Foto: Pixabay / geralt, Lizenz: Pixabay License

Die Abschaffung des digitalen Briefgeheimnisses:

Nachrichten- und Chatkontrolle!

Wie ist es soweit gekommen?

Die EU will private Chats, Nachrichten und E-Mails massenhaft, anlass- und unterschiedslos auf verdächtige Inhalte durchsuchen. Die Begründung: Strafverfolgung von Kinderpornographie. Die Konsequenz: Massenüberwachung durch vollautomatisierte Echtzeit-Chatkontrolle und damit die Abschaffung des digitalen Briefgeheimnisses. Am 26. Mai 2021 hat eine Mehrheit der Abgeordneten im Ausschuss für Bürgerliche Freiheiten dem Deal zum freiwilligen Einsatz der Chatkontrolle zugestimmt [1]. Nun muss die Chatkontrolle noch durch das Parlament abgestimmt werden!

Autor: Patrick Breyer

ist digitaler Freiheitskämpfer und seit 2019 Europa-Abgeordneter der Piratenpartei. Von Beruf Jurist, war er von 2012–2017 Abgeordneter der Piratenpartei im Landtag Schleswig-Holsteins und dort zeitweise Fraktionsvorsitzender. Als Europa-Abgeordneter ist er Mitglied des Ausschusses für Bürgerliche Freiheiten, Justiz und Inneres (LIBE) und stv. Mitglied des Rechtsausschusses (JURI). Die Abgeordneten der Europäischen Piratenpartei sind Mitglieder der Fraktion Grüne/Europäische Freie Allianz. Er ist im Arbeitskreis Vorratsdatenspeicherung aktiv: **www.vorratsdatenspeicherung.de** und Autor des Blogs „Daten-Speicherung.de – minimum data, maximum privacy“: **www.daten-speicherung.de**

Die Europäische Kommission hat 2020 einen Gesetzesvorschlag vorgelegt, der es erlauben soll, alle privaten Chats, Nachrichten und E-Mails verdachtslos und flächendeckend auf verbotene Darstellungen Minderjähriger und Anbahnungsversuche (Kontaktaufnahme zu Minderjährigen) zu durchsuchen [2]. Das heißt: Facebook Messenger, Gmail & Co sollen jede Kommunikation auf verdächtiges Text- und Bildmaterial scannen. Und zwar vollautomatisiert, durch den Einsatz von sog. ‘Künstlicher Intelligenz’ – ohne, dass ein Verdacht vorliegen muss.

Meldet ein Algorithmus einen Verdachtsfall, werden alle Nachrichteninhalte und Kontaktdaten automatisch und ohne menschliche Prüfung an eine private Verteilstelle und weiter an Polizeibehörden weltweit geleitet. Die Betroffenen sollen nie davon erfahren.

Einige US-Dienste wie GMail und Outlook.com praktizieren diese automatische Nachrichten- und Chatkontrolle bereits. Verschlüsselte Nachrichten sind zurzeit noch ausgenommen. Die EU-Kommission will mit einem zweiten Gesetz aber bald alle Anbieter zum Einsatz dieser Technologie verpflichten. Dabei zeigt eine im März 2021 durchgeführte Umfrage, dass die Mehrheit der EuropäerInnen den Einsatz der Chatkontrolle entschieden ablehnt [3]. (Detaillierte Umfrageergebnisse hier: [4])

Videos zur Chatkontrolle sind in dieser Playlist hinterlegt: [5]

Künstliche Intelligenz, auch artifizielle Intelligenz, englisch artificial intelligence ist ein Teilgebiet der Informatik, das sich mit der Automatisierung intelligenten Verhaltens und dem maschinellen Lernen befasst. (Foto: Pixabay / geralt Lizenz: Pixabay License)

Was hat das Ganze mit dir zu tun?

Alle deine Chats und E-Mails werden automatisch auf verdächtige Inhalte durchsucht. Nichts ist mehr vertraulich oder geheim. Kein Gericht muss diese Durchsuchung anordnen. Sie passiert immer und automatisch.

Falls die Maschinenprüfung anschlägt, werden deine privaten Fotos und Videos von Mitarbeitern von internationalen Konzernen und Polizeibehörden angesehen. Auch intime Nacktbilder von dir werden dann von unbekannten Menschen auf der ganzen Welt gesichtet, in deren Händen sie nicht sicher sind.

Flirts und Sexting werden mitgelesen, denn Texterkennungsfilter schlagen besonders häufig auf solche intimen Chats an.

Du kannst unschuldig in den Verdacht geraten, Material von Kindesmissbrauch zu verschicken. Denn die Bilderkennungsfilter sind bekannt dafür, dass sie auch auf völlig legale Urlaubsfotos mit Kindern am Strand anschlagen. 86% aller maschinell gemeldeten Verdachtsfälle erweisen sich als unbegründet, so die Schweizer Bundespolizei. 40% aller in Deutschland eingeleiteten Ermittlungsverfahren richten sich gegen Minderjährige.

> „Die Trefferquote ist dabei sehr tief: ‚2020 trafen bei uns rund 8000 Meldungen ein', sagt Fedpol-Sprecher Florian Näf. ‚Strafrechtlich relevant waren davon zirka 14 Prozent.'" [6]

Bei deiner nächsten Auslandsreise könnten dich große Probleme erwarten. Verdachtsmeldungen werden unkontrollierbar an Staaten wie die USA, wo es keinerlei Datenschutz gibt, weitergeleitet – mit unabsehbaren Konsequenzen.

