Bund Deutscher Kriminalbeamter

BDK |Wollankstraße 135|D-13187Berlin

An das Bundesministerium für Justiz
und Verbraucherschutz
Anton-Wilhelm-Amo-Str. 37
10117 Berlin

Per Mail: gesetzentwurf_stpo@bmjv.bund.de

**Bundesvorsitzender**

Ansprechpartner/in: Dirk Peglow
Funktion: Bundesvorsitzender

E-Mail: dirk.peglow@bdk.de
Telefon: +49 30 2463045-0

Datum: 30.01.2026

**Stellungnahme des Bund Deutscher Kriminalbeamter e.V. (BDK) zum Referentenentwurf zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren, Geschäftszeichen 411215#00005#0002**

## 1. Anlass und Gegenstand der Stellungnahme

Wir bedanken uns für die Gelegenheit, im Rahmen der Verbändeanhörung zu dem vorliegenden Referentenentwurf aus Sicht der kriminalpolizeilichen Praxis Stellung nehmen zu dürfen. Der Entwurf ordnet zentrale Regelungsbereiche der digitalen Strafverfolgung und Gefahrenabwehr neu und reagiert auf tiefgreifende Veränderungen der Kriminalitätswirklichkeit.

Tatbegehung, Vorbereitungshandlungen, Kommunikation und Verschleierung erfolgen heute in weiten Teilen über digitale Infrastrukturen. Ermittlungen sind daher zunehmend auf technische Anknüpfungspunkte angewiesen, die nicht lediglich unterstützende Funktion haben, sondern häufig den einzigen Zugang zu einem Sachverhalt darstellen.

Wir begrüßen den vorliegenden Referentenentwurf ausdrücklich. Er stellt einen wichtigen Schritt dar, um die Handlungsfähigkeit der Strafverfolgung und Gefahrenabwehr im digitalen Raum auf eine rechtssichere Grundlage zu stellen und bestehende strukturelle Ermittlungsdefizite zu adressieren.

Aus kriminalpolizeilicher Sicht greift der Entwurf zentrale Problemstellungen auf und setzt an den entscheidenden Schnittstellen zwischen technischer Datenverfügbarkeit und strafprozessualen Befugnissen an. Zugleich eröffnet er die Möglichkeit, digitale Ermittlungsinstrumente differenziert, zielgerichtet und unter Wahrung der verfassungs- und unionsrechtlichen Vorgaben

weiterzuentwickeln. Dabei bewegt sich der Gesetzgeber in einem durch nationale und europäische Rechtsprechung vorgeprägten Rahmen. Allgemeine und unterschiedslose Datenspeicherungen bezogen auf die Telekommunikationsverkehrs- und recht sensiblen Standortdaten die bei Telekommunikationsanbietern bei der Nutzung des Telefons anfallen sind unzulässig; zugleich sind gezielte, zeitlich begrenzte und zweckgebundene Regelungen zulässig, sofern sie verhältnismäßig ausgestaltet sind. Maßstab für die Bewertung des Entwurfs ist daher nicht allein die abstrakte Normstruktur, sondern insbesondere seine praktische Eignung zur Sicherstellung effektiver Strafverfolgung.

Der Europäische Gerichtshof hat in seiner neueren Rechtsprechung zwischenzeitlich klargestellt, dass eine begrenzte, streng zweckgebundene und zeitlich bemessene Speicherung von IP-Adressen unter engen Voraussetzungen unionsrechtlich hingegen zulässig sein kann, wenn sie insbesondere der Identifizierung von Anschlussinhabern dient und mit hohen Anforderungen an Datensicherheit, Zugriffsbeschränkung und Zweckbindung verbunden ist.

Eine solche Speicherpflicht ist nicht als allgemeine und unterschiedslose Vorratsdatenspeicherung zu qualifizieren, sofern sie sich auf das absolut Erforderliche beschränkt und weder die Auswertung von Kommunikationsinhalten noch die Erstellung von Bewegungs- oder Persönlichkeitsprofilen ermöglicht. Zugleich hat der Gerichtshof klargestellt, dass derartige Identifizierungsmaßnahmen nicht zwingend auf die Verfolgung schwerster Straftaten beschränkt sein müssen, sondern auch der Strafverfolgung im Allgemeinen dienen dürfen, wenn die Eingriffsintensität entsprechend begrenzt ist.

