



Stellungnahme der Gewerkschaft der Polizei (GdP)

zum Referentenentwurf des
Bundesministeriums der Justiz und für Verbraucherschutz

**Entwurf eines Gesetzes zur Einführung einer
Speicherungspflicht für IP-Adressen und zur Anpassung weiterer digitaler
Ermittlungsbefugnisse**

Berlin, 30.01.2026
Abt. Innenpolitik | 31, AL3

I. - Vorbemerkung

Die Gewerkschaft der Polizei (GdP) begrüßt ausdrücklich das Vorhaben des Bundesministeriums der Justiz und für Verbraucherschutz mit dem Referentenentwurf eines Gesetzes zur Einführung einer Speicherpflicht für IP-Adressen und zur Anpassung weiterer digitaler Ermittlungsbefugnisse einen rechtssicheren Rahmen zu schaffen.

Für Polizei und Strafverfolgungsbehörden ist die Sicherung und der rechtzeitige Zugriff auf bestimmte, nicht inhaltsbezogene Kommunikationsdaten - insbesondere IP-Adressen und Portnummern unverzichtbar, um Straftaten wirksam aufzuklären und die Sicherheit der Bürgerinnen und Bürger zu gewährleisten. Die derzeitige Rechtslage führt in der Praxis zu erheblichen Ermittlungsdefiziten und einer faktischen Einschränkung digitaler Strafverfolgung.

Dabei ist der GdP bewusst, dass Regelungen zur Speicherung und Nutzung von Daten in besonderem Maße grundrechtsrelevant sind und hohen verfassungs- und unionsrechtlichen Anforderungen unterliegen. Das Bundesverfassungsgericht hat eine Speicherung in der Vergangenheit nicht grundsätzlich verworfen, sondern insbesondere die unzureichenden Sicherungen der gespeicherten Daten sowie Defizite bei Zweckbindung, Transparenz und Rechtsschutz beanstandet. Der vorliegende Referentenentwurf trägt diesen Maßgaben ebenso Rechnung wie den Vorgaben des Europäischen Gerichtshofs und ist erkennbar darauf ausgerichtet, einen verfassungskonformen Ausgleich zwischen effektiver Strafverfolgung und dem Schutz der Grundrechte zu schaffen. Für die GdP ist es von zentraler Bedeutung, dass polizeiliche Ermittlungsbefugnisse stets auf einer klaren, rechtsstaatlich abgesicherten Grundlage beruhen. Die Sensibilität der betroffenen Daten ist der Polizei bewusst. Ihr Umgang erfordert rechtliche Begrenzungen, wirksame Kontrollmechanismen und ein ausreichendes Maß an Datenschutz. Eine rechtsstaatlich tragfähige Ausgestaltung ist daher nicht nur Voraussetzung für die Akzeptanz entsprechender Maßnahmen, sondern auch für ihre praktische Anwendbarkeit in der täglichen Ermittlungsarbeit.

Die GdP unterstützt daher das Ziel des Gesetzgebers mit dem vorliegenden Referentenentwurf endlich eine tragfähige, verfassungskonforme und zugleich praxistaugliche Regelung zu schaffen. Als mit über 210.000 Mitgliedern größte Polizeigewerkschaft in Deutschland bringt die GdP ihre Erfahrungen aus der täglichen Ermittlungsarbeit in das weitere Gesetzgebungsverfahren ein.

II. - Zum Vorhaben

Die aktuelle sicherheitspolitische Lage verdeutlicht in besonderer Weise die Notwendigkeit einer verpflichtenden Speicherung von IP-Adressen. Kriminalität verlagert sich zunehmend in den digitalen Raum. Die Bedeutung digitaler Spuren für Ermittlungsverfahren ist enorm. Insbesondere Cyberkriminalität zählt zu den am schnellsten wachsenden Kriminalitätsformen. Täterinnen und Täter agieren international, nutzen hochgradig arbeitsteilige Strukturen und bedienen sich zunehmend des Modells des sogenannten „Cybercrime-as-a-Service“. Parallel hierzu ist ein deutlicher Anstieg von Hasskriminalität, extremistischer Inhalte sowie gezielter Desinformationskampagnen im Internet zu verzeichnen. Diese Entwicklungen gefährden nicht nur einzelne Betroffene, sondern bedrohen auch demokratische Prozesse und die gesellschaftliche Stabilität insgesamt.

