BREKO
Bundesverband
Breitbandkommunikation e.V.

Stellungnahme

Referentenentwurf zur Einführung einer IP-Adressspeicherung

I. Einleitung

Das BMJV hat am 22.12.2025 einen Gesetzentwurf zur *„Einführung einer IP-Adressdatenspeicherung und zur Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren“* veröffentlicht.

Der Gesetzentwurf sieht neben der Speicherung, Sicherung und Löschung von Daten im Zuge einer neu eingeführten Sicherungsanordnung nach § 100g Abs.7 StPO auch eine allgemeine dreimonatige Speicherpflicht für IP-Adressdaten vor. Gespeichert werden sollen

- Die dem Anschlussinhaber für eine Internetverbindung zugewiesene, öffentliche IP-Adresse
- Eine eindeutige Kennung des Anschlusses, über den die Internetverbindung erfolgt sowie eine zugewiesene Benutzerkennung
- Das Datum und die sekundengenaue Uhrzeit von Beginn und Ende der Zuweisung der öffentlichen IP-Adresse an einen Anschlussinhaber unter Angabe der jeweiligen Zeitzone
- Die der IP-Adresse zugehörigen Portnummern und weitere Verkehrsdaten, soweit diese für eine Identifizierung des Anschlussinhabers anhand einer zu einem bestimmten Zeitpunkt zugewiesenen IP-Adresse erforderlich sind

Die Mitgliedsunternehmen des BREKO erkennen das öffentliche Interesse an einer effektiven Strafverfolgung an und sind auch bereit, hierzu beizutragen.

Allerdings müssen die Belastungen für die Unternehmen in einem angemessenen Verhältnis zur Notwendigkeit und den Erfolgsaussichten der jeweiligen Maßnahmen stehen. Insgesamt ist darauf zu achten, dass die Unternehmen bei der Mitwirkung an der Erfüllung einer öffentlichen Aufgabe nicht überfordert werden. Die im Gesetzentwurf angelegten Form der IP-Adressdatenspeicherung genügt diesen Verhältnismäßigkeitsanforderungen allerdings nicht und würde gerade kleine und mittlere Netzbetreiber überfordern.

II. Erhebliche Aufwände für die Unternehmen bei Umsetzung der IP-Adressdatenspeicherung

Die IP-Adressdatenspeicherung führt so, wie sei im Gesetzentwurf angelegt ist, zu ungerechtfertigt hohen Aufwänden für die Unternehmen, ohne dass diese nach allen bisherigen Erfahrungen durch eine Entschädigung nach dem JVEG hinreichend kompensiert werden. Zudem ist das Verfahren für die Geltendmachung einer Entschädigung nach dem JVEG kompliziert und für die Unternehmen mit neuen Aufwänden verbunden. Hier wäre in jedem Fall eine angemessene und einfach umzusetzende Entschädigungslösung zu finden.

Für die Umsetzung der IP-Adressdatenspeicherung entstehen für die verpflichteten Anbieter erhebliche Aufwände, u.a:

- Technische Implementierung:
    - Einrichtung, Überwachung, Sicherung, Härten des dedizierten, von anderen Verkehrsdaten separierten IP-Servers, incl. Firewall etc.
    - Aufsetzen von Schnittstellen, u.a. für die tägliche Kopie der unterschiedlichen Abrechnungs-CDRs auf den Server für die IP-.Adressspeicherung
    - Aufsetzen einer technisch nachweisbaren fristgerechten und irreversiblen Löschung nach 3 Monaten
    - Integration von Such- und Exportfunktionen, die eine unverzügliche Übermittlung von Auskünften und Daten ermöglichen
    - Anbindung an Schnittstelle nach TKPÜV/TR TKÜV zur Datenübermittlung. Ggf sind Änderungen an de ´n bestehenden Schnittstellen/ETSI-ESB vorzunehmen.
    - Aufwand für den laufenden Betrieb, z.B. für den Betrieb der Server und Speichersysteme, der Pflege der Datenverbindungen zwischen verschiedenen Systeme, Monitoring, Wartung, Fehlerbehebung,
    - Umsetzung von Updates zur Zugriffskontrolle, Protokollierung der Zugriffe und technische Überwachung der fristgerechten und irreversiblen Löschung
    - Aufgrund der noch fehlenden Verordnung bzw. Technischen Richtlinie sind die Anforderungen an die Datensicherung noch nicht abzuschätzen

