Bundesverwaltungsgericht

IM NAMEN DES VOLKES
URTEIL

BVerwG 6 C 7.22 (6 C 13.18)
9 K 7417/17

In der Verwaltungsstreitsache

ECLI:DE:BVerwG:2023:140823U6C7.22.0

hat der 6. Senat des Bundesverwaltungsgerichts
am 14. August 2023
durch den Vorsitzenden Richter am Bundesverwaltungsgericht Prof. Dr. Kraft,
die Richter am Bundesverwaltungsgericht Dr. Möller, Hahn und Dr. Tegethoff
sowie die Richterin am Bundesverwaltungsgericht Dr. Gamp

ohne mündliche Verhandlung für Recht erkannt:

Die Revision der Beklagten gegen das Urteil des Verwaltungsgerichts Köln vom 20. April 2018 wird mit der Maßgabe zurückgewiesen, dass der Feststellungsausspruch dahingehend gefasst wird, dass die Klägerin nicht verpflichtet ist, die in § 176 Abs. 3 Nr. 1 bis 3 TKG aufgeführten Telekommunikations-Verkehrsdaten ihrer Kunden, denen sie den Internet-Zugang vermittelt, und die in § 176 Abs. 2 Satz 1 und 2 TKG genannten Telekommunikations-Verkehrsdaten ihrer Kunden, denen sie den Zugang zu öffentlichen Telefondiensten vermittelt, zu speichern.

Die Beklagte trägt die Kosten des Revisionsverfahrens.

G r ü n d e :

I

1 Die Klägerin erbringt öffentlich zugängliche Telefondienste und Internetzugangsdienste. Sie wendet sich mit der Feststellungsklage gegen die ihr durch § 113a Abs. 1 in Verbindung mit § 113b des Telekommunikationsgesetzes vom 22. Juni 2004 (TKG a. F.) in der Fassung des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 (BGBI. I S. 2218 ff.) auferlegte Pflicht, ab dem 1. Juli 2017 Telekommunikations-Verkehrsdaten ihrer Kunden auf Vorrat zu speichern.

2 Mit Urteil vom 20. April 2018 hat das Verwaltungsgericht auf die Klage festgestellt, dass die Klägerin nicht verpflichtet ist, die in § 113b Abs. 3 TKG a. F. aufgeführten Telekommunikations-Verkehrsdaten ihrer Kunden, denen sie den Internetzugang vermittelt, zu speichern und die in § 113b Abs. 2 Satz 1 und 2 TKG a. F. genannten Telekommunikations-Verkehrsdaten ihrer Kunden, denen sie den Zugang zu öffentlichen Telefondiensten vermittelt, zu speichern. Die Spei-

cherpflicht verstoße gegen Unionsrecht und sei daher im Fall der Klägerin unanwendbar. Die grundsätzlichen Rechtsfragen zur Reichweite und zu den materiellrechtlichen Anforderungen des im vorliegenden Zusammenhang maßgeblichen Unionsrechts seien durch das Urteil des Gerichtshofs der Europäischen Union (EuGH) vom 21. Dezember 2016 in den verbundenen Rechtssachen C-203/15 (Tele2 Sverige) und C-698/15 (Watson u. a.) [ECLI:EU:C:2016:970] geklärt.

3 Auf die (Sprung-)Revision der Beklagten, mit der diese die Abweisung der Klage unter Änderung des Urteils des Verwaltungsgerichts erstrebt, hat der Senat das Verfahren mit Beschluss vom 25. September 2019 (BVerwG 6 C 13.18) ausgesetzt und eine Vorabentscheidung des EuGH gemäß Art. 267 AEUV eingeholt.

4 Mit Urteil vom 20. September 2022 (verbundene Rechtssachen C-793/19 und C-794/19 [ECLI:EU:C:2022:702], berichtigt durch Beschluss vom 27. Oktober 2022) hat der EuGH die Vorlage wie folgt beschieden:

> "Art. 15 Abs. 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) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 geänderten Fassung ist im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union
>
> dahin auszulegen, dass
>
> er nationalen Rechtsvorschriften entgegensteht, die präventiv zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen;
>
> er nationalen Rechtsvorschriften nicht entgegensteht, die
>
> - es zum Schutz der nationalen Sicherheit gestatten, den Betreibern elektronischer Kommunikationsdienste aufzugeben, Verkehrs- und Standortdaten allgemein und unterschiedslos auf Vorrat zu speichern, wenn sich der betreffende Mitgliedstaat einer als real und aktuell oder vorher-

sehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit gegenübersieht, sofern diese Anordnung Gegenstand einer wirksamen, zur Prüfung des Vorliegens einer solchen Situation sowie der Beachtung der vorzusehenden Bedingungen und Garantien dienenden Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle sein kann, deren Entscheidung bindend ist, und sofern die Anordnung nur für einen auf das absolut Notwendige begrenzten, aber im Fall des Fortbestands der Bedrohung verlängerbaren Zeitraum ergeht;

- zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit auf der Grundlage objektiver und nicht diskriminierender Kriterien anhand von Kategorien betroffener Personen oder mittels eines geografischen Kriteriums für einen auf das absolut Notwendige begrenzten, aber verlängerbaren Zeitraum eine gezielte Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen;

- zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit für einen auf das absolut Notwendige begrenzten Zeitraum eine allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, vorsehen;

- zum Schutz der nationalen Sicherheit, zur Bekämpfung der Kriminalität und zum Schutz der öffentlichen Sicherheit eine allgemeine und unterschiedslose Vorratsspeicherung der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten vorsehen;

- es zur Bekämpfung schwerer Kriminalität und, *a fortiori*, zum Schutz der nationalen Sicherheit gestatten, den Betreibern elektronischer Kommunikationsdienste mittels einer Entscheidung der zuständigen Behörde, die einer wirksamen gerichtlichen Kontrolle unterliegt, aufzugeben, während eines festgelegten Zeitraums die ihnen zur Verfügung stehenden Verkehrs- und Standortdaten umgehend zu sichern.

Diese Rechtsvorschriften müssen durch klare und präzise Regeln sicherstellen, dass bei der Speicherung der fraglichen Daten die für sie geltenden materiellen und prozeduralen Voraussetzungen eingehalten werden und dass die Betroffenen über wirksame Garantien zum Schutz vor Missbrauchsrisiken verfügen."

5 Die Beklagte hat sich in dem fortgeführten Revisionsverfahren nicht mehr zur Sache geäußert.

6 Die Klägerin tritt der Revision entgegen. Sie verteidigt das Urteil des Verwaltungsgerichts und führt ergänzend aus: Die §§ 113a ff. TKG a. F. genügten nicht den Anforderungen, die der EuGH in dem Urteil vom 20. September 2022 für die Vorratsdatenspeicherung aufstelle. Es fehle ein Zusammenhang zwischen den zu speichernden Daten und dem damit verfolgten Ziel. Lediglich für die Übermittlung der Daten an eine Strafverfolgungsbehörde nenne § 113c Abs. 1 TKG a. F. die Zwecke der Verfolgung besonders schwerer Straftaten (Nr. 1) und der Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes (Nr. 2). Für die Vorratsspeicherung selbst fehle eine solche Bestimmung. Der EuGH habe festgestellt, dass das deutsche TKG keine gezielte, sondern eine allgemeine Vorratsdatenspeicherung vorsehe. Denn sie betreffe nahezu alle die Bevölkerung bildenden Personen, ohne dass diese sich auch nur mittelbar in einer Lage befänden, die Anlass zur Strafverfolgung geben könnte. Eine allgemeine und unterschiedslose Speicherung von Verkehrs- und Standortdaten auf Vorrat sei nur bei einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit zulässig. Eine solche Anforderung regele das Telekommunikationsgesetz nicht und sie ergebe sich auch nicht aus einer unionsrechtskonformen Auslegung. Zwar wäre eine Vorratsspeicherung, die auf die Daten beschränkt sei, welche die Identität der Nutzer elektronischer Kommunikationsmittel betreffen, nach dem Urteil des EuGH vom 20. September 2022 zum Zweck der Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit zulässig. Aber auch eine solche Regelung sehe das Telekommunikationsgesetz nicht vor und sie ergebe sich auch nicht aus einer unionsrechtskonformen Auslegung.

