SCHLUSSANTRÄGE DES GENERALANWALTS

MANUEL CAMPOS SÁNCHEZ-BORDONA

vom 18. November 2021(1)

Verbundene Rechtssachen C-793/19 und C-794/19

Bundesrepublik Deutschland

gegen

SpaceNet AG (C-793/19)

Telekom Deutschland GmbH (C-794/19)

(Vorabentscheidungsersuchen des Bundesverwaltungsgerichts [Deutschland])

„Vorlage zur Vorabentscheidung – Telekommunikation – Verarbeitung personenbezogener Daten und Schutz des Privatlebens im Bereich der elektronischen Kommunikation – Richtlinie 2002/58/EG – Art. 15 Abs. 1 – Art. 4 Abs. 2 EUV – Charta der Grundrechte der Europäischen Union – Art. 6, 7, 8, 11 und 52 Abs. 1 – Allgemeine und unterschiedslose Vorratsspeicherung von Verbindungsdaten zum Zweck der Verfolgung schwerer Straftaten oder der Abwehr einer konkreten Gefahr für die nationale Sicherheit“

1. Die vorliegenden Vorabentscheidungsersuchen – zu denen das Vorabentscheidungsersuchen in der Rechtssache C-140/20(2) hinzukommt – zeigen erneut die Besorgnis, die die Rechtsprechung des Gerichtshofs zur Vorratsspeicherung und zum Zugang zu personenbezogenen Daten im Bereich der elektronischen Kommunikation bei einigen Mitgliedstaaten hervorgerufen hat.

2. In meinen Schlussanträgen in den Rechtssachen C-511/18 und C-512/18, La Quadrature du Net u. a.(3), und C-520/18, Ordre des barreaux francophones et germanophone u. a.(4), habe ich die folgenden Urteile als die wichtigsten bisherigen Beispiele dieser Rechtsprechung angeführt:

– das Urteil vom 8. April 2014, Digital Rights Ireland u. a.(5), in dem der Gerichtshof die Richtlinie 2006/24/EG(6) für ungültig erklärt hat, weil sie einen unverhältnismäßigen Eingriff in die in den Art. 7 und 8 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta) verankerten Rechte zuließ;

– das Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u. a.(7), in dem der Gerichtshof festgestellt hat, dass Art. 15 Abs. 1 der Richtlinie 2002/58/EG(8) einer nationalen Regelung entgegensteht, die die allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten zum Zweck der Bekämpfung schwerer Kriminalität vorsieht;

– das Urteil vom 2. Oktober 2018, Ministerio Fiscal(9), in dem der Gerichtshof die Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58 bestätigt und die insoweit zu beachtende Bedeutung des Grundsatzes der Verhältnismäßigkeit hervorgehoben hat.

3. Im Jahr 2018 äußerten einige Gerichte bestimmter Mitgliedstaaten in Vorabentscheidungsersuchen an den Gerichtshof ihre Besorgnis, dass den staatlichen Stellen infolge dieser Urteile (aus den Jahren 2014, 2016 und 2018) ein für den Schutz der nationalen Sicherheit und für die Bekämpfung von Kriminalität und Terrorismus notwendiges Instrument vorenthalten werde.

4. Vier dieser Vorabentscheidungsersuchen führten zu den Urteilen Privacy International(10) und La Quadrature du Net u. a.(11), beide vom 6. Oktober 2020, die im Wesentlichen die Erkenntnisse des Urteils Tele2 Sverige bestätigten, jedoch auch Ergänzungen einführten.

5. Aufgrund des Spruchkörpers (Große Kammer des Gerichtshofs) und des Inhalts der Urteile sowie aufgrund des Bestrebens des Gerichtshofs, im Dialog mit den vorlegenden Gerichten ausführlich die Gründe zu erläutern, die die in ihnen enthaltenen Thesen trotz allem rechtfertigen, wäre zu erwarten gewesen, dass diese beiden „zusammenfassenden" Urteile vom 6. Oktober 2020 der Debatte ein Ende gesetzt haben. Bei jedem weiteren Vorabentscheidungsersuchen zu dem gleichen Gegenstand müsste daher ein mit Gründen versehener Beschluss gemäß Art. 99 der Verfahrensordnung des Gerichtshofs ergehen.

6. Bis zum 6. Oktober 2020 gingen jedoch drei weitere Vorabentscheidungsersuchen (die zwei im vorliegenden Verfahren verbundenen Vorabentscheidungsersuchen und das Vorabentscheidungsersuchen in der Rechtssache C-140/20) beim Gerichtshof ein, mit denen die ständige Rechtsprechung zu Art. 15 Abs. 1 der Richtlinie 2002/58 erneut in Frage gestellt wird.

7. Der Gerichtshof hat die vorlegenden Gerichte über die Urteile vom 6. Oktober 2020 informiert für den Fall, dass sie ihre jeweiligen Vorabentscheidungsersuchen zurückziehen wollten. Da sie, wie ich nachstehend ausführen werde(12), darauf bestehen, sie aufrechtzuerhalten, ist beschlossen worden, dass Art. 99 der Verfahrensordnung nicht zur Anwendung kommt und die Große Kammer des Gerichtshofs die Vorabentscheidungsersuchen beantwortet.

I. Rechtlicher Rahmen

A. Unionsrecht. Richtlinie 2002/58

8. Art. 5 („Vertraulichkeit der Kommunikation") Abs. 1 bestimmt:

> „Die Mitgliedstaaten stellen die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten durch innerstaatliche Vorschriften sicher. Insbesondere untersagen sie 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, wenn keine Einwilligung der betroffenen Nutzer vorliegt, es sei denn, dass diese Personen gemäß Artikel 15 Absatz 1 gesetzlich dazu ermächtigt sind. Diese Bestimmung steht – unbeschadet des Grundsatzes der Vertraulichkeit – der für die Weiterleitung einer Nachricht erforderlichen technischen Speicherung nicht entgegen."

9. Art. 6 („Verkehrsdaten") sieht vor:

> „(1) Verkehrsdaten, die sich auf Teilnehmer und Nutzer beziehen und vom Betreiber eines öffentlichen Kommunikationsnetzes oder eines öffentlich zugänglichen Kommunikationsdienstes verarbeitet und gespeichert werden, sind unbeschadet der Absätze 2, 3 und 5 des vorliegenden Artikels und des Artikels 15 Absatz 1 zu löschen oder zu anonymisieren, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden.
>
> (2) Verkehrsdaten, die zum Zwecke der Gebührenabrechnung und der Bezahlung von Zusammenschaltungen erforderlich sind, dürfen verarbeitet werden. Diese Verarbeitung ist nur bis zum Ablauf der Frist zulässig, innerhalb deren die Rechnung rechtlich angefochten oder der

Anspruch auf Zahlung geltend gemacht werden kann.

