GESELLSCHAFT
FÜR INFORMATIK

Berlin, 29. Januar 2026

Stellungnahme

der Gesellschaft für Informatik e. V. (GI)

# Zu dem Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren

Stand 21.12.2025

GESELLSCHAFT
FÜR INFORMATIK

Die Gesellschaft für Informatik e.V. nimmt Stellung zum Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz vom 21.12.2025 zur Einführung einer Speicherpflicht für IP-Adressen und Portnummern. Dieser sieht eine dreimonatige anlasslose Speicherung von IP-Anschlussidentifizierung sowie ein Quick-Freeze-Verfahren für Verkehrs- und Funkzellendaten vor.

## Grundsätzliche Einschätzung

Fast jede Aktivität mit digitalem Bezug heutzutage erzeugt eine Datenspur: Im Netz zeichnen Datenströme ein präzises Bild unseres Handelns nach. Die Speicherung dieser teilweise sensiblen Daten kreiert eine Nachverfolgbarkeit und trägt damit zur Schaffung eines gläsernen Menschen bei. Das anlasslose Speichern von Bestandsdaten zum Zweck der Strafverfolgung, auch unterhalb der Schwelle der anlasslosen Speicherung von Verkehrsdaten, dringt tief in die Privatsphäre Unschuldiger ein und stellt jede Person unter Generalverdacht. **Aus Sicht der GI ist die flächendeckende, anlasslose Einführung einer IP-Adressenspeicherung vollständig auszuschließen.**

Grundsätzlich muss gefragt werden, ob eine zusätzliche Form der staatlichen Überwachung durch eine Speicherung von Verkehrsdaten überhaupt erforderlich ist. Aktivitäten lassen sich bereits durch private Datenabflüsse im Alltag zum Teil rekonstruieren. Studien zeigen, dass die Aufklärungsquote einiger Straftaten im digitalen Raum auch ohne das vorgeschlagene Instrument sehr hoch ist[1]. Strafverfolgungsbehörden verfügen bereits jetzt über ausreichend Instrumente zur Strafverfolgung und Aufklärung, welche sie zunächst vollständig ausschöpfen sollten, anstatt weitergehende Befugnisse zu fordern.

Eine funktionierende Demokratie setzt eine Bewegungs-, Versammlungs- und Meinungsäußerungsfreiheit voraus. Bereits die Möglichkeit einer Überwachung schreckt Bürger*innen von der Wahrnehmung ihrer grundrechtlich geschützten Freiheiten ab. Zum Schutz einer funktionierenden Zivilgesellschaft ist es daher notwendig, die Verhältnismäßigkeit einer einzelnen Überwachungsmaßnahme in Relation zum Kontext der gesamten nationalstaatlichen und EU-weiten Überwachung zu betrachten.

Die Einführung einer anlasslosen Speicherung von IP-Adressen würde in überproportionalem Maße unbescholtene Bürger*innen treffen, da diese mehrheitlich keine Schutzmechanismen nutzen, während Täter*innen in Vorbereitung ihrer Tat eine Speicherung der IP-Adresse ihres Anschlusses technisch leicht vermeiden können (z.B. durch TOR oder VPNs). Aufgrund dessen bleibt äußerst fraglich, ob eine Speicherung der IP-Adressen überhaupt in nennenswertem Umfang Fälle schwerer Straftaten erkennen und aufdecken könnte.

[1] vgl. u.a. https://web.archive.org/web/20160304041513/https://vds.brauchts.net/mpi_vds_studie.pdf; "Digitaler Betrug und Erpressung" von Anna Biselli, Ivan Gudymenko und Thorsten Strufe in: Michael Freytag (Hg.) Betrug in der digitalisierten Welt Erkennen. Vorbeugen. Schützen (2019); vgl. u.a. https://www.vorratsdatenspeicherung.de/images/rechtsgutachten_grundrechtecharta.pdf;

