Referentenentwurf

des Bundesministeriums der Justiz

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

A. Problem und Ziel

Vorschriften zur sogenannten Vorratsdatenspeicherung waren wiederholt Gegenstand der Rechtsprechung des Europäischen Gerichtshofs (EuGH) (zuletzt Urteil vom 30. April 2024 „La Quadrature du Net u. a. II – Hadopi“, C-470/21; grundlegend Urteil vom 8. April 2024 „Digital Rights“, C-293/12 und C-594/12, sowie vom 6. Oktober 2020 „La Quadrature du Net u. a.“, C-511/18, C-512/18 und C-520/18). Die zur Vorratsdatenspeicherung gefassten Vorschriften des deutschen Rechts sind nicht mit dem Unionsrecht vereinbar (Urteil vom 20. September 2022 „Spacenet und Telekom Deutschland“, C-793/19 und C-794/19; vergleiche hierzu auch Bundesverwaltungsgericht [BVerwG], Urteil vom 14. August 2023, 6 C 6.22 und 6 C 7.22). Das Bundesverfassungsgericht (BVerfG) hatte bereits mit Urteil vom 2. März 2010 (1 BvR 256/08) die damals geltenden §§ 113a und 113b des Telekommunikationsgesetzes (TKG) und auch § 100g Absatz 1 Satz 1 der Strafprozessordnung (StPO), soweit danach Verkehrsdaten nach § 113a TKG erhoben werden durften, wegen Verstoßes gegen Artikel 10 Absatz 1 des Grundgesetzes (GG) für nichtig erklärt. Mit der Entscheidung des BVerfG steht die Nichtigkeit der maßgeblichen Regelung zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 fest. Auch die im Jahr 2015 neu und restriktiver gefasste Regelung der Vorratsdatenspeicherung im TKG und in der StPO lief bisher weitgehend leer, nachdem das Oberverwaltungsgericht Nordrhein-Westfalen im Eilverfahren die Speicherpflicht gegenüber zwei klagenden Telekommunikationsdienste-Anbietern einstweilig ausgesetzt hatte (Beschluss vom 22. Juni 2017, 13 B 238/17). Bis zum rechtskräftigen Abschluss eines Hauptsacheverfahrens durch Urteil des BVerwG vom 14. August 2023 (6 C 6.22 und 6 C 7.22), das zur Feststellung der vollständigen Unanwendbarkeit der Vorschriften des deutschen Rechts zur Vorratsdatenspeicherung wegen Unvereinbarkeit mit dem Unionsrecht führte, sah daher die Bundesnetzagentur aufgrund der über den Einzelfall hinausgehenden Begründung dieser Entscheidung von jeglichen Maßnahmen zur Durchsetzung der gesetzlich bestehenden Speicherpflicht ab.

Vor diesem Hintergrund ist davon auszugehen, dass de facto seit über 14 Jahren in Deutschland keine Vorratsdatenspeicherung mehr durchgeführt und zu Strafverfolgungszwecken eingesetzt wird. 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. Gleichzeitig wird eine Speicherung von Daten aller Bürger kritisiert, da digitale Kommunikation für die Freiheitsentfaltung der Bürgerinnen und Bürger heute eine essentielle Bedeutung hat und eine anlasslose und unterschiedslose Vorratsdatenspeicherung auch in die Grundrechte von Bürgerinnen und Bürger eingreift, „bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte“ (EuGH, Urteil vom 8. April 2024 „Digital Rights“, C-293/12 und C-594/12, Rz. 58). Gegen die Neuregelung von 2015 zwischenzeitlich erhobene Verfassungsbeschwerden sind inzwischen von den Beschwerdeführern weitgehend für erledigt erklärt oder durch Nichtannahmebeschluss abgewiesen worden, weil die angegriffenen Normen vollständig mit dem Unionsrecht unvereinbar und unanwendbar sind; infolgedessen ist das Rechtsschutzbedürfnis entfallen (BVerfG, Beschluss vom 4. Dezember 2023, 1 BvR 229/16).

Eine Neuauflage der allgemeinen und unterschiedslosen Vorratsdatenspeicherung aller Verkehrsdaten ist aufgrund der höchstrichterlichen Vorgaben bereits rechtlich nicht möglich. Um den Strafverfolgungsbehörden bei gleichzeitiger Berücksichtigung der datenschutzrechtlichen Anforderungen einen wirksamen Zugriff auf die digitalen Beweismittel zu ermöglichen, gibt es aber eine Alternative: Mit einer anlassbezogenen Sicherung von Verkehrsdaten für einen festgelegten Zeitraum, die einer wirksamen richterlichen Kontrolle unterliegt, kann ein grundrechtsschonendes und zugleich effektives Ermittlungsinstrument zur Verfügung gestellt werden, das einer unionsrechtskonformen Regelung im Strafverfahrensrecht zugänglich ist. Dieser Entwurf steht im Kontext der Erreichung der Ziele der Resolution der Generalversammlung der Vereinten Nationen vom 25. September 2015 „Transformation unserer Welt: die UN-Agenda 2030 für nachhaltige Entwicklung“ und trägt zur Erreichung des Nachhaltigkeitsziels 16 bei, rechtsstaatliche und leistungsfähige Institutionen auf allen Ebenen aufzubauen.

B. Lösung

In einem neu gefassten § 100g Absatz 6 StPO wird 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 für betriebliche Zwecke 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 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.

Die Folgeänderungen im TKG, im Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) und in der Telekommunikations-Überwachungsverordnung (TKÜV) dienen dazu, die aus der neuen Sicherungsanordnung folgenden Speicherungs-, Übermittlungs- und Löschungspflichten für die Anbieter von Telekommunikationsdiensten zu regeln. Neben weiteren Folgeänderungen 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 6 StPO-E anfallenden Aufwand angemessen entschädigt werden.

C. Alternativen

Eine Alternative bestünde in dem Verzicht auf eine gesetzliche Regelung. 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 Anbieter von Telekommunikationsdiensten entsteht durch die Einführung der Sicherungsanordnung ein einmaliger Erfüllungsaufwand in Höhe von [...] Euro sowie ein jährlicher Erfüllungsaufwand in Höhe von [...] Euro. Dabei handelt es sich um Bürokratiekosten aus Informationspflichten. [*genaue Bezifferung – ggf. schätzungsweise – soll aufgrund des Ergebnisses der Verbändebeteiligung erfolgen*].

Im Übrigen entsteht für die Wirtschaft kein Erfüllungsaufwand.

Davon Bürokratiekosten aus Informationspflichten:

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

E.3 Erfüllungsaufwand der Verwaltung

Für die Strafverfolgungsbehörden der Länder ist von einem Erfüllungsaufwand in Höhe von jährlich [...] Euro auszugehen. Für die Strafverfolgungsbehörden des Bundes sowie für die Bundesnetzagentur entsteht ein jährlicher Erfüllungsaufwand in Höhe von [...] Euro. [*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 3 des Gesetzes vom 30. Juli 2024 (BGBl. 2024 I Nr. 255) 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) Absatz 1 wird durch die folgenden Absätze 1, 1a und 1b ersetzt:

   „(1) Verkehrsdaten (§§ 9 und 12 des Telekommunikation-Digitale-Dienste-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.

(1a) Die Erhebung gespeicherter (retrograder) Standortdaten ist abweichend von Absatz 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.

