BUNDESRECHTSANWALTSKAMMER

Stellungnahme Nr. 7
Januar 2026

„Entwurf eines Gesetzes zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren“ des Bundesministeriums der Justiz und für Verbraucherschutz („BMJV“)

Mitglieder des Ausschusses Strafrecht (Strauda)

RAin Dr. Carolin Arnemann
RA Prof. Dr. Jan Bockemühl
RA Prof. Dr. Alfred Dierlamm
RA Prof. Dr. Björn Gercke
RA Dr. Mayeul Hiéramente (Berichterstatter)
RA Thomas C. Knierim (Berichterstatter)
RA Dr. Daniel M. Krause
RAin Theres Kraußlach
RA Prof. Dr. Holger Matt (Vorsitzender und Berichterstatter)
RA Prof. Dr. Ralf Neuhaus
RA Prof. Dr. Tido Park
RAin Dr. Hellen Schilling (Berichterstatterin)
RA Dr. Jens Schmidt
RAin Dr. Annette von Stetten

Prof. Dr. Frank Saliger (Ständiger Gast und Berichterstatter)

RAin Leonora Holling, Schatzmeisterin, Bundesrechtsanwaltskammer

Mitglieder des Ausschusses Strafprozessrecht

RA Dr. Matthias Dann
RA Prof. Dr. Michael Gubitz
RAin Dr. Vera Hofmann, Berichterstatterin
RA Prof. Dr. Christoph Knauer (Vorsitzender)
RA Dr. jur. Andreas Minkoff
RA Maximilian Müller
RA Jürgen Pauly
RAin Anette Scharfenberg
RAin Dr. Alexandra Schmitz
RAin Stefanie Schott
Rechtsanwalt Prof. Dr. Gerson Trüg

RAin Leonora Holling, Schatzmeisterin der Bundesrechtsanwaltskammer
RAin Eva Melina Buchmann, Bundesrechtsanwaltskammer

Mitglieder des Ausschusses Datenschutzrecht

RA Klaus Brisch, LL.M.
RA Malte Dedden
RA Michael Dreßler
RA Peter Hense,
RA Prof. Dr. Armin Herb, (Vorsitzender)
RAin Heike Kraus, MLE, LL.M
RA Jörg Martin Mathis
RAin Simone Rosenthal
RA Dr. Hendrik Schöttle
RA Sebastian Schulz
RA Dr. Volker Schumacher

RA André Haug, Vizepräsident, Bundesrechtsanwaltskammer
RA Sebastian Aurich, LL.M., Bundesrechtsanwaltskammer
Ass. jur. Frederic Boog, LL.M., Bundesrechtsanwaltskammer, Brüssel

Verteiler: Bundesministerium der Justiz und für Verbraucherschutz
Bundesministerium des Innern
Justizministerien der Länder
Innenministerien der Länder
Rechtsausschuss des Deutschen Bundestages
Arbeitskreise Recht der Bundestagsfraktionen
Rechtsanwaltskammern
Der Generalbundesanwalt beim BGH
Bundesgerichtshof
Bundesverband der Freien Berufe
Bundesnotarkammer
Bundessteuerberaterkammer
Deutscher Steuerberaterverband
Wirtschaftsprüferkammer
Institut der Wirtschaftsprüfer
Deutscher Anwaltverein
Deutscher Notarverein
Deutscher Richterbund
Deutscher Juristinnenbund
Bundesvorstand Neue Richtervereinigung
Strafverteidigervereinigungen
Deutsche Strafverteidiger e.V.
Neue Richtervereinigung e.V.
Bund Deutscher Kriminalbeamter
Gesellschaft für Datenschutz und Datensicherheit e. V.
Berufsverband der Datenschutzbeauftragten Deutschlands e. V.
Deutsche Vereinigung für Datenschutz e. V.
Bitkom e. V.
davit – Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein e. V.
eco – Verband der Internetwirtschaft e. V.
VAUNET – Verband Privater Medien e. V.
Stiftung Datenschutz
Datenschutzberater
Computer und Recht
Redaktionen AnwBl, DRiZ, FamRZ, Die Welt, taz, Handelsblatt, dpa, Spiegel, Focus, Beck aktuell, netzpolitik.org, EDRi, NJW,
Beck Verlag, Deubner Verlag Online Recht, Jurion, Juris, LexisNexis, Otto Schmidt Verlag, ZAP Verlag
Strafverteidiger,
Neue Zeitschrift für Strafrecht,
Zeitschrift für höchstrichterliche Rechtsprechung im Strafrecht,
Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht,
wistra - Zeitschrift für Wirtschafts- und Steuerstrafrecht,
Zeitschrift HRR-Strafrecht,
Kriminalpolitische Zeitschrift
FAZ, Süddeutsche Zeitung, Die Welt, Handelsblatt, Tagesspiegel, LTO, Der Spiegel, Focus, Die ZEIT

Die Bundesrechtsanwaltskammer ist die Dachorganisation der anwaltlichen Selbstverwaltung. Sie vertritt die Interessen der 28 Rechtsanwaltskammern und damit der gesamten Anwaltschaft der Bundesrepublik Deutschland mit rund 166.000 Rechtsanwältinnen und Rechtsanwälten gegenüber Behörden, Gerichten und Organisationen – auf nationaler, europäischer und internationaler Ebene.

Zusammenfassung/Abstract

Die Bundesrechtsanwaltskammer (BRAK) begegnet dem Vorhaben, eine verpflichtende Internetprotokoll- Adressendatenspeicherung („IP-Adressen“) auf die Dauer von drei Monaten einzuführen, mit erheblicher Skepsis. IP-Adressen in den unterschiedlichsten Ausprägungen sind Bestandteile von Verkehrsdaten und Nutzungsdaten, damit sind sie Teil der Vorratsdaten im Sinne früherer Gesetzesvorhaben. Die BRAK hat sich stets gegen eine anlasslose und dauerhafte Speicherpflicht zu staatlichen Überwachungszwecken ausgesprochen. Eine solche gesetzliche Regelung greift ohne hinreichende Rechtfertigung in die Grundrechte des Einzelnen auf ungestörte, unüberwachte Telekommunikation, auf Wohnung, freie Entfaltung der Persönlichkeit, auf das Recht auf informationelle Selbstbestimmung sowie in die Freiheit der Berufsausübung ein – wie auch in die Grundrechte der Versammlungsfreiheit, der Vereinigungsfreiheit und der Medienunternehmen und der Rundfunkanstalten. Namentlich sind von diesen Eingriffen Rechtsanwälte[1] und Verteidigerinnen, Journalisten, Abgeordnete, Seelsorger und andere Berufsgeheimnisträger betroffen.

