VERBAND DER INTERNETWIRTSCHAFT E.V.

STELLUNGNAHME

zum Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz für ein Gesetz zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren

Berlin, 30. Januar 2026

I. Zusammenfassung

- Die Speicherungsanforderungen genügen nicht der Rechtsprechung des Europäischen Gerichtshofes
- Mangelnde Richtervorbehalte sorgen für Rechtsunsicherheit
- Der Aufbau einer Infrastruktur ist für die Internetwirtschaft kostspielig und hat keinen erkennbaren Nutzen

II. Einleitung

Im Koalitionsvertrag zwischen CDU, CSU und SPD vom 5. Mai 2025 hatten sich die Regierungsparteien darauf verständigt, eine „verhältnismäßige und europa- und verfassungsrechtskonforme dreimonatige Speicherpflicht für IP-Adressen und Portnummern“ einzuführen, „um diese einem Anschlussinhaber zuordnen zu können“. Die Koalitionspartner hatten sich für diese Neuregelung der Vorratsdatenspeicherung entschieden, nachdem der von der vorigen Bundesregierung verfolgte Ansatz eines Quick-Freeze Gesetzes in Diskontinuität gefallen war und nicht weiterverfolgt wurde.

Die Schaffung der IP-Adressspeicherung geschieht vor dem Hintergrund einer laufenden Debatte auf EU-Ebene, die zuletzt als grundrechtswidrig eingestufte Vorratsdatenspeicherung neu aufzulegen. Eine Sondierung dazu fand im Sommer 2025 statt. Auch die stehende Rechtsprechung des Europäischen Gerichtshofes (EuGH) zu diesem Themenkomplex aus den Jahren 2024 (C-470/21) und 2022(C-793/19 und C-794/19) ist hier für die Internetwirtschaft relevant. Dort wird klargestellt, dass eine Vorratsdatenspeicherung grundsätzlich nicht flächendeckend sein darf und einen hinreichenden Anlass benötigt.

Vor diesem Hintergrund nimmt eco – Verband der Internetwirtschaft e.V. zu dem Gesetzentwurf des Bundesministeriums der Justiz und für Verbraucherschutz vom 22. Dezember 2025 wie folgt Stellung:

III. Zu Artikel 1: Änderung der Strafprozessordnung

Mit dem geänderten § 100g der Strafprozessordnung (StPO) wird neben den bereits verpflichteten Anbietern bei der Erhebung von Verkehrsdaten klargestellt, dass dieser zusätzlich auch für Anbieter von nummernunabhängigen interpersonellen Kommunikationsdiensten (NI-ICS) gilt. Zusätzlich wird eine Vereinheitlichung der Erhebung bei sonstigen digitalen Diensten analog zu der Erhebung bei Telekommunikationsdiensten eingeführt (Neufassung §100k mit Bezug auf §100g). Der Adressatenkreis der Norm wird damit deutlich erweitert und auf die Abfragemöglichkeiten der neuen e-Evidence Regulierung angepasst, da ansonsten die erweiterten Abfragemöglichkeiten im EU-Ausland für die nationalen Strafverfolgungsbörden unzulässig wären.
Für Anbieter von NI-ICS sowie digitalen Diensten wird eine zusätzliche Abfragemöglichkeit zum Zwecke der reinen Identifikation des handelnden Kommunikationspartners mit deutlich verringerten Auflagen geschaffen, unter der Bedingung, dass der Inhalt der Kommunikation der Ermittlungsbehörde bereits bekannt ist (§100g Abs. 4, §100k Abs. 5). Die Erhebung bezieht sich in diesen Fällen ausschließlich auf die genutzte IP-Adresse und ggfs. die Portnummer.

