Bundesrat **Drucksache** **163/1/21**

15.03.21

Empfehlungen
der Ausschüsse

Wi - AV - G - In - K - R

zu **Punkt …** der 1002. Sitzung des Bundesrates am 26. März 2021

Entwurf eines Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien

A

Der **federführende Wirtschaftsausschuss** (Wi),

der **Ausschuss für Agrarpolitik und Verbraucherschutz** (AV),

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

der **Ausschuss für Kulturfragen** (K) und

der **Rechtsausschuss** (R)

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

In 1. Zu Artikel 1 (§ 1 Absatz 3 Satz 3 – neu – TTDSG)

Dem Artikel 1 § 1 Absatz 3 ist folgender Satz anzufügen:

„Die Länder sind befugt, für die Datenverarbeitung bei der Bereitstellung von Telemedien durch ihre öffentlichen Stellen von diesem Gesetz abweichende Regelungen zu treffen.“

…

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.betrifft-gesetze.de
ISSN 0720-2946

Begründung:

Bei der Bereitstellung von Telemedien durch öffentliche Stellen der Länder, insbesondere durch Polizeibehörden, kann es erforderlich sein, weitergehende Datenverarbeitungsbefugnisse zu regeln. Es sollte deshalb klargestellt werden, dass der Landesgesetzgeber insoweit gesetzgebungsbefugt ist.

AV 2. Zu Artikel 1 (§ 4 Satz 2 – neu – und 3 – neu – TTDSG)

In Artikel 1 sind dem § 4 folgende Sätze anzufügen:

„Der Anbieter hat sich über die Berechtigung der Erben sowie anderer berechtigter Personen zur Wahrnehmung der in Satz 1 genannten Rechte durch Vorlage geeigneter Nachweise zu vergewissern. Die Möglichkeit des Endnutzers, durch Vereinbarung oder im Wege einer letztwilligen Verfügung die Geheimhaltung oder Löschung der Daten zu verfügen, bleibt unberührt."

Begründung:

Es sind Konstellationen denkbar, in denen der Zugriff auf Daten durch Erben sowie sonstige Personen dem Willen des jeweiligen Endnutzers widersprechen kann. Dies kann namentlich im Falle des Todes des Endnutzers bei höchstpersönlichen E-Mails, Dokumenten sowie Bildern, die nicht den Zwecken einer ordnungsgemäßen Nachlassverwaltung und -abwicklung zu dienen bestimmt sind, der Fall sein. Auch können dem jeweiligen Endnutzer oder den tatsächlichen Erben erhebliche wirtschaftliche Schäden drohen, wenn und soweit Nichtberechtigte Zugriff auf die Daten erhalten und diese sodann für betrügerische oder sonst missbräuchliche Zwecke genutzt werden. Daher sollte zur Vermeidung von Automatismen bei der Herausgabe von Daten in § 4 die Klarstellung erfolgen, dass eine Preisgabe von Informationen gegenüber den Erben sowie sonstigen Personen nur zulässig ist, wenn und soweit diese ihre Berechtigung zur Wahrnehmung von Rechten im Sinne des § 4 Satz 1 ausreichend glaubhaft gemacht haben und keine anderslautende Verfügung des betroffenen Endnutzers vorliegt.

In 3. Zu Artikel 1 (§ 22 Absatz 1 Satz 2, § 23 TTDSG)

Artikel 1 ist wie folgt zu ändern:

a) In § 22 Absatz 1 Satz 2 ist das Wort „nicht" durch das Wort „auch" zu ersetzen.

b) § 23 ist zu streichen.

Begründung:

Das in § 22 Absatz 1 Satz 2 und § 23 TTDSG-E vorgesehene Auskunftsverfahren bei Passwörtern und anderen Zugangsdaten übernimmt mit geringfügigen redaktionellen Anpassungen die Regelungen der § 15a Absatz 1 Satz 2 und § 15b TMG des durch den Bundestag beschlossenen Gesetzes zur Anpassung der Regelungen über die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung des BVerfG vom 27. Mai 2020, welche wiederum aus dem nicht ausgefertigten Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität nahezu unverändert übernommen wurden.

Die Regelungen bewirken im Widerspruch zur namensgebenden Zielsetzung des Ursprungsgesetzes, den Rechtsextremismus und die Hasskriminalität zu bekämpfen, eine drastische Erhöhung der Voraussetzungen für Auskunftsverfahren bei Passwörtern und anderen Zugangsdaten im Vergleich zur derzeit geltenden Rechtslage, indem künftig das Auskunftsverfahren nur noch unter den hohen Hürden zugelassen wird, wie sie für eine technische Wohnraumüberwachung oder eine Online-Durchsuchung gelten.

Nach geltender Rechtslage gehören Passwörter und andere Zugangsdaten zu den Bestandsdaten im Sinne von § 14 Absatz 1 TMG (vergleiche Polenz, in: Kilian/Heussen, Computerrechts-Handbuch, Stand 34. Ergänzungslieferung Mai 2018, Teil 13: Telekommunikation und Telemedien Randnummer 20 [mit weiteren Nachweisen]). Das BVerfG hat diese Zuordnung für das parallele Auskunftsverfahren nach § 113 Absatz 1 Satz 2 TKG ausdrücklich gebilligt und die insoweit geltenden verfassungsrechtlichen Anforderungen wie folgt formuliert: „Erforderlich für eine effektive Strafverfolgung und Gefahrenabwehr ist lediglich, die Auskunftserteilung über solche Zugangssicherungen an diejenigen Voraussetzungen zu binden, die bezogen auf den in der Abfragesituation damit konkret erstrebten Nutzungszweck zu erfüllen sind“ (BVerfGE Band 130, Seite 151, hier Seite 209); auch in seiner jüngsten Entscheidung zur Bestandsdatenauskunft verlangt das BVerfG lediglich, dass „Zugangsdaten nicht unabhängig von den Anforderungen an deren Nutzung und damit gegebenenfalls unter leichteren Voraussetzungen abgefragt werden“ dürfen (BVerfG, Beschluss vom 27.5.2020 – 1 BvR 1873/13, 1 BvR 2618/13 – NJW 2020, 2699 (2716) Rn. 193). Zugleich hat das BVerfG aber auch klargestellt: „Der Verhältnismäßigkeitsgrundsatz gebietet allerdings auch nicht umgekehrt, die Erhebung der Zugangscodes ausnahmslos unter die Voraussetzungen zu stellen, die für deren eingriffsintensivste (‚maximale‘) Nutzungsmöglichkeit gegeben sein müssen“ (BVerfGE Band 130, Seite 151, hier Seite 209).

Genau von dieser „maximalen“ Nutzungsmöglichkeit gehen die Regelungen des § 22 Absatz 1 Satz 2 und § 23 TTDSG-E jedoch aus, indem sie für die Auskunft über Zugangsdaten an die Voraussetzungen der Online-Durchsuchung knüpfen. In der Begründung des Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität zu den als Vorbild dienenden §§ 15 Absatz 1 Satz 2 und § 15b TMG wird die gegenüber der Beauskunftung von Zugangsdaten nach dem TKG „deutlich eingeschränkt[e]“ Auskunft nach § 15b TMG mit einer höheren „Missbrauchsgefahr“ gerechtfertigt (BR-Drucksache 87/20, Seite 42 f.). Dies überzeugt jedoch nicht: Es gibt keinen Anlass, den Sicherheits- und Strafverfolgungsbehörden mit besonderem Misstrauen zu begegnen (vergleiche auch Masing, Zeitschrift für das gesamte Si-

cherheitsrecht 2018, Seite 7). Die von der Begründung unterstellte „Missbrauchsgefahr“ steht im Widerspruch zur besonderen beamtenrechtlichen Treuepflicht, die entsprechend der verfassungsrechtlichen Bindung der Exekutive an Recht und Gesetz (Artikel 20 Absatz 3 des Grundgesetzes) die volle persönliche Verantwortung der Beamtinnen und Beamten für die Rechtmäßigkeit ihrer dienstlichen Handlungen umfasst (§ 36 Absatz 1 BeamtStG). Die Gesetzesbegründung bleibt demgegenüber mit der Begründung, bei Telemediendienste scheine die Missbrauchsgefahr höher als bei Telekommunikationsdiensten, „weil diese so vielgestaltig sind“ (BR-Drucksache 87/20, Seite 42), unklar. Warum die Vielgestaltigkeit der Telemediendienste eine besondere Missbrauchsgefahr durch Beamte von Sicherheits- und Strafverfolgungsbehörden begründet, erhellt sich nicht. Obwohl entsprechende Auskunftsbefugnisse bereits seit dem Terrorismusbekämpfungsergänzungsgesetz vom 5. Januar 2007 (BGBl. I Seite 2) bestehen, sind aus der Praxis keine Fälle eines „Missbrauchs“ bekannt geworden.