…“

10. In Art. 15 („Anwendung einzelner Bestimmungen der Richtlinie 95/46/EG“)(13) Abs. 1 heißt es:

„Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 dieser Richtlinie beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 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. Alle in diesem Absatz genannten Maßnahmen müssen den allgemeinen Grundsätzen des Gemeinschaftsrechts einschließlich den in Artikel 6 Absätze 1 und 2 des Vertrags über die Europäische Union niedergelegten Grundsätzen entsprechen.“

B. Nationales Recht

1. Telekommunikationsgesetz (im Folgenden: TKG)

11. § 113a Abs. 1 sieht vor:

„Die Verpflichtungen zur Speicherung von Verkehrsdaten, zur Verwendung der Daten und zur Datensicherheit nach den §§ 113b bis 113g beziehen sich auf Erbringer öffentlich zugänglicher Telekommunikationsdienste für Endnutzer.“

12. § 113b bestimmt:

„(1) Die in § 113a Absatz 1 Genannten sind verpflichtet, Daten wie folgt im Inland zu speichern:

1. Daten nach den Absätzen 2 und 3 für zehn Wochen,

2. Standortdaten nach Absatz 4 für vier Wochen.

(2) Die Erbringer öffentlich zugänglicher Telefondienste speichern

1. die Rufnummer oder eine andere Kennung des anrufenden und des angerufenen Anschlusses sowie bei Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses,

2. Datum und Uhrzeit von Beginn und Ende der Verbindung unter Angabe der zugrunde liegenden Zeitzone,

3. Angaben zu dem genutzten Dienst, wenn im Rahmen des Telefondienstes unterschiedliche Dienste genutzt werden können,

4. im Fall mobiler Telefondienste ferner

   a) die internationale Kennung mobiler Teilnehmer für den anrufenden und den angerufenen Anschluss,

   b) die internationale Kennung des anrufenden und des angerufenen Endgerätes,

   c) Datum und Uhrzeit der ersten Aktivierung des Dienstes unter Angabe der zugrunde liegenden Zeitzone, wenn Dienste im Voraus bezahlt wurden,

5. im Fall von Internet-Telefondiensten auch die Internetprotokoll-Adressen des anrufenden und des angerufenen Anschlusses und zugewiesene Benutzerkennungen.

Satz 1 gilt entsprechend

1. bei der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht; hierbei treten an die Stelle der Angaben nach Satz 1 Nummer 2 die Zeitpunkte der Versendung und des Empfangs der Nachricht;

2. für unbeantwortete oder wegen eines Eingriffs des Netzwerkmanagements erfolglose Anrufe …

(3) Die Erbringer öffentlich zugänglicher Internetzugangsdienste speichern

1. die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse,

2. eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt, sowie eine zugewiesene Benutzerkennung,

3. Datum und Uhrzeit von Beginn und Ende der Internetnutzung unter der zugewiesenen Internetprotokoll-Adresse unter Angabe der zugrunde liegenden Zeitzone.

(4) Im Fall der Nutzung mobiler Telefondienste sind die Bezeichnungen der Funkzellen zu speichern, die durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzt wurden. Bei öffentlich zugänglichen Internetzugangsdiensten ist im Fall der mobilen Nutzung die Bezeichnung der bei Beginn der Internetverbindung genutzten Funkzelle zu speichern. Zusätzlich sind die Daten vorzuhalten, aus denen sich die geografische Lage und die Hauptstrahlrichtungen der die jeweilige Funkzelle versorgenden Funkantennen ergeben.

(5) Der Inhalt der Kommunikation, Daten über aufgerufene Internetseiten und Daten von Diensten der elektronischen Post dürfen auf Grund dieser Vorschrift nicht gespeichert werden.

(6) Daten, die den in § 99 Absatz 2 genannten Verbindungen zugrunde liegen, dürfen auf Grund dieser Vorschrift nicht gespeichert werden. Dies gilt entsprechend für Telefonverbindungen, die von den in § 99 Absatz 2 genannten Stellen ausgehen. § 99 Absatz 2 Satz 2 bis 7 gilt entsprechend[(14)].

…“

13. In § 113c heißt es:

„(1) Die auf Grund des § 113b gespeicherten Daten dürfen

1. an eine Strafverfolgungsbehörde übermittelt werden, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung, die ihr eine Erhebung der in § 113b genannten Daten zur Verfolgung besonders schwerer Straftaten erlaubt, verlangt;

2. an eine Gefahrenabwehrbehörde der Länder übermittelt werden, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung, die ihr eine Erhebung der in § 113b genannten Daten zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes erlaubt, verlangt;

3. durch den Erbringer öffentlich zugänglicher Telekommunikationsdienste für eine Auskunft nach § 113 Absatz 1 Satz 3 verwendet werden.

(2) Für andere Zwecke als die in Absatz 1 genannten dürfen die auf Grund des § 113b gespeicherten Daten von den nach § 113a Absatz 1 Verpflichteten nicht verwendet werden.

…“

14. § 113d lautet:

„Der nach § 113a Absatz 1 Verpflichtete hat sicherzustellen, dass die auf Grund der Speicherpflicht nach § 113b Absatz 1 gespeicherten Daten durch technische und organisatorische Maßnahmen nach dem Stand der Technik gegen unbefugte Kenntnisnahme und Verwendung geschützt werden. Die Maßnahmen umfassen insbesondere

1. den Einsatz eines besonders sicheren Verschlüsselungsverfahrens,

2. die Speicherung in gesonderten, von den für die üblichen betrieblichen Aufgaben getrennten Speichereinrichtungen,

3. die Speicherung mit einem hohen Schutz vor dem Zugriff aus dem Internet auf vom Internet entkoppelten Datenverarbeitungssystemen,

4. die Beschränkung des Zutritts zu den Datenverarbeitungsanlagen auf Personen, die durch den Verpflichteten besonders ermächtigt sind, und

5. die notwendige Mitwirkung von mindestens zwei Personen beim Zugriff auf die Daten, die dazu durch den Verpflichteten besonders ermächtigt worden sind.“

15. § 113e bestimmt:

„(1) Der nach § 113a Absatz 1 Verpflichtete hat sicherzustellen, dass für Zwecke der Datenschutzkontrolle jeder Zugriff, insbesondere das Lesen, Kopieren, Ändern, Löschen und Sperren der auf Grund der Speicherpflicht nach § 113b Absatz 1 gespeicherten Daten protokolliert wird. Zu protokollieren sind

1. der Zeitpunkt des Zugriffs,

2. die auf die Daten zugreifenden Personen,

3. Zweck und Art des Zugriffs.

(2) Für andere Zwecke als die der Datenschutzkontrolle dürfen die Protokolldaten nicht verwendet werden.

