



Ausschussdrucksache 21(6)122g
vom 6. Oktober 2026, 22:28 Uhr

Schriftliche Stellungnahme
des Sachverständigen Guido Limmer

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

Bayerisches Landeskriminalamt



Stellungnahme für die Sachverständigenanhörung des Ausschusses für Recht und
Verbraucherschutz im Deutschen Bundestag am 07.10.2026

zum Thema

**Einführung einer IP-Adressspeicherung und Weiterentwicklung der
Befugnisse zur Datenerhebung im Strafverfahren (BT-Drs. 21/6581)**

Vorbemerkung

Die Digitalisierung nahezu aller Lebensbereiche prägt auch die Entwicklung der Kriminalität. Straftaten werden im digitalen Raum vorbereitet, begangen und verschleiert; Kommunikation, Tatplanung, Vermögensverschiebungen und der Vertrieb illegaler Güter erfolgen zunehmend über internetbasierte Dienste. Dies betrifft insbesondere sexualisierte Gewalt gegen Kinder und Jugendliche, Cybercrime, Betrugsdelikte, den illegalen Handel mit Betäubungsmitteln und Waffen, extremistische Straftaten sowie die Vorbereitung schwerer Gewalttaten.

Digitale Spuren sind daher für die polizeiliche Gefahrenabwehr und Strafverfolgung von herausragender Bedeutung. Häufig bildet eine IP-Adresse den ersten, mitunter sogar den einzigen belastbaren Ansatz, um eine digitale Handlung einem Anschluss und in weiteren Ermittlungsschritten einer Person zuordnen zu können. Fehlen die entsprechenden Daten beim Diensteanbieter, da diese die Daten bislang nur speichern, soweit und solange dies für ihre betrieblichen Zwecke erforderlich ist, kann der Ermittlungsansatz endgültig verloren sein. Dies kann dazu führen, dass Tatverdächtige nicht identifiziert, Tatserien nicht unterbrochen und Gefahren nicht rechtzeitig abgewehrt werden können.

Vor diesem Hintergrund wird der Gesetzentwurf **aus polizeifachlicher Sicht grundsätzlich ausdrücklich begrüßt**. Die Einführung einer gesetzlichen Speicherpflicht von IP-Adressen, des neuen Instruments der Sicherungsanordnung und die Weiterentwicklung der strafprozessualen Befugnisse zur Erhebung und zum Abruf von Verkehrs- und Nutzungsdaten können die polizeiliche Arbeit wirksamer, schneller und rechtssicherer machen. Positiv ist insbesondere, dass der Gesetzentwurf nicht nur neue Zugriffsmöglichkeiten schafft, sondern vorhandene Befugnisse neu strukturiert und auf praktische Bedarfslagen ausrichtet.

Aus Sicht der Bayerischen Polizei besteht jedoch noch zwingender Änderungsbedarf. Die Stellungnahme konzentriert sich auf drei Aspekte:

- Die Befugnis zum Erlass einer **Sicherungsanordnung** muss auch für die **Gefahrenabwehr durch die Polizeien der Länder** rechtlich ermöglicht werden (sog. Länderöffnungsklausel).
- Die Sicherungsanordnung darf nicht auf Verkehrsdaten beschränkt bleiben, sondern muss **alle Datenkategorien – insbesondere Inhaltsdaten –** erfassen.
- Im **§ 175 Absatz 3 Nummer 2 TKG-E** muss aus Gründen der **Normenklarheit** ein **Rechtsgüterkatalog** eingefügt werden.

Dieser Nachbesserungsbedarf entspricht in seiner Zielrichtung den Forderungen des Bundesrates in dessen Stellungnahme vom 12. Juni 2026 (BR-Drucksache 263/26).