R

(bei Annahme entfällt Ziffer 5)

4. Zu Artikel 1 (§ 22 Absatz 1 Satz 3 TTDSG),
Artikel 2 Nummer 2 Buchstabe b (§ 100j Absatz 2 Satz 1 StPO),
Artikel 4a – neu – (§ 113 Absatz 1 Satz 3 TKG)

a) In Artikel 1 sind in § 22 Absatz 1 Satz 3 nach den Wörtern „Internetprotokoll-Adresse“ die Wörter „sowie einer Kennung nach § 3 Nummer 25 des Telekommunikationsgesetzes“ einzufügen.

b) In Artikel 2 Nummer 2 Buchstabe b sind nach dem Wort „werden“ die Wörter ‚nach dem Wort „Internetprotokoll-Adresse“ die Wörter „sowie einer Kennung nach § 3 Nummer 25 des Telekommunikationsgesetzes“ eingefügt und werden‘ einzufügen.

c) Nach Artikel 4 ist folgender Artikel einzufügen:

‚Artikel 4a

Änderung des Telekommunikationsgesetzes

In § 113 Absatz 1 Satz 3 des Telekommunikationsgesetzes vom 22. Juni 2004 (BGBl. I S. 1190) das zuletzt durch ... geändert worden ist, sind nach dem Wort „Internetprotokoll-Adresse“ die Wörter „sowie einer Kennung nach § 3 Nummer 25“ einzufügen.‘

Begründung:

Um eine effektive Strafverfolgung zu ermöglichen und der Forderung des Bundesverfassungsgerichts nach Normenklarheit nachzukommen, sind die Regelungen über die Bestandsdatenauskunft in § 22 TTDSG, § 100j StPO und § 113 TKG in der Fassung des sich im parlamentarischen Verfahren befindenden § 173 TKG des Gesetzentwurfs zum Telekommunikationsmodernisierungsgesetzes um die Beauskunftung anhand von Port-Nummern zu ergänzen.

Bei der heute gängigen Nutzung der NAPT-Technologie können mehrere Nutzer im öffentlichen Netz unter einer IP-Adresse agieren. Zu unterscheiden sind sie nur aufgrund der internen IP-Adresse sowie der zusätzlich vergebenen Port-Nummer. Eine Zuordnung der (öffentlichen) IP-Adresse zum Nutzer ist damit nur noch bei Kenntnis der internen IP-Adresse, mindestens aber des verwendeten Ports möglich. Selbst wenn die Ermittlungsbehörden nicht nur mittels der öffentlichen IP-Adresse, sondern auch mittels der Port-Nummer Auskunft über die Bestandsdaten des Nutzers begehren, läuft dies ins Leere, wenn insbesondere der Telekommunikationsdienstleister die Port-Nummer nicht gespeichert hat. Die Problematik fehlender Port-Nummern-Speicherung führt daher jedes Jahr zur Einstellung zahlreicher Ermittlungsverfahren.

Dass die Kenntnis der Port-Nummern für eine erfolgreiche Beauskunftung von Bedeutung ist, zeigt sich in der im Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität vorgesehenen Änderung des § 3a Absatz 4 Nummer 2 Netzwerkdurchsetzungsgesetzes. Dieser sieht ausdrücklich vor, dass von den Anbietern sozialer Netzwerke dem Bundeskriminalamt die IP-Adresse einschließlich der Port-Nummer, sofern vorhanden, zu übermitteln ist.

Eine eindeutige Regelung, dass im Rahmen einer Bestandsdatenauskunft zu einer IP-Adresse auf die Port-Nummern zurückgegriffen werden darf, fehlt bislang sowohl in § 100j StPO als auch in § 113 TKG. Gleiches gilt für § 15a TMG, jetzt § 22 TTDSG.

Die Auskunft anhand von Port-Nummern ist nicht bereits infolge einer Prüfbitte des Bundesrates in § 100j StPO implementiert worden. § 100j StPO bestimmt in Absatz 2, dass die Auskunft über Bestandsdaten auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen IP-Adresse verlangt werden kann und nimmt Bezug auf § 113 Absatz 1 Satz 3, § 113c Absatz 1 Nummer 3 TKG. Die geltende Fassung geht auf einen Vorschlag des Innenausschusses des Bundesrates zurück (BT-Drucksache 17/12879) und entspricht bis auf den Verweis auf § 113c Absatz 1 Nummer 3 TKG, welcher durch das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten aufgenommen wurde, nahezu wortgleich der Fassung des Gesetzentwurfs zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft vom 9. Januar 2013 (BT-Drucksache 17/12034). Der Bundesrat hatte im Rahmen des Gesetzgebungsverfahrens gebeten, zu prüfen, ob im Rahmen der Zuordnung dynamischer Internetprotokoll-Adressen eine technikoffenere Formulierung wie etwa „… anhand der zu bestimmten Zeitpunkten vergebenen IP-Adresse sowie weiterer zur Individualisierung erforderlicher technischer Daten …“ verwendet werden sollte (BT-Drucksache 17/12034, Seite 18). Die Bundesregierung wollte den Vorschlag im weiteren Gesetzgebungsverfahren prüfen. Eine Ergänzung des § 100j StPO ist bis heute nicht erfolgt.

§ 22 Absatz 1 Satz 3 TTDSG lässt nicht klar erkennen, dass für die Auskunfterteilung auch auf Port-Nummern zurückgegriffen werden darf. Vergleichbar mit § 113 TKG wird lediglich geregelt, dass die in eine Auskunft aufzunehmenden Bestandsdaten auf anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse bestimmt werden dürfen.

Gemäß § 113 Absatz 1 Satz 3 TKG dürfen die in eine Auskunft aufzunehmenden Daten auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen IP-Adresse bestimmt werden. Satz 4 der Norm bestimmt, dass für die Auskunftserteilung sämtliche unternehmensinterne Datenquellen zu berücksichtigen sind. Die geltende Fassung entspricht in ihrem Wortlaut ebenfalls weitestgehend der Fassung des Gesetzentwurfs der Bundesregierung (BT-Drucksache 17/12034). Dass es sich bei den unternehmensinternen Datenquellen um die in Rede stehenden Port-Nummern handelt, ist weder dem Wortlaut noch der Begründung des Gesetzes zu entnehmen. § 173 Absatz 1 Satz 3 und 4 TKG in der Fassung des Gesetzentwurfs 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 (Telekommunikationsmodernisierungsgesetz) übernehmen den Wortlaut des § 113 TKG ohne Änderung.

In § 3 Nummer 25 TKG in der Fassung des Gesetzentwurfs 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 (Telekommunikationsmodernisierungsgesetz) wird der Begriff der Kennung neu eingeführt. Laut Definition handelt es sich hierbei um eine einem Nutzer, einem Anschluss oder einem Endgerät zu einem bestimmten Zeitpunkt zugewiesene eindeutige Zahlenfolge, die eine eindeutige Identifizierung des Nutzers, des Anschlusses oder des Endgerätes ermöglicht. In der Begründung zu § 3 Nummer 25 TKG wird ausgeführt: „Der neu aufgenommene Begriff der Kennung stellt den Oberbegriff zu dem in Nummer 3 definierten Begriff der Anschlusskennung dar. Er erfasst neben der Anschlusskennung auch einem Nutzer, einem Anschluss oder einem Endgerät nur temporär zugewiesene Zeichenfolgen zur Identifikation desselbigen. Dabei kann es sich beispielsweise um Kennungen zur einmaligen oder wiederholten Nutzung eines Telekommunikationsdienstes, um dynamische IP-Adressen beziehungsweise Port-Nummern oder um sonstige Benutzerkennungen handeln. Der Begriff der Kennung ist insbesondere für die Regelungen im Teil 10 Abschnitt 1 Öffentliche Sicherheit relevant. Kennungen sind beispielsweise künftig von Erbringern nummernunabhängiger interpersoneller Telekommunikationsdienste zu speichern, damit sie gegenüber Sicherheitsbehörden beauskunftet werden können.“ Vom Begriff der Kennung gemäß § 3 Nummer 25 TKG sind somit Port-Nummern erfasst.

Gemäß § 2 Absatz 1 TTDSG gelten die Begriffsbestimmungen des TKG auch für das TTDSG.

In den Regelungen zur Auskunfterteilung in § 22 TTDSG und im Änderungsbefehl zu § 100j StPO findet sich der Rückgriff auf die Kennung gemäß § 3 Nummer 25 TKG nicht. Ein Änderungsbefehl für § 113 TKG beziehungsweise § 173 TKG fehlt gänzlich.