7 Die Bestimmungen des Telekommunikationsgesetzes über die Vorratsdatenspeicherung von IP-Adressen seien ebenfalls nicht mit dem Unionsrecht vereinbar. Zwar habe der EuGH entschieden, dass eine Rechtsvorschrift, die eine allgemeine und unterschiedslose Vorratsspeicherung allein der IP-Adressen der Quelle einer Verbindung vorsehe, grundsätzlich nicht gegen das Unionsrecht verstoße. Diese Möglichkeit müsse aber von der strikten Einhaltung der materiellen und prozeduralen Voraussetzungen abhängig gemacht werden, die die Nutzung dieser Daten regeln müssten. Angesichts der Schwere des mit der Vorratsdatenspeicherung verbundenen Eingriffs in die Grundrechte seien neben

dem Schutz der nationalen Sicherheit nur die Bekämpfung schwerer Kriminalität und die Verhütung schwerer Bedrohungen der öffentlichen Sicherheit geeignet, diesen Eingriff zu rechtfertigen. Ferner fehle es an einer Normierung der vom EuGH geforderten strengen Voraussetzungen und Garantien hinsichtlich der Auswertung dieser Daten in Form einer Nachverfolgung in Bezug auf die Online-Kommunikation und -Aktivitäten der Betroffenen.

8 Schließlich habe der EuGH festgestellt, dass die im Vorlagebeschluss hervorgehobenen Beschränkungen von Inhalt, Umfang und Dauer der Vorratsspeicherung nicht geeignet seien, die Übereinstimmung der §§ 113a ff. TKG a. F. mit den Bestimmungen des Unionsrechts herzustellen. Denn die auf Vorrat gespeicherten Daten ermöglichten insbesondere die Erstellung eines Profils der betroffenen Personen. Die Vorkehrungen, die die gespeicherten Daten gegen Missbrauchsrisiken und vor jedem unberechtigten Zugang schützen sollten, könnten nach der Entscheidung des EuGH den schwerwiegenden Eingriff, der in der vorausgegangenen Speicherung liege, weder beschränken noch beseitigen.

II

9 Die Revision der Beklagten, über die der Senat mit Einverständnis der Verfahrensbeteiligten ohne weitere mündliche Verhandlung entscheidet (§ 141 Satz 1, § 125 Abs. 1 Satz 1 i. V. m. § 101 Abs. 2 VwGO), ist unbegründet und daher zurückzuweisen (§ 144 Abs. 2 VwGO), wobei der Feststellungsausspruch durch die Bezugnahme auf die nunmehr maßgeblichen Vorschriften zu modifizieren ist. Das angefochtene Urteil beruht nicht auf der Verletzung revisiblen Rechts (§ 137 Abs. 1 VwGO). Das Verwaltungsgericht hat die Feststellungsklage nach § 43 VwGO zutreffend als zulässig (1.) und begründet (2.) erachtet.

10 1. Nach § 43 VwGO kann durch Klage die Feststellung des Bestehens oder Nichtbestehens eines Rechtsverhältnisses begehrt werden, wenn der Kläger ein berechtigtes Interesse an der baldigen Feststellung hat (§ 43 Abs. 1 VwGO) und soweit er seine Rechte nicht durch Gestaltungs- oder Leistungsklage verfolgen kann oder hätte verfolgen können (§ 43 Abs. 2 Satz 1 VwGO). Diese Vorausset-

zungen sind, wovon der Senat bereits in seinem Vorlagebeschluss vom 25. September 2019 (BVerwG 6 C 13.18) implizit ausgegangen ist, für die von der Klägerin erhobene Klage erfüllt.

11 a) Zwischen den Beteiligten steht ein konkretes und damit feststellungsfähiges Rechtsverhältnis in Streit. Die Klägerin hat mit ihrem Hauptantrag die Feststellung begehrt, dass sie nicht verpflichtet ist, die in § 113b Abs. 3 Nr. 1 bis 3 des Telekommunikationsgesetzes vom 22. Juni 2004 (TKG a. F.) in der Fassung von Art. 2 Nr. 2 des Gesetzes vom 10. Dezember 2015 (BGBI. I 2218) genannten Telekommunikations-Verkehrsdaten ihrer Kunden, denen sie den Internetzugang vermittelt, und die in § 113b Abs. 2 Satz 1 und 2 TKG a. F. genannten Telekommunikations-Verkehrsdaten ihrer Kunden, denen sie den Zugang zu öffentlichen Telefondiensten vermittelt, zu speichern. Da das Feststellungsbegehren der Klägerin erkennbar auf die Klärung ihrer künftigen Handlungspflichten zielt, ist zu berücksichtigen, dass das Telekommunikationsgesetz vom 22. Juni 2004 gemäß Art. 61 Abs. 1 des Gesetzes 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) vom 23. Juni 2021 (BGBl. I S. 1858) am 1. Dezember 2021 außer Kraft getreten ist. Abgesehen von einigen sprachlichen Anpassungen aufgrund geänderter Begriffsbestimmungen in § 3 TKG (vgl. hierzu BT-Drs. 19/26108 S. 369 f. zu den §§ 174 ff. in der Fassung des Gesetzentwurfs) sind die Vorschriften der bisherigen §§ 113a bis 113g TKG a. F. jedoch inhaltlich weitestgehend unverändert in den nunmehr geltenden §§ 175 bis 181 TKG übernommen worden.

12 Die Klägerin unterfällt nunmehr gemäß § 175 Abs. 1 Satz 1 TKG als Anbieter öffentlich zugänglicher Telekommunikationsdienste für Endnutzer, bei denen es sich nicht um nummernunabhängige interpersonelle Telekommunikationsdienste handelt, – ebenso wie zuvor nach § 113a Abs. 1 Satz 1 TKG a. F. als Erbringer öffentlich zugänglicher Telekommunikationsdienste für Endnutzer – den inhaltlich unveränderten Verpflichtungen zur Speicherung von Verkehrsdaten, zur Verwendung der Daten und zur Datensicherheit nach den §§ 176 bis 181

TKG (zuvor §§ 113b bis 113g TKG a. F.). Der Begriff der Telekommunikationsdienste umfasst gemäß § 3 Nr. 61 Buchst. a TKG auch Internetzugangsdienste.

13 Gegenstand des Rechtsverhältnisses ist zum einen das Bestehen der Verpflichtung der Klägerin, als Anbieterin von Sprachkommunikationsdiensten gemäß § 176 Abs. 2 Satz 1 Nr. 1 bis 5 TKG (§ 113b Abs. 2 Satz 1 Nr. 1 bis 5 TKG a. F.) die dort im Einzelnen genannten Daten zu speichern. Hierzu gehören die Rufnummer oder eine andere Kennung der beteiligten Anschlüsse, Datum und Uhrzeit von Beginn und Ende der Verbindung unter Angabe der zugrunde liegenden Zeitzone, Angaben zu dem genutzten Dienst, im Fall mobiler Sprachkommunikationsdienste ferner die internationale Kennung mobiler Endnutzer für den anrufenden und den angerufenen Anschluss, die internationale Kennung des anrufenden und des angerufenen Endgerätes, Datum und Uhrzeit der ersten Aktivierung bei im Voraus bezahlten Diensten, und im Falle von Internet-Sprachkommunikationsdiensten auch die Internetprotokoll-Adressen (im Folgenden: IP-Adressen) des anrufenden und des angerufenen Anschlusses und zugewiesene Benutzerkennungen. Das Rechtsverhältnis umfasst ferner das Bestehen oder Nichtbestehen der Verpflichtung der Klägerin gemäß § 176 Abs. 2 Satz 2 Nr. 1 und 2 TKG (§ 113b Abs. 2 Satz 2 Nr. 1 und 2 TKG a. F.) zur entsprechenden Speicherung der genannten Daten bei der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht, wobei hier die Zeitpunkte der Versendung und des Empfangs der Nachricht maßgeblich sind, sowie in bestimmten Fällen unbeantworteter oder wegen eines Eingriffs des Netzwerkmanagements erfolgloser Anrufe. Gegenstand des maßgeblichen Rechtsverhältnisses ist schließlich auch das Bestehen der Verpflichtung der Klägerin, als Anbieterin öffentlich zugänglicher Internetzugangsdienste gemäß § 176 Abs. 3 Nr. 1 bis 3 TKG (§ 113b Abs. 3 Nr. 1 bis 3 TKG a. F.) die dem Teilnehmer bzw. Endnutzer für eine Internetnutzung zugewiesene IP-Adresse, eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt, eine zugewiesene Benutzerkennung sowie Datum und Uhrzeit von Beginn und Ende der Internetnutzung unter der zugewiesenen IP-Adresse unter Angabe der zugrunde liegenden Zeitzone zu speichern.

