

I. Einleitung

Der Verband der Anbieter im Digital- und Telekommunikationsmarkt e.V. (VATM) bedankt sich für die Gelegenheit, zu dem Regierungsentwurf für ein Gesetz zur Einführung einer Speicherpflicht für IP-Adressen und zur Weiterentwicklung der Befugnisse zur Datenerhebung in Strafverfahren Stellung nehmen zu können.

Der Regierungsentwurf greift mit der IP-Adressspeicherung, der Sicherungsanordnung und der Neuordnung weiterer digitaler Ermittlungsbefugnisse tief in die technischen, organisatorischen und wirtschaftlichen Abläufe der Telekommunikationsanbieter ein. Der VATM erkennt das Ziel an, Strafverfolgungsbehörden im digitalen Raum wirksame und rechtssichere Ermittlungsinstrumente zur Verfügung zu stellen. Zugleich ist jedoch festzuhalten, dass der Entwurf für die betroffenen Unternehmen erhebliche Umsetzungs-, Kosten- und Rechtsrisiken auslöst. Dies insbesondere vor dem Hintergrund, dass die Telekommunikationswirtschaft bereits mehrfach gesetzliche Vorgaben zur Vorratsdatenspeicherung umgesetzt hat, die letztlich vor den Gerichten keinen Bestand hatten.

Aus Sicht des VATM kann daher die Einführung einer Pflicht zur IP-Adressspeicherung nur dann tragfähig sein, wenn die Regelungen verhältnismäßig, technologieneutral, rechtssicher und praxistauglich ausgestaltet sind und angemessene Entschädigungsregelungen vorsehen. Der Regierungsentwurf enthält insoweit einzelne sachgerechte Ansätze, insbesondere die grundsätzlich technologieneutrale Formulierung der technischen Umsetzung. Er bleibt jedoch gleichzeitig an mehreren Stellen hinter den Anforderungen zurück, die für eine rechtssichere und wirtschaftlich zumutbare Umsetzung erforderlich sind. Dies gilt insbesondere für die Umsetzungsfristen, die Abgrenzung der verpflichteten Anbieter, die Behandlung unterschiedlicher Geschäftsmodelle, die Kostenkompensation sowie die Verzahnung mit bereits bestehenden und künftigen europäischen Vorgaben.

Der Referentenentwurf und die Kabinettsfassung lassen deutlich die Absicht erkennen, einen insgesamt ausgewogenen Ansatz zwischen den vom Gerichtshof der Europäischen Union (EuGH) formulierten Anforderungen ebenso zu berücksichtigen wie die geltenden verfassungsrechtlichen Grenzen. Dies vorweggenommen, sehen wir jedoch insbesondere bei den folgenden Punkten Klarstellungs- oder Änderungsbedarf.

II. Einzelne Anmerkungen

1. Keine, bzw. zu kurze Umsetzungsfristen

Einen wesentlichen Kritikpunkt aus Sicht des VATM stellen die Umsetzungsfristen dar, die als nicht realisierbar anzusehen sind.

Dies gilt zum einen für die **unmittelbare Geltung einzelner Regelungen**, insbesondere für die **Sicherungsanordnung** des Änderungsgesetzes, bereits mit Verkündung. Zum anderen ist auch die **Frist von sechs Monaten** nach Inkrafttreten des Änderungsgesetzes für die Umsetzung der IP-Adressspeicherung **deutlich zu kurz** bemessen.

a) Problem der unmittelbaren Geltung der Regelungen zur Sicherungsanordnung gem. § 176 TKG-E

