber hinaus erörtern sie die Gefahr, dass eine solche Scantechnologie von repressiven Regimen zur Unterdrückung politisch Andersdenkender missbraucht werden könnte.

Der Bürgerrechtler und Jurist [Dr. Patrick Breyer](#) [8] (* 29. April 1977) ist Abgeordneter zum EU-Parlament der

Piratenpartei, wendet sich ebenfalls gegen die verdachtslose Chatkontrolle und [fordert die Beendigung](#) [9] der von US-Konzernen wie Meta, Google und Microsoft eigenmächtig praktizierte Chatkontrolle privater Nachrichten über Instagram Messenger, Facebook Messenger, GMail und Xbox.

Dr. Breyer kommentiert:

„Statt den neuen Vorschlag des EU-Parlaments zu einem wirksameren und gerichtsfesten Kinderschutz ohne Chatkontrolle aufzugreifen, beharrt EU-Kommissarin ‚Big Sister‘ [Ylva Johansson](#) [10] unverbesserlich auf einer Zerstörung des digitalen Briefgeheimnisses, spielt auf Zeit und hofft kritische EU-Staaten mit infamen Kampagnen und Falschinformationen zur Zustimmung zu manipulieren.

Diesen Machenschaften sollten wir eine klare Absage erteilen und auf den vom Parlament vorgeschlagenen Lösungen ohne Massenüberwachung bestehen.“

Patrick Breyer kritisiert das Instrument der freiwilligen Chatkontrolle scharf:

„Die freiwillige Massenüberwachung unserer persönlichen Nachrichten und Fotos durch US-Dienste wie Meta, Google oder Microsoft leistet keinen signifikanten Beitrag zur Rettung missbrauchter Kinder oder Überführung von Missbrauchtätern, sondern kriminalisiert umgekehrt tausende Minderjähriger, überlastet Strafverfolger und öffnet einer willkürlichen Privatjustiz der Internetkonzerne Tür und Tor. Wenn nach Johanssons eigenen Angaben nur jede vierte Meldung überhaupt für die Polizei relevant ist, bedeutet das für Deutschland Jahr für Jahr 75.000 ausgeleitete intime Strandfotos und Nacktbilder, die bei unbekannten Moderatoren im Ausland nicht sicher sind und in deren Händen nichts zu suchen haben.“

„Die Verordnung zur freiwilligen Chatkontrolle ist sowohl unnötig als auch grundrechtswidrig: Die sozialen Netzwerke als Hostingdienste brauchen zur Überprüfung öffentlicher Posts keine Verordnung. Dasselbe gilt für Verdachtsmeldungen durch Nutzer. Und die fehleranfälligen automatisierten Meldungen aus der Durchleuchtung privater Kommunikation durch Zuckerbergs Meta-Konzern, die 80% der Chatmeldungen ausmachen, werden durch die angekündigte Einführung von Ende-zu-Ende-Verschlüsselung ohnehin entfallen.

Das Rechtsgutachten einer ehemaligen EuGH-Richterin belegt, dass die freiwillige Chatkontrolle als verdachtslose und flächendeckende Überwachungsmaßnahme grundrechtswidrig ist. Ein Missbrauchsbetroffener und ich klagen dagegen. Und das Digitalministerium hat bestätigt, dass die Ausnahmeverordnung eine freiwillige Chatkontrolle in Deutschland überhaupt nicht möglich macht.“

Dr. Peter F. Mayer

» **Pressemitteilung von Patrick Breyer: Chatkontrolle heute im EU-Parlament, morgen (01.02.2024) vor Gericht.**

Der EU-Innenausschuss hat heute grünes Licht für eine Verlängerung der umstrittenen Chatkontrolle durch US-Internetkonzerne bis 2025 gegeben. Ein [Ablehnungsantrag](#) [11] (S. 3) wurde nur von Piraten, Grünen, Linke und FDP unterstützt, insgesamt jedoch mit den Stimmen von CDU, SPD und AfD [zurückgewiesen](#) [12] (S. 2). Gibt das EU-Parlament insgesamt in einer Plenarabstimmung nächste Woche grünes Licht, will das Parlament sich mit dem Rat noch im Februar einig werden.

Kläger Patrick Breyer kommentiert:

»Es macht mich wütend, dass sich US-Konzerne mithilfe fehleranfälliger Verdächtigungsmaschinen zum Privatkontrolleur unserer persönlichen Nachrichten aufschwingen wollen. Diese Anmaßung lässt jeden Respekt vor dem digitalen Briefgeheimnis vermissen. Unsere ohnehin überlasteten Ermittler mit vielfach falschen Maschinendenunziationen zu überfluten, hat mit Effizienz nichts zu tun. Folge ist vor allem die Kriminalisierung Jugendlicher wegen unbedachter Chatnachrichten – so wird das Gegenteil von Kinderschutz erreicht.

