Bundesrat **Drucksache** **263/1/26**

01.06.26

Empfehlungen
der Ausschüsse

R - DS - In

zu **Punkt ...** der 1066. Sitzung des Bundesrates am 12. Juni 2026

Entwurf eines Gesetzes zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren

A.

Der **federführende Rechtsausschuss** (R)

und der **Ausschuss für Innere Angelegenheiten** (In)

empfehlen dem Bundesrat,

zu dem Gesetzentwurf gemäß Artikel 76 Absatz 2 des Grundgesetzes wie folgt Stellung zu nehmen:

In 1. Zum Gesetzentwurf allgemein

Der Bundesrat begrüßt den vorliegenden Gesetzentwurf als einen wesentlichen Beitrag zur inneren Sicherheit.

Das neue Instrument der Sicherungsanordnung für künftig anfallende Verkehrsdaten sieht bislang nur den Zugriff der Strafverfolgungsbehörden des Bundes und der Länder vor. Zum Zwecke der Gefahrenabwehr sind ausschließlich das Bundeskriminalamt und die Bundespolizei vorgesehen. Dabei ist zu berücksichtigen, dass in erster Linie die Länder zur Gefahrenabwehr und insbesondere zur Verhütung von Straftaten zuständig sind.

Daher bittet der Bundesrat, die sogenannte erste Tür der vorgesehenen Siche-

...

Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln
Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.bundesanzeiger-verlag.de
ISSN 0720-2946

rungsanordnung auch für die Gefahrenabwehrbehörden sowie die Verfassungsschutzbehörden der Länder zu öffnen.

Begründung:

Die Rolle der Länder bei der Gefahrenabwehr wird in dem vorliegenden Gesetzentwurf nicht ausreichend berücksichtigt. So sind in erster Linie die Gefahrenabwehrbehörden der Länder für das Verhüten von Straftaten zuständig. Demgegenüber öffnet der Gesetzentwurf bislang nicht die sogenannte erste Tür der vorgesehenen Sicherungsanordnung für die Gefahrenabwehr- und Verfassungsschutzbehörden der Länder.

Der Gesetzgeber muss nach dem Bild einer Doppeltür sowohl für die Übermittlung der Daten durch die Anbieter von Telekommunikationsdiensten als auch für den Abruf dieser Daten durch die Behörden jeweils Rechtsgrundlagen schaffen (vgl. BVerfG Beschluss vom 27. Mai 2020 – 1 BvR 1873/13, 1 BvR 2618/13 – Bestandsdatenauskunft II). Bislang sieht der Entwurf die Übermittlungsbefugnis als erste Tür bei der Sicherungsanordnung nur strafprozessual und zum Zwecke der Gefahrenabwehr ausschließlich für Übermittlungen an das Bundeskriminalamt sowie die Bundespolizei vor. Insoweit liefen Abrufregelungen der Länder für ihre Polizei- und Verfassungsschutzbehörden nach der Rechtsprechung ins Leere.

In 2. Zum Gesetzentwurf allgemein

Der Bundesrat begrüßt den vorliegenden Gesetzentwurf als einen wesentlichen Beitrag zur inneren Sicherheit.

Mit dem Konzept der Mindestspeicherfristen für Verkehrsdaten zur Bekämpfung von Straftaten im Internet allein zur Anschlussinhaberfeststellung anhand einer dynamischen IP-Adresse setzt die Bundesregierung das nach der Rechtsprechung des EuGHs zwingende Mindestmaß um. Denn andernfalls bestünde „eine echte Gefahr der systemischen Straflosigkeit“ (EuGH Urteil vom 30. April 2024, Az. C-470/21 – Hadopi, Rn. 119).

Der Entwurf beschränkt sich im Wesentlichen auf das Instrument der Sicherungsanordnung („Quick Freeze“) sowie die Speicherung von IP-Adressen zur Anschlussinhaberfeststellung. Der Bundesrat weist darauf hin, dass der EuGH unter engen Voraussetzungen auch weitergehende Formen einer Vorratsdatenregelung insbesondere zum Schutz der nationalen Sicherheit sowie zur Bekämpfung schwerer Kriminalität weiterhin für zulässig erachtet. Ferner beruhen die derzeitigen Speichererfordernisse maßgeblich auf der dynamischen Vergabe

von IP-Adressen. Vor dem Hintergrund technischer Entwicklungen können künftig auch alternative Ansätze zur verbesserten Zuordenbarkeit internetbasierter Kommunikation in Betracht kommen.