Geheimdienste und Hacker können einfacher Zugriff auf deine privaten Chats und E-Mails erhalten. Denn sobald sichere Verschlüsselung für den Einsatz der Chatkontrolle ausgehebelt wird, ist die Tür offen zum massenhaften Auslesen deiner Nachrichten durch jeden, der die technischen Mittel dazu hat.

Das ist nur der Anfang. Ist die Technologie zur Nachrichten- und Chatkontrolle einmal etabliert, kann sie spielend leicht auch für andere Zwecke eingesetzt werden. Und wer garantiert, dass die Verdächtigungsmaschinen künftig nicht auch unsere Smartphones und Laptops kontrollieren?

Weitere Argumente gegen die Chatkontrolle siehe [7]. Was du gegen die Einführung der Chatkontrolle unternehmen kannst, siehe [8].

Der Zeitplan

Die Trilog-Verhandlungen über den Gesetzentwurf, in denen Vertreter des Europäischen Parlaments mit den EU-Regierungen unter Beteiligung der EU-Kommission verhandeln, sind im Mai abgeschlossen worden [9]. Die freiwillige Chatkontrolle kommt! Hier meine Pressemitteilung zum Verhandlungsergebnis, siehe [10].

Im Sommer 2021 will die EU-Kommission einen zweiten Gesetzentwurf vorlegen, der alle Anbieter von E-Mail-, Messaging- und Chatdiensten zur flächendeckenden und verdachtslosen Durchsuchung privater Nachrichten zwingen soll. [11]

Nach einem Urteil des Europäischen Gerichtshofs ist die dauerhafte und flächendeckende automatisierte Analyse privater Kommunikation grundrechtswidrig und verboten (Abs. 177) [12]. Der Europaabgeordnete Patrick Breyer hat aus diesem Grund die US-Unternehmen Facebook und Google wegen Verletzung der Datenschutz-Grundverordnung bei den Datenschutzbehörden angezeigt.

Die ehemalige EuGH-Richterin, Prof. Dr. Ninon Colneric, hat das Verfahren der Chatkontrolle einer umfangreichen Analyse unterzogen und kommt in ihrem Rechtsgutachten (englisch [13]) zu dem Ergebnis, dass die EU-Gesetzesvorhaben zur Chatkontrolle nicht im Einklang mit der Rechtsprechung des Europäischen Gerichtshofs stehen und die Grundrechte aller EU-Bürger*innen auf Achtung der Privatsphäre, auf Datenschutz und auf freie Meinungsäußerung verletzen.

14. Januar 2021: Interne technische Verhandlungen des Europaparlaments
15. Januar 2021: Technische Verhandlungen zwischen Rat, Kommission und Parlament (Technischer Trilog)
18. Januar 2021: Schattenberichterstatter-Treffen der Verhandler des Europäischen Parlaments

Publiziert auf Free21 am 23.07.2021, 06:00 Uhr

Patrick Breyer (1977) ist Bürgerrechtler und ein deutscher Jurist und Politiker der Piratenpartei Deutschland.Bei der Europawahl 2019 war Breyer Spitzenkandidat der Piratenpartei Deutschland und zog in das Europaparlament ein. (Foto: Wikipedia, Lizenz: gemeinfrei)*

19. Januar 2021: Interne technische Verhandlungen des Europaparlaments
20. Januar 2021: Technische Verhandlungen zwischen Rat, Kommission und Parlament (Technischer Trilog)
25. Januar 2021: Schattenberichterstatter-Treffen der Verhandler des Europäischen Parlaments
01. Februar 2021: Interne technische Verhandlungen des Europaparlaments
05. Februar 2021: Interne technische Verhandlungen des Europaparlaments
22. Februar 2021: Schattenberichterstatter-Treffen der Verhandler des Europäischen Parlaments
23. Februar 2021: Zweiter Politischer Trilog zwischen Rat, Kommission und Parlament
26. Februar 2021: Interne technische Verhandlungen des Europaparlaments
01. März 2021: Schattenberichterstatter-Treffen der Verhandler des Europäischen Parlaments
02. März 2021: Interne technische Verhandlungen des Europaparlaments
08. März 2021: Schattenberichterstatter-Treffen der Verhandler des Europäischen Parlaments
09. März 2021: Dritter Politischer Trilog zwischen Rat, Kommission und Parlament
23. März 2021: Schattenberichterstatter-Treffen der Verhandler des Europäischen Parlaments
25. März 2021: Vierter Politischer Trilog zwischen Rat, Kommission und Parlament
19. April: Interne technische Verhandlungen zwischen Europaparlament, Kommission und Rat
28. April: Schattenberichterstatter-Treffen der Verhandler des Europäischen Parlaments
29. April: Fünfter Politischer Trilog zwischen Rat, Kommission und Parlament
26. Mai: Abstimmung über das Verhandlungsergebnis des Trilogs im Innenausschuss [14]