14 Im Hinblick auf diese unmittelbar durch das Gesetz begründeten Speicherpflichten werden nicht lediglich abstrakte Rechtsfragen in Bezug auf möglicherweise eintretende Beeinträchtigungen im Wege der Feststellungsklage zur gerichtlichen Klärung gestellt. Eine weitere Verdichtung der Rechtsbeziehungen ist nicht erforderlich. Die Annahme eines konkreten und damit feststellungsfähigen Rechtsverhältnisses setzt insbesondere keine Aktualisierung der gesetzlichen Speicherpflichten durch einen behördlichen Vollzugsakt voraus. Ein Verwaltungsvollzug durch die Bundesnetzagentur ist zwar auf der Grundlage der gesetzlichen Befugnisnormen zur Kontrolle und Durchsetzung der Verpflichtungen möglich (vgl. § 183 TKG). Entscheidend ist jedoch, dass es sich bei den Regelungen der §§ 175, 176 TKG (§§ 113a, 113b TKG a. F.) um sog. "self-executing" Normen handelt, die von den betroffenen Unternehmen unmittelbar beachtet werden müssen und nicht auf eine Vollziehung durch die Verwaltung angewiesen sind.

15 Das in Rede stehende konkrete Rechtsverhältnis ist zwischen den Verfahrensbeteiligten streitig. Dass die Bundesnetzagentur als normanwendende Behörde von ihren Befugnissen nach § 183 TKG keinen Gebrauch machen würde, wenn die Klägerin die Verpflichtung zur Vorratsspeicherung der Telekommunikations-Verkehrsdaten missachtet, kann nicht angenommen werden (vgl. zu diesem Gesichtspunkt BVerwG, Urteil vom 23. August 2007 - 7 C 2.07 - BVerwGE 129, 199 Rn. 28). Nichts anderes folgt aus dem Umstand, dass die Bundesnetzagentur, nachdem das Oberverwaltungsgericht durch Beschluss vom 22. Juni 2017 dem Eilantrag eines anderen betroffenen Unternehmens im Beschwerdeverfahren vorläufig stattgegeben hatte, auf ihrer Internetseite die Mitteilung veröffentlicht hat, bis zum rechtskräftigen Abschluss eines Hauptsacheverfahrens von Anordnungen und sonstigen Maßnahmen zur Durchsetzung der in § 113a Abs. 1 i. V. m. § 113b TKG a. F. geregelten Speicherverpflichtung abzusehen und auch keine Bußgeldverfahren gegen die betreffenden Telekommunikationsunternehmen einzuleiten. Denn in der Revisionsbegründung hat die Beklagte klargestellt, dass sie diese Erklärung allein aus Gründen der Rechtsklarheit und zur Gleichbehandlung aller betroffenen Unternehmen abgegeben habe und von ihrer Rechtsposition – der Vereinbarkeit der Regelung mit nationalen und europäi-

schen Vorgaben – nicht abgerückt sei. Diesen Rechtsstandpunkt hat sie ungeachtet des Urteils des EuGH vom 20. September 2022 bisher nicht erkennbar aufgegeben.

16 b) Die Klägerin hat auch das erforderliche berechtigte Interesse an der begehrten Feststellung. Zwar würde sie sich im Fall der Nichtbefolgung der Speicherpflicht aus § 176 TKG (§ 113b TKG a. F.) nach nunmehr geltender Rechtslage nicht mehr dem vom Verwaltungsgericht hervorgehobenen Risiko einer Ahndung als Ordnungswidrigkeit aussetzen. Denn während gemäß § 149 Abs. 1 Nr. 36 TKG a. F. noch ordnungswidrig handelte, wer vorsätzlich oder fahrlässig entgegen § 113b Abs. 1 TKG a. F., auch in Verbindung mit § 113b Abs. 7 TKG a. F., Daten nicht, nicht richtig, nicht vollständig, nicht in der vorgeschriebenen Weise, nicht für die vorgeschriebene Dauer oder nicht rechtzeitig speicherte, enthält der Katalog in § 228 Abs. 2 TKG keine entsprechende Bußgeldvorschrift mehr. Hierdurch entfällt jedoch nicht das Interesse der Klägerin an der baldigen Herstellung von Rechtsklarheit im Zusammenhang mit dem Umfang ihrer rechtlichen Verpflichtungen bei der durch Art. 12 Abs. 1 GG geschützten Ausübung ihrer unternehmerischen Tätigkeit.

17 c) Wird die Gewährung vorbeugenden Rechtsschutzes begehrt, ist zwar zusätzlich ein besonderes schützenswertes Interesse in dem Sinn erforderlich, dass es für den Betroffenen nicht zumutbar ist, auf den von der Verwaltungsgerichtsordnung für den Regelfall vorgesehenen nachgängigen Rechtsschutz verwiesen zu werden (stRspr, vgl. BVerwG, Urteile vom 22. Oktober 2014 - 6 C 7.13 - Buchholz 402.41 Allgemeines Polizeirecht Nr. 104 Rn. 17 und vom 13. Dezember 2017 - 6 A 6.16 - BVerwGE 161, 76 Rn. 15). Entgegen der Auffassung des Verwaltungsgerichts liegt ein solcher Fall hier jedoch nicht vor. Nach der Übergangsvorschrift des § 150 Abs. 13 Satz 1 TKG a. F. waren die Speicherverpflichtung und die damit verbundenen Verpflichtungen nach den §§ 113b bis 113e und 113g TKG a. F. zwar erst ab dem 1. Juli 2017 zwingend zu erfüllen. Zum Zeitpunkt der Erhebung der Feststellungsklage im Mai 2017 handelte es sich also noch um eine zukünftige Verpflichtung. Diesem Umstand kommt jedoch im vorliegenden Zusammenhang keine Bedeutung mehr zu. Denn maßgebender Zeitpunkt für das Vorliegen der Sachurteilsvoraussetzungen ist der Zeitpunkt der letzten mündlichen Verhandlung oder – in den Fällen des § 101 Abs. 2 VwGO – der

Entscheidung des erkennenden Gerichts (vgl. BVerwG, Urteile vom 23. Juni 1995 - 3 C 6.94 - Buchholz 451.512 MGVO Nr. 110 S. 83 f. und vom 28. November 2018 - 6 C 3.17 - juris Rn. 29).

18 d) Der Zulässigkeit der Feststellungsklage steht schließlich nicht das Subsidiaritätsgebot des § 43 Abs. 2 Satz 1 VwGO entgegen. Das Verwaltungsgericht hat zutreffend ausgeführt, dass die Klägerin nicht auf die Möglichkeit verwiesen werden kann, eine (vorbeugende) Unterlassungsklage gegen im Fall der Nichterfüllung der in den §§ 175 f. TKG (§§ 113a f. TKG a. F.) geregelten Verpflichtungen zu erwartende Maßnahmen der Bundesnetzagentur auf der Grundlage des § 115 Abs. 1 Satz 1 TKG a. F. (jetzt: § 183 TKG) zu erheben. Gleiches gilt für Anfechtungsklagen nach Erlass derartiger – als Verwaltungsakte einzustufender – Maßnahmen. Die Vorschrift des § 43 Abs. 2 Satz 1 VwGO ist nach ständiger Rechtsprechung des Bundesverwaltungsgerichts ihrem Zweck entsprechend einschränkend auszulegen und anzuwenden. Droht keine Umgehung der für Anfechtungs- und Verpflichtungsklagen geltenden Bestimmungen über Fristen und die Durchführung eines Vorverfahrens, steht § 43 Abs. 2 VwGO der Feststellungsklage ebenso wenig entgegen wie in Fällen, in denen diese den effektiveren Rechtsschutz bietet. Kann die zwischen den Parteien streitige Frage sachgerecht und ihrem Rechtsschutzinteresse voll Rechnung tragend durch Feststellungsurteil geklärt werden, verbietet es sich, die Klägerin auf eine Gestaltungs- oder Leistungsklage zu verweisen, in deren Rahmen das Rechtsverhältnis, an dessen selbstständiger Feststellung sie ein berechtigtes Interesse hat, einerseits nur Vorfrage wäre, andererseits die weiteren Elemente des geltend zu machenden Anspruchs nur untergeordnete Bedeutung hätten (BVerwG, Urteile vom 29. April 1997 - 1 C 2.95 - Buchholz 310 § 43 VwGO Nr. 127 S. 9 und vom 30. Mai 2018 - 6 A 3.16 - BVerwGE 162, 179 Rn. 56). Diese Voraussetzungen liegen hier vor. Die Feststellungsklage bietet den sachgerechten und effektiveren Rechtsschutz. Denn die Klägerin wäre ansonsten gehalten, jede Einzelmaßnahme, die die Bundesnetzagentur zur Durchsetzung der in den § 175 Abs. 1 Satz 1 i. V. m. § 176 Abs. 2 und 3 TKG (§ 113a Abs. 1 Satz 1 i. V. m. § 113b Abs. 2 und 3 TKG a. F.) geregelten Verpflichtungen der Klägerin erlässt, gesondert anzugreifen, obwohl es ihr allein um die Klärung der Vorfrage geht, ob die gesetzliche Pflicht zur Speicherung der Telekommunikations-Verkehrsdaten überhaupt besteht.