Begründung:

Der Gesetzentwurf nutzt nicht den vom EuGH insbesondere zum Schutz der nationalen Sicherheit und unter weiteren Bedingungen zur Bekämpfung schwerer Kriminalität eröffneten Raum für eine Vorratsdatenregelung. So können selbst in diesen Fällen künftig weder Strafverfolgungs- noch Polizei- oder Verfassungsschutzbehörden auf retrograde Verkehrs- und Standortdaten zugreifen.

Der Entwurf hat den ursprünglichen Ansatz der retrograden Verkehrsdaten in Gänze verworfen. Lediglich zur Identifikation eines Anschlussinhabers anhand einer dynamischen IP-Adresse sind Verkehrsdaten nach dem Entwurf von den Anbietern von Telekommunikation auf Vorrat zu speichern.

Die derzeit bestehenden Speichererfordernisse beruhen maßgeblich darauf, dass IP-Adressen vielfach nur dynamisch und zeitlich begrenzt vergeben werden. Vor dem Hintergrund technischer Entwicklungen erscheint es angezeigt, auch alternative Ansätze zur verbesserten Zuordenbarkeit internetbasierter Kommunikation in den Blick zu nehmen, um eine effektive Strafverfolgung und Gefahrenabwehr auch unter veränderten technischen Rahmenbedingungen dauerhaft zu gewährleisten.

In bei Annahme entfällt Ziffer 5

3. Zu Artikel 6 Nummer 2 (§ 176 TKG)*

Der Bundesrat bittet, § 176 TKG-E nach dem Vorbild des bestehenden § 174 Absatz 3 TKG so auszugestalten, dass die Erbringer öffentlich zugänglicher Telekommunikationsdienste über die Fälle des künftigen § 100g Absatz 7 StPO hinaus nicht nur zur Erfüllung von Sicherungsanordnungen des Bundeskriminalamts und der Bundespolizei verpflichtet werden, sondern zur Erfüllung von Sicherungsanordnungen aller in § 174 Absatz 3 TKG aufgezählten Sicherheitsbehörden des Bundes und der Länder, einschließlich der Nachrichtendienste. Dabei sind auch die maßgeblichen Rechtsgüterschwellen im Einzelnen anzugeben oder durch Verweisung auf § 174 Absatz 3 TKG in Bezug zu nehmen.

Begründung:

Mit dem vorgelegten Gesetzentwurf wird unter anderem das neue Instrument der Sicherungsanordnung für Verkehrsdaten eingeführt. Dieses bietet die Mög-

* Aufgrund einer Konkurrenz zu Ziffer 5 wird diese Ziffer vorgezogen.

lichkeit, anlassbezogen mittels einer Anordnung gegenüber Telekommunikationsdiensteanbietern die Sicherung von Verkehrsdaten zu veranlassen, sofern und solange die rechtlichen oder tatsächlichen Voraussetzungen einer Datenerhebung noch nicht vorliegen.

Die Sicherungsanordnung bedarf nach dem vom Bundesverfassungsgericht entwickelten Doppeltür-Prinzip zweier korrespondierender Rechtsgrundlagen, vgl. BVerfG, Beschluss vom 27. Mai 2020, Az.: 1 BvR 1873/13, 1 BvR 2618/13 (Bestandsdatenauskunft II). Zum einen auf Seiten der anordnenden Behörde: Hier sollen seitens des Bundesgesetzgebers entsprechende Rechtsgrundlagen bisher nur für die Strafverfolgung in § 100g Absatz 7 StPO-E (vgl. BR-Drucksache 263/26), für das BKA in § 10b BKAG-E (vgl. BR-Drucksache 259/26 - Zentralstellenfunktion), in § 52 Absatz 3 BKAG-E (vgl. BR-Drucksache 259/26 - Gefahrenabwehr Internationaler Terrorismus) sowie für die Bundespolizei nach § 25a Absatz 1 BPolG-E (vgl. BR-Drucksache 263/26) geschaffen werden. Zum anderen bedarf es einer korrespondierenden Verarbeitungsbefugnis mit strikter Zweckbindung für die Anbieter öffentlich zugänglicher Telekommunikationsdienste. Diese wurde mit vorliegendem Entwurf in § 176 TKG-E geschaffen.

Allerdings beschränkt der aktuell vorliegende Entwurf von § 176 TKG-E die Befugnis und Pflicht zur erforderlichen Datensicherung ausdrücklich auf die in § 176 Absatz 1 Satz 1 Nummern 1 bis 3 TKG-E abschließend benannten Rechtsgrundlagen für Sicherungsanordnungen in der StPO, dem BKAG sowie dem BPolG und schließt folglich sämtliche anderen Sicherheitsbehörden von der Nutzung dieses wichtigen Ermittlungsinstruments aus.