Der vorliegende Gesetzentwurf greift diese Linie auf, indem er die Speicherpflicht eng auf IP-Adressen und weitere für eine eindeutige Identifizierung eines ermittlungsrelevanten Anschlusses zwingend erforderliche Daten beschränkt und ihre Verwendung eindeutig auf Identifizierungszwecke festlegt. Damit wird ein unionsrechtlich tragfähiger Rahmen geschaffen, der den Grundrechtsschutz wahrt und zugleich die praktische Ermittlungsfähigkeit im digitalen Raum sicherstellt.

**2. Grundsätzliche kriminalpolitische Einordnung**

Wir vertreten eine differenzierte Haltung zur Speicherung und Nutzung von Verkehrs-, Standort- und Nutzungsdaten. Eine anlasslose oder umfassende Datensammlung wird nicht befürwortet. Ebenso wenig kann jedoch hingenommen werden, dass rechtlich eröffnete Ermittlungsbefugnisse in der Praxis ins Leere laufen, weil die hierfür erforderlichen technischen Grundlagen nicht verfügbar sind.

Die vergangenen Jahre haben gezeigt, dass das vollständige Fehlen einer rechtssicheren Datenverfügbarkeit im digitalen Raum zu einem strukturellen Vollzugsdefizit geführt hat. Ermittlungen scheiterten nicht an fehlendem Tatverdacht oder mangelnder rechtlicher Befugnis, sondern

daran, dass digitale Spuren bereits gelöscht waren, bevor Ermittlungsmaßnahmen eingeleitet werden konnten. Diese Entwicklung hat nicht nur negative Auswirkungen auf die möglichst umfassend vorzunehmende Aufklärung von Straftaten, sondern auch auf das Vertrauen in die Durchsetzbarkeit staatlichen Strafanspruchs.

Vor diesem Hintergrund verfolgt der Gesetzentwurf einen Ansatz, der auf Differenzierung und Zweckbindung setzt. Ziel ist es, dort eine begrenzte Datenverfügbarkeit zu schaffen, wo sie für konkrete Ermittlungszwecke erforderlich ist, ohne in die Nähe früherer Konzepte einer umfassenden Vorratsdatenspeicherung zu geraten.

## 3. § 100g StPO-E – Erhebung von Verkehrsdaten

### 3.1 Zentrale Bedeutung für digitale Ermittlungen

§ 100g StPO-E stellt das zentrale strafprozessuale Instrument für die Erhebung von Verkehrsdaten dar. In einer Vielzahl von Verfahren ist diese Norm nicht lediglich ergänzend, sondern konstitutiv für das gesamte Ermittlungsverfahren. Ohne die Möglichkeit, Verkehrsdaten rechtssicher zu erheben, bleiben Ermittlungen im digitalen Raum häufig bereits im Ansatz stecken.

Die Neufassung trägt der Erkenntnis Rechnung, dass sich Kriminalität nicht nur punktuell, sondern strukturell in digitale Räume verlagert hat. Ermittlungsansätze entstehen regelmäßig aus technischen Spuren, etwa IP-Adressen, Verbindungsdaten oder Standortinformationen. Diese Daten bilden häufig den Ausgangspunkt für weitergehende Ermittlungen, etwa Durchsuchungen, Beschlagnahmen oder Vernehmungen.

### 3.2 Retrograde Standortdaten

Die Absenkung der Voraussetzungen für die Erhebung retrograder Standortdaten ist vor diesem Hintergrund sachgerecht. Standortdaten sind in zahlreichen Deliktsbereichen für die Aufklärung des Tatgeschehens von erheblicher Bedeutung, etwa zur Rekonstruktion von Tatabläufen, zur Überprüfung von Alibibehauptungen oder zur Eingrenzung von Tatzeiträumen.

