



Ausschussdrucksache 21(6)122c
vom 5. Oktober 2026, 15:39 Uhr

Schriftliche Stellungnahme
der Sachverständigen Martina Link

Öffentliche Anhörung

zu dem Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Einführung einer IP-Adressspeicherung und
Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren
BT-Drucksachen 21/6581, 21/7154



Bundeskriminalamt • 65173 Wiesbaden

Per E-Mail
Deutscher Bundestag
Ausschuss für Recht und Verbraucherschutz
Platz der Republik 1
11011 Berlin

Am Treptower Park 5-8
12435 Berlin

Zentrale Postanschrift:
65173 Wiesbaden

Tel. +49 611 55-0

bearbeitet von:
Leitungsstab 4

www.bka.de

Gesetzesentwurf zur Einführung einer IP-Adressenspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren

hier: Stellungnahme Bundeskriminalamt

Berlin, 05.10.2026
Seite 1 von 8

Vorbemerkung

Die zunehmende Digitalisierung nahezu aller Lebensbereiche hat auch viele Kriminalitätsphänomene verändert. Die Vorbereitung, Planung, Durchführung und Begehung von Straftaten verlagern sich zunehmend in den digitalen Raum. Dies gilt z. B. für die Kommunikation zwischen Tatbeteiligten, die Verbreitung von kinderpornografischem Material, die Vertreibung von Betäubungsmitteln oder auch die Vorbereitung und Planung von Anschlagstaten.

Mit zunehmender Nutzung digitaler Technologien im Zusammenhang mit Straftaten steigt die Bedeutung der dabei entstehenden digitalen Spuren. Bei der Nutzung von Smartphones, Computern, Messenger-Diensten oder internetbasierten Plattformen werden zahlreiche Daten erzeugt. Hierzu zählen u. a. Verkehrsdaten, wie Standortdaten sowie IP-Adressen. Diese Spuren können Rückschlüsse auf Planungen, Handlungen, Abläufe und Kommunikationsbeziehungen ermöglichen. Daher sind sie für Polizeibehörden zur Aufklärung und auch Vereitelung von Straftaten essentiell. Digitale Spuren können insbesondere für die Identifizierung von Tätern von erheblicher Bedeutung sein, da sie Verbindungen zwischen einer Person und einer konkreten Handlung oder einem Tatgeschehen aufzeigen können. Hinzu kommt, dass sie oftmals die vielversprechendste oder gar einzige Möglichkeit zur Identifizierung von Tätern bieten.



Seite 2 von 8

Digitale Spuren sind in Deutschland sehr flüchtig. Seitens der Provider wird in Bezug auf Verkehrsdaten maximal eine Speicherung zu Geschäftszwecken für höchstens eine Woche vorgenommen. Straftaten oder entsprechende Planungen werden den Strafverfolgungsbehörden sehr häufig jedoch erst mit zeitlichem Verzug bekannt. Eine Abfrage von Informationen, die zur Aufklärung oder Vereitelung von Straftaten notwendig sind, kann nur dann Erfolg haben, wenn diese Daten zum Zeitpunkt der Abfrage noch gespeichert sind.

Mit der Einführung einer Pflicht zur Speicherung von IP-Adressen wird den Strafverfolgungsbehörden und anderen berechtigten Stellen die Chance erhöht, einen Anschlussinhabers anhand einer IP-Adresse zuverlässig identifizieren zu können. Darüber hinaus schafft der Gesetzgeber für Verkehrsdaten, die noch zu Geschäftszwecken vorhanden sind, u. a. für den Bereich der Strafverfolgung das Instrument der Sicherungsanordnung. Dadurch können die Behörden die Sicherung von Verkehrsdaten beim Telekommunikationsanbieter veranlassen, sofern und solange die rechtlichen oder tatsächlichen Voraussetzungen einer Datenerhebung noch nicht vorliegen.

Für das Bundeskriminalamt sind die Befugnisse und damit auch die neuen Möglichkeiten sowohl als Ermittlungsbehörde als auch im Rahmen seiner Aufgabenwahrnehmung als Zentralstelle und Gefahrenabwehrbehörde von erheblicher Bedeutung.



