VERBAND DER INTERNETWIRTSCHAFT E.V.

LEITLINIEN

Vorratsdatenspeicherung

Berlin, 23.10.2025

Seit fast zwei Jahrzehnten steht die Vorratsdatenspeicherung (VDS) im Spannungsfeld zwischen Sicherheitsinteressen und Grundrechtsschutz. eco – Verband der Internetwirtschaft e. V. hat über viele Jahre maßgeblich dazu beigetragen, dass verfassungs- und europarechtswidrige Regelungen zur anlasslosen Datenspeicherung gestoppt wurden. Mit dem jüngsten EuGH-Urteil C-470/21 ist erneut deutlich geworden, dass eine anlasslose und flächendeckende Vorratsdatenspeicherung unvereinbar mit europäischem Recht bleibt. Dennoch plant die Bundesregierung, eine IP-Adressenspeicherung von bis zu drei Monaten einzuführen.

eco setzt sich weiterhin für eine rechtskonforme, verhältnismäßige und technisch umsetzbare Lösung beim Zugriff auf Daten von Bürger:innen ein. Dabei dürfen weder die Grundrechte gefährdet, noch das Vertrauen in digitale Dienste untergraben werden. Beides wäre für die Internetwirtschaft in Deutschland schädlich. Folgende Punkte müssen aus Sicht von eco bei weiteren Beratungen zum neuen Gesetzentwurf berücksichtigt werden:

1. Rechtssicherheit schaffen

Die vergangenen 15 Jahre haben gezeigt, dass jede pauschale Form der Vorratsdatenspeicherung früher oder später vor Gericht scheitert. Das jüngste EuGH-Urteil bestätigt, dass eine Speicherung nur unter engen Voraussetzungen zulässig ist, etwa bei konkretem Verdacht schwerer Straftaten und nur mit strikter Zweckbindung und Kontrolle. Ein geplanter neuer nationaler Ansatz muss klare, präzise und technische Schutzmechanismen enthalten, die eine missbräuchliche Nutzung ausschließen. Rechtssicherheit ist die Voraussetzung für Vertrauen sowohl bei Bürger:innen als auch bei Unternehmen. Eine erneute Auflage eines grundrechtswidrigen Gesetzes wäre ein Rückschritt.

2. Verhältnismäßige Speicherfristen

Aus Sicht der Ermittlungs- und Sicherheitsbehörden – darunter das Bundeskriminalamt (BKA) – zeigt sich, dass eine Speicherung von IP-Adressen über einen Zeitraum von etwa zwei bis drei Wochen hinaus nicht mehr merklich zur Aufklärung beiträgt. Eine deutlich längere Speicherung bedeutet hingegen einen größeren Eingriff in Grundrechte, höhere technische und organisatorische Kosten sowie ein gesteigertes Risiko von Missbrauch oder Fehlzuordnung von Informationen durch Sicherheitsbehörden. Vorzugswürdig ist eine zweckgebundene, zeitlich streng begrenzte Datensicherung. Alternativ kann das sogenannte „Quick Freeze-Verfahren“ Anwendung finden, das den Eingriff in Freiheitsrechte systematisch reduziert. Dieser Ansatz ermöglicht einen tragfähigen Ausgleich zwischen legitimen Sicherheitsinteressen und dem Schutz der persönlichen Freiheitsrechte. Die gesetzliche Regelung zur Speicherung von Verbindungs- oder IP-Daten sollte daher auf maximal zwei bis drei Wochen begrenzt werden. Speicherfristen darüber hinaus sind aus Sicht einer rechtsstaatlichen Bewertung und unter dem Aspekt der Verhältnismäßigkeit nicht zu legitimieren.

3. Vermeidung wirtschaftlicher Mehrbelastung

Die Einführung einer flächendeckenden Vorratsdatenspeicherung verursacht für Anbieter erhebliche Investitions- und Betriebskosten. Es müssen zusätzliche Speicher- und Serverinfrastrukturen aufgebaut, höhere IT-Sicherheitsstandards umgesetzt und wie in früheren Gesetzentwürfen vorgesehen gesetzlich vorgeschriebene Dienste (z. B. ein 24/7 Rechts- oder Compliance-Dienst) eingerichtet werden. Aus Erfahrungen früherer Vorhabensphasen lässt sich ableiten, dass solche Maßnahmen oft zu Preiserhöhungen für Endkund:innen, Wettbewerbsnachteilen für kleinere Anbieter und erhöhtem bürokratischem Aufwand führen. Ohne einen angemessenen Kostenausgleich für betroffene Anbieter und realistische, praktikable Umsetzungsfristen kann eine solche Pflicht zur Datenspeicherung die Wirtschaft überfordern sowohl technisch als auch finanziell. Wenn Kosten und Aufwand über das hinausgehen, was Unternehmen sinnvoll tragen können, drohen negative Nebenwirkungen für Infrastruktur, Preise und Marktvielfalt.

4. Datenschutz und Missbrauchsrisiken

Das Risiko von Datenlecks, Missbrauch oder Fehlzuordnungen durch Sicherheitsbehörden steigt mit wachsendem Umfang und Zeitraum der Datenspeicherung. Bei einer verpflichtenden Speicherung von IP-Adressen und Portnummern entsteht kein rein technischer Vorgang, sondern ein großer Bestand sensibler Metadaten (z. B. wer wann mit welcher IP über welchen Port kommuniziert). Solche Metadaten lassen sich mit weiteren Informationsbeständen (z. B. Standortdaten, Kundenkonten, Zahlungsinformationen) verknüpfen und ermöglichen Rückschlüsse auf persönliche Verhaltensmuster, Gewohnheiten oder Netzwerke. So können Einzelinformationen zusammen ein detailliertes Bild einer Person ergeben. Neue Sicherheitsversprechen dürfen daher nicht zur Sicherheitslücke werden, wenn Schutzmechanismen versagen.

5. Zweifel an Effektivität

Es gibt keine belastbaren empirischen Belege, dass die Vorratsdatenspeicherung zu einer signifikanten Steigerung der Aufklärungsraten führt. Professionelle Täter:innen umgehen solche Maßnahmen leicht bspw. durch VPNs, Anonymisierungsdienste oder das Darknet. Eine massenhafte Datenspeicherung aller Bürger:innen schafft daher viel Aufwand bei geringem Ertrag.
Statt ineffizienter Massenüberwachung sollte der Fokus auf den gezielten Einsatz digitaler Ermittlungsinstrumente und eine bessere internationale Zusammenarbeit gelegt werden.