19 2. Die angefochtene Entscheidung ist auch in der Sache nicht zu beanstanden. Das Verwaltungsgericht hat ohne Verstoß gegen revisibles Recht festgestellt, dass die Klägerin nicht verpflichtet ist, die in § 113b Abs. 3 Nr. 1 bis 3 TKG a. F. genannten Telekommunikations-Verkehrsdaten ihrer Kunden, denen sie den Internetzugang vermittelt, und die in § 113b Abs. 2 Satz 1 und 2 TKG a. F. genannten Telekommunikations-Verkehrsdaten ihrer Kunden, denen sie den Zugang zu öffentlichen Telefondiensten vermittelt, zu speichern. Der Feststellungsausspruch der Vorinstanz ist mit der Maßgabe aufrechtzuerhalten, dass die Klägerin nicht verpflichtet ist, die in § 176 Abs. 3 Nr. 1 bis 3 TKG aufgeführten Telekommunikations-Verkehrsdaten ihrer Kunden, denen sie den Internet-Zugang vermittelt, und die in § 176 Abs. 2 Satz 1 und 2 TKG genannten Telekommunikations-Verkehrsdaten ihrer Kunden, denen sie den Zugang zu öffentlichen Telefondiensten vermittelt, zu speichern. Durch die auf das Vorabentscheidungsersuchen des Senats ergangene Entscheidung des EuGH vom 20. September 2022 - C-793/19 und C-794/19 - ist geklärt, dass die in § 113a Abs. 1 i. V. m. § 113b TKG a. F. angeordnete Speicherpflicht gegen Unionsrecht verstößt. Dies gilt entsprechend für die nunmehr in § 175 Abs. 1 Satz 1 i. V. m. § 176 TKG geregelte, inhaltlich unveränderte Verpflichtung.

20 a) Nach der Rechtsprechung des EuGH fällt eine nationale Regelung, die die Betreiber elektronischer Kommunikationsdienste insbesondere zum Schutz der nationalen Sicherheit und zur Bekämpfung der Kriminalität zur Vorratsspeicherung von Verkehrs- und Standortdaten verpflichtet, in den Geltungsbereich 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) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 geänderten Fassung - Richtlinie 2002/58/EG - (EuGH, Urteil vom 20. September 2022 - C-793/19 und C-794/19 - Rn. 48). Hiervon ist auch der Senat bereits in seinem Vorabentscheidungsersuchen ausgegangen (BVerwG, Beschluss vom 25. September 2019 - 6 C 13.18 - juris Rn. 19).

21 b) Die in § 175 Abs. 1 Satz 1 i. V. m. § 176 TKG (§ 113a Abs. 1 Satz 1 i. V. m. § 113b TKG a. F.) geregelte Pflicht zur Speicherung der Telekommunikations-Verkehrsdaten beschränkt die in Art. 5 Abs. 1, Art. 6 Abs. 1 und Art. 9 Abs. 1 der Richtlinie 2002/58/EG geregelten Rechte und Pflichten.

22 Nach Art. 5 Abs. 1 Satz 1 und 2 der Richtlinie 2002/58/EG sind die Mitgliedstaaten verpflichtet, die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten durch innerstaatliche Vorschriften sicherzustellen. Sie sind insbesondere verpflichtet, das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Nachrichten und der damit verbundenen Verkehrsdaten durch andere Personen als die Nutzer zu untersagen, wenn keine Einwilligung der betroffenen Nutzer vorliegt, es sei denn, dass diese Personen gemäß Art. 15 Abs. 1 der Richtlinie gesetzlich dazu ermächtigt sind (EuGH, Urteil vom 20. September 2022 - C-793/19 und C-794/19 - Rn. 51). Insoweit hat der EuGH entschieden, dass in Art. 5 Abs. 1 der Richtlinie 2002/58/EG der Grundsatz der Vertraulichkeit sowohl elektronischer Nachrichten als auch der damit verbundenen Verkehrsdaten aufgestellt wird, der u. a. das grundsätzliche Verbot für jede andere Person als die Nutzer, ohne deren Einwilligung solche Nachrichten und Daten auf Vorrat zu speichern, impliziert (EuGH, Urteil vom 20. September 2022 - C-793/19 und C-794/19 - Rn. 52). Dass die in § 175 Abs. 1 Satz 1 i. V. m. § 176 TKG (§ 113a Abs. 1 Satz 1 i. V. m. § 113b TKG a. F.) geregelte Pflicht zur Speicherung der Telekommunikations-Verkehrsdaten einen Eingriff in die durch die Richtlinie geschützte Vertraulichkeit der elektronischen Kommunikation darstellt und dem Grundsatz widerspricht, dass es jeder anderen Person als dem Nutzer grundsätzlich untersagt ist, ohne dessen Einwilligung mit elektronischen Kommunikationen verbundene Verkehrsdaten zu speichern, hat der Senat in seinem Vorabentscheidungsersuchen bereits ausgeführt (BVerwG, Beschluss vom 25. September 2019 - 6 C 13.18 - juris Rn. 20).

23 Art. 6 Abs. 1 der Richtlinie 2002/58/EG sieht vor, dass die sich auf Teilnehmer und Nutzer beziehenden Verkehrsdaten von den Betreibern elektronischer Kommunikationsdienste zu löschen oder zu anonymisieren sind, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden. In Art. 6 Abs. 2

der Richtlinie wird klargestellt, dass Verkehrsdaten, die zum Zweck der Gebührenabrechnung und der Bezahlung von Zusammenschaltungen erforderlich sind, nur bis zum Ablauf der Frist verarbeitet werden dürfen, innerhalb deren die Rechnung rechtlich angefochten oder der Anspruch auf Zahlung geltend gemacht werden kann. Andere Standortdaten als Verkehrsdaten dürfen nach Art. 9 Abs. 1 der Richtlinie nur unter bestimmten Voraussetzungen und nur dann verarbeitet werden, wenn sie anonymisiert wurden oder wenn die Nutzer oder Teilnehmer ihre Einwilligung gegeben haben. Nach der Rechtsprechung des EuGH folgt hieraus, dass sich die Richtlinie 2002/58/EG nicht darauf beschränkt, den Zugang zu solchen Daten durch Garantien zu regeln, die Missbrauch verhindern sollen, sondern sie insbesondere auch den Grundsatz des Verbots der Speicherung dieser Daten durch Dritte regelt (EuGH, Urteil vom 20. September 2022 - C-793/19 und C-794/19 - Rn. 56). Diesem Grundsatz widerspricht die in § 175 Abs. 1 Satz 1 i. V. m. § 176 TKG (§ 113a Abs. 1 Satz 1 i. V. m. § 113b TKG a. F.) normierte Pflicht zur Speicherung der Telekommunikations-Verkehrsdaten, die sich nach § 176 Abs. 1 Nr. 2 i. V. m. Abs. 4 TKG (§ 113b Abs. 1 Nr. 2 i. V. m. Abs. 4 TKG a. F.) auch auf die dort genannten Standortdaten erstreckt (vgl. BVerwG, Beschluss vom 25. September 2019 - 6 C 13.18 - juris Rn. 20).