Zugleich handelt es sich um einen intensiven Grundrechtseingriff. Die Anwendung der Befugnis setzt daher eine besonders sorgfältige Einzelfallprüfung voraus. Entscheidend ist, dass Standortdaten gezielt, zeitlich eng begrenzt und ausschließlich zur Verfolgung konkreter Ermittlungsansätze erhoben werden. Die Norm muss so angewandt werden, dass sie Ermittlungen ermöglicht, ohne zu einer ausufernden Datenerhebung zu führen.

### 3.3 Funkzellenabfrage

Aus praktischer Sicht ist zudem zu betonen, dass die Funkzellenabfrage regelmäßig nicht als Selbstzweck eingesetzt wird, sondern der Eingrenzung eines zunächst unübersichtlichen Tatgeschehens dient. Typisch sind Sachverhalte, in denen weder Tatverdächtige noch konkrete

Kommunikationsmittel bekannt sind und erst durch die Auswertung erhobener Verkehrsdaten erste Ermittlungsansätze generiert werden können, und zwar dann, wenn besondere Auffälligkeiten festgestellt werden, die nach kriminalistischer Erfahrung einen Hinweis auf den oder die Täter geben könnten.

Die kriminalpolizeiliche Praxis zeigt, dass die rechtliche Bewertung der Funkzellenabfrage maßgeblich davon abhängt, ob der räumlich-zeitliche Zuschnitt der Maßnahme nachvollziehbar an den Tatablauf angepasst ist. Je präziser der Zuschnitt erfolgt und je früher nicht relevante Daten ausgefiltert werden, desto geringer ist die Drittbetroffenheit und desto eher ist die Maßnahme verhältnismäßig. Entscheidend ist dabei nicht die abstrakte Zahl der erfassten Datensätze, sondern die konkrete Ermittlungsnotwendigkeit im Einzelfall.

Vor diesem Hintergrund kommt der dokumentierten Einzelfallprüfung eine zentrale Bedeutung zu. Sie bildet nicht nur die Grundlage für die Anordnung, sondern ist auch maßgeblich für die spätere gerichtliche Überprüfung der Maßnahme. Eine gesetzliche Ausgestaltung, die diesen praxisorientierten Prüfungsmaßstab abbildet, stärkt sowohl die Rechtssicherheit als auch die Akzeptanz des Instruments.

Die Neuregelung der Funkzellenabfrage ist aus kriminalpolizeilicher Sicht von besonderer Bedeutung. Die in der Vergangenheit stark verengten Anwendungsvoraussetzungen führten dazu, dass dieses Ermittlungsinstrument selbst bei schweren Straftaten faktisch nicht mehr eingesetzt werden konnte. Dies hatte erhebliche Auswirkungen auf die Aufklärungsarbeit, insbesondere bei Delikten mit mehreren unbekannten Tatbeteiligten oder bei anonymen Tatbegehungsformen.

Die Rückkehr zur Schwelle der Straftat von im Einzelfall erheblicher Bedeutung stellt eine sachgerechte Korrektur dar. Zugleich bleibt die Funkzellenabfrage ein Ausnahmeinstrument mit regelmäßig hoher Drittbetroffenheit. Die gesetzliche Neuregelung verlagert den Schwerpunkt daher zu Recht auf die qualifizierte Einzelfallprüfung. Maßgeblich sind insbesondere der räumlich-zeitliche Zuschnitt der Maßnahme, die Prüfung milderer Mittel sowie die unverzügliche Filterung und Löschung nicht verfahrensrelevanter Daten.

**3.4 IP-Adressen zu Identifizierungszwecken**

Die Einführung einer ausdrücklichen Befugnis zur Erhebung von IP-Adressen zu Identifizierungszwecken bei nummernunabhängigen interpersonellen Telekommunikationsdiensten ist eine notwendige Anpassung an die heutige Kommunikationswirklichkeit. Klassische Telefonnummern verlieren zunehmend an Bedeutung; Kommunikation verlagert sich auf plattformbasierte Dienste.