Selbst intimste Nacktfotos und Sex-Chats können plötzlich bei zweifelhaftem und unterbezahltem Unternehmenspersonal oder der Polizei landen. Nach meinen Informationen war der Anteil der aus den USA geleakten Chatnachrichten und Privatfotos, die vom BKA als strafrechtlich völlig irrelevant eingestuft wurden, im letzten Jahr so hoch wie noch nie. Wer das digitale Briefgeheimnis zerstört, zerstört Vertrauen. Auf Sicherheit und Vertraulichkeit privater Kommunikation sind wir alle angewiesen: Menschen in Not, Missbrauchsoffer, Kinder, die Wirtschaft und auch Staatsbehörden.

Organisierte Kinderporno-Ringe benutzen keine E-Mails oder Messengerdienste, sondern abgeschottete selbst betriebene Foren. Dass Strafverfolger sich weigern, bekanntes Ausbeutungsmaterial löschen zu lassen, ist ein Skandal. Was wir brauchen, ist Löschen statt Schnüffeln!

Als Piratenabgeordneter werde ich nicht nur nächste Woche eine Plenarabstimmung über die heutige Fehlentscheidung des EU-Parlamentsausschusses erwirken, ich will die illegale Chatkontrolle vor Gericht stoppen lassen!«

Morgen (1. Februar 2024) wird vor dem Landgericht Kiel in öffentlicher Sitzung ab 09:30 Uhr (Az. 13 O 40/23) die Klage des profiliertesten Kritikers der Chatkontrolle, des Europaabgeordneten Dr. Patrick Breyer von der Piratenpartei verhandelt. Breyer verklagt Meta als Mutterkonzern von Facebook und Instagram, der für 80% der ausgeleiteten Chats und Privatfotos verantwortlich ist, auf Unterlassung. Meta hat vor Gericht versprochen, die Chatkontrolle in Direktnachrichten auf Facebook und Instagram einzustellen und sichere Ende-zu-Ende-Verschlüsselung einzuführen, jedoch ist dieses Versprechen bis heute nicht eingelöst.

Ergänzung vom 01.02.2024: Vor dem Landgericht Kiel wurde Breyers Klage heute verhandelt. Meta weigerte sich, sich zu verpflichten, die Chatkontrolle auch künftig zu unterlassen. Das Gericht will zunächst die Zulässigkeit der Klage klären. Es hat für den 27. März eine Entscheidung angekündigt. (Quelle>> [Pressemeldung](#) [13]).

▣» **EU-Chatkontrolle: Bericht zeigt verheerende Bilanz.**« Von Dr. Peter F. Mayer, tkp, 22.12.2023 >> [weiter](#) [14].

▣» **EU einigt sich auf KI-Gesetz für biometrische Massenüberwachung**« Von Dr. Peter F. Mayer, 12.12.2023 >> [weiter](#) [15].

▣» **Noch mehr Überwachung und Kontrolle der Bürger durch EU: Digitale Briefftasche als digitale ID**« Von Dr. Peter F. Mayer, tkp, 10.11.2023 >> [weiter](#) [16].

▣» **EU-Propagandamaschine zur totalen Chatkontrolle.**« Von Thomas Oysmüller, tkp, 17.10.2023 >> [weiter](#) [17].

▣» **Chatkontrolle: EU-Gesetzgebung einfach erklärt.** Am Beispiel der Chatkontrolle kann man ganz praktisch lernen, wie EU-Gesetzgebung vonstatten geht. Elisa Lindinger, Elina Eickstädt und Constanze Kurz erklären, wie ein Gesetz zustande kommt und welche Institutionen dabei mitwirken. Sie sprechen auch über die Beteiligung der Zivilgesellschaft – und über Ashton Kutcher.« Von Netzpolitik.org, 28.06.2023 >> [weiter](#) [18].

▣» **So führt EU-Kommissarin Ylva Johansson die Öffentlichkeit in die Irre.** Im Interview mit dem SPIEGEL verteidigt EU-Kommissarin Johansson die von der EU geplante Chatkontrolle. Dabei sagt sie drei Mal die Unwahrheit und verbreitet mindestens sieben Mal irreführende Aussagen.« Von Netzpolitik.org, 10.02.2023 >> [weiter](#) [19].