(3) Der nach § 113a Absatz 1 Verpflichtete hat sicherzustellen, dass die Protokolldaten nach einem Jahr gelöscht werden.“

2. Strafprozessordnung (im Folgenden: StPO)

16. § 100g bestimmt:

„…

(2) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer eine der in Satz 2 bezeichneten besonders schweren Straftaten begangen hat oder in Fällen, in denen der Versuch strafbar ist, eine solche Straftat zu begehen versucht hat, und wiegt die Tat auch im Einzelfall besonders schwer, dürfen die nach § 113b [TKG] gespeicherten Verkehrsdaten erhoben werden, soweit die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht.

…

(4) Die Erhebung von Verkehrsdaten nach Absatz 2, … die voraussichtlich Erkenntnisse erbringen würde, über die [die betreffende Person] das Zeugnis verweigern dürfte, ist unzulässig. …“

17. Nach § 101a Abs. 1 unterliegt die Erhebung von Verkehrsdaten nach § 100g StPO einem Richtervorbehalt. Nach § 101a Abs. 2 StPO sind in dem Beschluss einzelfallbezogen die wesentlichen Erwägungen zur Erforderlichkeit und Angemessenheit der Maßnahme darzulegen, und nach § 101 Abs. 6 StPO sind die an der betroffenen Telekommunikation beteiligten Personen von der Maßnahme zu benachrichtigen.

II. Sachverhalt der Ausgangsverfahren und Vorlagefragen

18. Die SpaceNet AG und die Telekom Deutschland GmbH erbringen in Deutschland öffentlich zugängliche Internetzugangsdienste.

19. Die beiden Gesellschaften haben jeweils vor dem Verwaltungsgericht (Deutschland) gegen die ihnen durch § 113a Abs. 1 in Verbindung mit § 113b TKG auferlegte Pflicht, ab dem 1. Juli 2017 Telekommunikations-Verkehrsdaten ihrer Kunden auf Vorrat zu speichern, Klage erhoben.

20. Nachdem das Verwaltungsgericht den Anträgen stattgegeben hatte, hat die Bundesnetzagentur in beiden Verfahren Revision beim Bundesverwaltungsgericht eingelegt, das beschlossen hat, vor Erlass seines Urteils dem Gerichtshof in beiden Verfahren jeweils die folgende Frage zur Vorabentscheidung vorzulegen:

Ist Art. 15 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta einerseits und des Art. 6 der Charta sowie des Art. 4 EUV andererseits dahin auszulegen, dass er einer nationalen Regelung entgegensteht, welche die Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste verpflichtet, Verkehrs- und Standortdaten der Endnutzer dieser Dienste auf Vorrat zu speichern, wenn diese Verpflichtung

– keinen spezifischen Anlass in örtlicher, zeitlicher oder räumlicher Hinsicht voraussetzt,

– Gegenstand der Pflicht zur Speicherung bei der Erbringung öffentlich zugänglicher Telefondienste – einschließlich der Übermittlung von Kurz-, Multimedia- oder ähnlichen Nachrichten sowie unbeantworteter oder erfolgloser Anrufe – folgende Daten sind:

  – die Rufnummer oder eine andere Kennung des anrufenden und des angerufenen Anschlusses sowie bei Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses,

  – Datum und Uhrzeit von Beginn und Ende der Verbindung bzw. – bei der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht – die Zeitpunkte der Versendung und des Empfangs der Nachricht unter Angabe der zugrunde liegenden Zeitzone,

  – Angaben zu dem genutzten Dienst, wenn im Rahmen des Telefondienstes unterschiedliche Dienste genutzt werden können,

  – im Fall mobiler Telefondienste ferner

    – die internationale Kennung mobiler Teilnehmer für den anrufenden und den angerufenen Anschluss,

    – die internationale Kennung des anrufenden und des angerufenen Endgerätes,

    – Datum und Uhrzeit der ersten Aktivierung des Dienstes unter Angabe der zugrunde liegenden Zeitzone, wenn Dienste im Voraus bezahlt wurden,

– die Bezeichnungen der Funkzellen, die durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzt wurden,

– im Fall von Internet-Telefondiensten auch die Internetprotokoll-Adressen des anrufenden und des angerufenen Anschlusses und zugewiesene Benutzerkennungen,

– Gegenstand der Pflicht zur Speicherung bei der Erbringung öffentlich zugänglicher Internetzugangsdienste folgende Daten sind:

– die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse,

– eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt, sowie eine zugewiesene Benutzerkennung,

– Datum und Uhrzeit von Beginn und Ende der Internetnutzung unter der zugewiesenen Internetprotokoll-Adresse unter Angabe der zugrunde liegenden Zeitzone,

– im Fall der mobilen Nutzung die Bezeichnung der bei Beginn der Internetverbindung genutzten Funkzelle,

– folgende Daten nicht gespeichert werden dürfen:

– der Inhalt der Kommunikation,

– Daten über aufgerufene Internetseiten,

– Daten von Diensten der elektronischen Post,

– Daten, die den Verbindungen zu oder von bestimmten Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen zugrunde liegen,

– die Dauer der Speicherung auf Vorrat für Standortdaten, d. h. die Bezeichnung der genutzten Funkzelle, vier Wochen und für die übrigen Daten zehn Wochen beträgt,

– ein wirksamer Schutz der auf Vorrat gespeicherten Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang gewährleistet ist, und

– die auf Vorrat gespeicherten Daten nur zur Verfolgung besonders schwerer Straftaten und zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes, verwendet werden dürfen, mit Ausnahme der dem Teilnehmer für eine Internetnutzung zugewiesenen Internetprotokoll-Adresse, deren Verwendung im Rahmen einer Bestandsdatenauskunft zur Verfolgung jeglicher Straftaten, zur Abwehr einer Gefahr für die öffentliche Sicherheit und Ordnung sowie zur Erfüllung der Aufgaben der Nachrichtendienste zulässig ist?