1. Einführung einer IP-Adressspeicherung

Die vorgesehene Speicherung von IP-Adressen ist ein wichtiger Beitrag zur Aufklärung von Straftaten und zur Abwehr von Gefahren. Dynamische IP-Adressen ermöglichen grundsätzlich die Zuordnung einer zu einem bestimmten Zeitpunkt erfolgten Internetnutzung zu einem Anschluss. Diese Zuordnung ist jedoch nur möglich, wenn beim Internetzugangsdiensteanbieter noch die hierfür erforderlichen Daten vorhanden sind.

In der polizeilichen Praxis werden Sachverhalte vielfach erst mit zeitlicher Verzögerung bekannt. Dies gilt etwa bei Meldungen aus dem Ausland, bei umfangreichen Auswertungen sichergestellter Datenträger, bei zunächst verdeckt gebliebenen Betrugstaten oder bei Taten zum Nachteil von Kindern und Jugendlichen. Eine allein von der freiwilligen und geschäftlichen Speicherungspraxis der Anbieter abhängige Datenverfügbarkeit wird diesen tatsächlichen Abläufen nicht gerecht.

Eine gesetzlich bestimmte und zeitlich begrenzte Speicherpflicht kann demgegenüber verlässliche Rahmenbedingungen schaffen. Sie ermöglicht zielgerichtete Anschlussinhaberfeststellungen und kann zugleich vermeiden, dass zur Identifizierung einer Person auf breiter angelegte oder eingriffsintensivere Ermittlungsmaßnahmen ausgewichen werden muss.

2. Sicherungsanordnung auch für die Gefahrenabwehr durch die Länder

2.1. Polizeifachlicher Bedarf

Die neu vorgesehene Sicherungsanordnung ist ein praxisrelevantes Instrument gegen drohenden Datenverlust. Sie soll gewährleisten, dass bereits vorhandene oder innerhalb des Anordnungszeitraums anfallende Verkehrsdaten nicht gelöscht werden, während die Voraussetzungen für ihre spätere Erhebung geprüft und die hierfür erforderlichen Entscheidungen eingeholt werden. Die bloße Sicherung ist dabei von der späteren Übermittlung und dem Abruf der Daten zu unterscheiden. Sie friert einen vorhandenen Datenbestand lediglich vorläufig ein und verhindert damit, dass eine spätere, rechtlich zulässige Datenerhebung allein durch Zeitablauf vereitelt wird.

Der Bedarf für den Erlass einer Sicherungsanordnung besteht nicht nur in der Strafverfolgung und bei den im Gesetzentwurf erfassten Bundesbehörden, sondern in gleicher Weise in der Gefahrenabwehr durch die Polizeien der Länder. Die allgemeine Gefahrenabwehr und insbesondere die Verhütung von Straftaten liegen in erster Linie in der Zuständigkeit der Länder. Landespolizeien müssen beispielsweise bei Gefahren für Leib, Leben oder Freiheit, bei terroristischen Bedrohungslagen, bei angekündigten schweren Gewalttaten oder bei akuten Gefahren für besonders gewichtige Rechtsgüter unverzüglich handeln können. Sie nehmen daher ebenfalls Aufgaben im Rahmen der Terrorismusabwehr wahr und schützen Rechtsgüter von vergleichbar hohem verfassungsrechtlichem Gewicht.

Gerade in dynamischen Gefahrenlagen kann es erforderlich sein, zunächst weitere Erkenntnisse zu gewinnen, Zuständigkeiten zu klären, einen Sachverhalt zu bewerten oder eine richterliche Entscheidung für die eigentliche Datenerhebung herbeizuführen. Werden währenddessen beim Telekommunikationsunternehmen Daten routinemäßig gelöscht, kann ein entscheidender Ansatz für die Identifizierung eines Störers oder die Lokalisierung einer Gefahrenquelle unwiederbringlich verloren gehen.

