Referentenentwurf

des Bundesministeriums der Justiz

Entwurf eines Gesetzes zur Einführung einer Sicherungsanordnung für Verkehrsdaten in der Strafprozessordnung

A. Problem und Ziel

Mit Urteil vom 20. September 2022 – C-793/19 und C-794/19 – hat der Gerichtshof der Europäischen Union (EuGH) entschieden, dass die Vorschriften des deutschen Rechts zur sogenannten Vorratsdatenspeicherung nicht mit dem Unionsrecht vereinbar sind. Diese Entscheidung fügt sich in die bisherige Rechtsprechung des Gerichtshofs seit dem Jahr 2014 ein, wonach eine generelle und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Nutzer auch zur Bekämpfung schwerer Kriminalität nicht mit dem Unionsrecht vereinbar ist.

Schon zuvor liefen die im Jahr 2015 eingeführten Regelungen zur „Vorratsdatenspeicherung“ in den §§ 175 bis 181 des Telekommunikationsgesetzes (TKG) und in § 100g Absatz 2 der Strafprozessordnung (StPO) weitgehend leer. Nachdem das Oberverwaltungsgericht Nordrhein-Westfalen im Juni 2017 im Eilverfahren die Speicherpflicht gegenüber den klagenden Telekommunikationsdienste-Anbietern einstweilig ausgesetzt hatte, verzichtete die Bundesnetzagentur nämlich bis zur endgültigen Klärung, ob diese Vorschriften europarechtskonform sind, auf jegliche Maßnahmen zur Durchsetzung der gesetzlich nach wie vor bestehenden Speicherpflicht.

Diese Klärung hat der EuGH nunmehr vorgenommen. Aus seinem Urteil folgt, dass der Versuch einer unionsrechtskonformen Ausgestaltung einer anlasslosen „Vorratsdatenspeicherung“ zu Strafverfolgungszwecken im nationalen Recht gescheitert ist; eine Neuauflage der allgemeinen und unterschiedslosen „Vorratsdatenspeicherung“ aller Verkehrsdaten ist aufgrund der höchstrichterlichen Vorgaben nicht möglich.

Zur effektiven Erlangung von digitalen Beweismitteln steht aber eine Alternative zur Verfügung. Der EuGH hat in seinem Urteil vom 20. September 2022 ausdrücklich ausgeführt, dass mit einer anlassbezogenen Sicherung von Verkehrsdaten für einen festgelegten Zeitraum, die einer wirksamen richterlichen Kontrolle unterliegt, ein grundrechtsschonenderes und effektives Ermittlungsinstrument vorhanden ist, welches einer unionsrechtskonformen Regelung im Strafverfahrensrecht zugänglich ist. Diese Vorgaben des Gerichtshofs zu einer unionsrechtskonformen, anlassbezogenen Verkehrsdatenspeicherung sollen mit diesem Gesetz umgesetzt werden.

B. Lösung

Mit diesem Gesetz werden zum einen als zwingende Folge des Urteils des EuGH vom 20. September 2022 – C-793/19 und C-794/19 – die gegen das Unionsrecht verstoßenden Regelungen der „Vorratsdatenspeicherung“ in § 100g Absatz 2 StPO und in den §§ 175 bis 181 TKG aufgehoben.

Zugleich wird in einem neu gefassten § 100g Absatz 5 StPO das Ermittlungsinstrument einer Sicherungsanordnung bereits vorhandener und künftig anfallender Verkehrsdaten eingeführt. Deren Sicherung soll anlassbezogen zur Verfolgung von erheblichen Straftaten

zulässig sein, soweit die Verkehrsdaten für die Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsorts eines Beschuldigten von Bedeutung sein können. Die Maßnahme soll im Grundsatz nur auf Anordnung eines Richters zulässig sein. Damit wird die Menge der zu speichernden Daten auf das notwendige Maß begrenzt, da nur die bei den Anbietern von Telekommunikationsdiensten aus geschäftlichen Gründen ohnehin bereits vorhandenen und künftig anfallenden Verkehrsdaten gesichert werden dürfen („Einfrieren"). Diese Daten stehen den Strafverfolgungsbehörden für eine begrenzte Zeit für eine spätere Erhebung und Auswertung zur Verfügung, die freilich einer erneuten richterlichen Anordnung bedarf („Auftauen").

Die vorgeschlagene Regelung – auch „Quick-Freeze-Regelung" genannt – steht im Einklang mit den Anforderungen, die der EuGH in seiner Rechtsprechung zur „Vorratsdatenspeicherung" seit 2014 formuliert hat. Auch das von der Bundesrepublik Deutschland unterzeichnete und ratifizierte Übereinkommen des Europarats über Computerkriminalität, die sogenannte Budapest-Konvention, enthält in Artikel 16 eine Verpflichtung der Vertragsstaaten, die zuständigen Behörden zu ermächtigen, die umgehende Sicherung von Verkehrsdaten anzuordnen.

Es handelt sich also um eine neue Ausgestaltung der verpflichtenden Verkehrsdatenspeicherung, die einerseits den Grundrechtsschutz der Nutzer von Telekommunikationsdiensten gewährleistet. Andererseits wird den Strafverfolgungsbehörden ein rechtssicheres und effektives Ermittlungsinstrument zur Bekämpfung schwerer Kriminalität im digitalen Raum an die Hand gegeben. Damit trägt der Entwurf zur Erreichung von Ziel 16 „Frieden, Gerechtigkeit und starke Institutionen" der Agenda 2030 für nachhaltige Entwicklung bei.

Die Folgeänderungen im TKG und in der Telekommunikations-Überwachungsverordnung (TKÜV) dienen dazu, auch die dortigen Vorschriften zur „Vorratsdatenspeicherung" aufzuheben und die aus der neuen Sicherungsanordnung folgenden Speicherungs-, Abfragungs-, Übermittlungs- und Löschungspflichten für die Telekommunikationsdienste-Anbieter zu regeln. Neben weiteren Folgeänderungen im Bundespolizeigesetz (BPolG), BSI-Gesetz, Bundeskriminalamtgesetz (BKAG), Zollfahndungsdienstgesetz (ZFdG) und im Einführungsgesetz zur Strafprozessordnung (EGStPO) soll durch Änderungen im Justizvergütungs- und -entschädigungsgesetz (JVEG) sichergestellt werden, dass die verpflichteten Unternehmen auch für ihren im Einzelfall im Rahmen der Sicherungsanordnung nach § 100g Absatz 5 StPO-E anfallenden Aufwand angemessen entschädigt werden.

C. Alternativen

Eine Alternative bestünde in der ersatzlosen Streichung der Regelungen zur „Vorratsdatenspeicherung". Jedoch wird durch die Einführung einer Sicherungsanordnung den Strafverfolgungsbehörden ein verfassungskonformes Instrument zur Verfügung gestellt, das dem berechtigten Anliegen Rechnung trägt, die Flüchtigkeit elektronischer Daten bei der Beweissicherung zu berücksichtigen, ohne Strafverfolgungsvorsorge zu Lasten aller Bürgerinnen und Bürger zu betreiben. Hierdurch wird ein ausgewogener Ausgleich zwischen dem Interesse an einer effektiven Strafverfolgung und dem Interesse der Bürgerinnen und Bürger am Schutz ihrer personenbezogenen Daten und der Vertraulichkeit ihrer Kommunikation geschaffen.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Keine.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Keiner.

E.2 Erfüllungsaufwand für die Wirtschaft

Für die betroffenen Telekommunikationsdienste-Anbieter entsteht durch die Einführung der Sicherungsanordnung ein gewisser Mehraufwand an übergeordneten Investitions- und gesteigerten Betriebskosten zur Umsetzung der Anforderungen aus § 175 TKG-E. Dem steht aber eine erhebliche Entlastung infolge der Abschaffung der „Vorratsdatenspeicherung“ gegenüber [*genaue Bezifferung – ggf. schätzungsweise – soll aufgrund des Ergebnisses der Verbändebeteiligung erfolgen*].

Im Übrigen entsteht für die Wirtschaft kein Erfüllungsaufwand.

Davon Bürokratiekosten aus Informationspflichten

Keine.

E.3 Erfüllungsaufwand der Verwaltung

Auch für die Strafverfolgungsbehörden des Bundes und der Länder ist von einem gewissen Mehraufwand durch die Einführung der Sicherungsanordnung in Form der damit verbundenen Entschädigungszahlungen nach JVEG sowie zusätzlichem Kontrollaufwand und Mehraufwand bei der Anwendung der neuen Bußgeldtatbestände auszugehen. Auch dieser Mehraufwand wird aber vom Minderaufwand infolge der Abschaffung der „Vorratsdatenspeicherung“ kompensiert [*genaue Bezifferung – ggf. schätzungsweise – soll aufgrund des Ergebnisses der Ressortabstimmung und der Länderbeteiligung erfolgen*].

F. Weitere Kosten

Durch das Erfordernis eines Gerichtsbeschlusses für die einzelfallbezogene Sicherungsanordnung ist von einem geringfügigen Mehraufwand für die Justiz auszugehen. [*genaue Bezifferung – ggf. schätzungsweise – soll aufgrund des Ergebnisses der Ressortabstimmung und der Länderbeteiligung erfolgen*]. Von weiteren Kosten ist nicht auszugehen.

Auswirkungen auf Einzelpreise und das allgemeine Preisniveau, insbesondere auf das Verbraucherpreisniveau für Telekommunikationsdienste, sind im Übrigen nicht zu erwarten.

Referentenentwurf des Bundesministeriums der Justiz

Entwurf eines Gesetzes zur Einführung einer Sicherungsanordnung für Verkehrsdaten in der Strafprozessordnung

Vom ...

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Änderung der Strafprozessordnung

Die Strafprozeßordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 2 des Gesetzes vom 25. März 2022 (BGBl. I S. 571) geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht wird die Angabe zu § 100g wie folgt gefasst:

   „§ 100g Erhebung von Verkehrsdaten und Sicherungsanordnung“.

2. § 100g wird wie folgt geändert:

   a) Die Überschrift wird wie folgt gefasst:

   „§ 100g

   Erhebung von Verkehrsdaten und Sicherungsanordnung“.

   b) Die Absätze 1 und 2 werden wie folgt gefasst:

   „(1) Verkehrsdaten (§§ 9 und 12 des Telekommunikation-Telemedien-Datenschutz-Gesetzes und § 2a Absatz 1 des BDBOS-Gesetzes) des Beschuldigten sowie von Personen, bei denen auf Grund 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, dürfen erhoben werden, wenn

   1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Absatz 2 bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat,

   2. die Erhebung der Verkehrsdaten für die Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist und

   3. die Erhebung der Verkehrsdaten in einem angemessenen Verhältnis zur Bedeutung der Sache steht.

   Die Erhebung gespeicherter (retrograder) Standortdaten ist abweichend von Satz 1 Nummer 1 und 2 nur zulässig, wenn

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in § 100a Absatz 2 bezeichnete Straftat, die auch im Einzelfall schwer wiegt, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat und

2. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

Im Übrigen ist die Erhebung von Standortdaten nur für künftig anfallende Verkehrsdaten oder in Echtzeit zulässig.

(2) Soweit die Straftat nicht von Absatz 1 erfasst wird, ist die Erhebung von Verkehrsdaten auch dann zur Erforschung des Sachverhalts zulässig, wenn

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine Straftat mittels Telekommunikation begangen hat, und

2. die Erforschung des Sachverhalts auf andere Weise aussichtslos wäre.

Satz 1 gilt nicht für die Erhebung von Standortdaten."

c) Absatz 3 wird wie folgt geändert:

aa) In Satz 1 Nummer 1 werden die Wörter „des Absatzes 1 Satz 1 Nummer 1" durch die Wörter „des Absatzes 1" ersetzt.

bb) Satz 2 wird aufgehoben.

d) Die Absätze 4 und 5 werden wie folgt gefasst:

„(4) Erfolgt die Erhebung von Verkehrsdaten nicht beim Erbringer öffentlich zugänglicher Telekommunikationsdienste, bestimmt sie sich nach Abschluss des Kommunikationsvorgangs nach den allgemeinen Vorschriften.

(5) Auch ohne das Wissen des Betroffenen darf angeordnet werden, dass die in § 175 Absatz 1 Satz 1 des Telekommunikationsgesetzes bezeichneten Anbieter öffentlich zugänglicher Telekommunikationsdienste die bei der Nutzung des Dienstes bereits erzeugten oder verarbeiteten sowie künftig anfallenden Verkehrsdaten unverzüglich zu sichern haben (Sicherungsanordnung), wenn zureichende tatsächliche Anhaltspunkte dafür vorliegen, dass eine in Absatz 1 bezeichnete Straftat begangen worden ist, und soweit die Verkehrsdaten für die Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes eines Beschuldigten von Bedeutung sein können. Die Erhebung der nach Satz 1 gesicherten Daten erfolgt nach den Absätzen 1 und 3."

3. In § 100j Absatz 2 Satz 1 werden nach den Wörtern „§ 174 Absatz 1 Satz 3" das Komma und die Wörter „§ 177 Absatz 1 Nummer 3" gestrichen.

4. § 100k Absatz 1 wird wie folgt gefasst:

„(1) Nutzungsdaten (§ 2 Absatz 2 Nummer 3 des Telekommunikation-Telemedien-Datenschutz-Gesetzes) dürfen von demjenigen, der geschäftsmäßig eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt, erhoben werden, wenn

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Absatz 2 bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat,

2. die Erhebung der Nutzungsdaten für die Erforschung des Sachverhalts erforderlich ist und

3. die Erhebung der Nutzungsdaten in einem angemessenen Verhältnis zur Bedeutung der Sache steht.

Die Erhebung gespeicherter (retrograder) Standortdaten ist abweichend von Satz 1 Nummer 1 und 2 nur unter den Voraussetzungen von § 100g Absatz 1 Satz 2 zulässig. Im Übrigen ist die Erhebung von Standortdaten nur für künftig anfallende Nutzungsdaten oder in Echtzeit zulässig, soweit sie für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist.“

5. § 101 wird wie folgt geändert:

a) In Absatz 1 werden nach der Angabe „100f,“ die Wörter „100g Absatz 5, den §§“ eingefügt:

b) In Absatz 2 Satz 1 wird nach der Angabe „100f,“ die Angabe „100g Absatz 5, §“ eingefügt.

c) In Absatz 4 Satz 1 Nummer 3 werden nach der Angabe „§ 100a“ die Wörter „und des § 100g Absatz 5“ eingefügt und wird das Wort „überwachten“ durch das Wort „betroffenen“ ersetzt.

6. § 101a wird wie folgt geändert:

a) Absatz 1 wird durch die folgenden Absätze 1 und 1a ersetzt:

„(1) Bei Erhebungen von Verkehrsdaten nach § 100g Absatz 1 bis 3 gelten § 100a Absatz 4 sowie § 100e Absatz 1, 3, 4 und 5 Satz 1 und 2 entsprechend mit der Maßgabe, dass

1. in der Entscheidungsformel nach § 100e Absatz 3 Satz 2 auch die zu übermittelnden Daten und der Zeitraum, für den sie übermittelt werden sollen, eindeutig anzugeben sind,

2. bei Funkzellenabfragen nach § 100g Absatz 3 abweichend von § 100e Absatz 3 Satz 2 Nummer 5 eine räumlich und zeitlich eng begrenzte und hinreichend bestimmte Bezeichnung der Telekommunikation genügt.

(1a) Bei Sicherungsanordnungen gelten § 100a Absatz 4 und § 100e Absatz 1, 3, 4 und 5 Satz 1 und 2 entsprechend mit der Maßgabe, dass

1. abweichend von § 100e Absatz 1 Satz 4 und 5 die Sicherungsanordnung auf höchstens einen Monat zu befristen ist; eine höchstens zweimalige Verlängerung der Sicherungsanordnung um jeweils nicht mehr als einen Monat ist zulässig, soweit deren Voraussetzungen fortbestehen,

2. in der Entscheidungsformel nach § 100e Absatz 3 Satz 2 auch die zu sichernden Daten eindeutig anzugeben sind.“

b) Der bisherige Absatz 1a wird Absatz 1b.

c) In Absatz 2 wird die Angabe „§ 100g“ durch die Wörter „nach § 100g Absatz 1 bis 3“ ersetzt.

d) Absatz 3 wird wie folgt geändert:

aa) In Satz 1 wird die Angabe „§ 100g“ durch die Wörter „§ 100g Absatz 1 bis 3“ ersetzt.

bb) Die Sätze 2 und 3 werden aufgehoben.

e) Die Absätze 4 und 5 werden aufgehoben.

f) Absatz 6 wird Absatz 4 und in Satz 1 wird die Angabe „§ 100g“ durch die Wörter „§ 100g Absatz 1 bis 3“ ersetzt.

g) Absatz 7 wird Absatz 5.