21. Wie das vorlegende Gericht ausführt, wurde die streitige Pflicht durch das Gesetz vom 10. Dezember 2015(15) neu geregelt, was notwendig geworden war,

– nachdem ein Urteil des Bundesverfassungsgerichts (Deutschland) vom 2. März 2010(16) die früheren Vorschriften, die die Vorratsdatenspeicherung regelten, für verfassungswidrig erklärt hatte und

– nachdem die Richtlinie 2006/24, zu deren Umsetzung diese früheren Vorschriften erlassen worden waren, für nichtig erklärt worden war.

22. Nach Auffassung des vorlegenden Gerichts beschränkt die streitige Speicherpflicht die Rechte gemäß Art. 5 Abs. 1, Art. 6 Abs. 1 und Art. 9 Abs. 1 der Richtlinie 2002/58. Diese Beschränkung sei nur

dann gerechtfertigt, wenn sie auf Art. 15 Abs. 1 der Richtlinie 2002/58 gestützt werden könne.

23. Ungeachtet der Erkenntnisse im Urteil Tele2 Sverige hält das vorlegende Gericht es nicht für ausgeschlossen, dass die streitige Pflicht auf Art. 15 Abs. 1 der Richtlinie 2002/58 gestützt werden könne, und zwar aus den folgenden Gründen:

– Die anwendbare nationale Regelung verpflichte nicht zur Vorratsspeicherung sämtlicher Telekommunikations-Verkehrsdaten *aller* Teilnehmer und registrierten Nutzer in Bezug auf *alle* elektronischen Kommunikationsmittel.

– Mit der Regelung sei die Speicherungsfrist im Vergleich zu der Frist, die in den im Urteil Tele2 Sverige geprüften Rechtsvorschriften vorgesehen gewesen sei, sowie der in der Richtlinie 2006/24 vorgesehenen Frist deutlich verkürzt worden (auf eine Höchstfrist von zehn Wochen), was die Profilerstellung erschwere.

– Die streitige Regelung unterliege strengen Beschränkungen im Hinblick auf den Schutz und die Nutzung der gespeicherten Daten sowie den Zugang zu diesen Daten.

– Der nationale Gesetzgeber sei den Handlungspflichten nachgekommen, die sich aus dem durch Art. 6 der Charta garantierten Recht auf Sicherheit ergäben(17).

– Für den Fall, dass eine „anlasslose“(18) Vorratsdatenspeicherung generell nicht auf Art. 15 Abs. 1 der Richtlinie 2002/58 gestützt werden könne (d. h., wenn es nicht auf die konkrete Form ankomme, in der die erfassten Kommunikationsmittel, die Kategorien der zu speichernden Daten, die Speicherdauer, die Voraussetzungen für den Zugang zu den gespeicherten Daten und der Schutz vor Missbrauchsrisiken geregelt seien), sei der Handlungsspielraum des nationalen Gesetzgebers in einem Bereich, der wie die Strafverfolgung und die öffentliche Sicherheit nach Art. 4 Abs. 2 Satz 3 EUV jedenfalls grundsätzlich weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten falle, erheblich eingeschränkt.

– Es müsse Kohärenz zwischen den in der Charta verankerten Rechten und den entsprechenden durch die Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten (im Folgenden: EMRK) in der Auslegung durch den Europäischen Gerichtshof für Menschenrechte (im Folgenden: EGMR) garantierten Rechten geschaffen werden, ohne dass dadurch die Eigenständigkeit des Unionsrechts und des Gerichtshofs der Europäischen Union berührt werde.

III. Verfahren vor dem Gerichtshof

24. Die Vorabentscheidungsersuchen sind am 29. Oktober 2019 beim Gerichtshof eingegangen.

25. SpaceNet, Telekom Deutschland, die dänische, die deutsche, die estnische, die finnische, die französische, die irische, die niederländische, die polnische, die schwedische und die spanische Regierung sowie die Kommission haben schriftliche Erklärungen eingereicht.

26. Nachdem das vorlegende Gericht gefragt worden war, ob es nach dem Erlass des Urteils La Quadrature du Net seine Vorabentscheidungsersuchen zurücknehmen wolle, hat es am 13. Januar 2021 erklärt, dass es dies nicht beabsichtige, da die Vorentscheidungsersuchen nicht als durch dieses Urteil erledigt angesehen werden könnten.

27. Die mündliche Verhandlung hat am 13. September 2021 gemeinsam mit der Verhandlung in der zusammenhängenden Rechtssache C-140/20 stattgefunden. Teilgenommen haben die Parteien, die in dem Verfahren schriftliche Erklärungen eingereicht haben, sowie die Bundesnetzagentur und der Europäische Datenschutzbeauftragte.

IV. Würdigung

A. Vorbemerkung

28. Die beiden Vorabentscheidungsersuchen können entweder in der Form gewürdigt werden, in der sie ursprünglich vorgelegt wurden, oder unter Berücksichtigung vorzugsweise der Argumente, die das vorlegende Gericht in seiner Antwort an den Gerichtshof vom 13. Januar 2021 geltend macht, um die Aufrechterhaltung der Vorabentscheidungsersuchen auch nach Erlass des Urteils La Quadrature du Net zu begründen.

29. Ich werde zwar kurz auf die wichtigsten Punkte der ursprünglichen Vorabentscheidungsersuchen eingehen, konzentriere mich jedoch auf die Prüfung der Gründe, aus denen nach Ansicht des vorlegenden Gerichts weiterhin eine Entscheidung des Gerichtshofs erforderlich ist. Alle diese Gründe beruhen im Wesentlichen darauf, dass zwischen den hier zugrunde liegenden Rechtsvorschriften und den im Urteil La Quadrature du Net geprüften Rechtsvorschriften Unterschiede bestünden.