24 c) Die Beschränkung der in Art. 5 Abs. 1, Art. 6 Abs. 1 und Art. 9 Abs. 1 der Richtlinie 2002/58/EG geregelten Rechte und Pflichten sowie der hierin zum Ausdruck kommenden Grundsätze der Vertraulichkeit der Kommunikation und des Verbots der Speicherung der damit verbundenen Daten durch die in § 175 Abs. 1 Satz 1 i. V. m. § 176 TKG (§ 113a Abs. 1 Satz 1 i. V. m. § 113b TKG a. F.) auferlegte Verpflichtung der Betreiber elektronischer Kommunikationsdienste zur Speicherung der Telekommunikations-Verkehrsdaten kann nicht auf Art. 15 Abs. 1 der Richtlinie 2002/58/EG gestützt werden. Dies ist durch das auf das Vorabentscheidungsersuchen des Senats ergangene Urteil des EuGH vom 20. September 2022 - C-793/19 und C-794/19 - nunmehr abschließend geklärt.

25 aa) Art. 15 Abs. 1 der Richtlinie 2002/58/EG ermächtigt die Mitgliedstaaten zum Erlass von Rechtsvorschriften, die die Rechte und Pflichten gemäß Art. 5, 6, 8 Abs. 1, 2, 3 und 4 sowie Art. 9 dieser Richtlinie beschränken, sofern eine

solche Beschränkung gemäß Art. 13 Abs. 1 der Richtlinie 95/46/EG für die nationale Sicherheit, (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zweck können die Mitgliedstaaten unter anderem durch Rechtsvorschriften vorsehen, dass Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden. Die Maßnahmen müssen den allgemeinen Grundsätzen des Unionsrechts einschließlich den in Art. 6 Abs. 1 und 2 des Vertrags über die Europäische Union (EUV) niedergelegten Grundsätzen entsprechen.

26 (1) Der EuGH hat in seiner Entscheidung vom 20. September 2022 hervorgehoben, dass Art. 15 Abs. 1 der Richtlinie 2002/58/EG als Ausnahmebestimmung eng auszulegen ist. Soll die Vorschrift nicht weitgehend ausgehöhlt werden, darf die Ausnahme von der grundsätzlichen Verpflichtung, die Vertraulichkeit der elektronischen Kommunikation und der damit verbundenen Daten sicherzustellen, und insbesondere von dem in Art. 5 der Richtlinie 2002/58/EG vorgesehenen Verbot, diese Daten zu speichern, nicht zur Regel werden. Die Aufzählung der in Art. 15 Abs. 1 Satz 1 der Richtlinie genannten Zwecke, die eine Beschränkung der insbesondere in Art. 5, 6 und 9 der Richtlinie 2002/58/EG vorgesehenen Rechte und Pflichten rechtfertigen, ist abschließend. Wie aus Art. 15 Abs. 1 Satz 3 der Richtlinie folgt, müssen außerdem die allgemeinen Grundsätze des Unionsrechts, zu denen der Grundsatz der Verhältnismäßigkeit gehört, und die durch die Charta der Grundrechte der Europäischen Union (GRC) garantierten Grundrechte beachtet werden. Die Speicherung der Verkehrs- und Standortdaten stellt als solche nicht nur eine Abweichung von dem nach Art. 5 Abs. 1 der Richtlinie 2002/58/EG für alle anderen Personen als die Nutzer geltenden Verbot der Speicherung dieser Daten dar, sondern auch einen Eingriff in die Grundrechte auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten, die in Art. 7 und 8 GRC verankert sind. Dabei spielt es keine Rolle, ob die betreffenden Informationen über das Privatleben sensiblen Charakter haben und ob die Betroffenen durch diesen Eingriff Nachteile erlitten haben oder ob die gespeicherten Daten in der Folge verwendet werden oder nicht. Denn die

Verkehrs- und Standortdaten können Informationen über eine Vielzahl von Aspekten des Privatlebens der Betroffenen enthalten und insbesondere die Erstellung eines Profils der Betroffenen ermöglichen, das im Hinblick auf das Recht auf Achtung des Privatlebens eine ebenso sensible Information darstellt wie der Inhalt der Kommunikationen selbst. Daher kann die Vorratsspeicherung von Verkehrs- und Standortdaten zu polizeilichen Zwecken nicht nur das in Art. 7 GRC verankerte Recht auf Achtung der Kommunikation beeinträchtigen, sondern die Nutzer elektronischer Kommunikationsmittel auch von der Ausübung ihrer durch Art. 11 GRC gewährleisteten Freiheit der Meinungsäußerung abhalten. Angesichts der großen Menge von Verkehrs- und Standortdaten, die durch eine Maßnahme allgemeiner und unterschiedsloser Vorratsspeicherung kontinuierlich gespeichert werden können, sowie des sensiblen Charakters der Informationen, die diese Daten liefern können, birgt die bloße Vorratsspeicherung durch die Betreiber elektronischer Kommunikationsdienste zudem Gefahren des Missbrauchs und des rechtswidrigen Zugangs (EuGH, Urteil vom 20. September 2022 - C-793/19 und C-794/19 - Rn. 57 bis 62).

27 (2) In Art. 15 Abs. 1 der Richtlinie 2002/58/EG kommt nach Ansicht des EuGH zwar zum Ausdruck, dass die in Art. 7, 8 und 11 GRC verankerten Rechte keine uneingeschränkte Geltung beanspruchen können, sondern im Hinblick auf ihre gesellschaftliche Funktion gesehen werden müssen. Denn nach Art. 52 Abs. 1 GRC sind Einschränkungen der Ausübung dieser Rechte zulässig, sofern sie gesetzlich vorgesehen sind und den Wesensgehalt dieser Rechte achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit müssen sie erforderlich sein und den von der Union anerkannten, dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen. Bei der Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58/EG im Licht der Charta muss somit auch berücksichtigt werden, welche Bedeutung den in Art. 3, 4, 6 und 7 GRC verankerten Rechten und den Zielen des Schutzes der nationalen Sicherheit und der Bekämpfung schwerer Kriminalität als Beitrag zum Schutz der Rechte und Freiheiten anderer zukommt. In Bezug auf die wirksame Bekämpfung von Straftaten, deren Opfer u. a. Minderjährige und andere schutzbedürftige Personen sind, verweist der EuGH auf die positiven Verpflichtungen, die sich aus Art. 7 GRC auch in Bezug auf den

Schutz der Wohnung und der Kommunikation sowie aus Art. 3 und 4 GRC hinsichtlich des Schutzes der körperlichen und geistigen Unversehrtheit der Menschen sowie des Verbots der Folter und unmenschlicher oder erniedrigender Behandlung ergeben können. Die verschiedenen betroffenen berechtigten Interessen und Rechte müssen daher miteinander in Einklang gebracht werden, und es ist ein rechtlicher Rahmen zu schaffen, der diesen Einklang ermöglicht. Der Schutz des Grundrechts auf Achtung des Privatlebens verlangt, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken. Eine dem Gemeinwohl dienende Zielsetzung muss mit den von der Maßnahme betroffenen Grundrechten mittels einer ausgewogenen Gewichtung in Einklang gebracht werden. Sie muss in angemessenem Verhältnis zur Schwere des Eingriffs stehen, der mit einer Beschränkung der u. a. in Art. 5, 6 und 9 der Richtlinie 2002/58/EG vorgesehenen Rechte und Pflichten verbunden ist (EuGH, Urteil vom 20. September 2022 - C-793/19 und C-794/19 - Rn. 63 bis 68).

28 (3) Der EuGH hat ferner klargestellt, dass nationale Rechtsvorschriften, um dem Erfordernis der Verhältnismäßigkeit zu genügen, klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindesterfordernisse aufstellen müssen, sodass die Personen, deren personenbezogene Daten betroffen sind, über ausreichende Garantien verfügen, die einen wirksamen Schutz dieser Daten vor Missbrauchsrisiken ermöglichen. Diese Rechtsvorschriften müssen nach nationalem Recht bindend sein und insbesondere Angaben dazu enthalten, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme, die die Verarbeitung solcher Daten vorsieht, getroffen werden darf, damit gewährleistet ist, dass sich der Eingriff auf das absolut Notwendige beschränkt. Nationale Rechtsvorschriften, die eine Vorratsspeicherung personenbezogener Daten vorsehen, müssen daher stets objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen (EuGH, Urteil vom 20. September 2022 - C-793/19 und C-794/19 - Rn. 69 f.).