In seiner Entscheidung vom 24. Januar 2012 – 1 BvR 1299/05 – hatte das Bundesverfassungsgericht moniert, dass der bis dato geltende § 113 TKG keine normenklare Befugnis zur Identifizierung von dynamischen IP-Adressen enthalte. Die Norm lasse nicht erkennen, dass die Telekommunikationsunternehmen in Vorbereitung von Bestandsdatenauskünften berechtigt und verpflichtet seien, IP-Adressen auszuwerten. Mit dem Gesetz zur Neuregelung der Bestandsdatenauskunft (BT-Drucksache 17/12034) wurde daher die Verwendung von IP-Adressen ausdrücklich in § 100j StPO und § 113 TKG aufgenommen. Zuletzt hat das Bundesverfassungsgericht in seiner Entscheidung vom 27. Mai 2020 – 1 BvR 1873/13, 1 BvR 2618/13 – normenklare Regelungen zur Bestandsdatenauskunft angemahnt. Im Interesse einer rechtssicheren Regelung, die auch den Anforderungen der Rechtsprechung des Bundesverfassungsgerichts genügt, sind in § 22 Absatz 1 Satz 3 TTDSG, § 100j Absatz 2 StPO sowie § 173 Absatz 1 Satz 3 TKG jeweils die Wörter „sowie einer Kennung nach § 3 Nummer 25 TKG“ anzufügen.

Allein eine Änderung von § 22 TTDSG und § 100j StPO würde die Beauskunftung anhand von Port-Nummern nur unvollständig regeln. Eine solches Vorgehen würde vielmehr die Frage aufwerfen, warum ein Rückgriff auf Port-Nummern im Rahmen von Bestandsdatenabfragen zu IP-Adressen nach dem TKG nicht geregelt worden ist und könnte zu dem Schluss führen, dass ein solcher Rückgriff im Anwendungsbereich des TKG unzulässig sei. Dies gilt es im Interesse einer effektiven Strafverfolgung zu vermeiden. Ein Gleichlauf der Normen ist anzustreben. Damit wird zugleich ein wesentliches Anliegen eines Beschlusses der Herbstkonferenz der Justizministerinnen und Justizminister am 26. und 27. November 2020 umgesetzt.

R

(entfällt bei Annahme von Ziffer 4)

5. Zu Artikel 1 (§ 22 Absatz 1 Satz 3 TTDSG),
Artikel 2 Nummer 2 Buchstabe b (§ 100j Absatz 2 Satz 1 StPO)

a) In Artikel 1 sind in § 22 Absatz 1 Satz 3 nach dem Wort „Internetprotokoll-Adresse“ die Wörter „sowie einer Kennung nach § 3 Nummer 25 des Telekommunikationsgesetzes“ einzufügen.

b) In Artikel 2 Nummer 2 Buchstabe b sind nach dem Wort „werden“ die Wörter ‚nach dem Wort „Internetprotokoll-Adresse“ die Wörter „sowie einer Kennung nach § 3 Nummer 25 des Telekommunikationsgesetzes“ eingefügt und werden‘ einzufügen.

Begründung:

Aus Gründen der Rechtsklarheit sowie zur Ermöglichung einer effektiven strafrechtlichen Verfolgung von Straftaten, die digital über das Internet begangen werden, ist es geboten, § 22 Absatz 1 Satz 3 TTDSG und § 100j Absatz 2 StPO so zu fassen, dass rechtssicher auch sogenannte Portnummern als Kennung im Sinne von § 2 Absatz 1 TTDSG in Verbindung mit § 3 Nummer 25 TKG den Strafverfolgungsbehörden übermittelt und von diesen abgefragt werden dürfen.

Nach § 2 Absatz 1 TTDSG gelten die Begriffsbestimmungen unter anderem des Telekommunikationsgesetzes auch für das TTDSG. Mangels abweichender Bestimmungen in § 2 Absatz 2 TTDSG gilt damit auch der Begriff der Kennung gemäß § 3 Nummer 25 TKG für das TTDSG. Bei einer Kennung handelt es sich um eine einem Nutzer, einem Anschluss oder einem Endgerät zu einem bestimmten Zeitpunkt zugewiesene eindeutige Zahlenfolge, die eine eindeutige Identifizierung des Nutzers, des Anschlusses oder des Endgerätes ermöglicht. In Einzelbegründung zu § 3 Nummer 25 TKG wird dargelegt, dass der Begriff der Kennung den Oberbegriff zu dem in Nummer 3 definierten Begriff der Anschlusskennung darstelle. Er erfasse neben der Anschlusskennung auch einem Nutzer, einem Anschluss oder einem Endgerät nur temporär zugewiesene Zeichenfolgen zur Identifikation desselbigen. Dabei könne es sich beispielsweise um Kennungen zur einmaligen oder wiederholten Nutzung eines Telekommunikationsdienstes, um dynamische IP-Adressen beziehungsweise Portnummern oder um sonstige Benutzerkennungen handeln (vergleiche BR-Drucksache 29/21, Seite 268).

Demgegenüber wird in § 22 Absatz 1 Satz 3 TTDSG und § 100j Absatz 2 StPO der Begriff der Kennung nicht ausdrücklich erwähnt. Hieraus ist für den Rechtsanwender nicht zuletzt vor dem Hintergrund der Rechtsprechung des Bundesverfassungsgerichts zum Erfordernis der Normenklarheit (nicht nur) von Regelungen zur Bestandsdatenauskunft (BVerfG, Beschluss vom 27. Mai 2020 – 1 BvR 1873/13, 1 BvR 2618/13) der Schluss zu ziehen, dass Port-nummern gerade nicht beauskunftet werden dürfen. Dies führte allerdings zu Lücken bei der Verfolgung „digitaler Kriminalität“. Denn die dem Kommunikationsmittel des Täters zugeordnete IP-Adresse stellt in diesem Bereich regelmäßig den einzigen erfolgversprechenden Ermittlungsansatz dar. Zu den für die Identifizierung erforderlichen Daten zählt nicht nur die IP-Adresse, sondern auch die sogenannte Portnummer. Denn IP-Adressen sind in der jetzt noch überwiegend genutzten IPv4-Version nur in begrenzter Zahl verfügbar. Telekommunikationsanbieter setzen daher die sogenannte NAPT-Technologie (= Network Adress Port Translation) ein, bei der dieselbe IP-Adresse gleichzeitig an eine oftmals sehr große Zahl von Nutzern vergeben wird. In derartigen Fällen kann die Zuordnung dieser IP-Adresse zu einem konkreten Nutzer im Rahmen einer Bestandsdatenauskunft nur gelingen, wenn neben der IP-Adresse auch die entsprechende Portnummer bekannt ist.

Auch nach Auffassung der Justizministerinnen und Justizminister besteht das Bedürfnis nach einer rechtssicheren Regelung zur Erfassung von Portnummern im Sinne des vorgeschlagenen Änderungsbefehls. Zudem würde hinsichtlich der vorgeschlagenen Änderung von § 100j StPO der Prüfbitte des Bundesrates aus dem Gesetzgebungsverfahren eines Gesetzes zur Änderung des Telekom-

munikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft vom 9. Januar 2013 (BT-Drucksache 17/12034) entsprochen werden. Der Bundesrat hatte gebeten, zu prüfen, ob im Rahmen der Zuordnung dynamischer Internetprotokoll-Adressen eine technikoffenere Formulierung wie etwa „… anhand der zu bestimmten Zeitpunkten vergebenen IP-Adresse sowie weiterer zur Individualisierung erforderlicher technischer Daten …“ verwendet werden sollte (vergleiche BT-Drucksache 17/12034, Seite 18). Die Bundesregierung wollte den Vorschlag im weiteren Verlauf des Gesetzgebungsverfahrens prüfen. Eine Ergänzung des § 100j StPO ist bis heute indessen nicht erfolgt.

In 6. Zu Artikel 1 (§ 22 Absatz 3 Nummer 2 Buchstabe a, b, c TTDSG)

Artikel 1 § 22 Absatz 3 Nummer 2 ist wie folgt zu ändern:

a) In Buchstabe a sind nach dem Wort „Sicherheit“ die Wörter „und Ordnung“ einzufügen.

b) In Buchstabe b sind die Wörter „ein Rechtsgut von erheblichem Gewicht“ durch die Wörter „Leib, Leben, Freiheit der Person, sexuelle Selbstbestimmung, den Bestand und die Sicherheit des Bundes und der Länder, die Grundlagen der Existenz der Menschen sowie nicht unerhebliche Sachwerte“ zu ersetzen.

c) In Buchstabe c sind die Wörter „ein besonders gewichtiges Rechtsgut“ durch die Wörter „Leib, Leben, Freiheit der Person, sexuelle Selbstbestimmung, den Bestand und die Sicherheit des Bundes und der Länder oder die Grundlagen der Existenz der Menschen“ zu ersetzen.