(1b) 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) In Absatz 3 Satz 1 Nummer 1 wird die Angabe „Absatz 1" durch die Angabe „Absatz 1a" ersetzt.

d) Folgender Absatz 6 wird angefügt:

„(6) Auch ohne das Wissen des Betroffenen darf angeordnet werden, dass Anbieter öffentlich zugänglicher Telekommunikationsdienste, bei denen es sich nicht um nummernunabhängige interpersonelle Telekommunikationsdienste handelt, die bei der Nutzung des Dienstes bereits erzeugten oder verarbeiteten und noch vorhandenen sowie künftig anfallenden Verkehrsdaten unverzüglich zu sichern haben (Sicherungsanordnung), wenn zureichende tatsächliche Anhaltspunkte dafür vorliegen, dass eine in Absatz 1 oder Absatz 1a 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, 1a und 3."

3. § 100k wird die folgt geändert:

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

„(1) Nutzungsdaten (§ 2 Absatz 2 Nummer 3 des Telekommunikation-Digitale-Dienste-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.

(1a) Die Erhebung gespeicherter (retrograder) Standortdaten ist abweichend von Absatz 1 Nummer 1 und 2 nur unter den Voraussetzungen von § 100g Absatz 1a 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.“

b) In Absatz 3 werden die Wörter „Absatz 1 und 2“ durch die Wörter „Absatz 1 bis 2“ ersetzt.

c) In Absatz 4 wird die Angabe „Absatz 1“ durch die Angabe „Absatz 1, 1a“ ersetzt.

4. § 101 wird wie folgt geändert:

a) In Absatz 1 werden nach der Angabe „100f,“ die Wörter „100g Absatz 6, den §§“ eingefügt.

b) In Absatz 2 Satz 1 wird nach der Angabe „100f,“ die Angabe „100g Absatz 6, §“ eingefügt.

c) In Absatz 4 Satz 1 Nummer 3 werden nach der Angabe „§ 100a“ die Wörter „und des § 100g Absatz 6“ eingefügt und wird das Wort „überwachten“ durch das Wort „betroffenen“ ersetzt.

5. § 101a wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) Satz 1 wird wie folgt geändert:

aaa) Im Satzteil vor Nummer 1 werden die Wörter „§ 100g gelten § 100a Absatz 3 und 4 und § 100e“ durch die Wörter „§ 100g Absatz 1 bis 3 gelten § 100a Absatz 4 sowie § 100e Absatz 1, 3, 4 und 5 Satz 1 und 2“ ersetzt.

bbb) In Nummer 2 wird der Punkt am Ende durch ein Komma ersetzt.

ccc) Folgende Nummer 3 wird angefügt:

„3. 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.“

bb) Satz 3 wird aufgehoben.

b) Nach Absatz 1 wird folgender Absatz 1a eingefügt:

„(1a) Bei Sicherungsanordnungen nach § 100g Absatz 6 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 die Sicherungsanordnung auf höchstens einen Monat zu befristen ist und abweichend von § 100e Absatz 1 Satz 5 eine höchstens zweimalige Verlängerung der Sicherungsanordnung um jeweils nicht mehr als einen Monat zulässig ist, soweit deren Voraussetzungen fortbestehen,

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

c) Der bisherige Absatz 1a wird Absatz 1b und die Wörter „§ 100k Absatz 1 und 2" werden durch die Wörter „§ 100k Absatz 1 bis 2" ersetzt.

d) In Absatz 2 und Absatz 3 Satz 1 werden jeweils die Wörter „§ 100g oder § 100k Absatz 1 oder Absatz 2" durch die Wörter „§ 100g Absatz 1 bis 3 oder § 100k Absatz 1, Absatz 1a oder Absatz 2" ersetzt.

e) In Absatz 6 Satz 1 wird die Angabe „§ 100g" durch die Wörter „§ 100g Absatz 1 bis 3" und werden die Wörter „§ 100k Absatz 1 und 2" durch die Wörter „§ 100k Absatz 1 bis 2" ersetzt.

6. § 101b wird wie folgt geändert:

a) Absatz 5 wird wie folgt geändert:

aa) In Nummer 1 Satzteil vor Buchstabe a werden die Wörter „Absatz 1, 2 und 3" durch die Wörter „Absatz 1 bis 1b, 2, 3 und 6" ersetzt.

bb) Nummer 2 wird wie folgt geändert:

aaa) In Buchstabe a wird die Angabe „Absatz 1" durch die Wörter „Absatz 1 bis 1b" ersetzt.

bbb) Nach Buchstabe c wird folgender Buchstabe d eingefügt:

„d) die Anzahl der Sicherungsanordnungen nach § 100g Absatz 6;".

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

b) In Absatz 6 Satzteil vor Nummer 1 werden die Wörter „Absätzen 1 und 2" durch die Wörter „Absätzen 1, 1a und 2" ersetzt.

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 4 des Gesetzes vom 12. Juli 2024 (BGBl. 2024 I S. 234) geändert worden ist, wird wie folgt gefasst:

„§ 12

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

Übersichten nach § 101b Absatz 5 der Strafprozessordnung in der vom … [einsetzen: Datum des Inkrafttretens nach Artikel 8 dieses Gesetzes] an geltenden Fassung sind erstmalig für das auf den … [einsetzen: Datum des Inkrafttretens nach Artikel 8 dieses Gesetzes] 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 Justizvergütungs- und -entschädigungsgesetzes

Das Justizvergütungs- und -entschädigungsgesetz vom 5. Mai 2004 (BGBl. I S. 718, 776), das zuletzt durch Artikel 5 des Gesetzes vom 7. Oktober 2024 (BGBl. 2024 I S. 302) geändert worden ist, wird wie folgt geändert:

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

2. Die 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 321 sowie nach den Abschnitten 4 bis 6“ ersetzt.

   b) Der Überschrift von Abschnitt 3 werden die Wörter „ohne vorausgegangene Sicherungsanordnung“ angefügt.

   c) Der Überschrift von Abschnitt 4 werden die Wörter „ohne vorausgegangene Sicherungsanordnung“ angefügt.

   d) Die folgenden Abschnitte 5 und 6 werden angefügt:

Nr.	Tätigkeit	Höhe
	„Abschnitt 5	
	Sicherung von Daten	
500	Sicherung von Verkehrsdaten: für jede Kennung, die der Sicherungsanordnung zugrunde liegt ..... Die Sicherung der die Kennung betreffenden Standortdaten ist mit abgegolten.	30,00 €
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 ..... Die Sicherung der Standortdaten der Zieladresse ist mit abgegolten.	90,00 €
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	Sicherung des letzten dem Netz bekannten Standortes eines Mobiltelefons	90,00 €
510	Verlängerung der Speicherung gesicherter Daten für jeden der in den Nummern 500 bis 502 und 504 bis 509 genannten Fällen	20,00 €
	Abschnitt 6	
	Auskünfte nach vorausgegangener Sicherungsanordnung	
600	Auskunft über Daten, soweit eine nach Abschnitt 5 zu entschädigende Sicherungsanordnung vorausgegangen ist: je Auskunftsersuchen	20,00 €“.

