FDP Weilburg

# VORRATSDATENSPEICHERUNG – 11 ARGUMENTE, WARUM WIR SIE IN EINER FREIHEITLICHEN GESELLSCHAFT NICHT BRAUCHEN

03.02.2026

Das Thema ist wichtig, sogar wichtiger denn je. Die FDP steht auf der Seite der Freiheit, der Demokratie. Auch in Weilburg. Deshalb teilen wir gerne diesen jüngsten Beitrag von Charlotte Zeller in vollem Wortlaut. Erstmalig ist der Beitrag am 27.01.2026 unter https://www.freiheit.org/de/deutschland/vorratsdatenspeicherung-11-argumente-warum-wir-sie-einer-freiheitlichen-gesellschaft erschienen.

***Immer wieder versuchen politische Kräfte, die anlasslose Vorratsdatenspeicherung einzuführen – trotz hoher rechtlicher Hürden und breiter Kritik. 11 Argumente, die gegen die anlasslose Speicherung privater Daten sprechen.***

Die Vorratsdatenspeicherung verpflichtet Telekommunikations- und Internetanbieter, Verbindungs- und Standortdaten systematisch und massenhaft zu speichern – und das ohne konkreten Anlass oder Verdacht. Dieses kriminalpolitische Instrument ist seit den 2000er Jahren immer wieder politisch und rechtlich gescheitert. Gerichte erklärten Regelungen zur anlasslosen Vorratsdatenspeicherungen wiederholt für grundrechts- und europarechtswidrig. Trotzdem wächst der politische Druck für eine Wiedereinführung der Vorratsdatenspeicherung, insbesondere der Speicherung von IP-Adressen, sowohl auf Bundesebene als auch auf EU-Ebene.

Elf zentrale Argumente gegen die Vorratsdatenspeicherung zeigen, warum diese Maßnahme nicht in eine freiheitliche Gesellschaft passt:

**1. Bürger stehen unter Generalverdacht**

Grundpfeiler eines demokratischen Rechtsstaates ist, dass der Staat für Ermittlungen

einen konkreten Anlass braucht. Mit der Vorratsdatenspeicherung werden aber alle Menschen unter Generalverdacht gestellt – unabhängig davon, ob sie verdächtig sind oder nicht.

**2. Vorratsdatenspeicherung beschränkt die persönliche Freiheit – Menschen verhalten sich anders**

Freiheit bedeutet, sich ohne Angst vor Überwachung bewegen und kommunizieren zu können – auch im Internet. Die meisten Menschen kommunizieren online, der private und berufliche Alltag spielt sich immer mehr im Internet ab. Deshalb gewähren Verkehrsdaten immer tiefere Einblicke in Verhalten und Leben der Menschen. Fühlen Menschen sich ständig überwacht, verhalten sie sich anders, selbst in alltäglichen Situationen. Sie zögern, ihre Meinung offen zu äußern oder unbefangen nach Informationen zu suchen.

**3. Menschen zögern, vertrauliche und wichtige Beratungsgespräche zu führen**

Denn auch, wenn die Inhalte der Kommunikation nicht gespeichert werden, reichen die Metadaten oft für Rückschlüsse auf das Verhalten, das Umfeld oder die Gedankenwelt einer Person aus. Allein die Tatsache, dass jemand einen Strafverteidiger, Onkologen oder Suchtberater aufsucht, erlaubt Rückschlüsse auf sehr persönliche, oft sensible Themen. Diese rechtlich besonders schützenswerten Kontakte werden bei der Vorratsdatenspeicherung technisch bedingt mitgespeichert. Dies kann dazu führen, dass Menschen Beratung und Hilfe meiden, aus Angst vor negativen Konsequenzen.

**4. Journalistische Quellen zögern aus Angst vor Entdeckung**

Besonders gefährdet ist die Arbeit von Journalisten, vor allem von freien Journalisten ohne institutionelle Anbindung. Anders als Rechtsanwälte oder Ärzte haben sie keine zentrale Berufsanerkennung, die ihnen pauschal einen besonderen Schutzstatus gewährt. Die Vorratsdatenspeicherung kann dazu führen, dass Informanten aus Angst vor Entdeckung zögern, Missstände oder brisante Informationen preiszugeben.

**5. Kumulierte Überwachungslast**

Überwachungsmaßnahmen wirken nicht isoliert, sondern greifen ineinander und verstärken sich wechselseitig – etwas, dass der Gesetzgeber berücksichtigen muss, wenn er neue Überwachungsmaßnahmen einführen will. Wie hoch die tatsächliche Überwachungslast ist, ist unklar. Die Überwachungsgesamtrechnung soll dies offenlegen,

damit der Gesetzgeber informierte Entscheidungen treffen kann. Es sollte uns zu denken geben, wenn Überwachungsbefürworter, die Überwachungsgesamtrechnung ablehnen.