Voraussichtlich im Juli/August 2021: Abstimmung im Europaparlament#
Voraussichtlich Sommer 2021: Gesetzesvorschlag der Kommission zum verpflichtenden Einsatz der Nachrichten- und Chatkontrolle

Was du tun kannst

- Rede darüber! Erzähle anderen von den Gefahren der Chatkontrolle. Dafür kannst du hier auf Sharepics und Videos zugreifen [15]. Du kannst natürlich auch selbst Bilder und Videos erstellen.
- Schaffe Aufmerksamkeit in den Sozialen Medien! Für einen Beispieltweet kannst du rechts auf die Schaltfläche klicken. Nutze dafür die Hashtags #Chatkontrolle und #digitalesBriefgeheimnis
- Verantwortliche anschreiben! Wende dich an die zuständigen Abgeordneten im Innenausschuss des Europäischen Parlaments [16]. Dazu sind hier Beispiel-Texte auf deutsch [17] und auf englisch [18] bereitgestellt. Erfahrungsgemäß haben selbstformulierte E-Mails jedoch mehr Erfolg.
- Und wende dich an die ständigen Vertretungen der Regierungen [19] (Ansprechpartner der ständige Vertretung Deutschlands bei der EU: info@bruessel-eu.diplo.de, Tel. +32-27871000, Fax +32-27872000) oder an das Innenministerium via Email oder Telefon (Ansprechpartner: Bundesinnenminister Seehofer unter poststelle@bmi.bund.de, Bundesjustizministerin Lambrecht unter poststelle@bmjv.bund.de).
- Medienberichte anstoßen! Journalistinnen und Journalisten haben die Nachrichten- und Chatkontrolle bisher kaum aufgegriffen. Wende dich direkt an Medienunternehmen und bitte sie, darüber zu schreiben – online und offline.
- Sprich mit deinen Anbietern! Vermeide Gmail, Facebook Messenger, outlook.com und die Chatfunktion der X-Box, wo schon heute verdachtslos durchleuchtet wird. Frage deine E-Mail-, Messenger- und Chatanbieter, ob sie private Nachrichten verdachtslos nach verbotenen Inhalten durchsuchen oder dies planen.

Weiterführende Informationen und Argumente gegen die Nachrichten- und Chatkontrolle

- Alle Bürgerinnen und Bürger werden ohne Anlass unter Verdacht gestellt, Straftaten zu begehen. Die Text- und Bilderkennungsfilter werten unterschiedslos alle Nachrichten aus – un-

abhängig davon, ob ein konkreter Verdacht vorliegt oder nicht. Kein Richter muss dieser Durchsuchung zustimmen – ganz im Gegensatz zur analogen Welt, in der das Briefgeheimnis und damit die Vertraulichkeit der schriftlichen Kommunikation gewährleistet ist. Laut der Rechtsprechung des Europäischen Gerichtshofes ist eine permanente und verdachtslose automatische Auswertung privater Kommunikation grundrechtswidrig [20] (Rechtssache C-511/18, Abs. 192 [21]). Die EU will die Gesetze trotzdem verabschieden. Sie vor Gericht zu stoppen kann Jahre dauern. Deswegen müssen die Gesetze bereits jetzt verhindert werden!

- Die Vertraulichkeit privater Kommunikation wird nachhaltig zerstört. Nutzerinnen und Nutzer von Messenger-Diensten und E-Mail müssen davon ausgehen, dass alle ihre Nachrichten künftig in Echtzeit mitgelesen und ausgewertet werden. Sensible Bild- und Textinhalte können an unbekannte Personen weltweit vollautomatisiert weitergeleitet werden und in falsche Hände geraten. Es sind bereits Fälle bekannt geworden, in denen die Mitarbeiter von US-Behörden abgefangene Nacktbilder von Nutzer*innen in Umlauf gebracht haben [22]. Auch Konzernmitarbeiter haben bereits Kinderdaten missbraucht [23].
- Die Chatkontrolle zeigt Tausende zu Unrecht an. Nach Angaben der Schweizer Bundespolizei sind 90% der maschinell angezeigten Inhalte nicht strafbar, etwa Urlaubsfotos am Strand mit nackten Kindern.
- Sicher verschlüsselte Kommunikation ist in Gefahr. Denn verschlüsselte Nachrichten können bisher nicht von den Algorithmen erfasst werden. Um die Chatkontrolle für jede Online-Kommunikation zu ermöglichen, müssen Hintertüren eingebaut werden. Sobald das geschieht, kann diese Sicherheitslücke von jeder und jedem, der oder die die technischen Mittel dazu hat, ausgenutzt werden. Private Kommunikation, aber auch Geschäftsgeheimnisse und sensible Regierungsinformationen, wären Angriffen ab dann schutzlos ausgesetzt. Sichere Verschlüsselung schützt Minderheiten, LGBTQI-Personen, Demokratieaktivisten, Journalisten usw.
- Strafverfolgung wird privatisiert. Denn in Zukunft entscheiden die Algorithmen von Unternehmen wie Facebook, Google und Microsoft, welche Inhalte als verdächtig eingestuft werden und welche nicht. Dabei geht es nicht nur um Bilder, sondern auch bestimmte Wort-Kombinationen, die den Chatfiltern verdächtig erscheinen. Eine Transparenzpflicht über die Algorithmen ist nicht vorgesehen. In einem Rechtsstaat gehört die Ermittlung von Straftaten aber in die Hände unabhängiger Beamter unter gerichtlicher Aufsicht.
- Die Chatkontrolle ist ein Dammbruch. Die Technologie zum automatischen Mitlesen privater online-Kommunikation ist gefährlich. Denn sie kann spielend leicht auch für andere Zwecke entfremdet werden. In autoritären Staaten werden solche Filter zur Verfolgung und Inhaftierung unliebsamer Regierungsgegner*innen verwendet [24]. Für die Algorithmen macht es keinen Unterschied, ob nach Kindesmissbrauch, nach Urheberrechtsverstößen, Drogenmissbrauch oder unliebsamen Meinungsäußerungen gesucht wird. Ist die Technik erst einmal flächendeckend etabliert, gibt es kein Zurück.
- Die zurzeit verhandelte Übergangsverordnung ist untauglich. Anders als beabsichtigt wird sie Facebook & Co. nicht erlauben, die Massenüberwachung fortzusetzen. Zwar wird die ePrivacy-Richtlinie eingeschränkt. Die Chatkontrolle verstößt aber mangels Rechtsgrundlage und Verhältnismäßigkeit weiterhin gegen die Datenschutz-Grundverordnung (DSGVO) Eine von Patrick Breyer eingereichte Beschwerde liegt der Datenschutzaufsicht bereits vor.