Inwieweit hiermit für Anbieter von nummernunabhängigen interpersonellen Kommunikationsdiensten oder digitalen Diensten neue Verpflichtungen zur Datenerhebung und Beauskunftung geschaffen werden, bleibt aufgrund deren unterschiedlicher Angebotsform und dem meist im europäischen Ausland liegenden Sitz unklar, da hierzu die Regelungen dieser Drittstaaten zu berücksichtigen sind. So werden typische NI-ICS, welche heute bereits über 80% der Kommunikationsbeziehungen ausmachen, zumeist von Anbietern in Irland erbracht, wo derzeit eine für 12 Monate bestehende Pflicht zur Vorratsdatenspeicherung besteht. Diese nach ausländischem Recht gespeicherten Vorratsdaten können nach den neuen, seit 18.08.2023 geltenden Regelungen zur e-Evidence jederzeit und alleine nach den Abfragevoraussetzungen des deutschen Rechts von deutschen Strafverfolgungsbörden zu Identifikationszwecken (vergl. §100h Abs. 5, §100k Abs. 4) ohne Richtervorbehalt abgefragt werden.

eco weist darauf hin, dass durch die Anbieter derartiger digitaler Dienste europaweit im Falle einer Abfrage sämtliche gespeicherten Daten, d.h. auch solche, die ausschließlich durch ein ggf. europarechtswidriges Gesetz zur Vorratsdatenspeicherung vorgehalten werden, an die abfragende berechtigte Stelle herausgegeben werden müssen. Abhängig vom verwendeten Dienst können diese beauskunfteten Daten daher bis zu sechs Jahre zurückreichen (Italien), ohne dass jedoch eine geeignete zeitliche Abfragebeschränkung eingeführt wird.

Eine derartige Regelung könnte z.B. als Voraussetzung einer Abfrage vorsehen, dass ausschließlich Daten für die in Deutschland zulässigen Speicherfristen erhoben werden dürfen. Eine solche Regelung wäre realisierbar, da der zu beauskunftende Zeitraum stets Bestandteil einer Entscheidungsformel nach §100e Abs. 3 Nr. 3 ist, dies für Bestandsdaten in der Regel jedoch nicht genutzt wird (Abfrage nach "allen Daten"). Es sollte als Bedingung aufgenommen werden, dass der benannte

Zeitraum die „nach nationalem Recht zulässigen Speicherzeiträume“ nicht überschreiten darf.

Aus Sicht der Internetwirtschaft sollten die hier festgesetzten Regelungen daher noch einmal grundlegend auf ihre Handhabbarkeit für die betroffenen Diensteanbieter sowie auf die Zulässigkeit der Anfragen als solche hin überprüft werden.

Der § 100g Abs. 7 (neu) schafft zusätzlich die Vorgabe zur Sicherung von Verkehrsdaten bei Telekommunikationsdiensten. Hier sollte unbedingt darauf geachtet werden, dass die hier geschaffenen Maßgaben nicht von denen abweichen, die durch die nationale Umsetzung des europäischen e-Evidence Pakets gesetzt werden. Beispielhaft soll den Erläuterungen der Gesetzesbegründung folgend (Zu Nr. 7, Seite 32 ff.) eine Sicherungsanordnung offenbar auch auf in die Zukunft wirkende Zeiträume möglich sein, dies war bei einer reinen Erhebung von Bestandsdaten (per Definition „Data at Rest“) bisher nicht vorgesehen und deckt sich nicht mit den nach der e-Evidence Verordnung im Rahmen einer EPOC-PR zu erhebenden Daten, welche sich alleine auf die zum Zeitpunkt des Eingangs einer Anordnung vorliegenden Daten beziehen. Bereits die technische Umsetzung einer solchen trivial erscheinenden Veränderung ist für die Betreiber jedoch nur mit einem äußerst hohen Aufwand verbunden, dies insbesondere unter Umsetzung der vorgesehenen getrennten, sicheren Datenspeicherung.

