

Sicherung, Speicherung, Identifizierung Der RegE vom 22.4.2026 und die strafprozessuale Neustrukturierung digitaler Ermittlungsdaten

von RA Dr. iur. Dr. rer. pol. Fabian
Teichmann, LL.M. (London), MBA (Oxford)*

Abstract

Der Regierungsentwurf zur IP-Adressspeicherung ordnet die strafprozessuale Datenerhebung nicht punktuell, sondern strukturell neu. Seine Leitfigur ist nicht das klassische Quick-Freeze-Modell, sondern ein Kombinationsmodell aus dreimonatiger IP-Adressspeicherung, anlassbezogener Sicherungsanordnung und neu justierten Erhebungsbefugnissen für Verkehrs-, Nutzungs- und Bestandsdaten.

The Government's draft bill on the retention of IP addresses restructures the gathering of data in criminal proceedings not selectively, but structurally. Its guiding model is not the classic quick-freeze approach, but a combined model consisting of a three-month retention of IP addresses, a case-specific preservation order, and recalibrated powers to collect traffic data, usage data and subscriber data.

I. Problemaufriss

Digitale Ermittlungen beginnen häufig nicht mit einem Namen, sondern mit einem technischen Fragment. Die IP-Adresse, ein Zeitstempel, eine Portnummer oder die Einbuchung in eine Funkzelle markieren den ersten tatsächlichen Zugriffspunkt staatlicher Strafverfolgung. Gerade bei Straftaten, die vollständig oder wesentlich über das Internet vorbereitet, begangen oder verschleiert werden, kann die Identifizierung des Anschlussinhabers anhand einer dynamischen IP-Adresse den einzigen realistischen Ermittlungsansatz bilden. Der RegE vom 22.4.2026 greift dieses Problem auf und reagiert auf zwei gegenläufige Entwicklungslinien: die unionsrechtliche Zurückdrängung der allgemeinen Vorratsdatenspeicherung und die praktische Erosion flüchtiger digitaler Spuren.¹

Der Entwurf verfolgt dabei keine bloße Reparaturtechnik. Er ersetzt die bisherige, unionsrechtlich belastete Vorratsdatenspeicherung nicht durch ein reines Quick-Freeze-In-

strument. Vielmehr entsteht eine neue dreistufige Architektur. Erstens werden Internetzugangsdiensteanbieter verpflichtet, bestimmte IP-Zuordnungsdaten drei Monate vorsorglich zu speichern; zweitens wird für Verkehrsdaten eine anlassbezogene Sicherungsanordnung eingeführt;² drittens werden die strafprozessualen Abrufnormen für Verkehrs-, Nutzungs- und Bestandsdaten neu sortiert. Damit verschiebt sich der Schwerpunkt von der Frage, ob Daten überhaupt vorhanden sind, hin zur dogmatischen Frage, auf welcher Ebene – Speicherung, Sicherung oder Erhebung – der jeweilige Grundrechtseingriff stattfindet.³

Die Arbeitsthese dieses Beitrags lautet daher, dass der RegE Teile der bisherigen Vorratsdatenspeicherung ablöst, aber zugleich ein eigenständiges Kombinationsmodell schafft, dessen dogmatische Brisanz in der Verknüpfung von vorsorglicher IP-Adressspeicherung, abgesenkter Sicherungsschwelle und gesetzgeberisch reaktiver Funkzellenabfrage liegt. Die strafprozessuale Bewertung darf sich deshalb nicht darauf beschränken, einzelne Normen zu referieren. Entscheidend ist, ob die Trennung zwischen Verkehrsdaten, Nutzungsdaten und Bestandsdaten praktisch belastbar bleibt und ob § 101a StPO-E die erforderlichen Kontroll-, Begründungs- und Transparenzsicherungen vermittelt.⁴

II. Entwicklungslinien: von der Vorratsdatenspeicherung zur IP-Identifizierung

Die unionsrechtliche Vorgeschichte ist für das Verständnis des Entwurfs konstitutiv. Der *EuGH* hat seit *Tele2 Sverige/Watson* allgemeine und unterschiedslose Speicherungspflichten für Verkehrs- und Standortdaten nur unter engsten Voraussetzungen akzeptiert. La Quadrature du Net I, Prokuratuur und SpaceNet/Telekom Deutschland haben diese Linie fortgeführt und insbesondere den Zugriff auf Verkehrs- und Standortdaten an eine anlassbezogene, zweckgebundene und regelmäßige unabhängige

* RA Dr. iur. Dr. rer. pol. Fabian Teichmann, LL.M. (London), MBA (Oxford) ist Rechtsanwalt und Notar in St. Gallen sowie Managing Partner der Teichmann International (Schweiz) AG.

¹ RegE Regierungsentwurf v. 22.4.2026 zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren, eingestellt vom BMJV und abrufbar unter: <https://bit.ly/4fCdjm3> (zuletzt abgerufen am 24.7.2026), im Folgenden nur RegE genannt; vgl. RegE, S. 1, 23 ff.; zur Einordnung des Entwurfs als Hybridmodell und zu seiner unions- und verfassungsrechtlichen Würdigung Teichmann, JR 2026, 441 ff.

² Ruppert, ZRP 2026, 82 (82).

³ RegE, S. 24 f., 25.

⁴ RegE, S. 24 f., 37.

Kontrolle gebunden. Das deutsche Speicherregime der §§ 175 ff. TKG a.F. war damit nicht nur praktisch suspendiert, sondern dogmatisch delegitimiert.⁵

La Quadrature du Net II/HADOPI differenziert diese Rechtsprechung. Der Gerichtshof akzeptiert eine allgemeine und unterschiedslose Vorratsspeicherung von IP-Adressen, wenn die Speicherung nach ihrem Zuschnitt nicht zu präzisen Schlüssen auf das Privatleben führt und eine wirksame strikte Trennung der verschiedenen Datenkategorien gewährleistet ist.⁶ Der Zugriff darf grundsätzlich auf die Identifizierung einer Person beschränkt bleiben, die im Verdacht steht, an einer Straftat beteiligt zu sein. Dieser Schritt ist kein Widerruf des Vorratsspeicherungsverbots, sondern eine Verfeinerung, bei der die IP-Adresse als identifizierungsbezogener Schlüssel behandelt wird und nicht als Kommunikations- oder Bewegungsprofil.⁷

Der RegE übernimmt diese Differenzierung, aber nicht in Gestalt eines bloßen HADOPI-Imports. Während das französische Modell in einem verwaltungsrechtlichen Kontext der Urheberrechtsdurchsetzung steht, fügt der deutsche Entwurf die IP-Adressspeicherung in das Strafprozessrecht ein. Das ist ein qualitativer Unterschied. Die Zuordnung einer IP-Adresse zu einem Anschlussinhaber ist im Strafverfahren regelmäßig nicht Endpunkt, sondern Ausgangspunkt weiterer Ermittlungen. Sie kann zur Durchsuchung, Telekommunikationsüberwachung, Beschlagnahme, Vermögensabschöpfung oder zur Verdichtung eines Tatverdachts führen. Gerade deshalb darf die Einstufung als Bestandsdatenauskunft nicht verdecken, dass der staatliche Zugriff auf einer vorgelagerten Speicherung von Verkehrsdaten beruht.