- Weitere einmalige Aufwände
    - Erarbeitung und Dokumentation eines Datenschutz- und Informationssicherheitskonzepts mit vorgelagerter Risikoanalyse
    - Entwicklung von Sicherheitsrollen- und Berechtigungskonzepten
    - Entwicklung von Löschkonzepten
    - Verfahrensdokumentation und Nachweisführung gegenüber Aufsichtsstellen

Die durch diese erheblichen Aufwände bei den Unternehmen entstehenden Kosten können verbandsseitig nicht allgemein beziffert werden, da sie von der besonderen Situation der jeweiligen Unternehmen abhängen – z.B. der vorhandenen Netzstruktur und IT-Landschaft, der Größe und dem Geschäftsmodell des Unternehmens und den Möglichkeiten zur Skalierung.

III. Carrier Grade NAT

Bei den oben dargestellten Aufwandspositionen sind bisher die besonderen Probleme außer Betracht geblieben, die durch den im Markt üblichen und angesichts der Knappheit öffentlicher IPv4-Adressen auch unverzichtbaren Einsatz von „Carrier Grade NAT“ (CGNAT) bedingt sind. Bei CGNAT teilen sich ggf. mehrere hundert Teilnehmer eine öffentliche IP-Adresse. Eine Unterscheidung erfolgt ausschließlich über die Portnummern. Je mehr Kunden ein ISP hat, desto mehr Kunden teilen sich die öffentliche IP-Adresse. Dies bedeutet aber nicht nur eine Vervielfachung der benötigten Speicherkapazitäten, sondern auch einen ganz erheblichen Mehraufwand durch die erforderliche Zuordnung, Erfassung und Abfrage von öffenticher IP-Adresse, interner Nutzer- und Anschlusskennung, Zeitstempel sowie Portdaten. Dadurch werden die Kosten der IP-Adressdatenspeicherung bei den Unternehmen massiv in die Höhe getrieben.

Der Gesetzentwurf geht offenbar von einer direkten Zuordnung der der Portnummer zu einem Nutzer aus (sog. „Cone-NAT“). In diesem Modell kann der Kunde aber lediglich ca. freie 250 Ports nutzen, was für die Nutzung moderner Webseiten oft nicht ausreichend ist.

Beim „Symmetric-NAT“ bekommt jede Verbindung zu einem Ziel-Server eine andere externe Portnummer, wodurch die Kapazität der nutzbaren Ports zwar erhöht wird, aber einerseits noch viel größere Datenmengen bewältigt und andererseits die Ziel-Server erfasst werden müssten. Die benötigte Information bei der Nutzung von „ Symmetric-NAT würde daher sein: *„Welcher Nutzer hatte zum Zeitpunkt x mit der IP y mit Port z eine Verbindung zum Ziel-Server a mit Port b“?*

Eine Information über den Ziel-Server wäre aber durch die neuere Rechtsprechung des EuGH nicht mehr gedeckt, weil aus dieser Information Persönlichkeitsprofile der Nutzer erstellt werden könnten (vgl. EuGH C470/21 v. 30.04.2024). Bereits die Speicherung von Portnummern an sich könnte fragwürdig sein, weil Portnummern in dem zitierten EuGH-Urteil nicht erwähnt werden.

IV. Nutzen der IP-Adressspeicherung?

Stehen auf der einen Seite sehr hohe und – für die Speicherung von im CGNAT-Verfahren generierte IP-Adressen derzeit kaum kalkulierbare - Kosten und mit Blick auf die EuGH-Rechtsprechung rechtliche Risiken, so stellt sich andererseits die Frage nach dem tatsächlichen Nutzen einer IP-Adressspeicherung für die Strafverfolgung.