Ausgeschlossen sind somit sämtliche weitere Sicherheits- und Gefahrenabwehrbehörden des Bundes und der Länder, wie sie – abgesehen von den Strafverfolgungsbehörden – im bestehenden § 174 Absatz 3 Nummer 1 bis 8 TKG aufgezählt sind. Zuvorderst sind dabei die für die Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung zuständigen Behörden, mithin also vor allem die Polizeien der Länder, aber zum Beispiel auch das Zollkriminalamt als Zentralstelle im Sinn des Zollfahndungsdienstgesetzes, die Nachrichtendienste des Bundes und der Länder oder das Bundesamt für Sicherheit in der Informationstechnik zu nennen.

Selbst bei Schaffung von Befugnissen zu Sicherungsanordnungen in den Polizeigesetzen der Länder oder den Verfassungsschutzgesetzen (zweite Tür) liefen diese ins Leere, da es aufgrund der Beschränkung in § 176 TKG-E (erste Tür) an der korrespondierenden Datenverarbeitungsbefugnis der Diensteanbieter fehlt.

Die Gefahrenabwehr ist jedoch im deutschen Verfassungsrecht primär Aufgabe der Länder und es sind vor allem die Landespolizeien, die originär Aufgaben im Rahmen der Terrorismusabwehr wahrnehmen und Rechtsgüter von vergleichbar hohem verfassungsrechtlichem Gewicht schützen. Auch die Nachrichtendienste nehmen Aufgaben im Bereich der Terrorismusabwehr wahr und schützen gleichermaßen Rechtsgüter von hohem verfassungsrechtlichem Gewicht.

Darüber hinaus sind neben den namentlich zu nennenden Behörden in § 176 TKG-E auch die für einen Datenabruf maßgeblichen Rechtsgüter im Einzelnen

aufzuzählen (Ausgestaltung der ersten Tür), wie es jetzt bereits in § 174 Absatz 3 TKG vorgezeichnet ist. Die Norm wurde im Jahr 2021 im Vermittlungsausschuss zwischen Bund und Ländern erarbeitet und kann hier als Vorbild dienen.

Abstrakte Beschreibungen wie z. B. „bedeutende Rechtsgüter“ sind dabei nicht ausreichend, da der Gesetzgeber für die zweite Tür ebenfalls gehalten ist, die Rechtsgüter möglichst normenklar konkret zu benennen, damit Dritte, wie z. B. die Telekommunikationsanbieter, diese Regelungen auch rechtssicher vollziehen können. Auch der Aufwand bei den Ländern würde deutlich reduziert werden, sodass eine schnellere und gleichermaßen rechtskonforme Umsetzung gewährleistet werden könnte.

Die Rechtsgüter sind folglich – abhängig vom Einzelfall – möglichst konkret zu benennen, wie z. B. „zum Schutz von Leib, Leben, Freiheit, des Bestands des Bundes und der Länder, Gütern der Allgemeinheit, deren Bedrohung die Existenz der Menschen berührt“, usw. oder „zur Verhütung einer schweren Straftat nach § 100a Absatz 2 StPO“. Nur so ist sichergestellt, dass Bund und Länder spiegelbildliche und deckungsgleiche Regelungen in Form einer zweiten Tür schaffen können.

Das könnte regelungstechnisch einfach durch eine Verweisung in § 176 Absatz 1 Satz 1 TKG-E auf § 174 Absatz 3 TKG umgesetzt und beispielsweise wie folgt formuliert werden:

„Wer öffentlich zugängliche Telekommunikationsdienste erbringt oder daran mitwirkt, darf unter den in § 174 Absatz 3 genannten Voraussetzungen Verkehrsdaten verarbeiten, soweit dies zur Erfüllung der Sicherungsanordnung einer dort genannten Behörde erforderlich ist.“

Alternativ könnten Behörden nebst den jeweiligen Eingriffsschwellen parallel zu § 174 Absatz 3 TKG einzeln aufgezählt werden.

R 4. Zu Artikel 1 Nummer 1a – neu – (§ 95b – neu – StPO), 2 (§ 100g Absatz 7 StPO), 4 (§ 101a Absatz 1 Satz 1 Nummer 3, Absatz 2 StPO), 5 Buchstabe b Doppelbuchstabe aa, bb (§ 101b Absatz 5 Nummer 1, 2 Buchstabe e StPO), Artikel 6 Nummer 2 (§ 176 Absatz 1 Satz 1, 1 Nummer 4 – neu –, Satz 2, 4 – neu – TKG), Artikel 8 Nummer 2 – neu – (§ 24b – neu – TDDDG)

a) Artikel 1 ist wie folgt zu ändern:

aa) Nach Nummer 1 ist die folgende Nummer 1a einzufügen:

