Chatkontrolle - An der digitalen Hundeleine

Dawid Snowden · Veröffentlicht: 10.07.2026

Eine Streitschrift über den 9. Juli 2026 und die Infrastruktur, die uns überleben wird

Stand: 10. Juli 2026

Dawid Snowden

> **Zur Einordnung:** Dieser Text ist eine Streitschrift. Er führt bewusst und mit voller Härte die Argumente gegen die Chatkontrolle, er ist kein neutraler Lagebericht. Die Fakten, Zahlen und Paragraphen sind belegt und nachprüfbar (siehe Quellen).

Zwei Dinge vorweg, damit niemand aneinander vorbeiredet: Es gibt zwei Chatkontrollen, und man muss sie auseinanderhalten, sonst wird man entweder in Panik oder in falsche Sicherheit geredet.

Chatkontrolle 1.0 ist die freiwillige Variante. Sie erlaubt Konzernen wie Meta, Google oder Microsoft, die Kommunikation ihrer Nutzer freiwillig nach Missbrauchsmaterial zu durchsuchen. Sie ist eine befristete Ausnahme vom europäischen Vertraulichkeitsgebot. Genau diese Variante wurde am 9. Juli 2026 im EU-Parlament durchgewinkt, verlängert bis 2028. Sie betrifft nach aktuellem Stand unverschlüsselte Inhalte; die Ende-zu-Ende-verschlüsselte Kommunikation wurde per Änderungsantrag ausdrücklich ausgenommen.

Chatkontrolle 2.0 ist die verpflichtende Variante, die dauerhafte CSA-Verordnung, über die parallel im sogenannten Trilog verhandelt wird. Sie könnte Anbieter zwingen, auch verschlüsselte Kommunikation direkt auf dem Gerät zu durchleuchten. Sie ist noch nicht beschlossen. Sie ist die eigentliche Bestie. Und sie ist noch nicht tot.

Einleitung: Der Strick und der Hund

Stell dir einen Menschen vor, dem man einen Strick um den Hals gelegt hat. Noch ist er nicht fest gezurrt, sondern locker genug, dass der Mensch atmen, reden und leben kann. Doch jedes Mal, wenn er das Falsche sagt, zieht eine unsichtbare Hand ihn ein Stück weiter zu, Wort für Wort, Zentimeter für Zentimeter. Nach einer Weile merkt der Mensch, dass er sich freier fühlt, wenn er schweigt, und so beginnt er zu schweigen. Er hat sich angepasst.

Oder stell dir einen Hofhund vor mit einem GPS-Halsband. Er darf über den Hof laufen, so weit er will, bis zu einer unsichtbaren Linie. Überschreitet er sie, kassiert er einen Stromschlag. Nach ein paar Tagen läuft der Hund nicht mehr an die Linie heran. Er läuft nicht einmal mehr in ihre Nähe. Man muss den Zaun gar nicht mehr elektrisch halten. Der Hund trägt den Zaun jetzt im Kopf.

Das ist keine Metapher über Hunde. Das ist die Blaupause der Chatkontrolle.

Immer dann, wenn die Herrschenden merken, dass die Bevölkerung langsam aufhört mitzuspielen, muss die Machtstruktur alles Erdenkliche im Vorfeld vorbereiten, um die breite Masse später durch Kontrolle, oder notfalls durch Gewalt, bei der Stange zu halten. Aus genau diesem Vorbereitungsdrang sind historisch die Geheimdienste entstanden: Sie dienten den Herrschenden, beschnüffelten die Bevölkerung und erstickten jeden Umsturz im Keim. Geheimdienste sind die Grundsäule jeder Herrschaft, gefolgt vom Gewaltmonopol aus Polizei und Militär, betrieben mit einem Betriebssystem aus Ideologie, Unterwerfung und falsch verstandener Loyalität.

Wir befinden uns gerade in einem transformativen Prozess. Der Sklave 1.0 soll auf Sklave 2.0 upgedatet werden. Der Sklave 1.0 musste noch von echten Menschen abgehört werden, personalintensiv, teuer und lückenhaft. Der Sklave 2.0 kann effizienter und vollständiger nicht nur überwacht, sondern gesteuert werden. Echtzeit-Algorithmen künstlicher Intelligenz stellen jedem Herrscher die Fähigkeit bereit, im Bruchteil einer Sekunde eine Sanktion zuzustellen, egal ob es die Transaktion ist, die die Selbstbedienungskasse verweigert, das E-Gate, das einen nicht mehr in den Supermarkt lässt, oder das EES-System an der Grenze, das dem Sklaven 2.0 das Verlassen der eigenen 15-Minuten-Zone verwehrt.

Die Überwachung ist keine neue Geschichte. Sie ist so alt wie die Menschheit. Neu ist nur die Skalierung. Früher schnitt ein Beamter ein Telefonat mit. Heute laufen die Sprachnachrichten von WhatsApp, Telegram und Signal durch Voice-to-Text-Modelle, werden in Text verwandelt, und ein Algorithmus liest in Echtzeit mit, Millionen Nachrichten gleichzeitig. Gibt es Menschen, die sich über einen Messenger für eine Demonstration organisieren wollen? Der Stream wird abgefangen, ausgewertet, gemeldet, und die Einsatztruppe der Polizei ist unterwegs, bevor der erste Mensch das Haus verlässt. So arbeiten autoritäre Strukturen, die kein Interesse daran haben, dass der Mensch je frei wird, sondern dass er eine verwertbare Ressource bleibt.

Und hier kommen wir zur Chatkontrolle. Sie ist die Basis dieser Infrastruktur. Sie verletzt die tiefsten freiheitlichen Grundwerte und treibt die Menschen in die Perspektive der ständigen Kontrolle, in die Angst, das Verkehrte zu denken, das Verkehrte zu sagen, das Verkehrte mit den eigenen Liebsten auszutauschen. Am Ende steht die Kriminalisierung der freien Gedanken.

Das sollte uns Sorgenfalten bereiten. Das sollte uns wachrütteln. Deswegen, in klarer Sprache, die ganze Sache in chronologischer Reihenfolge.

I. Was am 9. Juli 2026 geschah

Es war ein Donnerstag. Der letzte Plenardonnerstag vor der Sommerpause, der Tag, an dem in Straßburg die Bänke sich schon halb geleert haben, weil viele Abgeordnete längst im Urlaub sind, die Koffer in den Büros stehen und die Gedanken bei der Fußball-WM liegen oder bei der Frage, wie man das Steuergeld, das man den Bürgern im Verlauf des Jahres abgenommen hat, nun am schönsten auf den Kopf haut.

In diesen halbleeren Saal hinein wurde ein Gesetz gestimmt, das dasselbe Parlament zuvor zweimal abgelehnt hatte.

Wir kennen dieses Muster. Was passiert, wenn man abstimmt und nicht das gewünschte Ergebnis herauskommt? Man stimmt so oft ab, bis es passt. Man wartet, bis die richtigen Abgeordneten nicht mehr im Saal sind. Man nimmt sich großzügig Zeit, den einen oder anderen umzustimmen. Ein netter Vorschlag eines Kollegen hier, ein günstiger Termin dort, und schon geht die Rechnung auf.

Man muss sich das vorstellen wie eine Klassenabstimmung darüber, ob es Hausaufgaben gibt. Die Klasse stimmt zweimal mit klarer Mehrheit dagegen. Der Lehrer verlegt die dritte Abstimmung auf den letzten Schultag vor den Ferien, in die letzte Stunde, wenn die halbe Klasse schon auf dem Weg zum Bus ist, und zählt dann die leeren Stühle als Ja-Stimmen. Und weil nicht genug Kinder anwesend sind, um ausdrücklich Nein zu rufen, gibt es Hausaufgaben. Für alle. Bis 2028.

Die Zahlen, offiziell, aus der Pressemitteilung des Parlaments selbst:

1. Erste Abstimmung: 314 Ja, 276 Nein, 17 Enthaltungen, für die Ablehnung des Ratsstandpunkts.
2. Erforderlich für die Ablehnung: 360 Stimmen. Absolute Mehrheit. Zweite Lesung.

3. Ergebnis: Der Standpunkt des Rates fiel nicht. Er ging durch.
4. Zweite Abstimmung (über den geänderten Standpunkt): 276 Ja, 286 Nein, 30 Enthaltungen. Zweite Lesung abgeschlossen. [1]

Lies das noch einmal.

Eine Mehrheit der anwesenden Abgeordneten stimmte gegen die Chatkontrolle. Und die Chatkontrolle kam trotzdem.

Das ist, als würde ein Gericht einen Angeklagten mit sieben zu fünf Stimmen für unschuldig erklären, und ihn trotzdem einsperren, weil für den Freispruch nicht sieben, sondern neun Stimmen nötig gewesen wären und die beiden fehlenden Geschworenen gerade in der Mittagspause waren. Wer nicht da ist, hat zugestimmt. Wer krank ist, hat zugestimmt. Wer im Urlaub ist, hat zugestimmt.

Das ist keine Verschwörungstheorie. Das ist Artikel 294 AEUV, das ordentliche Gesetzgebungsverfahren, zweite Lesung. In dieser Phase kehrt sich die Beweislast um.