In der Praxis zeigt sich jedoch, dass die Erhebung der erforderlichen Ermittlungsansätze häufig nicht am fehlenden Anfangsverdacht scheitert, sondern daran, dass der strafbare Inhalt der Nutzung nicht beim jeweiligen Dienst bekannt ist. Strafbare Inhalte sind oftmals nur bei anderen Anbietern vorhanden oder werden erst im Zuge weiterer Ermittlungen bekannt. Eine praxistaugliche Ausgestaltung der Norm sollte daher Identifizierungsabfragen auch in diesen Konstellationen ermöglichen, sofern ein hinreichender Anfangsverdacht besteht und die Maßnahme verhältnismäßig ist. Andernfalls wäre zuvor eine eingriffsintensivere Erhebung von Inhalten gefordert, die jedoch gar nicht zur Aufklärung der Straftat wegen der ermittelt wird zwingende notwendig ist.

### 3.5 Sicherungsanordnung

Die Einführung einer eigenständigen Sicherungsanordnung für Verkehrsdaten trägt der polizeilichen Praxis digitaler Ermittlungen Rechnung. Verkehrsdaten stehen regelmäßig nur für begrenzte Zeiträume zur Verfügung und sind vielfach bereits gelöscht, bevor sich Ermittlungen so weit verdichtet haben, dass förmliche Erhebungsmaßnahmen rechtssicher angeordnet werden können.

Der Gesetzentwurf begegnet diesem Problem, indem er eine rechtlich klar konturierte Möglichkeit eröffnet, relevante Daten frühzeitig vor weiterem Verlust zu bewahren. Die Sicherungsanordnung ist dabei funktional von der eigentlichen Datenerhebung zu trennen. Sie dient nicht der Gewinnung von Erkenntnissen, sondern der Sicherung späterer Ermittlungsoptionen.

Die Maßnahme setzt voraus, dass tatsächliche Anhaltspunkte für eine Straftat vorliegen, deren Verfolgung eine Datenerhebung grundsätzlich tragen könnte, auch wenn sich der Ermittlungsstand noch nicht zu einer abschließenden Erhebungsentscheidung verdichtet hat. Damit wird dem Umstand Rechnung getragen, dass Ermittlungen im digitalen Raum häufig schrittweise verlaufen und sich relevante Tatsachen erst im weiteren Verlauf herausbilden.

Für die Bewertung der Eingriffsintensität ist entscheidend, dass die gesicherten Daten zunächst nicht an die Strafverfolgungsbehörden übermittelt werden, sondern weiterhin im Herrschaftsbereich des Verpflichteten verbleiben. Ein staatlicher Zugriff erfolgt erst nach einer gesonderten justiziell zu treffenden Entscheidung über die Erhebung. Diese gestufte Ausgestaltung reduziert die unmittelbare Grundrechtsrelevanz der Sicherungsanordnung und rechtfertigt es, die Maßnahme nicht generell einem Richtervorbehalt zu unterstellen. Dies erhöht die Praxistauglichkeit der neuen Befugnis insbesondere in zeitkritischen Fallkonstellationen. Gleichwohl bleibt eine sorgfältige Prüfung im Einzelfall unerlässlich.

Gerade bei Maßnahmen mit breiter Streuwirkung, etwa bei räumlich oder zeitlich weit gefassten Sicherungen, ist eine besonders strenge Verhältnismäßigkeitsprüfung geboten. Umfang, Dauer und sachlicher Zuschnitt der Sicherung müssen sich nachvollziehbar am konkreten

Ermittlungsanlass orientieren. Eine unzureichend begrenzte Sicherung birgt das Risiko, dass spätere Erhebungen rechtlich angreifbar werden und die Verwertbarkeit der gewonnenen Erkenntnisse in Frage steht. Die Qualität der anfänglichen Begründung ist daher nicht nur für die Rechtmäßigkeit der Sicherung selbst, sondern auch für den weiteren Verfahrensverlauf von zentraler Bedeutung.