Aus Sicht des VATM ist es höchst problematisch, dass die Regelungen zur Sicherungsanordnung ohne Umsetzungsfrist, unmittelbar mit Inkrafttreten des Gesetzes Geltung erlangen sollen. Nach unseren Informationen war für den Gesetzgeber hierfür die Annahme ursächlich, dass TK-Anbieter aufgrund der bereits im August in Kraft tretenden E-Evidence Verordnung, identische Sicherungsanordnungen umsetzen müssen und eine Notwendigkeit für weitere Umsetzungsfristen daher nicht gegeben ist. Tatsächlich fallen eine Vielzahl deutscher Telekommunikationsunternehmen unter eine Ausnahmeregelung des E-Evidence-Pakets, das nicht für Anbieter gilt, die ihre Dienste ausschließlich in Deutschland anbieten. Für diese Unternehmen ist eine gesonderte Umsetzungsfrist zur Erfüllung der Verpflichtungen im Kontext mit Sicherungsanordnungen unbedingt erforderlich.

b) Sechsmontatige Umsetzungsfrist zu knapp bemessen

Gerade vor dem Hintergrund, dass eine Vorratsdatenspeicherung in der Vergangenheit bereits zwei Mal gescheitert ist und die Adressaten der Speicherverpflichtungen entsprechende finanzielle Belastungen zu tragen hatten, dürfen Implementierungsmaßnahmen erst dann getroffen werden, wenn **die rechtlichen Vorgaben erlassen sind. Zwingend sollten daher zum einen zunächst die Anpassungen der TKÜV und TR TKÜV vorliegen**, bevor eine entsprechende Frist beginnt (vgl. § 175 Abs. 3 TKG E).

Nach dem Zeitplan der BNetzA soll die Überarbeitung der TKÜV im November mit Veröffentlichung abgeschlossen sein. Frühestens dann – vorausgesetzt, der parlamentarische

Prozess für das Gesetz zur IP-Datenspeicherung ist dann auch abgeschlossen – sollten Implementierungsfristen beginnen zu laufen.

Zum anderen ist auch aus technischen Gründen eine sechsmonatige Umsetzungsfrist zu kurz bemessen. **Neubeschaffung von Software, Lieferkettenprobleme, Umbauten in TK-Netzen und auch in der IT** (IT-Zyklen sind zu beachten) sowie **die Abnahme und Qualitätssicherung** führen dazu, **dass eine Umsetzung innerhalb von sechs Monaten unmöglich ist**. Ganz konkret lässt sich in diesem Kontext anführen, dass die Verfügbarkeit von Speicher (SSD und DRAM) aktuell kritisch ist. Die Hersteller haben beispielsweise bereits die gesamte Produktion 2026 von SSDs vollständig verkauft. Verwiesen werden kann in diesem Zusammenhang auch auf die IT-NRW. Diese steht im Bereich E-Evidence aus den gleichen Gründen vor Problemen mit der Bereitstellung der zentralen IT-Infrastruktur, obwohl hier die gesetzlichen Grundlagen bereits seit längerem bekannt sind.

2. Klarstellungs- und Änderungsbedarf bei § 177 TKG-E

§ 177 TKG-E verpflichtet nun erstmalig alle Anbieter von Internetzugangsdiensten zur Speicherung von IP-Adressen unabhängig von der Frage, ob sie die Zuweisung von IP-Adressen auch selbst vornehmen oder nicht. Erläuternd möchten wir an dieser Stelle darauf hinweisen, dass die Zuweisung von IP-Adressen eine technische und eine zeitliche Komponente enthält. Anbieter von Internetzugangsdiensten ohne eigenes Netz nehmen selbst keine Zuweisung von IP-Adressen vor und kennen weder die IP-Adresse noch den Zeitpunkt der Zuweisung und damit den Beginn der Speicherpflicht. Insofern geht auch die Gesetzesbegründung richtigerweise verschiedentlich davon aus, dass nur Anbieter mit einem Netz adressiert werden sollen. Undifferenziert alle Anbieter zu verpflichten, bringt dagegen keinen sicherheitstechnischen Mehrwert, führt aber zu Mehrfachspeicherungen und unnötigen Kosten und Aufwänden. Insofern sprechen wir uns an dieser Stelle klar dafür aus, die IP-Adressspeicherung auf Anbieter mit eigenem Netz zu begrenzen, da nur diese selbst IP-Adressen zuweisen.