7. § 101b Absatz 5 wird wie folgt geändert:

a) In Nummer 1 werden die Wörter „§ 100g Absatz 1, 2 und 3“ durch die Wörter „§ 100g Absatz 1 bis 3 und 5“ ersetzt.

b) Nummer 2 wird wie folgt geändert:

aa) Nach Buchstabe c wird folgender Buchstabe d eingefügt:

„d) die Anzahl der Anordnungen nach § 100g Absatz 5;“.

bb) Die bisherigen Buchstaben d und e werden die Buchstaben e und f.

8. In § 160a Absatz 5 wird nach der Angabe „97“ das Komma durch das Wort „und“ ersetzt und werden die Wörter „und § 100g Absatz 4“ gestrichen.

Artikel 2

Änderung des Einführungsgesetzes zur Strafprozessordnung

§ 12 des Einführungsgesetzes zur Strafprozeßordnung in der im Bundesgesetzblatt Teil III, Gliederungsnummer 312-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 6b des Gesetzes vom 16. September 2022 (BGBl. I S. 1454) geändert worden ist, wird wie folgt gefasst:

„§ 12

Übergangsregelung zum Gesetz zur Einführung einer Sicherungsanordnung von Verkehrsdaten in der Strafprozessordung

Übersichten nach § 101b Absatz 5 der Strafprozessordnung in der vom … [einsetzen: Datum des Inkrafttretens nach Artikel 11 dieses Gesetzes] an geltenden Fassung sind erstmalig für das auf den … [einsetzen: Datum des Inkrafttretens nach Artikel 11 dieses Geset-

zes] folgende Berichtsjahr zu erstellen. Für die vorangehenden Berichtsjahre ist § 101b Absatz 5 der Strafprozessordnung in der bis einschließlich … [einsetzen: Datum des Tages vor dem Inkrafttreten nach Artikel 11 dieses Gesetzes] geltenden Fassung anzuwenden."

Artikel 3

Änderung des Bundespolizeigesetzes

In § 22a Absatz 3 des Bundespolizeigesetzes vom 19. Oktober 1994 (BGBl. I S. 2978, 2979), das zuletzt durch Artikel 8 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982) geändert worden ist, werden in dem Satzteil vor Nummer 1 nach den Wörtern „§ 174 Absatz 1 Satz 3" das Komma und die Wörter „§ 177 Absatz 1 Nummer 3" gestrichen.

Artikel 4

Änderung des BSI-Gesetzes

In § 5c Absatz 2 Satz 1 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982) geändert worden ist, werden nach den Wörtern „174 Absatz 1 Satz 3" das Komma und die Wörter „§ 177 Absatz 1 Nummer 3" gestrichen.

Artikel 5

Änderung des Bundeskriminalamtgesetzes

In § 10 Absatz 3 Satz 1 des Bundeskriminalamtgesetzes vom 1. Juni 2017 (BGBl. I S. 1354; 2019 I S. 400), das zuletzt durch Artikel 2 des Gesetzes vom 21. Juli 2022 (BGBl. I S. 1182) geändert worden ist, werden nach den Wörtern „174 Absatz 1 Satz 3" das Komma und die Wörter „§ 177 Absatz 1 Nummer 3" gestrichen.

Artikel 6

Änderung des Justizvergütungs- und -entschädigungsgesetzes

Das Justizvergütungs- und -entschädigungsgesetz vom 5. Mai 2004 (BGBl. I S. 718, 776), das zuletzt durch Artikel 17 des Gesetzes vom 25. Juni 2021 (BGBl. I S. 2154) geändert worden ist, wird wie folgt geändert:

1. In § 23 Absatz 1 werden nach dem Wort „Telekommunikation" die Wörter „oder Sicherungsanordnungen" eingefügt.

2. Anlage 3 wird wie folgt geändert:

a) In Absatz 2 der Allgemeinen Vorbemerkung werden die Wörter „300 bis 321 und 400 bis 402“ durch die Wörter „300 bis 312, nach den Abschnitten 4 bis 6 sowie nach Nummer 700“ ersetzt.

b) Nummer 202 wird aufgehoben.

c) Die Abschnitte 3 und 4 werden durch die folgenden Abschnitte 3 bis 7 ersetzt:

Nr.	Tätigkeit	Höhe
	„Abschnitt 3	
	Auskünfte über Verkehrsdaten ohne vorhergehende Sicherungsanordnung	
300	Auskunft über gespeicherte Verkehrsdaten: für jede Kennung, die der Auskunftserteilung zugrunde liegt.....	30,00 €
	Die Mitteilung der die Kennung betreffenden Standortdaten ist mit abgegolten.	
301	Die Auskunft wird im Fall der Nummer 300 aufgrund eines einheitlichen Ersuchens auch oder ausschließlich für künftig anfallende Verkehrsdaten zu bestimmten Zeitpunkten erteilt: für die zweite und jede weitere in dem Ersuchen verlangte Teilauskunft	10,00 €
302	Auskunft über gespeicherte Verkehrsdaten zu Verbindungen, die zu einer bestimmten Zieladresse hergestellt wurden, durch Suche in allen Datensätzen der abgehenden Verbindungen eines Betreibers: je Zieladresse	90,00 €
	Die Mitteilung der Standortdaten der Zieladresse ist mit abgegolten.	
303	Die Auskunft wird im Fall der Nummer 302 aufgrund eines einheitlichen Ersuchens auch oder ausschließlich für künftig anfallende Verkehrsdaten zu bestimmten Zeitpunkten erteilt: für die zweite und jede weitere in dem Ersuchen verlangte Teilauskunft	70,00 €
304	Auskunft über gespeicherte Verkehrsdaten für eine von der Strafverfolgungsbehörde benannte Funkzelle	30,00 €
305	Auskunft über gespeicherte Verkehrsdaten für mehr als eine von der Strafverfolgungsbehörde benannte Funkzelle: Die Pauschale 304 erhöht sich für jede weitere Funkzelle um	4,00 €
306	Auskunft über gespeicherte Verkehrsdaten in Fällen, in denen lediglich Ort und Zeitraum bekannt sind: Die Abfrage erfolgt für einen bestimmten, durch eine Adresse bezeichneten Standort.	60,00 €
	Die Auskunft erfolgt für eine Fläche:	
307	Die Entfernung der am weitesten voneinander entfernten Punkte beträgt nicht mehr als 10 Kilometer: Die Pauschale 306 beträgt	190,00 €
308	Die Entfernung der am weitesten voneinander entfernten Punkte beträgt mehr als 10, aber nicht mehr als 25 Kilometer: Die Pauschale 306 beträgt	490,00 €
309	Die Entfernung der am weitesten voneinander entfernten Punkte beträgt mehr als 25, aber nicht mehr als 45 Kilometer: Die Pauschale 306 beträgt	930,00 €
	Liegen die am weitesten voneinander entfernten Punkte mehr als 45 Kilometer auseinander, ist für den darüber hinausgehenden Abstand die Entschädigung nach den Nummern 307 bis 309 gesondert zu berechnen.	
310	Die Auskunft erfolgt für eine bestimmte Wegstrecke: Die Pauschale 306 beträgt für jeweils angefangene 10 Kilometer Länge.....	110,00 €
311	Umsetzung einer Anordnung zur Übermittlung künftig anfallender Verkehrsdaten in Echtzeit: je Anschluss	100,00 €
	Mit der Entschädigung ist auch der Aufwand für die Abschaltung der Übermittlung und die Mitteilung der den Anschluss betreffenden Standortdaten entgolten.	
312	Verlängerung der Maßnahme im Fall der Nummer 311	35,00 €

	Leitungskosten für die Übermittlung der Verkehrsdaten in den Fällen der Nummern 311 und 312:	
313	– wenn die angeordnete Übermittlung nicht länger als eine Woche dauert	8,00 €
314	– wenn die angeordnete Übermittlung länger als eine Woche, aber nicht länger als zwei Wochen dauert	14,00 €
315	– wenn die angeordnete Übermittlung länger als zwei Wochen dauert: je angefangenem Monat	25,00 €
316	Übermittlung der Verkehrsdaten auf einem Datenträger	10,00 €

Abschnitt 4

Sonstige Auskünfte ohne vorhergehende Sicherungsanordnung

400	Auskunft über den letzten dem Netz bekannten Standort eines Mobiltelefons	90,00 €
401	Auskunft über die Struktur von Funkzellen: je Funkzelle	35,00 €

Abschnitt 5

Sicherungsanordnung für Verkehrsdaten

500	Sicherung von Verkehrsdaten: für jede Kennung, die der Sicherungsanordnung zugrunde liegt	30,00 €
	Die Sicherung der die Kennung betreffenden Standortdaten ist mit abgegolten.	
501	Sicherung von Verkehrsdaten zu Verbindungen, die zu einer bestimmten Zieladresse hergestellt wurden, durch Suche in allen Datensätzen der abgehenden Verbindungen eines Betreibers: je Zieladresse	90,00 €
	Die Sicherung der Standortdaten der Zieladresse ist mit abgegolten.	
502	Sicherung von Verkehrsdaten für eine von der Strafverfolgungsbehörde benannte Funkzelle	30,00 €
503	Sicherung von Verkehrsdaten für mehr als eine von der Strafverfolgungsbehörde benannte Funkzelle: Die Pauschale 502 erhöht sich für jede weitere Funkzelle um	4,00 €
504	Sicherung von Verkehrsdaten in Fällen, in denen lediglich Ort und Zeitraum bekannt sind: Die Sicherung erfolgt für einen bestimmten, durch eine Adresse bezeichneten Standort	60,00 €
	Die Sicherung erfolgt für eine Fläche:	
505	Die Entfernung der am weitesten voneinander entfernten Punkte beträgt nicht mehr als 10 Kilometer: Die Entschädigung nach Nummer 504 beträgt	190,00 €
506	Die Entfernung der am weitesten voneinander entfernten Punkte beträgt mehr als 10 und nicht mehr als 25 Kilometer: Die Entschädigung nach Nummer 504 beträgt	490,00 €
507	Die Entfernung der am weitesten voneinander entfernten Punkte beträgt mehr als 25, aber nicht mehr als 45 Kilometer: Die Entschädigung nach Nummer 504 beträgt	930,00 €
	Liegen die am weitesten voneinander entfernten Punkte mehr als 45 Kilometer auseinander, ist für den darüber hinausgehenden Abstand die Entschädigung nach den Nummern 505 bis 507 gesondert zu berechnen.	
508	Die Sicherung erfolgt für eine bestimmte Wegstrecke: Die Entschädigung nach Nummer 504 beträgt für jeweils angefangene 10 Kilometer Länge	110,00 €
509	Verlängerung der Speicherung gesicherter Daten für jeden der in den Nummern 500 bis 502 und 504 bis 508 genannten Fällen	20,00 €
	Die Entschädigung wird nicht neben einer Entschädigung nach den Nummern 500 bis 508 gewährt, wenn die Verlängerung der Speicherung denselben Fall betrifft.	

	Abschnitt 6	
	Sonstige Sicherung	
600	Sicherung des letzten dem Netz bekannten Standortes eines Mobiltelefons	90,00 €
	Abschnitt 7	
	Auskünfte nach vorhergehender Sicherungsanordnung	
700	Auskunft über Daten, soweit eine nach Abschnitt 5 oder Abschnitt 6 zu entschädigende Sicherungsanordnung vorausgegangen ist: je Auskunftsersuchen	20,00 €
701	Übermittlung der Verkehrsdaten auf einem Datenträger	10,00 €“.

Artikel 7

Änderung des Zollfahndungsdienstgesetzes

Das Zollfahndungsdienstgesetz vom 30. März 2021 (BGBl. I S. 402), das zuletzt durch Artikel 6 Absatz 1 des Gesetzes vom 5. Juli 2021 (BGBl. I S. 2274) geändert worden ist, wird wie folgt geändert:

1. In § 10 Absatz 3 Satz 1 werden nach den Wörtern „§ 174 Absatz 1 Satz 3“ das Komma und die Wörter „§ 177 Absatz 1 Nummer 3“ gestrichen.

2. In § 30 Absatz 4 Satz 1 werden nach den Wörtern „§ 174 Absatz 1 Satz 3“ das Komma und die Wörter „§ 177 Absatz 1 Nummer 3“ gestrichen.

Artikel 8

Änderung des Telekommunikationsgesetzes

Das Telekommunikationsgesetz vom 23. Juni 2021 (BGBl. I S. 1858), das zuletzt durch Artikel 9 des Gesetzes vom 20. Juli 2022 (BGBl. I S. 1166) geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht werden die Angaben zu den §§ 175 bis 181 wie folgt gefasst:

   „§ 175 Pflichten zur Speicherung von Verkehrsdaten aufgrund von Sicherungsanordnungen

   §§ 176 bis 181 (weggefallen)“.

2. § 175 wird wie folgt gefasst:

„§ 175

Pflichten zur Speicherung von Verkehrsdaten aufgrund von Sicherungsanordnungen

(1) Die Verpflichtung zur umgehenden Sicherung von Verkehrsdaten aufgrund von Sicherungsanordnungen nach § 100g Absatz 5 der Strafprozessordnung trifft sämtliche Anbieter öffentlich zugänglicher Telekommunikationsdienste für Endnutzer,

bei denen es sich nicht um nummernunabhängige interpersonelle Telekommunikationsdienste handelt. Die Speicherung der Verkehrsdaten hat so zu erfolgen, dass Ersuchen von Strafverfolgungsbehörden nach Übermittlung der Daten nach Absatz 2 unverzüglich nachgekommen werden kann.

(2) Die aufgrund von Sicherungsanordnungen nach § 100g Absatz 5 der Strafprozessordnung gespeicherten Verkehrsdaten dürfen an eine Strafverfolgungsbehörde übermittelt werden, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung verlangt, die ihr eine Erhebung dieser Verkehrsdaten zur Verfolgung von Straftaten erlaubt. Für andere Zwecke dürfen diese Verkehrsdaten, soweit sie allein aufgrund der Sicherungsanordnung nach § 100g Absatz 5 der Strafprozessordnung gespeichert wurden, von dem nach Absatz 1 Satz 1 Verpflichteten nicht verwendet werden.

(3) Der nach Absatz 1 Satz 1 Verpflichtete hat Verkehrsdaten, die aufgrund von Sicherungsanordnungen nach § 100g Absatz 5 der Strafprozessordnung gespeichert wurden, unverzüglich nach Ablauf der in der Sicherungsanordnung genannten Frist nach dem Stand der Technik irreversibel zu löschen oder die irreversible Löschung sicherzustellen. Die §§ 9 und 12 des Telekommunikation-Telemedien-Datenschutz-Gesetzes und § 19 des BDBOS-Gesetzes bleiben unberührt.“

3. Die §§ 176 bis 181 werden aufgehoben.

4. § 228 wird wie folgt geändert:

   a) Absatz 2 wird wie folgt geändert:

      aa) In Nummer 38 werden die Wörter „oder § 181 Satz 2“ gestrichen.

      bb) In Nummer 39 werden die Wörter „oder § 175 Absatz 1 Satz 2 Nummer 2“ gestrichen.

      cc) Die Nummern 57 und 58 werden wie folgt gefasst:

         „57. entgegen § 175 Absatz 2 dort genannte Daten für andere als die dort genannten Zwecke verwendet,

         58. entgegen § 175 Absatz 3 Daten nicht rechtzeitig löscht oder die Löschung nicht sicherstellt,“.

      dd) Die Nummern 59 und 60 werden aufgehoben.

      ee) Die Nummern 61 bis 68 werden die Nummern 59 bis 66.

   b) Absatz 7 wird wie folgt geändert:

      aa) In Nummer 2 werden die Wörter „und 57 bis 59“ durch ein Komma und die Angabe „57 und 58“ ersetzt.

      bb) In Nummer 3 wird die Angabe „50, 53 und 60“ durch die Angabe „50 und 53“ ersetzt.

      cc) In Nummer 4 werden die Wörter „61, 63 bis 66 und 68“ durch die Wörter „59, 61 bis 64 und 66“ ersetzt.

Artikel 9

Änderung der Telekommunikations-Überwachungsverordnung

Die Telekommunikations-Überwachungsverordnung in der Fassung der Bekanntmachung vom 11. Juli 2017 (BGBl. I S. 2316), die zuletzt durch Artikel 6 Absatz 3 des Gesetzes vom 5. Juli 2021 (BGBl. I S. 2274) geändert worden ist, wird wie folgt geändert:

1. § 2 wird wie folgt geändert:

   a) In Nummer 1 Buchstabe b werden die Wörter „nach § 100g in Verbindung mit § 101a Absatz 1 der Strafprozessordnung“ durch die Wörter „nach § 100g Absatz 1 bis 3 in Verbindung mit § 101a Absatz 1 der Strafprozessordnung“ ersetzt.

   b) Nummer 3 Buchstabe b wird wie folgt neu gefasst:

      „b) im Sinne des Teils 4 die Stelle, die nach § 101a in Verbindung mit § 100a Absatz 4 Satz 1 der Strafprozessordnung, § 8a Absatz 1 Satz 1 Nummer 4 des Bundesverfassungsschutzgesetzes, auch in Verbindung mit § 4a des MAD-Gesetzes oder § 3 des BND-Gesetzes, § 52 des Bundeskriminalamtgesetzes, § 77 des Zollfahndungsdienstgesetzes oder nach Landesrecht auf Grund der jeweiligen Anordnung berechtigt ist, Auskunftsverlangen über nach den §§ 9 und 12 des Telekommunikation-Telemedien-Datenschutz-Gesetzes erhobene Verkehrsdaten zu stellen;“.