Foto: Pixabay / Alexas_Fotos, Lizenz: Pixabay License

Warum die Nachrichten- und Chatkontrolle Kindern und Missbrauchsopfern besonders schadet

Die EU-Kommission argumentiert, dass die Chatkontrolle die Strafverfolgung von Kindesmissbrauch erleichtern soll. Das ist jedoch selbst unter Betroffenen von Missbrauch umstritten. Tatsächlich fügt das Vorhaben Opfern sexuellen Missbrauchs sowie Kindern und Jugendlichen im Allgemeinen am meisten Schaden zu:

1. Schutzräume werden zerstört. Gerade Betroffene sexualisierter Gewalt sind auf die Möglichkeit angewiesen, sicher und vertraulich kommunizieren zu können. Räume zum sicheren Austausch untereinander oder etwa mit Therapeut*innen und Anwält*innen helfen Betroffenen bei der Verarbeitung und dem Umgang mit ihren Erfahrungen. Diese sicheren Räume wer-

Publiziert auf Free21 am 23.07.2021, 06:00 Uhr

BUNDESRECHTSANWALTSKAMMER

Logo der Bundesrechtsanwaltskammer. (Foto: Wikipedia, Lizenz: gemeinfrei)

den ihnen nun durch die Einführung von Echtzeitüberwachung genommen. Das kann Opfer davon abhalten, Hilfe und Unterstützung zu suchen.

2. Selbst aufgenommene Nacktaufnahmen von Minderjährigen (Sexting) geraten in die Hände von Unternehmensmitarbeitern und Polizei, wo sie nicht hingehören und nicht sicher sind.
3. Jugendliche werden überproportional kriminalisiert. Laut Kriminalstatistik richteten sich in der Vergangenheit 40% aller eingeleiteten Ermittlungsverfahren wegen Kinderpornografie gegen Minderjährige.
4. Die Chatkontrollen dämmen den Austausch illegalen Materials nicht ein, sondern erschweren die Strafverfolgung von Kindesmissbrauch zusätzlich. Denn sie verdrängen kriminelle Täter in den Untergrund, wo sie kaum noch zu überwachen sind. Auch in offenen Kanälen haben die Kontrollen die Menge der weitergegebenen Darstellungen nicht eingedämmt, wie die von Jahr zu Jahr steigenden Zahlen an Verdachtsmeldungen belegen.

Dokumente zur Chatkontrolle

- Gesetzesvorschlag der EU-Kommission (10. September 2020) [25]
- Technische Lösungen zur Durchleuchtung Ende-zu-Ende-verschlüsselter Kommunikation (September 2020) [26]
- Bericht des Innenausschusses des Europäischen Parlaments (11. Dezember 2020) [27]
- Antworten der EU-Kommission auf Fragen der Parlamentsabgeordneten (28. September 2020) [28]
- Antworten der EU-Kommission auf Fragen der Parlamentsabgeordneten (27. Oktober 2020) [29]
- Gutachten des Wissenschaftlichen Dienstes des Europaparlaments (EPRS) (Englisch) (05. Februar 2021) [30]
- Geleakter Verhandlungsstand vom 05.03.2021 (Englisch) (05. März 2021) [31]
- Rechtsgutachten zur Vereinbarkeit der Chatkontrolle mit der Rechtsprechung des EuGH (Englisch) (März 2021) [32]
- Konsolidierte Fassung des Kompromisses zum Gesetzesvorschlag aus den Trilogverhandlungen (Englisch) (21. Mai 2021) [33]

Kritische Stellungnahmen und Hintergrundartikel zur Nachrichtendurchleuchtung

Jeremy Malcolm: „How the War against Child Abuse Material was lost" (19. August 2020) [34] „Wir müssen bessere Lösungen für die Menschen schaffen, die sich dazu hingezogen fühlen."