Ferner ist der § 177 Abs. 2 TKG-E systematisch verfehlt und ohne Wirkung. Denn zum einen sind die Netzbetreiber bzw. Vorleister von Erbringern von Internetzugangsdiensten ohne eigene IP-Zuweisung (sog. Reseller) in aller Regel selbst Erbringer von

Internetzugangsdiensten und damit bereits über § 177 Abs. 1 TKG-E zur Speicherung der IP-Adressen verpflichtet. Einer Sicherstellung der Speicherung von IP-Adressen durch den Reseller bedarf es dann nicht. Zum anderen hinge eine entsprechende Sicherstellung durch den Reseller allein von einer vertraglichen Vereinbarung mit dem Vorleister über die IP-Speicherung ab. Die Vorleister sind aber durch den derzeitigen Gesetzentwurf gar nicht verpflichtet entsprechende Zusagen gegenüber den Resellern zu machen.

Daneben erwarten wir hinsichtlich der Umsetzung des vorliegenden Gesetzesentwurfs prozessuale Aufwände, insbesondere im Bereich des Intercompany-Geschäfts, welche zum jetzigen Zeitpunkt noch nicht abzuschätzen sind. Darüber hinaus können sich bei einer doppelten Speicherung durch den IP-Adress-Eigentümer und terminierenden/adressierenden ISP ggf. Differenzen in der Datensystematik ergeben. Dieser Umstand sollte vom Gesetzgeber mitberücksichtigt werden.

3. Besondere Betroffenheit spezialisierter Geschäftskundenprodukte und solcher mit statischer IP-Adressvergabe

Der Regierungsentwurf differenziert bislang nicht hinreichend zwischen den verschiedenen Produkten und technischen Realitäten der betroffenen Anbieter. Insbesondere reine Geschäftskundenprodukte sowie Angebote, die überwiegend oder ausschließlich mit statischen IP-Adressen arbeiten, sind anders betroffen als Massenmarktanbieter mit dynamischer IP-Adressvergabe im Endkundengeschäft.

Bei statisch vergebenen IP-Adressen stellt sich die technische und ermittlungspraktische Ausgangslage anders dar. Die Zuordnung einer IP-Adresse zu einem Anschluss oder Kunden ist regelmäßig nicht in gleicher Weise flüchtig wie bei dynamischen Adressvergaben. Der zusätzliche Erkenntnisgewinn einer allgemeinen Speicherpflicht kann daher deutlich geringer sein, während zugleich erhebliche Vorhalte-, Prüf-, Dokumentations- und Compliance-Aufwände entstehen können.

Der VATM hält es deshalb für erforderlich, die Speicherpflicht enger an den tatsächlichen technischen Anwendungsfall zu knüpfen. Verpflichtet werden sollten nur Anbieter, die IP-Adressen tatsächlich selbst dynamisch zuweisen und bei denen die Speicherung für eine

spätere Identifizierung des Anschlussinhabers erforderlich ist. Für Anbieter ohne dynamische IP-Adressvergabe, für reine Geschäftskundenanbieter sowie für Anbieter ohne eigenes Endkundennetz sollte der Gesetzgeber Ausnahmen, zumindest aber Übergangs- und Erleichterungsregelungen vorsehen.

Hilfsweise sollte geprüft werden, Anbieter, die keine dynamischen IP-Adressen zuteilen und keine Verbraucher im Massenmarkt adressieren, für einen angemessenen Zeitraum von der Umsetzung auszunehmen, solange kein konkreter Bedarf und keine verhältnismäßige Kosten-Nutzen-Bewertung für diese Anbietergruppe vorliegen.