► **Quelle:** Dieser Beitrag wurde am 31. Januar 2024 veröffentlicht auf [TKP.at](#) [3] >> [Artikel](#) [20]. Eigentümer, Herausgeber und für den Inhalt verantwortlich ist Dr. Peter F. Mayer, 1215 Wien/A. (E-Mail: home@tkp.at). Das Urheberrecht der Inhalte von tkp.at liegt, wenn nicht anders gekennzeichnet, bei den jeweiligen Autoren.

Einzelne Artikel dürfen unter bestimmten Bedingungen übernommen werden. Es gilt die Creative Commons-Lizenz mit den folgenden Einschränkungen: Ein übernommener Artikel darf nicht kommerziell verwendet werden. AutorIn und tkp.at müssen als Ursprung klar ersichtlich genannt werden. In Online-Medien muss zusätzlich ohne nofollow-Tag oder ähnliche Mechanismen auf den ursprünglichen Beitrag verlinkt werden.

ACHTUNG: Die Bilder, Grafiken, Illustrationen und Karikaturen sind **nicht** Bestandteil der Originalveröffentlichung und wurden von KN-ADMIN Helmut Schnug eingefügt. Für sie gelten folgende Kriterien oder Lizenzen, siehe weiter unten. Grünfärbung von Zitaten im Artikel und einige zusätzliche Verlinkungen wurden ebenfalls von H.S. als Anreicherung gesetzt, ebenso die Komposition der Haupt- und Unterüberschrift(en) geändert.

► Bild- und Grafikquellen:

1. Chatkontrolle STOPPEN! Mitglieder des Ausschusses für bürgerliche Freiheiten ([LIBE](#) [21]) des Europäischen Parlaments haben im November 2023 gegen den Versuch von EU-Innenkommissarin Ylva Johansson gestimmt, private und verschlüsselte Nachrichten in ganz Europa anlasslos und massenhaft zu scannen. Die Abgeordneten stellen sich damit gegen die Pläne zur Chatkontrolle.

Bei der sogenannten Chatkontrolle geht es um eine Verordnung zur Bekämpfung von sexualisierter Gewalt gegen Kinder im Internet, die verschiedene Instrumente neben der eigentlichen Chatkontrolle bereithält. Die ursprünglichen Pläne der EU-Kommission würden mit der „Chatkontrolle“ eine neue Form anlassloser Massenüberwachung einführen – sogar von später verschlüsselter Kommunikation. **Foto/Grafik:** Konstantin Macher. **Quelle:** digitalcourage.de/ >> [Grafik](#) [22]. Die Datei ist mit der CC-Lizenz Namensnennung 4.0 International ([CC BY 4.0 Deed](#) [23]) lizenziert.

<https://digitalcourage.de/> [24]

2. Nicht einmal im Bett kann man sicher vor Überwachung sein. Die EU möchte Chats und Messenger überwachen. Chatkontrolle ist sehr intim. **Foto:** Jakob Rieger/Digitale Freiheit. **Quelle:** [Flickr](#) [25]. Die Datei ist mit der CC-Lizenz Namensnennung - Weitergabe unter gleichen Bedingungen 2.0 Generic ([CC BY-SA 2.0 Deed](#) [26]) lizenziert.

3. Dystopische Überwachungsmaschine: Leute in der U-Bahn werden beim Chatten von großem Auge überwacht.

Scantechnologie von repressiven Regimen kann (und wird) zur Unterdrückung politisch Andersdenkender genutzt. **Foto:** Maciej Sowilski/Digitale Freiheit. **Quelle:** [Flickr](#) [27]. Die Datei ist mit der CC-Lizenz Namensnennung - Weitergabe unter gleichen Bedingungen 2.0 Generic ([CC BY-SA 2.0 Deed](#) [26]) lizenziert.

4. Patrick Breyer (* 29. April 1977) ist Bürgerrechtler und ein deutscher Jurist und Politiker der Piratenpartei Deutschland. Von 2012 bis 2017 war er Landtagsabgeordneter in Schleswig-Holstein, von 2012 bis 2013 und 2016 bis 2017 als Fraktionsvorsitzender der Piratenfraktion. Bei der Europawahl 2019 war Breyer Spitzenkandidat der Piratenpartei Deutschland und zog in das Europaparlament ein. Hochauflösende Pressefotos von Patrick Breyer zur freien Verwendung durch Medien finden sich hier >> <https://www.patrick-breyer.de/pressefotos/> [28]. Soweit nicht anders unter dem Bild angegeben, ist keine Quellangabe erforderlich. **Foto:** Copyright © Gaëlle Lewyllie, photographer from Bruges.