Besonders gravierend ist der anhaltende Anstieg bei Straftaten im Zusammenhang mit Darstellungen sexualisierter Gewalt gegen Kinder. In einer Vielzahl dieser Verfahren stellen IP-Adressen in Verbindung mit Portnummern die einzige verwertbare Ermittlungsgrundlage dar. Hinweise werden den Strafverfolgungsbehörden zeitverzögert über internationale Meldestellen oder Kooperationspartner übermittelt. Derzeit besteht ein Vollzugsdefizit. Ohne eine gesetzlich normierte Speicherpflicht sind die relevanten Daten zum Zeitpunkt des Bekanntwerdens der Tat vielfach bereits gelöscht. Ermittlungen laufen ins Leere, Täter bleiben anonym und Opfer können nicht geschützt werden.

Hinzu kommt, dass Unternehmen und öffentliche Einrichtungen zunehmend Ziel massiver Cyberangriffe werden, die erhebliche wirtschaftliche Schäden verursachen und auch kritische Infrastrukturen gefährden können. Digitale Spuren spielen daher heute in nahezu jedem Ermittlungsverfahren eine zentrale Rolle. Gleichwohl speichern viele Telekommunikations- und Internetdiensteanbieter entsprechende Verkehrsdaten bislang ausschließlich für eigene betriebliche Zwecke und nur für sehr kurze Zeiträume. In Deutschland werden IP-Adressen lediglich für wenige Tage vorgehalten, Portnummern teilweise gar nicht. Für komplexe Ermittlungen, in denen relevante Informationen oft erst nach Wochen oder Monaten verfügbar werden, sind diese Speicherfristen völlig unzureichend.

Vor diesem Hintergrund ist die Einführung einer gesetzlich geregelten, verbindlichen und verlässlichen Speicherpflicht für IP-Adressen nicht nur ein kriminalistisches Instrument, sondern ein zentrales gesellschafts- und sicherheitspolitisches Erfordernis. Nur so kann die Handlungsfähigkeit der Strafverfolgungsbehörden im digitalen Raum wirksam sichergestellt werden.

III.- Im Einzelnen

Artikel 1 | Änderung der Strafprozessordnung

■ Neuregelung der Funkzellenabfrage § 100g Abs. 4 StPO-E

Die Neuregelung der Funkzellenabfrage trägt zur Wiederherstellung der praktischen Anwendbarkeit dieses wichtigen Ermittlungsinstruments bei und ist aus Sicht der GdP ausdrücklich zu begrüßen.

Anlass für die gesetzliche Klarstellung ist die Entscheidung des Bundesgerichtshofs vom 10. Januar 2024 (Az.: 2 StR 171/23). Der Bundesgerichtshof hat darin festgestellt, dass eine Funkzellenabfrage nach der bisherigen Fassung des § 100g Abs. 3 StPO ausschließlich bei Verdacht einer besonders schweren Straftat zulässig ist. Erfolgt eine Funkzellenabfrage außerhalb dieses Rahmens, ist sie unzulässig und die hierdurch gewonnenen Erkenntnisse unterliegen einem Beweisverwertungsverbot. In der polizeilichen Praxis führte dies dazu, dass Ermittlungsansätze frühzeitig abgeschnitten, Ort-Zeit-/Personenbeziehungen sowie Bewegungsprofile von Tatverdächtigen nicht mehr nachvollzogen werden konnten. Gerade in komplexen Ermittlungsverfahren wurde den Strafverfolgungsbehörden damit ein zentrales Werkzeug entzogen.

Der Gesetzentwurf reagiert hierauf, indem die Eingriffsschwelle nunmehr gesetzlich klar dahin gehend bestimmt wird, dass für die Anordnung einer Funkzellenabfrage das Vorliegen einer Straftat von erheblicher Bedeutung genügt.

