

ECKPUNKTE

zur Vorratsdatenspeicherung | Aktuelle politische und rechtliche Entwicklungen

Berlin, 12.06.2025

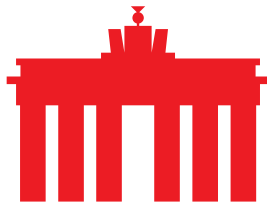
Seit 2006 steht die Vorratsdatenspeicherung (VDS) im Zentrum der Debatte um Sicherheit und Freiheit in der digitalen Gesellschaft. eco sieht in vertrauenswürdigen digitalen Diensten eine Grundlage für eine erfolgreiche Digitalisierung. Vertrauenswürdig können diese vor allem sein, wenn Bürger:innen vor unverhältnismäßiger staatlicher Überwachung sicher sind. Daher beobachtet eco derzeit die Entwicklung der Diskussion um die Vorratsdatenspeicherung sowohl auf nationaler als auch europäischer Ebene. Insbesondere die Pläne der neuen Bundesregierung, die laufende Konsultation der Europäischen Kommission zum Thema sowie das jüngste Urteil des Europäischen Gerichtshofs (EuGH) in der Rechtssache [C-470/21](#) sind besorgniserregende Signale.

1. Politischer Hintergrund und EU-Konsultation

Der Koalitionsvertrag der regierenden Parteien CDU, CSU und SPD sieht die Einführung einer „verhältnismäßigen und europa- und verfassungsrechtskonformen Speicherpflicht für IP-Adressen und Portnummern“¹ vor. Damit wird auf nationaler Ebene bereits zum vierten Mal die jahrelange Diskussion zur Vorratsdatenspeicherung entfacht. Innenminister Dobrindt wagte Mitte Mai einen ersten Vorstoß und kündigte die massenhafte Speicherung aller IP-Adressen und Portnummern an. Auch auf europäischer Ebene wird das Thema wieder lauter. Im Mai 2025 startete die Europäische Kommission eine öffentliche Konsultation zur Vorratsdatenspeicherung im Rahmen eines geplanten [Impact Assessments \(Ares\(2025\)4081079\)](#). Ziel ist es, eine mögliche EU-weite Harmonisierung der Speicherung sogenannter „non-content data“ für Zwecke der Strafverfolgung zu prüfen. Dazu zählen etwa IP-Adressen, Zeitstempel und Standortdaten. Die Kommission verweist auf Schwierigkeiten bei der grenzüberschreitenden Strafverfolgung und auf die Notwendigkeit einer einheitlichen Rechtslage. Eine solche Harmonisierung würde jedoch fundamentale Fragen der Verhältnismäßigkeit und Grundrechtskonformität aufwerfen.

Die Kommission verweist zwar explizit auf die Rechtsprechung des EuGH, insbesondere auf die Anforderungen an Zugangsbeschränkungen und Transparenz. Gleichzeitig bleibt unklar, wie eine neue Regelung konkret ausgestaltet werden soll, ohne erneut in Konflikt mit Artikel 7, 8 und 11 der Charta der Grundrechte der Europäischen Union zu geraten. Die Gefahr einer schleichenden Normalisierung massenhafter Überwachung unter dem Deckmantel der *gezielten und zeitlich begrenzten Speicherung* ist evident.

¹ https://www.koalitionsvertrag2025.de/sites/www.koalitionsvertrag2025.de/files/koav_2025.pdf, S. 82., Z. 2630.