30. In seinem Schreiben vom 13. Januar 2021 hat das vorlegende Gericht folgende Argumente angeführt:

– Zwischen den deutschen Rechtsvorschriften und den französischen bzw. belgischen Rechtsvorschriften, auf die sich das Urteil La Quadrature du Net beziehe, bestünden erhebliche Unterschiede. Die deutschen Rechtsvorschriften sähen vor, dass Daten über aufgerufene Internetseiten, Daten von Diensten der elektronischen Post sowie Daten, die den Verbindungen zu oder von bestimmten Anschlüssen in sozialen oder kirchlichen Bereichen zugrunde lägen, nicht gespeichert werden dürften.

– Einen weiteren, noch gewichtigeren Unterschied gebe es bei der Speicherungsfrist, die nach § 113b Abs. 1 TKG vier oder zehn Wochen betrage und nicht ein Jahr. Dies verringere die Gefahr der Erstellung eines umfassenden Profils der betroffenen Personen.

– Die deutschen Rechtsvorschriften böten einen wirksamen Schutz der gespeicherten Daten vor Missbrauch und unrechtmäßigem Zugang.

– Nach einem aktuellen Urteil des Bundesverfassungsgerichts zu § 113 TKG(19) sei die Gültigkeit dieser Vorschrift von Bedingungen abhängig, deren Vereinbarkeit mit dem Unionsrecht nur schwer festzustellen sei.

– Es sei zweifelhaft, welche Erfordernisse das Unionsrecht für IP-Adressen vorsehe, da aus dem Urteil La Quadrature du Net nicht eindeutig hervorgehe, ob ihre Speicherung generell ausgeschlossen sei, und ein gewisser Gegensatz zwischen den Rn. 168 und 155 des Urteils bestehe.

B. Anwendbarkeit der Richtlinie 2002/58

31. Die Republik Irland sowie die französische, die niederländische, die polnische und die schwedische Regierung machen im Wesentlichen geltend, die Richtlinie 2002/58 sei auf nationale Rechtsvorschriften wie die in den vorliegenden Rechtssachen in Rede stehenden nicht anwendbar. Da diese Vorschriften den Schutz der nationalen Sicherheit sowie die Verhütung und Verfolgung schwerer Straftaten zum Gegenstand hätten, unterlägen sie nach Art. 4 Abs. 2 EUV der ausschließlichen Zuständigkeit der Mitgliedstaaten.

32. Dieser Einwand ist vom Gerichtshof in seinem Urteil La Quadrature du Net eindeutig zurückgewiesen worden, in dem er feststellt, dass „eine nationale Regelung, die wie die in den Ausgangsverfahren in Rede stehenden die Betreiber elektronischer Kommunikationsdienste zum Schutz der nationalen Sicherheit und zur Bekämpfung der Kriminalität zur Vorratsspeicherung von Verkehrs- und Standortdaten verpflichtet, in den Geltungsbereich der Richtlinie 2002/58 fällt“(20).

33. Das vorlegende Gericht bestätigt die Feststellung der Vorinstanz und fügt hinzu, dass insoweit die Anwendbarkeit der Richtlinie 2005/58 durch das Urteil Tele2 Sverige „abschließend geklärt“ sei(21).

34. Auf diesen Punkt, zu dem ich mich seinerzeit im Sinne des Gerichtshofs in meinen Schlussanträgen La Quadrature du Net(22) geäußert habe, werde ich folglich nicht eingehen.

C. Allgemeine und unterschiedslose Vorratsspeicherung versus gezielte Vorratsspeicherung von Verkehrs- und Standortdaten

35. Im Mittelpunkt der Rechtsprechung des Gerichtshofs zur Richtlinie 2002/58 steht der Gedanke, dass Nutzer elektronischer Kommunikationsmittel grundsätzlich erwarten dürfen, dass ihre Nachrichten und die damit verbundenen Daten anonym bleiben und nicht gespeichert werden, es sei denn, sie haben darin eingewilligt(23).

36. Art. 15 Abs. 1 der Richtlinie 2002/58 ermöglicht Ausnahmen von der Verpflichtung zum Schutz der Vertraulichkeit und den entsprechenden Pflichten unter den Bedingungen, die ich nachstehend darstellen werde. Im Urteil La Quadrature du Net geht es um die Frage, wie diese Ausnahmen mit den Grundrechten, deren Ausübung betroffen sein kann, in Einklang zu bringen sind(24).

37. Nach Auffassung des Gerichtshofs kann die allgemeine und unterschiedslose Vorratsspeicherung von Verkehrsdaten nur durch das Ziel des Schutzes der nationalen Sicherheit gerechtfertigt werden, dessen Bedeutung „die der übrigen von Art. 15 Abs. 1 der Richtlinie 2002/58 erfassten Ziele“ übersteigt(25).

38. Für diesen Fall (den Fall der nationalen Sicherheit) stellt der Gerichtshof fest, dass Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta „*einer Rechtsvorschrift, mit der den zuständigen Behörden gestattet wird, den Betreibern elektronischer Kommunikationsdienste aufzugeben,* die Verkehrs- und Standortdaten aller Nutzer elektronischer Kommunikationsmittel *für begrenzte Zeit zu speichern*, grundsätzlich nicht entgegen[steht], sofern hinreichend konkrete Umstände die Annahme zulassen, dass sich der betreffende Mitgliedstaat einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit … gegenübersieht“(26).

39. Sicherlich führen diese Vorgaben zu einer strengeren Regelung als der, die sich aus der Rechtsprechung des EGMR zu Art. 8 EMRK ergibt. Der Umstand, dass die Rechte der Charta, die den durch die EMRK garantierten Rechten entsprechen, die gleiche „Bedeutung und Tragweite“ wie die Rechte aus der Konvention haben, steht nach Art. 52 Abs. 3 a. E. der Charta nicht dem entgegen, dass das Recht der Union einen weiter gehenden Schutz gewährt.

40. Darüber hinaus betrifft die Rechtsprechung des EGMR in seinen Urteilen vom 25. Mai 2021, Big Brother Watch u. a./Vereinigtes Königreich(27) und Centrum för Rättvisa/Schweden(28), sowie in seinem Urteil vom 4. Dezember 2015, Zakharov/Russland(29), Fälle, die, wie die Verfahrensbeteiligten in der mündlichen Verhandlung mehrheitlich vertreten haben, nicht mit den in den vorliegenden Vorabentscheidungsersuchen in Rede stehenden vergleichbar sind. Die Entscheidung über die vorliegenden Fälle muss durch Anwendung nationaler Rechtsvorschriften erfolgen, die mit der *erschöpfenden* Regelung der Richtlinie 2002/58 im Sinne ihrer Auslegung durch den Gerichtshof vereinbar sind.