Die Einführung neuer Ermittlungsmethoden, die einen Grundrechtseingriff darstellen, bedarf zunächst der Erforderlichkeit der Maßnahme. Im vorliegenden Entwurf fehlen jedwede Ausführungen hierzu, die jedoch im Hinblick darauf, dass nun seit de facto über 18 Jahren in Deutschland keine Vorratsdatenspeicherung durchgeführt wurde, sich förmlich aufdrängen. Zu betonen ist, dass der Referentenentwurf des BMJ zur Einführung einer Sicherungsanordnung für Verkehrsdaten in der StPO aus dem Jahr 2022 durchaus bemerkenswerte Ausführungen zur Erforderlichkeit beinhaltete. Dort hieß es:

„Aus empirischer Sicht kann festgestellt werden, dass trotz fehlender Vorratsdatenspeicherung in einer Vielzahl von Verfahren Verkehrsdaten erhoben werden können […] Ob und wie viele Fälle hätten aufgeklärt werden können, gäbe es die Vorratsdatenspeicherung, bleibt damit letztlich Spekulation.“ Sodann wird darauf hingewiesen, dass ausweislich der Polizeilichen Kriminalstatistik *„für das Jahr 2021 – auch ohne Anwendung der Vorschriften der Vorratsdatenspeicherung – beispielsweise gelungen ist, 90,8 Prozent der bekannt gewordenen Fälle der Verbreitung kinderpornographischer Inhalte“* aufzuklären. (Vgl. Referentenentwurf des BMJ zur Einführung einer Sicherungsanordnung für Verkehrsdaten in der StPO aus dem Jahr 2022, S. 16) Insoweit hegt die BRAK erhebliche Zweifel an der Erforderlichkeit der mit der Einführung der neuen Ermittlungsmethoden einhergehenden Grundrechtseingriffe.

Bereits in den Stellungnahmen Nr. 52/2022, 7/2025 und 44/2025 hat die BRAK festgestellt, dass in früheren Gesetzesvorhaben die Forderungen der Rechtsprechung des EuGH, des BVerfG und des BVerwG zur Ausgestaltung einer Vorratsdatenspeicherung nicht oder nur unzureichend umgesetzt waren.

Angesichts der im RefE vorgesehenen ausgeweiteten Eingriffsbefugnisse und der abgesenkten Eingriffsschwellen mahnt daher die BRAK die Beachtung der höchstrichterlichen Rechtsprechung insbesondere des EuGH und des BVerfG an. Der Schutz der Grundrechte nach der EU-GRCh, EMRK

[1] Im Interesse einer besseren Lesbarkeit wird nicht ausdrücklich in geschlechtsspezifischen Personenbezeichnungen differenziert. Die im Folgenden willkürlich gewählte weibliche oder männliche Form schließt alle Geschlechter gleichberechtigt ein.

und GG ist noch unzureichend ausgestaltet. Insbesondere ist für die vorgesehenen anlasslosen bzw. nur generalpräventiven Rechtseingriffe mit einer Dauer von drei Monaten, die allein aufgrund von polizeilichen Gefahrenprognosen ohne Richtervorbehalt angeordnet werden können, weder empirische eine Notwendigkeit noch die Verhältnismäßigkeit im Besonderen belegt. Die vorgesehene Mehrbelastung des einzelnen Bürgers erfolgt zudem ohne einen Ausgleich für die Beschränkungen der persönlichen Freiheit durch die Schaffung rechtlicher Freiräume, verbesserter Transparenz und durch einen Zugewinn an Rechtschutz für Betroffene. Bspw. fehlt es an einer unverzüglichen Informationspflicht, sowie an behördenunabhängigen regelmäßigen Auditierungen solcher Eingriffe. In geringerem Maß gilt das auch für die Eingriffsbefugnisse für die Strafverfolgungsbehörden nach dem RefE. Aufgrund des Fehlens eines Richtervorbehalts in den ersten drei Monaten werden schon die Anforderungen des BVerfG an den Eingriff in das Telekommunikationsgrundrecht nicht beachtet.

Der Referentenentwurf (RefE) umfasst ein Bündel von Maßnahmen, um Internetprotokoll-Adressen („IP-Adresse“) sowie weitergehende telekommunikationsrechtliche Verkehrsdaten für Aufgaben der Strafverfolgungsbehörden sowie für die Gefahrenabwehr über den bisherigen Rechtszustand hinaus verfügbar zu machen. Die Absicht des Gesetzgebers, eine gefestigte Rechtsprechung des EuGH umzusetzen, der sich das BVerfG und das BVerwG sowie die Instanzgerichte angeschlossen haben, kann nur begrüßt werden. Gleichwohl bestehen im Detail weitere Defizite, auf die die BRAK bereits in den Stellungnahmen Nr. 52/2022, 7/2025 und 44/2025 eingegangen ist. Besonders das Vertrauen der Bürger in eine staatlich unabhängige, vertrauenswürdige, nur den Interessen der Rechtsinhaber verpflichteten Rechtsanwaltschaft wird durch die Eingriffsbefugnisse weiter belastet.

I. Anlassunabhängige Speicherung von IP-Adressen

1. Telekommunikationsrechtliche Verpflichtung

Die Einführung einer generellen Speicherpflicht für IP-Adressen ist nur telekommunikationsrechtlich vorgesehen. Alle bei der BNetzA registrierte Internetdiensteanbieter sollen gem. der Neufassung des § 176 TKG-E öffentliche IP-Adressen sämtlicher Nutzer ohne konkreten Anlass drei Monate lang speichern. In einem gesonderten Datenbestand sollen die IP-Adresse, die Anschlusskennung, die zugewiesene Benutzerkennung, das Datum und die sekundengenaue Uhrzeit von Beginn und Ende der Zuweisung an einen Anschlussinhaber, die Angabe der zugehörigen Zeitzone, die zugehörige Portnummer sowie weitere, für die Identifizierung des Anschlussinhabers erforderlichen Informationen gespeichert werden (§ 176 Abs. 1 TKG-E). Die Ausgestaltung der Speicherpflicht gem. § 176 Abs. 2 Nr. 1 bis 4 TKG-E erfordert umfangreiche Maßnahmen des Internetdiensteanbieters zur Anlage und Pflege dieses Datenbestands, dessen Daten zum standardisierten Abruf bereitgehalten werden sollen. Diese sollen nach Ablauf von drei Monaten irreversibel gelöscht werden. Wer die durch diesen Eingriff in die bisherigen Speichermodalitäten der TK-Anbieter aus technischen oder vertraglichen Gründen entstehenden Kosten zu tragen hat, ist gesetzlich nicht bestimmt.