2. Bisherige Rechtsprechung des EuGH zur Vorratsdatenspeicherung

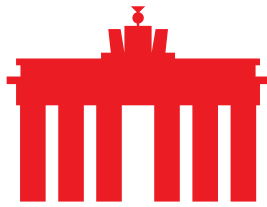
Die Rechtsprechung des EuGH setzt enge Grenzen für nationale Regelungen zur anlasslosen Vorratsdatenspeicherung. Maßgeblich ist dabei Artikel 15 der e-Privacy-Richtlinie, der in Verbindung mit der EU-Grundrechtecharta angewendet wird. Daraus ergeben sich zentrale Anforderungen an die Zulässigkeit solcher Maßnahmen. Im Grundsatz gilt danach der Schutz der Vertraulichkeit. Elektronische Kommunikation und damit verbundene Daten (z. B. IP-Adressen, Verbindungs- oder Standortdaten) sind grundsätzlich vertraulich. Ihre Speicherung ist laut EU-Recht nur in engen Ausnahmefällen zulässig bspw. zur Abwehr konkreter Gefahren oder zur Verfolgung schwerer Straftaten. Eine pauschale Vorratsspeicherung ohne Anlass stellt stets einen Eingriff in Grundrechte dar. Der EuGH stellt klar, dass bereits die Speicherung auf Vorrat die Grundrechte auf Privatleben und Datenschutz verletzt. Dabei ist es unerheblich, ob die Daten später tatsächlich genutzt werden oder nicht. Besonders kritisch ist die Möglichkeit, aus gespeicherten Daten genaue Bewegungs- oder Verhaltensprofile zu erstellen. Dies kann auch abschreckende Effekte auf die Meinungsfreiheit entfalten.

Eingriffe dieser Art und Intensität können nur unter bestimmten Bedingungen gerechtfertigt werden. Dazu zählen ein legitimer Zweck von hohem öffentlichem Interesse (z. B. nationale Sicherheit, Schutz vor schwerer Kriminalität) und ein angemessenes Verhältnis zwischen Eingriffsintensität und Schwere der Bedrohung. Je gravierender der Eingriff in ein Grundrecht, desto gewichtiger muss das verfolgte Ziel sein. Während leichte Eingriffe unter Umständen auch mit dem Ziel der allgemeinen Strafverfolgung gerechtfertigt sein können, erfordern schwerwiegende Eingriffe wie die umfassende Speicherung von IP-Adressen regelmäßig den Schutz der nationalen Sicherheit oder die Bekämpfung schwerer Straftaten.

Der EuGH verlangt eine enge Zweckbindung und eine strikte Verhältnismäßigkeitsprüfung. Die Datenspeicherung muss geeignet, erforderlich und auf das absolut Notwendige begrenzt sein. Nationale Regelungen müssen zudem objektive Kriterien vorgeben, wann welche Daten gespeichert und genutzt werden dürfen. Um unionsrechtlich Bestand zu haben, müssen nationale Vorschriften zur Vorratsdatenspeicherung durch klare und präzise gesetzliche Regeln abgesichert sein. Sie müssen wirksame Schutzvorkehrungen gegen Missbrauch enthalten und sicherstellen, dass sowohl die Speicherung als auch der spätere Zugang zu den Daten kontrolliert und rechtsstaatlich abgesichert erfolgen. Die bloße Tatsache, dass auf die Daten nur unter bestimmten Bedingungen zugegriffen werden kann, genügt nicht, denn schon die Speicherung selbst bedarf einer eigenständigen Rechtfertigung.

3. Neuere Rechtsprechung: EuGH – Urteil C-470/21

Mit [Urteil vom 30. April 2024 \(C-470/21\)](#) hat der EuGH eine französische Regelung zur Speicherung von IP-Adressen durch die Behörde Hadopi bewertet. Dabei hat er seine bisherige Rechtsprechung zur Vorratsdatenspeicherung präzisiert und differenziert weiterentwickelt. Gegenstand war die Frage, ob die allgemeine und unterschiedslose



Speicherung von IP-Adressen zur Verfolgung von Straftaten im Allgemeinen mit dem Unionsrecht vereinbar ist.

Der EuGH hat klargestellt, dass nicht jede allgemeine Vorratsspeicherung von IP-Adressen automatisch als schwerwiegender Eingriff in die Grundrechte zu werten ist. Entscheidend ist, ob aus den gespeicherten Daten z.B. durch Verknüpfung mit weiteren Verkehrs- oder Standortdaten Rückschlüsse auf das Privatleben der Betroffenen möglich sind. Solche tiefgehenden Profile sind im konkreten Fall auszuschließen, um den Eingriff als weniger gravierend zu qualifizieren.