European Digital Rights (EDRi): „Is surveilling children really protecting them? Our concerns on the interim CSAM regulation" (24. September 2020) [35]

„[D]die Verordnung überträgt privaten Unternehmen die Verantwortung für eine Angelegenheit, die von öffentlichen Behörden erledigt werden sollte."
Civil Society Organisations: „Open Letter: Civil society views on defending privacy while preventing criminal acts" (27. Oktober 2020) [36]

„Wir schlagen vor, dass die Kommission nicht-technischen Maßnahmen und der schnelleren Entfernung von anstößigen Websites den Vorrang vor clientseitiger Durchsuchung von Nachrichteninhalten einräumt"

Quellen:

[1] Patrick Breyer, „Chatkontrolle: Innenausschuß stimmt Gesetz zur flächendeckenden und verdachtslosen Durchsuchung der privaten Kommunikation zu", am 27.05.2021, *<https://www.patrick-breyer.de/chatkontrolle-innenausschuss-stimmt-gesetz-zur- flaechendeckenden-und-verdachtslosen-durchsuchung-der-privaten-kommunikation-zu/>*

[2] Europäische Komission, Der Präsident, „Verordnung des europäischen Parlaments und des Rates", am 10.09.2020, *<https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52020PC0568&from=EN>*

[3] Patrick Breyer, „Umfrage: 72% der Bürger*innen gegen EU-Pläne zur automatisierten Nachrichten- und Chatkontrolle mit Strafanzeigenautomatik", am 28.04.2021, *<https://www.patrick-breyer.de/umfrage-72-der-buergerinnen-gegen-eu-plaene-zur- automatisierten-nachrichten-und-chatkontrolle-mit-strafanzeigeautomatik/>*

[4] Pirate Party, Aimilia Givropoulou, „Results Public", *<https://nextcloud.pp-eu.eu/index.php/s/5bkdRGyxnAciNBz>*

[5] Peertube of European Pirates, Patrick Breyer, „#Chatkontrolle erklärt", im Mai 2020, *<https://peertube.european-pirates.eu/videos/ watch/playlist/fc03f7e0-cbcd-4e72-8af7-5e1e9fef1196>*

[6] Antira, „Medienspiegel 14. März 2021", am 14.03.2021, *<https://antira.org/2021/03/15/medienspiegel-14-maerz-2021/>*

[7] Patrick Breyer, „Weiterführende Informationen und Arggumente gegen die Nachrichten- und Chatkontrolle", *<https://www.patrick-breyer.de/beitraege/nachrichtendurchleuchtung/#WeitereArgumenteChatkontrolle>*

[8] Patrick Breyer, „Was du tun kannst", *<https://www.patrick-breyer.de/beitraege/nachrichtendurchleuchtung/#WasTun>*

[9] Europäische Komission, Der Präsident, „Verordnung des europäischen Parlaments und des Rates", am 10.09.2020, *<https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52020PC0568&from=EN>*

[10] Patrick Breyer, „EU-Deal zur Chatkontrolle: Flächendeckende und verdachtslose Durchsuchung von Privatnachrichten wird Gesetz", am 29.04.2021, *<https://www.patrick-breyer.de/eu-deal-zur-chatkontrolle-flaechendeckende-und-verdachtslose-durchsuchung-von- privatnachrichten-wird-gesetz/>*

[11] Europäische Komission, Der Präsident, „Verordnung des europäischen Parlaments und des Rates", am 10.09.2020, *<https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52020PC0568&from=EN>*

[12] InfoCuria, „Judgment of the Court", am 06.10.2020, *<http://curia.europa.eu/juris/document/document.jsf?text=&docid= 232084&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1>*

[13] Patrick Breyer, „Legal opinion", im März 2020, *<https://www.patrick-breyer.de/wp-content/uploads/2021/03/Legal-Opinion- Screening-for-child-pornography-2021-03-04.pdf>*

[14] Council of the European Union, „Regulation (EU) 2021/... of the European Parliament and of the Council", am 21.05.2021, *<https://www.patrick-breyer.de/wp-content/uploads/2021/05/202105_Chatcontrol_Trilogue_Agreement.pdf>*

[15] Pirate Party, Aimilia Givropoulou,"Mediapool Public", *<https://nextcloud.pp-eu.eu/index.php/s/qLreyoZRE3B9W3T>*

[16] Patrick Breyer, „LIBE Members", *<https://www.patrick-breyer.de/wp-content/uploads/2021/05/LIBE_Members.xlsx>*

[17] Pirate Party, Aimilia Givropoulou, „MdEP E-Mail Deutsch", *<https://nextcloud.pp-eu.eu/index.php/s/WLaYgxi85jdBT5Z>*

Quellen:

[18] Pirate Party, Aimilia Givropoulou, „MdEP E-Mail English“, <*https://nextcloud.pp-eu.eu/index.php/s/o6aRFH8y5e4sXrN*>

[19] Amt für Veröffentlichungen der Europäischen Union, „EU Whoiswho“, <*https://op.europa.eu/de/web/who-is-who/organization/ -/organization/REPRES_PERM/REPRES_PERM*>

[20] Patrick Breyer, „Legal Opinion Screening for child Pornography-“, am 04.03.2021, <*https://www.patrick-breyer.de/wp-content/ uploads/2021/03/Legal-Opinion-Screening-for-child-pornography-2021-03-04_incl_Logos.pdf*>