2. Stellungnahme

a) Die BRAK erkennt an, dass im RefE den in den BRAK-Stellungnahmen 52/2022, 7/2025 und 44/2025 mitgeteilten Bedenken Rechnung getragen worden ist. Dennoch stellt die geplante umfassende Speicherung von IP-Adressendaten trotz Änderung von Begrifflichkeiten ihrer Struktur nach eine Vorratsdatenspeicherung personenbezogener Daten dar, deren Besitz und Auswertungsmöglichkeiten die Erstellung personenbezogener Bewegungs- und Persönlichkeitsprofile ermöglicht. Daher sind die aus der Rechtsprechung von EuGH, BVerfG und BVerwG zur Vorratsdatenspeicherung entwickelnden unionsrechtlichen und verfassungsrechtlichen Vorgaben, insbesondere aufgrund des Umfangs, der

Dauer und der Kombinierbarkeit der Daten, uneingeschränkt auch auf die Speicherung von IP-Adressen und deren Abruf übertragbar.

b) Das informationelle Selbstbestimmungsrecht und die Vertraulichkeit der Kommunikation aller Nutzer ist bereits durch eine Vorratsspeicherung der IP-Adressen betroffen, da diese ausschließlich aufgrund einer staatlichen Erwartung und Zwecksetzung zur Verarbeitung zur Strafverfolgung und Gefahrenabwehr erfolgen soll. Die vom EuGH im Urteil vom 30.04.2024 C-470/21 beurteilte Konstellation betraf eine zur Verfolgung von Internetdelikten begründete Speicherung der IP-Adressen in Frankreich durch eine zentrale nicht-polizeiliche Stelle. Zwar hat der EuGH in diesem Fall die Speicherung der IP-Adressen erlaubt, allerdings auch bestimmte detaillierte Vorgaben gemacht, indem die Daten zu Bedingungen und unter technischen Modalitäten gespeichert werden müssen, die gewährleisten, dass *„… es ausgeschlossen ist, dass aus der Vorratsspeicherung genaue Schlüsse auf das Privatleben der Inhaber der IP-Adressen, z. B. durch Erstellung ihres detaillierten Profils, gezogen werden können. …“* Zudem muss die Gesamtnutzung verschiedener Daten, die auf Persönlichkeit und Lebenswandel der Person schließen lassen, durch geeignete Maßnahmen verhindert und die Dauer der Speicherung auf das absolut notwendige Maß beschränkt sein. Der EuGH geht noch weiter, indem auch der Zugang einer Behörde zu den gespeicherten Daten ausschließlich für die Identifikation von Personen ermöglicht werden darf, die schon im Verdacht einer Straftat stehen. Auch darf mit den Daten keine Profilerstellung ermöglicht werden. Schließlich hat sich der EuGH in der Entscheidung gegen automatisierte IT-Routinen ausgesprochen, die etwaige auf diesem Weg erlangte Daten mit anderen Daten verknüpfen könnten, die sich im Besitz der Behörden befinden oder über andere Maßnahmen erlangt worden sind. Daher sei es auch weiterhin verboten, durch Datenanalysen oder Verknüpfungen beliebiger Verbindungs- und Nutzungsdaten „… Schlüsse auf das Privatleben der Person zu ziehen, deren IP-Adresse für Aktivitäten genutzt wurde, die möglicherweise Urheberrechte oder verwandte Schutzrechte verletzen. …“. Ergänzend verlangt der EuGH auch eine regelmäßige Revision der Integrität der Datenverarbeitungssysteme der Behörden.

c) Während der EuGH[2] betont, dass durch eine Speicherung keine „genauen Schlüsse auf das Privatleben“ ermöglicht werden dürfen, kann eine solche Schwelle, bei moderner Tracking- und Logging-Praxis schnell überschritten werden. Die Pflichtspeicherung der IP-Adressen und der weiteren Identifikationsmerkmale gem. § 176 Abs. 1 TKG-E ermöglichen – jedenfalls im Zusammenspiel mit Provider-Bestandsdaten und weiteren Telemediendaten – dem Empfänger solcher Daten eine nachträgliche Zuordnung verschiedener Online-Aktivitäten der abgefragten Personen und damit eine erheblich tiefere Beeinträchtigung der bürgerlichen Privatsphäre, als es die abstrakte Kategorie „IP-Adresse“ zunächst vermuten lässt. Die in der Begründung des Referentenentwurfs (S. 28) enthaltene Aussage, aus der IP-Adressspeicherung ließen sich keine Rückschlüsse auf Kommunikationspartner von Berufsgeheimnisträgern ziehen (zu dem Schutz der Berufsgeheimnisträger folgen Ausführungen näher unten), ist in dieser Allgemeinheit und insbesondere mit Blick auf Mandatskontakte nicht tragfähig. Selbst wenn IP-Adressdaten für sich genommen noch keine vollständige Kommunikationsmatrix abbilden, fungieren sie in der Praxis als Schlüssel, um anderweitig erhobene Verkehrs- und Nutzungsdaten einer bestimmten Person und damit auch Mandatskontakten zuzuordnen. Diese Brückennutzung der IP-Adresse wird im Zusammenspiel mit den nach dem Entwurf teils mit zu erhebenden Nutzungs- und Provider-Bestandsdaten umso leichter möglich sein.

Daher ist im weiteren Gesetzgebungsverfahren zu berücksichtigen, dass es an entsprechenden technischen Kriterien fehlt, um der Vorgabe einer strikten Datenkategorien-Trennung, der Protokollierung, einer unabhängigen Kontrolle und einem effektiven Rechtsschutz für die Ausgestaltung einer solchen Trennung zu genügen. Die Ermächtigungsgrundlage des § 170 Abs. 5 TKG i. V. m. §§ 175 Abs. 3, 176 Abs. 4 TKG-E erscheint insoweit nicht ausreichend spezifisch und normenklar.