Vermisst wird im Rahmen von Sicherungsanordnungen nach §100g Abs. 7 (neu) sowie der Verfahrensregelungen des §101a (neu) zudem eine Regelung zum Schutz von Berufsgeheimnisträgern, analog den in der e-Evidence Verordnung enthalten Schutz- und Widerspruchsmöglichkeiten. Eventuell beim Provider bereits vorliegende Informationen über bekannte Schutzrechte von Personen, Nummern, Kennungen oder ähnlichem können so nicht berücksichtigt werden.

Es gilt dabei zu berücksichtigen, dass gespeicherte Daten jederzeit auch im Rahmen von Auskunftsanordnungen dritter Staaten zu beauskunften sind und ein rein nationales Verwertungsverbot, wie es sich beispielsweise aus §160a StPo ergibt, diesem Problem nicht hinreichend begegnet.

Auch sieht die Neuregelung des § 100 j der Strafprozessordnung nicht mehr ausdrücklich den Richtervorbehalt für die Durchführung von Bestandsdatenauskünften zu Passwörtern oder anderen technischen Schutzvorkehrungen vor. Dies wiegt umso schwerer, da mit diesen Daten unter Umständen auch weitere Informationen gewonnen werden können. Die Eingriffstiefe der Maßnahme steht damit in keinem angemessenen Verhältnis zu den damit verbundenen Rechtsschranken. eco fordert die Überprüfung der Auflagen des 100 j StPO.

In Bezug auf die Neuregelung des Richtervorbehalts in § 101a StPO (neu) appelliert eco daran, auch für die Sicherungsanordnung nach § 100g Abs. 7 StPO (neu) grundsätzlich eine Anordnung des Gerichts (Richtervorbehalt) vorzusehen, und das Gericht nicht erst bei der Verlängerung der Maßnahme einzubeziehen. Mit der

Sicherungsanordnung sollen Anbieter verpflichtet werden, Verkehrsdaten (neu) zu erheben. Sie dient damit der Vorbereitung von Auskünften zu Verkehrsdaten, so dass die Sicherungsanordnung eine erhebliche Eingriffstiefe mit sich bringt. Hier sollte daher ein Gleichlauf mit den übrigen Regeln in § 101a StPO (neu) hergestellt werden.

Ein Aufweichen der Regelungen zum Richtervorbehalt ist aus Sicht der Internetwirtschaft kritisch zu bewerten. Eine Benachrichtigungspflicht für alle von der Kommunikation Betroffenen heilt diesen Umstand nicht. Es wird zudem nicht klargestellt, dass die Benachrichtigungspflicht der von Überwachungsmaßnahmen betroffenen Personen bei der Ermittlungsbehörde und nicht beim Kommunikationsdiensteanbieter liegt.

IV. Zu Artikel 4: Änderung des Justizvergütungs- und -entschädigungs-gesetzes

Die Anpassung der Beträge für die Erteilung einer Bestandsdatenauskunft, insbesondere für Auskünfte unter Nutzung von Verkehrsdaten nach Nr. 200 und Nr. 201, welche durch die üblicherweise zeitgleich angefragten Kundendatensätze im Ergebnis für viele Unternehmen eine Reduzierung der Aufwandsentschädigung zur Folge haben wird, sind vor dem Hintergrund einer Einführung umfassender Speicherpflichten für die Internetwirtschaft in neu zu schaffenden, komplexen und hochsicheren Speichersystemen nicht nachvollziehbar. Die hiermit verbundenen Aufwände erhöhen sich zusätzlich durch die geplante Verpflichtung zur umfassenden Erhebung und Speicherung zusätzlicher, nur mit signifikantem Aufwand überhaupt erlangbarer Daten wie beispielsweise Portzuordnungen. Zwingend notwendig ist vor dem Hintergrund dieser zusätzlichen Verpflichtungen eine signifikante Erhöhung dieser Entschädigungen, um die für jede einzelne Auskunft entstehenden deutlich erhöhten Aufwände auszugleichen.