Was das bedeutet, muss man einmal in aller Ruhe sagen, weil es der eigentliche Trick ist. Normalerweise gilt: Wer etwas durchsetzen will, muss eine Mehrheit organisieren. In der zweiten Lesung gilt das Gegenteil: Wer etwas verhindern will, muss die Mehrheit organisieren, und zwar nicht irgendeine, sondern die absolute: 360 Stimmen, gerechnet auf alle Abgeordneten, nicht nur auf die anwesenden. Jeder leere Stuhl zählt faktisch für den Vorschlag.

Man stelle sich vor, ein Fußballspiel wird nach folgender Regel gepfiffen: Die Heimmannschaft (die Befürworter) gewinnt automatisch, es sei denn, die Gäste (die Gegner) schießen mindestens sechs Tore. Und dann sorgt man dafür, dass die Hälfte der Gästemannschaft gar nicht erst zum Anpfiff erscheint, weil man das Spiel überraschend auf einen Tag legt, an dem alle schon in den Ferien sind. Das ist kein Fußball. Das ist eine Inszenierung mit vorher feststehendem Ergebnis.

Man muss ein Gesetz nicht gewinnen. Man muss nur dafür sorgen, dass die anderen es nicht rechtzeitig verlieren können. Oder man schickt sie einfach in den Urlaub. Damit das Ergebnis stimmt.

II. Die Anatomie eines Verfahrenstricks

Rekonstruieren wir die Choreographie Schritt für Schritt. Sie ist lehrreich, nicht wegen der Chatkontrolle, sondern wegen dessen, was sie über das Verfahren selbst verrät.

26. März 2026: Das Parlament sagt Nein. Das Europäische Parlament lehnt die Verlängerung der Ausnahmeregelung ab. Was ist diese Ausnahmeregelung? Kurz gesagt: In Europa ist das Durchleuchten privater Kommunikation grundsätzlich verboten. Damit die Konzerne trotzdem freiwillig scannen dürfen, brauchen sie eine Sondererlaubnis, eine Ausnahme vom Verbot. Genau diese Ausnahme sollte verlängert werden. Das Parlament sagte: Nein. Erste Lesung abgeschlossen. [1]

3./4. April 2026: Das selbstgemachte Vakuum. Die Verordnung (EU) 2021/1232 läuft aus. Das ist die befristete Ausnahme vom Vertraulichkeitsgebot der ePrivacy-Richtlinie. Diese Richtlinie (2002/58/EG) ist das europäische Gesetz, das die Vertraulichkeit elektronischer Kommunikation schützt, sie ist der digitale Nachfahre des Briefgeheimnisses. Die Ausnahme von 2021 durchlöcherte diesen Schutz „vorübergehend", damit Konzerne scannen durften. Nun läuft sie aus, und plötzlich herrscht ein „Rechtsvakuum". Man muss sich klarmachen: Es ist ein Vakuum, das der Gesetzgeber selbst geschaffen hat, indem er eine Regelung, die laut eigener Beschreibung „streng befristet und außergewöhnlich" sein sollte, jahrelang immer weiter verlängerte. Man legt selbst Feuer und ruft dann nach der Feuerwehr. Man erzeugt selbst die Notlage, mit der man später die Notmaßnahme begründet. [7]

Ende Juni 2026: Die Auferstehung. Roberta Metsola holt den totgeglaubten Vorschlag zurück auf die Tagesordnung. Wer ist Metsola? Sie ist die Präsidentin des Europäischen Parlaments, eine maltesische Politikerin, Mitglied der EVP. Die EVP, Europäische Volkspartei, ist die größte Fraktion im EU-Parlament, die Familie der christdemokratischen und konservativen Parteien; CDU und CSU gehören dazu. Metsola nutzt ihre Position an der Spitze des Parlaments, um das Thema wieder aufzurufen. Gleichzeitig wird der Rat bewegt, seinen Standpunkt erneut ans Parlament zu senden. Mit „Rat" ist hier der Rat der Europäischen Union gemeint, das Gremium, in dem die Regierungen der Mitgliedstaaten sitzen. Nicht irgendein Rat aus Mittelerde, sondern die versammelten nationalen Regierungen, die im EU-Gesetzgebungsverfahren die zweite Kammer bilden. [2]

7. Juli 2026: Das Eilverfahren. Die EVP-Fraktion beantragt ein Dringlichkeitsverfahren, um noch vor der Sommerpause abstimmen zu können. Mit 331 zu 304 Stimmen, abgegeben im Plenum des EU-Parlaments in Straßburg, wird der Weg für die Neuabstimmung frei. [3] Der Sinn des Eilverfahrens ist durchsichtig: Es soll schnell gehen, bevor die Gegner sich formieren und bevor der volle Saal zusammenkommt.

9. Juli 2026: Der Beschluss. Die Abstimmung fand im Plenarsaal des Europäischen Parlaments in Straßburg statt, eingeleitet von der Parlamentsführung um Präsidentin Metsola. Die Bänke waren halb leer, im Saal herrschte Tumult, und am Ende ging der Vorschlag durch. [1][2][4]

Und jetzt? Der beschlossene Text, die verlängerte, „freiwillige" Chatkontrolle 1.0, geht zurück an den Rat der EU. Der muss binnen drei Monaten die Änderungen des Parlaments billigen oder ablehnen. Lehnt er ab, kommt der Vermittlungsausschuss. Das ist ein paritätisch besetztes Gremium aus Vertretern von Parlament und Rat, das bei Uneinigkeit einen Kompromisstext aushandeln muss, eine Art Schlichtungsstelle des EU-Gesetzgebungsverfahrens. [1] Bis dahin gilt: Die Erlaubnis zum freiwilligen Scannen soll bis 2028 laufen. [4]

Konstantin Macher von der Digitalen Gesellschaft nennt es einen „schlechten Tag für die europäische Demokratie". [2]

Ein schlechter Tag für die Demokratie? Nun ja, vielleicht ist genau das die Demokratie: eine Massenvergewaltigung, der sich kein Mensch entziehen kann. Und diese Betrachtung ist die bitterere, denn die Struktur, in der das geschieht, ist eine Struktur, die man nicht verlassen kann. Kein Mensch kann aus ihr austreten; man wird in sie hineingeboren und muss sie bis zum Lebensende akzeptieren. Das ist der Konstruktionsfehler: dass man bestehende, destruktive Systeme, die die Menschen missbrauchen, nicht abwählen und nicht stoppen kann. Und wer einmal in einer Machtposition sitzt, distanziert sich schon psychologisch von den Menschen unter ihm und handelt nicht mehr in ihrem Sinne. Solche Strukturen bilden niemals etwas ab, das dem Menschen dient. Sie bilden ab, was der Herrschaft und dem Machterhalt dient.

Wie treffend diese nüchterne Diagnose ist, zeigte sich noch am selben Tag im Plenarsaal selbst. Denn während draußen von einem schlechten Tag für die Demokratie die Rede war, brach drinnen Jubel aus. Einer, der ihn miterlebte, war Martin Sonneborn, und er hat den Vorgang trocken kommentiert. Sonneborn, wer ihn nicht kennt: ehemaliger Chefredakteur des Satiremagazins Titanic, Gründer und Frontmann der Satirepartei Die PARTEI, seit 2014 fraktionsloser Abgeordneter im Europäischen Parlament, berichtete, wie in den Reihen der EVP gejubelt wurde, als verkündet wurde, man werde „unsere Kinder schützen". Seine Antwort: „Wir sollten uns vor den Leuten schützen, die unsere Kinder schützen wollen." [4]

Beide, Macher und Sonneborn, haben recht. Aber das ist noch nicht das Schlimmste.

Das Schlimmste ist die Verkehrung des Arguments. Pädokriminelle Netzwerke reichen nicht selten tief in Regierungs- und Machtstrukturen hinein, der Epstein-Komplex hat das für alle sichtbar gemacht. Und nun stellen sich ausgerechnet jene als Beschützer der Kinder auf, die sich zuvor nie ernsthaft für Kinder eingesetzt, sondern jahrelang geschwiegen und verdrängt haben. Auf einmal fällt ihnen ein, dass sie Kinder schützen wollen, nicht durch schnellere Löschung, nicht durch Prävention, sondern durch die Durchleuchtung von 450 Millionen Unschuldigen. Das Kind wird zum rhetorischen Vehikel, zum trojanischen Pferd, in dessen Bauch die Massenüberwachung sitzt. Es ist die perfideste Taktik überhaupt: sich das Schutzbedürftigste zu greifen, um das Freiheitsraubende durchzusetzen. Denn gegen den Satz „Wir schützen Kinder" kann öffentlich niemand sein, und genau deshalb ist er das ideale trojanische Pferd.

III. Der Rechtsbruch, den alle kennen und niemand aufhält

Was da eigentlich außer Kraft gesetzt wird

Artikel 5 Absatz 1 der Richtlinie 2002/58/EG (ePrivacy) verpflichtet die Mitgliedstaaten, die Vertraulichkeit der Kommunikation sicherzustellen und „das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens" von Nachrichten durch andere als die Nutzer zu untersagen, ohne Einwilligung der Betroffenen.

Das ist die Norm. Die Chatkontrolle ist die Ausnahme von der Norm.