---

[2] EuGH, Urteil v. 30.04.2024 C-470/21

Gesetzlich angeordneter technischer Mindeststandards bedarf aus auch, weil das zentrale Online-Portal, in dem diese Daten gespeichert würden, ein lohnendes und hochkritisches Angriffsziel darstellt.

d) Für die vorgesehene Dauer einer Speicherung von drei Monaten fehlt es an empirischen Grundlagen. Die im RefE bemühte Wendung „die Praxiserfahrung zeigt“ (S. 53) verdeutlicht, dass es sich hier um eine unspezifizierte Erwartungshaltung handelt, der die erforderliche empirische Grundlage fehlt. Warum eine Frist von vier Wochen nicht ebenso ausreichen können soll, ist nicht ersichtlich. Schon im Zuge der Anhörung von Sachverständigen durch den Rechtsausschuss des Deutschen Bundestages am 11.10.2023 hatte sich gezeigt, dass es „objektiver Kriterien“ für die Annahme einer solchen Speicherdauer bedarf. Die Vizepräsidentin des BKA Martina Link äußerte in dieser Anhörung:[3] *„…Wir gehen davon aus, dass wir die IP-Adressen als werthaltigsten und erfolgsträchtigsten Ansatz, wenn wir hier Speicherfristen haben, für den Prozess NCMEC, habe ich gesagt, 2 bis 3 Wochen wären hier aus unserer Sicht schon ein signifikanter Gewinn, bei dem wir davon ausgehen, dass wir die Rate von 41 Prozent auf bis zu 80 Prozent steigern können. ,,,“*

Schließlich ist eine abstrakte Herleitung, wonach die IP-Adresse als Ansatz zur Bekämpfung illegaler Handelsplattformen im Internet dienen soll, keine Rechtfertigung für eine anlasslose Speicherung mit einer solchen Zeitspanne. Denn im Zuge der anlassabhängigen Speicherung von Verkehrs- und Nutzungsdaten nach den schon bestehenden Regelungen in §§ 100g, 100k StPO bzw. § 52 BKAG, und anderen Sicherheits- und Polizeigesetzen werden keine Defizite gemeldet, die eine dreimonatige Speicherung erfordern würden.

II. Anlassabhängige Speicherung und Abruf von Verkehrsdaten zur Strafverfolgung

1. Telekommunikationsrechtliche Verpflichtung

a) Gem. § 175 Abs. 1 TKG-E sollen Internetdiensteanbieter verpflichtet werden, verdachtsabhängig Verkehrsdaten insbesondere zu Zwecken der Strafverfolgung (§ 100g Abs. 7 StPO-E) zu speichern. Der Umfang der nach dieser Vorschrift zu speichernden Daten ist deutlich größer als bei der IP-Adressdatenspeicherung, da Verkehrsdaten sämtlichen technischen Informationen betreffen, die für die Herstellung, Aufrechterhaltung und Beendigung einer Einwahl erforderlich sind. Die Speicherdauer richtet sich nach den Vorgaben der Sicherungsanordnung und unterliegt keiner automatisierten Löschung. Die Ausgestaltung der Speicherpflicht (§ 175 Abs. 2 Nr. 1 bis 4 TKG-E) erfordert somit umfangreichere Maßnahmen vom Internetanbieter. Ein Kostenersatz für die durch Sicherungsanordnung auferlegten Maßnahmen (Speicherung und Auskunft) soll im JVG durch Pauschalen vorgesehen werden.

b) Aufgrund von Abruf- und Herausgabeanordnungen sollen die Internetdiensteanbieter sodann die gespeicherten Daten an die abfragende Behörde übermitteln. Das betrifft insbesondere Verkehrsdaten, Nutzungsdaten und Bestandsdaten. Diese Daten ermöglichen eine sofortige Zuordnung der IP-Adressen zum Anschluss, die Beurteilung von Zeit, Weg, Ort, Dauer der Nutzung und u. U. auch der Kommunikation mit anderen, allerdings ohne die Inhalte der Kommunikation zu konkretisieren. Der Internetdiensteanbieter wird hinsichtlich der erteilten Auskünfte zum Stillschweigen verpflichtet, d. h. er darf dem Anschlussinhaber keine Nachrichten über die Auskunft erteilen. Eine Löschung von abgerufenen Daten beim Versender ist durch Änderungen im TDDDG vorgesehen (RefE S. 48 f.). Eine Löschungsverpflichtung beim Empfänger wird nicht vorgegeben, vielmehr erfolgt sie bei strafprozessual

[3] BT-Prot. 20/68 Rechtsausschuss v. 11.10.2023, S. 27 li.; 68. Protokoll.

begründeten Abrufen gem. § 101 Abs. 8 StPO. Bei gefahrenabwehrrechtlich begründeten Abrufen erfolgt die Löschung auf der Grundlage der §§ 74 ff. BKAG.

2. Strafprozessuale Befugnisse

a) Die bisherigen strafprozessualen Eingriffsbefugnisse für Verkehrsdaten und Nutzungsdaten sollen ausgeweitet, durch Absenkung der Eingriffsschwellen erleichtert und durch Verfahrensvereinfachungen beschleunigt werden. Insbesondere sieht der RefE als neues Eingriffsinstrument die Sicherungsanordnung gem. § 100g Abs. 7 StPO-E vor. Die sog. Quick-Freeze-Anordnung bezweckt eine umfassende Speicherung von Verkehrsdaten von Betroffenen (nicht nur von IP-Adressen). Sie soll im Umfang des Anwendungsbereichs gem. § 100g Abs. 1 bis 4 StPO-E eingesetzt werden und ohne eine richterliche Einbindung allein von der Staatsanwaltschaft, bei Gefahr im Verzug auch von ihren Ermittlungspersonen, ausgeübt werden (§ 101a Abs. 1 Nr. 3 StPO-E). Eine Bestätigung von Eilentscheidungen der Polizei durch die Staatsanwaltschaft ist nicht vorgesehen. Lediglich bei einer einmalig möglichen Verlängerung der Sicherungsanordnung um drei weitere Monate soll noch eine gerichtliche Entscheidung erforderlich sein (§ 101a Abs. 1 Nr. 3 lit. a) StPO-E). Der Abruf der auf diese Weise gespeicherten Daten erfolgt allerdings nach Maßgabe der §§ 100g Abs. 1 bis 5, 101a Abs. 1 StPO-E. Für den Erlass einer Sicherungsanordnung reicht ein Anfangsverdacht gem. § 152 StPO aus.