Nr.	Tätigkeit	Höhe
	„***Abschnitt 5***	
	Sicherung von Daten	
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 ..... 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.	930,00 €
508	Die Sicherung erfolgt für eine bestimmte Wegstrecke: Die Entschädigung nach Nummer 504 beträgt für jeweils angefangene 10 Kilometer Länge	110,00 €
509	Sicherung des letzten dem Netz bekannten Standortes eines Mobiltelefons	90,00 €
510	Verlängerung der Speicherung gesicherter Daten für jeden der in den Nummern 500 bis 502 und 504 bis 509 genannten Fällen	20,00 €
	Abschnitt 6	
	Auskünfte nach vorausgegangener Sicherungsanordnung	
600	Auskunft über Daten, soweit eine nach Abschnitt 5 zu entschädigende Sicherungsanordnung vorausgegangen ist: je Auskunftsersuchen	20,00 €“.

Artikel 4

Änderung des Telekommunikationsgesetzes

Das Telekommunikationsgesetz vom 23. Juni 2021 (BGBl. I S. 1858), das zuletzt durch Artikel 35 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht wird nach der Angabe zu § 174 folgende Angabe eingefügt:

   „§ 174a Pflichten zur Speicherung von Verkehrsdaten aufgrund von Sicherungsanordnungen“.

2. Nach § 174 wird folgender § 174a eingefügt:

„§ 174a

Pflichten zur Speicherung von Verkehrsdaten aufgrund von Sicherungsanordnungen

(1) Anbieter öffentlich zugänglicher Telekommunikationsdienste, bei denen es sich nicht um nummernunabhängige interpersonelle Telekommunikationsdienste handelt, sind verpflichtet, die bei der Nutzung des Dienstes bereits erzeugten oder verarbeiteten und noch vorhandenen sowie künftig anfallenden Verkehrsdaten (§§ 9 und 12 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes) aufgrund einer Sicherungsanordnung nach § 100g Absatz 6 der Strafprozessordnung unverzüglich zu sichern. Die Sicherung hat dadurch zu erfolgen, dass bereits gespeicherte Daten für die in der Sicherungsanordnung genannte Frist nicht gelöscht werden und künftig anfallende Daten gespeichert und für die in der Sicherungsanordnung genannte Frist nicht gelöscht werden. Die Speicherung der Verkehrsdaten hat so zu erfolgen, dass die Übermittlung an Strafverfolgungsbehörden nach Absatz 4 unverzüglich erfolgen kann. Der Inhalt der Kommunikation, Daten über aufgerufene Internetseiten und Daten

von Diensten der elektronischen Post dürfen aufgrund dieser Vorschrift nicht gespeichert werden.

(2) Daten, die den in § 11 Absatz 5 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes genannten Verbindungen zugrunde liegen, dürfen aufgrund dieser Vorschrift nicht gespeichert werden. Dies gilt entsprechend für Telefonverbindungen, die von den in § 11 Absatz 5 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes genannten Stellen ausgehen. § 11 Absatz 6 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes gilt entsprechend.

(3) Der nach Absatz 1 Satz 1 Verpflichtete hat sicherzustellen, dass die aufgrund von Sicherungsanordnungen nach § 100g Absatz 6 der Strafprozessordnung gesicherten Daten durch technische und organisatorische Maßnahmen nach dem Stand der Technik gegen unbefugte Kenntnisnahme und Verwendung geschützt werden. Die ergriffenen Schutzmaßnahmen sind im Sicherheitskonzept nach § 166 Absatz 1 Nummer 3 darzustellen. Die Speicherung und irreversible Löschung der Daten erfolgt nach Maßgabe der Rechtsverordnung nach § 170 Absatz 5 und der Technischen Richtlinie nach § 170 Absatz 6.

(4) Die aufgrund von Sicherungsanordnungen nach § 100g Absatz 6 der Strafprozessordnung gesicherten 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. Die aufgrund von Sicherungsanordnungen nach § 100g Absatz 6 der Strafprozessordnung gesicherten Verkehrsdaten dürfen auch für eine Auskunft nach § 174 Absatz 1 Satz 3 verwendet werden. Für andere Zwecke dürfen diese Verkehrsdaten, soweit sie allein aufgrund der Sicherungsanordnung nach § 100g Absatz 6 der Strafprozessordnung gesichert wurden, von dem nach Absatz 1 Satz 1 Verpflichteten nicht verwendet werden. Die Übermittlung der Daten erfolgt nach Maßgabe der Rechtsverordnung nach § 170 Absatz 5 und der Technischen Richtlinie nach § 170 Absatz 6. Die Daten sind so zu kennzeichnen, dass erkennbar ist, dass es sich um Daten handelt, die aufgrund einer Sicherungsanordnung nach § 100g Absatz 6 der Strafprozessordnung gesichert waren. Nach Übermittlung an eine andere Stelle ist die Kennzeichnung durch diese aufrechtzuerhalten.

(5) Der nach Absatz 1 Satz 1 Verpflichtete hat Verkehrsdaten, die aufgrund von Sicherungsanordnungen nach § 100g Absatz 6 der Strafprozessordnung gesichert 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-Digitale-Dienste-Datenschutz-Gesetzes bleiben unberührt.“

3. Nach § 228 Absatz 2 Nummer 56 werden die folgenden Nummern 56a und 56b eingefügt:

„56a. entgegen § 174a Absatz 4 dort genannte Daten für andere als die dort genannten Zwecke verwendet,

56b. entgegen § 174a Absatz 5 Daten nicht rechtzeitig löscht oder die Löschung nicht sicherstellt,“.

Artikel 5

Änderung der Telekommunikations-Überwachungsverordnung

Die Telekommunikations-Überwachungsverordnung in der Fassung der Bekanntmachung vom 11. Juli 2017 (BGBl. I S. 2316), die zuletzt durch Artikel 33 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I S. 149) 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 Doppelbuchstabe aa wird wie folgt gefasst:

      „aa) 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-Digitale-Dienste-Datenschutz-Gesetzes erhobene Verkehrsdaten zu stellen, oder“.

2. In § 32 Absatz 1 Satz 1 und Absatz 2 Satz 3 werden jeweils nach den Wörtern „des Telekommunikationsgesetzes“ die Wörter „oder des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes“ eingefügt.

3. § 35 wird wie folgt geändert:

   a) In Satz 2 werden nach den Wörtern „des Telekommunikationsgesetzes“ die Wörter „oder des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes“ eingefügt.

   b) In Satz 3 Nummer 4 wird nach dem Wort „Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes“ die Angabe „oder § 174a“ eingefügt.

Artikel 6

Änderung des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes

Dem § 9 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982; 2022 I S. 1045), das zuletzt durch Artikel 44 des Gesetzes vom 12. Juli 2024 (BGBl. 2024 I Nr. 234) geändert worden ist, wird folgender Absatz 3 angefügt:

„(3) Nach § 3 Absatz 2 Satz 1 Nummer 1 Verpflichtete dürfen Verkehrsdaten verarbeiten, soweit dies für die Übermittlung von Verkehrsdaten nach § 174a Absatz 4 Satz 1 des Telekommunikationsgesetzes oder für eine Auskunft nach § 174 Absatz 1 Satz 3 des Telekommunikationsgesetzes erforderlich ist.“

Artikel 7

Einschränkung eines Grundrechts

Durch die Artikel 1 und 4 wird das Fernmeldegeheimnis (Artikel 10 Absatz 1 des Grundgesetzes) eingeschränkt.