29 (4) Hinsichtlich der dem Gemeinwohl dienenden Ziele, die eine nach Art. 15 Abs. 1 der Richtlinie 2002/58/EG erlassene Vorschrift rechtfertigen können, geht der EuGH davon aus, dass nach dem Grundsatz der Verhältnismäßigkeit

eine Hierarchie zwischen diesen Zielen entsprechend ihrer jeweiligen Bedeutung besteht und die Bedeutung des mit einer solchen Vorschrift verfolgten Ziels im Verhältnis zur Schwere des daraus resultierenden Eingriffs stehen muss (EuGH, Urteil vom 20. September 2022 - C-793/19 und C-794/19 - Rn. 71).

30 (a) In Bezug auf den Schutz der nationalen Sicherheit, dessen Bedeutung diejenige der übrigen von Art. 15 Abs. 1 der Richtlinie 2002/58/EG erfassten Ziele übersteigt, hat der EuGH festgestellt, dass diese Bestimmung im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 GRC Rechtsvorschriften nicht entgegensteht, die es zum Schutz der nationalen Sicherheit gestatten, den Betreibern elektronischer Kommunikationsdienste aufzugeben, Verkehrs- und Standortdaten allgemein und unterschiedslos auf Vorrat zu speichern. Das gilt aber nur dann, wenn sich der betreffende Mitgliedstaat einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit gegenübersieht, sofern diese Anordnung Gegenstand einer wirksamen, zur Prüfung des Vorliegens einer solchen Situation sowie der Beachtung der vorzusehenden Bedingungen und Garantien dienenden Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle sein kann, deren Entscheidung bindend ist, und sofern die Anordnung nur für einen auf das absolut Notwendige begrenzten, aber im Fall des Fortbestands der Bedrohung verlängerbaren Zeitraum ergeht (EuGH, Urteil vom 20. September 2022 - C-793/19 und C-794/19 - Rn. 72).

31 (b) Auf das Ziel der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten bezogen hat der EuGH entschieden, dass im Einklang mit dem Grundsatz der Verhältnismäßigkeit nur die Bekämpfung schwerer Kriminalität und die Verhütung ernster Bedrohungen der öffentlichen Sicherheit geeignet sind, die mit der Speicherung von Verkehrs- und Standortdaten verbundenen schweren Eingriffe in die Grundrechte zu rechtfertigen, die in Art. 7 und 8 GRC verankert sind. Weitergehend hat der EuGH in Bezug auf solche nationalen Rechtsvorschriften, die die allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen, hervorgehoben, dass diese angesichts des sensiblen Charakters der Informationen, die sich hieraus ergeben können und der abschreckenden Wirkungen, die die Speicherung dieser Daten auf die Ausübung der in Art. 7 und 11 GRC verankerten Grundrechte haben

kann, selbst dann die Grenzen des absolut Notwendigen überschreiten und nicht als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden können, wenn sie den Zielen der Bekämpfung schwerer Kriminalität und der Verhütung ernster Bedrohungen der öffentlichen Sicherheit dienen (EuGH, Urteil vom 20. September 2022 - C-793/19 und C-794/19 - Rn. 74).

32 Die Entscheidung des EuGH belässt es nicht bei diesen allgemeinen Grundsätzen. Sie enthält detaillierte Vorgaben dazu, mit welchem Regelungsinhalt und unter welchen Voraussetzungen nationale Rechtsvorschriften, die zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit eine Vorratsspeicherung von Daten vorsehen, mit Art. 15 Abs. 1 der Richtlinie 2002/58/EG im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 GRC vereinbar sind. Der EuGH unterscheidet insoweit vier Kategorien von Regelungen: Erstens können nationale Rechtsvorschriften auf der Grundlage objektiver und nicht diskriminierender Kriterien anhand von Kategorien betroffener Personen oder mittels eines geografischen Kriteriums für einen auf das absolut Notwendige begrenzten, aber verlängerbaren Zeitraum eine gezielte Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen. Zweitens können sie für einen auf das absolut Notwendige begrenzten Zeitraum eine allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, vorsehen. Drittens können sie eine allgemeine und unterschiedslose Vorratsspeicherung der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten vorsehen. Viertens können sie vorsehen, dass den Betreibern elektronischer Kommunikationsdienste mittels einer Entscheidung der zuständigen Behörde, die einer wirksamen gerichtlichen Kontrolle unterliegt, aufgegeben werden kann, während eines festgelegten Zeitraums die ihnen zur Verfügung stehenden Verkehrs- und Standortdaten umgehend zu sichern *(quick freeze)*. Der EuGH hebt hervor, dass diese Rechtsvorschriften durch klare und präzise Regeln sicherstellen müssen, dass bei der Speicherung der fraglichen Daten die für sie geltenden materiellen und prozeduralen Voraussetzungen eingehalten werden und dass die Betroffenen über wirksame Garantien zum Schutz vor Missbrauchsrisiken verfügen (EuGH, Urteil vom 20. September 2022 - C-793/19 und C-794/19 - Rn. 75).

33 bb) Hiervon ausgehend hat der EuGH die von dem erkennenden Senat als vorlegendem Gericht hervorgehobenen Merkmale der nationalen Regelung in § 113a Abs. 1 Satz 1 i. V. m. § 113b TKG a. F. unter Berücksichtigung der Erwägungen des Senats im Vorabentscheidungsersuchen (BVerwG, Beschluss vom 25. September 2019 - 6 C 13.18 - juris Rn. 26 ff.) konkret geprüft.

34 (1) Hinsichtlich des Umfangs der auf Vorrat gespeicherten Daten (vgl. hierzu BVerwG, Beschluss vom 25. September 2019 - 6 C 13.18 - juris Rn. 27) hat der EuGH darauf hingewiesen, dass die im Telekommunikationsgesetz vorgesehene Vorratsspeicherung von Verkehrs- und Standortdaten nahezu alle die Bevölkerung bildenden Personen betrifft, ohne dass diese sich auch nur mittelbar in einer Lage befänden, die Anlass zur Strafverfolgung geben könnte. Ebenso schreibt sie die anlasslose, flächendeckende und personell, zeitlich und geografisch undifferenzierte Vorratsspeicherung eines Großteils der Verkehrs- und Standortdaten vor. Es handelt sich somit nicht um eine gezielte Vorratsdatenspeicherung. Dieser Einschätzung steht nach Ansicht des EuGH weder der Umstand entgegen, dass die Regelung den Inhalt der Kommunikation sowie die Daten über aufgerufene Internetseiten von der Speicherpflicht ausnimmt und die Speicherung der Funkzellenkennung lediglich zu Beginn der Kommunikation vorschreibt, noch dass Daten betreffend E-Mail-Dienste sowie die elektronische Kommunikation bestimmter Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen nicht von der Pflicht zur Vorratsspeicherung erfasst werden (EuGH, Urteil vom 20. September 2022 - C-793/19 und C-794/19 - Rn. 76 bis 84).

35 (2) Weiter hat der EuGH zwar festgestellt, dass die Vorratsspeicherungsfristen, die gemäß § 113b Abs. 1 TKG a. F. vier Wochen für Standortdaten und zehn Wochen für sonstige Daten betragen (vgl. hierzu BVerwG, Beschluss vom 25. September 2019 - 6 C 13.18 - juris Rn. 28), deutlich kürzer als die Fristen sind, die in denjenigen nationalen Regelungen, die eine Pflicht zur allgemeinen und unterschiedslosen Vorratsspeicherung vorschreiben, vorgesehen sind, die er in seinen früheren Urteilen geprüft hat. Der EuGH hat jedoch hervorgehoben, dass die Speicherung von Verkehrs- oder Standortdaten, die Informationen über die Kommunikationen des Nutzers eines elektronischen Kommunikationsmittels oder über den Standort der von ihm verwendeten Endgeräte liefern können, in

jedem Fall schwerwiegend ist, unabhängig von der Länge des Speicherzeitraums und von der Menge oder Art der gespeicherten Daten, sofern der Datensatz geeignet ist, sehr genaue Schlüsse auf das Privatleben der betroffenen Person bzw. der betroffenen Personen zuzulassen. Hiervon ist nach Ansicht des EuGH auch im vorliegenden Fall bei den nach den §§ 113a f. TKG a. F. zu speichernden Daten auszugehen (EuGH, Urteil vom 20. September 2022 - C-793/19 und C-794/19 - Rn. 85 bis 90).