Begründung:

Das BVerfG hat in seiner Entscheidung vom 27. Mai 2020 1 BvR 1873/13, 1 BvR 2618/13 (sogenannte Bestandsdatenauskunft-II-Entscheidung) festgestellt, dass es grundsätzlich im Bereich der Gefahrenabwehr einer im Einzelfall vorliegenden konkreten Gefahr im Sinne der polizeirechtlichen Generalklauseln bedarf. Die polizeirechtliche Generalklausel beinhaltet stets die Befugnis zur Abwehr einer Gefahr für die öffentliche Sicherheit und Ordnung. Eine Einschränkung auf die öffentliche Sicherheit wird vom Bundesverfassungsgericht gerade nicht vorgenommen.

Die jeweiligen Rechtsgüter sollten ausdrücklich benannt werden: Das BVerfG hat in seiner Bestandsdatenauskunft-II-Entscheidung die Anforderung aufgestellt, dass der Gesetzgeber die Rechtsgüter von besonderem Gewicht selbst konkret benennen oder zumindest das erforderliche Gewicht normenklar festhalten muss. Dies sollte aus Gründen der Bestimmtheit sowohl für den Begriff der Rechtgüter von erheblichem Gewicht, als auch der Kategorie der besonders gewichtigen Rechtsgüter im Grundsatz gelten.

Rechtsgüter von erheblichem Gewicht stellen nach der Rechtsprechung des BVerfG die Rechtsgüter Leib, Leben, Freiheit der Person, den Bestand und die Sicherheit des Bundes und der Länder sowie nicht unerhebliche Sachwerte dar (vergleiche BVerfG, Beschluss vom 18. Dezember 2018 – 1 BvR 142/15, veröffentlicht in NJW 2019, Seite 827, hier Seite 835 Randnummer 99).

Von dem Begriff der besonders gewichtigen Rechtsgüter sind nach der Rechtsprechung des BVerfG die Rechtsgüter Leib, Leben, Freiheit der Person, Bestand und die Sicherheit des Bundes und der Länder sowie die Grundlagen der Existenz des Menschen erfasst (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 = NJW 2016, 1781, 1784 Rn. 108 m.w.N; BVerfG, Urteil vom 27. Februar 2008, BVerfGE Band 120, Seite 274, hier Seite 328).

Zu den Gütern der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berühren, zählen etwa auch die Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen (BVerfG, Urteil vom 27. Februar 2008, BVerfGE Band 120, Seite 274, hier Seite 328).

In seiner Entscheidung vom 1. Dezember 2020 (2 BvR 916/11, 2 BvR 636/12) hat das BVerfG darüber hinaus klargestellt, dass auch die sexuelle Selbstbestimmung unter die sogenannten hochrangigen Rechtsgüter zu fassen ist.

Das BVerfG verwendet die Begriffe der „hochrangigen“, der „überragend wichtigen“ und der „besonders gewichtigen“ Rechtsgüter synonym (BVerfG, Beschluss vom 27. Mai 2020 – 1 BvR 1873/13, 1 BvR 2618/13).

Da die Kategorie der besonders gewichtigen Rechtsgüter gegenüber den Rechtsgütern von erheblichem Gewicht grundsätzlich strenger gefasst ist, sind sowohl die Grundlagen der Existenz des Menschen als auch die sexuelle Selbstbestimmung erst Recht Rechtsgüter von erheblichem Gewicht.

In 7. Zu Artikel 1 (§ 22 Absatz 4 Satz 1 Nummer 2 TTDSG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob der Grundsatz der Bestimmtheit und die Rechtsprechung des BVerfG bei § 22 Absatz 4 Satz 1 Nummer 2 TTDSG-E eine Konkretisierung der Rechtsgüter „von hervorgehobenem“ Gewicht erfordern.

Begründung

Es ist dem Gesetz nicht zu entnehmen, was von der Kategorie der Rechtsgüter „von hervorgehobenem“ Gewicht, die in § 22 Absatz 4 Satz 1 Nummer 2 TTDSG-E als Tatbestandsvoraussetzung genannt werden, erfasst wird.

Nach der Rechtsprechung des BVerfG zählen zu den Rechtsgütern von hervorgehobenem Gewicht jedenfalls die durch das Strafrecht geschützten Rechtsgüter.

In 8. Zu Artikel 1 (§ 22 Absatz 4 Satz 1 Nummer 3 TTDSG)

In Artikel 1 § 22 Absatz 4 Satz 1 Nummer 3 sind die Wörter „Gefahr für besonders gewichtige Rechtsgüter oder die Verfolgung“ durch die Wörter „drohenden Gefahr für Leib, Leben, Freiheit der Person, sexuelle Selbstbestimmung, den Bestand und die Sicherheit des Bundes und der Länder, der Grundlagen der Existenz der Menschen oder die Verhütung“ zu ersetzen.

Begründung:

§ 22 Absatz 4 Satz 1 TTDSG-E sieht für die Auskunftserteilung von Bestandsdaten anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse und der damit möglichen automatisierten Auswertung von Nutzungsdaten nochmals verschärfte Anforderungen vor.

§ 22 Absatz 4 Satz 1 Nummer 3 TTDSG-E nimmt dabei Bezug auf die in § 22 Absatz 3 Nummer 2 Buchstabe b, c, Nummer 4 Buchstabe b Doppelbuchstabe bb, cc TTDSG-E geregelten erhöhten Anforderungen für Auskunftsverlangen im Rahmen der Auswertung anhand einer IP-Adresse im Falle des Vorliegens einer drohenden Gefahr. Dabei werden nochmals strengere Anforderungen aufgestellt, als dies bei Vorliegen einer Gefahr, gemeint ist damit eine konkrete Gefahr, nach § 22 Absatz 4 Satz 1 Nummer 2 TTDSG-E der Fall ist. Hierbei wird missverständlich formuliert, indem, wie schon bei § 22 Absatz 4 Satz 1 Nummer 2 TTDSG-E, nur die „Abwehr einer (konkreten) Gefahr“ genannt wird. Es sollte klargestellt werden, dass diese strengeren Anforderungen sich eben auf den Fall des Bestehens einer drohenden Gefahr beziehen, nicht auf das Bestehen einer konkreten Gefahr.

Die besonders gewichtigen Rechtsgüter sollten ausdrücklich benannt werden. Das BVerfG hat in seiner Entscheidung vom 27. Mai 2020 1 BvR 1873/13, 1 BvR 2618/13, Randnummer 180 (sogenannte Bestandsdatenauskunft-II-Entscheidung) die Anforderung aufgestellt, dass der Gesetzgeber die Rechtsgüter von besonderem Gewicht selbst konkret benennen oder zumindest das erforderliche Gewicht normenklar festhalten muss.

Von dem Begriff der besonders gewichtigen Rechtsgüter sind nach der Rechtsprechung des BVerfG die Rechtsgüter Leib, Leben, Freiheit der Person, Bestand und die Sicherheit des Bundes und der Länder sowie die Grundlagen der Existenz des Menschen erfasst (BVerfG, Urteil vom 20. April 2016 - 1 BvR 966/09, 1 BvR 1140/09, veröffentlicht in NJW 2016, Seite 1781, hier Seite 1784 Randnummer 108 mit weiteren Nachweisen; BVerfG, Urteil vom 27. Februar 2008, BVerfGE Band 120, Seite 274, hier Seite 328).

Zu den Gütern der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berühren zählen etwa auch die Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen (BVerfG, Urteil vom 27. Februar 2008, BVerfGE Band 120, Seite 274, hier Seite 328).

Zudem sollte auf die Verhütung von schweren Straftaten abgestellt werden, nicht auf ihre Verfolgung, da die entsprechende Bestimmung an die Gefahrenabwehrbehörden adressiert ist, nicht an die Strafverfolgungsbehörden.

AV 9. Zu Artikel 1 (§ 24 TTDSG)

Der Bundesrat begrüßt, dass mit dem Entwurf eines Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG) ein neues Stammgesetz geschaffen werden soll, in dem die wesentlichen datenschutzrechtlichen Bestimmungen des Telekommunikationsgesetzes (TKG) und des Telemediengesetzes (TMG) gebündelt werden.

AV 10. Der Bundesrat begrüßt dabei insbesondere, dass sich der in § 24 Absatz 1 geregelte Schutz der Privatsphäre bei Endeinrichtungen stärker am Wortlaut des Artikel 5 Absatz 3 der Richtlinie 2002/58/EG orientieren und mit den Vorgaben der Verordnung (EU) 2019/679 harmonisiert werden soll.

AV 11. Der Bundesrat stellt jedoch fest, dass auch vor dem Hintergrund des Verweises auf die Vorgaben der Verordnung (EU) 2016/679 in der Vorschrift des § 24 Absatz 1 Satz 2 sowie der Entscheidungen des Bundesgerichtshofs (BGH, Urteil vom 28. Mai 2020 – I ZR 07/16) und des Europäischen Gerichtshofs (EuGH, Urteil vom 1. Oktober 2019 – C-673/17) nach wie vor viele Rechtsfragen ungeklärt sind, die vor allem die Zulässigkeit des Setzens von Cookies sowie die Verarbeitung der mit ihnen erfassten Daten im Zusammenhang mit der Nutzung von Telemediendiensten betreffen.