Hinzu tritt die Sicherungsanordnung. Sie ist zwar anlassbezogen und deshalb näher am Quick-Freeze-Modell als die IP-Adressspeicherung. Gleichwohl ist auch sie kein klassisches Quick Freeze in Reinform. § 100g Abs. 7 StPO-E erlaubt die Sicherung nicht erst, wenn alle Voraussetzungen einer Erhebung vorliegen, sondern gerade für Fälle, in denen die spätere Erhebung möglich erscheinen soll. Die Sicherung konserviert Daten, die anderenfalls gelöscht würden. Sie ist damit ein vorgelagerter Eingriff in die Lösungs- und Verwendungsordnung, auch wenn sie noch keine Herausgabe an die Strafverfolgungsbehörden bewirkt.

Die dritte Entwicklungslinie betrifft die Funkzellenabfrage. Der BGH hat für die geltende Rechtslage entschieden, dass eine Funkzellenabfrage bei Erhebung geschäftlich gespeicherter Verkehrsdaten den Verdacht einer be-

sonders schweren Straftat nach § 100g Abs. 2 StPO voraussetzt. Der RegE korrigiert diese Lesart gesetzgeberisch und stellt die Funkzellenabfrage in § 100g Abs. 4 StPO-E unter die Schwelle der Straftat von auch im Einzelfall erheblicher Bedeutung. Damit wird eine Maßnahme mit erheblicher Drittbetroffenheit auf eine niedrigere Schwelle zurückgeführt. Das ist der praktisch schärfste Punkt des Entwurfs.⁸

III. Die Normarchitektur des RegE

Der Entwurf ordnet die digitale Ermittlungsdatengewinnung entlang dreier Funktionen: speichern, sichern und erheben. Diese Funktionen sind normativ verschiedenen Rechtsgrundlagen zugeordnet und dürfen nicht ineinander geschoben werden. § 177 TKG-E betrifft die vorsorgliche Speicherung bestimmter IP-Zuordnungsdaten. § 176 TKG-E betrifft die providerseitige Verarbeitung zur Erfüllung von Sicherungsanordnungen. § 175 TKG-E bildet die telekommunikationsrechtliche Verarbeitungs- und Auskunftgrundlage für Verkehrsdatenabrufe. Strafprozessual korrespondieren damit § 100g StPO-E für Verkehrsdaten, § 100j StPO-E für Bestandsdaten und § 100k StPO-E für Nutzungsdaten.

Die erste Ebene ist § 177 TKG-E. Verpflichtet sind Internetzugangsdiensteanbieter. Zu speichern sind die zugewiesene öffentliche IP-Adresse, zugehörige Portnummern und weitere für die Identifizierung erforderliche Verkehrsdaten, eine Anschluss- oder Benutzerkennung sowie Beginn und Ende der Zuweisung mit sekundengenaue Zeitangabe und Zeitzone. Die Speicherfrist beträgt drei Monate. Inhalte der Kommunikation sowie Daten über den Aufruf oder die Nutzung anderer Telekommunikationsdienste oder digitaler Dienste dürfen auf dieser Grundlage nicht gespeichert werden. Die Speicherpflicht ist damit nicht inhalts-, nicht kommunikationsbeziehungs- und nicht standortbezogen, sondern identifizierungsbezogen.⁹

Die zweite Ebene ist § 100g Abs. 7 StPO-E in Verbindung mit § 176 TKG-E. Die Strafverfolgungsbehörde kann anordnen, dass Verpflichtete Verkehrsdaten betroffener Personen unverzüglich sichern. Die Sicherung setzt zureichende tatsächliche Anhaltspunkte für eine Straftat voraus, welche eine spätere Erhebung nach § 100g Abs. 1 bis 4 StPO-E rechtfertigen würde, ferner einen persönlichen oder räumlichen Bezug der betroffenen Person zur Tat und eine mögliche Bedeutung der Daten für die jeweiligen Ermittlungszwecke. Die gesicherten Daten dürfen nur im Rahmen des Sicherungszwecks verwendet werden; sie sind getrennt und geschützt zu speichern und nach Übermittlung oder Fristablauf irreversibel zu löschen.¹⁰

⁵ *EuGH*, Ur. v. 21.12.2016 – C-203/15, C-698/15, NJW 2017, 717 (717); *EuGH*, Ur. v. 6.10.2020 – C-511/18, C-512/18, C-520/18, NJW 2021, 531 (531); *EuGH*, Ur. v. 2.3.2021 – C-746/18, ZD 2021, 517 (517); *EuGH*, Ur. v. 20.9.2022 – C-793/19, C-794/19, NJW 2022, 3135 (3135).

⁶ *Ruppert*, ZRP 2026, 82 (83).

⁷ *EuGH*, Ur. v. 30.4.2024 – C-470/21, NJW 2024, 2099 (2099); RegE, S. 25 f., dort Bezugnahme auf *EuGH*-Urteil Rn. 82 f., 101, 115; zum zweistufigen Prüfungsaufbau von Speicherung und Zugriff nach La Quadrature du Net II *Teichmann*, JR 2026, 441 (443 f.).

⁸ *BGH*, Ur. v. 10.1.2024 – 2 StR 171/23, NStZ 2024, 557 (557) 1. u. 2. Leitsatz; RegE, S. 24 f., 41; kritisch *Ruppert*, ZRP 2026, 82 (85).

⁹ RegE, S. 15 f., 66-69; eingehend zur Trennungsdogmatik des § 177 TKG-E und zu gesetzlichen Mindestanforderungen an die technische Trennung *Teichmann*, JR 2026, 441 (444 f.).

¹⁰ RegE, S. 5-6, 14 f., 42-44, 62-65.