Die Bayerische Polizei hatte in jüngerer Vergangenheit verschiedene herausragende Einsatzlagen zu bewältigen. Beispielhaft können die lebensbedrohlichen Einsatzlagen am 22. Juli 2016 am Münchner Olympia Einkaufszentrum, am 5. September 2024 am Münchner Karolinenplatz und am 8. Juli 2026 am Welfen-Gymnasium in Schongau genannt werden. In der Anfangsphase von derartigen Einsatzlagen ist oft längere Zeit nicht nur die Täteridentität, sondern auch die Anzahl der Tatbeteiligten, deren Aufenthalt,

bzw. ob eine Tatbeteiligung überhaupt vorliegt, ungeklärt. Bestandsdaten, Verkehrsdaten und Inhaltsdaten (z. B. live gestreamte Videos zum Tathergang) sind äußerst wichtige Anhaltspunkte, um der Polizei eine bestmögliche Gefahrenabwehr zu ermöglichen. Gerade in solchen Szenarien braucht die Polizei möglichst viele und vor allem wertige Informationen, um Menschenleben zu schützen und die Gefahren rasch und erfolgreich zu bekämpfen.

Darüber hinaus ließen sich bei der Mitigation von Gefahren durch Intensivtäter, im Bedrohungsmanagement, bei der gezielten Manipulation und Erniedrigung von Kindern durch sog. COM-Netzwerke, bei Vermisungen und Suizidankündigungen Menschenleben schützen, wenn die Polizei zuverlässig, schnell und gezielt die wesentlichen Informationen erhielte.

2.2. Erforderliche Öffnung der „ersten Tür“

Nach dem vom Bundesverfassungsgericht entwickelten Doppeltürmodell (vgl. Beschluss vom 27. Mai 2020 – 1 BvR 1873/13, 2618/13 – Bestandsdatenauskunft II) muss der Gesetzgeber sowohl für die Übermittlung der Daten durch die Telekommunikationsdiensteanbieter als auch für den Abruf der Daten durch die Behörden jeweils für sich genommen verhältnismäßige Rechtsgrundlagen schaffen.

Der bislang vorgesehene § 176 TKG-E öffnet die „erste Tür“ der Übermittlungsbefugnis bislang nur strafprozessual und gefahrenabwehrrechtlich für die dort abschließend genannten Behörden (Bundeskriminalamt, Bundespolizei). Eine entsprechende Befugnis zum Erlass einer Sicherungsanordnung ist für die Länderpolizeien hingegen nicht vorgesehen. Selbst wenn ein Landesgesetzgeber nun eine verhältnismäßige Abrufregelung als „zweite Tür“ schaffen würde, liefe diese mangels korrespondierender Übermittlungsbefugnis des Telekommunikationsanbieters ins Leere.

Diese Beschränkung überzeugt weder aus der föderalen Zuständigkeitsordnung noch aus polizeifachlicher Sicht. Das Schutzbedürfnis der betroffenen Rechtsgüter hängt nicht davon ab, ob im konkreten Fall eine Bundes- oder eine Landesbehörde zuständig ist. Die Bayerische Polizei nimmt originäre Aufgaben der Gefahrenabwehr wahr und trägt insbesondere auch bei länderübergreifenden oder internationalen Sachverhalten Verantwortung für den Schutz der Bevölkerung.

2.3. Änderungsvorschlag

§ 176 TKG-E sollte deshalb so ausgestaltet werden, dass Telekommunikationsdiensteanbieter auch Sicherungsanordnungen der für die Gefahrenabwehr zuständigen Behörden der Länder erfüllen müssen. Als regelungstechnisches Vorbild bietet sich der bestehende § 174 Absatz 3 TKG an. Denkbar ist insbesondere eine Verweisung auf die dort genannten Behörden und materiellen Voraussetzungen.

Aus polizeifachlicher Sicht sollte die Regelung jedenfalls folgende Punkte gewährleisten:

- Einbeziehung der Polizeien der Länder in den Kreis der anordnungsberechtigten Gefahrenabwehrbehörden,

- eine korrespondierende Verarbeitungsbefugnis und Verpflichtung der Diensteanbieter im TKG beziehungsweise – soweit digitale Dienste betroffen sind – im TDDDG,
- klare, bundeseinheitlich anschlussfähige Rechtsgüter- und Eingriffsschwellen sowie
- die Möglichkeit der Länder, hierzu spiegelbildliche Abruf- beziehungsweise Anordnungsbefugnisse in ihren Polizeigesetzen zu schaffen.