b) Der Abruf von Verkehrsdaten gem. § 100g Abs. 1 bis 4 StPO-E soll durch Streichung der bisherigen als zu eng empfundenen Vorgaben in § 100g Abs. 2 und Abs. 3 StPO erleichtert werden. So werden die Voraussetzungen für den Abruf von Standortdaten und Funkzellendaten (§ 100g Abs. 3, 4 StPO-E) angepasst, sowie der Abruf sämtlicher Funkzellendaten ohne Eingrenzung auf Zielpersonen mit räumlich und zeitlich beschränkter Reichweite (§ 100g Abs. 5 StPO-E) ohne die bisherigen Eingriffsschwellen (insbesondere ohne die Begrenzung auf schwerste Kriminalität, die allein Gerichten vorbehaltenen Sicherungs- und Abrufanordnungen sowie die Schutzvorschriften für Zeugnisverweigerungsberechtigte) ermöglicht.

c) Zur Abfrage von Bestandsdaten wird durch die Neuregelung in § 100j Abs. 3 StPO-E die Abfrage von zugriffsschützenden Merkmalen von Mobilgeräten, d. h. von Passwörtern oder anderen digital gespeicherten Schutzmechanismen eingeführt. Auf eine Angabe konkretisierender zeitlicher Begrenzungen in der Auskunftsentscheidung soll verzichtet werden (§ 101a Abs. 1 Satz 2 StPO-E). Die spezifische Benachrichtigungspflicht gem. § 100j Abs. 4 StPO soll gestrichen werden, dafür soll eine beschränkte Benachrichtigungspflicht eingeführt werden, die wiederum nach den geltenden Regelungen in § 101 Abs. 4 Satz 2 bis 5, Abs. 5 bis 7 StPO unterbleiben darf (§ 101a Abs. 4 StPO-E).

d) Die Neuregelung des Abrufs von Nutzungsdaten (§ 100k StPO-E) sieht im vergleichbaren Umfang die Absenkung der Eingriffsschwellen für die Abrufe von Nutzungsdaten vor, was jetzt die Standortdaten sowie Funkzellendaten einschließen soll.

e) Letztlich sieht der Referentenentwurf auch eine Verlagerung der Zuständigkeiten für die Verkehrsdatenerhebung sowie deren Sicherung aufgrund von Europäischen Sicherungsanordnungen vor. Im Elektronische-Beweismittel-Umsetzungs- und Durchführungsgesetz (EBUD), dem Ausführungsgesetz zur e-Evidence Verordnung (Verordnung (EU) 2023/1543), wird die Zuständigkeit für ausgehende Sicherungsanordnungen der Staatsanwaltschaft alleine zugewiesen (RefE S. 46). Nur bei einer über drei Monate hinausgehenden Sicherungsanordnung soll zukünftig noch eine gerichtliche Entscheidung erforderlich sein. Außerdem soll die Staatsanwaltschaft zuständige Stelle für Strafvollstreckungszwecke sein.

3. Stellungnahme

a) Die BRAK erkennt an, dass in Bezug auf das Quick-Freeze-Verfahren, das der RefE in § 100g Abs. 7 StPO-E vorsieht, einigen der in der BRAK-Stellungnahme-Nr. 7/2025 geäußerten Bedenken Rechnung getragen worden ist. Das neue Instrument der anlassbezogenen Sicherungsanordnung gem. § 100g Abs. 7 StPO-E, erfüllt einige Anforderungen des EuGH, so dieses Instrument für die Verfolgung von Internetkriminalität genutzt wird. Namentlich zählt hierzu auch die in § 175 Abs. 1 Satz 2 TKG-E vorgesehene Zweckbindung. Allerdings sollte diese dahingehend geschärft werden, dass eine Zweckbindung an die konkrete inhaltliche Begründung der Sicherungsanordnung erforderlich ist, um auch den späteren Abruf und die weitere Verarbeitung durch die Strafverfolgungsbehörde zu rechtfertigen. Die Eingrenzung „mittels Telekommunikation begangener Straftaten“ ist hierfür nicht geeignet. Zu der in § 100g StPO bereits verwendeten Formulierung zählen alle Taten, bei denen Telefon oder Computer mit Internetanbindung nicht nur das eigentliche Angriffsobjekt, sondern notwendiges oder nützliches Mittel der Tatausübung sind, somit nicht nur die Internetkriminalität. Eine schärfere Zweckbindung dient dem Schutz der Betroffenen und anderer Teilnehmer der Telekommunikation und unterscheidet außerdem bei sich überschneidenden Anordnungen zur Strafverfolgung und zur Gefahrenabwehr.

b) Das Fehlen eines Richtervorbehalts für die strafprozessuale Sicherungsanordnung gem. § 100g Abs. 7 StPO-E wird den Anforderungen des BVerfG nicht gerecht. Das BVerfG betont in ständiger Rechtsprechung,[4] dass für Eingriffe in das Grundrecht des Art 10 Abs. 1 GG ein strenger Richtervorbehalt vorzusehen ist, da es sich um ein Gebot des rechtsstaatlichen Gewaltenteilungsgrundsatzes handelt. Der RefE sieht nicht nur für die ersten drei Monate der Sicherungsanordnung eine Abkehr davon vor, sondern überlässt auch für Eilfälle die Eingriffsbefugnis den Ermittlungspersonen der Staatsanwaltschaft, ohne dass es einer weiteren Bestätigung bedarf. Damit wird auch eine objektive Kontrolle von Art und Umfang des Eingriffs verzichtet, wie sie von der Rechtsprechung des EuGH seit vielen Jahren gefordert wird.

