

Der Sättigungsangriff auf unsere Freiheitsrechte

Auf EU-Ebene laufen derzeit so viele Kontroll-Vorhaben parallel, dass man es schon fast als einen Sättigungsangriff auf die Abwehr der Bürger ansehen kann. Dieses Blatt fasst zusammen, was bereits gilt, was im Verfahren steckt und was diskutiert wird. Stand: 17. Juli 2026.



Die Baustellen im Überblick

Legende über den Status: **IN KRAFT** / **BESCHLOSSEN** | **IM VERFAHREN** | **DISKUSSION** / **STUDIE**

WIEDER IN KRAFT

Chatkontrolle 1.0 (Interims-Verordnung)

Erlaubt (verpflichtet nicht) Providern, unverschlüsselte private Nachrichten auf bekanntes Missbrauchsmaterial zu scannen. Lief am 3. April 2026 aus. Wurde am **9. Juli 2026** per Eilverfahren wieder eingesetzt, obwohl die Mehrheit dagegen stimmte (Seite 3). Gilt bis April 2028; Ende-zu-Ende-Verschlüsseltes ist ausgenommen. Zur Technik: Hash-Abgleich braucht zwar nicht die Bilder „anzusehen“, erkennt aber nur bekanntes Material und solches, das nicht gezielt verfälscht wurde.

IM TRILOG

Chatkontrolle 2.0 (CSA-Verordnung)

Die geplante Dauerregelung. Die Ratsposition (Nov. 2025) verzichtet auf verpflichtendes Scannen, enthält aber eine Review-Klausel, die die Pflicht zurückbringen kann. Umgehungstrick für Ende-zu-Ende-Verschlüsselung: Scannen auf dem

eigenen Gerät, vor der Verschlüsselung. 502 Kryptographen warnen; Signal droht mit EU-Abschaltung. Fünf Trilogrunden ohne Einigung („EU-Kuhhandel“).

GELTENDES RECHT

DSA & Trusted Flagger

Der Digital Services Act verpflichtet Plattformen zur Inhaltskontrolle in Kooperation mit Behörden. „Trusted Flagger“ melden Inhalte, die priorisiert bearbeitet werden müssen. Formal entscheidet die Plattform; faktisch löscht sie, weil sie unter Bußgeldandrohung keinen Ärger will: klare Anreize zur Überblockierung. Wer die Flagger auswählt, nimmt Entscheidungen vorweg. Dies ist eine klassische Technik spieltheoretisch optimierten Handelns.

GEPLANT (REFORM LÄUFT)

Priorisierung „vertrauenswürdiger“ Quellen

Im „European Democracy Shield“ (Nov. 2025) beklagt die Kommission, Algorithmen bevorzugten reißerische statt „zuverlässiger“ Inhalte. Deshalb will sie per AVMD-Reform (Audiovisuelle Mediendienste-Richtlinie) die Sichtbarkeit von „Mediendiensten von allgemeinem Interesse“ stärken, also von ÖR und etablierten Häusern. In Deutschland gilt Ähnliches bereits, aber abgeschwächt: § 84 Medienstaatsvertrag verordnet Benutzeroberflächen eine „Must-Show“-Pflicht für ÖR und ausgewählte „Qualitätsangebote“.

VORSCHLAG ERWARTET

Anlasslose Vorratsdatenspeicherung

Im Rahmen von „ProtectEU“ (zur Terrorismusbekämpfung) arbeitet die Kommission an einer Neuauflage: Metadaten aller Bürger (wer mit wem, wann, wo) sollen ohne Anlass gespeichert werden. Diskutiert wird die Ausweitung auf Messenger und Ausweisung für Prepaid-Karten. Dazu ein „Technologiefahrplan zur Verschlüsselung“. Der EuGH hat anschlusslose Totalspeicherung bislang wiederholt gekippt.

DISKUSSIONSPAPIERE

VPN-Einschränkungen

Ein Hintergrundpapier des Parlamentsdienstes und Kommissions-Äußerungen (VPNs als „Hochrisikodienste“) nähren die Debatte; ein Gesetzesvorschlag existiert nicht. Vorbild wäre China: kein Totalverbot, sondern Lizenzen für genehmigte VPNs. Das erinnert an die Schreibmaschinenregistrierung im Ostblock.

IN UMSETZUNG

Altersverifikation

Eine EU-weite App zur Altersprüfung soll bis Ende 2026 (!) kommen, Nachweis u. a. per Ausweis. Kann zum Trojanischen Pferd für Nutzeridentifizierung und Klarnamenpflicht werden. Entscheidend ist, ob der versprochene Zero-Knowledge-Ansatz (Nachweis ohne Identitätspreisgabe) technisch garantiert wird oder nur auf dem Papier steht.