‚1a. Nach § 95a wird der folgende § 95b eingefügt:

„§ 95b

Sicherungsanordnung

(1) Zum Zwecke einer Erhebung von Daten im Sinne von Absatz 2 nach anderen Vorschriften dieses Gesetzes darf angeordnet werden, dass Verpflichtete Daten unverzüglich zu sichern haben (Sicherungsanordnung),

1. wenn zureichende tatsächliche Anhaltspunkte dafür vorliegen, dass eine Straftat begangen worden ist, welche die Erhebung nach anderen Vorschriften rechtfertigen würde, und
2. soweit die Daten für die in den anderen Vorschriften jeweils genannten Zwecke von Bedeutung sein können.

Soweit sich eine Sicherungsanordnung auf Daten gemäß Absatz 2 Nummern 3 oder 4 bezieht, können diese erhoben werden, wenn die betroffene Person in einem persönlichen oder räumlichen Bezug zu der Straftat nach Satz 1 Nummer 1 steht. Die Erhebung der nach Satz 1 gesicherten Daten erfolgt nach anderen Vorschriften dieses Gesetzes.

(2) Daten im Sinne des Absatzes 1 sind

1. Bestandsdaten gemäß § 3 Nummer 6 und Daten nach § 172 des Telekommunikationsgesetzes,
2. Bestandsdaten gemäß § 2 Absatz 2 Nummer 2 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes,
3. Verkehrsdaten gemäß § 3 Nummer 70 des Telekommunikationsgesetzes,

4. Nutzungsdaten gemäß § 2 Absatz 2 Nummer 3 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes sowie

5. alle weiteren Daten in einem digitalen Format wie Text, Sprache, Videos, Bilder und Tonaufzeichnungen, die nicht von Ziffer 1. bis 4. erfasst werden (Inhaltsdaten).

(3) § 100e Absatz 1, 3 Satz 1 und 2 Nummer 1 bis 5 und Absatz 5 Satz 1 und 2 gilt entsprechend mit der Maßgabe, dass

1. abweichend von § 100e Absatz 1 Satz 1 bis 3 die Maßnahme durch die Staatsanwaltschaft für höchstens drei Monate angeordnet werden kann, bei Gefahr im Verzug auch durch ihre Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes), und die Maßnahme nur auf Antrag der Staatsanwaltschaft durch das Gericht um höchstens drei Monate verlängert werden kann,

2. in der Entscheidungsformel nach § 100e Absatz 3 Satz 2 auch die zu sichernden Daten und der Zeitraum, für den sie gesichert werden sollen, eindeutig anzugeben sind.“‘

bb) Nummer 2 § 100g Absatz 7 ist zu streichen.

cc) Nummer 4 § 101a ist wie folgt zu ändern:

aaa) Absatz 1 Satz 1 Nummer 3 ist zu streichen.

bbb) In Absatz 2 ist die Angabe „oder 7“ zu streichen.

dd) Nummer 5 Buchstabe b ist wie folgt zu ändern:

aaa) In Doppelbuchstabe aa ist die Angabe „1,2, 3, 4 und 7“ durch die Angabe „1, 2, 3 und 4“ zu ersetzen.

bbb) Doppelbuchstabe bb Dreifachbuchstabe aaa ist durch den folgenden Dreifachbuchstaben aaa zu ersetzen:

‚aaa) Nach Buchstabe c wird der folgende Buchstabe d eingefügt:

„d) die Anzahl der Anordnungen nach § 100g Absatz 4;“‘

b) Artikel 6 Nummer 2 § 176 ist wie folgt zu ändern:

aa) In der Überschrift ist die Angabe „Verkehrsdaten“ durch die Angabe „Bestands-, Verkehrs- und Inhaltsdaten“ zu ersetzen.

bb) Absatz 1 ist wie folgt zu ändern:

aaa) Satz 1 ist wie folgt zu ändern:

aaaa) Die Angabe „Verkehrsdaten“ ist durch die Angabe „Bestands-, Verkehrs- und Inhaltsdaten“ und die Angabe „100g Absatz 7“ durch die Angabe „95b Absatz 1“ zu ersetzen.