2. In § 35 Satz 3 Nummer 4 wird die Angabe „§ 176“ durch die Angabe „§ 175“ ersetzt.

[Artikel …]

[Änderung des Telekommunikation-Telemedien-Datenschutz-Gesetzes]

[Die Aufhebung der Regelungen zur Vorratsdatenspeicherung führt auch zur Aufhebung der §§ 176 bis 181 TKG. Für das Instrument der Sicherungsanordnung, welches ebenfalls zu Speicherverpflichtungen führt, auch wenn diese anlassbezogen, im Einzelfall und in deutlich geringerem Umfang erfolgen, dürften jedoch – neben den allgemeinen Regelungen – ebenfalls konkretisierende Regelungen zu Datenschutz und Datensicherheit erforderlich sein. Das Telekommunikationsrecht liegt federführend beim BMDV. Die Erarbeitung entsprechender Vorschriften im Einzelnen soll daher im Rahmen der Ressortabstimmung erfolgen.

Ferner soll in diesem Rahmen erörtert werden, ob die bisherige Rechtsgrundlage für die Übermittlung von Verkehrsdaten an die Strafverfolgungsbehörden nach § 100g Absatz 1 bis 3 StPO-E in § 101a Absatz 1 StPO-E i.V.m. § 100a Absatz 4 StPO sowie § 9 Absatz 1 Satz 4 TTDSG aus Gründen der Normenklarheit und Rechtssicherheit neu geregelt werden sollte.

Für beides erscheint das TTDSG der geeignete Regelungsort zu sein.]

Artikel 10

Einschränkung eines Grundrechts

Durch die Artikel 1 und 8 wird das Fernmeldegeheimnis (Artikel 10 Absatz 1 des Grundgesetzes) eingeschränkt.

Artikel 11

Inkrafttreten

Dieses Gesetz tritt am … [einsetzen: Datum des ersten Tages des auf die Verkündung folgenden Quartals] in Kraft.

Begründung

A. Allgemeiner Teil

I. Zielsetzung und Notwendigkeit der Regelungen

Mit dem Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherpflicht für Verkehrsdaten vom 10. Dezember 2015 (BGBl. I S. 2218) wurde eine Regelung zur zeitlich befristeten Speicherung von Verkehrsdaten zu Strafverfolgungszwecken (wieder)eingeführt. Kern dieser Reform war die sogenannte Vorratsdatenspeicherung, das heißt die Verpflichtung von Telekommunikationsdienste-Anbietern, sämtliche Verkehrsdaten mit Ausnahme der E-Mail-Daten aller Nutzer außer denen anonymer Hilfsangebote anlasslos für eine bestimmte Zeit zu speichern, §§ 113a bis 113g des Telekommunikationsgesetzes (TKG). Diese Vorschriften wurden mittlerweile inhaltlich unverändert in die §§ 175 bis 181 TKG übernommen, und zwar mit dem Gesetz zur Umsetzung der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) und zur Modernisierung des Telekommunikationsrechts vom 23. Juni 2021 (Telekommunikationsmodernisierungsgesetz, BGBl. I S. 1858). Die Erhebung dieser Daten durch Strafverfolgungsbehörden wurde nach Maßgabe von § 100g Absatz 2 der Strafprozessordnung (StPO) nur zur Verfolgung von besonders schweren, enumerativ genannten Straftaten erlaubt.

Dabei handelte es sich bereits um den zweiten Anlauf des Gesetzgebers, das Ermittlungsinstrument der „Vorratsdatenspeicherung“ rechtssicher einzuführen. Schon zuvor war mit dem Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 (BGBl. I S.3198) eine unterschiedslose, umfassende und anlasslose Speicherung der Verkehrsdaten sowohl bei Telefonaten als auch bei der Internet-Nutzung eingeführt worden. Diese Reform hatte seinerzeit zum größten Massenklageverfahren in der Geschichte der Bundesrepublik Deutschland mit über 30 000 Beschwerdeführern geführt. Aufgrund dieser Verfassungsbeschwerden hatte das Bundesverfassungsgericht mit seinem Urteil vom 2. März 2010 (1 BvR 256/08) die damals geltenden §§ 113a und 113b TKG und auch § 100g Absatz 1 Satz 1 StPO, soweit danach Verkehrsdaten nach § 113a TKG erhoben werden durften, wegen Verstoßes gegen Artikel 10 Absatz 1 des Grundgesetzes (GG) für nichtig erklärt und damit die maßgebliche Regelung zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 aufgehoben.

Auch die aufgrund aktueller Ereignisse im Jahr 2015 neu und restriktiver gefasste Regelung der „Vorratsdatenspeicherung“ im TKG und in der StPO lief indes bisher weitgehend leer, nachdem das Oberverwaltungsgericht Nordrhein-Westfalen im Eilverfahren die Speicherpflicht gegenüber den zwei klagenden Telekommunikationsdienste-Anbietern einstweilig ausgesetzt hatte (Beschluss vom 22. Juni 2017, 13 B 238/17). Vor diesem Hintergrund verzichtete die Bundesnetzagentur bis zur endgültigen Klärung, ob die Vorschriften des deutschen Rechts europarechtskonform sind, auf jegliche Maßnahmen zur Durchsetzung der nach wie vor bestehenden Speicherpflicht gemäß § 115 TKG alter Fassung (nunmehr § 183 TKG). Das Bundesverwaltungsgericht hat mit Beschluss vom 25. September 2019 (6 C 12/18) den Gerichtshof der Europäischen Union (EuGH) mit der Sache befasst.

De facto wird somit seit über 12 Jahren in Deutschland keine „Vorratsdatenspeicherung“ mehr durchgeführt und in nennenswertem Umfang zu Strafverfolgungszwecken eingesetzt. Dieser Umstand hat rechtspolitisch immer wieder zu Kritik geführt, da digitale Kommunikation eine immer größere Bedeutung erlangt hat und in vielen Strafverfahren neben digitalen Spuren kaum weitere Ermittlungsansätze zur Verfügung stehen. Dem steht die Kritik an der

hohen Eingriffstiefe einer Speicherung von Daten aller Bürger gegenüber, die auch zu entsprechenden Verfassungsbeschwerden gegen die Neuregelung von 2015 geführt hat, über die das Bundesverfassungsgericht allerdings noch nicht entschieden hat.

Aus empirischer Sicht kann festgestellt werden, dass trotz fehlender Vorratsdatenspeicherung in einer Vielzahl von Verfahren Verkehrsdaten erhoben werden können; dabei muss allerdings berücksichtigt werden, dass Gerichte von Anfragen absehen könnten, wenn für sie auf der Hand liegt, dass die benötigten Daten schon zu alt sind. Ob und wie viele Fälle hätten aufgeklärt werden können, gäbe es die Vorratsdatenspeicherung, bleibt damit letztlich Spekulation. Gleichwohl ist festzuhalten, dass es den Strafverfolgungsbehörden ausweislich der Polizeilichen Kriminalstatistik (PKS) für das Jahr 2021 – auch ohne Anwendung der Vorschriften zur Vorratsdatenspeicherung – beispielsweise gelungen ist, 90,8 Prozent der bekannt gewordenen Fälle der Verbreitung kinderpornographischer Inhalte im Sinne von § 184b Absatz 1 Satz 1 StGB a.F. aufzuklären.

Mit Urteil vom 20. September 2022 – C-793/19 und C-794/19 – hat der EuGH nunmehr die Vorlagefragen des Bundesverwaltungsgerichts beantwortet und entschieden, dass die 2015 eingeführten Vorschriften des deutschen Rechts nicht mit dem Unionsrecht vereinbar sind. Gegenstand dieser Entscheidung ist die Auslegung von Artikel 15 Absatz 1 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. 2002, L 201, S. 37) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 (ABl. 2009, L 337, S. 11) geänderten Fassung (im Folgenden: Richtlinie 2002/58) im Licht der Artikel 6 (Recht auf Freiheit und Sicherheit), Artikel 7 (Achtung des Privat- und Familienlebens), Artikel 8 (Schutz personenbezogener Daten) und Artikel 11 (Freiheit der Meinungsäußerung) sowie von Artikel 52 Absatz 1 der Charta der Grundrechte der Europäischen Union (im Folgenden: GRCh) und von Artikel 4 Absatz 2 EUV. Hierzu führt der EuGH aus, dass die Richtlinie 2002/58 den Grundsatz des Verbots der Speicherung von sich auf Teilnehmer und Nutzer beziehenden Verkehrsdaten durch Dritte regele (Rz. 56). Artikel 15 Absatz 1 der Richtlinie 2002/58 sehe die Möglichkeit vor, die sich im Übrigen aus der Richtlinie ergebenden Rechte und Pflichten der Betreiber elektronischer Kommunikationsdienste zu bestimmten dem Gemeinwohl dienenden Zwecken zu beschränken (Rz. 57). Die Aufzählung der dort genannten Zwecke sei abschließend (Rz. 58). Allein die Speicherung der Verkehrsdaten als solche stelle – unabhängig davon, ob sie später verwendet werden oder nicht – einen Eingriff in die Grundrechte auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten, die in den Artikeln 7 und 8 der GRCh verankert sind, dar (Rz. 60). Aus der Gesamtheit dieser Daten könnten sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten gespeichert wurden, gezogen werden (Rz. 61), was in Abhängigkeit von Menge und Vielfalt der auf Vorrat gespeicherten Daten auch dazu führen könne, dass die Nutzer elektronischer Kommunikationsmittel von der Ausübung ihrer durch Artikel 11 GRCh gewährleisteten Freiheit der Meinungsäußerung abgehalten würden (Rz. 62). Diese Rechte der Bürgerinnen und Bürger könnten jedoch nach Artikel 52 Absatz 1 GRCh durch eine gesetzliche Regelung, die den Wesensgehalt dieser Rechte achtet und den Grundsatzes der Verhältnismäßigkeit wahrt, eingeschränkt werden (Rz. 63). Die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen müssten sich jedoch auf das absolut Notwendige beschränken (Rz. 67). Ob eine nationale Regelung zur Beschränkung der unter anderen in den Artikeln 5, 6 und 9 der Richtlinie 2002/58 vorgesehenen Rechte und Pflichten zu rechtfertigen sei, sei danach zu beurteilen, ob die verfolgte dem Gemeinwohl dienende Zielsetzung in einem angemessenen Verhältnis zur Schwere des Eingriffs steht (Rz. 68), wobei zwischen den in Artikel 15 Absatz 1 der Richtlinie 2002/58 genannten Zwecken eine Hierarchie besteht (Rz. 71).

Ausgehend von diesen Grundsätzen hat der EuGH ausgeführt, dass allein der bedeutendste Zweck, nämlich der Schutz der nationalen Sicherheit, eine allgemeine und unterschiedslose Vorratsdatenspeicherung aller Verkehrsdaten zu rechtfertigen vermag, wenn

sich der betreffende Mitgliedstaat einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit gegenübersieht (hierzu im Einzelnen auch Rz. 92), die Anordnung einer wirksamen gerichtlichen Kontrolle unterliegt und nur für einen auf das absolut Notwendige begrenzten Zeitraum ergeht (Rz. 72). Hinsichtlich des Ziels der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten, könne – im Einklang mit dem Grundsatz der Verhältnismäßigkeit – allein die Bekämpfung schwerer Kriminalität und die Verhütung ernster Bedrohungen der öffentlichen Sicherheit eine Speicherverpflichtung für Verkehrsdaten überhaupt rechtfertigen (Rz. 73). Eine allgemeine und unterschiedslose Vorratsdatenspeicherung von allen Verkehrsdaten komme jedoch zur Verwirklichung dieses Ziels nicht in Betracht (Rz. 75). Zum Zweck der Bekämpfung schwerer Kriminalität und der Verhütung ernster Bedrohungen der öffentlichen Sicherheit hält der EuGH für zulässig (Rz. 75): (1) eine zeitlich und sachlich auf das absolut Notwendige begrenzte, gezielte Vorratsspeicherung von Verkehrsdaten (hierzu im Einzelnen auch Rz. 104 ff.); (2) eine allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, für einen auf das absolut Notwendige begrenzten Zeitraum (hierzu im Einzelnen auch Rz. 100 ff.); (3) eine allgemeine und unterschiedslose Vorratsspeicherung der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten (hierzu im Einzelnen auch Rz. 97 ff.) sowie (4) Verpflichtung der Betreiber elektronischer Kommunikationsdienste mittels einer Entscheidung der zuständigen Behörde, die einer wirksamen gerichtlichen Kontrolle unterliegt, während eines festgelegten Zeitraums die ihnen zur Verfügung stehenden Verkehrsdaten umgehend zu sichern (hierzu im Einzelnen auch Rz. 104 und 114 ff.).

Die derzeitigen deutschen Vorschriften sähen eine Vorratsspeicherung von Verkehrs- und Standortdaten nahezu alle die Bevölkerung bildenden Personen vor, ohne dass diese sich auch nur mittelbar in einer Lage befänden, die Anlass zur Strafverfolgung geben könnte. Ebenso schreibe sie die anlasslose, flächendeckende und personell, zeitlich und geografisch undifferenzierte Vorratsspeicherung eines Großteils der Verkehrs- und Standortdaten vor (Rz. 83). Sie könnten daher nicht als gezielte Vorratsdatenspeicherung im Sinne der Rechtsprechung des EuGH angesehen werden (Rz. 84). Ferner würden auch die vorgesehenen kurzen Speicherfristen die Eingriffsintensität nicht durchgreifend mindern, da selbst die Speicherung einer begrenzten Menge von Verkehrs- oder Standortdaten oder die Speicherung dieser Daten über einen kurzen Zeitraum geeignet seien, sehr genaue Informationen über das Privatleben des Nutzers eines elektronischen Kommunikationsmittels zu liefern (Rz. 87 ff.). Dasselbe gelte auch für die strengen Regelung zum Schutz der gespeicherten Daten vor Missbrauch, da die Vorratsspeicherung dieser Daten und der Zugang zu ihnen unterschiedliche Eingriffe in die in den Artikeln 7 und 11 GRCh garantierten Grundrechte darstellen, die eine gesonderte Rechtfertigung nach Artikel 52 Absatz 1 GRCh erfordern (Rz. 91).

Zur Zulässigkeit der umgehenden Sicherung der von den Betreibern elektronischer Kommunikationsdienste verarbeiteten und gespeicherten Verkehrsdaten (Quick Freeze) führt der EuGH detailliert aus, dass diese möglich sei, wenn ein begründeter Verdacht bestehe, dass eine schwere Straftat begangen wurde (Rz. 114), also bereits in einem frühen Stadium der Ermittlungen (Rz. 120). Sie könne mittels einer Entscheidung der zuständigen Behörde, die einer wirksamen gerichtlichen Kontrolle unterliegen muss, angeordnet werden (Rz. 115) und müsse sich nicht auf Personen, die konkret im Verdacht stehen, eine schwere Straftat begangen oder die nationale Sicherheit beeinträchtigt zu haben, beschränken; sie könne sich unter Einhaltung der Grenzen des absolut Notwendigen, auf die Verkehrsdaten anderer Personen erstrecken, sofern diese Daten auf der Grundlage objektiver und nicht diskriminierender Kriterien zur Aufdeckung einer solchen Straftat oder einer solchen Beeinträchtigung der nationalen Sicherheit beitragen können. Dazu gehören die Daten des Opfers sowie seines sozialen oder beruflichen Umfelds (Rz. 117 ff.). Ferner müsse die Anordnung in einem angemessenen Verhältnis zum verfolgten Ziel stehen (Rz. 122). Den Strafverfolgungsbehörden dürfe zu den gespeicherten Daten nur zur Erfüllung des dem Gemeinwohl

dienenden Ziels gewährt werden, zu dem die Speicherung den Betreibern auferlegt wurde oder einem höherrangigen Ziel (Rz. 128).