Damit eine Speicherung zur Bekämpfung von Straftaten im Allgemeinen gerechtfertigt sein kann, verlangt der Gerichtshof strenge technische und organisatorische Vorgaben. Insbesondere muss eine klare Trennung zwischen IP-Adressen, Identitätsdaten und sensiblen Kommunikationsdaten gewährleistet sein. Nur wenn diese Trennung wirksam und dauerhaft kontrolliert wird, kann die Speicherung ohne schwere Grundrechtseingriffe erfolgen und damit auf weniger gewichtige Gemeinwohlziele gestützt werden.

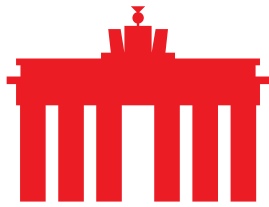
Auch im Urteil C-470/21 bleibt der Grundsatz der Verhältnismäßigkeit zentral. Der EuGH betont, dass der Zugriff auf die gespeicherten Daten nur erfolgen darf, wenn dies im Einzelfall notwendig ist und einem legitimen Zweck dient wie etwa der Identifikation von Tätern bei Online-Delikten. Gleichzeitig muss sichergestellt werden, dass dieser Zugriff nur von autorisierten Stellen unter klaren Bedingungen erfolgt.

Aus Sicht des eco bedeutet das Urteil keineswegs eine Kehrtwende, sondern eine Konkretisierung und Differenzierung der bisherigen Rechtsprechung. Die bisherige Unterscheidung zwischen leichten und schweren Eingriffen bleibt erhalten. Neu ist, dass eine allgemeine IP-Adressenspeicherung nicht automatisch als schwerer Eingriff qualifiziert wird, vorausgesetzt, dass durch gesetzliche und technische Vorgaben eine missbräuchliche Nutzung und die Erstellung von Persönlichkeitsprofilen ausgeschlossen werden können. Die Messlatte für die Schwere des Eingriffs bleibt somit hoch, ebenso das Erfordernis klarer, präziser und technisch abgesicherter gesetzlicher Regelungen. Damit setzt der EuGH die Hürden für eine verfassungskonforme Vorratsdatenspeicherung weiterhin sehr hoch.

Für den nationalen Gesetzgeber bedeutet das, dass eine pauschale Speicherung von IP-Adressen unter bestimmten Voraussetzungen mit dem Unionsrecht vereinbar sein kann, allerdings nur dann, wenn enge Grenzen eingehalten, effektive Schutzmechanismen etabliert und klare Verwendungszwecke definiert werden. Auch für den Zugang zu diesen Daten gelten abgestufte Anforderungen wie bspw. die Notwendigkeit einer unabhängigen Kontrolle bei wiederholten Zugriffen.

4. Anlasslose Datenspeicherung: Kritik und Gefahren

Die anlasslose Speicherung von Kommunikationsdaten stellt einen erheblichen Eingriff in die Grundrechte dar. Wie bereits in den Urteilen [Digital Rights Ireland \(C-293/12\)](#) und [La Quadrature du Net \(C-511/18 u.a.\)](#) festgestellt, ermöglichen Metadaten weitreichende



Rückschlüsse auf das Privatleben bis hin zur Erstellung detaillierter Bewegungs- und Sozialprofile. Der EuGH hat wiederholt betont, dass Vorratsdatenspeicherung nicht bloß eine Maßnahme zur Datensicherung, sondern ein eigener Grundrechtseingriff ist, der strengen verfassungsrechtlichen Maßstäben unterliegt.

Die Vorstellung, dass IP-Adressen per se weniger sensibel seien, verkennt die Realität moderner Datenanalyse. In Verbindung mit anderen öffentlich zugänglichen Informationen lassen sich aus IP-Daten hochindividuelle Profile erstellen. Dies widerspricht dem Grundsatz der Datenminimierung und dem Prinzip der Zweckbindung (vgl. Art. 5 DSGVO).