Mit der vorgeschlagenen Länderöffnungsklausel würde nicht automatisch eine Datenerhebung einhergehen. Die eigentliche Erhebung müsste weiterhin auf einer eigenständigen Befugnis beruhen und deren jeweilige Voraussetzungen erfüllen. Es geht vielmehr darum, einen endgültigen Datenverlust bis zur rechtlichen Prüfung und tatsächlichen Entscheidung zu verhindern.

3. Einbeziehung weiterer Datenkategorien und digitaler Dienste

3.1. Beschränkung auf Verkehrsdaten greift zu kurz

Der Gesetzentwurf beschränkt die strafprozessuale Sicherungsanordnung auf die Sicherung von Verkehrsdaten. Diese Beschränkung wird den praktischen Erfordernissen digitaler Ermittlungen nicht vollständig gerecht. Beweiserhebliche Daten befinden sich heute nicht nur bei klassischen Telekommunikationsunternehmen und nicht nur in Form von Verkehrsdaten. Relevante Informationen werden insbesondere auch bei E-Mail-Diensten, Messenger-Diensten, sozialen Netzwerken, Cloud-Diensten, Plattformen und sonstigen digitalen Diensten gespeichert.

Je nach Sachverhalt können neben Verkehrsdaten insbesondere folgende Kategorien für die spätere Beweiserhebung entscheidend sein:

- **Bestandsdaten**, etwa zur Zuordnung eines Kontos oder Anschlusses,
- **Nutzungsdaten**, insbesondere Anmelde-, Zugriffs- und Protokolldaten eines digitalen Dienstes, sowie
- **Inhaltsdaten**, etwa gespeicherte Nachrichten, E-Mails, Bilder, Videos, Sprach- oder sonstige Dateien.

Auch diese Daten können kurzfristig gelöscht, automatisiert überschrieben oder durch Nutzerinnen und Nutzer entfernt werden. Besteht bereits ein konkreter Ermittlungsanlass, darf die spätere rechtmäßige Beweiserhebung nicht daran scheitern, dass die betreffende Datenkategorie von der Sicherungsanordnung nicht erfasst wird.

3.2. Sicherung ist noch keine Erhebung

Die Erweiterung auf weitere Datenkategorien bedeutet keine voraussetzungslose Herausgabe der Daten an die Strafverfolgungsbehörden. Zwischen der vorläufigen Sicherung beim Anbieter und der späteren Erhebung durch die Behörde ist klar zu unterscheiden. Die Sicherungsanordnung dient allein der Bestandserhaltung. Ob und in

welchem Umfang die gesicherten Daten anschließend übermittelt und ausgewertet werden dürfen, richtet sich nach den jeweils einschlägigen Erhebungsbefugnissen und deren formellen und materiellen Voraussetzungen.

Eine differenzierte gesetzliche Ausgestaltung kann darüber hinaus der unterschiedlichen Eingriffsintensität der Datenkategorien Rechnung tragen. Erforderlich ist jedoch zunächst ein Instrument, das bei bestehendem Ermittlungsanlass den drohenden Verlust potenziell beweiserheblicher Daten verhindert.

3.3. Gleichlauf mit der E-Evidence-Verordnung

Für eine Erweiterung spricht auch der notwendige Gleichlauf mit der Verordnung (EU) 2023/1543 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel. Die europäische Regelung führt Sicherungsanordnungen für sämtliche Datenkategorien ein. Zugleich setzt der Erlass einer Europäischen Sicherungsanordnung voraus, dass eine vergleichbare Anordnung in einem entsprechenden innerstaatlichen Fall unter denselben Voraussetzungen erlassen werden könnte.