Die dritte Ebene bilden die Erhebungsnormen. § 100g StPO-E betrifft Verkehrsdaten bei Telekommunikationsdiensten; § 100k StPO-E überträgt die Logik auf Nutzungsdaten digitaler Dienste; § 100j StPO-E regelt die Bestandsdatenauskunft, einschließlich der Auskunft anhand einer zu einem bestimmten Zeitpunkt zugewiesenen IP-Adresse. Diese Unterscheidung ist kein begrifflicher Formalismus. Sie entscheidet über Eingriffsschwelle, Anordnungszuständigkeit, Benachrichtigung, Kennzeichnung, Löschung und spätere Verwertbarkeit.¹¹

IV. § 100g StPO-E als Grundnorm der Verkehrsdatenerhebung

1. Grundtatbestand

§ 100g Abs. 1 StPO-E erlaubt die Erhebung von Verkehrsdaten gemäß § 3 Nr. 70 TKG bei Anbietern öffentlich zugänglicher Telekommunikationsdienste oder Mitwirkenden. Voraussetzung sind bestimmte Tatsachen, die den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine Straftat von auch im Einzelfall erheblicher Bedeutung begangen, versucht oder vorbereitet hat; ferner müssen Erforderlichkeit und Angemessenheit gegeben sein.¹² Nachrichtenmittler werden einbezogen, wenn aufgrund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss oder ihr informationstechnisches System benutzt.¹³

Die zentrale Neuerung liegt im Ausschluss der nach § 177 Abs. 1 TKG-E gespeicherten Daten. § 100g Abs. 1 StPO-E stellt ausdrücklich klar, dass diese Daten nicht unmittelbar als Verkehrsdaten erhoben werden dürfen. Damit wird die IP-Speicherung vom klassischen Verkehrsdatenerhebungsregime abgekoppelt. Der Anschlussinhaber soll nicht dadurch ermittelt werden, dass die Strafverfolgungsbehörde IP-Speicherbestände als Verkehrsdaten erhält. Vielmehr soll der Anbieter die Zuordnung intern vornehmen und der Behörde eine Bestandsdatenauskunft erteilen.

Diese Lösung ist dogmatisch konsequent, weil sie die unionsrechtliche Begrenzung der IP-Speicherung auf Identifizierungszwecke im Strafprozessrecht nachvollzieht. Sie ist aber praktisch anspruchsvoll. Ermittlungsbehörden müssen in ihren Ersuchen künftig präzise unterscheiden, ob sie Verkehrsdaten nach § 100g StPO-E, Nutzungsdaten nach § 100k StPO-E oder Bestandsdaten nach § 100j StPO-E verlangen. Eine pauschale Anforderung „der IP-Daten“ genügt dem neuen System nicht.

2. Straftaten mittels Telekommunikation

§ 100g Abs. 2 StPO-E öffnet die Verkehrsdatenerhebung für Fälle, in denen keine Straftat von erheblicher Bedeutung vorliegt, die Tat aber mittels Telekommunikation begangen wurde. Die Norm verlangt bestimmte Tatsachen

für den Tatverdacht und eine gesteigerte Subsidiarität, was bedeutet, dass die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert sein müsste; eine Erhebung zur Aufenthaltsortermittlung bleibt ausgeschlossen.¹⁴

Die Vorschrift ist für digitale Alltagskriminalität bedeutsam. Betrug über Messenger, Drohungen, Beleidigungen, kleinere Vermögensdelikte oder kommunikative Vorbereitungshandlungen können ohne Verkehrsdaten schwer aufklärbar sein. Gleichwohl darf „mittels Telekommunikation“ nicht zu einem Auffangtatbestand für jede internetberührte Straftat werden. Die Telekommunikation muss tatfunktional sein. Wer eine Tat nur nachträglich per Chat kommentiert, begeht sie nicht mittels Telekommunikation. Anderenfalls verlöre die Schwelle der erheblichen Bedeutung ihre filternde Wirkung.

Zudem ist der Begriff der wesentlichen Erschwerung justiziabel auszufüllen. Er darf nicht schon dann bejaht werden, wenn Verkehrsdaten die Ermittlungen beschleunigen würden. Erforderlich ist vielmehr, dass andere Ermittlungsansätze nach Lage der Akten ernsthaft nicht denselben Erkenntniswert versprechen. Die Vorschrift verlangt daher eine konkrete Alternativenprüfung, nicht eine Routineformel.

3. Standortdaten und Funkzellenabfrage

§ 100g Abs. 3 StPO-E regelt Standortdaten. Sie dürfen nur unter den Voraussetzungen des Abs. 1 erhoben werden und zusätzlich nur, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre. Die Norm erfasst vorhandene und künftige Standortdaten einheitlich. Das ist sachgerecht, weil die Eingriffsintensität weniger vom Entstehungszeitpunkt als von der Möglichkeit abhängt, Aufenthalts- und Bewegungsmuster zu rekonstruieren.¹⁵

§ 100g Abs. 4 StPO-E bestimmt sodann: Die Erhebung aller in einer Funkzelle angefallenen Verkehrsdaten ist unter den Voraussetzungen des Abs. 3 zulässig. Die Funkzellenabfrage ist damit keine bloße Variante des Grundtatbestands, sondern eine streubreitenintensive Standortdatenmaßnahme. Sie erfasst notwendig eine Vielzahl unbeteiligter Personen, deren Daten allein deshalb in den staatlichen Auswertungsbereich gelangen, weil sie sich in einem bestimmten Zeitraum im Erfassungsbereich einer Funkzelle befanden.¹⁶

Gerade diese Streubreite zwingt zu einer eigenständigen Verhältnismäßigkeitsprüfung. Die Schwelle der Straftat von erheblicher Bedeutung ist nur tragfähig, wenn der Beschluss die räumliche und zeitliche Eingrenzung, den mutmaßlichen Erkenntniswert und die erwartbare Drittbetroffenheit konkret behandelt. § 101a Abs. 1 S. 1 Nr. 1 lit. b StPO-E verlangt eine räumlich und zeitlich eng begrenzte

¹¹ RegE, S. 4-7, 36-49.

¹² Kritisch Schweda, ZRP 2025, 6 (7).

¹³ RegE, S. 4, 5, 38-39.

¹⁴ RegE, S. 5, 39.

¹⁵ RegE, S. 5, 39-40.

¹⁶ RegE, S. 5, 40-41.

und hinreichend bestimmte Bezeichnung der Telekommunikation. Diese formale Anforderung muss materiell mit Leben gefüllt werden. Bei dicht besiedelten Innenstadtlagen oder großflächigen Funkzellen kann dieselbe Zeitspanne eine erheblich andere Eingriffsintensität aufweisen als in ländlichen Gebieten.

4. Identifizierungsdaten bei nummernunabhängigen interpersonellen Kommunikationsdiensten

§ 100g Abs. 5 StPO-E erlaubt der Strafverfolgungsbehörde bei einem nummernunabhängigen interpersonellen Kommunikationsdienst die Erhebung bestimmter Verkehrsdaten zum Zweck der Identifikation des Beschuldigten, wenn ihr der Inhalt der Nutzung des Dienstes bereits bekannt ist. Erfasst sind insbesondere die gespeicherte öffentliche IP-Adresse, Datum und sekundengenaue Uhrzeit unter Angabe der Zeitzone sowie Portnummern und weitere zur Identifizierung erforderliche Verkehrsdaten.¹⁷

Die Vorschrift bildet den ersten Schritt einer Identifizierungskette. Ein bereits bekannter Inhalt, wie etwa eine gemeldete Nachricht, ein Upload, eine rechtswidrige Kommunikation oder ein Accountvorgang, wird mit technischen Nutzungs- oder Verkehrsdaten verknüpft. Anschließend kann die IP-Adresse über § 100j Abs. 2 StPO-E und § 177 TKG-E einem Anschlussinhaber zugeordnet werden. Diese Kette ist praktisch effektiv, aber dogmatisch empfindlich. Denn die Eingriffsintensität ergibt sich nicht nur aus dem ersten Abruf beim Dienst, sondern aus der Verknüpfung verschiedener Rechtsgrundlagen.