Die gesetzlich vorgesehene zeitliche Begrenzung der Sicherungsanordnung gewährleistet, dass die Maßnahme ihren Charakter als vorübergehende Sicherung wahrt und nicht in eine faktische Dauerbevorratung umschlägt. Zugleich ist zu gewährleisten, dass gesicherte Verkehrsdaten innerhalb klar definierter Zweckbindungen auch dann nutzbar bleiben, wenn sich ein sachlich zusammenhängender Ermittlungsbedarf in einem weiteren Verfahren ergibt. Dies betrifft insbesondere arbeitsteilige Ermittlungsstrukturen, Verfahrensverbindungen oder zeitlich versetzte Erkenntnislagen. Eine solche Nutzungsmöglichkeit stärkt die Effektivität komplexer Ermittlungen, ohne den grundrechtlichen Schutzstandard zu relativieren.

Aus unserer Sicht ist es daher erforderlich, gesetzlich klarzustellen, dass gesicherte Verkehrsdaten innerhalb enger Zweckbindungen auch weiteren Verfahren, die wegen Straftaten von im Einzelfall erheblicher Bedeutung geführt werden, genutzt werden dürfen, sofern die jeweiligen Erhebungsvoraussetzungen erfüllt sind.

Insgesamt stellt die Sicherungsanordnung ein geeignetes Instrument dar, um die Handlungsfähigkeit der Strafverfolgung im digitalen Raum zu stabilisieren. Ihre Wirksamkeit hängt jedoch maßgeblich davon ab, dass sie zurückhaltend, präzise und dokumentationsfest angewandt wird. Nur so kann sie ihren Zweck erfüllen, Ermittlungen zu ermöglichen, ohne die Schwelle zur eigentlichen Datenerhebung unzulässig vorzuverlegen.

Entscheidend ist, dass Anordnungskompetenzen, Fristen und Dokumentationspflichten klar geregelt sind und auch die Nutzung bereits gesicherter Daten in weiteren Verfahren innerhalb der Zweckbindung für Straftaten von im Einzelfall erheblicher Bedeutung rechtssicher ermöglicht wird.

Positiv hervorzuheben ist, dass die Sicherungsanordnung nach § 100g Abs. 7 StPO-E ausdrücklich auch für Zwecke der Gefahrenabwehr sowie der Zentralstellenfunktion des Bundeskriminalamts nach §§ 52, 10b BKAG rechtssicher nutzbar ist. Gerade bei komplexen, arbeitsteiligen oder bundesländerübergreifenden Sachverhalten ermöglicht die frühzeitige Sicherung flüchtiger Verkehrsdaten, Ermittlungsansätze zu stabilisieren und eine spätere Aufklärung sowie Koordinierung durch die örtlich zuständige Ermittlungsbehörde effektiv vorzubereiten.

Aus Sicht der Praxis erscheint es darüber hinaus erforderlich, eine gleichlautende Befugnis auch für die Bundespolizei vorzusehen, um bei Gefahrenlagen, die nach BPolG zu bearbeiten sind, vergleichbare Beweismittelverluste zu vermeiden. Zur Aufklärung von Schleusungskriminalität,

bei der Verkehrs- und Standortdatenerhebungen sehr wichtige Ermittlungsansätze darstellen, kann die Bundespolizei mit der neuen Befugnis ebenfalls effektiv verhindern, dass Daten bereits gelöscht sind, bevor der richterliche Beschluss zur jeweiligen Datenerhebung an den Anbieter gerichtet werden konnte.

## 4. § 176 TKG-E – Speicherpflicht für IP-Adressen

### 4.1 Funktion als technische Grundlage

Die in § 176 TKG-E vorgesehene Speicherpflicht bildet die technische Grundlage für die Anwendung der strafprozessualen Befugnisse nach § 100j StPO-E. Ohne eine gesetzliche Verpflichtung zur Vorhaltung von IP-Zuordnungen laufen Identifizierungsbefugnisse auch in anderen Fachgesetzen wie dem BKAG, dem BPolG oder den Polizeigesetzen der Länder in einer Vielzahl von Fällen bereits nach wenigen Tagen ins Leere.