{R} = 5. entfällt bei Annahme von Ziffer 4

{bbbb) Nach Nummer 3 die folgende Nummer 4 einzufügen:

„4. einer auf Verkehrsdaten bezogenen Sicherungsanordnung der in § 174 Absatz 3 Nummern 2 und 5 genannten Behörden und unter den dort genannten Voraussetzungen.“}

bbb) In Satz 2 ist die Angabe „Verkehrsdaten“ durch die Angabe „Bestands-, Verkehrs- und Inhaltsdaten“ zu ersetzen und die Angabe „und unter den Voraussetzungen des § 175 beauskunftet“ zu streichen.

ccc) Nach Satz 3 ist der folgende Satz anzufügen:

„Eine Sicherung nach Absatz 1 Satz 1 Nummer 4 ist auf Anordnung der jeweiligen Behördenleitung oder ihrer Vertretung auf höchstens drei Monate zu beschränken und bedarf im Fall der Verlängerung um höchstens drei Monate einer richterlichen Anordnung.“

cc) In Absatz 2 ist die Angabe „Verkehrsdaten“ durch die Angabe „Daten“ zu ersetzen.

dd) In Absatz 4 Satz 1 ist die Angabe „Verkehrsdaten“ durch die Angabe „Daten“ zu ersetzen.

c) Artikel 8 ist durch den folgenden Artikel 8 zu ersetzen:

‚Artikel 8

Änderung des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes

Das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz vom 23. Juni 2021 (BGBl. I S. 1982; 2022 I S. 1045), das zuletzt durch Artikel 3 des Gesetzes vom 10. März 2026 (BGBl. 2026 I Nr. 64) geändert worden ist, wird wie folgt geändert:

1. § 13 wird durch den <<… weiter wie Vorlage …>>.

2. Nach § 24a wird der folgende § 24b eingefügt:

„§ 24b

Befugnis zur Verarbeitung von Bestands-, Nutzungs- und Inhaltsdaten zur Erfüllung von Sicherungsanordnungen

(1) Wer geschäftsmäßig digitale Dienste erbringt, daran mitwirkt oder den Zugang zur Nutzung daran vermittelt, darf Bestands-, Nutzungs- und Inhaltsdaten verwenden, soweit dies erforderlich ist

1. zur Erfüllung einer Sicherungsanordnung nach § 95b Absatz 1 der Strafprozessordnung,

2. zur Sicherung einer auf Nutzungsdaten bezogenen Auskunftspflicht nach § 24 Absatz 1 Satz 1, Absatz 3 Nummern 2 und 5.

Für die Erfüllung der Sicherungsanordnung sind sämtliche unternehmensinternen Datenquellen zu berücksichtigen.

(2) Auf die Verwendung der Daten zur Erfüllung von Sicherungsanordnungen nach Absatz 1 Satz 1 finden § 24 Absätze 2, 4 und 5 sowie § 176 Absatz 2 des Telekommunikationsgesetzes entsprechend Anwendung. Eine Sicherung nach Absatz 1 Satz 1 Nummer 2 ist auf Anordnung der jeweiligen Behördenleitung oder ihrer Vertretung auf höchstens drei Monate zu beschränken und bedarf im Fall der Verlängerung um höchstens drei Monate einer richterlichen Anordnung.“‘

Folgeänderung:

In Artikel 1 Nummer 1 ist vor Buchstabe a der folgende Buchstabe a_0 einzufügen:

‚a_0) Nach der Angabe zu § 95a ist die folgende Angabe einzufügen:

„§ 95 b Sicherungsanordnung“‘

Begründung:

Zu Artikel 1 Nummer 1a:

Die in § 100g Absatz 7 StPO-E vorgesehene Einführung einer auf die Sicherung von Verkehrsdaten beschränkten Sicherungsanordnung wird den Erfordernissen der Verordnung (EU) 2023/1543 (E-Evidence-VO) nicht gerecht, da diese zum 18. August 2026 das korrespondierende grenzüberschreitende Ermittlungsinstrument der Europäischen Sicherungsanordnung für sämtliche Datenkategorien einführt. Voraussetzung für den Erlass einer Europäischen Sicherungsanordnung ist dabei, dass sie in einem vergleichbaren nationalen Fall unter denselben Voraussetzungen hätte erlassen werden können (Artikel 6 Absatz 3 E-Evidence-VO). Im Hinblick auf Bestandsdaten, Nutzungsdaten und Inhaltsdaten wären deutsche Behörden deswegen angesichts der Beschränkung der Neuregelung auf Verkehrsdaten am Erlass von Europäischen Sicherungsanordnungen gehindert. Zudem würde die nicht hinnehmbare Situation entstehen, dass Strafverfolgungsbehörden aus anderen Mitgliedstaaten gegenüber in Deutschland ansässigen Diensteanbietern weitergehende Befugnisse hätten als die inländischen deutschen Strafverfolgungsbehörden.