Diese Entscheidung fügt sich in die bisherige Rechtsprechung des Gerichtshofs zum Themenkomplex der „Vorratsdatenspeicherung“ ein:

So hat der EuGH bereits mit Urteil vom 8. April 2014 („Digital Rights“, C-293/12 und C-594/12) die Richtlinie über die Vorratsdatenspeicherung 2006/24/EG vom 15. März 2006, welche Grundlage der ersten gesetzlichen Regelung der „Vorratsdatenspeicherung“ in Deutschland von 2007 gewesen ist, wegen Verstoßes gegen Artikel 7 (Achtung des Privat- und Familienlebens) und Artikel 8 (Schutz personenbezogener Daten) GRCh für ungültig erklärt.

Es folgte mit seinem Urteil vom 21. Dezember 2016 („Tele 2 Sverige“, C-203/15) eine Grundsatzentscheidung zur „Vorratsdatenspeicherung“, in welcher der Gerichtshof feststellte, dass eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Nutzer auch zur Bekämpfung schwerer Kriminalität nicht mit dem Unionsrecht vereinbar sei. Eine solche Regelung müsse sich nicht nur an dem in Artikel 7 GRCh gewährleisteten Grundrecht auf Achtung des Privatlebens sowie dem in Artikel 8 GRCh gewährleisteten Grundrecht auf Schutz personenbezogener Daten, sondern auch dem in Artikel 11 GRCh gewährleistete Grundrecht auf freie Meinungsäußerung messen lassen (Rz. 92). Ferner müsse nach Artikel 52 Absatz 1 GRCh jede Einschränkung der Ausübung der in der Charta anerkannten Rechte und Freiheiten gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürften Einschränkungen der Ausübung dieser Rechte und Freiheiten nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen (Rz. 94).

Diese Haltung präzisierte der EuGH in weiteren Vorlageverfahren. Er führte insbesondere in der Entscheidung vom 6. Oktober 2020 („La Quadrature du Net u.a.“, C-511/18, C-512/18 und C-520/18) aus, dass die Ziele der Bekämpfung schwerer Kriminalität, der Verhütung schwerer Beeinträchtigungen der öffentlichen Sicherheit in Anbetracht ihrer Bedeutung zwar keine anlass- und unterschiedslose, aber eine gezielte Vorratsspeicherung von Verkehrs- und Standortdaten rechtfertigen können (Rz. 141 f. und 146 f.). Die erforderliche Begrenzung einer solchen Vorratsdatenspeicherung könne insbesondere anhand der Kategorien betroffener Personen vorgenommen werden. Auch könne die Speicherung auf ein geografisches Kriterium gestützt werden, wenn die zuständigen nationalen Behörden aufgrund objektiver und nicht diskriminierender Anhaltspunkte davon ausgehen, dass in einem oder mehreren geografischen Gebieten eine durch ein erhöhtes Risiko der Vorbereitung oder Begehung schwerer Straftaten gekennzeichnete Situation bestehe (Rz. 147 ff.). Zudem müsse die Dauer der Speicherung auf das im Hinblick auf das verfolgte Ziel sowie die sie rechtfertigenden Umstände absolut Notwendige beschränkt werden, unbeschadet einer etwaigen Verlängerung wegen des fortbestehenden Erfordernisses einer solchen Speicherung (Rz. 151). In dem Verfahren „Prokuratuur“ hat der Gerichtshof mit Urteil vom 2. März 2021 (C 746/18) ergänzend hervorgehoben, dass es unabdingbar sei, dass der Zugang der zuständigen nationalen Behörden zu den wegen einer Bedrohung für die nationale Sicherheit gespeicherten Daten einer vorherigen Kontrolle durch ein Gericht oder durch eine unabhängige Verwaltungsstelle unterworfen werde. In der Entscheidung vom 5. April 2022 („Commissioner of An Garda Siochana“, C-140/20) hat der EuGH schließlich seine Rechtsprechung erneut bekräftigt, zugleich aber – wie zum Teil schon in vorangegangen Urteilen – die Fälle präzisiert, in den das Unionsrecht Rechtsvorschriften zur Speicherung von Verkehrsdaten unter bestimmten Voraussetzungen erlaube, darunter auch das Instrument einer anlassbezogenen, umgehenden Sicherung von bereits vorhandenen Daten zur Bekämpfung schwerer Kriminalität, das mit diesem Gesetz eingeführt werden soll (ausführlich zu den diesbezüglichen Anforderungen des EuGH unter II.).

Als Ergebnis der Rechtsprechung des Gerichtshofs bleibt festzuhalten, dass der Versuch einer unionsrechtskonformen Ausgestaltung einer anlasslosen „Vorratsdatenspeicherung“ zu Strafverfolgungszwecken im nationalen Recht gescheitert ist; eine Neuauflage der allgemeinen und unterschiedslosen „Vorratsdatenspeicherung“ aller Verkehrsdaten ist aufgrund der höchstrichterlichen Vorgaben nicht möglich.

Zur effektiven Erlangung von digitalen Beweismitteln steht aber eine Alternative zur Verfügung. Der EuGH hat – wie bereits ausgeführt – mehrfach präzisiert, dass mit einer anlassbezogenen Sicherung von Verkehrsdaten, die einer wirksamen richterlichen Kontrolle unterliegt, ein grundrechtsschonenderes und effektives Ermittlungsinstrument vorhanden ist, welches einer unionsrechtskonformen Regelung im Strafverfahrensrecht zugänglich ist. Diese Vorgaben des Gerichtshofs zu einer unionsrechtskonformen, anlassbezogenen Verkehrsdatenspeicherung sollen mit diesem Gesetz umgesetzt werden.

II. Wesentlicher Inhalt des Entwurfs

Mit diesem Entwurf werden zum einen als zwingende Folge des Urteils des EuGH vom 20. September 2022 – C-793/19 und C-794/19 – die gegen das Unionsrecht verstoßenden und bislang faktisch ausgesetzten Regelungen der „Vorratsdatenspeicherung“ in § 100g Absatz 2 StPO und in den §§ 175 bis 181 TKG aufgehoben.

Zugleich wird in einem neu gefassten § 100g Absatz 5 StPO das Ermittlungsinstrument einer Sicherungsanordnung bereits vorhandener und künftig anfallender Verkehrsdaten eingeführt. Die Sicherung derartiger Verkehrsdaten soll anlassbezogen zur Verfolgung von erheblichen, insbesondere in § 100a Absatz 2 StPO bezeichneten (das heißt einer Telekommunikationsüberwachung zugänglichen) Straftaten zulässig sein, wenn sie für die Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsorts eines Beschuldigten von Bedeutung sein können. Die Maßnahme soll im Grundsatz nur auf Anordnung eines Richters zulässig sein. Nur ausnahmsweise in Fällen von Gefahr im Verzug soll eine staatsanwaltschaftliche Anordnung ausreichen, die indes binnen drei Werktagen einer richterlichen Bestätigung bedarf, um in Kraft zu bleiben.

Mit dieser Regelung wird die Menge der zu speichernden Daten auf das notwendige Maß begrenzt, da nur die bei den Anbietern von Telekommunikationsdiensten aus geschäftlichen Gründen ohnehin bereits vorhandenen und künftig anfallenden Verkehrsdaten gesichert werden dürfen („Einfrieren“). Ferner müssen die zu sichernden Daten im oben genannten Sinn für die weiteren Ermittlungen zumindest von Bedeutung sein können. Diese Daten stehen den Strafverfolgungsbehörden für eine begrenzte Zeit, nämlich nach der ersten Anordnung maximal für einen Monat, für eine spätere Erhebung und Auswertung zur Verfügung. Diese Erhebung bedarf freilich einer erneuten richterlichen Anordnung („Auftauen“). Erstrecken kann sich die Sicherungsanordnung – unter strengen Erhebungsvoraussetzungen sowie strenger Zweckbindung, die sich künftig aus § 175 Absatz 2 TKG-E ergibt – auf die Verkehrsdaten sowohl des Beschuldigten als auch von anderen Personen, wobei zu beachten ist, dass eine spätere Erhebung und Auswertung der gesicherten Verkehrsdaten nur für solche Personen in Betracht kommt, gegen die sich aufgrund der anderweitigen Ermittlungen ein konkreter Tatverdacht ergeben hat oder die als Nachrichtenmittler anzusehen sind.

Die vorgeschlagene Regelung – in Fachkreisen auch „Quick-Freeze-Regelung“ genannt – steht im Einklang mit den Anforderungen des Gerichtshofs:

So erkennt der EuGH in mittlerweile ständiger Rechtsprechung an, dass während der Verarbeitung und Speicherung von Verkehrs- und Standortdaten durch Betreiber elektronischer Kommunikationsdienste, die diese zu geschäftlichen Zwecken erhoben haben, Situationen auftreten können, die es erforderlich machten, die betreffenden Daten zur Aufklärung schwerer Straftaten (oder von Beeinträchtigungen der nationalen Sicherheit) über die

gesetzlichen Löschungsfristen hinaus zu speichern; dies gelte sowohl dann, wenn die Taten (oder Beeinträchtigungen) bereits festgestellt werden konnten, als auch dann, wenn nach einer objektiven Prüfung aller relevanten Umstände der begründete Verdacht bestehe, dass sie vorlägen (so erstmals: Urteil vom 6. Oktober 2020 „La Quadrature du Net u.a.“, C-511/18, C-512/18 und C-520/18, Rz.160 ff.; quasi wortgleich bekräftig in: Urteil vom 2. März 2021 „Prokuratuur“, C 746/18, Rz. 46 ff. und Urteil vom 5.April 2022 „Commissioner of An Garda Siochana“, C-140/20, Rz. 85 bis 88, jew. zitiert nach juris). Dies hat der EuGH auch in seinem Urteil vom 20. September 2022 – C-793/19 und C-794/19 – wiederholt (Rz. 114).

In einer solchen Situation, so der EuGH weiter (a.a.O.), stehe es den Mitgliedstaaten frei, in Rechtsvorschriften vorzusehen, dass den Betreibern elektronischer Kommunikationsdienste mittels einer Entscheidung der zuständigen Behörde, die einer wirksamen gerichtlichen Kontrolle unterliege, aufgegeben werde, für einen festgelegten Zeitraum die ihnen zur Verfügung stehenden Verkehrs- und Standortdaten umgehend zu sichern. Da die Zielsetzung einer solchen umgehenden Sicherung nicht mehr den Zielsetzungen entspreche, aufgrund deren die Daten ursprünglich gesammelt und gespeichert wurden, und da nach Artikel 8 Absatz 2 GRCh jede Datenverarbeitung für festgelegte Zwecke zu erfolgen habe, müssten die Mitgliedstaaten in ihren Rechtsvorschriften angeben, mit welcher Zielsetzung die umgehende Sicherung der Daten vorgenommen werden könne. Angesichts der Schwere des Eingriffs in die Grundrechte der Artikel 7 und 8 GRCh, der mit einer solchen Speicherung verbunden sein könne, seien nur die Bekämpfung schwerer Kriminalität (und, a fortiori, der Schutz der nationalen Sicherheit) geeignet, diesen Eingriff zu rechtfertigen. Um sicherzustellen, dass der mit einer derartigen Maßnahme verbundene Eingriff auf das absolut Notwendige beschränkt bleibe, dürfe sich die Speicherungspflicht zudem zum einen nur auf Verkehrs- und Standortdaten erstrecken, die zur Aufdeckung der schweren Straftat (oder der Beeinträchtigung der nationalen Sicherheit) beitragen könnten. Zum anderen müsse die Speicherungsdauer auf das absolut Notwendige beschränkt bleiben, könne allerdings verlängert werden, wenn die Umstände und das mit der fraglichen Maßnahme verfolgte Ziel es rechtfertigten.

Der Gerichtshof hat explizit hinzugefügt (a.a.O.), dass sich eine solche umgehende Sicherung nicht auf die Daten der Personen beschränken müsse, die konkret im Verdacht stünden, eine Straftat begangen (oder die nationale Sicherheit beeinträchtigt) zu haben (…). Eine solche Maßnahme können vielmehr nach Wahl des Gesetzgebers, unter Einhaltung der Grenzen des absolut Notwendigen, auf die Verkehrs- und Standortdaten anderer als der Personen erstreckt werden, die im Verdacht stehen, eine schwere Straftat (oder eine Beeinträchtigung der nationalen Sicherheit) geplant oder begangen zu haben, sofern diese Daten auf der Grundlage objektiver und nicht diskriminierender Kriterien zur Aufdeckung einer solchen Straftat (oder einer solchen Beeinträchtigung der nationalen Sicherheit) beitragen könnten. Dazu gehörten die Daten des Opfers, seines sozialen oder beruflichen Umfelds oder bestimmter geographischer Zonen, etwa der Orte, an denen die fragliche Straftat (oder Beeinträchtigung der nationalen Sicherheit) begangen oder vorbereitet worden sei.

Zuletzt hat der EuGH im Urteil 20. September 2022 – C-793/19 und C-794/19 – zur Frage des Adressatenkreises einer Sicherungsanordnung ausdrücklich ergänzt, dass es unter anderem um Personen gehen könne, mit denen ein Opfer vor (dem Auftreten einer schweren Bedrohung der öffentlichen Sicherheit oder) der Begehung einer schweren Straftat unter Verwendung seiner elektronischen Kommunikationsmittel in Kontakt gestanden habe (Rz. 118). Er hat weiter klargestellt (a.a.O. Rz. 119), dass Gegenstand der Sicherungsanordnung – unter den vorstehend genannten Voraussetzungen – auch die Verkehrs- und Standortdaten sein könnten, die sich auf den Ort bezögen, an dem eine Person, die möglicherweise Opfer einer schweren Straftat ist, verschwunden sei. Schließlich hat der Gerichtshof klargestellt, dass die zuständigen nationalen Behörden nicht daran gehindert seien, bereits im ersten Stadium der Ermittlungen bezüglich einer (schweren Bedrohung der öffentlichen Sicherheit oder einer) möglichen schweren Straftat, das heißt ab dem Zeitpunkt, zu dem diese Behörden nach den einschlägigen Bestimmungen des nationalen

Rechts solche Ermittlungen einleiten könnten, eine umgehende Sicherung anzuordnen (a.a.O. Rz. 120).

Jedenfalls aber müssen, so die Anforderung des EuGH (Urteil vom 6. Oktober 2020 „La Quadrature du Net u.a.“, C-511/18, C-512/18 und C-520/18, Rz. 168, zitiert nach juris), die Rechtsvorschriften, die eine derartige Datensicherung regeln, durch klare und präzise Regeln sicherstellen, dass bei der Speicherung der fraglichen Daten die für sie geltenden materiellen und prozeduralen Voraussetzungen eingehalten würden und dass die Betroffenen über wirksame Garantien zum Schutz vor Missbrauchsrisiken verfügten (so auch EuGH, Urteil vom 20. September 2022 – C-793/19 und C-794/19 –, Rz. 75).

Was den Zugang der zuständigen Behörden zu den gesicherten Daten angeht – das heißt das „Auftauen“ -, verweist der Gerichtshof (Urteil vom 6. Oktober 2020 „La Quadrature du Net u.a.“, C-511/18, C-512/18 und C-520/18, Rz. 165) im Übrigen auf die Voraussetzungen für nationale Datenerhebungsregelungen, die er bereits im grundlegenden Urteil vom 21. Dezember 2016 zur „Vorratsdatenspeicherung“ („Tele 2“, C-203/15 und C-698/15, Rz. 118 ff.) ausgeführt hat. Danach muss die betreffende – gegenüber der Sicherungsanordnung eigenständige – Befugnisnorm nicht nur die Zweckbindung der Erhebung enthalten („zur Bekämpfung schwerer Straftaten“), sondern muss auch die materiell- und verfahrensrechtlichen Voraussetzungen für den Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten festlegen. Bei der Festlegung dieser Vorrausetzungen müsse sich die betreffende Regelung zudem auf objektive Kriterien stützen; insoweit dürfe im Zusammenhang mit dem Zweck der Bekämpfung von Straftaten Zugang grundsätzlich nur zu den Daten von Personen gewährt werden, die im Verdacht stehen, eine schwere Straftat zu planen, zu begehen oder begangen zu haben oder auf irgendeine Weise in eine solche Straftat verwickelt zu sein. Damit in der Praxis die vollständige Einhaltung dieser Voraussetzungen gewährleistet sei, sei es unabdingbar, dass der Zugang der zuständigen nationalen Behörden zu den Daten grundsätzlich – außer in hinreichend begründeten Eilfällen – einer vorherigen Kontrolle entweder durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen werde (…). Außerdem sei es wichtig, dass die zuständigen nationalen Behörden, denen Zugang zu den Daten gewährt worden sei, die betroffenen Personen im Rahmen der einschlägigen nationalen Verfahren davon in Kenntnis setzten, sobald die Mitteilung die behördlichen Ermittlungen nicht mehr beeinträchtigen könne.

