Stand: 07.09.2026 14:39:54

Vorgangsmappe für die Drucksache 19/12975

"Anlasslose digitale Chatkontrolle verhindern – Vertraulichkeit privater Kommunikation und sichere Ende-zu-Ende-Verschlüsselung schützen!"

Vorgangsverlauf:

1. Initiativdrucksache 19/12975 vom 21.07.2026
2. Plenarprotokoll Nr. 87 vom 23.07.2026

Bayerischer Landtag

19. Wahlperiode 21.07.2026 **Drucksache** 19/**12975**

Dringlichkeitsantrag

der Abgeordneten **Katrin Ebner-Steiner, Ulrich Singer, Christoph Maier, Richard Graupner, Andreas Winhart, Johannes Meier, Gerd Mannes, Benjamin Nolte, Markus Walbrunn, Dieter Arnold, Oskar Atzinger, Jörg Baumann, Franz Bergmüller, Martin Böhm, Rene Dierkes, Christin Gmelch, Daniel Halemba, Martin Huber, Andreas Jurca, Florian Köhler, Oskar Lipp, Stefan Löw, Roland Magerl, Ferdinand Mang, Harald Meußgeier, Johann Müller, Elena Roon, Franz Schmid, Ralf Stadler, Ramona Storm, Markus Striedl, Matthias Vogler** und **Fraktion (AfD)**

Anlasslose digitale Chatkontrolle verhindern – Vertraulichkeit privater Kommunikation und sichere Ende-zu-Ende-Verschlüsselung schützen!

Der Landtag wolle beschließen:

Die Staatsregierung wird aufgefordert, sich auf Bundes- und EU-Ebene dafür einzusetzen, dass

– von der Einführung einer allgemeinen, verdachtsunabhängigen und automatisierten Kontrolle privater digitaler Kommunikation durch Anbieter von Messenger-, E-Mail- oder sonstigen Kommunikationsdiensten Abstand genommen wird,

– weder die befristete Ausnahme von den Datenschutzbestimmungen der Richtlinie 2002/58/EG noch eine künftige dauerhafte europäische Regelung Anbieter dazu berechtigt oder verpflichtet, private Nachrichten, Bilder, Videos, Audiodateien oder sonstige Kommunikationsinhalte ohne konkreten, durch tatsächliche Anhaltspunkte begründeten Verdacht zu durchsuchen, zu analysieren oder an staatliche beziehungsweise private Stellen weiterzuleiten,

– Ende-zu-Ende-verschlüsselte Kommunikation ausnahmslos vor technischen Eingriffen geschützt wird und insbesondere keine gesetzlichen Vorgaben eingeführt werden, die eine Aufweichung, Umgehung oder faktische Abschaffung sicherer Verschlüsselungsverfahren durch sogenanntes Client-Side-Scanning, Hintertüren oder vergleichbare technische Maßnahmen zur Folge haben,

– Maßnahmen zur Bekämpfung der sexuellen Ausbeutung und des sexuellen Missbrauchs von Kindern auf gezielte, rechtsstaatlich kontrollierte Ermittlungen gegen konkret verdächtige Personen, die personelle und technische Stärkung der zuständigen Strafverfolgungsbehörden sowie die schnellere Löschung nachweislich rechtswidriger Inhalte konzentriert werden,

– Eingriffe in das Fernmeldegeheimnis und die Vertraulichkeit digitaler Kommunikation ausschließlich auf der Grundlage eines konkreten Tatverdachts, einer klaren gesetzlichen Ermächtigung, des Grundsatzes der Verhältnismäßigkeit und grundsätzlich einer vorherigen richterlichen Anordnung erfolgen,

– die Bundesregierung im Rat der Europäischen Union keiner Regelung zustimmt, die eine anlasslose Kontrolle privater Kommunikation ermöglicht, die Sicherheit verschlüsselter Kommunikation beeinträchtigt oder sämtliche Nutzer digitaler Kommunikationsdienste unter einen faktischen Generalverdacht stellt,

Drucksachen, Plenarprotokolle sowie die Tagesordnungen der Vollversammlung und der Ausschüsse sind im Internet unter www.bayern.landtag.de - Dokumente abrufbar. Die aktuelle Sitzungsübersicht steht unter www.bayern.landtag.de – Aktuelles/Sitzungen zur Verfügung.