Nun muss man ehrlich sein: Auch schon vor der Chatkontrolle gab es Wege, in die Telekommunikation einzugreifen. Über Gerichtsbeschlüsse, im Rahmen von Ermittlungsverfahren, unter dem Deckmantel der Terrorbekämpfung haben sich Behörden und Verwaltungen immer schon Freiräume geschaffen, um Telefonate abzuhören oder Nachrichten mitzuschneiden. Der Unterschied, und er ist entscheidend, ist der zwischen dem gezielten Eingriff mit richterlicher Kontrolle bei konkretem Verdacht und der anlasslosen Durchleuchtung aller. Das eine ist Strafverfolgung. Das andere ist Generalverdacht. Und man darf sich an dieser Stelle durchaus fragen, was schlimmer ist: wenn Konzerne auf unsere Daten zugreifen oder wenn Regierungen es tun. Die ehrliche Antwort lautet: Keinem von beiden sollte man zu viel Vertrauen schenken. Bei der Chatkontrolle arbeiten sie zusammen.

Die Ausnahme war 2021 als dreijähriges Provisorium gedacht, als frühe Form der Chatkontrolle 1.0. Wir sind im fünften Jahr. Sie soll bis 2028 laufen. Das Provisorium ist zum Normalzustand geworden: der Lehrbuchfall der Normalisierung.

Schon Edward Snowden hat es auf den Punkt gebracht: Einmal installierte Systeme bleiben. Jede Überwachungsinfrastruktur, die man über die Menschen errichtet, wird zum festen Bestandteil der Gesellschaft. Sie wird nicht mehr abgebaut. Sie wird bestenfalls „reformiert", und meist nur erweitert. Deswegen muss alles daran gesetzt werden, dass solche Strukturen gar nicht erst Bestand gewinnen und niemals ihr volles Potenzial entfalten. Denn der beste Zeitpunkt, ein Überwachungssystem zu stoppen, ist der Tag vor seinem Bau.

Was die Grundrechtecharta sagt, und was daraus geworden ist

Auf dem Papier klingt die Charta der Grundrechte der Europäischen Union glorreich. In der Praxis mussten wir seit 2020 erleben, wie belastbar diese Versprechen wirklich sind.

Art. 7 GRCh, Achtung des Privat- und Familienlebens, der Wohnung und der Kommunikation. Klingt ehrenvoll. Doch wir haben in der Plandemie gesehen, wie tief sich der Staat in Privatleben, Familien, Wohnungen und Kommunikation eingemischt hat: Er hat Menschen verboten zu protestieren, hat Demonstranten auf offener Straße niedergeknüppelt und mit Wasserwerfern auf Bürger geschossen. Ein Artikel, der die Wohnung schützt, hilft wenig, wenn dieselbe Hand, die ihn geschrieben hat, die Tür mit einem Rammbock aufbrechen lässt, nur weil man etwas Falsches gesagt oder im Internet gepostet hat.

Art. 8 GRCh, Schutz personenbezogener Daten. Schutz, vor wem? Vor den Regierungen und Konzernen, die sich zugleich alle Schlupflöcher verschaffen, um doch mitzulesen? Schon lange vor der Chatkontrolle wurde invasiv auf Daten zugegriffen, wurden Menschen getrackt und Bewegungsprofile aufgezeichnet, etwa durch die automatische Kennzeichenerkennung, wie sie in England längst Alltag ist, wo Fahrer in Zonen erfasst und abgerechnet werden. Der Datenschutzartikel ist so stark wie der Wille derer, die ihn achten sollen.

Art. 11 GRCh, Freiheit der Meinungsäußerung und Informationsfreiheit. Auch dieses Recht wurde in den vergangenen Jahren hart auf die Probe gestellt, von der Plandemie-Debatte bis zur Berichterstattung über Gaza, bei der Menschen, die kritisch berichteten oder protestierten, mit Verfahren, Kontosperrungen oder Schlimmerem überzogen wurden. Was damals Kritiker der Plandemiepolitik traf, könnte morgen jene treffen, die sich gegen den nächsten Krieg gegen Russland oder ein anderes Land positionieren.

Art. 52 Abs. 1 S. 2 GRCh, Verhältnismäßigkeit. Einschränkungen von Grundrechten sind nur zulässig, wenn sie erforderlich sind und den Zielen tatsächlich entsprechen. [6] Die entscheidende Frage lautet: Verhältnismäßig, für wen? Zu oft dient die behauptete „Verhältnismäßigkeit" dem Schutz des Systems, nicht dem des Menschen.

Was die Juristen sagen, die es wissen müssen

Und jetzt wird es ernst. Denn es sind nicht Netzaktivisten oder der Chaos Computer Club (CCC), die hier warnen, es sind die Hausjuristen der Mitgliedstaaten selbst.

Der Juristische Dienst des EU-Rates kam in seinem Gutachten (Dok. 8787/23 vom 26. April 2023) zu einem vernichtenden Schluss: Die anlasslose Chatkontrolle verstößt gegen die Grundrechtecharta, ist unverhältnismäßig und wird vor dem Europäischen Gerichtshof scheitern. Sie treffe alle Nutzer, „ohne dass diese Personen auch nur indirekt in eine Situation geraten, die eine strafrechtliche Verfolgung nach sich ziehen könnte". [8][6]

Man lasse diesen Satz wirken. Er bedeutet: Man durchsucht die Taschen von Millionen Menschen, die nicht einmal in der Nähe eines Verdachts stehen. Es ist, als würde die Polizei jeden Morgen in jede Wohnung des Landes gehen, jede Schublade öffnen, jedes Tagebuch lesen, nicht weil ein Verdacht besteht, sondern für den Fall der Fälle. Es ist die Umkehrung des Rechtsstaats: Nicht mehr der Verdacht rechtfertigt die Durchsuchung, sondern die Durchsuchung sucht sich den Verdacht.

Der frühere EuGH-Richter Christopher Vajda attestierte in einem Rechtsgutachten einen Eingriff in Art. 7 und 8 GRCh, der über alles hinausgehe, was ihm an früherer Gesetzgebung bekannt sei. [9] Wenn ein ehemaliger Richter des höchsten europäischen Gerichts sagt, so etwas habe er noch nie gesehen, dann ist das kein juristisches Detail, sondern ein Alarmsignal.

Die Gesellschaft für Freiheitsrechte (GFF) spricht von einem „besonders schwerwiegenden Eingriff in das Recht auf Privatsphäre". [10]

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), zur Zeit dieser Stellungnahme geleitet von Prof. Dr. Louisa Specht-Riemenschneider, die das Amt bis zum 30. September 2026 führte, bevor Prof. Dr. Moritz Hennemann übernahm, urteilte, der Entwurf respektiere „weder die Vorgaben zur Verhältnismäßigkeit noch die Grundrechte", die den Bürgern nach Charta und Grundgesetz zustehen. [11]

Die Wissenschaftlichen Dienste des Deutschen Bundestages haben das Ganze systematisch durchgeprüft, an Art. 7, 8 und 11 GRCh, am Verhältnismäßigkeitsgebot des Art. 52 Abs. 1 S. 2 GRCh und am Verhältnis zum Grundgesetz. [6]

Merkst du etwas? Die Juristen des Rates, ein Ex-EuGH-Richter, die Datenschutzbehörde des Bundes, der wissenschaftliche Dienst des Parlaments, sie alle sagen dasselbe. Und die Politik verhandelt einfach weiter, bis das Projekt steht.

Und was das Grundgesetz sagt

Art. 10 Abs. 1 GG: „Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich."

Unverletzlich. Nicht: „unverletzlich, sofern kein Hash-Abgleich stattfindet." Nicht: „unverletzlich, außer bei freiwilliger Durchleuchtung durch Konzerne aus Kalifornien."

Ein unverletzliches Recht ist wie eine Wand, die per Definition keine Tür hat. Wer eine Tür einbaut, und sei es eine winzige, nur für „die Guten", hat die Wand abgerissen und durch einen Vorhang ersetzt. Und durch einen Vorhang geht jeder, der stark genug zieht.

Das Bundesverfassungsgericht hat im Beschluss vom 24. Juni 2025 (1 BvR 180/23, „Trojaner II") § 100a Abs. 1 S. 2 StPO für nichtig erklärt, soweit die Quellen-Telekommunikationsüberwachung zur Aufklärung von Straftaten mit einer Höchststrafe von drei Jahren oder weniger zugelassen war. Die Begründung: Der Eingriff sei so intensiv, dass er nur durch Schwerstkriminalität, Terror, Mord, schwere Sexualdelikte, organisierte Kriminalität, zu rechtfertigen sei. [12][13]

Nun könnte man einwenden: Immerhin eine Grenze. Doch die Grenze ist beweglich. Die Herrschenden können sich jederzeit neue Höchststrafen ausdenken, um diese Limitierung zu umgehen. Wir haben in den letzten fünfzig Jahren gesehen, wie beweglich Strafrahmen sind, wie oft neue Gesetze und Paragraphen beschlossen wurden, ohne die Völker zu fragen, ohne sie abstimmen zu lassen. Die gesamte hier beschriebene Entwicklung basiert darauf, dass die Menschen keine Möglichkeit haben, ihre eigenen Entscheidungen zu treffen, sondern vor vollendete Tatsachen gestellt werden.

Halten wir fest, und das ist der Skandal in einem Satz: Der Staat darf mit richterlichem Beschluss und bei konkretem Verdacht nicht auf das Endgerät eines Beschuldigten zugreifen, wenn die Tat nur drei Jahre Höchststrafe trägt. Aber Meta, Google und Microsoft dürfen, „freiwillig", ohne Richter, ohne Verdacht, die Kommunikation von 450 Millionen Menschen durchleuchten.