Bleibt das nationale Recht auf Verkehrsdaten beschränkt, kann dies die Handlungsfähigkeit deutscher Strafverfolgungsbehörden in grenzüberschreitenden Verfahren beeinträchtigen. Zudem wäre es schwer vermittelbar, wenn Behörden anderer Mitgliedstaaten gegenüber einem in Deutschland ansässigen Telekommunikationsanbieter die Sicherung weitergehender Daten veranlassen könnten und damit weitergehende Befugnisse hätten als deutsche Strafverfolgungsbehörden in einem vergleichbaren nationalen Verfahren.

3.4. Änderungsvorschlag

Es wird daher angeregt, die Rechtsgrundlage der strafprozessualen Sicherungsanordnung auf alle Datenkategorien (d. h. Bestands-, Verkehrs-, Nutzungs- und Inhaltsdaten) zu erweitern. Der vom Bundesrat vorgeschlagene neue § 95b StPO bietet hierfür einen geeigneten Regelungsansatz.

Korrespondierend sind die anbieterseitigen Verarbeitungsbefugnisse anzupassen. Dies betrifft insbesondere:

- § 176 TKG-E für Telekommunikationsdienste und
- eine entsprechende Regelung im TDDDG für Anbieter digitaler Dienste.

4. Normenklare Fassung des § 175 Absatz 3 Nummer 2 TKG-E

4.1. Erfordernis konkreter Rechtsgüter

§ 175 TKG-E regelt die Verarbeitung von Verkehrsdaten durch Telekommunikationsanbieter sowie deren Auskunftserteilung an berechnigte Stellen. Nach § 175 Absatz 3 Nummer 2 TKG-E soll eine Auskunft an Gefahrenabwehrbehörden unter anderem zur

Abwehr einer konkretisierten Gefahr für ein Rechtsgut von zumindest erheblichem Gewicht zulässig sein.

Vor dem Hintergrund des vom Bundesverfassungsgericht entwickelten und oben bereits genannten Doppeltürmodells bedarf es zweier korrespondierender Rechtsgrundlagen sowohl für die Übermittlung als auch für den Abruf der Daten. Insoweit muss aber gerade schon der Gesetzgeber der Übermittlungsregelung eine klare und abschließende Entscheidung treffen. Er muss aus Gründen der Normenklarheit seiner Regelungsverantwortung vollständig gerecht werden und die Übermittlungsregelung für sich genommen verhältnismäßig ausgestalten. Deren Konkretisierung darf er nicht späterer Gesetzgebung – insbesondere der Länder – überlassen (vgl. BVerfG, Beschluss vom 27. Mai 2020 – 1 BvR 1873/13, 2618/13 – Bestandsdatenauskunft II, Rn. 134, 201). Die Formulierung „Rechtsgut von zumindest erheblichem Gewicht“ ist unter Zugrundelegung dieser Entscheidung für die Übermittlungsbefugnis zu unbestimmt und unspezifisch. Die Länder sind bei der Ausgestaltung ihrer polizeirechtlichen Abrufbefugnisse gehalten, konkrete Rechtsgüter normenklar zu benennen, um auch einen rechtssicheren Vollzug gewährleisten zu können.

4.2. Orientierung an § 174 Absatz 3 TKG

Die für eine Datenübermittlung bzw. einen Datenabruf maßgeblichen Rechtsgüter sind im Einzelnen zu benennen. Als Vorbild kann der bereits geltende § 174 Absatz 3 TKG dienen. Die dort gewählte Benennung der Rechtsgüter schafft einen normenklaren Anknüpfungspunkt für korrespondierende fachrechtliche Befugnisse. Ein konkreter Katalog erhöht die Normenklarheit, verbessert die Vollzugssicherheit und erleichtert den Ländern eine schnelle und rechtssichere Umsetzung.