**6. Überwachung wird als normal und unvermeidlich wahrgenommen**

Die schrittweise Ausweitung von Überwachungsmaßnahmen hat Überwachung normalisiert. Heute wird Überwachung ganz anders gesprochen als noch bei der Volkszählung von 1983. Überwachung wird zunehmend als unvermeidlich oder sogar normal wahrgenommen. Eine Gesellschaft, in der der demokratische Raum Schritt für Schritt unbemerkt eingeengt werden kann, ist verwundbar – denn sie erkennt den schleichenden Verlust von Freiheit erst, wenn es zu spät ist.

**7. Die Gefahr des Missbrauchs und der Zweckentfremdung ist hoch**

Wenn Daten gespeichert werden, besteht immer das Risiko von Missbrauch – auch in Staaten wie Deutschland in denen "Recht und Gesetz" gelten. Dies zeigen etwa die Vielzahl unberechtigter Datenabfragen durch Polizisten. Zwar können Richtervorbehalte und Protokollpflichten einen gewissen Schutz bieten, doch ein Restrisiko bleibt. In Zeiten, in denen über potentielle autoritär-populistische Regierungen und die Verwundbarkeit unserer Demokratie gesprochen wird, sollten wir auch bedenken, wie Bestimmungen und Befugnisse vom Staat gegen unsere Demokratie und unseren Rechtsstaat missbraucht werden können.

**8. Daten werden in Datenlecks oder Cyberangriffen missbraucht**

Die zentrale Speicherung großer Mengen sensibler Daten schafft ein erhebliches Sicherheitsrisiko, da ein zentraler Angriffspunkt t entsteht. Datenlecks und Cyberangriffe sind keine Seltenheit – und Verkehrsdaten sind auch für Kriminelle und autoritäre Regime attraktiv.

**9. Vorratsdatenspeicherung hilft wenig, um Kriminalität zu bekämpfen**

Die Vorratsdatenspeicherung bringt kaum messbaren Nutzen für die Kriminalitätsbekämpfung. Ermittlungsbehörden arbeiten auch ohne sie erfolgreich, indem sie bestehende Methoden gezielt nutzen. In Deutschland bleiben Verkehrsdatenabfragen – auch ohne Vorratsdatenspeicherung – selten erfolglos: Selbst bei Missbrauchsdarstellungen im Netz, auf die Ermittlungsbehörden nur durch Hinweise aus den USA aufmerksam werden, sind IP-Adressen nur im einstelligen Prozentbereich nicht abfragbar

. Zudem liefern Verkehrsdaten oft nicht den erhofften Erfolg. Dann nämlich, wenn Personen ihre Identität verschleiern (z. B. durch unregistrierte, gestohlene oder gekaperte SIM-Karten, öffentliche oder ungeschützte WLAN oder Anonymisierungsdienste wie Virtual Private Networks (VPN), Proxys oder Tor).

**10. Rechtsunsicherheit**

Ermittlungsbehörden brauchen rechtssichere Mittel zur Straftatbekämpfung – die Vorratsdatenspeicherung bietet diese Sicherheit jedoch nicht. Auch die jüngste Entscheidung des Europäischen Gerichtshofes (EuGH) ändert daran wenig. Zwar erlaubt der EuGH die Speicherung von IP-Adressen ausdrücklich, aber nur unter strengen Bedingungen zum Schutz der Privatsphäre. So darf die Speicherung nur für eine „auf das absolut Notwendige begrenzte Dauer“ erfolgen. Da der EuGH die genaue Speicherdauer offenlässt, bleibt das Risiko, dass auch eine IP-Vorratsspeicherung wieder vor Gericht scheitert.

**11. Es gibt grundrechtsschonendere Alternativen!**

Die Vorratsdatenspeicherung ist nicht alternativlos: Das weniger invasive Quick-Freeze-Verfahren bietet eine rechtsichere Option. Dafür setzte sich der damalige Bundesjustizminister Marco Buschmann zuletzt mit einem ressortabgestimmten Referentenentwurf ein. Dabei werden Daten nicht auf Vorrat gespeichert, sondern erst wenn ein Straftatverdacht besteht. Im ersten Schritt ordnet die Behörde an, dass der Provider relevante Daten umgehend einfriert und neu anfallende speichert. Im zweiten Schritt können die Daten abgerufen werden, sobald sich der Verdacht gegen eine Person konkretisiert.