Der Rechtsstaat verlangt vom Staat Zurückhaltung und lässt Private tun, was er selbst nicht darf. Das ist keine Lücke. Das ist ein Geschäftsmodell. Wir kennen das Prinzip aus der Welt der Geheimdienste: Deutsche Nachrichtendienste zahlen ausländische Dienste dafür, im eigenen Land Daten abzugreifen, die sie selbst gar nicht erheben dürften. Die schmutzige Wäsche wird im Ausland gewaschen, weil sie zu Hause verboten ist.

Und dann ist da Palantir. Man werfe einen Blick auf die Geschäftspraktiken dieses Datenkonzerns: Bereits heute nutzen deutsche Polizeibehörden Palantir-Software, um Metadaten zusammenzuführen und Personen zu verknüpfen, teils gespeichert in Cloud-Strukturen, an denen auch ausländische Dienste andocken können.

England hat sogar Gesundheitsdaten seiner Bürger in Palantir-Systeme eingespielt. Nun male man sich aus, was geschieht, wenn die Chatkontrolle mit einer solchen Datenkrake verknüpft wird: Geheimdienste und Polizei mit Zugriff auf brisanteste Kommunikationsdaten, die sich nach Belieben durchsuchen, filtern und neu interpretieren lassen, bis das Ergebnis passt und Kritiker noch effizienter verfolgt und abgestraft werden können.

Der CEO von Palantir hat den militärisch-tödlichen Einsatz seiner Software nie kleingeredet, sondern öffentlich damit kokettiert, ein Umstand, der jede rote Linie überschreitet, die man sich vorstellen kann. (Wer die Muster dieser Zukunft studieren will, findet sie nicht nur bei George Orwell, sondern auch in den Dystopien, die man uns längst zur Unterhaltung serviert: von Black Mirror, Demolition Man, Die Bestimmung – Divergent, Matrix bis Songbird. Man betrachte sie als Warnung, nicht als Drehbuch.)

Die EuGH-Rechtsprechung, die man ignoriert

Vier Mal hat der Europäische Gerichtshof die anlasslose Vorratsdatenspeicherung kassiert: Digital Rights Ireland (C-293/12), Tele2/Watson (C-203/15), La Quadrature du Net (C-511/18), SpaceNet (C-793/19).

Was heißt „kassiert"? Es heißt: für europarechtswidrig erklärt und in den Papierkorb geworfen. Und was ist Vorratsdatenspeicherung? Das anlasslose, pauschale Speichern von Metadaten, also nicht dem Inhalt der Kommunikation, sondern den Begleitdaten: wer mit wem, wann, wie lange, von wo. Der Gerichtshof sagte: Schon das Aufschreiben des Adressfeldes aller Bürger ist ein zu schwerer Eingriff.

Denk an den Umschlag eines Briefes. Auf dem Umschlag stehen Absender, Empfänger, Datum des Poststempels, das sind die Metadaten. Im Umschlag steckt der Brief, das ist der Inhalt. Der EuGH hat viermal gesagt: Ihr dürft nicht einmal anlasslos aufschreiben, wer wem schreibt.

Die Chatkontrolle aber geht darüber hinaus. Sie erfasst nicht das Adressfeld. Sie öffnet den Brief. [10]

Wir kennen das aus der Geschichte. In der DDR hat die Stasi über die Deutsche Post Briefe geöffnet, gelesen, wieder verschlossen, Dampf über den Kessel, Klinge unter die Lasche, ein ganzes Ministerium beschäftigt mit fremder Post. Und wir kennen es aus der Gegenwart: In deutschen Justizvollzugsanstalten wird die Post der Gefangenen geöffnet und mitgelesen. Genau dieses Prinzip, das Öffnen des verschlossenen Briefes durch Dritte, soll nun auf die gesamte Bevölkerung ausgedehnt werden, nur digital und in Echtzeit.

Wenn man diese Fähigkeit mit Systemen wie Palantir verknüpft und die Chatkontrolle ihre volle Perversion erreicht, dann werden sie alles über uns wissen. Und weil alle Informationen in Echtzeit vorliegen, kann man KI-Modelle damit füttern und jeden einzelnen Menschen anhand seiner Nachrichten einordnen: ob jemand intelligent ist, ob jemand kritisch eingestellt ist, ob man Kritiker ist, ob man Staatsfeind ist, ob man als Gefahr eingestuft wird, weil man sich nicht an das Narrativ hält und das herrschende System nicht als Freund definiert.

Das ist keine Science-Fiction. Das ist eine Datenbankoperation mit einem Sprachmodell davor.

IV. Die Technik ist die Politik

„Freiwillig" klingt harmlos. „Nur Hash-Abgleich bekannten Materials" klingt chirurgisch, sauber und präzise. Beides sind Nebelkerzen. Wer die Technik versteht, versteht die Politik.

Erstens: Der Scanner ist die Backdoor

Client-Side-Scanning durchleuchtet Nachrichten auf dem Gerät, bevor sie verschlüsselt werden. Die Verschlüsselung bleibt formal intakt, und ist praktisch bedeutungslos.

Stell es dir so vor: Du hast ein Handy mit Ende-zu-Ende-Verschlüsselung. Die Nachricht verlässt dein Gerät verschlüsselt, reist verschlüsselt durchs Netz, kommt verschlüsselt beim Empfänger an. Niemand auf dem Transportweg kann mitlesen. So weit, so sicher.

Aber: Dein eigenes Gerät muss die Nachricht ja zeigen. Auf deinem Bildschirm erscheint der Klartext, sonst könntest du ihn nicht lesen. Beim Empfänger genauso. Das Betriebssystem des Geräts sieht also immer den unverschlüsselten Inhalt, im Moment des Schreibens und im Moment des Lesens. Und genau da setzt die Backdoor an. Sie muss gar nichts entschlüsseln. Sie sitzt einfach im Betriebssystem und schneidet mit, vor dem Verschließen des Umschlags, nach dem Öffnen.

Man muss sich das vorstellen wie jemanden, der an der Wohnungstür lauscht. Er muss das Schloss nicht knacken. Er muss die Tür nicht aufbrechen. Er hört einfach mit, während drinnen gesprochen wird. Die stabilste Panzertür der Welt nützt nichts, wenn im Türrahmen ein Mikrofon steckt.

Über 600 Wissenschaftler aus 35 Ländern haben genau das in einem offenen Brief festgehalten: Das Scannen vor der Verschlüsselung zerstört den Zweck der Ende-zu-Ende-Verschlüsselung und schafft einen zentralen Angriffspunkt. [14][15]

Und sie haben recht: Es ist sinnlos, eine Verschlüsselung zu benutzen, wenn im Betriebssystem ein Mitleser sitzt. Es ist derselbe Effekt, den ein Trojaner hätte, etwa ein Keylogger, der jede Tastatureingabe abgreift und ins Netz schickt. Der Unterschied ist nur: Beim Trojaner ist es ein Krimineller, der eindringt. Beim Client-Side-Scanning ist es der Gesetzgeber, der den Keylogger gleich mitliefert.

Ein Schloss, das für eine Behörde aufgeht, geht auch für einen Nachrichtendienst auf, für einen Erpresser, für eine fremde Regierung oder für ein Regime, das eines Tages an die Macht kommt und diese Werkzeuge gegen die eigenen Menschen richtet. Verknüpft man das Ganze mit einer Auswertungsmaschinerie vom Kaliber Palantirs, entsteht eine Datenkrake, in die Milliarden fließen werden, nicht zufällig, sondern als Teil des Konzepts.

Friedrich Merz war jahrelang Aufsichtsratschef von BlackRock Deutschland; Alice Weidel begann ihre Karriere bei Goldman Sachs. Man muss daraus keine Verschwörung konstruieren, um die schlichte Frage zu stellen: In wessen Interesse wird Politik gemacht, wenn die Beteiligungslisten der großen Finanzhäuser sich mit den Machtpositionen des Landes überschneiden?

Zweitens: Fehlerquoten sind keine Statistik, sondern Existenzen

Die BfDI, die oberste Datenschutzbehörde des Bundes, hat vorgerechnet: Bei einem Dienst wie WhatsApp mit rund zwei Milliarden Nutzern könnten bis zu 240 Millionen Menschen zu Unrecht der Verbreitung von Missbrauchsmaterial beschuldigt werden. [11]

240 Millionen: Das ist keine abstrakte Fehlerquote, sondern das sind Existenzen. Betroffen wäre das Urlaubsfoto der eigenen Kinder am Strand ebenso wie der Nacktscan, den ein 15-Jähriger seiner Freundin schickt, oder die Beweisdokumentation einer Mutter, die ihr Kind vor einem Täter schützen will. Der Algorithmus sieht nur Pixel und Wahrscheinlichkeiten und kennt den Kontext nicht. Und wer einmal in einer Verdachtsdatenbank steht, bleibt dort, denn Rehabilitation ist ein zäher Verwaltungsakt und kein Reflex: Der Verdacht ist schnell erzeugt und nur langsam wieder gelöscht.