41. Unabhängig davon, welche Meinung in Bezug auf den Umstand vertreten wird, dass im Urteil La Quadrature du Net die nationale Sicherheit als Grund für eine unter bestimmten Bedingungen mögliche Aufhebung des Verbots der allgemeinen und unterschiedslosen Vorratsspeicherung von Verkehrs- und Standortdaten angeführt wird (meiner Ansicht nach sind die vom Gerichtshof gesetzten Grenzen zu weit gefasst), sind die in den Rn. 137 bis 139 dieses Urteils aufgezählten Voraussetzungen zu erfüllen.

42. Darüber hinaus ist zu prüfen, ob die nationale Rechtsvorschrift auf hinreichend *selektiven* Kriterien beruht, um die Voraussetzungen zu erfüllen, die nach der Rechtsprechung des Gerichtshofs einen besonders schwerwiegenden Eingriff in die betroffenen Grundrechte, wie er bei der Vorratsspeicherung

von Daten vorliegt, zu rechtfertigen vermögen.

43. Eckpfeiler der Rechtsprechung des Gerichtshofs in diesem Bereich ist die *gezielte Vorratsspeicherung* von Verkehrs- und Standortdaten(30). Die Auswahl im Rahmen einer gezielten Vorratsspeicherung kann u. a. auf der Grundlage der betroffenen Personengruppen(31) oder auf der Grundlage geografischer Kriterien(32) erfolgen.

44. Sowohl das vorlegende Gericht als auch die Mehrheit der Parteien, die schriftliche Erklärungen eingereicht haben, verweisen übereinstimmend auf die Schwierigkeiten, die mit den vom Gerichtshof genannten Kriterien einhergehen. Ich selbst habe in meinen Schlussanträgen Ordre des barreaux francophones et germanophone(33)auf einige dieser Schwierigkeiten hingewiesen(34).

45. Es kann jedoch nicht ausgeschlossen werden, dass auf diesen Kriterien basierende Formeln für eine gezielte Vorratsspeicherung gefunden werden können, die für die Erreichung der genannten Ziele geeignet und gleichzeitig nicht diskriminierend sind. Die Festlegung solcher mit dem durch die Charta garantierten Grundrechtsschutz im Einklang stehenden Formeln ist Aufgabe der gesetzgebenden Gewalt der Mitgliedstaaten und nicht des Gerichtshofs(35).

46. Im Übrigen wäre es ein Fehler, anzunehmen, dass persönliche oder geografische Kriterien die einzigen Kriterien sind, die mit Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der durch die Charta garantierten Grundrechte vereinbar sind.

47. Auch wenn die französische Regierung der Auffassung ist, sie hätten sich als unwirksam erwiesen(36), meine ich, dass die Modalitäten, die von den Arbeitsgruppen des Rates(37), die sich mit der Ausarbeitung von mit der Rechtsprechung des Gerichtshofs in Einklang stehenden Vorschriften über Speicherung und Zugang befassen, vorgeschlagen wurden, nicht außer Acht gelassen werden sollten(38).

48. Meiner Überzeugung nach wäre eine vorübergehende Speicherung bestimmter *Kategorien* von Verkehrs- und Standortdaten vorzuziehen, die streng nach den Sicherheitsanforderungen begrenzt sind und in ihrer Gesamtheit kein genaues und detailliertes Abbild vom Leben der betroffenen Personen liefern können. In der Praxis bedeutet dies, dass von den beiden Hauptkategorien (Verkehrs- und Standortdaten) mit Hilfe der entsprechenden Filter nur das Minimum an Daten gespeichert werden darf, das für die wirksame Verhütung und Kontrolle der Kriminalität sowie für die nationale Sicherheit als absolut unerlässlich erachtet wird(39).

49. Auf jeden Fall ist es Aufgabe der Mitgliedstaaten bzw. der Unionsorgane, diese Auswahl auf gesetzgeberischem Wege (mit Hilfe ihrer jeweiligen Sachverständigen) vorzunehmen und dabei jeden Versuch der Einführung einer allgemeinen und unterschiedslosen Speicherung aller Verkehrs- und Standortdaten zu unterlassen(40).

50. Daher habe ich in meinen Schlussanträgen Ordre des barreaux francophones et germanophone klargestellt, „dass [i]ch [zugebe], dass es für den Gesetzgeber schwierig ist, die Fälle und Bedingungen, unter denen eine gezielte Vorratsspeicherung durchgeführt werden kann, genau zu bestimmen, doch rechtfertigt dies meines Erachtens nicht, dass die Mitgliedstaaten die Ausnahme zur Regel und die allgemeine Speicherung personenbezogener Daten zum Kernprinzip ihrer Rechtsvorschriften machen. Ansonsten käme es zu einer unbefristeten schwerwiegenden Verletzung des Rechts auf Schutz der personenbezogenen Daten“(41).

D. Urteil La Quadrature du Net, Rn. 168

51. Meiner Ansicht nach ergeben sich die erforderlichen Elemente für eine Antwort an das vorlegende Gericht unmittelbar aus der Rechtsprechung des Gerichtshofs zu Art. 15 Abs. 1 der Richtlinie 2002/58, wie sie im Urteil La Quadrature du Net zusammengefasst wird.

52. Ich möchte daher zunächst an die Rechtsprechung des Gerichtshofs erinnern, die in Rn. 168 dieses Urteils wie folgt wiedergegeben wird:

„… Art. 15 Abs. 1 der Richtlinie 2002/58 [ist] im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta dahin auszulegen …, dass er Rechtsvorschriften entgegensteht, die zu den in Art. 15 Abs. 1 genannten Zwecken präventiv eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen. Dagegen steht Art. 15 Abs. 1 der Richtlinie im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta Rechtsvorschriften nicht entgegen, 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 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;

– 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 schwerer 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.“

E. Beurteilung der in den vorliegenden Vorabentscheidungsersuchen streitigen Rechtsvorschriften im Licht des Urteils La Quadrature du Net

53. Das vorlegende Gericht, das allein für die Auslegung der nationalen Rechtsvorschriften zuständig ist, führt aus, dass es sich bei den deutschen Rechtsvorschriften um eine Regelung handle, die „eine anlasslose, flächendeckende und personell, zeitlich und geografisch undifferenzierte Speicherung eines Großteils aller relevanten Telekommunikations-Verkehrsdaten“ vorschreibe(42).