Daraus folgt, dass § 100g Abs. 5 StPO-E nicht als niedrigschwelliger Ersatz für eine umfassende Verkehrsdatenerhebung verstanden werden darf. Die Norm setzt voraus, dass der Inhalt der Nutzung bereits bekannt ist. Sie dient der Identifikation, nicht der Aufklärung unbekannter Kommunikationsbeziehungen. Der Begriff des Identifizierungszwecks muss deshalb eng verstanden werden.

V. § 100j StPO-E und § 177 TKG-E: Bestandsdatenauskunft anhand der IP-Adresse

Die wichtigste dogmatische Weichenstellung des Entwurfs liegt im Verhältnis von § 100g StPO-E zu § 100j StPO-E und § 177 TKG-E. § 177 TKG-E speichert technisch Verkehrsdaten. Strafprozessual sollen diese Daten aber nicht als Verkehrsdaten abgerufen werden. § 100g Abs. 1 StPO-E schließt dies ausdrücklich aus. Der Zugriff erfolgt vielmehr über § 100j Abs. 2 StPO-E als Auskunft anhand einer zu einem bestimmten Zeitpunkt zugewiesenen IP-Adresse.¹⁸

Formal bleibt die Antwort eine Bestandsdatenauskunft. Die Behörde erhält nicht die Kommunikationsbeziehungen, nicht die Dauer einer Verbindung, nicht den Verlauf der Nutzung und nicht den Standort, sondern die Identität oder Anschlusszuordnung. Materiell beruht diese Antwort jedoch auf einer Auswertung vorsorglich gespeicherter

Verkehrsdaten. Der Eingriff ist deshalb nicht dadurch erledigt, dass die Behörde nur Bestandsdaten erhält. Die Speicher- und Auswertungskette bleibt grundrechtlich relevant.

Diese Doppelnatur ist für die Verteidigung und für die gerichtliche Kontrolle zentral. Es ist zu dokumentieren, ob eine Identifizierung auf Daten beruhte, die aufgrund der dreimonatigen Speicherpflicht des § 177 TKG-E vorhanden waren, oder ob sie aus betriebsbedingt gespeicherten Daten erfolgte. Nur dann lässt sich prüfen, ob die gesetzlichen Voraussetzungen eingehalten, Speicherfristen gewahrt und Zweckbindungen beachtet wurden. Eine quellenneutrale Aktenführung würde die Kontrolle des gesamten Modells schwächen.

Zugleich ist die Trennung zwischen Bestandsdaten, Verkehrsdaten und Nutzungsdaten von praktischer Bedeutung. § 100j Abs. 1 Nr. 1 StPO-E betrifft Bestandsdaten nach dem TKG und die nach § 172 Abs. 1 TKG erhobenen Daten bei Telekommunikationsdiensten. § 100j Abs. 1 Nr. 2 StPO-E betrifft Bestandsdaten nach dem TDDDG bei digitalen Diensten. § 100k StPO-E betrifft Nutzungsdaten digitaler Dienste. Diese Unterscheidung verhindert, dass digitale Dienste und Telekommunikationsdienste unter einer konturlosen „Plattformdaten“-Kategorie zusammengezogen werden.¹⁹

VI. Nutzungsdaten nach § 100k StPO-E

§ 100k StPO-E ist im Entwurf nicht bloß Begleitnorm, sondern Ausdruck einer zweiten Achse digitaler Ermittlungen. Während § 100g StPO-E den Telekommunikationsbereich adressiert, erfasst § 100k StPO-E digitale Dienste. Nutzungsdaten des Beschuldigten dürfen unter den Voraussetzungen des § 100g Abs. 1 S. 1 StPO-E erhoben werden; bei mittels eines digitalen Dienstes begangenen Straftaten gilt § 100g Abs. 2 entsprechend. Standortdaten bei digitalen Diensten unterfallen § 100k Abs. 3 StPO-E; Identifizierungsdaten werden über § 100k Abs. 4 StPO-E in Parallele zu § 100g Abs. 5 StPO-E erfasst.²⁰

Diese Parallelisierung ist grundsätzlich sachgerecht. Kriminalität verlagert sich nicht allein in Telekommunikationsnetze, sondern in Plattformen, Cloud-Dienste, soziale Netzwerke, Marktplätze und Messenger-Ökosysteme. Strafprozessual wäre es dogmatisch unbefriedigend, vergleichbare Identifizierungsbedürfnisse je nach Dienstarchitektur völlig unterschiedlich zu behandeln. Gleichwohl muss die Parallelisierung Grenzen behalten. Nutzungsdaten können, je nach Dienst, erheblich aussagekräftiger sein als klassische Verkehrsdaten. Login-Historien, Accountaktivitäten, Upload-Zeitpunkte oder Standortfunktionen digitaler Dienste können in ihrer Gesamtheit ein detailliertes Nutzungsprofil ergeben.

§ 100k Abs. 5 StPO-E verlangt deshalb folgerichtig, dass aufgrund von Tatsachen die Annahme gerechtfertigt ist,

¹⁷ RegE, S. 5 f., 41-42.

¹⁸ RegE, S. 4, 6, 45-46.

¹⁹ RegE, S. 6-7, 45-49.

²⁰ RegE, S. 7, 47-49.

dass die betroffene Person den digitalen Dienst des Verpflichteten nutzt. Diese Voraussetzung verhindert zwar keinen Profilbildungszugriff, zwingt aber zu einer konkreten Dienstbezogenheit. Gerade bei großen Plattformen genügt nicht die allgemeine Vermutung, ein Beschuldiger könne „irgendeinen“ Account nutzen. Die Maßnahme muss account-, dienst- und zweckbezogen begründet werden.