Seite 3 von 8

IP-Adressenspeicherung

Bei Straftaten im digitalen Raum ist vor allem die IP-Adresse in einer Vielzahl der Fälle der einzige und wertigste Ansatz zur Identifizierung von Tatverdächtigen. Mit ihrer Hilfe lässt sich ermitteln, über welchen Anschluss ein Täter die Internetverbindung hergestellt hat, über die eine konkrete Straftat begangen wurde.

Durch das Aussetzen der in 2015 gesetzlich geschaffenen Regelung für eine zeitliche Speicherung sind die Polizeibehörden derzeit auf das Speicherverhalten der Internetzugangsanbieter angewiesen. Diese speichern die IP-Adresse in der Regel zu Geschäftszwecken für höchstens eine Woche. Der Erfolg oder Nichterfolg einer Identifizierung ist somit derzeit vom freiwilligen Speicherverhalten der Internetzugangsdienste, das aber nie länger als eine Woche beträgt, und vom Zeitpunkt des Bekanntwerdens der zur Tatbegehung genutzten IP-Adresse abhängig.

So wurde beispielsweise in einem Ermittlungsverfahren gegen unbekannte Betreiber einer kriminellen Handelsplattform, über welche Betäubungsmittel sowie Cybercrime-as-a-Service angeboten wurden, eine IP-Adresse eines umsatzstarken Betäubungsmittel-Verkäufers bekannt. Diese IP-Adresse hatte der Täter acht Wochen zuvor genutzt.

Aufgrund der fehlenden Speicherfrist lief die Anfrage ins Leere, der Betäubungsmittel-Verkäufer konnte nicht identifiziert werden.

Sofern neben der IP-Adresse alternative Möglichkeiten zur Identifizierung von Tatverdächtigen bestehen, sind diese häufig mit eingriffsintensiveren Maßnahmen verbunden: Liegen beispielsweise zusätzliche Hinweise auf einen Social-Media-Account vor, welcher dem Tatverdächtigen zuzuordnen ist, würden beim Digitale-Dienste-Anbieter Nutzungsdaten zum Account angefragt. Sollte auch darüber die Identifizierung des Tatverdächtigen nicht gelingen, würden Informationen zu weiteren Accounts angefragt. Die Abfrage von Nutzungsdaten stellt jedoch eine eingriffsintensivere Maßnahme als eine Zuordnung zu Kundenbestandsdaten mittels polizeibekannter IP-Adresse zum Tatzeitpunkt dar.

Mit der gesetzlichen Regelung zur Speicherung von IP-Adressen wird es zukünftig effizient und zielgerichtet möglich sein, im Zeitraum von drei Monaten den von einem Tatverdächtigen oder Störer genutzten Anschluss zu identifizieren, ohne dass andere zeitaufwändigere und eingriffsintensivere Maßnahmen zur Nutzeridentifizierung vorgenommen werden müssen.



Seite 4 von 8

Der EuGH hat mit seinen Urteilen vom 20.09.2022 und 30.04.2024 dem deutschen Gesetzgeber Leitplanken für eine rechtssichere Speicherung von Daten gegeben. Hierbei wurde dargelegt, dass eine allgemeine und unterschiedslose Speicherung von IP-Adressen rechtlich zulässig ist, sofern die Speicherung auf das zeitlich Nötigste beschränkt ist.

Bei strukturierten Meldeprozessen wie z. B. dem sog. NCMEC¹-Prozess würde bereits eine mehrwöchige Speicherfrist zu einem deutlichen Anstieg der Identifizierungsansätze führen. Derartige Meldeprozesse decken jedoch nur einen kleinen Teilbereich der polizeilichen Arbeit ab. Die polizeiliche Praxiserfahrung zeigt, dass mit einer Speicherdauer von drei Monaten voraussichtlich ein relevanter Teil der maßgeblichen polizeilichen Sachverhalte abgedeckt werden kann, so beispielsweise auch zum oben aufgeführten Sachverhalt die Identifizierung des Betreibers einer kriminellen Handelsplattform. Darüber hinaus existieren jedoch auch Bedarfslagen, bei denen eine Speicherfrist von 3 Monaten nicht ausreichend sein dürfte. Dies trifft insbesondere auf komplexe Ermittlungsverfahren zu.