54. Die streitige nationale Regelung beschränkt sich nicht darauf, die zuständigen Behörden zu ermächtigen, die Speicherung von Verkehrs- und Standortdaten für einen begrenzten Zeitraum zu verlangen: Es ist vielmehr der Gesetzgeber selbst, der unmittelbar und unbestimmt die Pflicht zur

Datenspeicherung auferlegt.

55. Das vorlegende Gericht hat in seinem Schreiben vom 13. Januar 2021 die Unterschiede zwischen der nationalen Regelung und den im Urteil La Quadrature du Net in Rede stehenden Vorschriften aufgezählt, die dazu führen könnten, dass hier eine andere Entscheidung als in jener Rechtssache ergehen könnte.

56. Ich werde diese Unterschiede in der gleichen Reihenfolge prüfen, in der das vorlegende Gericht diese aufführt, zuvor jedoch möchte ich anerkennen, dass sich der deutsche Gesetzgeber ernsthaft bemüht hat, die nationale Regelung an die Erfordernisse anzupassen, die sich insoweit aus der vom Gerichtshof entwickelten Rechtsprechung ergeben.

57. Wie das vorlegende Gericht hervorhebt, ist die streitige Rechtsvorschrift das Ergebnis einer Gesetzesänderung, die infolge der Rechtsprechung des Bundesverfassungsgerichts und der im Urteil Digital Rights entwickelten Rechtsprechung erforderlich wurde.

58. Die Änderungen, die dank des entschiedenen Willens zur Anpassung an die Rechtsprechung des Gerichtshofs in der streitigen nationalen Regelung vorgenommen wurden, stellen folglich einen lobenswerten Fortschritt dar.

59. Allerdings hat sich der Gesetzgeber stärker auf den Schutz und den Zugang zu den gespeicherten Daten konzentriert, und weniger auf die selektive Auswahl der Daten, zu deren Speicherung er verpflichtet wird.

1. Art der gespeicherten Daten

60. Die Art der gespeicherten Daten (nicht gespeichert werden Daten über aufgerufene Internetseiten, Daten von Diensten der elektronischen Post oder Daten, die den Verbindungen zu oder von bestimmten Anschlüssen von telefonischen Beratungsdiensten in sozialen oder kirchlichen Bereichen zugrunde liegen) darf nach meiner Meinung nicht davon ablenken, dass sich die Pflicht zur allgemeinen und unterschiedslosen Vorratsspeicherung auf eine große Anzahl sonstiger Verkehrs- und Standortdaten erstreckt, die insgesamt mit denen, die im Urteil La Quadrature du Net in Rede standen, vergleichbar sind.

61. Die Tatsache, dass Daten, die Verbindungen zu oder von bestimmten Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen zugrunde liegen, ausgeschlossen werden, ist insoweit aufgrund ihrer besonderen Merkmale und ihres sehr geringen Anteils an der Gesamtanzahl(43) nahezu unerheblich.

62. Ebenso wenig ist maßgeblich, dass die Speicherpflicht nicht die Inhalte (der aufgerufenen Internetseiten oder der elektronischen Post) umfasst, da sich das Urteil La Quadrature du Net nicht auf diese bezog, sondern auf die Verkehrs- und Standortdaten der elektronischen Kommunikation.

2. Dauer der Pflicht zur Vorratsspeicherung von Daten

63. Der größte Unterschied zu den nationalen Rechtsvorschriften, die im Urteil La Quadrature du Net in Rede standen, betrifft die Speicherdauer, die nach § 113b Abs. 1 TKG vier oder zehn Wochen (vier Wochen bei Standortdaten und zehn Wochen bei sonstigen Daten) und nicht ein Jahr beträgt.

64. Sowohl das vorlegende Gericht als auch einige beteiligte Regierungen betonen diesen Umstand sowie die Tatsache, dass dies eine deutliche Verkürzung der Dauer der Datenspeicherung darstelle. Nach Ansicht des vorlegenden Gerichts verringert die kürzere Speicherdauer die Gefahr der Erstellung eines umfassenden Profils der betroffenen Personen.

65. Wie ich in meinen Schlussanträgen Ordre des barreaux francophones et germanophone ausgeführt habe, in denen ich die im vorliegenden Verfahren in Rede stehende nationale Regelung als Beispiel nenne, dürfen die Daten nur für einen begrenzten Zeitraum gespeichert werden(44), der davon abhängt, welcher

Datenkategorie sie angehören(45).

66. Selbst wenn die zeitliche Begrenzung der Speicherungsfrist ein wesentliches Element für die Beurteilung der streitigen Regelung darstellt, so ändert dies jedoch nichts daran, dass diese Regelung eine Pflicht zur allgemeinen und unterschiedslosen Vorratsspeicherung von Verkehrs- und Standortdaten auferlegt.

67. Ich habe bereits dargelegt, dass nach der Rechtsprechung des Gerichtshofs – abgesehen von dem durch die Verteidigung der nationalen Sicherheit gerechtfertigten Fall – aufgrund der schwerwiegenden Gefahr, die mit einer allgemeinen Vorratsspeicherung verbunden ist, nur eine gezielte bzw. selektive Vorratsspeicherung von Daten elektronischer Kommunikationsvorgänge in Frage kommt.

68. Es ist letztendlich diese Gefahr, die in der einschlägigen Rechtsprechung des Gerichtshofs Berücksichtigung findet: „[D]ie Verkehrs- und Standortdaten [können] Informationen über eine Vielzahl von Aspekten des Privatlebens der Betroffenen enthalten …, einschließlich sensibler Informationen wie sexuelle Orientierung, politische Meinungen, religiöse, philosophische, gesellschaftliche oder andere Überzeugungen sowie den Gesundheitszustand, wobei solche Daten im Übrigen im Unionsrecht besonderen Schutz genießen. Aus der Gesamtheit dieser Daten können sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten gespeichert wurden, gezogen werden, etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen dieser Personen und das soziale Umfeld, in dem sie verkehren. Diese Daten ermöglichen insbesondere die Erstellung eines Profils der Betroffenen, das im Hinblick auf das Recht auf Achtung des Privatlebens eine ebenso sensible Information darstellt wie der Inhalt der Kommunikationen selbst.“(46)

69. Zwar kann, wie das vorlegende Gericht zutreffend feststellt, eine strenge Begrenzung der Speicherdauer die Profilerstellung erschweren.