BESCHLOSSEN

Digitale ID & EUDI-Wallet

Jeder Mitgliedstaat muss bis Ende 2026 eine digitale Brieftasche anbieten: Ausweis, Führerschein, weitere Nachweise (Gesundheitsdaten?). Die Nutzung ist rechtlich freiwillig. Möglich sind Dienste, die die Wallet voraussetzen, was die Freiwilligkeit einschränkt.

GESETZGEBUNG LÄUFT

Digitaler Euro

Online-Zahlungen sind identifiziert (Geldwäscheregeln); nur die Offline-Funktion verspricht bargeldnahe Privatsphäre. Das ist ein Versprechen, kein technischer Garant. Programmierbarkeit ist im Entwurf ausgeschlossen, „bedingte Zahlungsdienste“ sind aber möglich: Die Infrastruktur entsteht, die Regel kann später geändert werden. Pilot mit 36 Zahlungsdienstleistern ab 2027.

MACHBARKEITSSTUDIE

EU-Vermögensregister

Eine 2024 veröffentlichte Kommissionsstudie prüft die zentrale Erfassung von Immobilien, Firmenbeteiligungen, Bankkonten, Wertpapieren, Krypto, Edelmetallen, Kunst und Luxusgütern. Beschlossen ist das Gesamtregister nicht. Teilregister (Eigentümer, Bankkonten, Krypto) und die Geldwäschebehörde AMLA kommen aber bereits.

Betriebssysteme werden geöffnet

Per Digital Markets Act (Wettbewerbsrecht, nicht DSA) muss Google Android für fremde KI-Assistenten öffnen: elf Systemfunktionen, Kontext aus Apps, Bildschirm, Sensoren. Nur nach Nutzerfreigabe, aber die Schnittstellen müssen existieren. Google warnt selbst, das gefährde die Gerätesicherheit. Wer profitiert? Datenhändler und Geheimdienste. Apple hält seine KI Siri deshalb in der EU zurück.

Rieck's Rasiermesser

Gehe von Absicht aus, auch wenn Dummheit die bequemere Erklärung ist.

Übrigens: Dieselbe EU hat uns zum Schutz unserer Daten die Cookie-Banner (e-Privacy), die DSGVO und den Cyber Resilience Act beschert, der den Herstellern IT-Sicherheit gesetzlich vorschreibt. Sie selbst höhlt diese Sicherheitsanforderungen nun aus.

Der Trick vom 9. Juli: Abgelehnt – und trotzdem angenommen

314 dagegen · 276 dafür · 360 nötig zur Ablehnung

Abstimmung vom 9. Juli 2026: Die Mehrheit stimmte gegen die Verlängerung der Chatkontrolle 1. Zur Ablehnung fehlten dennoch 46 Stimmen, weil die absolute Mehrheit aller Abgeordneten nötig war, nicht die der Anwesenden. Ergebnis: Die Verlängerung gilt als angenommen.

Im März 2026 lehnte das EU-Parlament die Verlängerung der Chatkontrolle 1.0 klar ab (311 : 228 Stimmen), und die Regelung lief am 3. April aus. Damit schien das Thema erledigt. Solange, bis Parlamentspräsidentin Metsola es per Eilverfahren zurück auf die Tagesordnung setzte: terminiert auf den letzten Sitzungstag vor der Sommerpause.

Der Kern des Tricks liegt in der zweiten Lesung des Gesetzgebungsverfahrens (Art. 294 AEUV). Dort kehrt sich die Logik um: Der Standpunkt des Rates gilt automatisch als angenommen, wenn ihn nicht die **absolute Mehrheit aller 719 Abgeordneten** aktiv ablehnt. Wer im Urlaub ist, zählt damit faktisch wie eine Ja-Stimme für das Gesetz.

Spieltheoretisch ein Lehrbuchfall von optimierter Regelanwendung: Wer Verfahrensstufe und Zeitpunkt wählt, wählt die Mehrheitsregel mit und damit das Ergebnis. Abgeordnete rügten zudem, die Geschäftsordnung erlaube in der zweiten Lesung gar kein Dringlichkeitsverfahren. Immerhin: Ein angenommener Änderungsantrag nimmt verschlüsselte Inhalte vom Geltungsbereich aus. Der Text ging deshalb zurück an den Rat.

Sanktion ohne Urteil: Der Fall Jacques Baud

Der Schweizer Ex-Oberst wurde im Dezember 2025 wegen angeblich prorussischer Äußerungen per Ratsbeschluss auf die EU-Sanktionsliste gesetzt, und zwar ohne Anklage, ohne Anhörung, ohne Gericht. Folge: Konten gesperrt, Unterstützung ist strafbar. Erst nach Wochen kam eine humanitäre Ausnahme fürs Lebensnotwendigste. Sogar seine Schweizer UBS sperrte seine Karten. Rechtsschutz gibt es nur nachträglich, per Klage vor dem EU-Gericht, soweit das mit gesperrten Konten möglich ist.