[21] De Jure, „ Generalanwalt beim EuGH“, am 15.01.2020, <*https://dejure.org/dienste/vernetzung/rechtsprechung?Text=C-511/18*>

[22] The New York Times, Michael S. Schmidt, „Racy Photos Were Often Shared at N.S.A., Snowden Says“, am 20.07.2014, <*https://www.nytimes.com/2014/07/21/us/politics/edward-snowden-at-nsa-sexually-explicit-photos-often-shared.html?_r=0*>

[23] Gawker, Adrian Chen, „GCreep: Google Engineer Stalked Teens, Spied on Chats (Updated)“, am 14.09.2010. <*https://gawker.com/ 5637234/gcreep-google-engineer-stalked-teens-spied-on-chats*>

[24] The Citizen Lab, Jeffrey Knockel und Ruohan Xiong, „(Can't) Picture This 2“, am 15.07.2019, <*https://citizenlab.ca/2019/07/cant- picture-this-2-an-analysis-of-wechats-realtime-image-filtering-in-chats/*>

[25] Europäische Komission, Der Präsident, „Verordnung des europäischen Parlaments und des Rates“, am 10.09.2020, <*https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52020PC0568&from=EN*>

[26] Politico, Europäische Komission, „Technical Solutions to detect child sexual abuse in end-to-end encrypted communications“, <*https://www.politico.eu/wp-content/uploads/2020/09/SKM_C45820090717470-1_new.pdf*>

[27] Europäisches Parlament, Birgit Sippel, „Plenarsitzungsdokument A9-0258/2020“, am 11.12.2020, <*https://www.europarl.europa.eu/doceo/document/A-9-2020-0258_DE.pdf*>

[28] European Parliament, Birgit Sippel, „Questions for written answer to the Commission by the EP rapporteur Birgit Sippel, S&D, and her shadows“, am 28.09.2020, <*https://www.euractiv.com/wp-content/uploads/sites/2/2021/01/EP-questions-9-October-final.pdf*>

[29] European Parliament, Birgit Sippel, „Questions for written answer to the Commission by the EP rapporteur Birgit Sippel, S&D, and her shadows“,am 28.09.2020, <*https://www.euractiv.com/wp-content/uploads/sites/2/2021/01/EP-questions-9-October-final.pdf*>

[30] European Parliament, „Commission proposal on the temporary derogation from the e-Privacy Directive for the purpose of fighting online child sexual abuse“, im Februar 2021, <*https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662598/EPRS_STU(2021)662598_EN.pdf*>

[31] European Parliament, „Reggulation of the European Parliament and of the Council“, am 05.03.2021, <*http://bit.ly/200258EC*>

[32] The Greens/EFA Group, Patrick Breyer, „Legal opinion“, im März 2021, <*https://www.patrick-breyer.de/wp-content/uploads/2021/03/Legal-Opinion-Screening-for-child-pornography-2021-03-04.pdf*>

[33] Patrick Breyer, <*https://www.patrick-breyer.de/wp-content/uploads ainst-child-abuse-material-was-lost/*>

[35] EDRi, „Is surveilling children really protecting them? Our concerns on the interim CSAM regulation“, am 24.09.2020, <*https://edri.org/our-work/is-surveilling-children-really-protecting-them-our-concerns-on-the-interim-csam-regulation/*>

Europäischer Datenschutzbeauftragter: „Opinion on the proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online” (10. November 2020) [37]

„Die in dem Vorschlag vorgesehenen Maßnahmen würden einen Eingriff in die Grundrechte auf Achtung des Privatlebens und den Datenschutz aller Nutzer sehr beliebter elektronischer Kommunikationsdienste, wie Instant-Messaging-Plattformen und -Anwendungen, darstellen. Die Vertraulichkeit der Kommunikation ist ein Eckpfeiler der Grundrechte auf Achtung des Privat- und Familienlebens. Selbst freiwillige Maßnahmen privater Unternehmen stellen einen Eingriff in diese Rechte dar, wenn die Maßnahmen die Überwachung und Analyse des Inhalts der Kommunikation und die Verarbeitung personenbezogener Daten beinhalten.”

Alexander Hanff (Victim of Child Abuse and Privacy Activist): „Why I don't support privacy invasive measures to tackle child abuse.” (11. November 2020) [38]

„Als Missbrauchsüberlebender bin ich (und Millionen anderer Überlebender auf der ganzen Welt) auf vertrauliche Kommunikation angewiesen, um Unterstützung zu finden und die Verbrechen gegen uns zu melden – unsere Rechte auf Privatsphäre und Vertraulichkeit zu beschneiden, bedeutet, uns weiteren Verletzungen auszusetzen, und offen gesagt, haben wir genug gelitten. […] es spielt keine Rolle, welche Schritte wir unternehmen, um Täter zu finden, es spielt keine Rolle, wie viele Freiheiten oder verfassungsmäßige Rechte wir zerstören, um diese Agenda zu erfüllen – es wird Kinder NICHT vor Missbrauch schützen, es wird den Missbrauch einfach weiter in den Untergrund treiben, es immer schwieriger machen, ihn zu entdecken und letztendlich dazu führen, dass mehr Kinder als Endergebnis missbraucht werden.”