Deswegen wird mit dem neu einzufügenden § 95b StPO-E eine Rechtsgrundlage für die Sicherungsanordnung geschaffen, die alle Datenkategorien umfasst. Die Norm ist inhaltlich im Übrigen entsprechend der im Regierungsentwurf in § 100g Absatz 7 StPO-E vorgesehenen Regelung ausgestaltet. Auch die Beschränkung auf Daten betroffener Personen wird in § 95b Absatz 1 Satz 2 StPO-E übernommen, allerdings nur, sofern eine Sicherungsanordnung Verkehrs- oder Nutzungsdaten betrifft, da andernfalls hinsichtlich der übrigen Datenkategorien die bloße Sicherung von Daten strengeren Voraussetzungen unterliegen würde als die Erhebung derselben Daten.

Die in § 95b Absatz 2 Nummer 5 StPO-E vorgesehene Legaldefinition der Inhaltsdaten entspricht der in Artikel 3 Nummer 12 E-Evidence-VO für Inhaltsdaten vorgesehenen Definition.

Zu Artikel 1 Nummern 2 und 4:

Da der Regelungsgehalt von §§ 100g Absatz 7, 101a Absatz 1 Satz 1 Nummer 3 StPO-E von § 95b StPO-E mitumfasst ist, können § 100g Absatz 7 StPO-E und die sich darauf beziehenden Regelungen in §§ 101a und 101b StPO-E gestrichen werden.

Zu Artikel 1 Nummer 5:

Eine Berücksichtigung von bloßen Datensicherungen ist im Rahmen der auf

Datenerhebungen ausgerichteten Berichtspflichten nach § 101 b StPO nicht erforderlich.

Zu Artikel 6:

Nach der Rechtsprechung des BVerfG zum sog. „Doppeltürmodell (s. dazu Begründung zum RegE S. 61) muss die im Antrag durch die Einfügung von § 95b StPO-E vorgesehene Erweiterung der Sicherungsanordnung sowohl in TKG und TDDDG durch entsprechende Verwendungsbefugnisse ergänzt werden, die es den Diensteanbietern ermöglichen, Sicherungsanordnungen auch dann zu erfüllen, wenn andere Daten als Verkehrsdaten gesichert werden sollen.

Die Änderungen erweitern daher die in § 176 TKG-E für Telekommunikationsanbieter vorgesehene Verwendungsbefugnis entsprechend auf die Sicherung anderer Daten als Verkehrsdaten.

{Zudem erfolgt durch die Anpassung eine Erweiterung der Verwendungsbefugnis auf in Landespolizei- sowie in Landesverfassungsschutzgesetzen geregelte Sicherungsanordnungen bezüglich Verkehrsdaten. Für Sicherungsanordnungen bezüglich weiterer Datenkategorien wird hinsichtlich der genannten Stellen kein praktisches Bedürfnis gesehen, so dass auch die Verwendungsbefugnis insoweit auf Verkehrsdaten beschränkt bleiben kann.}

Zu Artikel 8:

Nach der Rechtsprechung des BVerfG zum sog. „Doppeltürmodell (s. dazu Begründung zum RegE S. 61) muss die im Antrag durch die Einfügung von § 95b StPO-E vorgesehene Erweiterung der Sicherungsanordnung sowohl im TKG als auch im TDDDG durch entsprechende Verwendungsbefugnisse ergänzt werden, die es den Diensteanbietern ermöglichen, Sicherungsanordnungen auch dann zu erfüllen, wenn andere Daten als Verkehrsdaten gesichert werden sollen.

Da das TDDDG bisher keine Verwendungsbefugnis für die Erfüllung von Sicherungsanordnungen durch Anbieter digitaler Dienste enthält, ist dazu ein neuer § 24b TDDDG einzufügen. Die Verweisungen in Absatz 2 stellen einen Gleichlauf der Regelung mit der Parallelnorm des § 176 TKG-E her. Es kann zu diesem Zweck größtenteils auf bereits in der Verwendungsbefugnis für Auskunftsersuchen zu Nutzungsdaten in § 24 TDDDG enthaltene Regelungen Bezug genommen werden. § 24 Absatz 3 TDDDG ist dabei von der Verweisung ausgenommen, da die dort normierten Einschränkungen der Verwendungsbefugnis für die Verwendung zur bloßen Datensicherung nicht erforderlich sind. Da eine entsprechende Norm im TDDDG nicht existiert, muss für die erforderlichen Sicherheitsvorgaben auf § 176 Absatz 2 TKG verwiesen werden.