Insofern steht auch bei den weiteren Festsetzungen infrage, inwieweit diese Entschädigungen der den Kosten einer signifikant erweiterten Überwachungsinfrastruktur, die der Gesetzgeber den Unternehmen aufzuerlegen plant, sinnvoll entgegenstehen. Aus Sicht der Internetwirtschaft sind entsprechende Anregungen nicht nachvollziehbar, da die Einzelfallentschädigung nicht sinnvoll mit der Errichtung und dem Betrieb dieser Überwachungsinfrastruktur gegengerechnet werden kann. eco bezweifelt zudem, dass die Errichtung und der Betrieb dieser Infrastruktur grundrechtskonform sind und lehnt diese daher ab.

V. Zu Artikel 6: Änderung des Telekommunikationsgesetzes

Die Neufassung des § 175 des Telekommunikationsgesetzes (TKG) sieht eine Verarbeitung von Verkehrsdaten vor, sofern sie den Anforderungen gemäß § 100g StPO, § 10b Abs. 1 oder § 52 Abs. 3 des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKA-Gesetz) genügen und ein Auskunftsverlangen mit Bezug darauf vorliegt. Die Auflagen der Sicherung der zur Verarbeitung zu speichernden Daten sind aus Sicht der Internetwirtschaft sehr aufwändig und werden zu enormen

Mehrkosten führen. Dies begründet sich maßgeblich darin, dass die Daten „technisch wirksam getrennt von allen anderen beim Verpflichteten vorhandenen Daten zu Anschlussinhabern durch eine abgesicherte und zuverlässige Datenverarbeitungseinrichtung gespeichert“ werden sollen. Diese getrennte Speicherung und die geforderte sichere Löschung führen dazu, dass eine separate Dateninfrastruktur geschaffen wird, die ausschließlich zu Überwachungs- und Kontrollzwecken betrieben werden soll. Diese muss ähnlich hohe oder – abhängig vom Geschäftsmodell – darüberhinausgehende Anforderungen an Datenspeicherung stellen, wie die vom Netzbetreiber ohnehin betriebene Infrastruktur. Sie wird zusätzlich auf die Anforderungen von Ermittlungsbehörden ausgerichtet werden müssen bspw. bei der Definition von Schnittstellen zur Datenübergabe und Interoperabilität, was die Frage aufwirft, wie sicher diese Infrastruktur tatsächlich sein kann.

Wird – wie im Entwurf vorgesehen – der Startpunkt einer Session weiterhin für drei Monate ab Endpunkt der Session gespeichert, ist eine Zuordnung einer IP-Adresse zu einem Endkunden nicht nur für drei Monate im Nachhinein möglich, sondern faktisch für die gesetzliche Speicherfrist zuzüglich der Dauer der Session. In der Praxis könnten damit auch nach fünf, sechs oder mehr Monaten noch Zuordnungen vorgenommen werden, wenn die Zuordnung einer derart gespeicherten IP-Adresse verlangt wird. Dies widerspricht dem Ziel einer strikt zeitlich begrenzten Speicherung.

Aus Sicht der Internetwirtschaft sollte daher gesetzlich nicht der Startpunkt einer Session maßgeblich sein, sondern vielmehr, dass IP-Adresszuordnungen nach einer Trennung vom Router für eine bestimmte Dauer zugeordnet werden können, Auskünfte jedoch keine Zeiträume früher als drei Monate vor Abfragezeitpunkt ausweisen dürfen. In diesem Fällen sollte eine vereinbarte Antwort (z.B. „verfristet“) an Stelle des ursprünglichen Startdatums treten und das Startdatum beim Anbieter bereits gelöscht werden dürfen. Die konkrete technische Umsetzung sollte – auch hier – technologieoffen ausgestaltet werden.