AccessNow: „The fundamental rights concerns at the heart of new EU online content rules” (19. November 2020) [39]

„In der Praxis bedeutet dies, dass private Unternehmen mit einer Angelegenheit betraut würden, die eigentlich von öffentlichen Behörden behandelt werden sollte”

Bundesrechtsanwaltskammer: „Stellungnahme zur Übergangsverordnung gegen Kindesmissbrauch im Internet” (24. November 2020) [40]

„Sowohl hinsichtlich des Mandatsgeheimnisses als auch im Hinblick auf [die Rechte der Anwälte] erscheinen die mit den Vorschlägen der Kommission für Anwältinnen und Anwälte und […] für deren Mandantschaft einhergehenden Risiken besonders hoch. Denn die Bewertung von mit Kindesmissbrauch in Zusammenhang stehenden Sachverhalten gehört zum Aufgabenbereich der Anwaltschaft. Dementsprechend häufig wird die zwischen Anwälten und Mandanten ausgetauschten Kommunikation entsprechende Schlagwörter beinhalten. […] Nach den Vorschlägen der Kommission [steht] zu befürchten, dass es in allen genannten Konstellationen aufgrund der unvermeidbaren Verwendung einschlägiger Begrifflichkeiten regelmäßig zu einem Bruch der Vertraulichkeit kommen wird. Ein solches Ergebnis wäre aus Gründen der Rechtsstaatlichkeit sowie zum Schutze der Rechte von Mandanten und Rechtsanwälten schlechterdings inakzeptabel. Die Vertraulichkeit der Kommunikation zwischen Anwälten und Mandanten muss in jedem Fall gewährleistet bleiben. Sie ist nicht verhandelbar.“

Alexander Hanff (Victim of Child Abuse and Privacy Activist): „EU Parliament are about to pass a derogation which will result in the total surveillance of over 500M Europeans” (4. Dezember 2020) [41]

„Ich hatte keine vertraulichen Kommunikationsmittel, als ich vergewaltigt wurde; meine gesamte Kommunikation wurde von meinen Tätern überwacht – es gab nichts, was ich tun konnte, es gab kein Vertrauen. […] Ich kann nicht umhin, mich zu fragen, wie viel anders mein Leben verlaufen wäre, wenn ich Zugang zu diesen modernen Technologien gehabt hätte. [Die geplante Abstimmung über die e-Privacy-Ausnahmeregelung] wird Missbrauch in den Untergrund treiben, was es viel schwieriger macht, ihn zu entdecken; es wird Selbsthilfegruppen da-

ran hindern, Missbrauchsopfern zu helfen – ES WIRD LEBEN ZERSTÖREN."

Bundesdatenschutzbeauftragter: „BfDI kritisiert versäumte Umsetzung von EU Richtlinie" (17. Dezember 2020) [42]

„Eine flächendeckende und anlasslose Überwachung von digitalen Kommunikationskanälen ist weder zielführend noch erforderlich, um Online-Kindesmissbrauch aufzuspüren. Die Bekämpfung von sexualisierter Gewalt an Kindern muss mit zielgerichteten und konkreteren Maßnahmen angegangen werden. Die Ermittlungsarbeit ist Aufgabe der Strafverfolgungsbehörden und darf nicht auf private Betreiber von Messenger-Diensten ausgelagert werden."

European Digital Rights (EDRi): Wiretapping children's private communications: Four sets of fundamental rights problems for children (and everyone else) (Englisch) (10. Februar 2021) [43]

„Wie bei anderen Arten des Scannens von Inhalten (ob auf Plattformen wie YouTube oder in der privaten Kommunikation) schafft das ständige Scannen von allem und jedem ein enormes Risiko, zu einer Massenüberwachung zu führen, indem es den Test der Notwendigkeit und Verhältnismäßigkeit nicht besteht. Darüber hinaus entsteht ein Dammbruch, bei dem wir mit dem Scannen für weniger schädliche Fälle (Urheberrecht) beginnen und dann zu härteren Themen übergehen (sexueller Kindesmissbrauch, Terrorismus) und bevor wir wissen, was passiert ist, wird das ständige Scannen von allem zum neuen Normalzustand."

Deutscher Anwaltsverein (DAV): „Anlassloses Inhalte-Scannen ist unverhältnismäßig" (8. März 2021) [44]

„Der DAV spricht sich ausdrücklich dafür aus, die Vorbereitung und Begehung von sexuellem Kindesmissbrauch und deren Verbreitung über das Internet durch wirksame Maßnahmen auf europäischer Ebene zu bekämpfen. Die von der Kommission vorgeschlagene Übergangs-VO würde jedoch eklatant unverhältnismäßige Eingriffe in die Freiheitsgrundrechte von redlichen Nutzern internet-basierter Kommunikationsdienste ermöglichen. Darüber hinaus lässt der Verordnungsvorschlag hinreichende prozessuale Absicherungen für Betroffene vermissen. Das Gesetzesvorhaben ist daher insgesamt abzulehnen." Schreiben der Präsidentin des Deutschen Anwaltvereins (DAV) und des Präsidents der Bundesrechtsanwaltskammer (BRAK) (8. März 2021) [45]

„Positive Treffer mit nachfolgender Offenbarung gegenüber staatlichen und nichtstaatlichen Stellen würden neben Beschuldigten vor allem die Opfer sexuellen Kindesmissbrauchs zu befürchten haben. Dabei ist die absolute Vertraulichkeit der anwaltlichen Beratung gerade in diesen häufig mit Scham behafteten Sachverhalten im Interesse der Opfer unabdingbar. Die Entscheidungshoheit darüber, welche Mandatsinhalte gegenüber wem offenbart werden dürfen, muss gerade in diesen Fällen bei der Mandantschaft verbleiben. Es stünde sonst zu befürchten, dass Opfer sexuellen Kindesmissbrauchs keine anwaltliche Beratung in Anspruch nehmen."