36 (3) Die in der deutschen Regelung vorgesehenen Garantien, die die gespeicherten Daten gegen Missbrauchsrisiken und vor jedem unberechtigten Zugang schützen sollen (vgl. hierzu BVerwG, Beschluss vom 25. September 2019 - 6 C 13.18 - juris Rn. 29 f.), hat der EuGH im vorliegenden Zusammenhang nicht für relevant gehalten. Denn die Vorratsspeicherung dieser Daten und der Zugang zu ihnen stellen unterschiedliche Eingriffe in die in Art. 7 und 11 GRC garantierten Grundrechte dar, die eine gesonderte Rechtfertigung nach Art. 52 Abs. 1 GRC erfordern. Daher können nationale Rechtsvorschriften, die die vollständige Einhaltung der Voraussetzungen gewährleisten, die sich im Bereich des Zugangs zu auf Vorrat gespeicherten Daten aus der Rechtsprechung zur Auslegung der Richtlinie 2002/58/EG ergeben, den schwerwiegenden Eingriff weder beschränken noch beseitigen, der sich aus der nach diesen nationalen Rechtsvorschriften vorgesehenen allgemeinen Vorratsspeicherung dieser Daten in die Rechte ergeben würde, die in Art. 5 und 6 dieser Richtlinie und in den durch diese Vorschriften konkretisierten Grundrechten garantiert werden (EuGH, Urteil vom 20. September 2022 - C-793/19 und C-794/19 - Rn. 91).

37 (4) Der EuGH ist außerdem der – seitens der Kommission befürworteten – Gleichsetzung von schwerer Kriminalität und einer Bedrohung der nationalen Sicherheit entgegengetreten. In diesem Zusammenhang hat er klargestellt, dass das Ziel der Wahrung der nationalen Sicherheit dem zentralen Anliegen entspricht, die wesentlichen Funktionen des Staates und die grundlegenden Interessen der Gesellschaft durch die Verhütung und Repression von Tätigkeiten zu schützen, die geeignet sind, die tragenden Strukturen eines Landes im Bereich der Verfassung, Politik oder Wirtschaft oder im sozialen Bereich in schwerwiegender Weise zu destabilisieren und insbesondere die Gesellschaft, die Bevölke-

rung oder den Staat als solchen unmittelbar zu bedrohen, wie etwa terroristische Aktivitäten. Im Unterschied zur Kriminalität – auch besonders schwerer Kriminalität – muss eine Bedrohung für die nationale Sicherheit real und aktuell, zumindest aber vorhersehbar sein, was das Eintreten hinreichend konkreter Umstände voraussetzt, um eine Maßnahme allgemeiner und unterschiedsloser Vorratsspeicherung von Verkehrs- und Standortdaten für einen begrenzten Zeitraum rechtfertigen zu können. Eine solche Bedrohung unterscheidet sich somit ihrer Art, ihrer Schwere und der Besonderheit der sie begründenden Umstände nach von der allgemeinen und ständigen Gefahr, dass – auch schwere – Spannungen oder Störungen der öffentlichen Sicherheit auftreten, oder schwerer Straftaten (EuGH, Urteil vom 20. September 2022 - C-793/19 und C-794/19 - Rn. 92 bis 94).

38 cc) Aus den Ausführungen des EuGH zu dem Vorabentscheidungsersuchen des Senats ergibt sich nunmehr zweifelsfrei, dass die in § 175 Abs. 1 Satz 1 i. V. m. § 176 TKG (§ 113a Abs. 1 Satz 1 i. V. m. § 113b TKG a. F.) geregelte Verpflichtung der Anbieter öffentlich zugänglicher Telekommunikationsdienste zur Speicherung der dort genannten Telekommunikations-Verkehrsdaten in vollem Umfang unvereinbar mit Art. 15 Abs. 1 der Richtlinie 2002/58/EG im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 GRC ist. Denn die Regelung im Telekommunikationsgesetz schreibt keine gezielte Vorratsdatenspeicherung, sondern eine anlasslose, flächendeckende und personell, zeitlich und geografisch undifferenzierte Vorratsspeicherung eines Großteils der Verkehrs- und Standortdaten vor (EuGH, Urteil vom 20. September 2022 - C-793/19 und C-794/19 - Rn. 83 f.). Die vom EuGH herausgearbeiteten engen Voraussetzungen hinsichtlich der Bestimmtheit und Normenklarheit der Regelung, der zulässigen Zwecke sowie der weiteren inhaltlichen und verfahrensmäßigen Anforderungen für eine solche Vorratsdatenspeicherung liegen nicht vor.

39 (1) Die in § 175 Abs. 1 Satz 1 i. V. m. § 176 TKG (§ 113a Abs. 1 Satz 1 i. V. m. § 113b TKG a. F.) geregelte Speicherung der Telekommunikations-Verkehrsdaten genügt insgesamt schon deshalb nicht den unionsrechtlichen Anforderungen, weil keine objektiven Kriterien bestimmt werden, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen. Diese Normen im Telekommunikationsgesetz sehen weder klare und präzise

Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vor noch stellen sie Mindesterfordernisse mit dem Ziel auf, dass die Personen, deren personenbezogene Daten betroffen sind, über ausreichende Garantien verfügen, die einen wirksamen Schutz dieser Daten vor Missbrauchsrisiken ermöglichen. Insbesondere enthalten die genannten Bestimmungen keine Angaben dazu, unter welchen Umständen und Voraussetzungen eine Maßnahme, die die Verarbeitung solcher Daten vorsieht, getroffen werden darf, damit gewährleistet ist, dass sich der Eingriff auf das absolut Notwendige beschränkt (EuGH, Urteil vom 20. September 2022 - C-793/19 und C-794/19 - Rn. 69 f.).

40 Zwar dürfen – mit Ausnahme von IP-Adressen im Rahmen einer Bestandsdatenauskunft, worauf unter (3) noch einzugehen ist – die auf Vorrat gespeicherten Daten nach § 177 Abs. 1 TKG (§ 113c Abs. 1 TKG a. F.) bzw. nur zur Verfolgung besonders schwerer Straftaten oder zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes verwendet werden. Da jedoch die Vorratsspeicherung der genannten Daten und der Zugang zu ihnen unterschiedliche Eingriffe in die in den Art. 7 und 11 GRC garantierten Grundrechte darstellen, die eine gesonderte Rechtfertigung nach Art. 52 Abs. 1 GRC erfordern (EuGH, Urteil vom 20. September 2022 - C-793/19 und C-794/19 - Rn. 91), ist die Begrenzung der Verwendungszwecke in § 177 Abs. 1 TKG (§ 113c Abs. 1 TKG a. F.) von vornherein nicht geeignet, die unionsrechtliche Anforderung klarer und präziser Regeln für die vorgelagerte Maßnahme der Speicherung der Daten zu erfüllen.

41 (2) Soweit die Regelung in § 175 Abs. 1 Satz 1 i. V. m. § 176 Abs. 2 und 4 Satz 1 und 3 TKG (§ 113a Abs. 1 Satz 1 i. V. m. § 113b Abs. 2 und 4 Satz 1 und 3 TKG a. F.) die Erbringung von Telefondiensten und in diesem Zusammenhang insbesondere die Daten betrifft, die erforderlich sind, um die Quelle und den Adressaten einer Nachricht, Datum und Uhrzeit von Beginn und Ende der Verbindung oder – im Fall der Übermittlung von Kurz-, Multimedia- oder ähnlichen Nachrichten – die Zeitpunkte der Versendung und des Empfangs der Nachricht sowie, im Fall der mobilen Nutzung, die Bezeichnung der Funkzellen, die vom Anrufer und vom Angerufenen bei Beginn der Verbindung genutzt wurden, zu identifizieren (vgl. EuGH, Urteil vom 20. September 2022 - C-793/19 und C-794/19 - Rn. 77), fehlt es außerdem an der vom EuGH geforderten strikten

Begrenzung der allgemeinen und unterschiedslosen Vorratsspeicherung von Verkehrs- und Standortdaten auf den Zweck des Schutzes der nationalen Sicherheit (EuGH, Urteil vom 20. September 2022 - C-793/19 und C-794/19 - Rn. 72, 131). Dies gilt selbst dann, wenn die Regelung der Verwendungszwecke in § 177 Abs. 1 TKG (§ 113c Abs. 1 TKG a. F.) auch die vorgelagerte Ebene der Vorratsspeicherung der genannten Daten erfassen würde.