Darüber hinaus enthält auch das von Deutschland unterzeichnete und ratifizierte Übereinkommen des Europarats über Computerkriminalität, die sogenannte Budapest-Konvention, in Artikel 16 eine Verpflichtung der Vertragsstaaten, die zuständigen Behörden zu ermächtigen, die umgehende Sicherung von Verkehrsdaten anzuordnen. Personen, in deren Kontrolle sich solche Daten befinden, müssen verpflichtet werden können, diese kurzfristig und unversehrt zu sichern, um den zuständigen Behörden zu ermöglichen, deren Weitergabe zu erwirken (BGBl 2008 II S. 1242, vgl. Bundestagsdrucksache 16/5846). Auf diese Verpflichtung aus der Budapest-Konvention weist der EuGH in seiner Rechtsprechung zur Sicherungsanordnung ausdrücklich hin (Urteil vom 6. Oktober 2020 „La Quadrature du Net u.a.“, C-511/18, C-512/18 und C-520/18, Rz. 162, zitiert nach juris).

Bei der Sicherungsanordnung nach § 100g Absatz 5 StPO handelt sich nach alledem um eine neue Ausgestaltung der verpflichtenden Verkehrsdatenspeicherung, die einerseits den vom EuGH vorgegebenen Grundrechtsschutz der Nutzer von Telekommunikationsdiensten gewährleistet. Andererseits wird den Strafverfolgungsbehörden ein rechtssicheres und effektives Ermittlungsinstrument zur Bekämpfung schwerer Kriminalität im digitalen Raum an die Hand gegeben.

Die Einführung der Sicherungsanordnung nach § 100g Absatz 5 StPO-E trägt damit zur Verwirklichung von Ziel 16 „Friedliche und inklusive Gesellschaften für eine nachhaltige Entwicklung fördern, allen Menschen Zugang zur Justiz ermöglichen und leistungsfähige, rechenschaftspflichtige und inklusive Institutionen auf allen Ebenen aufbauen“ der Agenda

2030 für nachhaltige Entwicklung bei. Die vorgeschlagene Regelung ermöglicht eine effektive Bekämpfung schwerer Kriminalität, wie sie insbesondere von den Unterzielen 16.1, 16.2, 16.4 und 16.5 gefordert wird. Gleichzeitig gewährleisten die Ausgestaltung der neuen Regelung sowie die Aufhebung der Regelungen zur „Vorratsdatenspeicherung“ den von Unterziel 16.10 verlangten Schutz der Grundfreiheiten.

Die Folgeänderungen im TKG und in der Telekommunikations-Überwachungsverordnung (TKÜV) dienen dazu, auch die dortigen Vorschriften zur „Vorratsdatenspeicherung“ zu streichen und die aus der neuen Sicherungsanordnung folgenden Speicherungs-, Abfragungs-, Übermittelungs- und Löschungspflichten für die Telekommunikationsdienste-Anbieter zu regeln.

Neben weiteren Folgeänderungen im Bundespolizeigesetz (BPolG), BSI-Gesetz, Bundeskriminalamtgesetz (BKAG), Zollfahndungsdienstgesetz (ZFdG) und im Einführungsgesetz zur Strafprozessordnung (EGStPO) soll durch Änderungen im Anwendungsbereich des Justizvergütungs- und Entschädigungsgesetzes (JVEG) sichergestellt werden, dass die verpflichteten Unternehmen auch für ihren im Einzelfall im Rahmen der Sicherungsanordnung nach § 100g Absatz 5 StPO anfallenden Aufwand angemessen entschädigt werden.

III. Alternativen

Alternativ könnten die Regelungen zur „Vorratsdatenspeicherung“ ersatzlos gestrichen werden. Jedoch führt die Neuregelung gegenüber dem seit 12 Jahren unbefriedigenden Status quo zu verbesserten Ermittlungsmöglichkeiten, ohne durch eine anlasslose Speicherung der Daten aller Bürgerinnen und Bürger tief in deren Recht auf informationelle Selbstbestimmung einzugreifen. Ferner wird den Strafverfolgungsbehörden mit der Sicherungsanordnung ein Instrument an die Hand gegeben, dass es ihnen – zeitlich begrenzt – ermöglicht, zunächst weitere Ermittlungen durchzuführen, ohne hierdurch einen Verlust relevanter, aber flüchtiger Verkehrsdaten befürchten zu müssen.

IV. Gesetzgebungskompetenz

Die Gesetzgebungskompetenz des Bundes folgt aus Artikel 74 Absatz 1 Nummer 1 GG (gerichtliches Verfahren, betrifft Artikel 1, 2 und 6 dieses Gesetzes), aus Artikel 73 Absatz 1 Nummer 7 GG (Telekommunikation, betrifft Artikel 4, 8 und 9 dieses Gesetzes), aus Artikel 73 Absatz 1 Nummer 5 GG (Zollschutz, betrifft Artikel 7 dieses Gesetzes), aus Artikel 73 Absatz 1 Nummer 10 (Zusammenarbeit des Bundes und der Länder in der Kriminalpolizei, betrifft Artikel 5 dieses Gesetzes) sowie aus Artikel 87 Absatz 1 Satz 2 in Verbindung mit Artikel 73 Absatz 1 Nummer 5 GG (Grenzschutz, betrifft Artikel 3 dieses Gesetzes).

V. Vereinbarkeit mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen

Der Entwurf ist mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen, die die Bundesrepublik Deutschland abgeschlossen hat, vereinbar.

Insbesondere ist die Aufhebung der Regelungen der „Vorratsdatenspeicherung“ in § 100g Absatz 2 StPO und in den §§ 175 bis 181 TKG eine zwingende Folge des Urteils des EuGH vom 20. September 2022 – C-793/19 und C-794/19 –, der befunden hat, dass diese nationalen Vorschriften gegen das Unionsrecht verstoßen. Vor diesem Hintergrund ist die gesetzliche Bestimmung einer anlass- und unterschiedslosen sowie unbeschränkten Vorratsdatenspeicherung gescheitert und wird auch nicht erneut aufgegriffen. Die vorgeschlagene Regelung einer Sicherungsanordnung in § 100g Absatz 5 StPO-E steht hingegen im Einklang mit den diesbezüglichen Anforderungen des EuGH. Sie erfolgt anlassbezogen und

ist in sachlicher Hinsicht beschränkt. Darüber hinaus enthält auch das von Deutschland unterzeichnete und ratifizierte Übereinkommen des Europarats über Computerkriminalität, die sogenannte Budapest-Konvention, in Artikel 16 eine Verpflichtung der Vertragsstaaten, die zuständigen Behörden zu ermächtigen, die umgehende Sicherung von Verkehrsdaten anzuordnen.

VI. Gesetzesfolgen

1. Rechts- und Verwaltungsvereinfachung

Insbesondere der Wegfall der gesetzlichen Aufsichtspflichten im Rahmen der nunmehr aufgehobenen „Vorratsdatenspeicherung“ kann zu Rechts- und Verwaltungsvereinfachungen bei der Bundesnetzagentur führen.

2. Nachhaltigkeitsaspekte

Der Entwurf steht im Einklang mit den Leitgedanken der Bundesregierung zur nachhaltigen Entwicklung im Sinne der Deutschen Nachhaltigkeitsstrategie, die der Umsetzung der UN-Agenda 2030 für nachhaltige Entwicklung dient.

Die beabsichtigte Einführung der Sicherungsanordnung nach § 100g Absatz 5 StPO-E trägt zur Verwirklichung von Ziel 16 „Friedliche und inklusive Gesellschaften für eine nachhaltige Entwicklung fördern, allen Menschen Zugang zur Justiz ermöglichen und leistungsfähige, rechenschaftspflichtige und inklusive Institutionen auf allen Ebenen aufbauen“ der Agenda 2030 für nachhaltige Entwicklung bei. Denn mit Unterzielen 16.1, 16.2, 16.4 und 16.5 verlangt dieses Nachhaltigkeitsziel unter anderem, alle Formen der Gewalt und die gewaltbedingte Sterblichkeit überall deutlich zu verringern, alle Formen von Gewalt gegen Kinder zu beenden, alle Formen organisierter Kriminalität zu bekämpfen und Korruption und Bestechung erheblich zu reduzieren. Die Sicherungsanordnung nach § 100g Absatz 5 StPO-E leistet einen Beitrag zur Erreichung dieser Ziele, indem sie die Erfassung und Verwertung digitaler Spuren ermöglicht, die für die Strafverfolgung bisher nicht zugänglich waren.

Die Aufhebung der Regelungen zur „Vorratsdatenspeicherung“ sowie die Ausgestaltung der Regelungen zur Sicherungsanordnung nach § 100g Absatz 5 StPO-E gewährleisten zudem den von Unterziel 16.10 erfassten Schutz der Grundfreiheiten.

Somit trägt der Entwurf zur Gewährleistung einer funktionierenden Strafrechtspflege bei und fördert damit die Rechtsstaatlichkeit auf nationaler Ebene.

3. Haushaltsausgaben ohne Erfüllungsaufwand

Keine.

4. Erfüllungsaufwand

a) Erfüllungsaufwand für die Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger entsteht oder entfällt kein Erfüllungsaufwand.

b) Erfüllungsaufwand für die Wirtschaft

Für die betroffenen Telekommunikationsdienste-Anbieter entsteht durch die Einführung der Sicherungsanordnung ein gewisser Mehraufwand, dem aber eine erhebliche Entlastung infolge der Abschaffung der „Vorratsdatenspeicherung“ gegenübersteht.

Der zusätzliche Aufwand der Anbieter durch die Verpflichtung zur Umsetzung der Sicherungsanordnung nach § 100g Absatz 5 StPO und einer sich daran in der Regel anschließenden Auskunftserteilung nach § 100g Absatz 1 oder 3 StPO wird schon deshalb moderat ausfallen, weil sie für die Kosten für die Sicherung und Beauskunftung im Einzelfall nach § 23 JVEG-E entschädigt werden. Verbleibende übergeordnete Investitions- und gesteigerte Betriebskosten zur Umsetzung der Anforderungen aus § 175 TKG-E sind demgegenüber nicht belastbar abzuschätzen. Sie dürften aber ebenfalls vergleichsweise überschaubar ausfallen, da es lediglich um die notwendigen technischen Vorkehrungen für die Sicherung von Daten geht, die ohnehin bereits nach geltendem Recht zu geschäftlichen Zwecken gespeichert werden. Von quantifizierbaren und wesentlichen Auswirkungen auf die Verbraucherpreise für Telekommunikationsdienste als deren Folge ist nicht auszugehen.

Erheblichere Minderkosten für die Anbieter sind durch die Abschaffung der „Vorratsdatenspeicherung“ zu erwarten, mit der auch die strengen Pflichten für die Unternehmen aus den bislang geltenden §§ 175 bis 181 TKG aufgehoben werden – auch wenn dieser Mehraufwand wegen der faktischen Aussetzung der Speicherpflichten bei den meisten Anbietern in den letzten Jahren real nicht angefallen sein dürfte.

[*Diese Ausführungen stehen unter dem Vorbehalt des Ergebnisses der endgültigen Abstimmung mit dem BMDV sowie der Verbändebeteiligung zur Frage, ob und in welchem Umfang Datensicherheitsvorschriften erhalten bleiben müssen*]

[*Genaue Bezifferung – ggf. schätzungsweise – soll aufgrund des Ergebnisses der Verbändebeteiligung erfolgen*].

Im Übrigen entsteht für die Wirtschaft kein Erfüllungsaufwand.

c) Erfüllungsaufwand der Verwaltung

Auch für die Strafverfolgungsbehörden des Bundes und der Länder ist von einem gewissen Mehraufwand durch die Einführung der Sicherungsanordnung auszugehen, der aber vom Minderaufwand infolge der Abschaffung der „Vorratsdatenspeicherung“ kompensiert wird.

Durch die Einführung der Sicherungsanordnung wird es auf der einen Seite zu mehr Entschädigungszahlungen nach Maßgabe von § 23 in Verbindung mit den neuen Anlagen 5 bis 7 des JVEG kommen. Dieser Mehraufwand ist derzeit nicht verlässlich abschätzbar, da er davon abhängt, in welchem Umfang die Praxis von dem neuen Ermittlungsinstrument Gebrauch machen wird. Ein zusätzlicher Kontrollaufwand, ob die Telekommunikationsdienste-Anbieter die neuen Pflichten nach § 175 TKG-E einhalten, wird auch bei der Bundesnetzagentur anfallen. Hinzu kommt ein Mehraufwand bei der Anwendung der neuen Bußgeldtatbestände. Auf der anderen Seite ist von kostenrelevanten Effektivitätsgewinnen durch die Einführung der Anordnung nach § 100g Absatz 5 StPO auszugehen: Durch Sicherungsanordnungen kann die Anzahl von vormals erfolglosen Erhebungsanordnungen ohne vorherige Sicherung abnehmen. Durch die zu erwartenden Ermittlungserfolge können aufwendigere alternative Ermittlungsmaßnahmen vermieden werden. Auch diese Kostenersparnis lässt sich indes aus Ex-ante-Sicht der Höhe nach nicht verlässlich bestimmen.

Die Abschaffung der „Vorratsdatenspeicherung“ wird demgegenüber zu einem signifikanten Minderaufwand der Bundesnetzagentur führen, da ihre gesetzliche Verpflichtung aus § 180 TKG wegfällt, einen Anforderungskatalog bezüglich der Datensicherheit und der Datenqualität im Rahmen der Speicherung nach den §§ 175 bis 181 TKG zu erstellen, fortlaufend zu überprüfen und gegebenenfalls anzupassen. Es entfällt zudem der Kontrollaufwand im Rahmen der Aufsicht der Anbieter bei der „Vorratsdatenspeicherung“ sowie der Aufwand bei der Anwendung der alten Bußgeldtatbestände. Schließlich wird auch eine Ersparnis an Entschädigungszahlungen nach dem JVEG eintreten, da alle Kostennummern in dessen Anlage 3 mit diesem Gesetz aufgehoben werden, die sich auf die Erhebung von Daten aus der „Vorratsdatenspeicherung“ bezogen. Die genaue Höhe dieses Minderaufwands lässt

sich ebenfalls nicht genau beziffern, wobei auch hier zu beachten ist, dass ein Großteil des vorgenannten, nun de lege lata wegfallenden Aufwands faktisch seit 2017 wegen des globalen Aussetzens der Pflichten nach den §§ 175 bis 181 TKG nicht mehr entstanden sein dürfte.

[*Diese Ausführungen stehen unter dem Vorbehalt des Ergebnisses der endgültigen Abstimmung mit dem BMDV zur Frage, ob und in welchem Umfang Datensicherheitsvorschriften erhalten bleiben müssen*]

[*Genaue Bezifferung – ggf. schätzungsweise – soll aufgrund des Ergebnisses der Ressortabstimmung und der Länderbeteiligung erfolgen*]

5. Weitere Kosten

Von weiteren Kosten ist nicht auszugehen, insbesondere nicht von nennenswerten Mehrkosten im richterlichen Kernbereich.

Auswirkungen auf Einzelpreise und das allgemeine Preisniveau, insbesondere auf das Verbraucherpreisniveau für Telekommunikationsdienste, sind im Übrigen nicht zu erwarten.

6. Weitere Gesetzesfolgen

Die Regelungen sind inhaltlich geschlechtsneutral und betreffen alle Menschen ungeachtet ihrer sexuellen und geschlechtlichen Identität. Im Übrigen werden die Regelungen des Entwurfs keine Auswirkungen auf Verbraucherinnen und Verbraucher haben. Demografische Auswirkungen oder Auswirkungen auf die Gleichwertigkeit der Lebensverhältnisse in Deutschland sind ebenfalls nicht zu erwarten.

VII. Befristung; Evaluierung

Eine Befristung der vorgeschlagenen Gesetzesänderungen kommt nicht in Betracht. Sie betreffen den Kernbereich des Strafverfahrensrechts und des dazugehörigen Telekommunikationsrechts und sind auf Dauer angelegt.

Evaluierung [*ggf. nach genauer Bezifferung von Erfüllungsaufwand und Kosten, s.o.*].

B. Besonderer Teil

Zu Artikel 1 (Änderung der Strafprozessordnung)

Zu Nummer 1 (Inhaltsübersicht)

Das amtliche Inhaltsverzeichnis ist entsprechend der unter Nummer 2 Buchstabe a erfolgenden Änderung, die untenstehend erläutert wird, anzupassen.

Zu Nummer 2 (§ 100g)

Zu Buchstabe a

Zunächst soll die amtliche Überschrift von § 100g StPO-E um die neue Befugnis der Sicherungsanordnung von Verkehrsdaten ergänzt werden, die künftig in § 100g Absatz 5 StPO geregelt sein wird.