AV 12. So fehlt es nach Ansicht des Bundesrates insbesondere an klaren gesetzlichen Leitlinien, die es erlauben würden, die Anforderungen an die Freiwilligkeit, die Informiertheit und die Form der Einwilligung in die Erhebung und Verarbeitung von personenbezogenen Daten rechtssicher und im Sinne der Nutzerinnen und Nutzer umzusetzen. Der Bundesrat bittet die Bundesregierung deshalb, sich auf europäischer Ebene dafür einzusetzen, dass die datenschutzrechtlichen Vorgaben betreffend die Zulässigkeit des Setzens von Cookies sowie die Verarbeitung der mit ihnen erfassten Daten weiter konkretisiert und darüber hinaus rechtssicher sowie nutzerfreundlich ausgestaltet werden.

AV 13. Der Bundesrat begrüßt ferner die Entwicklung, dass Bürgerinnen und Bürger zunehmend von den Vorteilen des digitalen Wandels profitieren, der insbesondere den Zugang zu einem vielfältigeren Angebot an Waren, Dienstleistungen und Informationen und damit eine stärkere Teilhabe am gesellschaftlichen Leben ermöglicht. Gleichwohl stellt der Bundesrat fest, dass Bürgerinnen und Bürgern der Zugang zu Angeboten auf Telemedien erschwert wird, wenn dieser, wie zunehmend festzustellen ist, von einer Einwilligung in die Erhebung und Verarbeitung von personenbezogenen Daten abhängig gemacht wird. Der Bundesrat bittet deshalb die Bundesregierung, sich auf europäischer Ebene für eine Regelung einzusetzen, die eine datensparsame Inanspruchnahme von Telemediendiensten zum Zwecke der Erstinformation gestattet, ohne dass von den jeweiligen Nutzerinnen und Nutzern eine Einwilligung in die Erhebung und Verarbeitung von personenbezogenen Daten wie beispielsweise zum Zwecke der Werbung gefordert wird.

In 14. Zu Artikel 1 (§ 24 TTDSG)

a) Der Bundesrat begrüßt die erforderliche Einwilligung in die Speicherung von Informationen in der Endeinrichtung der Endnutzerinnen und Endnutzer in Bezug auf den Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind.

b) Der Bundesrat stellt fest, dass die Nutzung des Internets durch diese – sinnvolle – Einwilligung beschwerlicher geworden ist und es zur Umsetzung weiterer vereinheitlichender Regelungen bedarf.

c) Der Bundesrat bittet deshalb, im weiteren Gesetzgebungsverfahren eine Regelung in das TTDSG-E aufzunehmen, die klarstellt, dass eine Einwilligung, sowie eine Ablehnung der Einwilligung in die Speicherung und Nutzung von Informationen auf dem Endgerät der Endnutzerinnen und Endnutzer grundsätzlich auch dadurch möglich ist, dass die Nutzerinnen und Nutzer eine entsprechende Voreinstellung im Browser wählen. Es muss dabei allerdings sichergestellt bleiben, dass die Nutzerinnen und Nutzer für unterschiedliche Internetauftritte im Einzelfall von den generellen Vorgaben im Browser auf einfache Weise abweichen können, ohne die generelle Einstellung zu ändern.

[In] = (bei Annahme entfällt Ziffer 23)

15. **[**d) Der Bundesrat spricht sich dementsprechend dafür aus, eine Regelung zu Browsereinstellungen in das TTDSG-E aufzunehmen, die verhindert, dass Browser herstellerseitig so eingestellt werden, dass der Zugriff auf die Informationen in Endeinrichtungen verhindert wird, auch wenn die Endnutzerinnen und Endnutzer eingewilligt haben. Hierbei geht es nicht darum, den Schutz der Nutzerinnen und Nutzer, die ihre Einwilligung erteilt haben, herabzusetzen, sondern darum, die von Browserinhabern abhängigen Anbieter vor nachteiligen Einstellungen zu schützen, die ihnen die Durchführung ihrer Geschäftsmodelle erschweren oder unmöglich machen.**]**

e) Der Bundesrat bittet um Schaffung einer Ermächtigungsgrundlage, um damit für Nutzerinnen und Nutzer eine einfachere und standardisierte Handhabung in Bezug auf die Ausgestaltung ihrer Einwilligung nach § 24 TTDSG-E zu ermöglichen.

f) Der Bundesrat weist darauf hin, dass Software, die den Abruf von Informationen aus dem Internet oder einer elektronische Kommunikation erlaubt, grundsätzlich stets datenschutzfreundlich voreingestellt sein sollte.

Begründung:

Nutzerinnen und Nutzer sind derzeit im Internet zahlreichen Einwilligungsanfragen für die Speicherung mittels „Cookies“ unterworfen. Die Notwendigkeit, die Einwilligung der Nutzerinnen und Nutzer abzufragen, ergibt sich aus – nun durch § 24 TTDSG-E in Umsetzung befindlichem – § 5 Absatz 3 der E-Privacy-Richtlinie 2009 (2009/136/EG) in Verbindung mit entsprechenden

Urteilen des EuGH vom 1. Oktober 2019 und des BGH vom 28. Mai 2020, woraus sich das Erfordernis eines sogenannten Opt-Ins für diese Einwilligungen ergibt. Dies ist im Sinne der Datensouveränität der Nutzerinnen und Nutzer ausdrücklich zu begrüßen.

Mit der zunehmenden Umsetzung dieser Regelung wird der Besuch von Internetseiten für Endnutzerinnen und Endnutzer jedoch zunehmend beschwerlicher. Um eine für Endnutzerinnen und Endnutzer einfache und schnelle Handhabe zu ermöglichen, erscheint eine einfache Gestaltung beispielsweise mithilfe von nur zwei Buttons („Einwilligen“, „Ablehnen“) zielführend.

Auch eine technische Umsetzung auf Browser-Ebene erscheint zielführend. Diese sollte jedoch Einzeleinwilligungen als Ausnahme berücksichtigen müssen, damit einzelne Einwilligungen weiter möglich sind und darauf basierende Geschäftsmodelle geschützt werden.

Wi 16. Zu Artikel 1 (§ 24 Absatz 2 Nummer 2 TTDSG)

Um Deutschland wettbewerbsfähig zu halten und der Innovationsfähigkeit der Digitalwirtschaft Raum zu lassen, bittet der Bundesrat um Klarstellung, dass Leistungs-, Nutzungs- und Reichweitenmessungen, ebenfalls von § 24 Absatz 2 Nummer 2 TTDSG umfasst sind. Diese Messungen sind für Anbieter von erheblicher Bedeutung, um die von Nutzerinnen und Nutzern ausdrücklich gewünschten Dienste technisch störungsfrei zur Verfügung stellen zu können und selbst unter anderem einen Überblick über die Nutzung ihrer Angebote zu haben.

In 17. Zu Artikel 1 (§ 24 Absatz 2 Nummer 3 – neu – TTDSG)

Dem Artikel 1 § 24 Absatz 2 Nummer 2 ist folgende Nummer anzufügen:

„3. wenn die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen zur Erfüllung gesetzlicher Verpflichtungen erforderlich ist.“

Folgeänderung:

In Artikel 1 § 24 Absatz 2 Nummer 1 sind die Wörter „ist oder“ durch das Wort „ist,“ und in Nummer 2 ist der Punkt am Ende durch das Wort „oder“ zu ersetzen.

Begründung

Es ist ein weiterer Ausnahmetatbestand von der Einwilligungspflicht in § 24 Absatz 1 TTDSG-E erforderlich. Gerade der einwilligungsfreie Zugriff auf Endeinrichtungen des Endnutzers zur Ausführung sicherheitsrelevanter Funktionen vor allem beim vernetzten Fahren ist alternativlos. Datenverarbeitungen im Zuge des sogenannten eCall-Systems sind von der VO (EU) 2015/758 (im Folgenden eCall-VO) vorgegeben, die Verarbeitung ist demnach zur Erfüllung einer gesetzlichen Verpflichtung nach Artikel 6 Absatz 1 Buchstabe c DSGVO beziehungsweise nach Artikel 9 Absatz 2 Buchstabe c DSGVO erforderlich. Eine konkret-individuelle Einwilligung ist hier unmöglich.