## Datenschutzrechtliche und grundrechtliche Aspekte

Die anlasslose Speicherung von IP-Adressen birgt schwerwiegende Risiken für Datenschutz und Grundrechte. Der Europäische Gerichtshof (EuGH) hat 2022 klargestellt, dass eine allgemeine und unterschiedslose Speicherung von Verkehrs- und Standortdaten mit der EU-Grundrechtecharta unvereinbar ist. Das Bundesverwaltungsgericht hat 2023 bestätigt, dass die deutsche Regelung unionsrechtswidrig ist und nicht angewendet werden darf. Bereits 2010 bewertete das Bundesverfassungsgericht die anlasslose Speicherung als „besonders schweren Eingriff". Auch das jüngste EuGH-Urteil von 2024 ändert daran im Kern nichts: Es bestätigt strenge Grenzen und lässt allenfalls eng begrenzte, technisch strikt getrennte Lösungen für IP-Adressen zur reinen Identifizierung ohne Profilbildung unter wirksamen Garantien zu[2], die auf den vorliegenden Gesetzesentwurf Anwendung finden. Zugleich betont der Gerichtshof die Gefahren für Privatheit, Datenschutz und Meinungsfreiheit. **Aus Sicht der GI ist aufgrund der grundrechtlichen Gefahren eine allgemeine und unterschiedslose Speicherung von Bestandsdaten abzulehnen. Mindestens jedoch müsste zwingend eine scharfe Trennung der IP-Adressspeicherung von anderen persönlichen Daten im Rahmen des Gesetzesentwurfs erfolgen.**

Aus Sicht der GI haben die erheblichen technischen Bedenken, die die GI mehrfach geäußert wurden, weiterhin Bestand: Die massenhafte Speicherung hochsensibler Daten schafft zentrale Angriffspunkte für Cyberkriminalität.[3] Bereits einzelne Sicherheitslücken können zu massiven Datenlecks führen, deren Folgen irreversibel wären. Hinzu kommt, dass die schiere Datenmenge nicht grundsätzlich eine höhere Qualität der Strafverfolgung verspricht – vielmehr droht eine Überlastung durch Datenmassen[4], die nur schwerlich unter Beachtung von Datenschutz- und Souveränitätsstandards auswertbar sind, während gleichzeitig erhebliche Risiken für Missbrauch und Fehlinterpretationen entstehen[5]. Sollte eine Vorratsdatenspeicherung eine sichere Identifizierung auch bei Verwendung von Carrier-Grade NAT ermöglichen, wäre hierfür potenziell noch eine viel umfangreichere Datenspeicherung erforderlich, die Rückschlüsse auf genutzte Dienste und letztlich eine detaillierte Profilbildung ermöglichen kann, was dem Urteil des EuGH entgegensteht. Carrier-Grade NAT wird als Verfahren von Internetserviceanbietern genutzt, um die Zahl der benötigten öffentlichen IPv4-Adressen zu reduzieren, indem die IPv4-Adressen z.B. von mehreren Kunden in eine einzige öffentliche IP-Adresse übersetzt werden. Dies erschwert – abhängig von der konkreten Umsetzung – die sichere Identifizierung einzelner Anschlussinhaber mittels der öffentlichen IP-Adresse ohne eine o.g. umfassende Datenspeicherung. Die Internetserviceanbieter können dem durch eine Anpassung ihrer Implementierung von Carrier-Grade NAT begegnen. Der vorliegende Entwurf adressiert diese Notwendigkeit einer datensparsamen Umsetzung und den möglicherweise entstehenden Umsetzungsaufwand jedoch nicht.

---

[2] https://curia.europa.eu/juris/document/document.jsf?text=&docid=285361&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1

[3] https://edri.org/wp-content/uploads/2025/06/Joint-civil-society-response-to-the-Commissions-call-for-evidence-on-Data-Retention.pdf

[4] https://netzpolitik.org/2025/europol-bericht-zu-cybercrime-europol-kaempft-mit-der-datenflut/

[5] https://gi.de/fileadmin/GI/Positionen/2025-08-12_GI_Stellungnahme_BfDI_Konsultation_Umgang_mit_personenbezogenen_Daten_in_KI-Modellen_fnl.pdf

Ob deutsche Internetserviceanbieter bereits eine Implementierung verwenden, die datensparsames Logging ermöglicht[6], ist der GI nicht bekannt.