c) Generell fehlt es an Bestimmungen, die die vorgesehene Mehrbelastung des einzelnen Bürgers kompensieren. So hat der EuGH in ständiger Rechtsprechung entschieden, dass ein Ausgleich für die Beschränkungen der persönlichen Freiheit durch die Schaffung rechtlicher Freiräume, verbesserter Transparenz und durch einen Zugewinn an Rechtschutz für Betroffenen ermöglicht werden muss. Bspw. fehlt es an einer unverzüglichen Informationspflicht, sowie an behördenunabhängigen regelmäßigen Auditierungen solcher Eingriffe. Der Abbau von Eingriffsschwellen und die Beibehaltung der defizitär ausgestalteten Datenauskunfts-, Informations- und Einsichtsrechte der Betroffenen in die von den Gefahrenabwehr- und Strafverfolgungsbehörden angeordneten Sicherungen und Abrufen von Daten erzeugt eine erhebliche Unsicherheit über Art und Umfang der tatsächlich durch staatliche Behörden ausgeübten Überwachung. Dies wirkt sich insbesondere auf den unvoreingenommenen Umgang mit Angehörigen der rechtsberatenden Berufe und der Verteidiger aus.

d) Die vorbezeichnete Rechtsprechung des BVerfG steht der Neuregelung der Sicherung und des Abrufs retrograder Standortdaten (aktuelle Regelung in § 100g Abs. 1 Satz 3 StPO) entgegen. Während der RefE diesen Abruf dem Abruf von Verkehrsdaten gleichstellen und auf die Unterscheidung retrograder und progressiver Standortdaten verzichten will (RefE S. 30), hatte das BVerfG[5] einen solchen Eingriff zur Erstellung von Bewegungsprofilen nur unter den engen Voraussetzungen des Katalogs von § 100g Abs. 2 StPO bzw. eines dem § 100c Abs. 2 StPO vergleichbaren Katalogs zugelassen. Zudem war nur ein Abruf von vier Wochen alten Daten für zulässig erachtet worden. Retrograde Standortdaten offenbaren Kernbereiche der Persönlichkeitsentfaltung (Art. 1 Abs. 1,

---

4 BVerfGE 30, 1, Rn. 32-60; 50, 226; 96, 34; 120, 313; 125, 260 (Rn. 142); 141, 220 usw.

5 BVerfGE 141, 220

Art. 2 Abs. 1 GG), deren Schutz von Verfassungswegen nur für die Aufklärung schwerster Kriminalität und unter Anwendung eines besonders strengen Verhältnismäßigkeitsvorbehalts erlaubt sein darf. Diese im geltenden Recht geregelten Vorgaben gibt der RefE zu Unrecht und ohne nachvollziehbare empirische Begründung auf.

e) Das zu d) Gesagte gilt auch für die Neuregelung in § 100k Abs. 3 StPO-E, da auch die dort vorgesehene Neuregelung die Einbeziehung retrograder Standortdaten in die Nutzungsdaten für die Bewegungsprofilerstellung erlauben soll.

f) Ebenso steht die Rechtsprechung des BVerfG[6] der Neuregelung der Sicherung und des Abrufs von Funkzellendaten (aktuelle Regelung in § 100g Abs. 3 Satz 2 StPO) entgegen. Während der RefE sowohl die Sicherung als auch den Abruf von Funkzellendaten im wesentlichen Punkten dem Abruf von Verkehrsdaten gleichstellen will, hatte das BVerfG es nicht für zulässig gehalten, solche Daten zur Aufklärung nach dem Katalog des § 100a Abs. 2 StPO Daten abzurufen. Auch der BGH[7] hatte entgegen der Ansicht des RefE (S. 23, 26, 30), die besondere Sensibilität eines solchen Eingriffs betont und es – entgegen einzelnen Entscheidungen von Instanzgerichten – für unzulässig gehalten, die Funkzellenabfrage zur Bekämpfung einfacher Kriminalität einzusetzen. Der Eingriff in Funkzellendaten stellt eine Kriminalisierung sämtlicher Nutzer der Internetdienste und der Telekommunikation in der Funkzelle dar, in deren Grundrechte nur unter einem engen Verhältnismäßigkeitsvorbehalt eingegriffen werden soll. Der Grundrechtsschutz gebietet daher die Unterscheidung nach schwerwiegenden Delikten, der anderweitigen Aussichtslosigkeit und einem strengen Verhältnismäßigkeitsmaßstab.

g) Der spezielle Schutz zeugnisverweigerungsberechtigter Personen durch ein absolutes Verwertungsverbot (bisher § 100g Abs. 4 StPO) soll nach dem RefE vollständig entfallen. Als Konsequenz soll der Verweis auf diese Regelung (bisher § 160a Abs. 5 StPO) ersatzlos gestrichen werden. Zwar soll nach dem RefE der Schutz der Berufsgeheimnisträger durch die Regelungen des § 160a StPO gewahrt sein, das führt aber zu einer Relativierung des Schutzes von Mandanten und Patienten namentlich von Rechtsanwälten, Suchtberatungsstellen und Journalisten, für die nur ein relativer Schutz gem. § 160a Abs. 2 StPO gewährleistet ist. Damit setzen sich die Bedenken der BRAK gegen die Eingriffe in die Mandantenkommunikation fort (vgl. dazu BRAK-Stellungnahme-Nr. 52/2022 S. 3, 7 f.).

Der besondere Schutz der Berufsgeheimnisträger (§ 53 StPO) gebietet bei Gesetzesvorhaben die besonders sorgfältige Prüfung der Eingriffsvoraussetzungen und des Grundsatzes der Verhältnismäßigkeit. Das BVerfG[8] führte jüngst aus: *„Richtet sich eine strafrechtliche Ermittlungsmaßnahme gegen einen Berufsgeheimnisträger in der räumlichen Sphäre seiner Berufsausübung, so bringt dies regelmäßig die Gefahr mit sich, dass unter dem Schutz des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG stehende Daten von Nichtbeschuldigten, etwa den Mandanten eines Rechtsanwalts, zur Kenntnis der Ermittlungsbehörden gelangen, die die Betroffenen in der Sphäre des Berufsgeheimnisträgers gerade sicher wähnen durften. Dadurch werden die Grundrechte der Mandanten berührt. Der Schutz der Vertrauensbeziehung zwischen Anwalt und Mandant liegt darüber hinaus auch im Interesse der Allgemeinheit an einer wirksamen und geordneten Rechtspflege. Diese Belange verlangen eine besondere Beachtung“.* Es verweist hierbei ausdrücklich auf die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte zu Art. 8 EMRK und der besonderen Vertraulichkeitserwartung hinsichtlich Rechtsanwaltskorrespondenz. Im RefE ist der Schutz der Anwaltschaft und insbesondere ihrer Mandantenkontakte defizitär ausgestaltet. Der Schutz der Vertraulichkeit der Mandatskontakte bedarf einer ausdrücklichen Regelung, die im Kern den

---

6 BVerfGE 141, 220

7 BGH, Beschl. v. 10.01.2024 – 2 StR 171/23, Rn. 14 ff., NJW 2024, 2336 = NStZ 2024, 557

8 BVerfG, Nichtannahmebeschluss vom 21. Juli 2025 – 1 BvR 398/2

Vorgaben des § 100g Abs. 4 StPO entspricht, (Stellungnahme der BRAK Nr. 52/2022, S. 3, 9, 10 mit konkreten Regelungsvorschlägen) nicht lediglich Ausführungen in der Gesetzesbegründung, die auch inhaltlich nicht tragen (s. dazu oben Ziffer I. 2. c sowie sogleich).