Artikel 8

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 Höchstspeicherfrist 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 Anbietern von Telekommunikationsdiensten, 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) in der damaligen Fassung. Diese Vorschriften wurden im Jahr 2021 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 um den zweiten Anlauf des Gesetzgebers, das Ermittlungsinstrument der Vorratsdatenspeicherung rechtssicher einzuführen. 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 Anbietern von Telekommunikationsdiensten einstweilig ausgesetzt hatte (Beschluss vom 22. Juni 2017, 13 B 238/17). Vor diesem Hintergrund sah die Bundesnetzagentur aufgrund der über den Einzelfall hinausgehenden Begründung dieser Entscheidung bis zum rechtskräftigen Abschluss eines Hauptsacheverfahrens von jeglichen Maßnahmen zur Durchsetzung der nach wie vor bestehenden Speicherpflicht gemäß § 115 TKG alter Fassung (nunmehr § 183 TKG) ab. Das Bundesverwaltungsgericht hat mit Beschluss vom 25. September 2019 (6 C 12/18) den Gerichtshof der Europäischen Union (EuGH) mit der Sache befasst.

Vor diesem Hintergrund ist davon auszugehen, dass de facto seit über 14 Jahren in Deutschland keine Vorratsdatenspeicherung mehr durchgeführt und zu Strafverfolgungszwecken eingesetzt wird. 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. Gleichzeitig wird eine Speicherung von Daten aller Bürger kritisiert, da digitale Kommunikation für die Freiheitsentfaltung der Bürgerinnen und Bürger heute eine essentielle Bedeutung hat und eine anlasslose und unterschiedslose Vorratsdatenspeicherung auch in die Grundrechte von Bürgerinnen und Bürger eingreift, „bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte“ (EuGH, Urteil vom 8. April 2024 „Digital Rights“, C-293/12 und C-594/12, Rz. 58). Gegen die Neuregelung von 2015 zwischenzeitlich erhobene Verfassungsbeschwerden sind inzwischen von den Beschwerdeführern weitgehend für erledigt erklärt oder durch Nichtannahmebeschluss abgewiesen worden, weil die angegriffenen Normen vollständig mit dem Unionsrecht unvereinbar und unanwendbar sind; infolgedessen ist das Rechtsschutzbedürfnis entfallen (BVerfG, Beschluss vom 4. Dezember 2023, 1 BvR 229/16).

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 bereits gelöscht sind. Ob und wie viele Fälle hätten aufgeklärt werden können, gäbe es die Vorratsdatenspeicherung, bleibt damit letztlich Spekulation. Den Strafverfolgungsbehörden ist es ausweislich der Polizeilichen Kriminalstatistik (PKS) für das Jahr 2023 gelungen, 87,2 Prozent der bekannt gewordenen Fälle der Verbreitung kinderpornographischer Inhalte im Sinne von § 184b Absatz 1 Satz 1 des Strafgesetzbuchs a.F. aufzuklären.

Mit Urteil vom 20. September 2022 „Spacenet und Telekom Deutschland“, 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 Grundsatz 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 könne eine Speicherverpflichtung für Verkehrsdaten überhaupt rechtfertigen (Rz. 73). Eine allgemeine und unterschiedslose Vorratsdatenspeicherung von allen Verkehrsdaten komme zur Verwirklichung dieses Ziels nicht in Betracht (Rz. 75). Die derzeitigen deutschen Vorschriften sähen eine Vorratsspeicherung von Verkehrs- und Standortdaten nahezu aller 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 Zugang 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 („Tele2 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.).

In seinem Urteil vom 30. April 2024 „La Quadrature du Net u. a. II – Hadopi “, C-470/21, hat der EuGH entschieden, dass Mitgliedstaaten den Internetzugangsanbietern mit dem Ziel der Bekämpfung von Straftaten im Allgemeinen eine Pflicht zur allgemeinen und unterschiedslosen Vorratsspeicherung von IP-Adressen auferlegen können, sofern eine solche Speicherung keine genauen Schlüsse auf das Privatleben der fraglichen Person zulässt (Rz. 92). Der EuGH betont, dass eine den Betreibern elektronischer

Kommunikationsdienste auferlegte Pflicht, die allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen sicherzustellen, gegebenenfalls durch das Ziel der Bekämpfung von Straftaten im Allgemeinen gerechtfertigt sein könne, wenn tatsächlich ausgeschlossen sei, dass diese Speicherung schwere Eingriffe in das Privatleben des Betroffenen zur Folge haben könnten, die darauf beruhten, dass insbesondere durch eine Verknüpfung der IP-Adresse mit einem von den Betreibern ebenfalls gespeicherten Satz von Verkehrs- und Standortdaten die Möglichkeit bestehe, genaue Schlüsse in Bezug auf ihn zu ziehen (Rz. 82). Daher müsse sich ein Mitgliedsstaat, der den Betreibern elektronischer Kommunikationsdienste eine solche Pflicht auferlegen möchte, um ein mit der Bekämpfung von Straftaten im Allgemeinen verbundenes Ziel zu erreichen, vergewissern, dass die Modalitäten der Vorratsspeicherung es ausschlössen, dass genaue Schlüsse auf das Privatleben der Person gezogen werden könnten (Rz. 83). Dafür können Speichermodalitäten sorgen, die eine wirksame strikte Trennung der IP-Adressen und der übrigen Kategorien personenbezogener Daten, insbesondere der Identitätsdaten, gewährleisten (Rz. 85 ff.). Schließlich müsse eine entsprechende gesetzliche Regelung eine auf das absolut Notwendige begrenzte Dauer der Speicherung vorsehen und 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 Missbrauchsgefahren sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung verfügten (Rz. 93).

Mit Urteil vom 14. August 2023 (6 C 6.22 und 6 C 7.22) hat das Bundesverwaltungsgericht entschieden, dass die in § 175 Absatz 1 Satz 1 in Verbindung mit § 176 TKG (§ 113a Absatz 1 Satz 1 in Verbindung mit § 113b TKG alte Fassung) geregelte Verpflichtung der Anbieter öffentlich zugänglicher Telekommunikationsdienste zur Speicherung der dort genannten Telekommunikations-Verkehrsdaten in vollem Umfang unvereinbar mit Artikel15 Absatz 1 der Datenschutzrichtlinie für elektronische Kommunikation (Richtlinie 2002/58/EG) und daher nicht anwendbar ist. Da eine unionsrechtskonforme Auslegung wegen des vom EuGH hervorgehobenen Grundsatzes der Bestimmtheit und Normenklarheit nicht in Betracht komme, dürfe die Regelung im Telekommunikationsgesetz wegen des Anwendungsvorrangs des Unionsrechts nicht angewendet werden (Rz. 46). Die im Jahr 2015 eingeführten Vorschriften waren auch Gegenstand einer Verfassungsbeschwerde. Nachdem die Beschwerdeführenden das Verfahren mit Blick auf die nun feststehende Europarechtswidrigkeit der Normen für erledigt erklärt hatten, gewährte das Bundesverfassungsgericht ihnen die Erstattung ihrer notwendigen Auslagen (BVerfG, Beschluss vom 4. Dezember 2023, 1 BvR 229/16, mit Wiedergabe des fachgerichtlichen Verfahrens in Rn. 6 ff.).

In dem unwahrscheinlichen Fall, dass ein Telekommunikationsanbieter auf Basis der europarechtswidrigen Normen Daten speichert und eine Strafverfolgungsbehörde diese erhebt, kann sich je nach Ausgestaltung des Einzelfalls aufgrund der Rechtsprechung des EuGH bereits ein unionsrechtliches Beweisverwertungsverbot ergeben (Urteil vom 20. September 2022 „VD und SR“, C-339/20 und C-397/20, Rn. 106). Ungeachtet dessen dürfte aber auch nach der nach der deutschen Rechtsprechung anwendbaren Abwägungslehre ein Beweisverwertungsverbot bestehen, wenn unionsrechtswidrig gespeicherte Daten erhoben werden und Strafverfolgungsbehörden damit bewusst gegen Unionsrecht verstoßen.