– bei den weiteren Beratungen über eine europäische Regelung zur Bekämpfung des sexuellen Missbrauchs von Kindern ein transparentes Gesetzgebungsverfahren gewährleistet wird, in dem datenschutzrechtliche, verfassungsrechtliche, technische und kriminalpolitische Einwände umfassend berücksichtigt werden.

Begründung:

Der Schutz von Kindern vor sexueller Ausbeutung, sexuellem Missbrauch und der Verbreitung entsprechender Darstellungen ist eine zentrale Aufgabe des Rechtsstaates. Dieses legitime und notwendige Ziel darf jedoch nicht dazu führen, die private Kommunikation der gesamten Bevölkerung ohne konkreten Tatverdacht automatisiert zu durchsuchen. Die auf europäischer Ebene geplanten beziehungsweise verlängerten Regelungen werden in der öffentlichen und politischen Debatte daher zusammenfassend als „anlasslose digitale Chatkontrolle“ bezeichnet. Gemeint ist damit die automatisierte Untersuchung privater Nachrichten, Bilder, Videos, Audiodateien und sonstiger Kommunikationsinhalte durch Anbieter digitaler Dienste, obwohl gegen die betroffenen Nutzer keine konkreten tatsächlichen Anhaltspunkte für eine Straftat vorliegen. Eine solche flächendeckende Kontrolle stellt sämtliche Nutzer unter einen faktischen Generalverdacht und greift tief in das Fernmeldegeheimnis, den Datenschutz und die Vertraulichkeit digitaler Kommunikation ein. Kinderschutz und der Schutz elementarer Freiheitsrechte dürfen daher nicht gegeneinander ausgespielt werden.

Die sogenannte Chatkontrolle beruht bislang auf einer zeitlich begrenzten Ausnahme von bestimmten Vorschriften der europäischen Datenschutzrichtlinie für elektronische Kommunikation. Die Verordnung (EU) 2021/1232 gestattet Anbietern nummernunabhängiger interpersoneller Kommunikationsdienste, bestimmte Technologien zur freiwilligen Erkennung von Darstellungen sexuellen Kindesmissbrauchs und der Kontaktanbahnung gegenüber Kindern einzusetzen. Die vorangegangene Übergangsregelung lief am 3. April 2026 aus, nachdem sich das Europäische Parlament und der Rat nicht rechtzeitig auf eine weitere Verlängerung einigen konnten. Der Rat legte dem Parlament anschließend erneut eine Position vor, durch die die ausgelaufene Ausnahme faktisch wieder in Kraft gesetzt werden sollte.

Am 9. Juli 2026 stimmte das Europäische Parlament über einen Antrag auf Zurückweisung der Ratsposition zur erneuten Verlängerung der sogenannten Chatkontrolle ab. Für die Zurückweisung votierten 314 Abgeordnete, dagegen 276 Abgeordnete; 17 Abgeordnete enthielten sich. Obwohl damit eine klare Mehrheit der an der Abstimmung teilnehmenden Abgeordneten die Ratsposition ablehnte, scheiterte der Zurückweisungsantrag an der für die zweite Lesung geltenden absoluten Mehrheit von 360 Mitgliedern. In einer weiteren Abstimmung votierten 276 Abgeordnete für die Zurückweisung der geänderten Parlamentsposition, 286 dagegen und 30 enthielten sich; der geänderte Text wurde daraufhin an den Rat weitergeleitet. Dieses Ergebnis war nicht Ausdruck einer neuen politischen Mehrheit zugunsten der Chatkontrolle, sondern Folge der gewählten Verfahrenskonstruktion. Nachdem die Verlängerung zuvor bereits wiederholt keine parlamentarische Mehrheit gefunden hatte, wurde die inzwischen ausgelaufene Regelung auf Betreiben der EVP kurzfristig im Dringlichkeitsverfahren nach Art. 170 Abs. 6 der Geschäftsordnung des Europäischen Parlaments erneut auf die Tagesordnung gesetzt – unmittelbar vor der parlamentarischen Sommerpause und unter Verfahrensbedingungen, bei denen selbst eine deutliche Mehrheit der Abstimmenden die Vorlage nicht mehr mit einfacher Mehrheit zurückweisen konnte. Das Vorgehen mag formal auf die Geschäftsordnung gestützt worden sein; es widerspricht jedoch dem demokratischen Grundgedanken parlamentarischer Entscheidungsverfahren, wenn ein politisch unerwünschtes Abstimmungsergebnis durch eine kurzfristige Neuansetzung und die Nutzung einer erhöhten Mehrheitshürde faktisch überwunden wird. Dadurch entsteht der begründete Eindruck, dass nicht um eine neue inhaltliche Mehrheit geworben, sondern ein bereits mehrfach gescheitertes Vorhaben mithilfe verfahrenstechnischer Mittel doch noch durchgesetzt werden sollte. Zusätzlich wirft es Fragen nach der gebotenen politischen Transparenz auf, dass Parlamentspräsidentin Roberta Metsola, die das Verfahren leitete, erst wenige Wochen zuvor vom 26. bis 28. Mai 2026 im Silicon Valley mit Spitzenvertretern zahlreicher großer Technologieunternehmen zusammengetroffen