Und hier die ehrliche, unbequeme Frage, halb ironisch, halb todernst: Würden eigentlich auch die Handys der Bundestagsabgeordneten gescannt? Die der Geheimdienstler? Der Polizeiführung? Der Konzernbosse? Der Bankvorstände? Jener Mitglieder pädokrimineller Netzwerke, die in hohen Positionen sitzen? Oder gibt es Ausnahmen? Und wenn es Ausnahmen gibt, wer überwacht die Ausgenommenen? Ein Gesetz, das die Mächtigen von der eigenen Kontrolle ausnimmt, ist kein Schutzgesetz. Es ist ein Herrschaftsgesetz.

Drittens: Signal geht

Der Betreiber des Messengers Signal hat unmissverständlich erklärt, was ein verpflichtendes On-Device-Scanning bedeuten würde: „we will leave the EU market rather than undermine our privacy guarantees." [15] Man würde eher den europäischen Markt verlassen, als die eigenen Sicherheitsgarantien zu untergraben.

Stell dir vor, was das heißt. Der sicherste Messenger der Welt zieht sich zurück, weil er in Europa nicht mehr sicher sein darf. Zurück bleiben die Dienste, die scannen. Es ist, als würde man alle einbruchsicheren Schlösser verbieten und nur noch jene erlauben, für die die Behörde einen Zweitschlüssel besitzt. Europa würde dadurch nicht sicherer. Es würde ärmer an sicherer Kommunikation, und reicher an Hintertüren, die früher oder später jemand findet, für den sie nie gedacht waren.

V. Die eigentliche Gefahr: Sie bauen ein Haus, in das ein anderer einzieht

Und hier beginnt das Kapitel, das man in Brüssel nicht diskutieren will.

Nehmen wir für einen Moment an, großzügig und gegen jede Erfahrung, dass jede heute handelnde Person in Kommission, Rat und Parlament ausschließlich Kinder schützen will, dass es also keine Lobbyisten gibt, keine Karrieren, keine Eitelkeiten und keine Netzwerke, in die irgendjemand verstrickt ist.

Es ändert nichts.

Denn was hier entsteht, ist keine Politik. Es ist Infrastruktur. Und Infrastruktur überlebt ihre Erbauer. Sie wird bleiben, und sie wird immer weiter ausgebaut. Lässt man den ersten Spatenstich zu, aktiviert man die Überwachungsmaschinerie überhaupt erst einmal, dann wird man zusehen müssen, wie Menschen mundtot gemacht werden oder wie sie aus Angst vor Bestrafung diese Netzwerke gar nicht mehr nutzen.

Vielleicht, und das ist der einzige hoffnungsvolle Nebeneffekt, kehrt sich der Prozess dann um: Vielleicht kommunizieren die Menschen wieder weniger über Messenger und treffen sich stattdessen wieder öfter persönlich, und lassen die Wanzen zu Hause. Denn Wanzen sind es inzwischen viele: das Smartphone, die Smartwatch, der Smart TV, der Sprachassistent im Wohnzimmer, und neuerdings das Auto. Die General Safety Regulation (EU) 2019/2144 zeigt die Richtung: immer mehr verpflichtende Aufzeichnungs- und Assistenzsysteme im Fahrzeug. Überall wird uns gesagt, es gehe um unseren Schutz. In Wahrheit legt man die Grundlagen, um Milliarden zu verdienen, Macht zu festigen und die Menschen in der leisen Dauerangst zu halten, für irgendetwas abgestraft zu werden.

Ein Gesetz kann man in einer Legislaturperiode ändern. Eine technische Fähigkeit, die auf 450 Millionen Endgeräten installiert ist, ändert man nicht. Einmal eingerichtet, ist sie da und liegt bereit, und sie wartet nur noch auf eine Regierung, die die Trefferliste erweitert.

Und die Erweiterung ist trivial. Sie ist eine Datenbankoperation.

Wie ein Hash-Abgleich wirklich funktioniert

Ein Hash-Abgleich prüft nicht, was ein Bild zeigt. Er prüft, ob ein Bild in einer Liste steht. Ein „Hash" ist so etwas wie ein digitaler Fingerabdruck einer Datei, eine eindeutige Zeichenfolge, die man mit einer Datenbank abgleichen kann.

Stell dir vor, es gibt ein Bild mit der Aufschrift „Stoppt den Krieg in Gaza!" oder „Stoppt den Krieg gegen Russland!". Dieses Bild hat einen Hash-Wert. Nun wird dieser Hash-Wert in eine zentrale Datenbank aufgenommen und als „kriminell" markiert. Von diesem Moment an muss niemand das Bild mehr ansehen. Es genügt, dass die Datei auf deinem Handy oder Computer liegt. Das Betriebssystem macht den Abgleich in Echtzeit, findet es den Fingerabdruck, meldet es ihn einer Behörde. Und du hast den Schlamassel, ohne je eine Straftat begangen zu haben.

Wer die Liste kontrolliert, kontrolliert, wonach gefahndet wird. Ob in dieser Liste Missbrauchsdarstellungen stehen oder ein Demonstrationsaufruf, ein Meme über den Regierungschef, das Logo einer verbotenen Organisation oder eine Seite aus einem verbotenen Buch, der Scanner kennt den Unterschied nicht. Er kennt nur zwei Antworten, nämlich Treffer oder kein Treffer.

Die Technik ist moralisch blind. Sie dient und liefert jedem Herrn, jedem Herrscher, jedem Diktator und jeder parteipolitischen Perversion das gewünschte Ergebnis, jedem also, der sich heute oder in Zukunft an die Spitze der Menschheit stellt und sich anmaßt, über fremde Menschen zu bestimmen.

Das Szenario, das niemand aussprechen will

Setz den Fall, und Europa im Jahr 2026 hat wenig Anlass, ihn für abwegig zu halten, dass in einem oder mehreren Mitgliedstaaten eine Regierung an die Macht kommt, die den freien Menschen als Hindernis begreift, die ihn noch effizienter ausbeuten und ihn notfalls in Kriegen opfern will, weil hinter ihr womöglich eine Sektenstruktur steht, die Gewaltenteilung nicht als Errungenschaft, sondern als lästige Bremse empfindet.

Sie muss nichts neu erfinden, nichts durchsetzen und keine Überwachungsgesetze mehr gegen Widerstand durchboxen.

Sie erbt.

Stell dir einen neuen Machthaber vor, der am ersten Tag seiner Amtszeit die Schlüssel zu einem fertig gebauten Haus überreicht bekommt. In diesem Haus liegt bereits alles bereit: eine gesetzliche Erlaubnis, private Kommunikation zu scannen. Eine europaweite Meldeinfrastruktur, die Verdachtsfälle automatisch weiterleitet. Ein EU-Zentrum mit einer Verdachtsfalldatenbank, womöglich längst an ein System wie Palantir angeschlossen, sodass jede Behörde in Echtzeit mitlesen und sich per Stichwort benachrichtigen lassen kann, sobald ein Chatverlauf in eine unerwünschte Richtung läuft. Eine verpflichtende Altersverifikation, die anonyme Kommunikation faktisch beendet. Erkennungssoftware auf jedem Endgerät. Und eine Bevölkerung, die sich an das Gescanntwerden längst gewöhnt hat. [5][11]

Der neue Machthaber muss nichts davon bauen. Er muss lediglich die Liste ändern und einen einzigen Erwägungsgrund umschreiben. Aus dem Kampf gegen „sexuellen Missbrauch von Kindern" wird dann Schritt für Schritt der Kampf gegen „schwere Kriminalität", daraus der Kampf gegen „Terrorismus", dann gegen „Extremismus", schließlich gegen „Desinformation" und am Ende gegen alles, was sich als „staatsgefährdender Inhalt" deklarieren lässt. Der Scanner bleibt derselbe, nur der Suchbegriff wandert immer weiter, bis er jeden erfassen kann.

Jeder dieser Schritte hat, für sich genommen, eine plausible Begründung. Das ist ja gerade der Punkt. Niemand baut einen Überwachungsstaat, indem er einen Überwachungsstaat baut. Man baut ihn, indem man Kinder schützt, dann Opfer von Terror schützt, dann die Demokratie vor Lügen schützt. Und irgendwann schützt man sie vor ihren Bürgern.

Auf diesem Weg befinden wir uns bereits. Wer wissen will, wohin die Reise geht, muss nicht spekulieren, er muss nur die Gegenwart lesen: In welchen Ländern werden heute schon Menschen an der Ausreise gehindert, wenn sie zu kritischen Kundgebungen ins Ausland wollen? Wo werden Rückkehrer von der Bundespolizei festgesetzt und verhört, wie man es aus den Filmen über die DDR kennt? Wo werden Menschen für das falsche Posting verfolgt? Die Antworten sind unbequem, weil sie näher liegen, als uns lieb ist.

Der Chilling Effect ist kein Nebeneffekt, er ist der Zweck

Das Bundesverfassungsgericht hat 1983 im Volkszählungsurteil (BVerfGE 65, 1) einen Gedanken formuliert, der heute wichtiger ist denn je. Es hat das Grundrecht auf informationelle Selbstbestimmung begründet und sinngemäß festgehalten: Wer nicht mit hinreichender Sicherheit überschauen kann, wer was wann über ihn weiß, wird aus Vorsicht darauf verzichten, von seinen Grundrechten Gebrauch zu machen.