Wichtig ist aus polizeifachlicher Sicht, dass die angedachte Frist zur Umsetzung der Speicherpflicht für die Internetzugangsdienste in § 230 Abs. 17 TKG-E so kurz wie möglich ausgestaltet wird. Durch diese Frist wird den Internetzugangsdiensten ausreichend Zeit gegeben, nach Inkrafttreten des Gesetzes die gesetzlichen und technischen Anforderungen für die Speicherung der IP-Adressen zu schaffen. Im aktuellen Gesetzesentwurf sind hierfür sechs Monate vorgesehen. Das bedeutet folglich, dass erst sechs Monate nach Inkrafttreten des Gesetzes für die Ermittlungsbehörden die Möglichkeit besteht, erfolgreich bis zu 3 Monate alte IP-Adressen abzufragen. Die Internetzugangsanbieter erfüllen in vielen anderen EU-Mitgliedsstaaten vergleichbare Speicherverpflichtungen. Sie verfügen somit über Erfahrungen in der Umsetzung derartiger gesetzlicher Anforderungen. Vor diesem Hintergrund könnte eine Umsetzung auch in kürzerer Frist gelingen.

¹ Der NCMEC-Prozess bezeichnet den Prozess, in dem das halbstaatliche National Center für exploited and missing Children Meldungen von Providern über den Verdacht der Verbreitung kinder- und jugendpornografischen Materials direkt dem BKA ausleitet. Im BKA sind hierzu im Jahr 2025 220.141 Meldungen eingegangen.



Neustrukturierung der Regelungen für die Erhebung von Verkehrs- und Nutzungsdaten

Verkehrs- und Nutzungsdaten spielen in der Ermittlungspraxis eine wichtige Rolle. Sie geben z. B. Auskunft darüber, wer mit wem, wann und wie lange telefoniert hat oder online war. Standortdaten, als Unterfall dieser Datenkategorie, geben den Ermittlungsbehörden einen Hinweis darauf, wo sich ein Mobiltelefon während seiner Nutzung befand. Anhand der Daten lässt sich auch nachzuvollziehen, wie und wann ein Nutzer einen Digitalen Dienst zur Vorbereitung oder Begehung einer konkreten Tat nutzte. Diese Informationen sind wertvolle Spurenansätze für die Aufklärung von Straftaten oder liefern sehr häufig die ausschlaggebenden Beweise für den Tatnachweis.

Die den Telekommunikationsanbietern (TK-Anbieter) und Digitalen Diensten gegenüber bereits vorhandenen Datenerhebungsbefugnisse für Verkehrs- und Nutzungsdaten werden neu strukturiert und einander angeglichen. Dies wird aus Sicht des BKA begrüßt. Zudem wird eine neue Befugnis zur Sicherungsanordnung für Verkehrsdaten gegenüber den TK-Anbietern eingeführt. Darüber hinaus wird klargestellt, dass die Möglichkeit eine Funkzellenabfrage durchzuführen, auch bei Straftaten von im Einzelfall erheblicher Bedeutung zulässig ist.

Zugleich wird aus polizeifachlicher Sicht eine ausgewogenere Regelung zur Erhebung von anschlussbezogenen Standortdaten (retrograd sowie in Echtzeit) geschaffen, insbesondere vor dem Hintergrund, dass diese Daten in der Regel nur noch wenige Tage zu Geschäftszwecken gespeichert werden.

Die neu strukturierten Befugnisse sind aus Sicht des BKA praxisnah ausgestaltet. Die Regelungen werden zur verbesserten Aufklärung von Straftaten von im Einzelfall erheblicher Bedeutung und schwerwiegender Kriminalität beitragen. Sowohl das BKA als auch die Länder berichten seit längerem über diesen Rechtsänderungsbedarf bezogen auf die Verkehrsdatenerhebung nach § 100 g StPO. Hier wird nun Abhilfe geschaffen.

Das neue Instrument zur vorläufigen Sicherung von Verkehrsdaten beim TK-Anbieter wird dann, wenn die Löschung von möglicherweise beweisrelevanten Daten droht, obwohl bereits der Verdacht einer Straftat polizeibekannt ist, seine Wirkung entfalten: Beweisrelevante Daten können nach richterlicher Genehmigung noch vollständig erhoben werden.