VII. Die Sicherungsanordnung nach § 100g Abs. 7 StPO-E

Die Sicherungsanordnung ist das eigenständigste neue strafprozessuale Instrument des Entwurfs. Sie erlaubt keine Erhebung, sondern eine Konservierung. § 100g Abs. 7 S. 2 StPO-E stellt ausdrücklich klar, dass die spätere Erhebung der gesicherten Daten nach § 100g Abs. 1 bis 4 StPO-E erfolgt. Damit ist die Sicherung akzessorisch. Sie darf nur Daten betreffen, deren spätere Erhebung nach der Struktur der Abs. 1 bis 4 überhaupt in Betracht kommt.²¹

Der Entwurf begründet die Maßnahme mit der Flüchtigkeit von Verkehrsdaten und der Notwendigkeit, Löschung zu verhindern, wenn die Erhebungsvoraussetzungen aus tatsächlichen oder rechtlichen Gründen noch nicht vollständig geklärt sind. Dieser Ansatz ist plausibel.²² Gerade zu Beginn eines Ermittlungsverfahrens kann unklar sein, welcher Anschluss, welche Person, welcher Zeitraum oder welcher Dienst betroffen ist.²³ Ohne Sicherung können relevante Daten verloren sein, bevor ein richterlicher Beschluss substantiell vorbereitet werden kann.²⁴

Gleichwohl ist die Sicherungsanordnung nicht eingriffsneutral. Sie ändert die datenschutzrechtliche Lage. Daten, die nach den allgemeinen Regeln zu löschen wären oder nur kurzfristig verfügbar blieben, werden aufgrund staatlicher Anordnung erhalten und für eine spätere Verwendung verfügbar gemacht. Der Eingriff liegt nicht in der behördlichen Kenntnisnahme, sondern in der staatlich veranlassten Zweckänderung und Aufbewahrung. Dieser Eingriff kann gering sein, wenn einzelne Daten eines Beschuldigten kurzfristig gesichert werden; er kann erheblich sein, wenn Funkzellendaten, Standortdaten oder Daten zahlreicher Dritter betroffen sind.

Problematisch ist deshalb die Eingriffsschwelle. § 100g Abs. 7 StPO-E verlangt lediglich zureichende tatsächliche Anhaltspunkte für eine Straftat, welche die spätere Erhebung rechtfertigen würde, einen persönlichen oder räumlichen Bezug der betroffenen Person zur Tat und eine mögliche Bedeutung der Daten. Diese Schwelle liegt bewusst unterhalb der Erhebungsschwelle. Sie ist hinnehmbar, solange die Sicherung eng begrenzt und kontrolliert wird. Sie wird fragwürdig, wenn der räumliche Bezug genügt, um breite Datenmengen zu konservieren.²⁵

Die Norm sollte daher nicht als Ermittlungsreservoir verstanden werden. „Räumlicher Bezug“ darf nicht bedeuten, dass alle in Tatortnähe anfallenden Verkehrsdaten routinemäßig gesichert werden. Erforderlich ist eine plausible Hypothese, warum gerade diese Daten später für die Erforschung des Sachverhalts oder die Aufenthaltsortermittlung bedeutsam sein können. Das gilt besonders bei Funkzellen, weil hier die Drittbetroffenheit strukturell angelegt ist.

VIII. Verfahrenssicherungen nach § 101a StPO-E

§ 101a StPO-E ist der prozessuale Knotenpunkt des Entwurfs. Die Norm bündelt Verfahrensregelungen für Verkehrs-, Nutzungs- und Bestandsdaten. Für Erhebungen nach § 100g Abs. 1 bis 4 StPO-E gilt § 100e Abs. 1, 3 und 5 StPO entsprechend. Damit bleibt es grundsätzlich beim Richtervorbehalt; die Entscheidungsformel muss die zu übermittelnden Daten und den Zeitraum eindeutig bezeichnen. Für Funkzellenabfragen genügt eine räumlich und zeitlich eng begrenzte und hinreichend bestimmte Bezeichnung der Telekommunikation.²⁶

Für Sicherungsanordnungen sieht § 101a Abs. 1 S. 1 Nr. 3 lit. a StPO-E eine abweichende Kompetenzordnung vor. Die Staatsanwaltschaft kann die Maßnahme für höchstens drei Monate anordnen; bei Gefahr im Verzug auch ihre Ermittlungspersonen. Nur eine Verlängerung um höchstens weitere drei Monate bedarf gerichtlicher Entscheidung. Diese Konstruktion ist der Schnelligkeit der Sicherung geschuldet.²⁷ Sie führt aber dazu, dass die erste Sicherungsphase ohne richterliche Anordnung und ohne zwingende nachträgliche Bestätigung auskommt.²⁸

Der Entwurf rechtfertigt dies mit der geringeren Eingriffstiefe. Weil die Daten zunächst nicht an die Behörde herausgegeben werden, sei die Sicherung weniger belastend als die Erhebung. Diese Überlegung trägt im Grundsatz, aber nicht unterschiedslos. Die Eingriffstiefe hängt nicht allein von der Herausgabe ab. Sie hängt auch von Umfang, Dauer, Datenart und Streubreite ab. Eine Sicherung einzelner Verkehrsdaten eines Beschuldigten ist anders zu bewerten als die Sicherung aller Daten einer Funkzelle oder mehrerer Standortdaten über längere Zeiträume.

§ 101a Abs. 2 StPO-E verlangt bei Anordnung oder Verlängerung einer Maßnahme nach § 100g Abs. 1 bis 4 oder 7, § 100j Abs. 3 oder § 100k Abs. 1 bis 3 StPO-E eine einzelfallbezogene Begründung, insbesondere zu Erforderlichkeit, Angemessenheit, Umfang und Zeitraum.²⁹ Diese Begründungspflicht ist zentral. Sie muss in der Praxis verhindern, dass die neuen Normen zu Textbausteininstrumenten werden. Der Antrag hat darzulegen, welche Daten benötigt werden, warum sie für den konkreten Ermittlungszweck Bedeutung haben können und weshalb

²¹ RegE, S. 6, 44-45.

²² Krause, ZRP 2023, 169 (170).

²³ Stellungnahme des Bund Deutscher Kriminalbeamter (BDK) v. 30.1.2026, Punkt 2. zum Referentenentwurf, abrufbar unter: <https://bit.ly/4fBh507> (zuletzt abgerufen am 20.5.2026).

²⁴ RegE, S. 24-25, 44-45.

²⁵ RegE, S. 6, 44; zum Risiko des Over-Freezing bei breiten, namentlich funkzellenbezogenen Sicherungen Teichmann, JR 2026, 441 (446).

²⁶ RegE, S. 7-8, 49-51.

²⁷ Krause, ZRP 2023, 169 (170).

²⁸ RegE, S. 8, 51, 52.

²⁹ Schweda, ZRP 2025, 6 (7)

mildere Maßnahmen nicht genügen.³⁰

Lückenhaft ist § 101a Abs. 2 StPO-E bei den Identifizierungsmaßnahmen. § 100g Abs. 5, § 100j Abs. 2 und § 100k Abs. 4 StPO-E werden von der ausdrücklichen Begründungsregel nicht erfasst. Das ist dogmatisch erklärbar, weil es sich um weniger eingriffsintensive Identifizierungszugriffe handeln soll. Praktisch überzeugt es nicht vollständig. Gerade die Verkettung von § 100g Abs. 5 oder § 100k Abs. 4 mit § 100j Abs. 2 und § 177 TKG-E kann erhebliche Ermittlungsfolgen auslösen. Eine kurze, aktenkundige Begründung sollte auch hier verlangt werden.