Übersetzt für den Alltag: Wenn du nicht weißt, ob dir gerade jemand zuhört, verhältst du dich, als hörte dir immer jemand zu. Du sagst das Unverfängliche. Du unterschreibst die Petition nicht. Du gehst nicht auf die Demo. Du löschst die Nachricht lieber, bevor du sie schickst, oder schreibst sie erst gar nicht. Und das schädigt nicht nur dich, es schädigt das Gemeinwesen, denn Selbstbestimmung ist die Voraussetzung eines freien Menschen. Ein Volk, das schweigt, kann sich nicht selbst regieren.

Das ist die schärfste Waffe der Überwachung: Sie muss gar nicht angewandt werden. Sie muss nur möglich sein. Der Hofhund braucht keinen Stromschlag mehr, wenn er den Zaun im Kopf trägt.

Und das ist nicht bloß Rhetorik, es ist empirisch belegt. Die Kommunikationswissenschaftlerin Elizabeth Stoycheff hat nach den Enthüllungen von Edward Snowden untersucht, wie sich das Wissen um Überwachung auf das Verhalten auswirkt. Ergebnis: Menschen, die sich überwacht fühlen, äußern abweichende oder Minderheitsmeinungen seltener öffentlich, sie zensieren sich selbst. Sie nannte es die „Spirale des Schweigens" (aufbauend auf Elisabeth Noelle-Neumanns Theorie von 1974) unter Überwachungsbedingungen. In einer Folgestudie (Privacy and the Panopticon, 2019) zeigte sie, dass Überwachung nicht nur Kriminelles, sondern gerade auch politisches Verhalten unterdrückt, quer durch verschiedene Gruppen und Kontexte.

Der Begriff „Panopticon" stammt von Jeremy Bentham und wurde von Michel Foucault zur Herrschaftstheorie ausgebaut: ein Gefängnis, in dem ein einziger Wächter im Zentrum alle Zellen sehen könnte, und in dem die Gefangenen, weil sie nie wissen, ob gerade jemand hinsieht, sich verhalten, als ob immer jemand hinsähe. Sie bewachen sich am Ende selbst. Die moderne Forschung (Büchi, Festic, Latzer 2022) spricht vom „Dataveillance"-Effekt: Schon das Gefühl permanenter Datenüberwachung senkt die Bereitschaft, sich legal und legitim zu äußern. Und Jonathon Penney wies nach, dass die Zugriffszahlen auf sensible Wikipedia-Artikel nach den Snowden-Enthüllungen messbar einbrachen, die Menschen trauten sich nicht einmal mehr, nachzulesen.

Psychologisch bedeutet Dauerüberwachung chronischen Stress: Hypervigilanz, das ständige Gefühl, beobachtet zu werden, erhöhte Grundanspannung, ein schleichender Verlust an Spontaneität und Kreativität. Ein Mensch, der sich permanent selbst kontrolliert, lebt nicht mehr frei, er funktioniert. Der EuGH hat diesen Zusammenhang mehrfach angemahnt: Anlasslose Massenüberwachung schlägt mittelbar auf die Meinungsfreiheit (Art. 11 GRCh) durch, weil sich vorsichtiger äußert, wer der Vertraulichkeit seiner Kommunikation nicht sicher sein kann. [10]

Vorsichtige Bürger sind bequeme Bürger. Und es könnte sein, dass das kein Betriebsunfall ist, sondern das eigentliche Ziel.

VI. Wen es zuerst trifft

Es trifft nicht zuerst dich und nicht mich, sondern jene, deren Beruf die Vertraulichkeit ist.

Journalisten und ihre Quellen. Das Redaktionsgeheimnis ist ein Grundrecht, kein Feature, das WhatsApp einbaut. Journalisten recherchieren über Telefon, E-Mail, Messenger. Doch was ist, wenn jede Recherche mitgelesen wird? Was, wenn kritische Berichterstattung unter Verdacht steht und jeder Versuch, einer Sache auf den Grund zu gehen, sofort ein Signal an die Behörde sendet? Dann endet die vierte Gewalt nicht mit einem Verbot, sondern mit einem Scanner. Die Recherche stirbt an der stillen Gewissheit, dass jemand mitliest.

Whistleblower. Die EU hat eine Whistleblower-Richtlinie, und zugleich einen Kanal, der sie ausliest. Stell dir einen Mitarbeiter vor, der einen Skandal aufdecken will. Er weiß: Sein Handy ist über die SIM-Karte jederzeit ortbar. Seine Nachrichten sind abfangbar. Sein Foto des belastenden Dokuments hat einen Hash-Wert. In einer Welt der Chatkontrolle wird der Whistleblower zur aussterbenden Spezies, nicht weil man ihn verbietet, sondern weil er weiß, dass der erste Schritt der letzte sein könnte: Festsetzung, Verhör und Repression. Wer nie sicher sein kann, schweigt. Und wer schweigt, deckt nichts mehr auf.

Ärzte, Anwälte, Seelsorger, Beratungsstellen. § 203 StGB schützt das Berufsgeheimnis. Der Scanner kennt keinen § 203. Und die Folgen reichen tiefer, als man denkt: Die seelischen Nöte eines Menschen, die Diagnose, die Sucht, die Verzweiflung, die er nur seinem Therapeuten anvertraut, werden zu abgreifbaren Daten. In den falschen Händen werden sie zur Waffe gegen genau die Menschen, die Hilfe suchten. Man kann einen Kritiker mit dem brechen, was er in seiner schwächsten Stunde einem Arzt gestand.

Wie dehnbar dieses Ärztegeheimnis in Wahrheit ist, mussten wir schon in der Plandemiezeit mit Sorge beobachten. Damals rückten vermummte Sondereinsatzkräfte in Praxen und Kliniken ein, durchsuchten Räume, beschlagnahmten ganze Aktenbestände und nahmen Ärzte fest, nur um herauszufinden, wem diese Ärzte per Attest eine Befreiung von der Maskenpflicht ausgestellt hatten.

Auf die Schweigepflicht wurde dabei, auf gut Deutsch, geschissen. Genau daran erkennt man, wie biegsam diese Systeme sind: Sie zimmern sich das Recht so zurecht, wie sie es gerade brauchen, um weiter herrschen zu können und die Menschen notfalls in die nächste Krise zu treiben. Wenn schon ein Papierattest ausreichte, um die Panzertür des Berufsgeheimnisses aufzubrechen, was glaubt man wohl, wie lange sie vor einem fertig installierten Scanner standhält?

Missbrauchsopfer selbst. Die Ironie ist bitter bis zur Grausamkeit. Eine Mutter sichert Beweise gegen einen Täter, ein Foto, eine Nachricht, eine Dokumentation, und schickt sie über einen Messenger an ihre Anwältin. Der Scanner kann dieses Material nicht von Täterkommunikation unterscheiden. Er sieht nur: Treffer. Und plötzlich steht das Opfer selbst unter Verdacht. Das Gesetz, das Kinder schützen soll, kriminalisiert jene, die sie schützen wollen.

Die Opposition. Nicht unbedingt die von heute, sondern jede, die morgen aus der Gunst der Macht fällt. Denn das Werkzeug fragt nicht danach, wer gerade regiert, es dient immer dem, der es in der Hand hält, und richtet sich gegen den, der gerade nicht an der Macht ist. Wer sich für Freiheit einsetzt, gegen einen Krieg positioniert, gegen eine als absurd empfundene Politik mobilisiert und dafür mit Verhaftung, Verfahren und Repression rechnen muss, der lebt nicht in einer Demokratie, sondern in ihrer Fassade. Es ist eher eine Plutokratie, die einer Zwangsherrschaft gleicht als einer echten Volksherrschaft, wo das Volk bestimmt. Und genau darin liegt der eigentliche Zweck der Chatkontrolle: die Macht so weit zu festigen, dass niemand mehr gegen die verabschiedete Perversion aufbegehren kann. Dabei ist es gerade das Anderssein, das Andersdenken, das eine Gesellschaft stabil hält und Regierungen davon abhält, vollends zu entgleisen.

Und der Deutsche Kinderschutzbund? Er hat sich gegen die Chatkontrolle ausgesprochen und zielgerichtete Maßnahmen statt anlassloser Massenüberwachung gefordert. [16]

Man lasse sich das auf der Zunge zergehen: Die Kinderschützer sind gegen das Gesetz, das die Kinder schützen soll. Wer bleibt dann übrig, der dafür ist? (Wobei man auch dem Kinderschutz-Apparat insgesamt kritische Fragen stellen darf, man denke an die vielen Eltern, allen voran Alleinerziehende, die dem Handeln von Jugendämtern ohnmächtig gegenüberstehen. Missbrauch von Schutzgewalt geht nicht selten von den Institutionen selbst aus. Aber das ist eine andere Streitschrift.)

VII. Der Preis, der nicht bezahlt wird: Es funktioniert nicht einmal

Die Befürworter argumentieren mit einer Regelungslücke: Acht von zehn Ermittlungen würden durch Hinweise von Plattformen ausgelöst. Also müsse man weiterscannen. Prüfen wir das.

1. Nach Angaben der Bundesregierung wurde seit dem Auslaufen der Verordnung am 3. April kein außergewöhnlicher Rückgang entsprechender Meldungen festgestellt. [4] Die angebliche Katastrophe blieb aus.