Zu Buchstabe b

Der Neufassung der Absätze 1 und 2 von § 100g StPO liegen die folgenden Erwägungen zugrunde:

Aufgehoben werden soll die bislang in § 100g Absatz 2 StPO geregelte Befugnis zur Erhebung der nach § 176 TKG a.F. anlasslos gespeicherten Verkehrsdaten einschließlich des dazugehörigen Straftatenkatalogs. Die Abschaffung dieser „Vorratsdatenspeicherung“ und des strafprozessualen Zugriffs darauf ist das zentrale Anliegen dieses Entwurfs.

Der Sache nach unverändert bleiben soll hingegen die bislang in § 100g Absatz 1 StPO vorgesehene Befugnis zur Erhebung von zu geschäftlichen Zwecken bei den Telekommunikationsdienste-Anbietern gespeicherten Verkehrsdaten, die aus verfassungsrechtlicher Sicht nicht zu beanstanden ist (vgl. BVerfG, Urteil vom 12. März 2003, 1 BvR 330/96, Rz. 78 ff.; Beschluss vom 17. Juni 2006, 2 BvR 1085/05, Rz. 16 ff., jeweils zitiert nach juris). Allerdings ist der derzeit geltende § 100g Absatz 1 StPO durch die Reformgesetzgebung der letzten Jahre redaktionell für den Rechtsanwender zunehmend unübersichtlich geworden. Dies gilt umso mehr, als durch die Einführung von § 100k StPO, der die Erhebung von Nutzungsdaten betrifft, im Jahr 2021 eine weitere Regelung geschaffen wurde, die sich auf ähnliche Sachverhalte bezieht, aber teilweise abweichend formuliert und aufgebaut wurde.

Der bisherigen Systematik folgend sollen die Verfahrensvorschriften zur Anordnung der Erhebung von Verkehrsdaten in § 101a StPO geregelt bleiben. Zur besseren Verständlichkeit der Vorschrift, wurden die Regelungen zu möglichen Betroffenen der Anordnung unmittelbar in Absatz 1 aufgenommen; eine inhaltliche Änderung ist damit nicht verbunden. Auch weiterhin kann sich die Erhebungsanordnung gegen den Beschuldigten sowie Personen richten, bei denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben (sogenannte Nachrichtenmittler) oder dass der Beschuldigte ihren Anschluss oder ihr informationstechnisches System benutzt.

In § 100g Absatz 1 StPO ist derzeit die Erhebung von Verkehrsdaten wegen des Verdachts von Straftaten von auch im Einzelfall erheblicher Bedeutung, insbesondere solchen, die in § 100a StPO bezeichnet sind, einerseits und von Verkehrsdaten wegen des Verdachts von mittels Telekommunikation begangener Straftaten andererseits im Ausgangspunkt zusammen geregelt (§ 100g Absatz 1 Satz 1 StPO der gegenwärtigen Fassung). Sie folgt aber unterschiedlichen Anordnungsvoraussetzungen und ermächtigt auch nicht zum Zugriff auf denselben Umfang von Verkehrsdaten, wie sich aus den Rückverweisen in § 100g Absatz 1 Satz 2 bis 4 StPO der gegenwärtigen Fassung ergibt.

Diese Systematik soll redaktionell deutlicher gefasst werden, indem die Befugnisse in zwei getrennten Absätzen geregelt werden, die künftig zudem eine übersichtlichere Nummerierung der jeweiligen Voraussetzungen für eine Anordnung enthalten sollen. Im neuen § 100g Absatz 1 Satz 1 StPO-E soll daher allein die Befugnis zur Erhebung von Verkehrsdaten wegen des Verdachts von Straftaten von erheblicher Bedeutung geregelt werden. Der neu gefasste § 100g Absatz 2 Satz 1 StPO-E soll hingegen die darüber hinaus gehende Befugnis zur Erhebung von Verkehrsdaten wegen des Verdachts von mittels Telekommunikation begangener Straftaten enthalten. Eine derartige Spezialregelung für diese Deliktsgruppe ist auch im Übereinkommen des Europarats über Computerkriminalität, der sogenannte Budapest-Konvention, vorgesehen (vgl. dort Artikel 14 Absatz 2 Buchstabe b). Dies betrifft weniger schwerwiegende als die in Absatz 1 genannten Straftaten. Daher verbindet die Norm die Befugnis mit einer höheren Schwelle der Verhältnismäßigkeit. Ebenfalls im Vergleich zu Absatz 1 restriktiver ist die Zweckbindung von § 100g Absatz 2 Satz 1 StPO-E, wonach eine Verkehrsdatenerhebung ausschließlich „zur Erforschung des Sachverhalts“ erlaubt ist. Diese Zweckbindung schließt implizit die Erhebung von Standortdaten aus. Gleichwohl soll dies durch Satz 2 noch einmal ausdrücklich klargestellt werden. Eine inhaltliche Änderung ist damit nicht verbunden.

Auch wenn durch die Aufhebung der Regelungen zur anlasslosen Vorratsdatenspeicherung retrograde Standortdaten nur noch dann vorhanden sein können, wenn diese seitens der Anbieter von Telekommunikationsdiensten aus geschäftlichen Gründen gespeichert werden, soll deren Erhebung nur unter strengen Voraussetzungen möglich sein. Hierzu bedarf es zukünftig eines Anfangsverdachts hinsichtlich einer der in § 100a Absatz 2 StPO bezeichneten Straftaten, der aber um eine hinreichend sichere Tatsachenbasis für das Vorliegen einer solchen Straftat erweitertes Beweismaterial erfordert („bestimmte Tatsachen", vgl. BeckOK-StPO/Bär, 44. Ed. 1. Juli 2022, StPO § 100g Rz. 6). Ein Anfangsverdacht hinsichtlich einer sonstigen Straftat von auch im Einzelfall erheblicher Bedeutung genügt hingegen nicht. Ferner muss ohne die Erhebung der Standortdaten, wie auch nach bisheriger Rechtslage, die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos sein und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache stehen. Nach Absatz 1 Satz 1 kommt nur die Erhebung von Standortdaten für künftig anfallende Verkehrsdaten oder in Echtzeit in Betracht, was durch Satz 3 klargestellt wird.

Zu Buchstabe c

Bei den Anpassungen in § 100g Absatz 3 StPO, der die Befugnis zur Funkzellenabfrage regelt, handelt es sich um Folgeänderungen zu den Änderungen unter Nummer 2 Buchstabe b. Insbesondere soll der Satz 2 von Absatz 4 infolge der Aufhebung der Regelungen zur „Vorratsdatenspeicherung" in § 100g Absatz 2 StPO a.F. und § 176 TKG seinerseits aufgehoben werden. Inhaltliche Änderungen des Satzes 1 von Absatz 3 sollen mit den Anpassungen nicht verbunden sein – die Verkehrsdatenerhebung im Rahmen einer Funkzellenabfrage soll unter denselben restriktiven Voraussetzungen zulässig bleiben wie bisher.

Zu Buchstabe d

Zu Absatz 4

Bisher enthielt der Absatz 4 von § 100g StPO eine Spezialvorschrift zum Schutz von Berufsgeheimnisträgern mit Zeugnisverweigerungsrecht im Rahmen der „Vorratsdatenspeicherung". Nach dieser Vorschrift ist die Anordnung einer Verkehrsdatenerhebung nach § 100g Absatz 2 StPO die sich gegen eine der in § 53 Absatz 1 Satz 1 Nummer 1 bis 5 genannten Personen richtet und die voraussichtlich Erkenntnisse erbringen würde, über die diese das Zeugnis verweigern dürfte, unzulässig. Mit der Aufhebung des bisherigen § 100g Absatz 2 StPO soll folgerichtig auch diese Regelung entfallen. Es handelt sich mithin um eine Folgeänderung zur Änderung unter Nummer 2 Buchstabe b. In der Sache bleibt der Schutz von zeugnisverweigerungsberechtigten Berufsgeheimnisträgern im Rahmen der von nun an in § 100g StPO geregelten Ermittlungsmaßnahmen unabhängig davon erhalten. Er wird bereits ausreichend von der allgemeinen Schutzvorschrift des § 160a StPO gewährleistet, welcher auch bisher für die Erhebung von Verkehrsdaten galt, die nicht aufgrund der Regelungen zur Vorratsdatenspeicherung erhoben wurden. Die Regelung in § 160a Absatz 1 Satz 1 StPO ist hinsichtlich der in § 53 Absatz 1 Satz 1 Nummer 1, 2 oder Nummer 4 StPO genannten Personen (unter anderen Geistliche und Verteidiger) sowie für Rechtsanwälte und Kammerbeistände mit dem bisher geltenden § 100g Absatz 4 Satz 1 StPO inhaltlich identisch. Gegen diesen Personenkreis werden Maßnahmen nach § 100g StPO-E auch künftig unzulässig sein. Dies gilt auch für das neue Ermittlungsinstrument der Sicherungsanordnung. Diese Regelung sieht somit für einen engen Kreis von auf besondere Vertraulichkeit angewiesenen Telekommunikationsverbindungen ein grundsätzliches Erhebungsverbot vor, insbesondere für Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen, die grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten (vgl. BVerfG, Urteil vom 2. März 2010 – 1 BvR 256/08, Rz. 238). Nach § 160a Absatz 2 Satz 1 StPO gilt für die übrigen in § 53 Absatz 1 Satz 1 StPO genannten zeugnisverweigerungsberechtigten Personen (unter anderen Ärzte, Angehörige der Bera-

tungsstellen nach dem Schwangerschaftskonfliktgesetz oder für Betäubungsmittelabhängigkeit und Journalisten), dass bei Maßnahmen, durch die voraussichtlich Erkenntnisse erlangt würden, über die diese Person das Zeugnis verweigern dürfte, dies im Rahmen der Prüfung der Verhältnismäßigkeit besonders zu berücksichtigen ist; betrifft das Verfahren keine Straftat von erheblicher Bedeutung, ist in der Regel nicht von einem Überwiegen des Strafverfolgungsinteresses auszugehen. Hierdurch wird der Schutz auch dieses Personenkreises weiterhin gewährleistet und sichergestellt, dass ihre Interessen bereits bei einer Anordnung nach § 100g Absatz 1 bis 3 und Absatz 5 StPO-E berücksichtigt werden. Bei diesem abgestuften Regelungssystem war zu berücksichtigen, dass es dem Gesetzgeber nach der Rechtsprechung des Bundesverfassungsgerichts nicht freisteht, der Presse- und Rundfunkfreiheit den absoluten Vorrang vor anderen wichtigen Rechtsgütern, wie etwa dem Gebot der Wahrheitserforschung im Strafprozess, einzuräumen (BVerfG, Beschluss vom 12. Oktober 2011 – 2 BvR 236/08 –, Rz. 268 – zitiert nach juris).

Im neu gefassten § 100g Absatz 4 StPO-E soll an die Stelle dieser Spezialvorschrift die Regelung über die Erhebung von Verkehrsdaten nach Abschluss des Kommunikationsvorgangs in anderer Weise als durch eine Auskunftsanordnung an den Erbringer öffentlich zugänglicher Telekommunikationsdienste treten. Diese ist bislang in § 100g Absatz 5 StPO enthalten und soll inhaltlich wie redaktionell unverändert in den Absatz 4 der Vorschrift „vorgezogen“ werden. Die Absätze 1 bis 4 von § 100g StPO-E regeln also künftig en bloc die Erhebung von Verkehrsdaten, die neue Befugnis der Sicherungsanordnung für Verkehrsdaten soll sich in Absatz 5 anschließen.

Zu Absatz 5

Im neuen Absatz 5 von § 100g StPO soll das Ermittlungsinstrument einer Sicherungsanordnung bereits vorhandener und künftig anfallender Verkehrsdaten geregelt werden. Damit soll einerseits die Einschränkung grundrechtlich geschützter Interessen im Einklang mit den Vorgaben des EuGH auf ein zur Sicherung der Belange der effektiven Strafverfolgung erforderliches Maß begrenzt werden. Andererseits soll den Bedürfnissen der Strafverfolgungsbehörden nach einer erweiterten Speicherung und Erhebung von Telekommunikationsverkehrsdaten auf angemessene und rechtssichere Weise Rechnung getragen werden.

Grammatikalisch spiegelbildlich zu den Absätzen 1 bis 3 von § 100g StPO-E soll der neue Absatz 5 im ersten Halbsatz die neue Befugnis zur Sicherung von Verkehrsdaten definieren sowie im zweiten Halbsatz die materiellen Voraussetzungen für deren Anordnung auflisten.

Halbsatz 1 verweist hinsichtlich der Verpflichteten auf § 175 Absatz 1 Satz 1 TKG-E. Damit können durch die Sicherungsanordnung sämtliche Anbieter öffentlich zugänglicher Telekommunikationsdienste für Endnutzer, bei denen es sich nicht um nummernunabhängige interpersonelle Telekommunikationsdienste (§ 3 Nummer 40 TKG) handelt, verpflichtet werden. Nicht erfasst sind damit Anbieter eines interpersonellen Telekommunikationsdienstes, der weder eine Verbindung zu öffentlich zugeteilten Nummerierungsressourcen, nämlich Nummern nationaler oder internationaler Nummernpläne, herstellt noch die Telekommunikation mit Nummern nationaler oder internationaler Nummernpläne ermöglicht. Dies schließt die Anwendung der Sicherungsanordnung auf Voice-over-IP- (VoIP-) oder Over-The-Top- (OTT-)Dienste nicht per se aus. VoIP- oder OTT-Dienste, die ihrerseits eine Verbindung in das oder aus dem öffentlichen Telefonnetz herstellen, unterliegen der Sicherungsanordnung.

Halbsatz 2 von §100g Absatz 5 StPO-E regelt die Voraussetzungen einer Sicherungsanordnung:

Die Sicherung von vorhandenen und künftig anfallenden Verkehrsdaten soll nur dann zulässig sein, wenn zureichende tatsächliche Anhaltspunkte dafür vorliegen, dass eine in § 100g Absatz 1 StPO bezeichnete Straftat begangen worden ist. Es handelt sich neben den Kapitaldelikten in erster Linie um bestimmte schwere Straftaten des Strafgesetzbuchs,

etwa solche der Gefährdung des demokratischen Rechtsstaates, Delikte gegen die sexuelle Selbstbestimmung und gegen die persönliche Freiheit sowie um bestimmte schwerwiegende Vermögensdelikte. Hinzu kommen bestimmte schwere Straftaten des Nebenstrafrechts, insbesondere solche der Abgabenordnung, des Betäubungsmittel- und Waffengesetzes. Diese Limitierung auf Straftaten, die auch im Einzelfall von erheblicher Bedeutung sein müssen, steht im Einklang mit den Anforderungen des EuGH, der die umgehende Sicherung von Verkehrsdaten explizit nur zur „Bekämpfung schwerer Kriminalität“ bzw. zur „Aufdeckung einer schweren Straftat“ erlaubt (siehe oben die Nachweise unter Abschnitt A Teil II des Begründungsteils). Nicht zulässig soll die Sicherungsanordnung hingegen beim bloßen Verdacht von mittels Telekommunikation begangenen Straftaten sein, deren Erhebung – ohne die Möglichkeit einer vorangehenden Sicherung – nunmehr in § 100g Absatz 2 StPO-E geregelt wird.

Dass zureichende tatsächliche Anhaltspunkte für die Begehung einer derartigen schweren Straftat vorliegen müssen, bedeutet, dass ein von konkreten Tatsachen gestützter Anfangsverdacht gegeben sein muss, der über vage Anhaltspunkte und Vermutungen hinausgeht (Schmitt, in: Meyer-Goßner/Schmitt, StPO, 65. Auflage 2022, § 98a Rz. 7, § 152 Rz. 4). Diese Eingriffsschwelle, die der der Rasterfahndung (§ 98a StPO) entspricht, ist im Vergleich zu der Regelung für die Erhebung („Auftauen“) der Verkehrsdaten nach § 100g Absatz 1 oder Absatz 3 StPO-E niedriger; gefordert wird zu diesem Zeitpunkt noch kein qualifizierter, sich gegen eine bestimmte Person richtender Tatverdacht (§ 100g Absatz 1: „Begründen bestimmte Tatsachen den Verdacht, dass jemand...“), wie er sich typischerweise erst im Laufe von weiteren Ermittlungen ergibt. Dieser Unterschied ist entscheidend: Die unverzügliche Sicherung von Verkehrsdaten kann unmittelbar nach Entdeckung der Begehung einer schweren Straftat angeordnet werden, auch wenn weitere Einzelheiten noch nicht feststehen, so dass es für die Strafverfolgungsbehörden möglich sein wird, die Löschung von Daten zu verhindern, die sich im weiteren Verlauf der Untersuchung als relevant erweisen. Auch dies steht im Einklang mit der Rechtsprechung des EuGH, der zuletzt noch einmal dezidiert klargestellt hat (siehe oben unter Abschnitt A Teil II des Begründungsteils), dass eine „Quick-Freeze“-Anordnung schon „im ersten Stadium der Ermittlungen bezüglich einer möglichen schweren Straftat“ zulässig sei. Von der gesetzlichen Formulierung „dass eine (…) Straftat begangen worden ist“ werden im Übrigen aufgrund von gefestigter Auslegung nicht nur vollendete Straftaten, sondern auch Fälle des strafbaren Tatversuchs sowie alle Formen der Täterschaft und Teilnahme erfasst (Meyer/Goßner-Schmitt, a.a.O., m.w.N.).