Zuletzt hatte die BRAK in der Stellungnahme 7/2025 Absicherungen zum Schutz der Offenbarung von Mandatskontakten angemahnt. Solche sind weiterhin dringend erforderlich und nicht in ausreichendem Maß vorhanden. Insoweit wird zwar in der Entwurfsbegründung des RefE darauf verwiesen, dass § 160a StPO einen hinreichenden Schutz gewährleiste. Das ist aber nur bedingt der Fall. Die in §§ 175, 176 TKG-E vorgesehenen technisch-organisatorischen Maßnahmen gegen unbefugte Kenntnisnahmen der gespeicherten Daten sind unbestimmt und nicht geeignet, den fehlenden Schutz zu kompensieren. Insbesondere wird darin kein grundrechtsschonender Aussonderungsmechanismus beschrieben. Ein solcher erscheint auch schwerlich möglich, da jede Aussonderung zunächst die Erkennung und damit einen gewissen Grad an Offenbarung voraussetzt. Die Einführung einer anlasslosen IP-Vorratsspeicherung und der Sicherungsinstrumente für Verkehrsdatenabfragen muss einen solchen Schutz vorsehen. Mindestens sollten aber konkrete Vorgaben für ein möglichst schonendes Aussonderungsverfahren gemacht werden. Denkbar – wenn auch nicht ausreichend – wären u. a. die Aufnahme von auszusondernden Telekommunikationsdaten in eine Positivliste analog zu § 11 Abs. 5, 6 TDDSG (dann mit einer Erstreckung auf § 203 Abs. 1 Nr. 3 StPO) sowie ein frühzeitiger automatisierter Abgleich mit dem BRAV.

III. Gefahrenabwehrrechtlich begründete Sicherung und Abruf von Verkehrsdaten

1. Telekommunikationsrechtliche Verpflichtung

a) Schließlich sollen Internetdiensteanbieter gem. § 175 Abs. 1 TKG-E verpflichtet sein, Verkehrsdaten zu **gefahrenabwehrrechtlichen Zwecken** zu speichern. Wie auch die Speicherung nach strafprozessualen Zwecksetzungen setzt dies eine Sicherungs- und spätere Abrufanordnung auf gesetzlicher Grundlage nach den Polizeigesetzen oder den Verfassungsschutzgesetzen voraus. Hierfür gelten die Ausführungen unter II.1..

2. Gefahrenabwehrrechtliche Befugnisse

a) Mit den gefahrenabwehrrechtlichen Eingriffsbefugnissen weitet der Referentenentwurf die Kompetenzen des BKA als Zentralstelle für kriminalpolizeiliche Aufgaben und Kontaktstelle für die Bundespolizei und die Länderpolizeibehörden aus. Neben die bisher schon in §§ 10, 10a BKAG geregelten Befugnisse zur Einholung von Bestandsdatenauskünften und Nutzungsdatenerhebung soll eine eigenständige Befugnis treten, vorsorgende Sicherungsanordnungen ohne Richtervorbehalt zu erlassen (§ 10b BKAG-E). Zusätzlich soll für die Erfüllung eigener Aufgaben des BKA die Befugnis zur Erhebung von Verkehrsdaten um die Möglichkeit einer verlängerbaren Sicherungsanordnung erweitert werden (§ 52 Abs. 3 BKAG-E). Die Regelung dient der Festigung des BKA als Zentralstelle zur Gewährleistung des polizeilichen Datenaustauschs innerhalb und außerhalb Deutschlands.

b) Die Sicherungsanordnung gem. § 10b BKAG-E als vorsorgende Maßnahme des BKA als Zentralstelle bezweckt die Speicherung von Verkehrsdaten (nicht nur von IP-Adressen). Sie soll bereits im Vorfeld von Straftaten zulässig sein, wenn „eine zuständige Strafverfolgungsbehörde oder Polizeidienststelle noch nicht erkennbar ist“ und

- wenn aufgrund zureichender tatsächlicher Anhaltspunkte für eine Straftat eine Abfrage im Geltungsbereich des § 100g Abs. 1 bis 4 StPO-E zu erwarten ist (Abs. 1 Nr. 1), oder

- wenn aufgrund tatsächlicher Anhaltspunkte eine Person innerhalb eines „übersehbaren“ Zeitraums eine Straftat im Sinne von § 100g Abs. 1 Satz 1 Nr. 1 StPO-E begehen wird (Abs. 1 Nr. 2), oder

- wenn dies eine vorsorgende Dienstleistung für eine nach Landespolizeirecht zuständige Polizeibehörde nach deren Eingriffsbefugnissen darstellt (Abs. 1 Nr. 3).