Zur effektiven Erlangung von digitalen Beweismitteln steht eine Alternative zur Verfügung. Der EuGH hat 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.

Dieser Entwurf steht im Kontext der gefährdeten rechtzeitigen Erreichung der Ziele der Resolution der Generalversammlung der Vereinten Nationen vom 25. September 2015

„Transformation unserer Welt: die UN-Agenda 2030 für nachhaltige Entwicklung“ und trägt zur Erreichung des Nachhaltigkeitsziels 16 bei, rechtsstaatliche und leistungsfähige Institutionen auf allen Ebenen aufzubauen.

II. Wesentlicher Inhalt des Entwurfs

Mit diesem Entwurf wird 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 betrieblichen Zwecken 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 – 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 Anbieter elektronischer Kommunikationsdienste, die diese für betriebliche Zwecke 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). Dies hat der EuGH auch in seinem Urteil vom 20. September 2022 wiederholt („Spacenet und Telekom Deutschland“, C-793/19 und C-794/19, Rz. 114; zu etwaigen Möglichkeiten, einen eingeschränkten Datenkranz auch zu anderen Zwecken zu nutzen, Urteil vom 30. April 2024 „La Quadrature du Net u. a. II – Hadopi“, C-470/21, Rz. 82 ff.).

In einer solchen Situation, so der EuGH weiter (a.a.O.), stehe es den Mitgliedstaaten frei, in Rechtsvorschriften vorzusehen, dass den Anbietern 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 „Spacenet und Telekom Deutschland “, 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), 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 „Spacenet und Telekom Deutschland“, 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 („Tele2“, 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, vergleiche 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).

Bei der Sicherungsanordnung nach § 100g Absatz 6 StPO handelt es 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 passt außerdem das nationale Strafverfahrensrecht an die Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates vom 12. Juli 2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren an. Artikel 6 der Verordnung sieht eine Europäische Sicherungsanordnung vor. Gemäß Artikel 6 Absatz 3 ist für den Erlass Voraussetzung, dass sie in einem vergleichbaren nationalen Fall unter denselben Voraussetzungen hätte erlassen werden können.

Die Einführung der Sicherungsanordnung nach § 100g Absatz 6 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 Zielvorgaben 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 Zielvorgabe 16.10 verlangten Schutz der Grundfreiheiten.

Die Folgeänderungen im TKG und in der Telekommunikations-Überwachungsverordnung (TKÜV) dienen dazu, die aus der neuen Sicherungsanordnung folgenden Speicherungs-, Übermittlungs- und Löschungspflichten für die Anbieter von Telekommunikationsdiensten zu regeln.

Die Folgeänderungen im TKG, im Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) und in der Telekommunikations-Überwachungsverordnung (TKÜV) dienen dazu, die aus der neuen Sicherungsanordnung folgenden Speicherungs-, Übermittlungs- und Löschungspflichten für die Anbieter von Telekommunikationsdiensten zu regeln. Neben weiteren Folgeänderungen 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 6 StPO-E anfallenden Aufwand angemessen entschädigt werden.

III. Exekutiver Fußabdruck

Es haben keine Interessenvertreter sowie beauftragte Dritte wesentlich zum Inhalt des Entwurfs beigetragen.

IV. Alternativen

Alternativ könnte auf eine gesetzliche Regelung verzichtet werden. Jedoch führt die Neuregelung gegenüber dem seit 14 Jahren unbefriedigenden Status quo zu verbesserten Ermittlungsmöglichkeiten. Den Strafverfolgungsbehörden wird 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.

V. Gesetzgebungskompetenz

Die Gesetzgebungskompetenz des Bundes folgt aus Artikel 74 Absatz 1 Nummer 1 GG (gerichtliches Verfahren, betrifft Artikel 1 bis 3 dieses Gesetzes) und aus Artikel 73 Absatz 1 Nummer 7 GG (Telekommunikation, betrifft Artikel 4 bis 6 dieses Gesetzes).

VI. 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.

Die vorgeschlagene Regelung einer Sicherungsanordnung in § 100g Absatz 6 StPO-E steht 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.

VII. Gesetzesfolgen

1. Rechts- und Verwaltungsvereinfachung

Insbesondere der Wegfall der gesetzlichen Aufsichtspflichten im Rahmen der nunmehr dauerhaft nicht anwendbaren 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 6 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. Dieses Nachhaltigkeitsziel verlangt mit seinen Zielvorgaben 16.3 und 16.6, die Rechtsstaatlichkeit auf nationaler und internationaler Ebene zu fördern und leistungsfähige, rechenschaftspflichtige und transparente Institutionen auf allen Ebenen aufzubauen. Der Entwurf fördert die Erreichung dieser Zielvorgaben, indem er die Erhebung und Auswertung von Verkehrsdaten durch die Strafverfolgungsbehörden an richterliche Anordnungen knüpft.

Mit Zielvorgaben 16.1, 16.2, 16.4 und 16.5 verlangt dieses Nachhaltigkeitsziel außerdem, 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 6 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.

Der Entwurf folgt damit den Nachhaltigkeitsprinzipien der DNS „(1.) Nachhaltige Entwicklung als Leitprinzip konsequent in allen Bereichen und bei allen Entscheidungen an-wenden“, „(2.) Global Verantwortung wahrnehmen“ und „(5.) Sozialen Zusammenhalt in einer offenen Gesellschaft wahren und verbessern“.

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 Anbieter von Telekommunikationsdiensten entsteht durch die Einführung der Sicherungsanordnung ein Mehraufwand in Höhe von [...] Euro.

Der zusätzliche Aufwand der Anbieter durch die Verpflichtung zur Umsetzung der Sicherungsanordnung nach § 100g Absatz 6 StPO und einer sich daran in der Regel anschließenden Auskunftserteilung nach § 100g Absatz 1, 1a, 1b oder 3 StPO wird durch die Entschädigung für die Kosten für die Sicherung und Beauskunftung im Einzelfall nach § 23

JVEG-E ausgeglichen, so dass insoweit kein Erfüllungsaufwand entsteht. Jedoch ist mit einmaligem Erfüllungsaufwand für Investitionskosten in Höhe von [...] Euro sowie dauerhaft gesteigerten Betriebskosten zur Umsetzung der Anforderungen aus § 174a TKG-E in Höhe von [...] Euro zu rechnen.

[*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

aa) Länder

Für die Strafverfolgungsbehörden der Länder ist von einem Mehraufwand durch die Einführung der Sicherungsanordnung in Höhe von [...] Euro auszugehen. Auf der anderen Seite ist von kostenrelevanten Effektivitätsgewinnen durch die Einführung der Anordnung nach § 100g Absatz 6 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.

bb) Bund

Ein zusätzlicher Kontrollaufwand, ob die Anbieter von Telekommunikationsdiensten die neuen Pflichten nach § 174a TKG-E einhalten, wird auch bei der Bundesnetzagentur anfallen. Hinzu kommt ein Mehraufwand bei der Anwendung der neuen Bußgeldtatbestände. Die kostenrelevanten Effektivitätsgewinne sind auch bei der Strafverfolgung zu erwarten, die dem Bund obliegt.