Nach § 100g Absatz 5 Satz 1 Halbsatz 2 StPO-E ist die Sicherungsanordnung von Verkehrsdaten darüber hinaus nur zulässig, wenn die betreffenden Verkehrsdaten für die Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes eines Beschuldigten von Bedeutung sein können.

Diese Zweckbindung der Sicherungsanordnung, die neben der Erforschung des Sachverhalts auch Belange der Aufenthaltsermittlung von Beschuldigten, das heißt auch Fahndungszwecke, umfasst, ist einerseits so weit gefasst, dass die Sicherungsanordnung im frühen Ermittlungsstadium, in dem typischerweise noch relativ wenig Ermittlungserkenntnisse vorliegen, einen effektiven Beitrag zur Arbeit der Strafverfolgungsbehörden leisten kann. Andererseits handelt es sich um eine Zweckbindung, die sicherstellt, dass keine Verkehrsdaten ins Blaue hinein gespeichert werden, sondern auch insoweit den Vorgaben des EuGH zur Gewährleistung eines effektiven Grundrechtsschutzes entsprochen wird – schließlich verlangt der EuGH, dass die Mitgliedstaaten ausdrücklich kodifizieren, mit welcher Zielsetzung die umgehende Sicherung der Daten vorgenommen werden könne; die auf das absolut Notwendige beschränkte Datensicherung müsse zudem auf Grundlage objektiver Kriterien zur Aufdeckung einer schweren Straftat beitragen können (siehe oben unter Abschnitt A Teil II des Begründungsteils). Zudem wird hierdurch verhindert, dass die Speicherung der Daten einen systematischen Charakter erhält.

Die Verkehrsdaten, die Gegenstand der Sicherungsanordnung sind, müssen schließlich für diese Ermittlungszwecke „von Bedeutung sein können." Um die Sicherungsanordnung effizient auszugestalten und sie gleichzeitig im Sinne der Verhältnismäßigkeit zu beschränken, soll also an die potentielle Beweisbedeutung der zu sichernden Verkehrsdaten angeknüpft werden. Dies folgt dem Beispiel der bestehenden Regelungen über die Sicherstellung und Beschlagnahme von Gegenständen zu Beweiszwecken in § 94 Absatz 1 StPO („die als Beweismittel für die Untersuchung von Bedeutung sein können") sowie über die Durchsicht von elektronischen Speichermedien in § 110 Absatz 3 StPO („Daten, die für die Untersuchung von Bedeutung sein können, dürfen gesichert werden."), die ebenfalls typischerweise in einem frühen Ermittlungsstadium angeordnet werden. Auf die insoweit gefestigte Auslegung zu diesen Begriffen soll künftig auch im Rahmen von § 100g Absatz 5 StPO-E zurückgegriffen werden. Danach reicht es aus, dass im Moment der Sicherungsanordnung die Möglichkeit besteht, dass die Verkehrsdaten für die Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes eines Beschuldigten verwendet werden können; als ausreichend wird insoweit die Erwartung im Sinne einer ex ante-Prognose angesehen, dass die Verkehrsdaten Schlussfolgerungen auf relevante Tatsachen zulassen; für welche Beweisführung sie im Einzelnen in Betracht kommen und ob sie später tatsächlich relevant werden, braucht hingegen noch nicht festzustehen. Ausgeschlossen wird die Sicherungsanordnung hingegen sein, wenn im Zeitpunkt der Anordnung die fehlende Beweisbedeutung schon sicher feststeht (vgl. zu alledem: Köhler, in Meyer-Goßner/Schmitt, StPO, 65. Auflage 2022, § 94 Rz. 6; Hauschild, in Münchener Kommentar zur StPO, 1. Auflage 2014, § 94 Rz. 21, jeweils m.w.N.). Dies ist etwa der Fall, wenn das Vorliegen eines Verfahrenshindernisses bereits sicher feststeht. Erfasst sein können aber bei der Sicherungsanordnung auch Fälle, in denen sicher absehbar ist, dass die Voraussetzungen einer späteren Erhebung der Verkehrsdaten nach § 100g Absatz 1 oder 3 StPO-E nicht vorliegen werden.

Liegen die Voraussetzungen von § 100g Absatz 5 Satz 1 Halbsatz 2 StPO-E vor, darf angeordnet werden, was im Halbsatz 1 der Norm als Legaldefinition der Sicherungsanordnung bestimmt ist: Danach darf auch ohne das Wissen des Betroffenen angeordnet werden, dass die in § 175 Absatz 1 Satz 1 des TKG bezeichneten Anbieter öffentlich zugänglicher Telekommunikationsdienste sämtliche bei der Nutzung des Dienstes bereits erzeugten oder verarbeiteten sowie künftig anfallenden Verkehrsdaten umgehend zu sichern haben.

Der Kreis der Verpflichteten der Sicherungsanordnung soll also aus sämtlichen Anbietern öffentlich zugänglicher Telekommunikationsdienste für Endnutzer bestehen, bei denen es sich, wie § 175 Absatz 1 Satz 1 TKG-E bestimmt, nicht um nummernunabhängige interpersonelle Telekommunikationsdienste handelt. Im Vergleich zum Kreis der Verpflichteten der nunmehr aufgehobenen „Vorratsdatenspeicherung" ergibt sich kein Unterschied.

Der Begriff der zu sichernden Verkehrsdaten ist derselbe wie bei der etablierten Verkehrsdatenerhebung des § 100g Absatz 1 StPO, der seinerseits auf die §§ 9 und 12 des TTDSG und § 2a Absatz 1 des Gesetzes über die Errichtung einer Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOSG) verweist. Es handelt sich also in erster Linie um die in § 9 Absatz 1 TTDSG genannten Verkehrsdaten, welche die Telekommunikationsdienste-Anbieter zu geschäftlichen Zwecken – namentlich zum Aufbau und zur Aufrechterhaltung der Telekommunikation, zur Entgeltabrechnung oder zum Aufbau weiterer Verbindungen – verarbeitet haben bzw. im Anordnungszeitraum nach Erlass der Sicherungsanordnung verarbeiten. Dazu gehören insbesondere die Nummer oder Kennung der beteiligten Anschlüsse, bei mobilen Anschlüssen auch die Standortdaten, der Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen. Der Umfang der zu sichernden Verkehrsdaten („Einfrieren") entspricht also dem der potentiell auch einer Erhebung („Auftauen") zugänglichen Verkehrsdaten. Die Sicherung sowie die Erhebung von Inhalten der Telekommunikation soll hingegen – nach wie vor – von § 100g StPO nicht erlaubt sein.

Ausgestaltet ist die Sicherungsanordnung als verdeckte Ermittlungsmaßnahme („ohne das Wissen des Betroffenen"), wobei im Falle der Erhebung und Auswertung (das heißt des

„Auftauens“) der gesicherten Daten nach § 100g Absatz 1 StPO die (nachträglichen) Benachrichtigungs- und Rechtsschutzmöglichkeiten nach Maßgabe von § 101a Absatz 4 StPO-E greifen. Aufgrund von § 101 Absatz 4 Satz 1 Nummer 3 StPO-E erfolgt eine Benachrichtigung der Betroffenen aber auch dann, wenn die nach § 100g Absatz 5 StPO-E gesicherten Daten später nicht erhoben werden. Diese betrifft allerdings nur die Personen, deren Identität bereits aufgedeckt wurde, die also im zugrundeliegenden Beschluss bereits benannt wurden. Es müssen keine Personen identifiziert bzw. zusätzliche Daten erhoben werden, nur um die Benachrichtigungspflicht zu erfüllen.

Bewusst weit soll in § 100g Absatz 5 StPO-E schließlich der Kreis der Personen gefasst sein, deren Verkehrsdaten von einer Sicherungsanordnung umfasst sein können („des Betroffenen“). Um die Sicherungsanordnung effizient auszugestalten, sollen nämlich nicht nur Verkehrsdaten von Tatverdächtigen oder von sogenannten Nachrichtenmittlern gesichert werden können, sondern – in den Grenzen der vorgenannten Zweckbindung – auch von anderen Personen.

Gerade im frühen Ermittlungsstadium ist es regelmäßig entscheidend für einen späteren Ermittlungserfolg, dass im Rahmen des Erforderlichen auch Daten von Dritten gesichert werden dürfen, die in einem persönlichen oder räumlichen Bezug zum Opfer bzw. Tatort stehen. Dieses Interesse hat ausdrücklich der EuGH anerkannt, der wiederholt betont hat, dass „nach Wahl des Gesetzgebers unter Einhaltung der Grenze des absolut Notwendigen auch eine Erstreckung auf die Verkehrs- und Standortdaten anderer Personen möglich“ sei. Dazu gehörten etwa „Daten des Opfers, seines sozialen oder beruflichen Umfelds oder bestimmter geografischer Zonen, etwa der Orte, an denen die fragliche Straftat begangen oder vorbereitet wurde“. Auch könne es um Personen gehen, mit denen das Opfer vor der Begehung einer schweren Straftat auf elektronischem Wege kommuniziert habe (siehe oben unter Abschnitt A Teil II des Begründungsteils). Diese Datensicherung auch von potentiell unbeteiligten Personen ist mit den Belangen des Grundrechtsschutzes vereinbar – gerade vor dem Hintergrund, dass es zu einer nachfolgenden Erhebung und Auswertung der Daten nach § 100g Absatz 1 StPO, das heißt einem vertieften Grundrechtseingriff, nur kommen kann, wenn sich im weiteren Ermittlungsverlauf konkretisiert, dass es sich bei diesen Personen um Beschuldigte oder Nachrichtenmittler handelt und diese Erhebung nach nochmaliger Prüfung eigens richterlich angeordnet wird.

Die Sicherungsanordnung nach § 100g Absatz 5 StPO-E kann für die Praxis auch einen Zeitgewinn für die Auswertung umfangreichen Materials aus dem Bereich der Kinderpornografie bedeuten. In der Regel muss eine zeitintensive Auswertung der erhaltenen Daten erfolgen, um überhaupt relevante Sachverhalte mit entsprechenden IP-Adressen zu ermitteln, um dann eine Bestandsdatenabfrage gemäß § 100j StPO zu erwirken. Erhält eine Strafverfolgungsbehörde große Datenmengen von einer Behörde oder Organisation (aus dem In- oder Ausland) auf eine Art und Weise, welche – zum Beispiel aufgrund der den deutschen Ermittlungsbehörden bekannten sorgfältigen Vorabprüfung oder früherer Zusammenarbeit – die berechtigte Annahme begründet, dass ihre Auswertung zur Aufdeckung strafrechtlich relevanter Sachverhalte führen werden, kann allein diese Übermittlung zureichende tatsächliche Anhaltspunkte im Sinne des § 100g Absatz 5 StPO-E begründen. Erfolgt zeitnah eine Sicherungsanordnung kann der Verlust relevanter Daten dadurch verhindert werden. Bei Gefahr im Verzug, bspw. aufgrund des Umstandes, dass die Einzelauswertung der übermittelten Daten durch das Gericht zu einem Verlust flüchtiger Verkehrsdaten führen würde, kann auch die Staatsanwaltschaft von ihrer Eilkompetenz zum Erlass einer Sicherungsanordnung gemäß § 100e Absatz 1 Satz 2 StPO Gebrauch machen.

Zu Nummer 3 (§ 100j)

Bei der Anpassung in § 100j Absatz 2 Satz 1 handelt es sich um eine Folgeänderung zu der Änderung unter Artikel 5 Nummer 3.

Zu Nummer 4 (§ 100k)

Bei der Neufassung von § 100k Absatz 1 StPO handelt es sich um eine Folgeänderung zur Neufassung der Absätze 1 und 2 von § 100g StPO (siehe oben Nummer 2 Buchstabe b).

Die Befugnis zur Erhebung von Nutzungsdaten bei Telemediendiensten soll spiegelbildlich zur Befugnis nach § 100g Absatz 1 StPO-E gefasst werden. Daher soll der Satz 1 von § 100k Absatz 1 StPO – ohne Änderung in der Sache – redaktionell dergestalt neu gefasst werden, dass er der grammatikalischen Struktur von § 100g Absatz 1 Satz 1 StPO-E folgt (Befugnis in Halbsatz 1, nummerierte Anordnungsvoraussetzungen in Halbsatz 2). Für die Erhebung von Standortdaten werden, wie in § 100g Absatz 1 StPO-E, weiterhin gesonderte Regelungen in Absatz 1 Satz 2 und 3 getroffen, wobei für die Erhebung gespeicherter (retrograder) Standortdaten auf die Voraussetzungen des § 100g Absatz 1 Satz 2 StPO-E verwiesen wird.

Ergänzender Vorschriften zur Einführung einer sogenannten Login-Falle, also der Erhebung einer aktuellen IP-Adresse bei der nächsten Nutzung eines Telemediendienstes zum Zwecke der Identifizierung des Nutzers, bedarf es nicht. Eine Erhebung von IP-Adressen bei Telemedienplattformen ist bereits im geltendem Recht in § 100k StPO verankert. Auch im Bereich von Hatespeech und Cybercrime können gemäß § 100k Absatz 2 StPO bereits heute IP-Adressen erhoben werden, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos wäre. In beiden Fällen bedarf die Erhebung auch nachgeltendem Recht – wie auch in der Konzeption der „Login-Falle“ – einer richterlichen Anordnung gemäß § 101a Absatz 1a, § 100e Absatz 1 Satz 1 StPO. Zudem ist es den Anbietern von Telemedien nach § 24 Absatz 1, Absatz 2 Satz 1 und Absatz 3 Nummer 1 TTDSG bereits heute gestattet, Nutzungsdaten an die Strafverfolgungsbehörden zu übermitteln.

Zu Nummer 5 (§ 101)

Bei der neu geschaffenen Sicherungsanordnung handelt es sich um eine heimliche Ermittlungsmaßnahme, die eine Verarbeitung personenbezogener Daten darstellt. Dies gilt bereits für die Sicherung der Daten, unabhängig davon ob diese später nach § 100g Absatz 1 oder Absatz 3 erhoben werden.

Die damit einhergehende Benachrichtigungspflicht wird nunmehr durch die Ergänzung von § 101 Absatz 4 Satz 1 Nummer 3 StPO ausdrücklich gesetzlich geregelt. Die Benachrichtigungspflicht betrifft allerdings nur die Personen, deren Identität bereits aufgedeckt wurde, die also im zugrundeliegenden Beschluss bereits benannt wurden. Es müssen keine Personen identifiziert bzw. zusätzliche Daten erhoben werden, nur um die Benachrichtigungspflicht zu erfüllen; § 101 Absatz 4 Satz 5 StPO. Hinsichtlich der Benachrichtigungspflicht sind auch §§ 55 f. des Bundesdatenschutzgesetzes, die Artikel 13 Absatz 1 der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (Amtsblatt L 119 vom 04. Mai 2016, S. 89 ff.) umsetzten, zu berücksichtigen. Aufgrund der Aufnahme von Maßnahmen nach § 100g Absatz 5 StPO-E wird § 101 Absatz 4 Satz 1 Nummer 3 StPO ferner dahingehend geändert, dass die Beteiligten der betroffenen Telekommunikation und nicht der überwachten Telekommunikation zu benachrichtigen sind. Eine inhaltliche Änderung ist damit für die Benachrichtigung bei Maßnahmen nach § 100a StPO nicht verbunden.

Zu Nummer 6 (§ 101a)

In § 101a StPO werden – meist im Wege von Rückverweisungen auf die Vorschriften der § 100a 4 und § 100e StPO – Regelungen über das Anordnungsverfahren bei Maßnahmen der Verkehrsdatenerhebung nach § 100g StPO und der Nutzungsdatenerhebung nach

§ 100k StPO getroffen, insbesondere über Auskunftsverpflichtungen der Anbieter, über Anordnungsfristen und über die gerichtliche oder staatsanwaltschaftliche Anordnungskompetenz. Auch hier sollen als notwendige Folgeänderung die Vorschriften, die sich allein auf die aufzuhebende „Vorratsdatenspeicherung“ nach § 100g Absatz 2 StPO beziehen, aufgehoben werden (betrifft vor allem den Absatz 1 von § 101a StPO). Zugleich sollen in einem neu gefassten Absatz 1a Verfahrensregelungen für das neue Ermittlungsinstrument der Sicherungsanordnung nach § 100g Absatz 5 StPO-E geschaffen werden, insbesondere ein Richtervorbehalt und eine Höchstfrist der Maßnahme von einem Monat, die mit Erlass der Sicherungsanordnung zu laufen beginnt.