Aus polizeifachlicher Sicht sollte § 175 Absatz 3 Nummer 2 TKG-E deshalb ausdrücklich Gefahren oder konkretisierte Gefahren insbesondere für folgende Rechtsgüter erfassen:

- Leib,
- Leben,
- Freiheit der Person,
- sexuelle Selbstbestimmung,
- Bestand und Sicherheit des Bundes oder eines Landes sowie
- Güter der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt.

4.3. Formulierungsvorschlag

In Anlehnung an die Stellungnahme des Bundesrates könnte § 175 Absatz 3 Nummer 2 TKG-E wie folgt gefasst werden:

„eine für die Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung zuständige Behörde, soweit dies auf richterliche Anordnung im Einzelfall zur Abwehr einer Gefahr oder konkretisierten Gefahr für Leib, Leben, Freiheit der Person, die sexuelle Selbstbestimmung, den Bestand und die Sicherheit des Bundes oder eines Landes sowie Güter der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt, erforderlich ist,“

Nur so ist sichergestellt, dass Bund und Länder spiegelbildliche und deckungsgleiche Regelungen in Form einer zweiten Tür schaffen können.

Fazit

In der dynamischen Welt der digitalen Daten, in der wir die Verschiebung großer Teile der Kommunikation von der klassischen Telefonie hin zur Verwendung von Messengerdiensten und die Ausweitung der Verfügbarkeit von Anonymisierungsdiensten beobachten, sind wir aus polizeilicher Sicht dankbar, dass in Deutschland nunmehr ein tragfähiger Gesetzentwurf für eine verfassungs- und europarechtskonforme Regelungslage zur Speicherung von IP-Adressen vorgelegt wird.

Der Gesetzentwurf setzt aus Sicht der Bayerischen Polizei **wichtige und überfällige Impulse** für eine wirksame Strafverfolgung und Gefahrenabwehr im digitalen Raum. Die Speicherung von IP-Adressen verbessert die Möglichkeit, bislang anonyme Tatverdächtige zu identifizieren. Die Sicherungsanordnung kann verhindern, dass beweis- oder gefahrenabwehrrelevante Daten während laufender Prüfungs- und Entscheidungsprozesse gelöscht werden. Die Neustrukturierung der Befugnisse zur Datenerhebung trägt zu mehr Praxistauglichkeit bei.

Damit das Regelungskonzept seine Wirkung vollständig entfalten kann, sollten im weiteren Gesetzgebungsverfahren jedoch **drei Änderungen** vorgenommen werden:

Länderöffnungsklausel: Die anbieterseitige Rechtsgrundlage für Sicherungsanordnungen muss auch die Gefahrenabwehr durch die Polizeien der Länder erfassen. Die Länder müssen die Möglichkeit erhalten, korrespondierende Befugnisse in ihren Polizeigesetzen zu schaffen.

Erfassung sämtlicher Datenkategorien: Die strafprozessuale Sicherungsanordnung sollte Bestands-, Verkehrs-, Nutzungs- und Inhaltsdaten umfassen und neben Telekommunikationsdiensten auch Anbieter digitaler Dienste einbeziehen. Die Voraussetzungen der späteren Datenerhebung bleiben hiervon unberührt.

Normenklarheit in § 175 Absatz 3 Nummer 2 TKG-E: Die für eine Übermittlung maßgeblichen Rechtsgüter sollten konkret und abschließend beziehungsweise hinreichend bestimmt benannt werden. Eine Orientierung an § 174 Absatz 3 TKG und am Formulierungsvorschlag des Bundesrates ist sachgerecht.

Mit diesen punktuellen Anpassungen kann der Gesetzentwurf zu einem kohärenten, föderal anschlussfähigen und praxistauglichen Rechtsrahmen weiterentwickelt werden. Er würde den Sicherheitsbehörden von Bund und Ländern wirksame Instrumente an die Hand geben, ohne die gesetzlichen Voraussetzungen für die eigentliche Erhebung und Nutzung der Daten abzusenken.

München, 06. Oktober 2026

gez. Guido Limmer
Polizeivizepräsident
des Bayerischen Landeskriminalamts