5. Ylva Johansson (* 13. Februar 1964 in Huddinge, Schweden) ist eine sozialdemokratische schwedische Politikerin und Kommissarin für Inneres in der Kommission von der Leyen. Johansson ist Mitglied der sozialdemokratischen Arbeiterpartei und war Schul- und Wohlfahrtsministerin unter Göran Persson sowie Arbeitsministerin in den Regierungen Löfven I und Löfven II.

In einem Interview mit dem SPIEGEL im Februar 2023 verteidigte sie die von der EU geplante Chatkontrolle. Dabei sagte sie nach dem Internetportal netzpolitik.org [drei Mal die Unwahrheit](#) [19] und verbreitete sieben Mal irreführende Aussagen. Stand Juni 2023 habe sie sich bzgl. der Chatkontrolle noch kein einziges Mal mit Vertretern der Zivilgesellschaft getroffen, aber dafür [schon unzählige Male](#) [18] mit Unternehmern und Lobbyisten, allein 2–3 Mal mit dem US-Schauspieler Ashton Kutcher in dessen Funktion als Unternehmer und Lobbyist. **Urheber:** belgium24.eu. © Belgian Presidency of the Council of the European Union / Julien Nizet. **Quelle1:** [Flickr](#) [29]. **Quelle2:** [Wikimedia Commons](#) [30]. Diese Datei ist unter der Creative-Commons-Lizenz „Namensnennung 2.0 generisch“ (US-amerikanisch) ([CC BY 2.0 Deed](#) [31]) lizenziert.

6. DIKTATUR DER SICHERHEIT. **Foto:** Sven Steinmeyer. **Quelle:** [Flickr](#) [32]. **Verbreitung** mit CC-Lizenz Namensnennung - Weitergabe unter gleichen Bedingungen 2.0 Generic ([CC BY-SA 2.0](#) [26]).

Quell-URL: <https://kritisches-netzwerk.de/forum/anlasslose-biometrische-massenkontrolle>

Links

- [1] <https://kritisches-netzwerk.de/user/login?destination=comment/reply/10838%23comment-form>
- [2] <https://kritisches-netzwerk.de/forum/anlasslose-biometrische-massenkontrolle>
- [3] <https://tkp.at/>
- [4] https://de.wikipedia.org/wiki/Birgit_Sippel
- [5] <https://reclaimthenet.org/privacy-companies-push-back-against-eu-plot-to-end-online-privacy>
- [6] <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act>
- [7] https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/Cyber-Security-Act/cyber-security-act_node.html
- [8] <https://www.patrick-breyer.de/>
- [9] <https://www.patrick-breyer.de/piraten-beantragen-ende-der-freiwilligen-chatkontrolle-durch-big-tech-unternehmen/>
- [10] https://de.wikipedia.org/wiki/Ylva_Johansson
- [11] https://www.europarl.europa.eu/doceo/document/LIBE-AM-758191_DE.pdf
- [12] https://www.europarl.europa.eu/cmsdata/280531/Vote%20results_31%20January%202024.pdf
- [13] <https://www.patrick-breyer.de/chatkontrolle-heute-im-eu-parlament-morgen-vor-gericht/>
- [14] <https://tkp.at/2023/12/22/eu-chatkontrolle-bericht-zeigt-verheerende-bilanz/>
- [15] <https://tkp.at/2023/12/12/eu-einigt-sich-auf-ki-gesetz-fuer-biometrische-masseneüberwachung/>
- [16] <https://tkp.at/2023/11/10/noch-mehr-überwachung-und-kontrolle-der-bürger-durch-eu-digitale-brieftasche-als-digitale-id/>
- [17] <https://tkp.at/2023/10/17/eu-propagandamaschine-zur-totalen-chatkontrolle/>
- [18] <https://netzpolitik.org/2023/chatkontrolle-eu-gesetzgebung-einfach-erklärt/>
- [19] <https://netzpolitik.org/2023/chatkontrolle-so-fuehrt-eu-kommissarin-ylva-johansson-die-öffentlichkeit-in-die-irre/>
- [20] <https://tkp.at/2024/01/31/die-eu-will-die-möglichkeit-zur-privaten-kommunikation-abschaffen/>
- [21] <https://www.europarl.europa.eu/committees/en/libe/home/highlights>
- [22] <https://digitalcourage.de/blog/2023/chatkontrolle-libe-beschluss>
- [23] <http://https://creativecommons.org/licenses/by/4.0/deed.de>
- [24] <https://digitalcourage.de/>
- [25] https://www.flickr.com/photos/digitale_freiheit/52560352488/
- [26] <https://creativecommons.org/licenses/by-sa/2.0/deed.de>
- [27] https://www.flickr.com/photos/digitale_freiheit/52560281958/
- [28] <https://www.patrick-breyer.de/pressefotos/>
- [29] <https://www.flickr.com/photos/199745783@N03/53484242712/>
- [30] https://commons.wikimedia.org/wiki/File:EU2024BE_240124_Launch_of_the_European_Ports_Alliance_Havenhuis_-_64.jpg
- [31] <https://creativecommons.org/licenses/by/2.0/deed.de>
- [32] <https://www.flickr.com/photos/swelt/3334646471/>
- [33] <https://kritisches-netzwerk.de/tags/act-cyber-resilience-act>