4. Konkretisierung des Begriffs des „irreversiblen Löschens“

Der im Referentenentwurf an verschiedenen Stellen verwendete Begriff des „irreversiblen Löschens“ bedarf einer näheren Konkretisierung. Ohne eine gesetzliche oder zumindest normkonkretisierende Definition besteht die Gefahr erheblicher Rechtsunsicherheiten für die Verpflichteten, insbesondere im Hinblick auf technische Umsetzungsfragen und Prüfmaßstäbe.

5. Anpassungsbedarf bei § 100j StPO neu als Ermächtigungsgrundlage zur Erhebung von Bestandsdaten

Der neu zu fassende § 100j StPO stellt nach Auffassung des VATM keine taugliche und verfassungsgemäße Ermächtigungsgrundlage für die Erhebung von Bestandsdaten dar. Der Entwurf leidet – ebenso wie die derzeit geltende Fassung des § 100j StPO – daran, dass er die zuständige ersuchende Behörde nicht ausdrücklich benennt.

Telekommunikationsanbieter dürfen gemäß § 174 Abs. 2 Satz 1 TKG Auskünfte nur erteilen, wenn ihnen eine gesetzliche Bestimmung genannt wird, welche die ersuchende Stelle eindeutig bezeichnet. Diese Anforderung folgt nicht nur aus einfachem Recht, sondern ist auch verfassungsrechtlich zwingend. Das Bundesverfassungsgericht hat wiederholt klargestellt, dass eine hinreichend bestimmte Benennung der abrufberechtigten Behörden erforderlich ist (vgl. BVerfG, 1 BvR 1299/05, Rn. 171; 1 BvR 1873/13 sowie 1 BvR 2618/13, Rn. 137).

6. Keine Herabsenkung der JVEG-Entschädigungssätze

Kritisch sehen wir, dass die im JVEG enthaltenen Entschädigungssätze nicht an die allgemeine Preisentwicklung angepasst wurden. Vielmehr sieht § 23 JVEGneu in Verbindung mit Anlage 3 Nr. 507 sogar eine Absenkung von bisher 45 Euro auf 25 Euro für die Verlängerung der Speicherung gesicherter Daten vor.

Diesbezüglich fordert der VATM, die Absenkung rückgängig zu machen, da der Aufwand für eine Speicherung nicht allein deshalb niedriger wird, weil es sich um eine Verlängerung handelt.

Daneben sehen wir es sehr kritisch, dass das System derzeit kleine Anbieter mit wenigen Kunden gegenüber großen Anbietern benachteiligt. Hier sollte ein Entschädigungssystem gefunden werden, das den berechtigten Interessen aller Anbieter an einer Refinanzierung ihrer Investitionen gerecht wird.

7. Sensibilisierung für geopolitische Risiken im Zusammenspiel von Datenspeicherungen und E-Evidence

Der Regierungsentwurf verbindet mit der IP-Adressspeicherung und der Sicherungsanordnung zwei Instrumente, die unterschiedlichen regulatorischen Logiken folgen. Die IP-Adressspeicherung ist als allgemeine, vorsorgliche Speicherung ausgestaltet. Die Sicherungsanordnung ist demgegenüber ihrem Charakter nach ein anlassbezogenes Instrument zur vorübergehenden Sicherung bereits vorhandener Daten. Beide Instrumente tragen dazu bei, dass nach in Kraft treten des Gesetzes bisher nicht existente Daten-Poole entstehen. Wir möchten an dieser Stelle darauf hinweisen, dass künftig auch Justizbehörden aus dem EU-Ausland Zugriff auf diese Daten bekommen und für die damit einhergehenden geopolitischen Risiken sensibilisieren.