Wir weisen darauf hin, dass auch ein Aufgreifen dieses Problems alleine durch ein vom BMJV ins Spiel gebrachtes nationales Verwertungsverbot vor dem Hintergrund der e-Evidence Regulation zu kurz greift. Denn im Rahmen der Verordnung wird vielmehr mandatiert, dass alle möglichen Auskünfte, die nach nationalem Recht des anfragenden Staates zulässig und aus den vorhandenen Daten des Anbieters möglich sind, auszuführen sind. Sollten die Startdaten der Verbindungen daher weiterhin in den Daten der Anbieter vorliegen, sind Auskünfte je nach Realisierung der technischen Haltezeiten beim Provider auch über Zeiträume von signifikant über drei Monaten hinaus (d.h. konkret drei Monate zuzüglich der Laufzeit der Verbindung, welche ohne weiteres drei, sechs und mehr Monaten umfassen kann), ohne weiteres möglich.

Die Neufassung des § 176 TKG sieht eine Speicherung von IP-Adressdaten für drei Monate vor. Aus Sicht der Internetwirtschaft genügt diese Vorgabe nicht den Anforderungen des Urteils des EuGH (C-793/19 und C-794/19) da eine Korrelation der IP-Adressdaten mit den Verkehrs- und Nutzungsdaten, welche europaweit von

Diensteanbietern zu speichern und unter Maßgabe von EU 2023/1543 auf erste Anforderung an die Strafverfolgungsbehörden auszuleiten sind, nicht berücksichtigt wird.

Die durch die Vorgaben des Gerichts auszuschließende, vollständige und massenhafte Erfassung des Nutzungsverhaltens von Einzelpersonen wird so ohne weiteres ermöglicht, da vollständige Nutzungsprofile ohne weiteres zu erstellen ist.

Da gleichzeitig im Gesetzentwurf keine der seitens des EuGH beispielhaft genannten Einschränkungen wie Regionale oder auf Personengruppen basierende Kriterien vorgesehen werden, bleibt die erneute anlasslose Datenerhebung grundrechtswidrig, da eine Speicherung nicht nur bei Vorliegen eines hinreichend begründeten Verdachts erfolgt.

Die Internetwirtschaft sieht daher den Anlass begründet, den vorliegenden Gesetzentwurf zurückzuziehen und eine grundrechtskonforme, mit den Vorgaben des EuGH kompatible Regelung anzustreben, welche sämtliche aktuell vorhandenen Abfragemöglichkeiten der Strafverfolgungsbehörden und die sich hieraus ergebenden Korrelationsmöglichkeiten berücksichtigt.

Ergänzend hierzu weist eco auf die Untersuchung des Bundeskriminalamtes (BKA) hin, welche ergeben hat, dass die Speicherung von Verkehrsdaten in rechtlich begründeten Fällen nur wenigen Wochen nach Datenanfall gerechtfertigt ist. Die mit dem vorliegenden Gesetzentwurf festgelegte Speicherung ist damit aus Sicht des eco nicht nur grundrechtswidrig, sondern darüber hinaus auch unverhältnismäßig.

Die konkrete Umsetzung erfordert zudem weiterhin die Klärung zahlreicher offener technischer Fragen – u. a. zu geeigneten Schnittstellen (z. B. ETSI) und zur Handhabung international vergebener IP-Adressen.

VI. Zu Artikel 8: Änderung des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes

Artikel 8 des Gesetzentwurfs sieht die Ergänzung der bisher nur geplanten §§ 13a und 24a des „Entwurfs eines Gesetzes zur Umsetzung der Richtlinie (EU) 2023/1544 und zur Durchführung der Verordnung (EU) 2023/1543 über die grenzüberschreitende Sicherung und Herausgabe elektronischer Beweismittel in Strafverfahren innerhalb der Europäischen Union“ vor.

Die vorgeschlagenen Änderungen stehen nicht im Zusammenhang mit der geplanten Einführung einer IP-Vorratsdatenspeicherung und sollten sinnvollerweise in o.G., ebenfalls mit heutigem Datum noch nicht beendeten Gesetzgebungsverfahren als Änderungsanträge eingebracht werden.