[34] <https://kritisches-netzwerk.de/tags/alltagsuberwachung>
[35] <https://kritisches-netzwerk.de/tags/anlasslose-biometrische-massenkontrolle>
[36] <https://kritisches-netzwerk.de/tags/ausspähprogramme>
[37] <https://kritisches-netzwerk.de/tags/birgit-sippel>
[38] <https://kritisches-netzwerk.de/tags/briefgeheimnis>
[39] <https://kritisches-netzwerk.de/tags/bürgerliche-freiheiten>
[40] <https://kritisches-netzwerk.de/tags/chat-control>
[41] <https://kritisches-netzwerk.de/tags/chatkontrolle-20>
[42] <https://kritisches-netzwerk.de/tags/client-side-scanning>
[43] <https://kritisches-netzwerk.de/tags/cybersecurity-act>
[44] <https://kritisches-netzwerk.de/tags/cybersicherheit>
[45] <https://kritisches-netzwerk.de/tags/digitalministerium>
[46] <https://kritisches-netzwerk.de/tags/dystopische-überwachungsmaschine>
[47] <https://kritisches-netzwerk.de/tags/ende-zu-ende-verschlüsselung>
[48] <https://kritisches-netzwerk.de/tags/hash-funktion>
[49] <https://kritisches-netzwerk.de/tags/hash-werte>
[50] <https://kritisches-netzwerk.de/tags/interpersonelle-kommunikation>
[51] <https://kritisches-netzwerk.de/tags/kommunikationsverschlüsselung>
[52] <https://kritisches-netzwerk.de/tags/libe>
[53] <https://kritisches-netzwerk.de/tags/massenscanning>
[54] <https://kritisches-netzwerk.de/tags/massenüberwachung>
[55] <https://kritisches-netzwerk.de/tags/nextcloud>
[56] <https://kritisches-netzwerk.de/tags/patrick-breyer>
[57] <https://kritisches-netzwerk.de/tags/peter-f-mayer>
[58] <https://kritisches-netzwerk.de/tags/privatsphäre>
[59] <https://kritisches-netzwerk.de/tags/privatsphäreingriff>
[60] <https://kritisches-netzwerk.de/tags/privatsphäreuntergrabung>
[61] <https://kritisches-netzwerk.de/tags/privatsphäreverletzung>
[62] <https://kritisches-netzwerk.de/tags/proton>
[63] <https://kritisches-netzwerk.de/tags/scantechnologie>
[64] <https://kritisches-netzwerk.de/tags/schnuffelstaat>
[65] <https://kritisches-netzwerk.de/tags/sicherheitsintegrität>
[66] <https://kritisches-netzwerk.de/tags/tuta-mail>
[67] <https://kritisches-netzwerk.de/tags/überwachungsdystopie>
[68] <https://kritisches-netzwerk.de/tags/überwachungsfunktion>
[69] <https://kritisches-netzwerk.de/tags/überwachungsinfrastruktur>
[70] <https://kritisches-netzwerk.de/tags/überwachungsmaßnahme>
[71] <https://kritisches-netzwerk.de/tags/überwachungspflicht>
[72] <https://kritisches-netzwerk.de/tags/überwachungsstaat>
[73] <https://kritisches-netzwerk.de/tags/überwachungsverordnung>
[74] <https://kritisches-netzwerk.de/tags/verdachtslose-automatisierte-durchsuchen-von-dateien>
[75] <https://kritisches-netzwerk.de/tags/verschlüsselung>
[76] <https://kritisches-netzwerk.de/tags/verschlüsselungsaushebelung>
[77] <https://kritisches-netzwerk.de/tags/verschlüsselungsumgehung>
[78] <https://kritisches-netzwerk.de/tags/ylva-johansson>