Es spricht Vieles dafür, dass dieser Nutzen geringer ist, als im Gesetzentwurf unterstellt. Bereits heute haben die Strafverfolgungs- und die Gefahrenabwehrbehörden einen umfassenden Zugriff auf Verkehrsdaten. Die in den §§ 100g Abs.7 StPO, 175 TKG der Entwurfsfassung neu eingeführte Sicherungsanordnung bietet zudem die Möglichkeit, eine Löschung der beim Provider vorliegenden Daten für einen Zeitraum von 3 Monaten (mit einer dreimonatigen Verlängerungsmöglichkeit) zu verhindern.

Die Nutzung der auf Vorrat gespeicherten IP-Adressdaten setzt zudem den Aufbau erheblicher sachlicher und personeller Ressourcen mit entsprechendem IT-Kenntnissen bei den Strafverfolgungsbehörden voraus.

Entscheidend dürfte aber sein, dass Nutzer strafrechtlich relevanter Webseiten und krimineller Inhalte in der Regel über die Möglichkeiten informiert sein dürften, eine IP-Adressspeicherung zu umgehen (z.B. VPNs, Darknet, öffentliche Zugänge).

Vor diesem Hintergrund scheint der begrenzte Nutzen einer IP-Adressspeicherung die hohen Umsetzungsosten und die rechtlichen Unsicherheiten nicht zu überwiegen.

V. Lösungsvorschläge

Nach Auffassung des BREKO ist ein „Quick Freeze“-Verfahren einer IP-Adressdatenspeicherung vorzuziehen. Ein entsprechender Ansatz findet sich im Gesetzentwurf mit der Einführung einer Sicherungsanordnung. Mit der

Sicherungsanordnung wird den Strafverfolgungsbehörden ein taugliches Instrument zur Aufklärung schwerer oder mittels Telekommunikation begangener Straftaten.

Sollte die Bundesregierung gleichwohl an einer IP-Adressspeicherung festhalten wollen, müsste unter Verhältnismäßigkeitsgesichtspunkten darüber nachgedacht werden, CGNAT-Adressen von der Speicherung auszunehmen. Damit bestünden allerdings nur überschaubare Unterschiede zur gegenwärtigen Rechtslage.

In jedem Fall wäre aber angesichts der erheblichen Umsetzungsaufwände für die Unternehme eine „de-minimis-Regelung“ für kleinere und mittlere sowie neu in den Markt eintretende Unternehmen aufzunehmen, wie sie in anderen Regelungszusammenhängen im Telekommunikationsrecht bereits bestehen. So sind nach § 3 Abs.2 Nr.5 TKÜV Betreiber von der Telekommunikationsanlagen, an die nicht mehr als 10.000 Nutzer angeschlossen sind, von der Verpflichtung zur Telekommunikationsüberwachung ausgeschlossen.

VI. Einzelfragen

1. Definition des Merkmals „unverzüglich“

Der Gesetzentwurf verwendet an mehreren Stellen den Begriff *„unverzüglich“*. So sind nach § 175 Abs.2 Nr.3 und § 176 Abs.2 Nr.3 TKG des Entwurfs Daten so zu speichern, dass eine Übermittlung an die Strafverfolgungsbehörden *„unverzüglich“* erfolgen kann.

Nach § 175 Abs.2 Nr.4 bzw. § 176 Abs.2 Nr.4 TKG des Entwurfs sind die Daten nach dem „Stand der Technik *unverzüglich* irreversibel“ zu löschen.

Im Rahmen der Vorratsdatenspeicherung 2015 (§ 176 TKG a.F.) gab es einen Zusatz, wonach gespeicherte Daten *„unverzüglich, spätestens jedoch binnen einer Woche nach Ablauf der Speicherfristen irreversibel zu löschen“* sind. Eine entsprechende Klarstellung wäre auch im vorliegenden Gesetzentwurf wünschenswert. Wäre *„unverzüglich“* dagegen im Sinne einer Echtzeitanforderung zu verstehen, würde das erhebliche weitere Kosten auslösen.