Der Bedarf wird an folgendem Beispiel deutlich: Unverzüglich nach Bekanntwerden eines mehrere Tage zuvor erfolgten Tötungsdeliktes dürfen mit der Neuregelung beweisrelevante Funkzellendaten an den mutmaßlichen Handlungsorten des Täters in der Tatvor- und Tatnachbereitungsphase beim TK-Anbieter gesichert werden. Dies wird veranlasst, noch während ein Ausschussdrucksache 21(6)122c



Seite 6 von 8

richterlicher Beschluss zur Erhebung der Daten beantragt wird. Notwendig ist das, da die beweiserheblichen Funkzellendaten bereits nach Ablauf von 8 Tagen bei den Netzanbietern routinemäßig aus Datenschutzgründen gelöscht werden müssen. Die von der Justiz vorzunehmende Verhältnismäßigkeitsprüfung für die Datenerhebung muss sorgfältig durchgeführt werden. Durch die Sicherungsanordnung für Verkehrsdaten wird eine Beweisvernichtung während dieses Prüfprozesses ausgeschlossen.

Von großem Vorteil für die Praxistauglichkeit dieser Maßnahme ist es, dass die Anordnung durch die Staatsanwaltschaft oder bei Gefahr im Verzug auch durch ihre Ermittlungspersonen ausgesprochen werden kann.

Die Polizei darf künftig auch bei Anbietern Digitaler Dienste Log-In-Daten zu einem Account erheben, die zur Nutzeridentifizierung notwendig sind. Bislang war dies ausschließlich der Staatsanwaltschaft vorbehalten. Eine derartige Befugnis soll der Polizei als Strafverfolgungsbehörde zukünftig auch gegenüber Telekommunikationsdiensten zur Verfügung stehen. Für diese Datenerhebung war bislang ein richterlicher Beschluss notwendig. Dadurch ergeben sich weitere Erleichterungen für die Polizei und Justiz. Außerdem werden bürokratische Aufwände reduziert.

Sicherungsanordnung für das BKA als Zentralstelle und zur Gefahrenabwehr

Die Befugnis der Sicherungsanordnung ist für das BKA auch als Zentralstelle sowie für seine Zuständigkeit zur Abwehr von Gefahren des internationalen Terrorismus erforderlich.

Der Gesetzentwurf berücksichtigt dies bereits bei der Ausgestaltung der mit dieser Maßnahme korrespondierenden Verarbeitungsbefugnis für die TK-Anbieter im TKG (vgl. § 176 Abs. 1 Nr. 2 TKG-E).

Im Übrigen verweist das BKA hinsichtlich der Notwendigkeit einer Ergänzung des BKAG um diese Befugnis auf die entsprechenden Ausführungen in seiner Stellungnahme zum Gesetzentwurf „Digitale Ermittlungsbefugnisse“ vom 17.09.2026 unter Punkt 3 (Ausschussdrucksache 21(4)214 F vom 18.09.2026).



Erforderlicher weiterer Anpassungsbedarf der aktuellen Rechtslage

In Bezug auf die Ausformung der Sicherungsanordnung besteht aus Sicht des BKA noch folgender Anpassungsbedarf:

1) Die Befugnis zur Sicherungsanordnung sollte in der StPO auch gegenüber Digitalen Diensten geschaffen werden. Im TDDDG² ist derzeit zudem keine Verarbeitungsbefugnis für Nutzungsdaten zur Erfüllung von Sicherungsanordnungen durch Anbieter digitaler Dienste nach nationalem Strafverfahrens- oder Gefahrenabwehrrecht vorgesehen. Die E-Evidence-Verordnung (EU) 2023/1543 (E-Evidence VO) sieht eine derartige Befugnis für das grenzüberschreitende Strafverfahren jedoch vor. Aufgrund den nach der E-Evidence VO geltenden sog. Entsprechungsklauseln³ kann sich eine Europäische Sicherungsanordnung deutscher Strafverfolgungsbehörden bislang nur bezogen auf Verkehrsdaten an Telekommunikationsdienste richten.