AV

18. Zu Artikel 1 (§ 24 Absatz 3 - neu - TTDSG)

(bei Annahme entfällt Ziffer 19)

In Artikel 1 ist dem § 24 folgender Absatz anzufügen:

„(3) In den Fällen des Absatzes 1 sind die Einwilligung in die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder in den Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, wie auch die entsprechende Ablehnung so zu gestalten, dass der Nutzer seine Einwilligung oder seine Ablehnung durch Nutzung von Schaltflächen, die gut lesbar mit nichts anderem als den Wörtern „Einwilligung“ und „Ablehnung“ beschriftet sind, erklären kann. Die Schaltflächen müssen auf derselben Ebene graphisch gleichwertig dargestellt werden. Die Pflicht zur Information nach Absatz 1 sowie die Zulässigkeit der Nutzung einer weiteren Schaltfläche, die dem Nutzer auf einer graphisch separat gestalteten Ebene eine aufgeschlüsselte und individuelle Einwilligung in die Nutzung einzelner Speicherungen oder Zugriffe im Sinne von Satz 1 ermöglicht, bleiben hiervon unberührt.“

Begründung:

Mit § 24 TTDSG-E werden die Vorgaben des Artikel 5 Absatz 3 der ePrivacy-Richtlinie zur Einwilligung von Nutzern in die Verwendung optionaler Cookies unter Berücksichtigung der Rechtsprechung des BGH grundsätzlich sachgerecht umgesetzt. Dabei sieht der Gesetzentwurf indessen davon ab, auch eine Regelung zur Ablehnung optionaler Cookies vorzusehen. Dies erscheint angesichts der vermehrt auftretenden Verwendung schwer verständlicher oder sogar irreführender „Cookie-Banner“ (sogenannte „Consent Management Platform“) nur schwer vermittelbar, führen diese doch zu breitem Unmut und zu erheblichen Einschränkungen bei der Internetnutzung. Es ist davon auszugehen, dass auch § 24 TTDSG-E in der im Gesetzentwurf vorgesehenen Form an diesem Umstand nichts ändern wird, bleibt es den Websitebetreibern doch weiterhin möglich, die Ablehnung optionaler Cookies durch entsprechende Gestaltung der Cookie-Banner deutlich zu erschweren.

Mit § 24 Absatz 3 TTDSG-E wird dem Anbieter der Website beziehungsweise der CMP aufgegeben, in Fällen des § 24 Absatz 1 TTDSG-E zumindest zwei Schaltflächen anzuzeigen, mit deren Betätigung der Endnutzer in die Verwendung optionaler Cookies mit nur einer Handlung einwilligen oder diese ablehnen kann. Verschachtelte Auswahlebenen, die durch geschickte Formulierung eine Abwahl von optionalen Cookies erschweren, wären demnach künftig unzulässig. Die Vorgabe klarer Kriterien für die graphische Gestaltung von Cookie-Bannern würde ein vereinheitlichtes beziehungsweise standardisiertes Cookie-Management-System etablieren, das die Optionen eines Nutzers einfach und verständlich vermittelt. Gleichzeitig wird es den Anbietern erschwert, das Verhalten von Internetnutzern durch das sogenannte „Nudging“ beziehungsweise „Dark Pattern“ unterbewusst zu steuern. Den Nutzern ist es damit künftig auf Grundlage der zur Verfügung zu stellenden Informationen eher möglich, eine informierte und weitgehend unbeeinflusste Entscheidung hinsichtlich der Einwilligung in Cookies zu treffen.

Die Möglichkeit der Websitebetreiber, den Zugang zu einer Website von der Zahlung eines Entgelts abhängig zu machen („Paywall“), bleibt von der Regelung unberührt. Websites, die lediglich notwendige Cookies im Sinne von § 24 Absatz 2 TTDSG verwenden, sind von der Regelung ausgenommen. Sofern es sich bei der Endeinrichtung nicht um einen PC oder ein Smartphone, sondern zum Beispiel um einen Gegenstand im Internet der Dinge handelt, dürfte eine Einwilligung regelmäßig bereits nach § 24 Absatz 2 Nummer 2 TTDSG-E entbehrlich sein. Sollen indessen optionale, das heißt technisch nicht unbedingt notwendige Informationen gespeichert oder auf entsprechende Informationen zugegriffen werden, erscheint es dem Hersteller der Gegenstände zumutbar, entsprechende Möglichkeiten zur Einwilligung oder Ablehnung zu schaffen (zum Beispiel im Rahmen einer „Begleitapp“).

Aufgrund des akuten Handlungsbedarfs kann insoweit auch nicht länger das Tätigwerden des Unionsgesetzgebers abgewartet werden. Die bisherige Historie der ePrivacy-Verordnung hat gezeigt, dass trotz erneuertem Verhandlungsmandat keinesfalls mit ihrem zeitnahen Erlass zu rechnen ist. Vor diesem Hintergrund wird man gleichwohl § 24 Absatz 3 – neu – TTDSG fortlaufend bewerten müssen, um im Fall des nahenden Inkrafttretens der ePrivacy-Verordnung auf drohende Verstöße gegen höherrangiges Unionsrechts beziehungsweise das Normwiederholungsverbot rechtzeitig reagieren zu können.

AV

(entfällt bei Annahme von Ziffer 18)

19. Hilfsempfehlung zu Ziffer 18

Zu Artikel 1 (§ 24 Absatz 3 – neu – TTDSG)

In Artikel 1 ist dem § 24 folgender Absatz anzufügen:

„(3) In den Fällen des Absatzes 1 muss dem Nutzer auch eine im Vergleich zur Einwilligung gleichwertige Möglichkeit zur umfassenden Ablehnung der Speicherung von Informationen in der Endeinrichtung des Endnutzers oder des Zugriffs auf Informationen eingeräumt werden.“

...

Begründung:

Mit § 24 TTDSG-E werden die Vorgaben des Artikel 5 Absatz 3 der ePrivacy-Richtlinie zur Einwilligung von Nutzern in die Verwendung optionaler Cookies unter Berücksichtigung der Rechtsprechung des BGH grundsätzlich sachgerecht umgesetzt. Dabei sieht der Gesetzentwurf indessen davon ab, auch eine Regelung zur Ablehnung optionaler Cookies vorzusehen. Dies erscheint angesichts der vermehrt auftretenden Verwendung schwer verständlicher oder sogar irreführender „Cookie-Banner“ (sogenannte „Consent Management Platform“) nur schwer vermittelbar, führen diese doch zu breitem Unmut und zu erheblichen Einschränkungen bei der Internetnutzung. Es ist davon auszugehen, dass auch § 24 TTDSG-E in der im Gesetzentwurf vorgesehenen Form an diesem Umstand nichts ändern wird, bleibt es den Websitebetreibern doch weiterhin möglich, die Ablehnung optionaler Cookies durch entsprechende Gestaltung der Cookie-Banner deutlich zu erschweren.

Die Normierung einer Pflicht der Websitebetreiber, Nutzern eine im Vergleich zur Einwilligung gleichwertige Möglichkeit zur umfassenden Ablehnung von Cookies anzubieten, erscheint geeignet, diese Missstände zu beseitigen. Dabei orientiert sich der Vorschlag an der Formulierung des Verhandlungsmandats des Europäischen Rates vom 10. Februar 2021, nach dem der Nutzer zwischen der Einwilligung „und einem gleichwertigen Angebot des gleichen Anbieters wählen kann, das nicht mit der Einwilligung zu Cookies einhergeht.“ Zugleich entspricht eine derartige Vorgabe dem Willen des europäischen Gesetzgebers, der in Erwägungsgrund 66 der Richtlinie 2009/136/EG zur Änderung der ePrivacy-Richtlinie von 2002 in diesem Kontext davon spricht, dass „die Einräumung des Rechts, diese abzulehnen, […] so benutzerfreundlich wie möglich gestaltet werden“ solle.

Die Möglichkeit der Websitebetreiber, den Zugang zu einer Website von der Zahlung eines Entgelts abhängig zu machen („Paywall“), bleibt von der Regelung unberührt. Websites, die lediglich notwendige Cookies im Sinne von § 24 Absatz 2 TTDSG verwenden, sind von der Regelung ohnehin ausgenommen.

Sofern es sich bei der Endeinrichtung nicht um einen PC oder ein Smartphone, sondern zum Beispiel um einen Gegenstand im Internet der Dinge handelt, dürfte eine Einwilligung regelmäßig bereits nach § 24 Absatz 2 Nummer 2 TTDSG-E entbehrlich sein. Sollen indessen optionale, das heißt technisch nicht unbedingt notwendige Informationen gespeichert oder auf entsprechende Informationen zugegriffen werden, erscheint es dem Hersteller der Gegenstände zumutbar, entsprechende Möglichkeiten zur Einwilligung oder Ablehnung zu schaffen (zum Beispiel im Rahmen einer „Begleitapp“).

Aufgrund des akuten Handlungsbedarfs kann insoweit auch nicht länger das Tätigwerden des Unionsgesetzgebers abgewartet werden. Die bisherige Historie der ePrivacy-Verordnung hat gezeigt, dass trotz erneuertem Verhandlungsmandat wohl nicht mit ihrem zeitnahen Erlass zu rechnen ist. Vor diesem Hintergrund wird man gleichwohl § 24 Absatz 3 - neu - TTDSG fortlaufend bewerten müssen, um im Fall des Inkrafttretens der ePrivacy-Verordnung auf dann drohende Verstöße des neuen § 24 Absatz 3 TTDSG gegen höherrangiges Unionsrecht beziehungsweise das Normwiederholungsverbot rechtzeitig reagieren zu können.