war. Angesichts der weitreichenden Auswirkungen der Regelung auf digitale Plattformen und Kommunikationsdienste wäre jedoch eine vollständige Offenlegung der Gesprächsinhalte und der dabei vertretenen Interessen erforderlich gewesen.

Besonders bemerkenswert ist das gegensätzliche Abstimmungsverhalten der bayerischen Regierungsparteien auf europäischer Ebene. Abgeordnete der CSU stimmten für die Fortführung der anlasslosen digitalen Chatkontrolle. Demgegenüber stimmten Abgeordnete der FREIEN WÄHLER für die Zurückweisung der Ratsposition und damit gegen die Fortführung der Chatkontrolle in der vorgelegten Form.

Die CSU muss sich daher den Vorwurf gefallen lassen, dass ihre Europaabgeordneten eine Regelung unterstützt haben, die erhebliche Gefahren für das Fernmeldegeheimnis, den Datenschutz und die Vertraulichkeit privater Kommunikation birgt. Das geschlossene Abstimmungsverhalten ihrer Vertreter steht zugleich in einem deutlichen Gegensatz zu früheren öffentlichen Aussagen führender Unionspolitiker gegen eine allgemeine Chatkontrolle. Es ist nicht überzeugend, im nationalen politischen Raum vor einer anlasslosen Überwachung privater Nachrichten zu warnen, während die eigenen Abgeordneten auf europäischer Ebene den Fortgang einer entsprechenden Regelung ermöglichen.

Die vom Europäischen Parlament vorgenommenen Änderungen, insbesondere der beabsichtigte Ausschluss von Kommunikation, auf die Ende-zu-Ende-Verschlüsselung angewendet wird oder werden soll, sind zwar grundsätzlich zu begrüßen, sie beseitigen jedoch nicht sämtliche rechtsstaatlichen und technischen Bedenken. Der weitere Gesetzgebungsprozess ist nicht abgeschlossen. Der Rat kann die Änderungen annehmen oder zurückweisen; nimmt er sie nicht vollständig an, schließt sich ein Vermittlungsverfahren zwischen Parlament und Rat an. Damit besteht weiterhin die Gefahr, dass Schutzvorschriften im weiteren Verfahren abgeschwächt oder technisch unzureichend ausgestaltet werden.

Eine automatisierte Durchsuchung privater Kommunikation unterscheidet nicht begründet und anlassbezogen zwischen Beschuldigten, sonstigen Verdächtigen und unbescholtenen Bürgern. Vielmehr werden sämtliche Nutzer eines betroffenen Dienstes einer technischen Kontrolle unterworfen. Damit wird die grundrechtlich gebotene Ausnahme – die Überwachung einer konkret verdächtigen Person unter rechtsstaatlich festgelegten Voraussetzungen – in ihr Gegenteil verkehrt. Nicht mehr der konkrete Verdacht löst eine Überwachungsmaßnahme aus. Vielmehr wird die gesamte Kommunikation vorsorglich untersucht, um möglicherweise einen Verdacht zu erzeugen.