Zu Buchstabe a

Zu Absatz 1

Der neu gefasste Absatz 1 von § 101a StPO soll nach wie vor das Verfahren bei *Erhebungen* von Verkehrsdaten nach § 100g StPO regeln, allerdings redaktionell gestrafft und angepasst an die Neuregelungen in § 100g Absatz 1 bis Absatz 4 StPO-E. Als Folgeänderung der Aufhebung von § 100g Absatz 2 alter Fassung und von §§ 176 bis 181 TKG sollen zunächst die Regelungen, die sich alleine auf die „Vorratsdatenspeicherung“ beziehen, nicht in die Neufassung übernommen werden (betrifft Satz 1 Nummer 2 und Satz 2 der gegenwärtigen Fassung von § 101a Absatz 1 StPO, die wegfallen sollen). Ansonsten soll die Regelung in Absatz 1, was die – nunmehr in § 100g Absatz 1 bis 3 StPO-E geregelten – Befugnisse zur Verkehrsdatenerhebung angeht, inhaltlich unverändert bleiben, wobei zum besseren redaktionellen Verständnis der Norm die gegenwärtig im Satz 3 von § 101a Absatz 1 StPO verortete Regelung betreffend die Funkzellenabfrage in die neu gefasste Nummer 2 des Absatzes aufgenommen werden soll.

Zu Absatz 1a

Im neu gefassten Absatz 1a sollen im Wege der § 101a StPO eigenen Verweisungstechnik die Verfahrensregelungen für das neue Ermittlungsinstrument der Sicherungsanordnung von Verkehrsdaten nach § 100g Absatz 5 StPO-E geschaffen werden. Im Einzelnen regelt der Verweis auf:

- § 100a Absatz 4 StPO, dass die von einer Sicherungsanordnung betroffenen Telekommunikationsdienste-Anbieter dem Gericht und den Strafverfolgungsbehörden diese Maßnahme – nach § 95 Absatz 2 StPO zwangs- und ordnungsmittelbewehrt – zu ermöglichen und die erforderlichen Auskünfte unverzüglich zu erteilen haben, wobei sich Art und Umfang der hierfür zu treffenden Vorkehrungen nach dem TKG und der TKÜV bestimmen (siehe hierzu die Änderungen unter Artikel 5 und 6 dieses Entwurfs),

- § 100e Absatz 1 StPO, dass

    - die Sicherungsanordnung nach § 100g Absatz 5 StPO-E nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden darf; bei Gefahr im Verzug kann die Anordnung auch durch die Staatsanwaltschaft getroffen werden; soweit die Anordnung der Staatsanwalt nicht binnen drei Werktagen von dem Gericht bestätigt wird, tritt sie außer Kraft – das neue Ermittlungsinstrument soll also, ebenso wie die spätere Erhebung der gesicherten Verkehrsdaten, grundsätzlich unter Richtervorbehalt stehen; dies gebietet schon wegen der möglichen Breitenwirkung der Maßnahme, von der auch andere Personen als Beschuldigte und/oder Nachrichtenmittler betroffen sein können, der effektive Grundrechtsschutz; in der Praxis wird freilich im Sinne der Effektivität der Strafverfolgung auf möglichst rasche ermittlungsrichterliche Anordnungswege zu achten sein, gegebenenfalls über richterli-

che Bereitschafts- und Nachtdienste in besonderen Eilfällen, wird ausnahmsweise ein Rückgriff auf die vorläufige staatsanwaltliche Anordnungsbefugnis wegen Gefahr im Verzug möglich sein; umgesetzt wird damit die Anforderung des EuGH, wonach die Entscheidung der zuständigen Behörde über eine Sicherungsanordnung „einer wirksamen gerichtlichen Kontrolle unterliegen“ müsse (a.a.O.),

- die Sicherungsanordnung ausdrücklich befristet werden muss, wobei dies laut § 101a Absatz 1a Halbsatz 2 Nummer 1 StPO-E mit der Maßgabe zu geschehen hat, dass die Höchstfrist für die Anordnung einen Monat beträgt, jedoch eine höchstens zweimalige Verlängerung der Maßnahme um jeweils nicht mehr als einen Monat zulässig ist, soweit die Voraussetzungen der Anordnung fortbestehen – Daraus folgt eine absolute Höchstfrist für die Sicherung von Verkehrsdaten von drei Monaten. Es handelt sich dabei um eine angemessene Dauer, die einerseits lang genug ist, um zuverlässig im Einzelfall weitergehende Ermittlungen zu ermöglichen, welche die Voraussetzungen für ein Erheben („Auftauen“) der gesicherten Daten nach § 100g Absatz 1 oder 3 StPO-Es schaffen; andererseits ist die Höchstfrist im Sinne des vom EuGH geforderten Grundrechtsschutzes auf das absolut Notwendige begrenzt (ohne dass der Rechtsprechung des EuGH freilich genau bezifferte Anordnungsfristen oder die Einschränkung auf nur 2 Verlängerungsmöglichkeiten zu entnehmen ist).

- § 100e Absatz 3 und 4 StPO, dass auch für die Sicherungsanordnung nach § 100g Absatz 5 StPO-E besonders strenge Schriftlichkeits- und Begründungsanforderungen bestehen (soweit sie sinngemäß auf die Sicherungsanordnung übertragbar sind), wobei laut § 101a Absatz 1a Halbsatz 2 Nummer 2 StPO-E in die Entscheidungsformel darüber hinaus Art und Umfang der zu sichernden Daten genau angegeben werden müssen, und

- § 100e Absatz 5 Satz 1 und 2 StPO, dass die aufgrund der Sicherungsanordnung ergriffenen Maßnahmen unverzüglich zu beenden sind, sobald die Voraussetzungen der Anordnung nicht mehr vorliegen und dass das anordnende Gericht nach Beendigung der Maßnahme über deren Ergebnisse zu unterrichten sein wird.

Zu Buchstabe b

Es handelt sich um eine Folgeänderung zu der Änderung unter Nummer 6 Buchstabe a.

Zu Buchstabe c

Es handelt sich um eine Folgeänderung zu der Neufassung von § 100g StPO. Die Befugnisse zur Erhebung von Verkehrsdaten, auf die sich § 101a Absatz 2 StPO bezieht, sind nunmehr in § 100g Absatz 1 bis 3 StPO-E geregelt; der Verweis in § 101a Absatz 2 StPO muss dementsprechend präzisiert werden.

Zu Buchstabe d

Die Folgeänderung unter Doppelbuchstabe aa erfolgt aus denselben Gründen wie die vorstehende Änderung unter Nummer 6 Buchstabe c.

Die Aufhebung der bisherigen Sätze 2 und 3 von § 101a Absatz 3 StPO ist eine Folgeänderung zur Aufhebung von § 176 TKG (Artikel 5 Nummer 3 dieses Entwurfs).

Zu Buchstabe e

Die Aufhebung der bisherigen Absätze 4 und 5 ist eine Folgeänderung zur Neufassung von § 100g Absatz 2 und zur Aufhebung von § 176 TKG. Die Verwendungsbeschränkungen ergeben sich nunmehr aus § 175 Absatz 2 TKG-E in Verbindung mit § 100g Absatz 5 Satz 2 StPO-E, die Löschungsverpflichtung aus § 175 Absatz 3 TKG-E. Wie auch bisher ergeben sich die Verwendungsbeschränkungen der Daten nach der erfolgten Erhebung aus den allgemeinen Vorschriften; § 161 Absatz 3 StPO, § 479 Absatz 2 StPO.

Zu Buchstabe f

Es handelt sich zum einen um eine Folgeänderung zur vorstehenden Änderung in Nummer 6 Buchstabe e. Zum anderen soll auch hier der Verweis auf die nunmehr in § 100g Absatz 1 bis 3 StPO-E geregelten Befugnisse zur Verkehrsdatenerhebung präzisiert werden (siehe schon die obenstehenden Änderungen unter Nummer 6 Buchstabe c und d).

Zu Buchstabe g

Es handelt sich um eine Folgeänderung zu den vorstehenden Änderungen unter Nummer 6 Buchstabe e und f.

Zu Nummer 7 (§ 101b)

§ 101b StPO regelt die Anforderungen an die statistische Erfassung von Maßnahmen der §§ 100a ff. StPO – darunter auch solchen nach § 100g StPO – und die darauf aufbauenden Berichtspflichten der Länder und des Generalbundesanwalts. Als notwendige Folgeänderung zur Einführung der Sicherungsanordnung nach § 100g Absatz 5 StPO-E muss der Absatz 5 von § 101b StPO, welcher den Inhalt und die Gliederung der zu § 100g StPO zu erstellenden Übersicht regelt, entsprechend angepasst werden.

Zur Frage, wann erstmals eine Übersicht nach § 101b Absatz 5 StPO-E zu erstellen ist, soll im Übrigen in § 12 EGStPO-E eine Übergangsregelung getroffen werden (vgl. Artikel 2 dieses Entwurfs).

Zu Nummer 8 (§ 160a)

Es handelt sich um eine Folgeänderung zur Änderung unter Nummer 2 Buchstabe d.

Zu Artikel 2 (Änderung des Einführungsgesetzes zur Strafprozessordnung)

Artikel 2 legt das Jahr fest, für das die geänderten Berichtspflichten nach Artikel 1 Nummer 7 erstmals Wirkung entfalten sollen.

Zu Artikel 3 (Änderung des Bundespolizeigesetzes)

Es handelt sich um eine Folgeänderung zu den in Artikel 8 des Gesetzentwurfs vorgenommenen Änderungen im Telekommunikationsgesetz.

Zu Artikel 4 (Änderung des BSI-Gesetzes)

Es handelt sich um eine Folgeänderung zu Artikel 8 des Gesetzentwurfs vorgenommenen Änderungen im Telekommunikationsgesetz.

Zu Artikel 5 (Änderung des Bundeskriminalamtgesetzes)

Es handelt sich um eine Folgeänderung zu Artikel 8 des Gesetzentwurfs vorgenommenen Änderungen im Telekommunikationsgesetz.

Zu Artikel 6 (Änderung des Justizvergütungs- und -entschädigungsgesetzes)

Die Änderungen tragen zum einen der Abschaffung der Vorratsdatenspeicherung Rechnung und regeln andererseits erstmals die für die Durchführung einer Sicherungsanordnung anfallenden Entschädigungsbeträge. Dabei orientieren sie sich an der Höhe der bisher bezahlten Summen.

Zu Artikel 7 (Änderung des Zollfahndungsdienstgesetzes)

Es handelt sich um eine Folgeänderung zu Artikel 8 des Gesetzentwurfs vorgenommenen Änderungen im Telekommunikationsgesetz.

Zu Artikel 8 (Änderung des Telekommunikationsgesetzes)

Die spezifischen Regelungen zur Vorratsdatenspeicherung in den §§ 176 bis 181 TKG sollen aufgehoben werden, es verbleibt bei der Regelung in Artikel 8 Nummer 2, der zum einen den Adressatenkreis der Sicherungsanordnung festlegt (bisher § 175 Absatz 1 TKG) und zum anderen die Art und Weise der vorübergehenden Sicherung bestimmt (bisher § 176 Absatz 7 TKG). § 175 Absatz 2 TKG-E enthält spezifische Übermittlungsbefugnisse unter Berufung auf eine gesetzliche Bestimmung und Verwendungsbefugnisse sowie ein Verwendungsverbot für andere Zwecke (bisher § 177 TKG). § 175 Absatz 3 TKG-E enthält eine Löschverpflichtung für die Daten nach Ablauf der in der Sicherungsanordnung genannten Frist (bisher § 176 Absatz 8 TKG).

Die strengen Datenschutz- und Datensicherheitsvorschriften der §§ 176 bis 181 TKG sind in direkter Umsetzung des Urteils des Bundesverfassungsgerichts entstanden, das die erste deutsche Regelung zur Vorratsdatenspeicherung für verfassungswidrig erklärt hatte (Urteil des Ersten Senats vom 2. März 2010 - 1 BvR 256/08 u.a.). Sie werden nach der Aufhebung der Vorratsdatenspeicherung nicht mehr in vollem Umfang benötigt, da nunmehr kein dauerhaft vorhandener Datenpool mit entsprechenden Gefahren missbräuchlicher Nutzung mehr vorgesehen ist. Die Datenspeicherung bei der Sicherungsanordnung erfolgt nämlich im Gegensatz zur Vorratsdatenspeicherung anlassbezogen, im Einzelfall, für einen begrenzten Zeitraum und nur hinsichtlich eines beschränkten Datenumfangs. Ferner ist nicht öffentlich bekannt, ob, in welchem Umfang und wen betreffend Daten gespeichert werden. Damit sind die aufgrund einer Sicherungsanordnung gespeicherten Verkehrsdaten ein deutlich weniger reizvolles Ziel für potentielle Angriffe von außen. Für die aus geschäftlichen Gründen gespeicherten Verkehrsdaten sind im bisher geltenden Recht, insbesondere in der DSGVO, im BDSG, im TKG und im TTDSG, Regelungen zu Datenschutz und Datensicherheit vorgesehen, die auch für die aufgrund der Sicherungsanordnung gespeicherten Daten gelten werden. Auch die in den nunmehr aufgehobenen Vorschriften enthaltenen, sehr ausführlichen Bestimmungen der zu speichernden Daten (§ 176 TKG), sind nicht mehr erforderlich, da die möglichen zu speichernden Verkehrsdaten durch die Verweisung in § 100g Absatz 1 Satz 1 StPO-E in §§ 9 und 12 des TTDSG und § 2a Absatz 1 des BDBOS-Gesetzes abschließend definiert sind.

[*Diese Ausführungen stehen unter dem Vorbehalt des Ergebnisses der endgültigen Abstimmung mit dem BMDV sowie der Verbändebeteiligung zur Frage, ob und in welchem Umfang Datensicherheitsvorschriften erhalten bleiben müssen*]

Zu Artikel 9 (Änderung der Telekommunikations-Überwachungsverordnung)

Es handelt sich um Folgeänderungen zu gemäß Artikel 1 des Gesetzes vorgenommenen Änderungen in der Strafprozessordnung und zu gemäß Artikel 8 des Gesetzentwurfs vorgenommenen Änderungen im Telekommunikationsgesetz.

[Zu Artikel … (Änderung des Telekommunikation-Telemedien-Datenschutz-Gesetz)

Obwohl die Vorratsdatenspeicherung und die Sicherungsanordnung wesensverschieden sind, handelt es sich auch bei der Sicherungsanordnung letztlich um eine gesetzliche Speicherverpflichtung – beziehungsweise im technischen Sinne um ein zeitlich begrenztes Verbot, aus geschäftlichen Gründen erhobene Verkehrsdaten zu löschen. Daher könnte es sich als erforderlich erweisen, für diese Daten besondere gesetzliche Regelungen zu Datenschutz und Datensicherheit zu treffen. In Betracht kommt beispielsweise eine entsprechende Übernahme der Regelungen des bisherigen § 178 Satz 1 und 2 Nummer 1, 2 und 4 TKG, zur Protokollierung gemäß § 179 TKG sowie zum Sicherheitskonzept nach § 181 TKG. Das Telekommunikationsrecht liegt federführend beim BMDV. Die Erarbeitung entsprechender Vorschriften im Einzelnen soll daher im Rahmen der Ressortabstimmung erfolgen. Hierdurch soll eine normenklare und einfach verständliche Regelung, die im Einklang mit den übrigen Vorschriften des Telekommunikationsrechts steht, geschaffen werden.

Ferner soll im Rahmen der Ressortabstimmung geklärt werden, ob die bisher geltenden Vorschriften für die Übermittlung der Daten an die Strafverfolgungsbehörden im Telekommunikationsrecht (Stichwort: Doppeltürmodell) im Rahmen des hiesigen Gesetzentwurfs neu gefasst oder umgestaltet werden sollten oder müssen. Bisher finden sich die entsprechenden Vorschriften bei Verkehrsdatenerhebungen nach § 100g Absatz 1 bis 3 StPO-E in § 101a Absatz 1 StPO-E i.V.m. § 100a Absatz 4 StPO sowie § 9 Absatz 1 Satz 4 TTDSG. Da dies jedoch erhebliche Implikationen für bestehende Regelungen sowohl der StPO als auch des TKG bzw. TTDSG haben kann, ist bisher von einem konkreten Regelungsvorschlag abgesehen worden.]

Zu Artikel 10 (Einschränkung eines Grundrechts)

Die Vorschrift entspricht dem Zitiergebot, da das Grundrecht aus Artikel 10 GG durch die Regelungen in Artikel 1 und Artikel 8 eingeschränkt wird.

Zu Artikel 11 (Inkrafttreten)

Die Vorschrift regelt das Inkrafttreten.