Strategische Autonomie in Gefahr: Europäische Tech-Unternehmen warnen vor einer Absenkung des Datenschutzniveaus in der EU (Englisch) (15. April 2021) [46]

„Im Zuge der Initiative ‚Fighting child sexual abuse: detection, removal, and reporting of illegal content' plant die Europäische Union die Abschaffung des digitalen Briefgeheimnisses. Um illegale Inhalte automatisch zu erkennen, sollen künftig alle privaten Chat-Nachrichten durchleuchtet werden. Dies soll auch für Inhalte gelten, die bisher mit einer starken Ende-zu-Ende-Verschlüsselung geschützt sind. Sollte diese Initiative nach dem jetzigen Plan umgesetzt werden, würde sie unseren europäischen Idealen und den unbestreitbaren Grundlagen unserer Demokratie, nämlich der Meinungsfreiheit und dem Schutz der Privatsphäre, enorm schaden […]. Die Initiative würde auch der strategischen Autonomie Europas und damit den in der EU ansässigen Unternehmen schwer schaden."

Quellen:

[36] EDRi, „Open Letter: Civil society views on defending privacy while preventing criminal acts", am 27.10.2020, *<https://edri.org/wp-content/uploads/2020/10/20201020-EDRi-Open-letter-CSAM-and-encryption-FINAL.pdf>*

[37] European Data Protection Supervisor, „Opinion on the proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online", am 10.11.2020, *<https://edps.europa.eu/data-protection/our-work/publications/opinions/ opinion-proposal-temporary-derogations-directive_en>*

[38] LinkedIn, Alexander Hanff, „Why I don't support privacy invasive measures to tackle child abuse.", am 11.11.2020, *<https://www.linkedin.com/pulse/why-i-dont-support-privacy-invasive-measures-tackle-child-hanff>*

[39] Euroaktiv, Eliš ka Pírková, „The fundamental rights concerns at the heart of new EU online content rules", am 19.11.2020, *<https://www.euractiv.com/section/digital/opinion/the-fundamental-rights-concerns-at-the-heart-of-new-eu-online-content-rules/>*

[40] Bundesrechtsanwaltskammer, „Mitteilung der Kommission zu ihrer Strategie für einen effektiveren Kampf gegen sexuellen Kindesmissbrauch und zur Übergangsverordnung gegen Kindesmissbrauch im Internet", im November 2020, *<https://www.patrick-breyer.de/wp-content/uploads/2021/01/202011_Stellungnahme_BRAK_ePrivacy_Derogation.pdf>*

[41] LinkedIn, Alexander Hanff, „EU Parliament are about to pass a derogation which will result in the total surveillance of over 500M Europeans", am 04.12.2020, *<https://www.linkedin.com/pulse/eu-parliament-pass-derogation-which-result-total-over-alexander-hanff/?published=t>*

[42] BfDI, „BfDI kritisiert versäumte Umsetzung von EU Richtlinie", am 17.12.2020, *<https://www.bfdi.bund.de/DE/Infothek/ Pressemitteilungen/2020/30_Umsetzung-EU-Richtlinie.html>*

[43] EDRi, „Wiretapping children's private communications: Four sets of fundamental rights problems for children (and everyone else)", am 10.02.2021, *<https://edri.org/our-work/children-private-communications-csam-fundamental-rights-issues/>*

[44] Deutscher Anwalt Verein, „SN 25/21: Anlassloses Inhalte-Scannen ist unverhältnismäßig", am 09-03.2021, *<https://anwaltverein.de/ de/newsroom/sn-25-21-anlassloses-inhalte-scannen-ist-unverh%C3%A4ltnism%C3%A4%C3%9Fig>*

[45] Bundesrechtsanwaltskammer, „Trilog-Verhandlungen zum Vorschlag einer Übergangsverordnung zur Bekämpfung sexuellen **Kindesmissbrauchs** im Internet", am 08.03.2021, *<https://www.patrick-breyer.de/wp-content/uploads/2021/03/Praesidentenschreiben -BRAK-DAV_Trilog-Uebergangs-VO.pdf>*

[46] Tutanota, Arne, „Strategic autonomy in danger: European Tech companies warn of lowering data protection levels in the EU.", am 15.04.2021, *<https://tutanota.com/blog/posts/european-autonomy-in-danger/>*

Dieser Text wurde zuerst am TT.MM.JJJJ auf www.patrick-breyer.de unter der URL ‹https://www.patrick-breyer.de/beitraege/nachrichtendurchleuchtung/› veröffentlicht.
Lizenz: Patrick Breyer, CC BY-NC-ND 4.0