§ 101a Abs. 3 StPO-E regelt Kennzeichnung, unverzügliche Auswertung und Löschung für personenbezogene Daten aus Maßnahmen nach § 100g Abs. 1 bis 4, § 100j Abs. 3 und § 100k Abs. 1 bis 3 StPO-E. Nicht erfasst sind § 100j Abs. 2 StPO-E, § 100g Abs. 5 StPO-E und § 100k Abs. 4 StPO-E. Auch insoweit besteht Nachschärfungsbedarf. Die Herkunft einer IP-basierten Identifizierung muss kenntlich bleiben, weil nur so kontrolliert werden kann, ob sie auf § 177 TKG-E beruhte und ob die dortigen Verwendungsgrenzen eingehalten wurden.³¹

Die Benachrichtigung nach § 101a Abs. 4 StPO-E erfasst Erhebungen nach § 100g Abs. 1 bis 5, § 100j Abs. 2 und 3 sowie § 100k Abs. 1 bis 4 StPO-E. Für die bloße Sicherungsanordnung besteht keine Benachrichtigungspflicht. Das ist nachvollziehbar, wenn die Daten nie erhoben und fristgerecht gelöscht werden. Bei umfangreichen Sicherungen mit hoher Drittbetroffenheit überzeugt der völlige Verzicht auf Transparenz jedoch nicht. Jedenfalls eine gerichtliche oder datenschutzaufsichtliche Nachkontrolle wäre angezeigt.³²

IX. Funkzellenabfrage: gesetzgeberische Reaktion auf den BGH

Die Funkzellenabfrage ist der kriminalpraktische Kristallisationspunkt des Entwurfs. Der BGH-Beschluss vom 10.1.2024 hatte die Anordnung bei geschäftlich gespeicherten Verkehrsdaten an den Verdacht einer besonders schweren Straftat nach § 100g Abs. 2 StPO gebunden. Der RegE reagiert, indem er die Funkzellenabfrage in § 100g Abs. 4 StPO-E eigenständig regelt und die Schwelle der Straftat von auch im Einzelfall erheblicher Bedeutung genügen lässt.³³

Diese Reaktion ist aus Sicht der Praxis verständlich. Der RegE weist darauf hin, dass die überwiegende Strafverfolgungspraxis vor der BGH-Entscheidung von dieser niedrigeren Schwelle ausgegangen war. Zudem zeigen die Zahlen des Entwurfs, dass Funkzellenabfragen einen erheblichen Anteil der Maßnahmen nach § 100g StPO ausmachen. Die Neuregelung beseitigt damit Unsicherheit

und stellt ein etabliertes Ermittlungsinstrument wieder auf eine klare gesetzliche Grundlage.³⁴

Doch die dogmatische Frage ist damit nicht erledigt. Die Funkzellenabfrage ist nicht individualisiert. Sie arbeitet mit räumlicher und zeitlicher Verdichtung, nicht mit zielpersonenbezogener Auswahl. Ihr Erkenntniswert beruht gerade darauf, dass zunächst eine Vielzahl von Daten erhoben und anschließend durch Abgleich, Ausschluss und Verdichtung gefiltert wird. Damit entsteht ein struktureller Konflikt zwischen Ermittlungslogik und Verhältnismäßigkeit.³⁵

Die Schwelle „Straftat von erheblicher Bedeutung“ muss deshalb einzelfallbezogen ernst genommen werden. Es genügt nicht, dass der Deliktstyp abstrakt bedeutsam ist. § 100g Abs. 1 StPO-E verlangt ausdrücklich eine Straftat von auch im Einzelfall erheblicher Bedeutung. Bei Vermögensdelikten, Serientaten oder bandenbezogenen Sachverhalten kann dies vorliegen; bei Bagatel- oder Randfällen nicht. Die Maßnahme muss zudem subsidiär sein. Eine Funkzellenabfrage darf nicht angeordnet werden, wenn naheliegende weniger streubreite Ermittlungsansätze bestehen.

Besondere Bedeutung kommt der Streubreite zu. Die Anordnung sollte die erwartete Zahl potentiell betroffener Anschlüsse, die räumliche Dichte der Funkzelle, den Zeitraum, die Tatortnähe und den geplanten Auswertungsmodus ansprechen. Je breiter die Maßnahme streut, desto konkreter muss der Erkenntnisgewinn begründet werden. Der Entwurf enthält hierfür bisher keine ausdrückliche Streubreitenklausel. § 101a Abs. 1 S. 1 Nr. 1 lit. b StPO-E bietet eine formale Begrenzung; eine materielle Streubreitenprüfung sollte ergänzt werden.

Hinzu kommt eine redaktionelle Unschärfe. § 101a Abs. 1 S. 1 Nr. 3 lit. c StPO-E verweist bei der Sicherung von Daten einer Funkzelle auf § 100g Abs. 3 StPO-E. Die Funkzellenabfrage ist jedoch in § 100g Abs. 4 StPO-E geregelt. Dieser Verweis sollte korrigiert werden. In einem Normkomplex, der Datenarten, Eingriffsstufen und Kontrollregime präzise unterscheiden will, ist Normenklarheit keine Nebensache.³⁶

X. Art. 10 GG, ePrivacy-RL und Grundrechtecharta

Die verfassungsrechtliche Bewertung beginnt bei Art. 10 Abs. 1 GG. Der RegE selbst ordnet an, dass durch die Änderungen unter anderem das Fernmeldegeheimnis eingeschränkt wird. Verkehrsdaten- und Standortdatenerhebungen berühren Art. 10 GG unmittelbar. Bestandsdatenauskünfte anhand einer IP-Adresse stehen jedenfalls im Schutzbereich des Rechts auf informationelle Selbstbestimmung; soweit sie auf die Zuordnung eines Telekommunikationsvorgangs bezogen sind, besteht eine Nähe zu

³⁰ RegE, S. 8, 53.

³¹ RegE, S. 8, 53.

³² RegE, S. 8, 54-55.

³³ BGH, Beschl. v. 10.01.2024 – 2 StR 171/23, NStZ 2024, 557 (557), 1. u. 2. Leitsatz; RegE, S. 5, 24-25, 40-41.

³⁴ RegE, S. 31.

³⁵ Puschke, GSZ 2024, 23 (25); für engere Begründungs-, Reduktions- und Löschungspflichten bei Funkzellenabfragen Teichmann, JR 2026, 441 (446 f.).

³⁶ RegE, S. 5, 8.