Über einen langen Zeitraum war eine verlässliche Anschlussinhaberfeststellung nur eingeschränkt möglich, da eine vorsorgliche Speicherung zu Ermittlungszwecken rechtlich nicht abgesichert war. Gespeichert wurde, soweit überhaupt, ausschließlich aus eigenbetrieblichen Gründen der Anbieter.

Diese Situation ist Ergebnis einer längerfristigen rechtlichen Entwicklung, in deren Folge frühere Ansätze einer umfassenden Speicherung unionsrechtlich nicht tragfähig waren. In der Konsequenz fehlte eine rechtssichere Grundlage für eine begrenzte, gezielte Datenverfügbarkeit zu Identifizierungszwecken.

### 4.2 Deliktsrelevanz der IP-Speicherung

Die praktische Relevanz der Speicherpflicht zeigt sich insbesondere in Deliktsbereichen mit überwiegend digitaler Tatbegehung oder -anbahnung. Hierzu zählen internetgestützte Betrugsdelikte, Identitätsmissbrauch, die Verbreitung schädlicher Software, sexualbezogene Delikte im Internet, Bedrohungs- und Nötigungssachverhalte über digitale Kommunikationsdienste sowie die Veröffentlichung strafbarer Inhalte auf Plattformen und in sozialen Netzwerken.

Auch bei arbeitsteiligen und organisierten Begehungsformen, bei denen digitale Infrastrukturen zur Koordination, Verschleierung oder anonymisierten Kommunikation genutzt werden, ist die IP-Zuordnung häufig Voraussetzung für die Aufnahme strukturierter Ermittlungen.

### 4.3 Speicherdauer und Umsetzungsfrist

Die vorgesehene Speicherdauer von drei Monaten trägt dem Grundsatz der Datensparsamkeit Rechnung. Gleichzeitig beginnen Ermittlungen im digitalen Raum häufig zeitverzögert. Anzeigen werden nicht selten erst Wochen nach Tatbegehung erstattet; Hinweise Dritter oder aus dem Ausland gehen verspätet ein. Die Wirksamkeit der Regelung hängt daher maßgeblich davon ab, dass die Speicherfrist in einem realistischen Verhältnis zu Ermittlungsabläufen steht.

Die in § 176 TKG-E vorgesehene Speicherpflicht ist als „Ermöglichungsnorm“ nur dann wirksam, wenn sie tatsächlich in den Netzen umgesetzt ist. Die in § 230 Abs. 16 TKG-E vorgesehene Umsetzungsfrist von sechs Monaten führt jedoch dazu, dass die seit Jahren bekannten Ermittlungsdefizite für einen weiteren, klar kalkulierbaren Zeitraum fortbestehen.

Damit entsteht eine faktische Schutzlücke, die nicht nur theoretisch ist, sondern sich unmittelbar in derzeit laufenden Verfahren auswirkt. Gerade digitale Ermittlungen sind in besonderer Weise zeitkritisch. Anzeigen werden häufig verzögert erstattet, Hinweise treffen zeitversetzt ein, und Ermittlungsansätze verdichten sich nicht selten erst nach Wochen – genau in dem Zeitraum, in dem eine verlässliche Anschlussinhaberfeststellung über dynamische IP-Zuordnungen bislang regelmäßig scheitert.

Besonders problematisch ist, dass die Umsetzungsfrist ein „Fenster der Vorhersehbarkeit“ eröffnet. Täter wissen – oder können jedenfalls naheliegend annehmen –, dass eine Identifizierung über IP-Zuordnungen in den kommenden Monaten weiterhin in vielen Fällen ins Leere läuft. Das erhöht die Attraktivität digitaler Tatbegehungen und begünstigt Verlagerungseffekte. Hinzu kommt: Die Speicherdauer beträgt lediglich drei Monate. Jeder weitere Monat ohne Umsetzung ist damit nicht nur ein zusätzlicher Verzögerungsmonat, sondern bedeutet faktisch auch, dass im Übergangszeitraum ein erheblicher Teil potenziell relevanter IP-Zuordnungen endgültig verloren geht. Die Norm erreicht ihre intendierte Wirkung dann nicht „nach sechs Monaten“, sondern in der Breite erst deutlich später, weil erst nach Inbetriebnahme der Systeme ein relevanter Datenbestand überhaupt entstehen kann.