[*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.

VIII. 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 6 StPO geregelt sein wird.

Zu Buchstabe b

Der Neufassung von § 100g Absatz 1 StPO liegen die folgenden Erwägungen zugrunde:

Der Sache nach unverändert bleiben soll die bislang in § 100g Absatz 1 StPO vorgesehene Befugnis zur Erhebung von zu betrieblichen Zwecken bei den Anbietern von Telekommunikationsdiensten gespeicherten Verkehrsdaten, die aus verfassungsrechtlicher Sicht nicht zu beanstanden ist (vergleiche 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 verschiedenen Daten zusammen geregelt. Dies sind erstens Verkehrsdaten wegen des Verdachts von Straftaten von auch im Einzelfall erheblicher Bedeutung, insbesondere solchen, die in § 100a StPO bezeichnet sind, zweitens von Standortdaten und drittens von Verkehrsdaten wegen des Verdachts von mittels Telekommunikation begangener Straftaten. Die Erhebung 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 drei getrennten Absätzen geregelt werden, die künftig zudem eine übersichtlichere Nummerierung der jeweiligen Voraussetzungen für eine Anordnung enthalten sollen:

Im neuen § 100g Absatz 1 StPO-E soll allein die Befugnis zur Erhebung von Verkehrsdaten wegen des Verdachts von Straftaten von erheblicher Bedeutung geregelt werden.

§ 100g Absatz 1a StPO enthält zukünftig die Regelung zur Erhebung gespeicherter (retrograder) Standortdaten, in dem die von Absatz 1 Nummer 1 und 2 abweichenden Voraussetzungen geregelt sind. Absatz 1 Nummer 3, der die Verhältnismäßigkeit betrifft, gilt auch in den Fällen des Absatz 1a. Auch wenn durch die dauerhafte Nichtanwendung der Regelungen zur anlasslosen Vorratsdatenspeicherung retrograde Standortdaten nur noch dann vorhanden sein können, wenn diese seitens der Anbieter von Telekommunikationsdiensten für betriebliche Zwecke gespeichert werden, soll deren Erhebung nur unter strengen Voraussetzungen möglich sein. Hierzu bedarf es gemäß Absatz 1a Satz 1 Nummer 1 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“, vergleiche 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 (Absatz 1a Satz 1 Nummer 2). Nach Absatz 1a Satz 1 kommt nur die Erhebung von Standortdaten für künftig anfallende Verkehrsdaten oder in Echtzeit in Betracht, was durch Satz 2 klargestellt wird.

Der neu gefasste § 100g Absatz 1b 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 (vergleiche 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 1b 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.

Einer Erstreckung des Absatzes 4 von § 100g StPO auf Absatz 1 bis 1 b und 3 bedarf es nicht, da der Schutz von Berufsgeheimnisträgern bereits nach der allgemeinen Schutzvorschrift des § 160a StPO gewährleistet ist und eine Erstreckung verfassungsrechtlich problematisch wäre. Durch die Anwendbarkeit des § 160a StPO ist gewährleistet, dass unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts (vergleiche BVerfG, Beschluss vom 12. Oktober 2011 – 2 BvR 236/08 –, Rz. 268 – zitiert nach juris, zur Frage des Vorrangs der Presse- und Rundfunkfreiheit vor anderen wichtigen Rechtsgütern) ein abgestuftes Schutzkonzept gilt und der Gesetzgeber daher auch daran gehindert wäre, den Schutz von Berufsgeheimnisträgern, insbesondere Journalisten, auszuweiten.§ 100g Absatz 4 StPO ist eine Spezialvorschrift zum Schutz von Berufsgeheimnisträgern mit Zeugnisverweigerungsrecht im Rahmen der nicht mehr anwendbaren 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. Der Schutz von zeugnisverweigerungsberechtigten Berufsgeheimnisträgern im Rahmen der von nun an in § 100g Absatz 1 bis 1b StPO geregelten Ermittlungsmaßnahmen ist unabhängig davon gewährleistet. 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 zum einen auch künftig Maßnahmen nach § 100g Absatz 1 bis 1b und 3 StPO-E unzulässig sein. Da der Schutz von Berufsgeheimnisträgern nach § 160a StPO Ermittlungsinstrumente im Allgemeinen erfasst, erstreckt sich dieser darüber hinaus aber auch auf das neue Ermittlungsinstrument der Sicherungsanordnung (§ 100g Absatz 6 StPO). Die Regelung des § 160a Absatz 1 Satz 1 StPO sieht somit für einen engen Kreis von auf besondere Vertraulichkeit angewiesenen Telekommunikationsverbindungen ein grundsätzliches, lückenloses Verbot der Erhebung und Sicherung von Daten 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 (vergleiche 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 Beratungsstellen 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 1b und 3 StPO sowie wiederum auch bei der Sicherungsanordnung nach § 100g Absatz 6 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).

Zu Buchstabe c

Die Änderung betrifft § 100g Absatz 3 StPO, der die Funkzellenabfrage regelt, also die Erhebung aller in einer Funkzelle angefallenen Verkehrsdaten. Es wird durch den Verweis in Absatz 3 Satz 1 Nummer 1 auf Absatz 1a Satz 1 Nummer 1 ausdrücklich geregelt, dass – wie bei Erhebung gespeicherter (retrograder) Standortdaten – ein Verdacht hinsichtlich einer Straftat aus dem Katalog des § 100a Absatz 2 StPO erforderlich ist. Dass die im Vergleich zur Verkehrsdatenerhebung nach § 100g Absatz 1 StPO erhöhten Anforderungen an die Erhebung retrograder Standortdaten auch im Falle einer Funkzellenabfrage erfüllt sein müssen, entspricht der bisherigen Rechtslage (vgl. Bundesgerichtshof, Beschluss vom 10. Januar 2024 – 2 StR 171/23 – zum damaligen Erfordernis eines Verdachts hinsichtlich einer Katalogtat nach § 100g Absatz 2 StPO).

Zu Buchstabe d

Im neuen Absatz 6 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.

Spiegelbildlich zu den Absätzen 1, 1a und 3 von § 100g StPO-E soll der neue Absatz 6 im ersten Halbsatz die neue Befugnis zur Sicherung von Verkehrsdaten definieren sowie im zweiten Halbsatz die materiellen Voraussetzungen für deren Anordnung auflisten.

Nach Halbsatz 1 können durch die Sicherungsanordnung sämtliche Anbieter öffentlich zugänglicher Telekommunikationsdienste für Endnutzer, bei denen es sich nicht um nummernunabhängige interpersonelle Telekommunikationsdienste (vergleiche § 3 Nummer 40 TKG) handelt, verpflichtet werden. Erfasst werden damit Anbieter von Internetzugangsdiensten, nummerngebundenen interpersonellen Telekommunikationsdiensten sowie von Diensten, die ganz oder überwiegend in der Übertragung von Signalen bestehen, wie Übertragungsdienste, die für Maschine-Maschine-Kommunikation und für den Rundfunk genutzt werden (vergleiche § 3 Nr. 61 TKG). Lediglich nummernunabhängige interpersonelle Telekommunikationsdienste, die weder eine Verbindung zu öffentlich zugeteilten Nummerierungsressourcen, nämlich Nummern nationaler oder internationaler Nummernpläne, herstellen noch die Telekommunikation mit Nummern nationaler oder internationaler Nummernpläne ermöglichen, sind vom Anwendungsbereich der Norm ausgeschlossen.