Aus Sicht der GdP ist die Funkzellenabfrage in vielen Verfahren ein unverzichtbares Mittel zur Aufklärung schwerer Straftaten und zur Rekonstruktion von Personenbeziehungen sowie Täterbewegungen. Der Wegfall dieses Instruments hätte nicht nur die Erfolgsquote polizeilicher Ermittlungen erheblich beeinträchtigt, sondern auch zu einer zusätzlichen Belastung der Kolleginnen und Kollegen geführt, die unter wachsendem Arbeitsdruck versuchen müssten, Ermittlungen, ohne dieses effektive Werkzeug zu führen. Die nun vorgesehene Neuregelung stärkt daher die Handlungsfähigkeit der Strafverfolgungsbehörden und ist ausdrücklich zu unterstützen.

■ **Sicherungsanordnung bei Verkehrsdaten § 100g Abs. 7 StPO-E**

Die GdP begrüßt ausdrücklich die Einführung der Sicherungsanordnung in § 100g Absatz 7 StPO. Mit diesem Instrument wird eine erhebliche Lücke in der digitalen Strafverfolgung geschlossen, da insbesondere Verkehrsdaten häufig nur für sehr kurze Zeiträume gespeichert werden und ohne ein vorgelagertes Sicherungsinstrument frühzeitig verloren gehen würden.

Die Sicherungsanordnung ermöglicht es, flüchtige Verkehrsdaten zu sichern, ohne bereits eine Datenerhebung oder -auswertung vorzunehmen. Sie ist als akzessorische Maßnahme ausgestaltet, streng zweckgebunden und auf Verkehrsdaten beschränkt. Inhaltsdaten sind ausdrücklich nicht erfasst. Der Eingriff bleibt damit von begrenzter Intensität, trägt jedoch entscheidend zur Sicherung späterer Ermittlungsansätze bei. Positiv hervorzuheben ist, dass die Sicherungsanordnung bereits bei Vorliegen zureichender tatsächlicher Anhaltspunkte für eine Straftat angeordnet werden kann, ohne dass zu diesem Zeitpunkt bereits ein personalisierter Tatverdacht bestehen muss. Dies entspricht der Ermittlungsrealität in frühen Verfahrensstadien.

Darüber hinaus ist die nationale Sicherungsanordnung zwingende Voraussetzung für die Anwendung der Europäischen Sicherungsanordnung nach der E-Evidence-Verordnung. Erst durch diese Regelung wird es den deutschen Strafverfolgungsbehörden ermöglicht, entsprechende europäische Instrumente effektiv zu nutzen. Die GdP unterstützt die Neuregelung daher ausdrücklich.

Artikel 6 | Änderung des Telekommunikationsgesetzes

■ **Speicherpflicht und Verwendungsbefugnis von Verkehrsdaten zur Identifizierung von Anschlussinhabern § 176 TKG**

Die GdP begrüßt ausdrücklich die Einführung einer gesetzlichen Speicherpflicht für IP-Adressen und weiterer zugehöriger Daten zur Identifizierung von Anschlussinhabern. Die Neuregelung stellt einen längst überfälligen Schritt dar, um die Ermittlungsfähigkeit der Strafverfolgungsbehörden im digitalen Raum wiederherzustellen. In der polizeilichen Praxis sind IP-Adressen häufig der einzige Ansatzpunkt zur Identifizierung von Tatverdächtigen, insbesondere bei Straftaten, die über das Internet begangen werden. Das bislang fehlende oder uneinheitliche Vorhalten dieser Daten hat regelmäßig dazu geführt, dass Ermittlungen bereits im Anfangsstadium ins Leere liefen. Die nun vorgesehene, klar begrenzte und zweckgebundene Speicherpflicht schafft hier endlich wieder eine verlässliche und rechtssichere Grundlage. Die Einführung einer Speicherpflicht in Deutschland trägt auch zur Angleichung der Ermittlungsbedingungen innerhalb Europas bei und stärkt die grenzüberschreitende Zusammenarbeit. Auch wenn aus kriminalistischer Sicht eine längere Speicherfrist - etwa von sechs Monaten - wünschenswert gewesen wäre, bewertet die GdP die nun vorgesehene dreimonatige Speicherpflicht als wichtigen und

richtigen Einstieg. Entscheidend ist, dass mit der Neuregelung erstmals wieder eine verbindliche Speicherverpflichtung geschaffen wird, die effektive Strafverfolgung im digitalen Raum ermöglicht und zugleich klare rechtliche Grenzen setzt. Perspektivisch hält die GdP es für erforderlich, im Rahmen einer europaweit harmonisierten Regelung zu einer weitergehenden Vereinheitlichung der Speicherfristen und -standards zu gelangen, um vergleichbare Ermittlungsbedingungen in allen Mitgliedstaaten zu gewährleisten und die grenzüberschreitende Strafverfolgung weiter zu stärken.