Durch die Regelung in Absatz 1 Satz 1 Nummer 2 und Absatz 2 Satz 2 erfolgt eine Erweiterung der Verwendungsbefugnis auf in Landespolizei- sowie Landesverfassungsschutzgesetzen geregelte Sicherungsanordnungen bezüglich Nutzungsdaten. Für Sicherungsanordnungen bezüglich weiterer Datenkategorien wird hinsichtlich der genannten Stellen kein praktisches Bedürfnis gesehen, so dass auch die Verwendungsbefugnis insoweit auf Nutzungsdaten beschränkt bleiben kann.

In 6. Zu Artikel 6 Nummer 2 (§ 175 Absatz 3 Nummer 2, Absatz 4 TKG)

Artikel 6 Nummer 2 § 175 ist wie folgt zu ändern:

a) Absatz 3 Nummer 2 ist durch die folgende Nummer 2 zu ersetzen:

„2. eine für die Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung zuständige Behörde, soweit dies auf richterliche Anordnung im Einzelfall zur Abwehr einer Gefahr oder konkretisierten Gefahr für Leib, Leben, Freiheit der Person, die sexuelle Selbstbestimmung, den Bestand und die Sicherheit des Bundes oder eines Landes, sowie Güter der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt, erforderlich ist,“

b) In Absatz 4 ist die Angabe „Satz 2“ zu streichen.

Begründung:

Zu Buchstabe a:

Mit dem vorgelegten Gesetzentwurf wird unter anderem die Verarbeitung von Verkehrsdaten durch Telekommunikationsanbieter sowie die Auskunftserteilung an Behörden in § 175 TKG-E neu geregelt.

Die Übermittlung und der Abruf von Verkehrsdaten bedarf nach dem vom Bundesverfassungsgericht entwickelten Doppeltür-Prinzip zweier korrespondierender Rechtsgrundlagen, vgl. BVerfG, Beschluss vom 27.Mai 2020, Az.: 1 BvR 1873/13, 1 BvR 2618/13 (Bestandsdatenauskunft II). Zum einen auf Seiten des Gesetzgebers für die erste Tür (Übermittlung): Hier ist bislang in § 175 Absatz 3 Nummer 2 TKG-E vorgesehen, dass eine Auskunft an die Gefahrenabwehrbehörden der Länder zulässig sein soll, soweit dies im Einzelfall erforderlich ist zur Abwehr einer konkretisierten Gefahr von zumindest erheblichem Gewicht oder zur Abwehr einer konkreten Gefahr für die öffentliche Sicherheit. Das Rechtsgut der öffentlichen Sicherheit ist soweit ausreichend konkret formuliert und zweckmäßig ausgestaltet. Hingegen ist ein „Rechtsgut von zumindest erheblichem Gewicht“ zu unbestimmt und zu unspezifisch, weil die Gesetzgeber für die zweite Tür, etwa die Länder für die Abrufregelungen in den Ländergesetzen, ihrerseits gehalten sind, konkrete Rechtsgüter normenklar zu benennen, damit Dritte, wie z. B. die Telekommunikationsanbieter, diese Regelungen auch rechtssicher vollziehen können.

Die für eine Datenübermittlung bzw. einen Datenabruf maßgeblichen Rechtsgüter sind im Einzelnen aufzuzählen (Ausgestaltung der ersten Tür), wie es jetzt bereits in § 174 Absatz 3 Nummer 2 TKG vorgezeichnet ist. Die Norm wurde im Jahr 2021 im Vermittlungsausschuss zwischen Bund und Ländern erarbeitet und kann hier als Vorbild dienen.

Die Rechtsgüter sind folglich – abhängig vom Einzelfall – möglichst konkret zu benennen, wie z. B. „zum Schutz von Leib, Leben, Freiheit, dem Bestand

des Bundes und der Länder, Gütern der Allgemeinheit, deren Bedrohung die Existenz der Menschen berührt“ usw. oder „zur Verhütung einer schweren Straftat nach § 100a Absatz 2 StPO“. Nur so ist sichergestellt, dass Bund und Länder spiegelbildliche und deckungsgleiche Regelungen in Form einer zweiten Tür schaffen können.

Zu Buchstabe b:

Die Streichung der Angabe „Satz 2“ dient dazu auf den vollständigen § 174 Absatz 6 TKG zu verweisen, sodass dessen Satz 1 auch zur Anwendung kommt. Dort ist die Pflicht der Diensteanbieter geregelt, dass die zu beauskunftenden Daten unverzüglich und vollständig zu übermitteln sind.

In 7. Zu Artikel 6 Nummer 2 (§ 177 Absatz 1 Satz 2 TKG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob die Daten nach § 177 Absatz 1 Satz 1 TKG-E bis zu sechs Monate gespeichert werden können.