In 20. Zu Artikel 1 (§ 26 Absatz 1 Satz 2 – neu – TTDSG)

Dem Artikel 1 § 26 Absatz 1 ist folgender Satz anzufügen:

„Auf öffentliche Stellen der Länder findet diese Vorschrift keine Anwendung; es steht den Ländern frei, entsprechende Bußgeldvorschriften zu erlassen."

Begründung:

Die DSGVO sieht in Artikel 83 Absatz 7 ausdrücklich vor, dass für öffentliche Stellen die Verhängung von Geldbußen nach dieser Verordnung ausgeschlossen werden kann. Davon haben die Länder im Anwendungsbereich der DSGVO weitgehend Gebrauch gemacht. Soweit personenbezogene Daten von einem Verstoß gegen die Vorgaben des TTDSG betroffen sind, scheidet eine Bußgeldbewehrung des Handelns öffentlicher Stellen der Länder durch Bundesrecht deshalb aus, weil damit die Entscheidung der Länder im Rahmen des Landesrechts untergraben werden würde. Nur in äußerst seltenen Einzelfällen könnte es denkbar sein, dass ein Verstoß gegen das TTDSG auch begangen werden könnte, ohne dass personenbezogene Daten davon betroffen sind. Auch insoweit sollten aber gleichlaufend mit der Kompetenzverteilung beim Vollzug der DSGVO die Länder die Entscheidungshoheit behalten, um beispielsweise eine Regelung treffen zu können, wonach - wie in den meisten Ländern auch im Anwendungsbereich der DSGVO - Geldbußen nur verhängt werden dürfen, soweit öffentlich-rechtlich organisierte Stellen als Unternehmen am Wettbewerb teilnehmen. Ein Gleichlauf mit den datenschutzrechtlichen Regelungen ist schon deshalb wünschenswert, weil in der Praxis die Abgrenzung zwischen der Verarbeitung personenbezogener und nicht-personenbezogener Daten mitunter schwierig ist und Unklarheiten über das Konkurrenzverhältnis zwischen abweichenden Regelungen entstehen könnten.

In 21. Zu Artikel 1 (§ 26 Absatz 3 Nummer 2,
§ 27 Absatz 1a – neu –, Absatz 2, 3,
§ 28 Absatz 1 Satz 1, 2 – neu – TTDSG)

Artikel 1 ist wie folgt zu ändern:

a) § 26 Absatz 3 Nummer 2 ist wie folgt zu fassen:

„2. die zuständige Datenschutzaufsichtsbehörde oder soweit die Länder eine abweichende Aufgabenzuweisung vorgenommen haben, die danach zuständige Aufsichtsbehörde; die Zuständigkeitsabgrenzung zwischen Bundes- und Landesaufsichtsbehörden entspricht der Abgrenzung in den §§ 40, 9 Bundesdatenschutzgesetz, § 115 Absatz 4 Telekommunikationsgesetz."

b) § 27 ist wie folgt zu ändern:

aa) Nach Absatz 1 ist folgender Absatz einzufügen:

„(1a) Soweit für Dienste, welche nicht für Zwecke der geschäftsmäßigen Erbringung von Telekommunikationsdiensten erbracht werden, Daten von natürlichen oder juristischen Personen im Anwendungsbereich dieses Gesetzes verarbeitet werden, sind die Datenschutzaufsichtsbehörden der Länder gemäß § 40 Bundesdatenschutzgesetz die zuständigen Aufsichtsbehörden, soweit die Länder keine abweichende Kompetenzzuweisung getroffen haben. Die Zuständigkeit erstreckt sich auch auf sonstige Vorschriften des Telekommunikationsgesetzes und des Telemediengesetzes, soweit dort eine Abstimmung mit Datenschutzaufsichtsbehörden vorgesehen ist und entsprechend der Kompetenzverteilung gemäß §§ 40, 9 Bundesdatenschutzgesetz, § 115 Absatz 4 Telekommunikationsgesetz die Zuständigkeit bei den Ländern liegt."

bb) In Absatz 2 sind die Wörter „durch Anbieter von Telekommunikationsdiensten" durch die Wörter „für Zwecke der Erbringung von Telekommunikationsdiensten" zu ersetzen.

cc) Absatz 3 ist wie folgt zu ändern:

aaa) Die Wörter „des oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit" sind durch die Wörter „der zuständigen Aufsichtsbehörden entsprechend der Kompetenzverteilung in den §§ 40, 9 Bundesdatenschutzgesetz, § 115 Absatz 4 Telekommunikationsgesetz" zu ersetzen.

bbb) Die Wörter „seiner oder" sind zu streichen.

ccc) Das Wort „Anwendung." ist durch die Wörter „Anwendung; für öffentliche Stellen der Länder verbleibt es bei der Kompetenzzuweisung durch die Datenschutz-Grundverordnung sowie die Landesgesetze in Umsetzung der Richtlinie (EU) 2016/680." zu ersetzen.

c) § 28 Absatz 1 ist wie folgt zu ändern:

aa) Die Wörter „des oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit“ sind durch die Wörter „der Datenschutzaufsichtsbehörden von Bund und Ländern oder einer nach Landesrecht besonders bestimmten Aufsichtsbehörde“ zu ersetzen.

bb) Folgender Satz ist anzufügen:

„Die Bundesnetzagentur hat ihr Vorgehen im Einzelfall mit der gemäß § 27 zuständigen Stelle abzustimmen, soweit deren Interessen betroffen sein können.“

Begründung:

Um Kompetenzüberschneidungen zwischen Bundes- und Landesdatenschutzaufsichtsbehörden zu vermeiden und insbesondere nicht die Zuständigkeiten der Landesdatenschutzbehörden zu beschneiden, sollte die Kompetenzverteilung im Rahmen des TTDSG strikt an der Kompetenzverteilung im allgemeinen Datenschutzrecht orientiert werden. Dabei muss insbesondere die Zitierung von § 115 Absatz 4 TKG voraussichtlich noch mit weiteren aktuellen Gesetzgebungsvorhaben abgestimmt werden. Bei der Zuständigkeitsabgrenzung ist insbesondere auch zu berücksichtigen, dass sich die Aufsichtszuständigkeit des Bundes gemäß der Kompetenzverteilung des Grundgesetzes zwar umfassend auf die Telekommunikation erstreckt. Dies beinhaltet allerdings nicht die Aufsichtszuständigkeit des Bundes auf jegliche Tätigkeiten von Telekommunikationsunternehmen. Soweit diese Telemedien bereitstellen, ist die Zuständigkeit der Landesaufsichtsbehörden eröffnet. Da schon nach bisheriger Rechtslage die Länder für die Bußgeldverfolgung im Anwendungsbereich des § 16 TMG zuständig waren und diese Zuständigkeit teilweise auch anderen öffentlichen Stellen der Länder als den Datenschutzaufsichtsbehörden zugewiesen war, sollte es den Ländern weiterhin unbenommen bleiben, insoweit Kompetenzen innerhalb der Landesverwaltung zuzuweisen.

In 22. Zum Gesetzentwurf allgemein

a) Der Bundesrat begrüßt das mit dem TTDSG verfolgte Ziel, die nationale Rechtslage besser an europarechtliche Vorgaben anzupassen. Gleichwohl stellt der Bundesrat fest, dass eine stärkere Einbindung der Länder im Vorfeld wünschenswert gewesen wäre. Das Verständnis der Länder für die Intentionen des Bundesgesetzgebers leidet insbesondere auch darunter, dass

im Rahmen von mehreren Gesetzgebungsverfahren Regelungen getroffen wurden, welche sich auf die Zuständigkeitsverteilung zwischen den Datenschutzaufsichtsbehörden von Bund und Ländern auswirken können, ohne dass dies in der Gesetzesbegründung offengelegt worden wäre.

b) Soweit die Neuregelungen originäre Kompetenzen und Interessen der Länder berühren, wird ein dringender Nachbesserungsbedarf des TTDSG gesehen. Es ist bereits im Grundgesetz eine grundsätzliche Länderzuständigkeit verankert. Es sollte deshalb auch vorliegend eindeutig klargestellt werden, dass die bisher schon den Datenschutzaufsichtsbehörden der Länder zugewiesene Zuständigkeit für die Aufsicht über Telemedien im Rahmen der DSGVO (vergleiche dazu gemeinsame Orientierungshilfe der Aufsichtsbehörden von Bund und Ländern für Anbieter von Telemedien, abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf) durch die Umsetzung der ePrivacy-Richtlinie und sonstiger europarechtlicher Vorgaben unangetastet bleiben. Auch soweit nichtpersonenbezogene Daten einer Aufsicht unterliegen, können für die Kompetenzverteilung zwischen Bund und Ländern keine anderen Maßstäbe als im Rahmen der Datenschutzaufsicht nach der DSGVO gelten.