Quellen: Blick, SRF, Infosperber (Feb. 2026)

Sind die Daten dort sicher, wo sie gesammelt werden müssen?

272.000 Ledger-Leak (2020): Namen, Telefonnummern und Wohnadressen von Krypto-Kunden landeten offen im Netz (plus 1,1 Mio. E-Mail-Adressen). Danach: Erpressungswellen mit Drohungen, zu Hause anzugreifen, unter Nennung der Wohnadresse; 171 Phishing-Seiten in zwei Monaten.

400 Mio. \$ Coinbase-Leak (2025): Kriminelle haben Support-Mitarbeiter bestochen und erbeuteten Namen, Adressen und Ausweisbilder. Geschätzte Schadenssumme bis 400 Mio. Dollar; Branchenvertreter warnen vor Entführungs- und Überfallrisiken für Betroffene.

215+ Physische Angriffe auf Krypto-Besitzer („Wrench Attacks“ = Folter) seit 2020. Die Fallzahl hat sich 2025 nahezu verdoppelt. Kriminelle suchen Opfer zu Hause auf und erpressen die Herausgabe der Schlüssel, teils mit Folter.

Selbst Informationen aus Hausdurchsuchungen sind schon an die Presse geraten.

Könnte man es besser machen?

Wenn überhaupt, dann Eingriffe nur bei konkretem Verdacht und mit Richtervorbehalt. Aber jede Scan-Infrastruktur braucht eine Hintertür, und die steht potenziell für alle offen. Wo Nachweise nötig sind: Zero-Knowledge-Verifikation, bei der die Eigenschaft (etwa das Alter) bewiesen wird, ohne die Identität preiszugeben. Alles andere schafft Datenberge, die Begehrlichkeiten wecken, sowohl bei Behörden als auch bei Kriminellen.

Es gilt die einfache Regel: Was missbraucht werden kann, wird auch irgendwann missbraucht.

Quellen & weiterführende Links

- Chatkontrolle, Abstimmung 9.7.2026: [netzpolitik.org](https://netzpolitik.org/de/freiwillige-chatkontrolle-geht-mit-verfahrenstrick-durch/) – „Freiwillige Chatkontrolle geht mit Verfahrenstrick durch“; [golem.de](https://golem.de/de/die-anlasslose-chatkontrolle-ist-wieder-da/) – „Die anlasslose Chatkontrolle ist wieder da“
- Chatkontrolle 2.0 / Trilog: [netzpolitik.org](https://netzpolitik.org/de/interne-dokumente-trilog-zur-chatkontrolle-geht-in-entscheidende-phase/) – „Interne Dokumente: Trilog zur Chatkontrolle geht in entscheidende Phase“ (2026)
- Priorisierung von Quellen: „European Democracy Shield“, JOIN(2025) 791 final (EUR-Lex); AVMD-Sondierung der Kommission (24.11.2025); § 84 Medienstaatsvertrag
- DMA / Android-Öffnung: [heise.de](https://heise.de/de/android-muss-fuer-ki-assistenten-von-fremdanbietern-komplett-oeffnen-16-7-2026) – „Android muss für KI-Assistenten von Fremdanbietern komplett öffnen“ (16.7.2026)
- Vorratsdatenspeicherung: [heise.de](https://heise.de/de/eu-fahrplan-fuer-entschluesselung-und-vorratsdatenspeicherung-steht-16-7-2026) „EU-Fahrplan für Entschlüsselung und Vorratsdatenspeicherung steht“; [netzpolitik.org](https://netzpolitik.org/de/going-dark-fahrplan/) – „Going Dark“-Fahrplan
- Vermögensregister: [wiwo.de](https://wiwo.de/de/entscheidung-ueber-eu-vermoegensregister-inkl-machbarkeitsstudie-juli-2024) – „Entscheidung über EU-Vermögensregister“ (inkl. Machbarkeitsstudie Juli 2024)
- Digitaler Euro: EZB-Rede „Der digitale Euro: Ein gemeinsamer Schritt“ (Nov. 2025) – Nicht-Programmierbarkeit, Bargeld bleibt
- Datenlecks: [theblock.co](https://theblock.co/ledger/) (Ledger); [coindesk.com](https://coindesk.com/ledger-leak-has-cascading-consequences/) – „Ledger Leak Has Cascading Consequences“; [onlinesicherheit.gv.at](https://onlinesicherheit.gv.at/coinbase/) (Coinbase); J. Lopp – „Known Physical Bitcoin Attacks“
- Fall Baud: [blick.ch](https://blick.ch/baud-erhaelt-beschränkten-kontozugriff/) – „Baud erhält beschränkten Kontozugriff“; [srf.ch](https://srf.ch/warum-die-eu-einen-schweizer-blockiert/) – „Warum die EU einen Schweizer blockiert“; infosperber.ch
- Eingangs-Comic erstellt von Sancho Bonanza