Halbsatz 2 von §100g Absatz 6 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 oder 1a 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 1b 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, 67. Auflage 2024 § 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, 1a oder 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 6 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 6 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 (vergleiche zu alledem: Köhler, in Meyer-Goßner/Schmitt, StPO, 67. Auflage 2024, § 94 Rz. 6; Hauschild, in Münchener Kommentar zur StPO, 2. Auflage 2023, § 94 Rz. 21, 22, 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, 1a oder 3 StPO-E nicht vorliegen werden.

Liegen die Voraussetzungen von § 100g Absatz 6 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 Anbieter öffentlich zugänglicher Telekommunikationsdienste, bei denen es sich nicht um nummernunabhängige interpersonelle Telekommunikationsdienste handelt, 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 nicht um nummernunabhängige interpersonelle Telekommunikationsdienste handelt. Im Vergleich zum Kreis der Verpflichteten der nunmehr dauerhaft unanwendbaren 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 TDDDG 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 TDDDG genannten Verkehrsdaten, welche die Anbieter von Telekommunikationsdiensten für betriebliche Zwecke – 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 und 1a StPO die (nachträglichen) Benachrichtigungs- und Rechtsschutzmöglichkeiten nach Maßgabe von § 101a Absatz 6 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 6 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 6 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 und 1a 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 6 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 6 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 (§ 100k)

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

Die Befugnis zur Erhebung von Nutzungsdaten bei Telemediendiensten nach dem Entwurf soll spiegelbildlich zur Befugnis nach § 100g Absatz 1 und 1a 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 Struktur von § 100g Absatz 1 StPO-E folgt (Befugnis in Halbsatz 1, nummerierte Anordnungsvoraussetzungen in Halbsatz 2). Für die Erhebung von Standortdaten werden, wie in § 100g Absatz 1a StPO-E, weiterhin gesonderte Regelungen in Absatz 1a getroffen, wobei für die Erhebung gespeicherter (retrograder) Standortdaten auf die Voraussetzungen des § 100g Absatz 1a 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 TDDDG bereits heute gestattet, Nutzungsdaten an die Strafverfolgungsbehörden zu übermitteln.

Die Änderungen in Absatz 2 und 4 betreffen redaktionelle Folgeänderungen, die mit der Aufteilung von Absatz 1 einhergehen; inhaltliche Änderungen sind damit nicht verbunden.

Zu Nummer 4 (§ 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, 1a 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 § 56 des Bundesdatenschutzgesetzes, der ebenfalls Artikel 13 Absatz 2 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.) umsetzt, zu berücksichtigen. Aufgrund der Aufnahme von Maßnahmen nach § 100g Absatz 6 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 5 (§ 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. In einem neu gefassten Absatz 1a sollen Verfahrensregelungen für das neue Ermittlungsinstrument der Sicherungsanordnung nach § 100g Absatz 6 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

§ 101a Absatz 1 StPO enthält Verweisungen auf die §§ 100a Absatz 3 und 4 sowie § 100e mit Maßgabebestimmungen. Im Anwendungsbereich wird klargestellt, dass diese Regelung nur für § 100g Absatz 1 bis 3 gilt, also nicht für die Sicherungsanordnung in Absatz 6 (siehe hierfür die Änderung unter Buchstabe b). Dass diese Klarstellung auch den dauerhaft nicht mehr anwendbaren § 100g Absatz 2 umfasst, ist allein redaktionell bedingt.

Die Verweisung auf § 100a Absatz 3, der die möglichen Betroffenen einer Anordnung betrifft, kann entfallen, ohne dass damit eine Änderung der Rechtslage verbunden ist. Denn § 100g Absatz 1 StPO-E enthält künftig selbst eine Regelung zu den möglichen Betroffenen einer Anordnung. Ansonsten soll die Regelung in Absatz 1, was 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 angefügte Nummer 3 des Absatzes aufgenommen werden soll.

Zu Buchstabe b

Im neuen Absatz 1a sollen im Wege der § 101a StPO eigenen Verweisungstechnik die Verfahrensregelungen für das neue Ermittlungsinstrument der Sicherungsanordnung von Verkehrsdaten nach § 100g Absatz 6 StPO-E geschaffen werden. Im Einzelnen:

Verweisungsziel § 100a Absatz 4 StPO: Dies bewirkt, dass die von einer Sicherungsanordnung betroffenen Anbieter von Telekommunikationsdiensten 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 4 und 5 dieses Entwurfs).

Verweisungsziel § 100e Absatz 1 StPO. Dies regelt zwei Aspekte:

Zum einen die Zuständigkeit. So darf infolge der Verweisung die Sicherungsanordnung nach § 100g Absatz 6 StPO-E nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden. 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 richterliche 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.).

Zum anderen die Befristung. Infolge der Verweisung auf § 100e Absatz 1 StPO muss die Sicherungsanordnung ausdrücklich befristet werden, 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, 1a 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 zwei Verlängerungsmöglichkeiten zu entnehmen ist).

Verweisungsziel § 100e Absatz 3 und 4 StPO: Danach gilt, dass auch für die Sicherungsanordnung nach § 100g Absatz 6 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.

Verweisungsziel § 100e Absatz 5 Satz 1 und 2 StPO: Danach sind die aufgrund der Sicherungsanordnung ergriffenen Maßnahmen unverzüglich zu beenden, 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 c

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

Zu Buchstabe d

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 e

Die Folgeänderung erfolgt aus denselben Gründen wie die vorstehende Änderung unter Nummer 6 Buchstabe d.

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 Nummer 6 (§ 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.

Die Änderung von § 101b Absatz 6 ist eine Folgeänderung zur Anpassung des § 100k; veränderte Rechtswirkungen sind damit nicht verbunden.

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 (vergleiche Artikel 2 dieses Entwurfs).

Zu Artikel 2 (Änderung des Einführungsgesetzes zur Strafprozessordnung)

Artikel 2 legt das Jahr fest, für das die geänderten Berichtspflichten nach Artikel 1 Nummer 6 erstmals Wirkung entfalten sollen.

Zu Artikel 3 (Änderung des Justizvergütungs- und -entschädigungsgesetzes)

In das Justizvergütungs- und Entschädigungsgesetz (JVEG) sollen Entschädigungsregelungen für diejenigen Leistungen aufgenommen werden, die von Telekommunikationsunternehmen im Zusammenhang mit Sicherungsanordnungen zu erbringen sind.

Die Ermäßigungsregelung nach Absatz 2 der Allgemeinen Vorbemerkung soll auch für den Fall der Sicherungsanordnung gelten. Zudem sind die Überschriften der Abschnitte 3 und 4 anzupassen.

Der vorgeschlagene neue Abschnitt 5 enthält Entschädigungsregelungen insbesondere für die Sicherung von Verkehrsdaten durch Telekommunikationsunternehmen. Die Tatbestände sowie die Entschädigungsbeträge orientieren sich an den jeweils korrespondierenden Vorschriften der Abschnitte 3 und 4 zur Entschädigung von Auskünften ohne vorhergehende Sicherungsanordnung.

Für die Auskunft über Daten, die aufgrund einer vorausgegangenen Sicherungsanordnung vom Telekommunikationsunternehmen gespeichert sind, wird im neuen Abschnitt 6 eine Entschädigung in Höhe von 20 Euro vorgeschlagen. Dabei wird davon ausgegangen, dass aufgrund der Vorbefassung im Rahmen der Umsetzung der Sicherungsanordnung der Aufwand für die spätere Beauskunftung dieser Daten vergleichsweise gering ist.