Aus kriminalpolizeilicher Sicht sollte daher eine möglichst zeitnahe Umsetzung erreicht werden. Dies kann etwa dadurch unterstützt werden, dass die Umsetzungsfrist in § 230 Abs. 16 TKG-E eng geführt wird und zugleich klar geregelt wird, dass die Anbieter frühzeitig organisatorische und technische Maßnahmen zu treffen haben. Zudem sollte verhindert werden, dass sich die Frist in der Praxis durch nachgelagerte Umsetzungsdiskussionen faktisch verlängert. Gerade weil der Entwurf bewusst auf eine eng begrenzte Speicherpflicht (nur IP-Adresse, klare Zweckbindung zur Identifizierung) setzt, ist es nicht überzeugend, den Vollzug über einen langen Übergangszeitraum aufzuschieben.

**4.4 Technische Anforderungen**

Für die praktische Wirksamkeit der Speicherpflicht ist entscheidend, dass IP-Adressen mit einer hinreichend präzisen zeitlichen Zuordnung gemeinsam mit eventuell zugewiesenen Ports gespeichert werden. Nur so ist eine eindeutige Identifizierung möglich. Unklare oder uneinheitliche technische Vorgaben führen zu Rechtsunsicherheit und nicht verwertbaren Ergebnissen.

**5. Flankierende Regelungen**

Die Neuregelungen zu Begründung, Kennzeichnung und Löschung erhobener Daten stärken Transparenz und Nachvollziehbarkeit. Die Qualität der Dokumentation entscheidet künftig maßgeblich über die Rechtmäßigkeit und Verwertbarkeit der Maßnahmen.

Die Wiedereinführung einer wirksamen Bußgeldbewehrung bei Verstößen gegen Mitwirkungspflichten ist erforderlich, um die Zielrichtung der gesetzlichen Regelungen auch systematisch abzusichern. Ermittlungsbefugnisse entfalten nur dann Wirkung, wenn sie auch praktisch durchsetzbar sind und bei Nichtbefolgung auch Bußgelder verhängt werden können, die in der Folge dazu führen können, dass keine Negativauskünfte einzelner Anbieter mehr erfolgen.

Positiv hervorzuheben ist in diesem Zusammenhang auch die Anpassung der Kostenregelung nach dem JVEG, wonach die Auskunft zu Bestandsdaten anhand einer IP-Adresse künftig mit 15 Euro für bis zu drei Kennungen in demselben Verfahren vergütet wird. Diese Klarstellung trägt zu einer Vereinheitlichung der Praxis bei und reduziert Fehlanreize, die einer zügigen Mitwirkung der Anbieter entgegenstehen können.

Ergänzend halten wir es für erforderlich, die Anwendung der neuen Befugnisse durch geeignete Qualifizierungs- und Fortbildungsmaßnahmen sowie durch Mindeststandards für Dokumentation und Begründung abzusichern.

**6. Gesamteinordnung und Schlussbemerkung**

Der Gesetzentwurf enthält wesentliche Ansätze zur Stärkung der Handlungsfähigkeit der Strafverfolgung im digitalen Raum. Damit diese ihre Wirkung entfalten können, müssen die Regelungen praxisnah, verhältnismäßig und technisch eindeutig ausgestaltet werden. Effektive Strafverfolgung und Grundrechtsschutz stehen dabei nicht im Widerspruch, sondern bedingen einander.

Damit diese Ansätze ihre Wirkung entfalten können, erwartet der BDK eine praxisnahe Umsetzung, sowie die Bereitschaft des Gesetzgebers, auf erkannte Vollzugsprobleme zeitnah zu reagieren.

Mit freundlichen Grüßen

Dirk Peglow
Bundesvorsitzender