42 (3) Soweit sich die in § 175 Abs. 1 Satz 1 i. V. m. § 176 Abs. 3 und 4 Satz 2 und 3 TKG (§ 113a Abs. 1 Satz 1 i. V. m. § 113b Abs. 3 und 4 Satz 2 und 3 TKG a. F.) geregelte Pflicht zur allgemeinen und unterschiedslosen Vorratsspeicherung auf die Bereitstellung von Internetzugangsdiensten und in diesem Rahmen u. a. auf die dem Teilnehmer zugewiesene IP-Adresse, Datum und Uhrzeit von Beginn und Ende der Internetnutzung unter der zugewiesenen IP-Adresse und, im Fall der mobilen Nutzung, die Bezeichnung der bei Beginn der Internetverbindung genutzten Funkzelle bezieht, fehlt es ebenfalls an der unionsrechtlich gebotenen Begrenzung der Zwecke. Diese umfassen im Fall der IP-Adressen zwar neben dem Schutz der nationalen Sicherheit auch die Bekämpfung schwerer Kriminalität und die Verhütung schwerer Bedrohungen der öffentlichen Sicherheit (EuGH, Urteil vom 20. September 2022 - C-793/19 und C-794/19 - Rn. 75, 83 f.). Eine entsprechende Beschränkung der Speicherungszwecke sieht die Regelung im Telekommunikationsgesetz jedoch nicht vor. Die für die Ermittlung der Speicherungszwecke maßgebliche Regelung der Verwendungszwecke im Rahmen einer Bestandsdatenauskunft geht deutlich über den unionsrechtlichen Rahmen hinaus. Für die frühere Rechtslage nach § 113c Abs. 1 Nr. 3 i. V. m. § 113 Abs. 1 Satz 3 TKG a. F. ist dies offenkundig. Denn danach durfte die dem Teilnehmer für eine Internetnutzung zugewiesene IP-Adresse im Rahmen einer Bestandsdatenauskunft zur Verfolgung jeglicher Straftaten, zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung sowie generell zur Erfüllung der Aufgaben der Nachrichtendienste verwendet werden.

43 Die strengen unionsrechtlichen Anforderungen verfehlt jedoch auch die nunmehr geltende Regelung in § 177 Abs. 1 Nr. 3 i. V. m. § 174 Abs. 1 Satz 3 TKG, die auf die Änderung des § 113 TKG a. F. durch das am 2. April 2021 in Kraft getretene Gesetz vom 30. März 2021 zur Anpassung der Regelungen über die Be-

standsdatenauskunft an die Vorgaben aus der Entscheidung des Bundesverfassungsgerichts vom 27. Mai 2020 (BGBl. I S. 48) zurückgeht. Die Fälle, in denen die in eine Bestandsdatenauskunft aufzunehmenden Daten auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen IP-Adresse bestimmt werden dürfen, sind nunmehr in § 174 Abs. 5 TKG geregelt. Danach reicht es etwa aus, dass zureichende tatsächliche Anhaltspunkte für eine Straftat vorliegen und die in die Auskunft aufzunehmenden Daten erforderlich sind, um den Sachverhalt zu erforschen, den Aufenthaltsort eines Beschuldigten zu ermitteln oder eine Strafe zu vollstrecken (§ 174 Abs. 5 Nr. 1 TKG). Die vom EuGH geforderte Beschränkung auf die Bekämpfung schwerer Kriminalität sieht die Vorschrift nicht vor. Die IP-Adresse kann ferner auch dann Grundlage einer Bestandsdatenauskunft sein, wenn dies im Einzelfall zum Schutz nicht unerheblicher Sachwerte oder zur Verhütung einer Straftat erforderlich ist (§ 174 Abs. 5 Nr. 2 Buchst. a, Nr. 4 Buchst. b Doppelbuchst. aa TKG). Der Schutz nicht unerheblicher Sachwerte kann jedenfalls nicht ohne Weiteres dem vom EuGH herausgearbeiteten Zweck der Verhütung schwerer Bedrohungen der öffentlichen Sicherheit zugeordnet werden. Zudem fehlt es auch in diesem Zusammenhang an einer Begrenzung der zu verhütenden Straftaten auf Fälle schwerer Kriminalität.

44 Eine Verwendung von IP-Adressen im Rahmen einer Bestandsdatenauskunft lässt das Telekommunikationsgesetz ferner auch zur Aufklärung bestimmter Bestrebungen oder Tätigkeiten nach § 3 Abs. 1 des Bundesverfassungsschutzgesetzes (§ 174 Abs. 5 Nr. 5 Buchst. a TKG) oder zur politischen Unterrichtung der Bundesregierung zu, wenn im Einzelfall tatsächliche Anhaltspunkte dafür vorliegen, dass durch die Auskunft Informationen über das Ausland gewonnen werden können, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind und zu deren Aufklärung das Bundeskanzleramt den Bundesnachrichtendienst beauftragt hat (§ 174 Abs. 5 Nr. 7 Buchst. a TKG). Diese Regelungen können nicht ohne Weiteres auf den unionsrechtlich zulässigen Zweck der Verhütung schwerer Bedrohungen der öffentlichen Sicherheit gestützt werden und gehen insbesondere auch über den Zweck des Schutzes der nationalen Sicherheit hinaus, den der EuGH – wie erwähnt – nur dann für einschlägig hält, wenn tragende Strukturen eines Landes im Bereich der Verfassung, Politik oder Wirtschaft oder im sozialen Bereich in schwerwiegender

Weise destabilisiert zu werden drohen (EuGH, Urteil vom 20. September 2022 - C-793/19 und C-794/19 - Rn. 92).

45 dd) Eine unionsrechtskonforme Auslegung kommt wegen des vom EuGH hervorgehobenen Grundsatzes der Bestimmtheit und Normenklarheit weder hinsichtlich der Regelungen in § 175 Abs. 1 Satz 1 i. V. m. § 176 TKG noch derjenigen in § 177 Abs. 1 Nr. 3 i. V. m. § 174 Abs. 1 Satz 3 TKG in Betracht. Wie bereits erwähnt, müssen nationale Rechtsvorschriften, um dem unionsrechtlichen Erfordernis der Verhältnismäßigkeit zu genügen, klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindesterfordernisse aufstellen, sodass die Personen, deren personenbezogene Daten betroffen sind, über ausreichende Garantien verfügen, die einen wirksamen Schutz dieser Daten vor Missbrauchsrisiken ermöglichen. Diese Rechtsvorschriften müssen nach nationalem Recht bindend sein und insbesondere Angaben dazu enthalten, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme, die die Verarbeitung solcher Daten vorsieht, getroffen werden darf, damit gewährleistet ist, dass sich der Eingriff auf das absolut Notwendige beschränkt (EuGH, Urteil vom 20. September 2022 - C-793/19 und C-794/19 - Rn. 69). Die Bestimmung präziser Eingriffsvoraussetzungen für die Vorratsdatenspeicherung im Rahmen des unionsrechtlich Zulässigen ist daher nicht Sache der Gerichte, sondern des Gesetzgebers.

46 ee) Ist § 175 Abs. 1 Satz 1 i. V. m. § 176 TKG (§ 113a Abs. 1 Satz 1 i. V. m. § 113b TKG a. F.) nach alledem mit dem Unionsrecht nicht vereinbar und kommt eine unionsrechtskonforme Auslegung nicht in Betracht, darf die Regelung wegen des Grundsatzes des Vorrangs des Unionsrechts nicht angewendet werden (stRspr, vgl. EuGH, Urteile vom 9. März 1978 - Rs. 106/77 [ECLI:EU:C:1978:49], Simmenthal - Rn. 24, vom 3. Mai 2005 - C-387/02, C-391/02 und C-403/02 [ECLI:EU:C:2005:270], Berlusconi u. a. - Rn. 72, vom 22. Juni 2010 - C-188/10 und C-189/10 [ECLI:EU:C:2010:363], Melki und Abdeli - Rn. 43 sowie vom 18. September 2014 - C-487/12 [ECLI:EU:C:2014:2232], Vueling Airlines - Rn. 48).

47 3. Die Kostenentscheidung folgt aus § 154 Abs. 2 VwGO.

Prof. Dr. Kraft Dr. Möller Hahn

Dr. Tegethoff Dr. Gamp

B e s c h l u s s

Der Wert des Streitgegenstandes wird für das Revisionsverfahren auf 500 000 € festgesetzt (§ 47 Abs. 1 Satz 1, § 52 Abs. 1 GKG).

Prof. Dr. Kraft Dr. Möller Hahn