Zu Artikel 4 (Änderung des Telekommunikationsgesetzes)

§ 174a TKG-E enthält Vorgaben, die die Umsetzung einer Sicherungsanordnung durch die verpflichteten Anbieter von Telekommunikationsdiensten regeln.

§ 174a Absatz 1 TKG-E gibt vor, dass die verpflichteten Anbieter, die bei der Nutzung des Dienstes bereits erzeugten oder verarbeiteten und noch vorhandenen sowie künftig anfallenden Verkehrsdaten (§§ 9 und 12 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes) aufgrund einer Sicherungsanordnung unverzüglich zu sichern haben. Die Sicherung hat dadurch zu erfolgen, dass bereits gespeicherte Daten für die in der Sicherungsanordnung genannten Frist nicht gelöscht werden und künftig anfallende Daten gespeichert und für die in der Sicherungsanordnung genannten Frist nicht gelöscht werden. Die Speicherung hat – wie auch nach § 176 Absatz 7 TKG, der sich auf die dauerhaft unanwendbare Vorratsdatenspeicherung bezieht – so zu erfolgen, dass Übermittlungsersuchen von Strafverfolgungsbehörden unverzüglich nachgekommen werden kann. Zudem stellt Absatz 1 klar, dass der Inhalt der Kommunikation, Daten über aufgerufene Internetseiten und Daten von Diensten der elektronischen Post nicht gespeichert werden dürfen. Die Regelung entspricht insofern § 176 Absatz 5 TKG.

Nicht gespeichert werden dürfen – wie auch nach § 176 Absatz 6 TKG – ferner Daten, die den in § 11 Absatz 5 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes genannten Verbindungen zugrunde liegen, was § 174a Absatz 2 TKG-E klarstellt.

Nach § 174a Absatz 3 TKG-E hat der nach Absatz 1 Satz 1 Verpflichtete sicherzustellen, dass die aufgrund von Sicherungsanordnungen gesicherten Daten durch technische und organisatorische Maßnahmen nach dem Stand der Technik gegen unbefugte Kenntnisnahme und Verwendung geschützt werden. Die ergriffenen Schutzmaßnahmen sind im Sicherheitskonzept nach § 166 Absatz 1 Nummer 3 darzustellen. Die Speicherung und irreversible Löschung der Daten erfolgt nach Maßgabe der Rechtsverordnung nach § 170 Absatz 5 und der Technischen Richtlinie nach § 170 Absatz 6 TKG. § 175 Absatz 3 TKG-E gewährleistet somit, dass die Anforderungen an Datenschutz und Datensicherheit gewährleistet werden. Weitere Vorgaben für die Speicherung und die irreversible Löschung der Daten erfolgen in der Rechtsverordnung nach § 170 Absatz 5 TKG und der Technischen Richtlinie nach § 170 Absatz 6 TKG. Die Anforderungen an den Schutz der zu sichernden Daten bleiben damit bewusst hinter den Vorgaben zum Schutz und zur Sicherheit der §§ 176 bis 181 TKG zurück. 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 müssen für die Sicherungsanordnung – abgesehen von den zuvor genannten Vorschriften – nicht nachgebildet werden, da insoweit kein dauerhaft vorhandener Datenpool mit entsprechenden Gefahren missbräuchlicher Nutzung 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 zu betrieblichen Zwecken gespeicherten Verkehrsdaten sind im bisher geltenden Recht, insbesondere im TKG und im TDDDG, strenge Regelungen zu Datenschutz und Datensicherheit vorgesehen, die auch für die aufgrund der Sicherungsanordnung gespeicherten Daten gelten werden. Auch die sehr ausführlichen Bestimmungen der zu speichernden Daten (§ 176 TKG), sind nicht erforderlich, da die möglichen zu speichernden Verkehrsdaten durch die Verweisung in § 100g Absatz 1 Satz 1 StPO-E in den §§ 9 und 12 des TDDDG und § 2a Absatz 1 des BDBOS-Gesetzes abschließend definiert sind.

§ 174a Absatz 4 TKG-E enthält spezifische Übermittlungsbefugnisse und Verwendungsbefugnisse für Sicherungsanordnungen nach § 100g Absatz 6 StPO-E sowie ein Verwendungsverbot für andere Zwecke (vergleichbar § 177 TKG). Die Regelung stellt die nach der Rechtsprechung des Bundesverfassungsgerichts erforderliche zweite Tür zur Übermittlungsregelung der StPO – als der im Bild der Doppeltür ersten Tür – dar. Die Vorgaben zur Übermittlung der gesicherten Daten entsprechen im Wesentlichen denen des § 177 Absatz 3 TKG.

§ 174a Absatz 5 TKG-E enthält eine Löschverpflichtung für die Daten nach Ablauf der in der Sicherungsanordnung genannten Frist (vergleichbar § 176 Absatz 8 TKG).

Zu Artikel 5 (Änderung der Telekommunikations-Überwachungsverordnung)

Es handelt sich um Folgeänderungen zu gemäß Artikel 1 des Entwurfs vorgenommenen Änderungen in der Strafprozessordnung und zu gemäß Artikel 4 des Entwurfs vorgenommenen Änderungen im Telekommunikationsgesetz.

Zu Artikel 6 (Änderung des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes)

Mit der Änderung in § 9 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes (TDDDG) wird die Befugnis geschaffen, die es Anbietern von öffentlich zugänglichen Telekommunikationsdiensten ermöglicht, Verkehrsdaten zu verarbeiten, soweit dies für die Übermittlung von Verkehrsdaten nach § 174a Absatz 4 Satz 1 des Telekommunikationsgesetzes oder für eine Auskunft nach § 174a Absatz 1 Satz 3 des Telekommunikationsgesetzes erforderlich ist. Die Regelung ist erforderlich, denn einer entsprechenden Sicherungsanordnung folgt nicht automatisch eine Befugnis zur Datenverarbeitung durch die Diensteanbieter. Vielmehr regelt die Strafprozessordnung die Befugnisse der Strafverfolgungsbehörden, jedoch nicht die Befugnis der betroffenen Diensteanbieter. Insofern bedarf es einer klaren ergänzenden Regelung. § 9 Absatz 3 TDDDG-E und § 174a Absatz 4 TKG-E ermöglichen, dass der Diensteanbieter befugt ist, die Verkehrsdaten zu verarbeiten und an die Strafverfolgungsbehörden zu übermitteln. Die Regelung in § 9 Absatz 3 TDDDG entspricht darüber hinaus den Anforderungen des Artikels 15 Absatz 1 der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, die im TDDDG umgesetzt wird. Artikel 15 Absatz 1 der Richtlinie erlaubt den Mitgliedstaaten der Europäischen Union Rechtsvorschriften zur Beschränkung der Rechte und Pflichten der Richtlinie im Hinblick auf die Verarbeitung von Verkehrsdaten, soweit dies unter anderem für die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten verhältnismäßig ist.

Zu Artikel 7 (Einschränkung eines Grundrechts)

Die Vorschrift entspricht dem Zitiergebot, da das Grundrecht aus Artikel 10 GG durch die Regelungen in Artikel 1 und Artikel 4 eingeschränkt wird.

Zu Artikel 8 (Inkrafttreten)

Die Vorschrift regelt das Inkrafttreten.