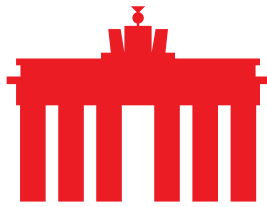
Auch Missbrauchs- und Fehleranfälligkeit gespeicherter Daten dürfen nicht außer Acht gelassen werden. Je größer und länger Kommunikationsdaten auf Vorrat gespeichert werden, desto höher sind die Risiken von Datenmissbrauch, Sicherheitslücken oder falschen Rückschlüssen bei der Nutzung. Der EuGH betont daher, dass schon die Speicherung durch klare gesetzliche Vorgaben und technische Schutzmaßnahmen abgesichert sein muss. In der Praxis sind diese Anforderungen in vielen nationalen Regelungen nicht eingehalten worden.

Darüber hinaus fehlen weitgehend empirische Belege dafür, dass die anlasslose Vorratsdatenspeicherung einen entscheidenden Beitrag zur Bekämpfung schwerer Kriminalität leistet. Vor allem der tatsächliche Nutzen und das Verhältnis zum Aufwand der Speicherung sollten kritisch hinterfragt werden. Effiziente Strafverfolgung ist auch ohne pauschale Datenspeicherung möglich. Diese kann vor allem durch gezielte Maßnahmen im Einzelfall oder durch zeitlich und sachlich begrenzte Sicherungen (z. B. „Quick-Freeze“-Verfahren) erreicht werden.

5. Fazit

Die Diskussion um Vorratsdatenspeicherung wird in den kommenden Monaten sowohl auf nationaler Ebene durch die Pläne des Innenministeriums, als auch auf europäischer Ebene durch das laufende Impact Assessment und die angekündigte Konsultation weiter an Fahrt gewinnen. Dabei hat der EuGH mit seinem jüngsten Urteil erneut deutlich gemacht, dass die Speicherung von IP-Adressen nur unter strengsten technischen, rechtlichen und organisatorischen Vorgaben erfolgen darf wie bspw. durch die wirksame Trennung von Datenkategorien, eine enge Zweckbindung, unabhängige Kontrolle und den Schutz vor Profilbildung. Eine echte „anlasslose“ Vorratsdatenspeicherung im unionsrechtlichen Rahmen lässt sich so faktisch kaum rechtssicher ausgestalten.

Die pauschale Vorratsdatenspeicherung ist rechtlich riskant, grundrechtlich bedenklich und sicherheitspolitisch unverhältnismäßig. Statt massenhafter Überwachung der europäischen und deutschen Bürger:innen bedarf es gezielter, rechtsstaatlicher Maßnahmen zur Strafverfolgung, die im Einklang mit der Grundrechtecharta stehen. Der EuGH liefert hierfür mit seiner differenzierten Rechtsprechung klare Leitplanken. Es ist jetzt an der Zeit, ein klares zivilgesellschaftliches und politisches Gegengewicht zu setzen. Die in Jahrzehnten etablierten Grundsätze des Datenschutzes und das Recht auf



VERBAND DER INTERNETWIRTSCHAFT E.V.



informationelle Selbstbestimmung dürfen in der Gesamtabwägung nicht hinter die Effizienz der Strafverfolgungsbehörden rücken.

Über eco: Mit rund 1.000 Mitgliedsunternehmen ist eco (www.eco.de) der führende Verband der Internetwirtschaft in Europa. Seit 1995 gestaltet eco maßgeblich das Internet, fördert neue Technologien, schafft Rahmenbedingungen und vertritt die Interessen seiner Mitglieder gegenüber der Politik und in internationalen Gremien. eco hat Standorte in Köln, Berlin und Brüssel. eco setzt sich in seiner Arbeit vorrangig für ein leistungsfähiges, zuverlässiges und vertrauenswürdiges Ökosystem digitaler Infrastrukturen und Dienste ein.