2. Unternehmen wie Google haben angekündigt, ohnehin weiterhin freiwillig zu scannen. [4] Die „Lücke" schließt sich in der Praxis von selbst.
3. Mehr als 60 Prozent der Verdachtsmeldungen stammen nach offiziellen EU-Zahlen aus dem Scannen öffentlicher Beiträge und Cloud-Speicher, Bereiche, die die Übergangsverordnung überhaupt nicht erfasst. [4]

Der letzte Punkt hat eine praktische Konsequenz für jeden von uns: Spiel deine Daten nicht in fremde Clouds. Kein Google Drive, keine Apple-Cloud für das, was privat bleiben soll. Es sind deine Daten, also behalte sie auf deinen Geräten. Schalte die Cloud-Synchronisation ab, so bequem sie auch ist. Der Weg zurück in die Freiheit führt über die Dezentralisierung: zurück zur Unabhängigkeit, zurück zur Datenhoheit. Niemand sollte das Recht haben, in deinem Leben zu schnüffeln, und die Cloud ist die Tür, die du selbst offen lässt.

Die „Lücke", deren Schließung 450 Millionen Menschen ihre Kommunikationsfreiheit kosten soll, ist zu einem erheblichen Teil eine rhetorische Lücke.

Und die SPD-Berichterstatterin Birgit Sippel, die dem Text zähneknirschend zustimmte, hielt selbst fest: „Die Faktenlage reicht nach wie vor nicht aus, um einen breiten Anwendungsbereich zu rechtfertigen." [7]

Die Berichterstatterin. Über ihren eigenen Bericht. Wenn selbst diejenige, die das Gesetz durchs Parlament trägt, sagt, die Faktenbasis trage nicht, dann geht es nicht um Fakten. Dann geht es darum, die richtigen Leute in die richtigen Positionen zu bringen, um die Sache bis zur letzten Stufe durchzusetzen.

VIII. Und das war erst Version 1.0

Machen wir uns nichts vor über den Umfang dessen, was am 9. Juli 2026 geschah, und über das, was noch kommt.

Was durchging, ist Chatkontrolle 1.0: die freiwillige Variante. Sie betrifft unverschlüsselte Inhalte; ein Änderungsantrag der Grünen nimmt Ende-zu-Ende-verschlüsselte Kommunikation ausdrücklich aus dem Geltungsbereich. [1][2] Man kann sich das vorstellen wie eine Erlaubnis für den Postboten, offene Postkarten zu lesen, die verschlossenen Briefe (die verschlüsselten Chats) bleiben vorerst tabu. Das ist die gute Nachricht. Sie ist klein.

Denn parallel läuft der Trilog zur CSA-Verordnung, der dauerhaften, potenziell verpflichtenden Chatkontrolle 2.0.

Was ist die CSA-Verordnung? „CSA" steht für Child Sexual Abuse. Die EU-Kommission legte den Verordnungsentwurf erstmals im Mai 2022 vor. Sein Kern: Anbieter sollen verpflichtet werden, ihre Dienste auf Missbrauchsmaterial und Anbahnungsversuche zu durchsuchen, notfalls per behördlicher „Aufdeckungsanordnung", auch in verschlüsselten Diensten. Und „Trilog"? Das ist die Verhandlungsrunde zwischen den drei EU-Institutionen, Europäisches Parlament, Rat der EU und Europäische Kommission, in der der endgültige Gesetzestext hinter verschlossenen Türen ausgehandelt wird.

Das Verhandlungsteam des Europäischen Parlaments erklärte am 29. Juni 2026, man habe sich auf nahezu die gesamte Verordnung geeinigt, offen sei „insbesondere die Aufdeckung" (detection). [17]

Offen ist also genau das, worum es geht.

Die Ratsposition vom 26. November 2025 verzichtet zwar auf verpflichtende Aufdeckungsanordnungen, enthält aber eine Review-Klausel: Die Kommission muss binnen drei Jahren prüfen, ob Detection-Pflichten „notwendig und machbar" sind. [18]

Das ist keine Entwarnung. Das ist ein Terminkalender. Man baut die Waffe, entschärft sie sichtbar für die Öffentlichkeit, und schreibt ins Kleingedruckte, wann man sie scharf machen darf. Genau an dieser Stelle wäre ein gesellschaftlicher Notausknopf überfällig: ein Mechanismus, der jede solche Entscheidung stoppen kann, fest verankert, dem Zugriff der Herrschenden entzogen, damit der Missbrauch gar nicht erst greifen kann. Dass es einen solchen Knopf nicht gibt, ist kein Versehen. Es ist das Betriebsprinzip.

Hinzu kommt der neue Schauplatz: die verpflichtende Altersverifikation, die anonyme Kommunikation faktisch beenden und zu einer Ausweispflicht im Internet führen würde. [5][11] Und die Verdachtsfalldatenbank des neuen EU-Zentrums. [11]

Jetzt zoomen wir heraus und betrachten das Gesamtbild. Da ist der digitale Euro, die digitale Zentralbankwährung, mit der jede Transaktion nachvollziehbar und potenziell steuerbar wird; da ist die Altersverifikation, die das Ende der Anonymität bedeutet; und da ist die Chatkontrolle, die das Ende des Kommunikationsgeheimnisses bringt. Jedes dieser Module wird für sich mit guten Gründen präsentiert, doch zusammen ergeben sie eine lückenlose Architektur der Nachvollziehbarkeit und Überwachung.

Man baut sie nicht in einem Zug. Man baut sie modular, Stein für Stein, Gesetz für Gesetz, jedes für sich harmlos. Und der eigentliche Trick besteht darin, dass niemand jemals über das fertige Gebäude abstimmt. Man stimmt über die Fenster ab, über die Türen, über die Statik, nie über das Haus. Und wenn es steht, verbindet man die Module: den digitalen Euro mit der Altersverifikation, die Altersverifikation mit der Chatkontrolle, und alles zusammen mit einer Auswertungsmaschine vom Kaliber Palantirs. Das Ergebnis wäre eine digitale Monstrosität, die man dann gegen die gesamte Bevölkerung richten kann.

IX. Was zu tun bleibt

1. Namen merken, vor allem die der Befürworter.
Die treibende Kraft hinter der Wiederauferstehung war die EVP-Fraktion um ihren Fraktionschef Manfred Weber (CSU), gemeinsam mit Parlamentspräsidentin Roberta Metsola (EVP), die das Thema überhaupt erst wieder auf die Tagesordnung setzte und das Eilverfahren möglich machte. Getragen wurde die Chatkontrolle vor allem von der EVP, zu der CDU und CSU gehören, sowie von Teilen der Sozialdemokraten. Besonders pikant: Jens Spahn, Vorsitzender der CDU/CSU-Bundestagsfraktion, hatte im Oktober 2025 noch öffentlich versprochen, eine anlasslose Chatkontrolle werde es „mit uns nicht geben" und verglich sie selbst damit, „vorsorglich mal alle Briefe" zu öffnen. Wenige Monate später stimmten seine Parteifreunde im Europaparlament genau dafür.

Diese deutschen Abgeordneten stimmten am 9. Juli 2026 für die Chatkontrolle (Quelle: RCV-Protokoll des EU-Parlaments sowie die namentliche Übersicht der Berliner Zeitung vom 10.07.2026 [19][28]):

1. **CDU (EVP):** Hildegard Bentele, Stefan Berger, Lena Düpont, Christian Ehler, Michael Gahler, Jens Gieseke, Niclas Herbst, Norbert Herhammer, Marie-Sophie Lanig, Peter Liese, Norbert Lins, David McAllister, Alexandra Mehnert, Verena Mertens, Angelika Niebler, Dennis Radtke, Oliver Schenk, Andreas Schwab, Sven Simon, Sabine Verheyen, Axel Voss, Marion Walsmann, Andrea Wechsler.
2. **CSU (EVP):** Christian Doleschal, Markus Ferber, Monika Hohlmeier, Stefan Köhler, Manfred Weber.
3. **SPD (S&D):** Tobias Cremer, Matthias Ecke, Bernd Lange, Maria Noichl, René Repasi, Sabrina Repp.
4. **Familien-Partei Deutschlands (EVP):** Niels Geuking.

Enthalten hat sich Delara Burkhardt (SPD). Nicht anwesend waren unter anderem Katarina Barley (SPD), Ralf Seekatz (CDU), Christine Anderson und Alexander Sell (beide AfD), Thomas Geisel (BSW) und Martin Schirdewan (Die Linke), deren Abwesenheit im gewählten Verfahren faktisch wie eine Zustimmung wirkte.

Der Widerstand kam quer durch die anderen Lager: von den Grünen, von der FDP (der Europaabgeordnete Moritz Körner nannte das Vorgehen das „Schmutzigste", was er im Parlament je erlebt habe), vom BSW (Fabio De Masi, Friedrich Pürner) und von der AfD (Mary Khan sprach von einem „demokratischen Skandal") sowie vom fraktionslosen Martin Sonneborn (Die PARTEI). Die vollständige, namentliche Aufschlüsselung jeder einzelnen Stimme steht im offiziellen RCV-Protokoll [19]; wer einen bestimmten Abgeordneten prüfen will, findet ihn dort.