Vor dem Hintergrund dieser IT-Sicherheitsbedenken ist nicht ersichtlich, warum der Art. 6 des neuen Entwurfs statt der skizzierten weniger invasiven Lösung direkt von einer dreimonatigen Speicherung ausgeht. Selbst wenn von einer Notwendigkeit einer Vorratsdatenspeicherung zur Identifizierung von Internetnutzern ausgegangen würde, sollte jedenfalls die Speicherdauer möglichst kurz gewählt werden. Die GI sieht keine hinreichende Evidenz für die im Gesetzentwurf vorgesehene dreimonatige Speicherung. In einem Positionspapier des BKA[7] heißt es konkret mit Bezug zum sog. NCMEC-Verfahren: „Gemessen an den wahrscheinlichsten Fallkonstellationen wäre eine Speicherverpflichtung von 2 bis 3 Wochen auch bei besonderen (terroristischen) Gefahrenlagen regelmäßig ausreichend und damit ein signifikanter Sicherheitsgewinn“. Das wird auch anhand von Fallzahlen untermauert; bei 14 Tagen Speicherdauer geht man von einer erfolgreichen Zuordnung von 84,5% der angefragten IP-Adressen aus, was sich bei 21 Tagen auf 88,4% steigern ließe. Das gleiche Positionspapier weist auf Bedarfslagen hin, die eine längere Speicherdauer erfordern könnten, benennt aber keine Untersuchungen, die diesen Befund stützen. Nach Überzeugung der GI wäre eine Speicherung über drei Monate ohne überzeugende empirische Begründung abzulehnen, auch wenn die Notwendigkeit einer Speicherverpflichtung an sich bejaht würde.

## Eingriffsschwellen für den Zugriff auf IP-Adressen

Im Gesetzesentwurf ist zur Abfrage von IP-Adressen bei Anlassbezug keinerlei Richtervorbehalt vorgesehen. Berichte aus der Ermittlungspraxis zeigen hingegen, dass sogar der Mechanismus des doppelten Richtervorbehalts nicht ausreicht, um den Missbrauch von Überwachungsmaßnahmen vollständig abzuwehren, besonders bei politischen Protestbewegungen. Die Möglichkeit der Anordnung durch Ermittlungspersonen, häufig selbst Polizeibeamte, nach Art. 1 Nr. 4 des Gesetzesentwurfs sowie Bedienstete des BKA gemäß Art. 10 Nr. 2 stellt angesichts der invasiven Natur der Datenspeicherung keine angemessene Hürde dar. Der erste Richtervorbehalt würde Strafverfolgungsbehörden ermöglichen, für ihre Ermittlung möglicherweise notwendige Daten für einen begrenzten Zeitraum zu sichern, während der zweite Richtervorbehalt erfordert, konkret zu ermitteln, für welche Personen ein Auftauen der Daten zu Ermittlungszwecken benötigt wird. **Vor diesem Hintergrund ist es aus Sicht der GI nicht zu rechtfertigen, einen Zugriff auf IP-Adressen ohne jeglichen Richtervorbehalt und Anlassbezug gesetzlich zu ermöglichen.**

Die GI begrüßt zwar, dass eine Sicherungsanordnung sowie die Funkzellenabfrage von vornherein nur eingeschränkt und anlassbezogen eingesetzt werden dürfen. Gleichzeitig kritisiert die GI, dass bereits bei dem Verdacht auf das künftige Begehen einer Straftat eine Sicherungsanordnung nach Art. 10b Nr. 2 (künftiger §10b Abs. 1 Nr. 2 BKAG) des Gesetzesentwurfs verfügt werden kann. Weiterhin beinhaltet der Gesetzesentwurf keine ausreichenden Garantien gegen den Missbrauch der zwei Instrumente und keine Evaluation der Maßnahmen. In diesem Zusammenhang warnt die GI insbesondere vor

[6] Etwa in Anlehnung an RfC 7422, https://www.rfc-editor.org/rfc/rfc7422
[7] Bundeskriminalamt, Erforderliche Speicherung von IP-Adressen, https://www.bka.de/SharedDocs/Downloads/DE/AktuelleInformationen/240118_Mindestspeicherfrist_IP-Adressen.pdf?__blob=publicationFile&v=9 (Seite 7).

den Risiken, die durch die Speicherungspflicht entstehen. So kann diese sogenannte „Chilling Effects“ auslösen, bei welchen Bürger*innen aus Angst vor staatlicher Überwachung und Kontrolle die Wahrnehmung ihrer Freiheitsrechte wie Meinungs- und Versammlungsfreiheit einschränken. Weiterhin spricht sich die GI dafür aus, dass sowohl die ursprüngliche Sicherungsanordnung als auch die Verlängerung unbedingt unter dem Vorbehalt eines Richterbeschlusses stehen sollten.