■ **Bußgeldvorschriften § 228 TKG n. F.**

Zu begrüßen ist ausdrücklich, dass die Übermittlungspflicht der Telekommunikationsunternehmen zur Sicherstellung der praktischen Wirksamkeit des § 176 TKG durch eine bußgeldbewehrte Regelung flankiert wird.

■ **Übergangsvorschriften § 230 Abs. 16 TKG-E**

Die GdP hält es für zwingend erforderlich, dass die in § 176 TKG-E vorgesehene Speicherpflicht so schnell wie möglich umgesetzt wird. Angesichts der bestehenden und seit Jahren bekannten Ermittlungsdefizite im digitalen Raum darf die Übergangsfrist nicht weiter ausgedehnt werden. Die im Referentenentwurf vorgesehene Frist von sechs Monaten stellt aus Sicht der GdP bereits das äußerste vertretbare Maß dar. Eine darüberhinausgehende Verzögerung würde die praktische Wirksamkeit der Neuregelung erheblich beeinträchtigen und dazu führen, dass Ermittlungsverfahren weiterhin mangels verfügbarer Daten scheitern.

Zudem ist davon auszugehen, dass die technische Umsetzung für die Telekommunikationsanbieter in einem überschaubaren Zeitraum möglich ist. In einigen europäischen Staaten bestehen bereits vergleichbare Speicherpflichten, an deren technischen und organisatorischen Lösungen sich die Anbieter orientieren können. Vor diesem Hintergrund regt die GdP an, die Übergangsfrist möglichst kurz zu halten, um eine schnellstmögliche Anwendung der Speicherpflicht sicherzustellen.

Artikel 10 | Änderung des Bundeskriminalamtgesetzes

■ **Sicherung von Verkehrsdaten § 10b BKAG-E**

Künftig gibt § 10b BKAG-E dem BKA in seiner Funktion als Zentralstelle die Befugnis, Verkehrsdaten vorläufig sichern zu lassen, wenn noch nicht feststeht, welche konkrete Strafverfolgungs- oder Polizeibehörde zuständig ist. Dies ist zu begrüßen.

Die Regelung trägt dem Umstand Rechnung, dass bei länderübergreifenden oder international relevanten Sachverhalten die Zuständigkeit häufig erst im weiteren Verlauf geklärt werden kann, während Verkehrsdaten bereits frühzeitig verloren zu gehen drohen. Die Möglichkeit des BKA, in dieser Phase vorläufig die Sicherung der Daten zu veranlassen, verhindert den endgültigen Verlust zentraler Ermittlungsansätze.

■ **Erhebung von Telekommunikationsverkehrsdaten und Nutzungsdaten, § 52 BKAG n. F.**

Zu begrüßen ist, dass die Sicherung flüchtiger Verkehrsdaten auch im Rahmen der Aufgabewahrnehmung des BKA zur Abwehr von Gefahren des internationalen Terrorismus ermöglicht wird. Die Regelung trägt der besonderen Ermittlungsrealität in frühen Phasen der Gefahren-

erforschung Rechnung, in denen belastbare Erkenntnisse häufig noch nicht hinreichend konkret einzelnen Gefährdern oder Störern zugeordnet werden können. Die Möglichkeit, Verkehrsdaten bereits in diesem Stadium vorläufig zu sichern, verhindert den unwiederbringlichen Verlust potenziell relevanter Erkenntnisse und schafft die notwendige Grundlage für eine weitere Verdichtung der Lage, die Identifizierung von Gefährdern sowie die Aufklärung von Beziehungs- und Kommunikationsstrukturen.