Art. 10 GG.³⁷

Das *BVerfG* hat die Speicherung und Verwendung von Telekommunikationsverkehrsdaten stets als besonders rechtfertigungsbedürftig angesehen. Zugleich unterscheidet es nach Datenart, Umfang, Zweckbindung und Zugriffstiefe. Diese Differenzierung entspricht der unionsrechtlichen Linie. Eine punktuelle IP-Identifizierung ist nicht mit einer umfassenden Vorratsdatenspeicherung von Verkehrs- und Standortdaten gleichzusetzen. Sie bleibt aber ein Eingriff, dessen Rechtfertigung an Normenklarheit, Zweckbindung, Datensicherheit, Löschung und Rechtsschutz hängt.³⁸

Unionsrechtlich ist Art. 15 Abs. 1 ePrivacy-RL maßgeblich. Die Norm erlaubt Beschränkungen der Vertraulichkeit elektronischer Kommunikation nur, wenn sie in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig sind und einem anerkannten Ziel dienen. Art. 7³⁹, 8⁴⁰, 11⁴¹ und 52 Abs. 1 GRCh⁴² konkretisieren diese Anforderungen. Die Speicherung von IP-Adressen ist nach *La Quadrature du Net II/HADOPI* zulässig, wenn sie nicht zu präzisen Schlüssen auf das Privatleben führt und wenn die Trennung verschiedener Datenkategorien wirksam gewährleistet wird.⁴³

Der RegE versucht, diese Anforderungen durch Beschränkung der Speicherpflicht, Ausschluss von Inhalts- und Nutzungsdaten, technische Trennung und Zweckbindung umzusetzen. § 177 Abs. 3 TKG-E verlangt Schutz nach dem Stand der Technik, technisch wirksame Trennung von anderen Endnutzerdaten, unverzügliche Auskunftsfähigkeit und irreversible Löschung nach Ablauf der Speicherfrist. § 177 Abs. 4 TKG-E begrenzt die Verwendung auf Auskünfte zur Identifizierung von Anschlussinhabern und bestimmte e-Evidence-Konstellationen. Dies ist unionsrechtlich der richtige Ansatz.⁴⁴

Kritisch bleibt die Dreimonatsfrist, die aus dem Koalitionsvertrag der aktuellen Bundesregierung entstanden ist.⁴⁵ Der Entwurf begründet sie mit praktischen Erfolgsquoten und der Erfahrung, dass bisherige Speicherungen häufig nur wenige Tage reichen. Als Grundlage für die Festlegung auf die dreimonatige Frist werden die polizeilichen Erfahrungen im Zusammenhang mit dem oft erst verspäteten Bekanntwerden der Straftat und dem damit verbundenen Ermittlungsbeginn gemacht.⁴⁶ Diese Frist

wird teilweise dahin kritisch gesehen, ob sie dem Grundsatz der Verhältnismäßigkeit, der Erforderlichkeit und Datenminimierung entspricht.⁴⁷ Vom Deutschen Richterbund wird sie als praxisgerecht bewertet.⁴⁸ Eine dreimonatige Frist ist nicht evident unverhältnismäßig, aber sie bedarf einer belastbaren Evaluation. Entscheidend wird sein, ob die Frist tatsächlich in relevanten Deliktgruppen erforderlich ist oder ob ein kürzerer Zeitraum bei vergleichbarer Effektivität genügt. Eine Sunset- oder Evaluationsklausel wäre deshalb nicht nur rechtspolitisch, sondern verhältnismäßigkeitsdogmatisch naheliegend.⁴⁹

Die Sicherungsanordnung ist unionsrechtlich anders zu bewerten als die IP-Speicherung. Sie ist anlassbezogen und sachlich beschränkt. Damit liegt sie näher an dem vom EuGH anerkannten Quick-Freeze-Gedanken. Allerdings darf der anlassbezogene Charakter nicht durch weite Sicherungsanordnungen entleert werden. Je größer die Datenmenge und Drittbetroffenheit, desto stärker sind Richtervorbehalt, Begründung und nachträgliche Kontrolle zu gewichten.⁵⁰

XI. Praktische Konsequenzen

Für Ermittlungsrichter wird die Prüfung kleinteiliger. Zunächst ist die richtige Datenkategorie zu bestimmen in Form von Verkehrsdaten, Nutzungsdaten oder Bestandsdaten. Sodann ist zu klären, ob die Maßnahme Erhebung, Sicherung oder Identifizierung betrifft. Schließlich sind Zeitraum, Datenumfang, Verpflichteter, Zielperson und Ermittlungszweck zu konkretisieren. Gerade bei Funkzellenabfragen muss die richterliche Entscheidung mehr leisten als die Bestätigung eines Formularantrags.

Für Staatsanwaltschaften steigt die Begründungs- und Dokumentationslast. Sicherungsanordnungen müssen den Anfangsverdacht, den persönlichen oder räumlichen Bezug, die mögliche Beweisbedeutung und die Dauer der Sicherung erkennen lassen. Bei Gefahr im Verzug durch Ermittlungspersonen ist besonders sorgfältig zu dokumentieren, warum eine staatsanwaltschaftliche oder gerichtliche Befassung nicht rechtzeitig möglich war. Andernfalls drohen spätere Verwertungsstreitigkeiten.

Für die Verteidigung entstehen neue Prüfungsachsen. Erstens ist zu prüfen, ob die Behörde die richtige Eingriffsnorm gewählt hat. Zweitens ist zu fragen, ob § 177

³⁷ RegE, S. 22; *Gusy*, in: Huber/Voßkuhle, GG, 8. Aufl. (2024), Art. 10 Rn. 73–78; *Jarass*, in: Jarass/Pieroth, GG, 18. Aufl. (2024), Art. 2 Rn. 43–57.

³⁸ *BVerfG*, Urt. v. 2.3.2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, BVerfGE 125, 260; *BVerfG*, Beschl. v. 27.5.2020 – 1 BvR 1873/13, 1 BvR 2618/13, BVerfGE 155, 119 Rn. 17, 19, 93–95, 201.

³⁹ *Jarass*, GRCh, 4. Aufl. (2021), Art. 7 Rn. 27; *Kingreen*, in: Calliess/Ruffert, EUV/AEUV, 6. Aufl. (2022), EU-GRCharta Art. 7 Rn. 10; *Bernsdorff*, in: Meyer/Hölscheidt, Charta der Grundrechte der Europäischen Union, 6. Aufl. (2024), Art. 7 Rn. 12.

⁴⁰ *Kingreen*, in: Calliess/Ruffert, EUV/AEUV, EU-GRCharta Art. 8 Rn. 13–14.

⁴¹ *Jarass*, GRCh, Art. 11 Rn. 20–21; *Bernsdorff*, in: Meyer/Hölscheidt, Charta der Grundrechte der Europäischen Union, Art. 11 Rn. 15.

⁴² *Kainer*, in: Pechstein/Nowak/Häde, EUV/GRCh/AEUV, 2. Aufl. (2023), GRCh Art. 52 Rn. 15; *Jarass*, GRCh, Art. 52 Rn. 23–26.

⁴³ RL (EU) 2002/58/EG, ABl. L. 201, Art. 15; zu atypischen Verknüpfungslagen, in denen die IP-Auskunft mittelbar sensible Kontakte zu Berufsgeheimnisträgern offenbaren kann, *Teichmann*, JR 2026, 441 (447 f.).