2. Gemeinsame Speicherung mit Daten für die europäische Sicherungs- und Herausgabeanordnung

§ 176 Abs.3 TK des Entwurfs ermöglicht die gemeinsame Speicherung der IP-Adressdaten mit Daten, die im Rahmen der Europäischen Sicherungs- und

Herausgabeanordnung („E-Evidence-Verordnung“ EU 2023/1543) gespeichert werden.

Diese Maßnahme mag als Erleichterung für die TK-Anbieter und als kostenreduzierende Maßnahme gedacht sein, jedoch kann sie dies nicht leisten. In den beiden Regelungswerken bestehen unterschiedliche Speicher- und Löschfristen. Außerdem bezieht sich die geplante Gesetzgebung zur IP-Adressdatenspeicherung ausschließlich auf IP-Adressen bzw. die weiteren in § 176 Abs.1 TKG des Entwurfs genannten Daten, während die E-Evidence-VO deutlich weitgehender auf Verkehrs- und Inhaltsdaten abstellt.

Schließlich ist auch der Adressatenkreis bei beiden Normen unterschiedlich. Während sich der Entwurf zur IP-Adressspeicherung an Internetzugangsanbieter richtet, bezieht sich die E-Evidence-VO wiederum erheblich weitgehender auf alle Diensteanbieter.

Kostensenkende Synergien durch die gemeinsame Speicherung der Daten nach dem Gesetz zur IP-Adressspeicherung und Daten nach der E-Evidence-VO könnten nur dann eintreten, wenn insbesondere hinsichtlich der Speicher- und Löschfristen und der Art der zu speichernden Daten eine Anpassung der E-Evidence-VO an die deutsche Regelung zur IP-Adressdatenspeicherung erfolgen würde. Umgekehrt ist eine Synchronisierung der deutschen Regelung zur IP-Adressspeicherung an die E-Evidence-VO wegen der Restriktionen der EuGH-Rechtsprechung nicht möglich.

3. Vordienstleister und Reseller

Nicht wenige Netzbetreiber bieten Vorleistungen an, in dessen Rahmen sie Vorleistungsnachfragern den Zugang zum öffentlichen TK-Netz ermöglichen. Die Vorleistungsnachfrager bieten dann auf dieser Basis Zugänge zum Internet an. Hier wäre zu klären, in welchem Verhältnis Vordienstleistungsgeber und Vordienstleistungsnachfrager bzgl. der Verpflichtungen aus §§ 175, 176 TKG der Entwurfsfassung stehen. In der Regel wird der Vordienstleistungsnachfrager seine Verpflichtungen nicht ohne Mitwirkung des Vorleistungsgeber erfüllen können. Diesbezüglich wäre eine Klarstellung sinnvoll, wer in dieser Konstellation welche Verpflichtungen direkt oder indirekt zu erfüllen hat.

Dabei ist zu berücksichtigen, dass dem Vorleistungsgeber bei der Erfüllung oder der Mitwirkung bzgl. der Pflichten des Vorleistungsnachfragers weitere Kosten für die technische Datenhaltung entstehen, etwa für eine mandantenfähige Erfassung und Abfrage.

VII. Fazit

Zusammenfassend ist festzuhalten, dass insbesondere die Einführung einer IP-Adressspeicherung mit erheblichen, heute noch nicht abzuschätzenden Aufwänden für die Unternehmen verbunden ist. Dies gilt insbesondere mit Blick auf die Einbeziehung der öffentlichen IP-Adressen im CGNAT-Verfahren, die aufgrund der vielfach größeren Datenmengen ökonomisch nicht darstellbar und rechtlich unsicher ist.

Zudem sind die positiven Effekte der IP-Adreesspeicherung für die Strafverfolgung zweifelhaft. Der Gesetzentwurf sollte daher auf die Einführung einer Sicherungsanordnung beschränkt werden, durch die den Interessen der Strafverfolgungsbehörden in angemessener Weise Rechnung getragen wird.

Für Rückfragen oder eine tiefere Diskussion der in der Stellungnahme angesprochenen Punkte steht der BREKO gerne zur Verfügung.