Die mit diesem Gesetz neu eingefügte Verarbeitungsbefugnis für Nutzungsdaten zur Erfüllung einer Europäischen Sicherungsanordnung nach dem E-Evidence-Mechanismus (vgl. Artikel 8 des Gesetzentwurfs zur Einführung eines neuen § 13a TDDDG) berücksichtigt zudem nur den Fall von Ersuchen aus anderen EU-Mitgliedsstaaten. Möchte hingegen eine deutsche Strafverfolgungsbehörde in Deutschland gegenüber einem Anbieter Digitaler Dienste Nutzungsdaten sichern lassen, so steht weder ihr noch dem Dienstanbieter bislang eine entsprechende Befugnis zur Verfügung. Daher votiert das BKA aus polizeifachlicher Sicht für eine entsprechende Ergänzung der StPO und für die Regelung einer korrespondierenden Verarbeitungsbefugnis auch für die Anbieter Digitaler Dienste.

2) Die vorgesehenen Befugnisse zur Sicherungsanordnung sind auf die Sicherung von Verkehrsdaten beschränkt. Mit diesem Regelungsumfang wird die bisherige Regelungslage den Erfordernissen der E-Evidence VO allerdings nicht gerecht. Durch die E-Evidence VO wurde zum 18.08.2026 das korrespondierende grenzüberschreitende Ermittlungsinstrument der Europäischen Sicherungsanordnung für sämtliche Datenkategorien, also auch Inhaltsdaten, in den Wirkbetrieb überführt.

Es ist bisher nicht vorgesehen, dass das in der E-Evidence VO vorgesehene Instrument der Sicherungsanordnung auch für die gespeicherten Inhaltsdaten bei TK-Anbietern (z. B. E-Mail-Anbieter) oder Inhalts- und Nutzungsdaten bei den Anbietern Digitaler Dienste ins nationale Strafverfahrensrecht eingeführt wird.

² Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz.

³ D. h. eine vergleichbare Anordnung hätte in einem vergleichbaren nationalen Fall unter denselben Voraussetzungen ergehen können.



Seite 8 von 8

Eine derartige Regelungslage wäre aus Sicht der Strafverfolgungsbehörden jedoch fachlich sinnvoll, um z. B. in einem deutschen Strafverfahren gegenüber einem französischen Anbieter eine entsprechende Sicherungsanordnung über den E-Evidence-Prozess aussprechen zu können.

Die fehlende Regelungslage führt dazu, dass für ein Strafverfahren eines anderen EU-Mitgliedsstaates ein deutscher E-Mail-Anbieter gespeicherte Inhaltsdaten und zugehörige Verkehrsdaten sichern muss. Dies kann für ein deutsches Strafverfahren zwar bezogen auf Verkehrsdaten, nicht jedoch für die gleichermaßen ermittlungsrelevanten Inhaltsdaten angeordnet werden.

Die E-Evidence VO sieht in diesen Fällen jedoch vor, dass Inhalts- und zugehörige Verkehrsdaten gesichert werden, um einen Beweismittelverlust zu verhindern. Dies soll verhindern, dass Täter diese Daten aus dem Account löschen können, bevor die eigentliche Datenerhebung stattfinden konnte. Aus polizeilicher Sicht wären daher entsprechende Befugnisnormen in der StPO notwendig und empfehlenswert, da ansonsten nur auf die allgemeinen Datenerhebungsbefugnisse der §§ 94 ff. StPO verwiesen werden könnte.

Auf diese Anpassungserfordernisse hat bereits der Vizepräsident des Bundeskriminalamts, Herr Kurenbach, in der öffentlichen Anhörung zur E-Evidence VO am 12.01.2026 hingewiesen.

Fazit

Das Bundeskriminalamt begrüßt die mit dem Gesetzentwurf vorgesehene Schaffung der entsprechenden Befugnisse ausdrücklich. Der Gesetzentwurf umfasst wichtige Regelungsinhalte, die den Strafverfolgungsbehörden von Bund und Ländern bedeutsame und effiziente Möglichkeiten zur Identifizierung von Tatverdächtigen, Aufklärung von Straftaten und Abwehr von Gefahren bieten. Mit Einführung dieser gesetzlichen Regelungen wird in vielen Fällen und in unterschiedlichsten Deliktsbereichen vermieden, dass Täter anonym bleiben und schwere Straftaten nicht aufgeklärt werden können. Dies trägt nicht zuletzt auch zum Schutz von Betroffenen, die Opfer einer Straftat geworden sind, bei.

Zu den wenigen aus polizeilicher Sicht noch offenen Anpassungsbedarfen insbesondere im Zuge der Umsetzung der E-Evidence VO hat das BKA in der Stellungnahme ausgeführt.