## Zielgerichtete und grundrechtskonforme Alternativen, z.B. das Quick-Freeze-Verfahren

Die GI fordert dazu auf, stattdessen alternative, zielgerichtete und grundrechtskonforme Ansätze bei konkretem Verdacht zu entwickeln. Innerhalb der deutschen Bundesregierung wurde bereits 2024 ein Quick-Freeze-Verfahren als mögliche grundrechtskonforme Ausgestaltung einer Vorratsdatenspeicherung diskutiert. Diese sollte anstelle einer anlass- und unterschiedslosen Speicherung zumindest eine zeitliche, räumliche und sachbezogene Begrenzung beinhalten. So sollten im Verdachtsfall Strafverfolgungsbehörden Telekommunikationsanbieter auffordern können, die Verkehrsdaten von Verdächtigen von schweren Straftaten und Personen in deren sozialen und beruflichen Umfeld zu speichern („Einfrieren“). Verkehrsdaten umfassen u.a. Rufnummern, Angaben über Beginn und Ende einer Verbindung und ggf. Standortdaten oder die übermittelte Datenmenge und werden bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt. Im Quick-Freeze-Entwurf von 2024 wurde den Behörden noch einen Monat Zeit gegeben, weitere Erkenntnisse zu sammeln und ein „Auftauen“ der Daten zu erwirken, um diese auszuwerten. Diese Frist sollte zweimal um jeweils einen Monat verlängert werden können. Beide Schritte hätten unter dem Vorbehalt eines Richterbeschlusses stehen sollen.

Angesichts jahrelanger Auseinandersetzungen und breiter gesellschaftlicher Kritik an einer unverhältnismäßigen Einschränkung der informationellen Selbstbestimmung durch eine präventive Speicherpflicht von Metadaten ist bezeichnend, dass die Bundesregierung plant, einen neuen Entwurf der Vorratsdatenspeicherung zu unternehmen. Eine anlassbezogene IP-Adressspeicherung in Kombination mit einem Quick-Freeze-Verfahren kann zwar eine Alternative zur anlasslosen Vorratsdatenspeicherung sämtlicher Verkehrsdaten sein. Die damit einhergehende Überwachung, die neben Straftäter*innen auch Unschuldige treffen kann, die zur falschen Zeit am falschen Ort waren, sowie der entstehende Eindruck von der Möglichkeit einer Überwachung, verlieren trotz einem abgeschwächtem Vorschlag dabei nicht an Bedeutung.

## Fazit

Aus Sicht der GI ist aus grundrechtlicher und technischer Perspektive die Einführung einer anlasslosen Speicherung von IP-Adressen weder gerechtfertigt noch verhältnismäßig. Sie gefährdet insbesondere durch fehlende Garantien Grundrechte und schafft IT-Risiken ohne einen bedeutend hohen Sicherheitsgewinn. Vor diesem Hintergrund sollten Strafverfolgungsbehörden zunächst das bereits bestehende Instrumentarium vollständig nutzen und anwenden sowie deren Effizienz prüfen, bevor die Einführung weitgehender neuer Befugnisse gefordert wird, ohne deren Effekt auf den Ermittlungserfolg klar benennen zu können. Die GI weist mit Sorge darauf hin, dass eine Speicherung jeglicher Verkehrsdaten mehr die Gefahr eines Überwachungsinstruments als ei-

nes sinnvollen Werkzeugs der Strafverfolgung birgt. Vor diesem Hintergrund fordert die GI, dass die geäußerten Sorgen hinsichtlich der Konsequenzen für Grundrechte und das Recht auf Privatsphäre ernst genommen werden und eine Umsetzung des Quick-Freeze-Verfahrens datenminimierend und anlassbezogen in Kombination mit hohen Sicherheitsstandards, richterlicher Kontrolle und klar definierten Eingriffsschwellen in den Blick genommen wird.

GESELLSCHAFT
FÜR INFORMATIK

## Über die Gesellschaft für Informatik e. V. (GI)

Die Gesellschaft für Informatik e.V. (GI) ist die größte Fachgesellschaft für Informatik im deutschsprachigen Raum. Seit 1969 vertritt sie die Interessen der Informatikerinnen und Informatiker in Wissenschaft, Gesellschaft und Politik und setzt sich für eine gemeinwohlorientierte Digitalisierung ein. Mit 14 Fachbereichen, über 30 aktiven Regionalgruppen und unzähligen Fachgruppen ist die GI Plattform und Sprachrohr für alle Disziplinen in der Informatik. Die GI hat sich Ethische Leitlinien gegeben, die ihren Mitgliedern als Orientierung dienen. Weitere Informationen finden Sie unter www.gi.de.