Das Bundesverfassungsgericht hat mit der Doppeltürtheorie einen verfassungsrechtlichen Rahmen geschaffen, der bei staatlichen Zugriffen auf Telekommunikationsdaten zwei voneinander unabhängige Eingriffsstufen identifiziert: Die anlasslose Speicherung der Daten durch private Telekommunikationsanbieter einerseits und den behördlichen Abruf dieser Daten andererseits. Beide Eingriffe bedürfen jeweils einer eigenständigen, verhältnismäßigen

Rechtsgrundlage. Dieses Modell wurde in einer Zeit entwickelt, in der der Zugriff auf gespeicherte Vorratsdaten im Wesentlichen durch inländische Behörden auf Grundlage nationaler Abrufnormen erfolgte. Bei einer etwaigen Neueinführung einer Verpflichtung zur Vorratsdatenspeicherung kann diese Prämisse jedoch nicht mehr uneingeschränkt aufrechterhalten werden. Denn mit dem Inkrafttreten der E-Evidence-Verordnung (Verordnung (EU) 2023/1543) ist ein unionsrechtliches Instrument geschaffen worden, das ausländischen Justizbehörden einen weitgehend eigenständigen und unmittelbaren Zugang zu den bei deutschen Telekommunikationsanbietern gespeicherten Daten ermöglicht – eine weit offenstehende dritte Tür, die der deutsche Gesetzgeber weder im Einzelfall kontrolliert noch durch nationale Verfahrensgarantien in gleicher Weise absichern kann.

Solange keine Vorratsdatenspeicherung besteht, bleibt die durch die E-Evidence-Verordnung eröffnete dritte Tür praktisch weitgehend folgenlos, da schlicht keine anlasslos gespeicherten Datenbestände existieren, auf die zugegriffen werden könnte. Wird nun aber eine neue Speicherpflicht eingeführt, verändert sich die verfassungsrechtliche Gesamtbewertung grundlegend. Der Gesetzgeber schafft mit der ersten Tür – der Speicherpflicht – zugleich den Datenbestand, der nicht nur durch die zweite Tür nationaler Abrufbefugnisse, sondern eben auch durch die bereits weit offenstehende dritte Tür der E-Evidence-Verordnung zugänglich wird. Die Verhältnismäßigkeit der Speicherpflicht kann daher nicht mehr isoliert im Zwei-Türen-Modell beurteilt werden. Vielmehr muss bei der verfassungsrechtlichen Prüfung der ersten Tür die kumulative Eingriffsintensität aller bestehenden Zugriffsmöglichkeiten – einschließlich des unionsrechtlich determinierten Zugriffs ausländischer Behörden – in die Gesamtabwägung einbezogen werden. Andernfalls würde die Einführung einer Speicherpflicht sehenden Auges einen Datenbestand schaffen, dessen Schutz durch die zweite Tür nationaler Abrufschranken allein nicht mehr gewährleistet werden kann.

III. Schlussbemerkung

Der VATM bittet darum, die vorstehenden Anmerkungen und Vorschläge in die weiteren Beratungen des Gesetzentwurfs einfließen zu lassen. Gerne stehen wir für einen weitergehenden fachlichen Austausch zur Verfügung.

Berlin, 18. Juni 2026

Dem VATM gehören die größten deutschen Telekommunikationsunternehmen an, insgesamt rund 180 auch regional anbietende Netzbetreiber, Diensteanbieter, aber auch Zulieferunternehmen. Zudem steht der Verband für wichtige Investoren, die den Glasfaserausbau in Deutschland deutlich voranbringen werden. Die VATM-Mitgliedsunternehmen versorgen 80 Prozent aller Festnetzkunden und nahezu alle Mobilfunkkunden außerhalb der Telekom. Seit der Marktöffnung im Jahr 1998 haben die Wettbewerber im Festnetz- und Mobilfunkbereich Investitionen in Höhe von rund 127 Milliarden Euro vorgenommen. Sie investieren auch am stärksten in den zukunftssicheren Glasfaserausbau direkt bis in die Häuser. 86 Prozent der Haushalte, die gigabitfähige Anschlüsse nutzen, sind Kunden der Wettbewerber.