Dies berührt insbesondere das durch Art. 10 Abs. 1 des Grundgesetzes geschützte Brief-, Post- und Fernmeldegeheimnis sowie die unionsrechtlich gewährleisteten Rechte auf Achtung des Privat- und Familienlebens und auf Schutz personenbezogener Daten nach Art. 7 und Art. 8 der Charta der Grundrechte der Europäischen Union. Eingriffe in diese Rechte müssen gesetzlich bestimmt, zur Erreichung eines legitimen Ziels geeignet und erforderlich sowie im engeren Sinne verhältnismäßig sein. Eine flächendeckende und verdachtsunabhängige Untersuchung privater Nachrichten begegnet vor diesem Hintergrund erheblichen Bedenken, weil sie nicht auf einen begrenzten Kreis konkret verdächtiger Personen beschränkt bleibt.

Hinzu kommen erhebliche technische Risiken. Ende-zu-Ende-Verschlüsselung schützt private Kommunikation, Geschäftsgeheimnisse, journalistische Quellen, anwaltliche und ärztliche Vertraulichkeit sowie staatliche und unternehmerische Informationssysteme. Eine technische Schwächung dieses Schutzes würde nicht ausschließlich Strafverfolgungsbehörden zugutekommen. Einmal geschaffene Schwachstellen können ebenso von ausländischen Nachrichtendiensten, kriminellen Vereinigungen, Wirtschaftsspionen und sonstigen Angreifern ausgenutzt werden. Die Sicherheit verschlüsselter Kommunikation ist daher kein Hindernis für den Rechtsstaat, sondern ein wesentlicher Bestandteil der digitalen Sicherheit von Bürgern, Unternehmen und staatlichen Einrichtungen.

Auch ein sogenanntes Client-Side-Scanning löst dieses Problem nicht. Dabei werden Inhalte bereits auf dem Endgerät untersucht, bevor sie verschlüsselt versandt werden. Die Verschlüsselung des Übertragungsweges bliebe formal bestehen, die Vertraulichkeit der Kommunikation würde jedoch vor der Verschlüsselung durchbrochen. Eine solche Konstruktion käme funktional einer Umgehung sicherer Ende-zu-Ende-

Verschlüsselung gleich und könnte zugleich eine technische Infrastruktur schaffen, deren Anwendungsbereich später auf weitere Delikte oder Inhaltskategorien ausgeweitet werden könnte.

Ein wirksamer Kinderschutz erfordert stattdessen zielgerichtete Maßnahmen. Hierzu gehören eine bessere personelle und technische Ausstattung der Ermittlungsbehörden, eine engere internationale Zusammenarbeit, die konsequente Verfolgung identifizierter Täter, die Auswertung bereits vorhandener Verdachtsmeldungen, die schnelle Sicherung und Löschung nachweislich illegaler Inhalte sowie eine wirksame Präventions- und Opferhilfe. Diese Maßnahmen richten sich gegen Täter und konkrete Gefahren, ohne die private Kommunikation der gesamten Bevölkerung einem pauschalen Kontrollsystem zu unterwerfen.

Die Staatsregierung ist deshalb aufgefordert, auf Bundes- und EU-Ebene eine eindeutige Position gegen jede Form der anlasslosen Chatkontrolle einzunehmen. Der Schutz von Kindern muss mit rechtsstaatlichen, zielgerichteten und technisch tragfähigen Mitteln gewährleistet werden. Eine allgemeine Durchleuchtung privater Kommunikation, die Schwächung sicherer Verschlüsselung und die Behandlung sämtlicher Bürger als potenzielle Verdächtige sind mit einem freiheitlichen Rechtsstaat nicht vereinbar.

Redner zu nachfolgendem Tagesordnungspunkt

Präsidentin Ilse Aigner

Präsidentin Ilse Aigner: Keine weiteren Wortmeldungen liegen mir vor. Die Dringlichkeitsanträge auf den Drucksachen 19/12975 mit 19/12977 werden im Anschluss an die heutige Sitzung in den jeweils zuständigen federführenden Ausschuss verwiesen und dort beraten.