Die Einführung einer Speicherfrist von drei Monaten nach § 177 Absatz 1 Satz 2 TKG-E würde zwar für die seit Jahren bestehenden Ermittlungseinschränkungen und insbesondere für die Bekämpfung des sexuellen Missbrauchs von Kindern und Jugendlichen (sMvKJ) sowie der Verbreitung der Darstellung des sMvKJ (DsMvK/J) eine dringend notwendige und für sich schon deutlich zu befürwortende Verbesserung bedeuten. Aus polizeifachlicher Sicht ist jedoch eine Speicherfrist von mindestens sechs Monaten anzustreben, um darüber hinaus auch die Erfolgschancen in der polizeilichen Ermittlungspraxis im Zusammenhang mit internetbasierter Kriminalität wirksam zu erhöhen.

Begründung:

Auch die Innenminister und -senatoren der Länder sehen die zeitnahe Umsetzung der fachlichen Empfehlung der Speicherung spezifischer Daten zur Anschlussidentifizierung für einen Zeitraum von mindestens sechs Monaten durch die Telekommunikationsprovider (TP) sowie die Verpflichtung der Serviceprovider (SP) zur Sicherung bzw. Speicherung von entsprechenden Identifizierungsdaten als erforderlich an.

Grundlage hierfür waren die polizeifachlichen Feststellungen und Empfehlungen im Abschlussbericht der Bund-Länder-Projektgruppe (BLPG) „Kampf gegen Kindesmissbrauch und Kinderpornografie intensivieren – Sicherungsmechanismen und -zeiträume von IP-Adressen“ (Stand: 20. Januar 2023). In der durch das Land Hessen geleiteten polizeilichen Projektgruppe wirkten neben dem BKA die Länder Baden-Württemberg, Bayern, Niedersachsen, Nordrhein-Westfalen sowie Schleswig-Holstein mit.

Die BLPG stellte in diesem Zusammenhang in ihrem Abschlussbericht fest, dass sich in den auf die initiale NCMEC-Befassung folgenden weiteren Ermittlungen regelmäßig Sicherstellungen von IT-Asservaten ergeben. Deren forensische Auswertung bleibt zeitaufwändig. Sollten dabei weitere strafbare Inhalte festgestellt werden, führt dies zur Einleitung von Folgeverfahren und zu möglicherweise noch unbekannten Tätern. Auch hier kann dann eine übermittelte IP-Adresse der einzige Anhaltspunkt zur Ermittlung eines Täters sein. Insbesondere wenn eine Auswertung von IT-Asservaten auf ein Netzwerk von Personen mit entsprechender sexueller Neigung hinweist, ist die Anschlussidentifizierung aufgrund eines möglichen Gefahrenüberhanges von erheblicher Bedeutung.

Die BLPG empfahl im Hinblick auf strafrechtlich relevante Inhalte, die den Ermittlungsbehörden erst nach mehreren Monaten oder Jahren bekannt werden, dass der absolut notwendige Sicherungszeitraum weitaus länger sein müsse, und eine möglichst grundrechtsschonende Regelung, alle Telekommunikationsprovider zur Speicherung von spezifischen Daten zur Anschlussidentifizierung für einen Zeitraum von mindestens sechs Monaten verpflichten solle.

Insgesamt ist die IP-Adresse als digitale Spur von Bedeutung, um den Ermittlungsbehörden im Zusammenhang mit kriminellen Aktivitäten eindeutig natürliche Personen den von ihnen genutzten technischen Endgeräten zuzuordnen. Dies ist auch im Kontext verschlüsselter Kommunikation im Bereich organisierter Rauschgiftkriminalität (z. B. Nutzung von EncroChat-ähnlichen Plattformen) von zentraler Bedeutung. Darüber hinaus können durch die Auswertung gespeicherter IP-Adressen bisher nicht identifizierte Nutzerkreise in kriminellen Infrastrukturen (z. B. Darknet-Marktplätze, Logistiknetzwerke für Rauschgifthandel) identifiziert und einer strafrechtlichen Bewertung zugeführt werden. Dies stellt ein unverzichtbares Instrument zur Bekämpfung krimineller Strukturen dar. Die rechtssichere Dokumentation und Nachverfolgung der IP-Nutzung in zeitlicher und technischer Hinsicht trägt zur Erhöhung der Beweisqualität und zur gerichtsfesten Feststellung von Tatnachweisen bei. Dies ist insbesondere bei komplexen Tatstrukturen mit internationalem Bezug von entscheidender Bedeutung.

B.

8. Der **Ausschuss für Digitales und Staatsmodernisierung**

empfiehlt dem Bundesrat,

gegen den Gesetzentwurf gemäß Artikel 76 Absatz 2 des Grundgesetzes keine Einwendungen zu erheben.