2. Verschlüsselung benutzen.

Nicht, weil man etwas zu verbergen hat, sondern weil ein Recht, das niemand ausübt, aufhört, ein Recht zu sein. Und noch besser: Behandle die Messenger, WhatsApp, Telegram, Signal und alle anderen, nur als Prothese, nicht als Ersatz für echte Nähe. Fasse die digitale Kommunikation kurz. Gibt es Wichtiges zu besprechen, dann triff dich persönlich. Von Angesicht zu Angesicht, im Café, und die Abhörwanze, das Handy, lass zu Hause. Die sicherste Ende-zu-Ende-Verschlüsselung ist immer noch das gesprochene Wort zwischen zwei Menschen an einem Tisch.

3. Das Argument nicht überlassen.
Wer Kinderschutz gegen Bürgerrechte ausspielt, lügt in beide Richtungen. Und wenn du diese demokratische Perversion schon unbedingt beibehalten willst, dann fordere wenigstens das, was tatsächlich und punktuell wirkt: schnellere Löschung und richterlich angeordnete Überwachung konkreter Verdächtiger. Nichts davon braucht die Durchleuchtung von 450 Millionen Unschuldigen.

4. Aufhören, „aber ich habe nichts zu verbergen" zu sagen.
In Wahrheit hast du eine Menge zu verbergen, und zwar völlig zu Recht: deine Bankdaten, deine ärztliche Diagnose, deine Scheidung, deine Meinung über deinen Chef und deine Meinung über deine Regierung. Letztere ist heute noch harmlos, morgen aber vielleicht schon der Anlass für die erste Hausdurchsuchung, weil man das Falsche in einen Chat getippt hat. Man muss sich nur erinnern, wie weit die Behörden bereits in den Pandemiejahren gingen, als Menschen wegen gepostеter Bilder zu Hause aufgesucht und ihre Computer, USB-Sticks und Datenträger beschlagnahmt wurden. „Nichts zu verbergen" ist deshalb kein Argument, sondern eine Kapitulation, formuliert von jemandem, der bloß noch nicht an der Reihe war.

Schluss

Sie haben nicht deine Nachrichten gelesen. Noch nicht.

Sie haben etwas anderes getan, das schlimmer ist: Sie haben die Frage entschieden, ob deine Nachrichten grundsätzlich lesbar sein dürfen. Und sie haben sie mit Ja beantwortet, in einem halbleeren Saal, gegen die Mehrheit der Anwesenden, in der Woche vor der Sommerpause.

Erinnere dich an den Strick vom Anfang. An den Hund mit dem Zaun im Kopf. Das Fernmeldegeheimnis ist ein Grundrecht. Grundrechte sterben nicht durch Abschaffung, niemand steht auf und ruft „ab heute keine Freiheit mehr". Sie sterben durch Ausnahmeregelungen, die verlängert werden. Durch Provisorien, die dauerhaft werden. Durch Infrastruktur, die harmlos beginnt. Sie sterben leise, in einem Nebensatz, in einer Review-Klausel, an einem Donnerstag im Juli.

Und eines dürfen wir dabei nie vergessen: Ein Kanal, der an einer Stelle mitlesen kann, kann dort auch schreiben. Wer hineinschauen kann, kann auch etwas hineinlegen. Damit steht die Tür nicht nur zum Ausspähen offen, sondern zum Fälschen, bis hin dazu, einem Unbequemen die passenden Beweise unterzuschieben, für ein Verbrechen, das er nie begangen hat. Das ist die eigentliche Endstufe des politischen Missbrauchs: nicht nur zu wissen, was du sagst, sondern zu bestimmen, was du gesagt haben sollst.

Und wenn eines Tages jemand kommt, der die Liste ändert, wird er sich nicht bedanken müssen. Er wird nichts bauen müssen. Wir haben ihm das Haus gebaut. Wir haben ihm die Schlüssel dagelassen. Wir waren im Urlaub.

Quellen

1. Europäisches Parlament, Pressemitteilung: „Bekämpfung sexuellen Kindesmissbrauchs: EP für enger gefasste Ausnahmeregelung", 09.07.2026. REF 20260706IPR46318. → https://www.europarl.europa.eu/news/de/press-room/20260706IPR46318/
2. netzpolitik.org: „EU-Parlament: Freiwillige Chatkontrolle geht mit Verfahrenstrick durch", 09.07.2026. → https://netzpolitik.org/2026/eu-parlament-freiwillige-chatkontrolle-geht-mit-verfahrenstrick-durch/
3. Dr. Web: „Chatkontrolle: Das EU-Parlament ebnet per Eilverfahren den Weg zur Neuabstimmung", Juli 2026.
4. Berliner Zeitung: „Grünes Licht für Chatkontrolle im EU-Parlament", 09./10.07.2026. → https://www.berliner-zeitung.de/article/eu-parlament-verabschiedet-chatkontrolle-10181552 · sowie ZDFheute, 09.07.2026.
5. alarm.de: „ChatControl und CSAR, Wenn der Staat an deine Verschlüsselung will", Stand 29.06.2026.

6. Deutscher Bundestag, Wissenschaftliche Dienste / Fachbereich Europa: EU 6 - 3000 - 061/25; WD 3 - 3000 - 080/25 (2025). → https://www.bundestag.de/resource/blob/1132100/EU-6-061-25-WD-3-080-25.pdf
7. netzpolitik.org: „Freiwillige Chatkontrolle: Ausnahmeregel wird zum zweiten Mal verlängert", 06.02.2026.
8. netzpolitik.org: „Juristisches Gutachten: Chatkontrolle ist grundrechtswidrig und wird scheitern", 17.05.2023 (JD des Rates, Dok. 8787/23 v. 26.04.2023).
9. netzpolitik.org: „Rechtsgutachten: Chatkontrolle unvereinbar mit Grundrechte-Charta" (Gutachten Christopher Vajda), 2023.
10. Gesellschaft für Freiheitsrechte (GFF): „Chatkontrolle: Mit Grundrechten unvereinbar". → https://freiheitsrechte.org/themen/freiheit-im-digitalen-zeitalter/chatkontrolle
11. BfDI: „Die geplante EU-Verordnung … die sogenannte ‚Chatkontrolle'". → https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Telemedien/CSA_Verordnung.html (Amtsinhaberin bis 30.09.2026: Prof. Dr. Louisa Specht-Riemenschneider; Nachfolger ab 01.10.2026: Prof. Dr. Moritz Hennemann).
12. BVerfG, Beschluss vom 24.06.2025 – 1 BvR 180/23 („Trojaner II"); zugleich 1 BvR 2466/19.
13. Kanzlei Tsambikakis / rechtundpolitik.com: Analysen zum Trojaner-II-Beschluss.
14. netzpolitik.org: „Offener Brief: Hunderte Wissenschaftler:innen stellen sich gegen Chatkontrolle", 09.09.2025.
15. Security-Insider: „Über 600 Experten kritisieren Überwachung durch Chatkontrolle", 09/2025 (inkl. Signal-Statement).
16. Deutscher Kinderschutzbund, Stellungnahme Oktober 2025.
17. Europäisches Parlament: „Statement by the EP negotiating team on combatting child sexual abuse online", 29.06.2026. REF 20260629IPR46216.
18. SecurityToday: „EU Chatkontrolle 2026 …", 27.03.2026 (Ratsposition v. 26.11.2025, Review-Klausel).
19. Europäisches Parlament, namentliche Abstimmungsergebnisse (RCV) vom 09.07.2026. → https://www.europarl.europa.eu/doceo/document/PV-10-2026-07-09-RCV_EN.html
20. ZDFheute: „‚Chatkontrolle': EU-Parlament stimmt für Verlängerung", 09.07.2026.

Zur psychologischen und historischen Untermauerung (Kapitel V/VI):

1. E. Stoycheff: „Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring", Journalism & Mass Communication Quarterly 93 (2016).
2. E. Stoycheff u. a.: „Privacy and the Panopticon: Online mass surveillance's deterrence and chilling effects", New Media & Society 21 (2019).
3. M. Büchi, N. Festic, M. Latzer: „The Chilling Effects of Digital Dataveillance", Big Data & Society (2022).
4. E. Noelle-Neumann: „The Spiral of Silence" (1974); J. Bentham / M. Foucault: Panopticon / Überwachen und Strafen (1975).
5. J. Penney: „Chilling Effects: Online Surveillance and Wikipedia Use", Berkeley Technology Law Journal (2016).
6. BVerfG, Volkszählungsurteil vom 15.12.1983 (BVerfGE 65, 1), Recht auf informationelle Selbstbestimmung.
7. Verordnung (EU) 2019/2144 (General Safety Regulation), verpflichtende Fahrzeug-Assistenz-/Aufzeichnungssysteme.

Zur namentlichen Abstimmung (Kapitel IX):

1. Berliner Zeitung (Franz Becchi): „Diese deutschen EU-Abgeordneten haben für die Chatkontrolle gestimmt", 10.07.2026, gestützt auf das namentliche Abstimmungsprotokoll (RCV) des Europäischen Parlaments.

Rechtsstand: 10. Juli 2026. Das Verfahren ist nicht abgeschlossen: Der Rat hat drei Monate Zeit, die Änderungen des Parlaments zu billigen oder abzulehnen; scheitert das, folgt der Vermittlungsausschuss. Der Trilog zur dauerhaften CSA-Verordnung (Chatkontrolle 2.0) läuft weiter. Der Damm ist noch nicht gebrochen, aber der erste Spatenstich ist getan.