⁴⁴ RegE, S. 16, 69–70.

⁴⁵ Koalitionsvertrag der 21. Legislaturperiode, Zeilen 2630–2632, abrufbar unter <https://bit.ly/3QVuvLf> (zuletzt abgerufen am 20.5.2026).

⁴⁶ RegE, S. 68, 69.

⁴⁷ *Ruppert*, ZRP 2026, 82 (84).

⁴⁸ DRB v. 29.1.2026, 2/2026, abrufbar unter: <https://bit.ly/4vw0JuC> (zuletzt abgerufen am 20.5.2026).

⁴⁹ RegE, S. 69–70; ebenso für eine Evaluationsklausel mit automatischer Rückführung auf eine kürzere Frist *Teichmann*, JR 2026, 441 (445, 449).

⁵⁰ RegE, S. 26; *EuGH*, Urt. v. 6.10.2020 – C-511/18, C-512/18, C-520/18, NJW 2021, 531 (531); VO (EU) 2023/1543, ABl. L. 191, Art. 6.

TKG-E unzulässig über § 100g StPO-E instrumentalisiert wurde. Drittens ist bei IP-basierten Identifizierungen zu klären, ob Zeitstempel, Zeitzone und Portnummern hinreichend bestimmt waren. Viertens ist bei Funkzellenabfragen die konkrete Streubreite anzugreifen. Fünftens sind Benachrichtigung, Kennzeichnung und Löschung zu kontrollieren.

Besondere Bedeutung hat die Aktenführung. Die Ermittlungsakte muss erkennen lassen, auf welcher Grundlage ein Anschlussinhaber identifiziert wurde. Wurde die Zuordnung auf § 177 TKG-E gestützt, muss dies vermerkt sein. Wurde zuvor ein Dienst nach § 100g Abs. 5 oder § 100k Abs. 4 StPO-E abgefragt, muss die Identifizierungskette dokumentiert werden. Nur eine solche Transparenz ermöglicht effektive Verteidigung und gerichtliche Kontrolle.

XII. Änderungsvorschläge

Erstens sollte § 101a Abs. 1 S. 1 Nr. 3 lit. c StPO-E redaktionell korrigiert werden. Bei der Sicherung von Funkzellendaten ist auf § 100g Abs. 4 StPO-E zu verweisen, nicht auf § 100g Abs. 3 StPO-E. Die Korrektur ist klein, aber normenklarheitsrelevant.

Zweitens sollte für Sicherungsanordnungen mit erheblicher Streubreite eine zeitnahe gerichtliche Bestätigungspflicht eingeführt werden. Dies betrifft insbesondere Funkzellendaten, Standortdaten und sonstige Sicherungen, die eine Vielzahl unbeteiligter Personen erfassen können. Die Erstkompetenz der Staatsanwaltschaft kann zur Sicherung flüchtiger Daten erhalten bleiben; eine nachträgliche gerichtliche Bestätigung binnen weniger Tage würde den Zweck nicht vereiteln.

Drittens sollte § 100g Abs. 7 S. 1 Nr. 2 StPO-E präzisiert werden. Der persönliche oder räumliche Bezug zur Tat sollte auf konkrete Tatsachen gestützt werden müssen. Bloße Tatortnähe darf nicht ausreichen, wenn nicht plausibel dargelegt wird, weshalb gerade die Daten der betroffenen Person oder des betroffenen Raums später beweisbedeutsam sein können.

Viertens sollte § 101a Abs. 2 StPO-E auf die Identifizierungsmaßnahmen nach § 100g Abs. 5, § 100j Abs. 2 und § 100k Abs. 4 StPO-E erstreckt werden. Die Begründung kann weniger streng ausfallen als bei umfassenden Verkehrsdatenabrufen. Sie sollte aber festhalten, welcher Inhalt bereits bekannt ist, welcher Identifizierungszweck verfolgt wird und warum die IP-basierte Zuordnung erforderlich ist.

Fünftens sollte § 101a Abs. 3 StPO-E eine Kennzeichnungspflicht für Daten und Erkenntnisse aufnehmen, die

aus einer Auskunft unter Rückgriff auf § 177 TKG-E stammen. Dies betrifft nicht nur die Rohdaten, sondern auch die daraus abgeleitete Identität des Anschlussinhabers. Ohne Kennzeichnung wird die Zweckbindungs- und Löschungskontrolle faktisch erschwert.

Sechstens sollte § 177 TKG-E evaluiert werden. Die Dreimonatsfrist ist der Grundrechtsschwerpunkt der vorsorglichen IP-Adressspeicherung. Der Gesetzgeber sollte nach Ablauf einer festen Frist prüfen, in welchen Deliktgruppen die Speicherung tatsächlich zu Aufklärungserfolgen geführt hat, wie häufig Fehlsicherungen auftraten, welche Datenmengen gespeichert wurden und ob eine kürzere Frist genügt.

XIII. Fazit in sieben Thesen

1. Der RegE ist kein Quick-Freeze-Gesetz in Reinform. Er kombiniert vorsorgliche IP-Adressspeicherung, anlassbezogene Sicherungsanordnung und neu strukturierte Erhebungsnormen.
2. Die ausdrückliche Herausnahme der nach § 177 TKG-E gespeicherten Daten aus § 100g Abs. 1 StPO-E ist die zentrale dogmatische Sicherung des Entwurfs. Sie verhindert den unmittelbaren Verkehrsdatendurchgriff auf den IP-Speicher.
3. § 100j Abs. 2 StPO-E wird durch § 177 TKG-E praktisch erheblich aufgewertet. Formal bleibt es bei Bestandsdatenauskunft; funktional entsteht ein verlässliches Identifizierungsinstrument.
4. Die Sicherungsanordnung nach § 100g Abs. 7 StPO-E ist nicht nur vorbereitend, sondern eingriffsrelevant. Sie konserviert Daten staatlich veranlasst und bedarf deshalb bei hoher Streubreite zusätzlicher Kontrolle.
5. Die Funkzellenabfrage wird gesetzgeberisch reaktiviert. Die Rückführung auf die Schwelle der Straftat von erheblicher Bedeutung ist nur bei strenger Subsidiaritäts-, Streubreiten- und Begründungsprüfung tragfähig.
6. § 101a StPO-E verbessert die Systematik, weist aber Lücken bei Identifizierungsmaßnahmen, Kennzeichnung und Sicherungsanordnungen auf. Diese Lücken sollten vor Inkrafttreten geschlossen werden.
7. Die Vereinbarkeit mit Art. 10 GG, Art. 15 Abs. 1 ePrivacy-RL sowie Art. 7, 8, 11 und 52 GRCh hängt weniger am Etikett der Maßnahme als an der praktischen Trennung von Speicherung, Sicherung und Erhebung. Nur wenn diese Trennung aktenkundig, technisch wirksam und gerichtlich kontrollierbar bleibt, trägt das Modell.