Damit soll dem BKA die Möglichkeit zugewiesen werden, unabhängig von den gesetzlichen Zuständigkeitsregelungen und vor der Klärung von Zuständigkeiten vorauseilend für eigene und landespolizeiliche präventive wie repressive Eingriffsbefugnisse vorsorglich einen Datenvorrat über Verkehrsdaten zu sichern. Ausdrücklich sollen diese Befugnisse allein durch eine Abteilungsleitung, deren Stellvertretung oder kraft Delegation durch ausgewählte BKA-Beamte, ohne Zustimmung des Gerichts ausgeübt werden können (§ 10b Abs. 2 BKAG-E). Hinsichtlich der Eingriffsschwellen wird auf § 100g Abs. 1 bis 4 StPO-E Bezug genommen, die Sicherungsanordnung soll schriftlich ergehen und ist auf drei Monate befristet (§ 10b Abs. 4 BKAG-E). Ein Abruf des nach dieser Norm gesicherten Datenvorrats kann sowohl nach der StPO, dem BKAG als auch nach den LPolizeiG erfolgen. Der Sache nach handelt es sich um eine tief in den Grundrechtsschutz eingreifende Überwachungsbefugnis, die jedenfalls in der dritten Alternative weder normenklar noch hinreichend bestimmt ist.

c) Die Befugnis zum Erlass einer Sicherungsanordnung im gefahrenabwehrrechtlichen Aufgabenbereich des BKA soll in § 52 Abs. 3 BKAG-E geschaffen werden. Grundlage der Sicherungsanordnung soll die Erhebungsbefugnis gem. § 52 Abs. 1 BKAG sein. Die Ausführung der Sicherungsanordnung ist nicht nur auf 3 Monate befristet, sondern kann mit Zustimmung eines Gerichts um drei Monate verlängert werden. Für die Sicherungsanordnung sollen die Bestimmungen des § 51 BKAG nicht gelten, mithin ist auch kein Schutz von Berufsgeheimnissen oder des höchstpersönlichen Lebensbereichs (§ 51 Abs. 7 BKAG) vorgesehen.

d) Die Erhebung der gesicherten Daten, d. h. der Abruf von Verkehrsdaten im Aufgabenbereich des BKA erfolgt nach Maßgabe des § 52 BKAG. Wie bisher auch ist auch für den Abruf von Verkehrsdaten für Ermittlungsaufgaben des BKA kein Schutz von Berufsgeheimnisträgern oder des höchstpersönlichen Lebensbereichs im Sinne von § 51 Abs. 7 BKAG vorgesehen. Auch § 160a StPO greift insoweit nicht.

3. Stellungnahme

a) Für die präventivpolizeiliche Sicherungsanordnung gem. § 10b BKAG-E gelten hinsichtlich der Eingriffsbefugnisse die bereits zur strafprozessualen Regelung des § 100g Abs. 7 StPO-E dargestellten Bedenken (II.3.a) bis f)).

b) Darüber hinaus ist der vorsorgenden, dreimonatigen Sicherungsanordnung von Verkehrsdaten gem. § 10b Abs. 1 Nr. 2 und 3 BKAG-E ohne richterliche Zustimmung zu widersprechen. Diese Sicherungsanordnungen haben – entgegen den Voraussetzungen, die das BVerfG für solche Zugriffe aufgestellt hat – keinen Strafverfolgungscharakter, sondern sind reine Instrumente der Gefahrenabwehr. Zudem sind die tatbestandlichen Eingriffsvoraussetzungen zu unbestimmt. Es fehlt an empirischen Gründen für die Notwendigkeit einer dreimonatigen Sicherung, Beispiele aus der Gefahrenabwehrpraxis oder der Strafverfolgungspraxis fehlen (RefE S. 56/57).

c) Namentlich für die Befugnis gem. § 10b Abs. 1 Nr. 2 BKAG-E soll es für die Sicherung von Verkehrsdaten von betroffenen Personen genügen, dass bereits polizeilich bekannt ist, dass diese eine Straftat begehen wird. Dann ist es allerdings widersinnig, eine Zuständigkeit des BKA über einen Zeitraum von drei Monaten regeln, zumal die Vorbereitungs- und Versuchsstrafbarkeit schwerer

Kriminalitätsformen gem. § 30 StGB bereits zur Strafverfolgung berechtigt. Sollen aber durch diese Vorschrift fehlende länderpolizeiliche Kompetenzen „überholt“ oder „kompensiert“ werden, würde diese Vorschrift als Umgehung landesrechtlicher Zuständigkeiten wirken.

d) Hinsichtlich der Befugnis gem. § 10b Abs. 1 Nr. 3 BKAG-E wird eine Gefahr zwischen der betroffenen Person (Satz 1 1. Halbsatz) und einer weiteren Person im Vorfeld einer Straftat unterstellt, die keine Verbindung durch Telekommunikation voraussetzt, sondern jegliche persönliche Interaktion betrifft. Damit wird tief in die Persönlichkeit, das familiäre Gefüge und den privaten Umgang mit anderen Personen eingegriffen, indem Observationsüberlegungen in Überwachung der Telekommunikation umgemünzt werden. Mithin geht es hier der Sache nach um eine Überwachung Nichtbetroffener, die nicht voraussetzt, dass von ihnen eine Gefahr für die öffentliche Sicherheit und Ordnung ausgeht. Damit handelt es sich um eine in ihren Voraussetzungen und Folgen unbestimmte Eingriffsnorm. Als Begründung für eine Sicherungsanordnung soll eine nicht näher nachzuweisende Erwartung des veranlassenden Beamten beim BKA ausreichen, dass zukünftig Straftaten begangen werden (RefE S. 58/59).

Gegen die Ermöglichung einer Sicherungsanordnung gegen weitere Personen, die nicht unter Verdacht stehen, spricht auch, dass der Grundrechtseingriff andere Personen einbezieht, die ebenfalls mit der weiteren Person kommunizieren. In der Praxis wäre namentlich an statistische Wahrscheinlichkeiten zu denken, insbesondere Straftaten, die während Demonstrationen begangen würde. Dann wären die Demonstrationsteilnehmer diese weiteren Personen, wenn der potentielle Straftäter alleine schon bekannt ist. Vergleichbares würde für Sportveranstaltungen oder öffentliche Reiseunternehmen gelten. Die Folge wäre eine dichte Raumüberwachung der Internetdienste und der Telekommunikation allein aus präventiv-polizeilichen Zwecken, die nicht richterlich kontrolliert ist und keinen sonstigen Anforderungen an den Grundrechtsschutz genügt.

Einem allgemeinem Kriminalisierungsverdacht haben der EuGH und das BVerfG stets widersprochen. Für präventiv-polizeiliche Aufgaben sieht das geltende Recht bereits hinreichende Befugnisse für Bundespolizei, Zollfahndung und Landespolizeien vor, so dass es einer vorauseilenden Sammlung von Verkehrsdaten durch das BKA als Zentralstelle in den gem. § 10b Abs. 1 Ziff. 3 BKAG-E anzunehmenden Fällen nicht bedarf.

* * *