c) Der Bundesrat bittet in diesem Zusammenhang auch, im weiteren Gesetzgebungsverfahren zu prüfen, ob und inwieweit der für die oder den BfDI nun im Entwurf eines TTDSG geltend gemachte Mehraufwand tatsächlich durch die Umsetzung des TTDSG entsteht. Ein Mehraufwand für die oder den BfDI wird im Gesetzentwurf mit den „erweiterten Begriffsbestimmungen des Telekommunikationsmodernisierungsgesetzes und den erweiterten Aufgaben für den BfDI als Aufsichtsbehörde“ begründet. Es ist nicht nachvollziehbar, warum dieser Mehraufwand, welcher nach der Gesetzesbegründung zum TTDSG-E gerade im Rahmen der Neuregelungen im Rahmen des Telekommunikationsmodernisierungsgesetzes entstehen soll, nun erst im Rahmen des gegenständlichen Gesetzentwurfs geltend gemacht wird. Ein entsprechender Aufwand müsste im Gesetzgebungsverfahren zum Telekommunikationsmodernisierungsgesetz dargelegt werden, um dem Bundesrat ebenso wie dem Bundestag die Auswirkungen dieses Gesetzes, insbesondere eine Aufgabenmehrung bei Bundesbehörden, umfassend vor Augen zu führen. Da außerdem der Bundesrat in seiner Stellungnahme vom 12. Februar 2021, BR-Drucksache 29/21 (Beschluss) unter Ziffer 5 gerade Einwendungen gegen diese Definitionserweiterung erhoben hat, kann

jedenfalls im Rahmen des gegenständlichen Gesetzentwurfs nicht beurteilt werden, ob der geltend gemachte Aufgabenzuwachs insoweit überhaupt zu erwarten ist. Diese Einwendungen wurden erhoben, weil die vorgeschlagene Definitionsänderung insbesondere auch zu einer Verschiebung von Aufsichtsbefugnissen der Landesdatenschutzbehörden hin zur Zuständigkeit der oder des BfDI führen würde, ohne dass dies im Rahmen des Gesetzgebungsverfahrens offengelegt worden wäre.

d) Gleichzeitig muss, soweit ein Mehraufwand tatsächlich dadurch entsteht, dass über den Anwendungsbereich der DSGVO hinausgehende Aufsichtszuständigkeiten entstehen, auch ein entsprechender Mehrbedarf der Datenschutzaufsichtsbehörden der Länder benannt werden. Beispielsweise durch die Einbeziehung von juristischen Personen in den Schutzbereich der Datenschutzregelungen könnte ein Mehraufwand bei allen Aufsichtsbehörden zu verzeichnen sein. Der Bundesrat bittet deshalb, neue Kompetenzen von Bundes- und Landesbehörden unter Darlegung der entsprechenden Gesetzgebungsbefugnisse ausführlich zu erläutern, um insbesondere auch in Kenntnis der damit verbundenen Kosten eine legislative Entscheidung treffen zu können.

e) Der Bundesrat bittet, im Rahmen des TTDSG-E zu prüfen, an welchen Stellen des Gesetzentwurfs anstelle des Begriffs „Telekommunikationsdienst“ der Begriff „elektronischer Kommunikationsdienst“ verwendet werden sollte. Entsprechend der im Rahmen des Telekommunikationsmodernisierungsgesetzes verfolgten Intention des Gesetzentwurfs (siehe dazu Ziffer 5 , BR-Drucksache 29/21(Beschluss)), sämtliche Regelungen zur Telekommunikation auf Bereiche auszudehnen, welche nach bisherigem Verständnis dem Telemedienrecht zuzurechnen sind, sollte nun im Einzelfall geprüft werden, ob eine Erweiterung des Anwendungsbereiches der Regelungen beispielsweise auf interpersonelle Kommunikationsdienste gewünscht und ohne Einschränkung der Länderkompetenzen auch möglich ist. Insbesondere muss dabei die Kompetenzverteilung zwischen Bundes- und Landesaufsichtsbehörden gleichlaufend mit der Kompetenzverteilung in den §§ 40, 9 BDSG, § 115 Absatz 4 TKG berücksichtigt werden. Soweit das TKG in der dann gültigen Fassung Aufsichtsbefugnisse der Bundesnetzagentur regelt, welche sich auch auf Telemedien und insbesondere dort auf personenbezogene Daten beziehen (vergleiche dazu beispielsweise § 109 TKG in der Fassung des IT-Sicherheitsgesetzes, dazu Ziffer 23 , BR-Drucksache 16/21 (Beschluss)), sollte eine Pflicht der Bundesnetzagentur aufgenommen wer-

den, Entscheidungen über Vorgaben im Einvernehmen mit der insoweit zuständigen Aufsichtsbehörde und nicht nur grundsätzlich mit der oder dem BfDI zu treffen. Bei der Zuständigkeitsverteilung zwischen den Datenschutzaufsichtsbehörden von Bund und Ländern ist insbesondere der Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 12. September 2019 „Sachliche Zuständigkeit für E-Mail und andere Over-the-top (OTT)-Dienste“, https://www.datenschutzkonferenz-online.de/media/dskb/20190912_beschluss_zu_ott_diensten.pdf, zu beachten.

Wi 23. Zum Gesetzentwurf allgemein

(entfällt bei Annahme von Ziffer 15)

a) Der Bundesrat spricht sich dafür aus, eine Regelung zu Browsereinstellungen in das TTDSG aufzunehmen, die verhindert, dass Browser herstellerseitig so eingestellt werden, dass der Zugriff auf die Informationen in Endeinrichtungen verhindert wird, auch wenn der Endnutzer eingewilligt hat. Hierbei geht es nicht darum, den Schutz der Nutzerinnen und Nutzer, die ihre Einwilligung erteilt haben, herab zu setzen, sondern darum, die von Browserinhabern abhängigen Anbieter vor nachteiligen Einstellungen zu schützen, die ihnen die Durchführung ihrer Geschäftsmodelle erschweren oder unmöglich machen.

[Wi] = 24. [b) Der Bundesrat ist der Auffassung, dass mit dem TTDSG ein Rechtsrahmen für Datenmanagementsysteme beziehungsweise Personal Information Management Systems (PIMS) geschaffen werden sollte. Derzeit besteht große Rechtsunsicherheit für die Unternehmen die Datenschutzmanagementsysteme entwickeln oder einsetzen möchten. Dabei profitieren Nutzerinnen und Nutzer durch den Einsatz von mehr Datensouveränität und leichter Handhabbarkeit; Unternehmen können ihre Prozesse optimieren und Ressourcen sparen. Die durch den fehlenden konkreten Rechtsrahmen bestehende Rechtsunsicherheit muss beseitigt werden, damit Deutschland auf diesem Gebiet Vorreiter werden und gegebenenfalls die Weichen für die Entwicklungen auf europäischer Ebene stellen kann (Daten-Governance-Gesetz).]

...

K 25. Zum Gesetzentwurf allgemein

a) Der Bundesrat weist darauf hin, dass für Medienanbieter besondere Datenschutzbestimmungen gelten. In Umsetzung der Vorgaben der DSGVO (insbesondere Artikel 85) und in Wahrnehmung ihrer Kompetenzen als Medien- beziehungsweise Rundfunkgesetzgeber haben die Länder insbesondere für die Datenschutzaufsicht über Rundfunk- und Presseunternehmen sowie für den öffentlich-rechtlichen Rundfunk besondere Vorschriften erlassen (siehe beispielhaft §§ 16 ff ZDF-StV, § 50 LMG RP, § 50 LMG BW). Materiell-rechtlich sind für die Datenverarbeitung zu journalistischen Zwecken ebenfalls besondere Bestimmungen maßgeblich (siehe beispielhaft §§ 12, 23 MStV sowie § 13 LMG RP).

b) Der Bundesrat geht davon aus, dass Rundfunk- und Presseunternehmen sowie deren Datenverarbeitung zu journalistischen Zwecken von den vorgeschlagenen Regelungen für ein TTDSG nicht erfasst werden, wie dies auch schon unter Geltung der Vorgängerregelungen im TKG und TMG der Fall war. Da jedoch weder der Regelungstext noch die Begründung des TTDSG-E einen entsprechenden Hinweis auf die besonderen Vorschriften im Medienbereich enthalten, würde der Bundesrat eine Klarstellung begrüßen, dass diese auch weiterhin von den Vorgaben des TTDSG unberührt bleiben.

B

26. Der **Gesundheitsausschuss**

empfiehlt dem Bundesrat, gegen den Gesetzentwurf gemäß Artikel 76 Absatz 2 des Grundgesetzes k e i n e Einwendungen zu erheben.