VII. Zu Artikel 10: Änderung des Bundeskriminalamtgesetzes

Die Neuschaffung des § 10b des Bundeskriminalamtgesetzes (BKA-Gesetz) sieht eine Auffangregelung vor, die es dem BKA ermöglicht, Sicherungsanordnungen auszugeben, wenn eine zuständige Ermittlungsbehörde noch nicht bekannt ist. Dies

mag vordergründig nachvollziehbar sein. Es sollte jedoch im Weiteren klargestellt werden, dass das BKA oder eine zuständige andere Strafverfolgungsbehörde im Nachgang zur Sicherungsanordnung zu weiteren Handlungen verpflichtet ist, da die ansonsten zur Durchführung einer Sicherungsanordnung geschaffenen Regelungen ins Leere laufen. Zudem bleibt unklar, wie eine weitere Zuordnung der zuständigen Stelle aufgrund der Inhalte der durch die Sicherungsanordnung umfassten Daten überhaupt erfolgen soll, wenn eine Herausgabe der Daten erst durch die zuständige Stelle veranlasst werden kann. Da das BKA als Zentralstelle insbesondere bei mittels Telekommunikation begangener Straftaten auftritt, sollte diese Regelungslücke aufgelöst werden.

Darüber hinaus sieht eco in dieser Regelung keinen Richtervorbehalt, so dass die Eingriffsschwelle unter Umständen zu niedrig sein könnte. Denkbar wäre insofern eine Anordnung durch das Gericht am Sitz des BKA. Zumindest aber sollte insofern ein Gleichlauf mit der Sicherungsanordnung nach § 100g Abs. 7 StPO (neu) hergestellt werden. Zuletzt hinterfragt eco, ob die in § 3 Abs. 3 (neu) dargelegte Schriftformerfordernis den Maßgaben der Zeit entspricht, diese sollte jedenfalls auch elektronisch möglich sein.

Einen wesentlichen Kritikpunkt aus Sicht der Internetwirtschaft stellen die Umsetzungsfristen dar, die in der Praxis als nicht realistisch 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. Diese viel zu kurz bemessene Umsetzungszeit wiegt umso schwerer, da die in dieser Stellungnahme aufgezeigten rechtlichen ungeklärten Fragen zu einer erheblichen Rechtsunsicherheit führen.

VIII. Fazit

Aus Sicht der Internetwirtschaft genügt der vorliegende Gesetzentwurf nicht den Anforderungen der Rechtsprechung des EuGH. eco erachtet die vorgesehenen Speicherpflichten und Grundrechtseingriffe als unverhältnismäßig und unangemessen. Die Vorgaben schaffen eine umfassende Überwachungsinfrastruktur, die insbesondere unter den Vorzeichen einer mangelnden richterlichen Kontrolle zu Missbrauch einlädt und unverhältnismäßige Auflagen für die Internetwirtschaft erzeugt. Verbunden mit dieser Unsicherheit ist zudem, dass die betroffenen Unternehmen erneut – nunmehr zum dritten Mal – massive Investitionen in eine erneut als unzulässig zu erwartende Infrastruktur tragen sollen.

Wir gehen davon aus, dass eine Erstattung dieser zwingenden Aufwendungen für bereits bei Einführung unzulässigen Infrastrukturen seitens der betroffenen Unternehmen bei den verantwortlichen Stellen eingefordert wird.

Angesichts der massiven Investitionen, die TK- und Internetanbieter bereits auf Basis früherer – später für verfassungswidrig erklärter – Regelungen tätigen

mussten, betont eco, dass zukünftige Vorhaben sorgfältig vorbereitet, breit abgestimmt und grundrechtskonform sein müssen. Einseitige Verpflichtungen gefährden nicht nur die unternehmerische Planung, sondern auch den Standort Deutschland. Überwachungs- und Ermittlungsbefugnisse dürfen kein Selbstzweck sein, sondern müssen sich an Verhältnismäßigkeit und Praktikabilität orientieren.

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.