70. Ob die Profilerstellung erschwert wird oder nicht, hängt jedoch nicht nur von der Speicherdauer ab, sondern auch von der Menge und der Qualität der gespeicherten Daten: Je mehr Daten vorliegen, desto größer ist auch die Möglichkeit, daraus sensible Informationen abzuleiten, wobei die hierfür erforderlichen Zeiträume wiederum von der Entwicklung der Technik für Überwachung, Abgleich und Auswertung aller Daten elektronischer Kommunikationsvorgänge abhängig sind. Ein Zeitraum, der heutzutage nicht für die Sammlung von Informationen, mit denen eine Profilerstellung möglich ist, ausreicht, wird in mehr oder weniger naher Zukunft eventuell mehr als ausreichend sein(47).

71. Auf jeden Fall ist nach Überzeugung des Gerichtshofs „[d]er mit dem Zugang einer Behörde zu einem Satz 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, verbundene Eingriff in die Grundrechte, die in den Art. 7 und 8 der Charta verankert sind, … in jedem Fall schwerwiegend, *unabhängig von der Länge des Zeitraums, für den der Zugang zu den genannten Daten begehrt wird*, und von der Menge oder Art der für einen solchen Zeitraum verfügbaren Daten, sofern der Datensatz … geeignet ist, genaue Schlüsse auf das Privatleben des oder der Betroffenen zuzulassen“(48).

72. Letztlich führen meiner Auffassung nach trotz der vom vorlegenden Gericht dargestellten Unterschiede die maßgeblichen Ähnlichkeiten zwischen den im Ausgangsverfahren streitigen Rechtsvorschriften und den Rechtsvorschriften, die Gegenstand des dem Urteil La Quadrature du Net zugrunde liegenden Verfahrens waren, dazu, dass von der Rechtsprechung aus diesem Urteil nicht abgewichen werden darf.

3. Schutz der Daten vor unrechtmäßigem Zugang

73. Nach Meinung des vorlegenden Gerichts bieten die deutschen Rechtsvorschriften einen wirksamen Schutz der gespeicherten Daten vor Missbrauch und unrechtmäßigem Zugang.

74. Ohne den Gesetzgebungsbemühungen im Bereich des Datenschutzes und des Zugangs zu den Daten Wert absprechen zu wollen, darf nicht vergessen werden, dass nach Überzeugung des Gerichtshofs „die Speicherung der Verkehrs- und Standortdaten *als solche* … einen Eingriff in die Grundrechte auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten“(49) darstellt. Insoweit ist „der Zugriff auf solche Daten, unabhängig von ihrer späteren Verwendung, [als ein] *gesonderte[r] Eingriff*“ in die genannten Grundrechte anzusehen(50).

75. Für den vorliegenden Fall ist es somit unerheblich, ob nach der vom deutschen Gesetzgeber vorgesehenen Regelung zum Schutz der gespeicherten Daten: a) ein wirksamer Schutz der Daten gewährleistet ist, b) strenge und effiziente Zugangsbedingungen festgelegt werden, mit denen der Personenkreis, der Zugriff auf die Daten hat, eingeschränkt wird, und c) die auf Vorrat gespeicherten Daten nur zur Verfolgung besonders schwerer Straftaten und zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person oder für die nationale Sicherheit verwendet werden dürfen.

76. Tatsächlich entscheidend ist vielmehr, wie auch das vorlegende Gericht hervorhebt, dass die streitige Pflicht zur Vorratsdatenspeicherung als solche keiner besonderen Voraussetzung unterliegt.

4. Auswirkungen des Urteils des Bundesverfassungsgerichts vom 27. Mai 2020

77. Das vorlegende Gericht verweist auf ein Urteil des Bundesverfassungsgerichts zu § 113 TKG(51), in dem die Vorschrift für verfassungswidrig erklärt und die Gültigkeit dieser Vorschrift von Bedingungen abhängig gemacht wird, deren Vereinbarkeit mit dem Unionsrecht nur schwer festzustellen sei.

78. Es ist zum gegenwärtigen Zeitpunkt nicht Aufgabe des Gerichtshofs, sich zu den Auswirkungen jenes Urteils oder zu den Grenzen der neuen Vorschriften, die der deutsche Gesetzgeber erlassen wird (oder bereits erlassen hat), zu äußern.

79. Wenn sich das vorlegende Gericht, wie es feststellt, in seinem Revisionsurteil nach den zum Zeitpunkt des Urteils geltenden Rechtsvorschriften zu richten hat, muss es selbst prüfen, ob diese Rechtsvorschriften im Licht der Rechtsprechung des Gerichtshofs zum Schutz von Daten über die elektronische Kommunikation mit dem Unionsrecht vereinbar sind.

5. IP-Adressen

80. Nach Ansicht des vorlegenden Gerichts geht aus Rn. 168 des Urteils La Quadrature du Net hervor, dass der Gerichtshof für IP-Adressen einen Speicherungsgrund fordere, der mit dem Schutz der nationalen Sicherheit, der Bekämpfung schwerer Kriminalität und der Verhütung schwerer Bedrohungen der öffentlichen Sicherheit in Verbindung stehe. Aus Rn. 155 hingegen gehe hervor, dass IP-Adressen ohne besonderen Grund gespeichert werden dürften und nur für die Verwendung der gespeicherten Daten ein mit diesem Zweck verbundener Grund erforderlich sei.

81. Ich kann hier jedoch kein Spannungsverhältnis (geschweige denn einen Widerspruch) erkennen. Während in Rn. 155 festgestellt wird, dass eine allgemeine und unterschiedslose Vorratsspeicherung allein der IP-Adressen der Quelle einer Verbindung „grundsätzlich nicht gegen Art. 15 Abs. 1 der Richtlinie 2002/58“ verstößt, wird in Rn. 156 weiter ausgeführt, dass „[a]ngesichts der Schwere des mit dieser Vorratsdatenspeicherung verbundenen Eingriffs in die Grundrechte … neben dem Schutz der nationalen Sicherheit nur die Bekämpfung schwerer Kriminalität und die Verhütung schwerer Bedrohungen der öffentlichen Sicherheit geeignet [sind], diesen Eingriff zu rechtfertigen …“.

82. Aus dem Zusammenspiel der Rn. 155 und 156 des Urteils La Quadrature du Net ergibt sich die Antwort, die der Gerichtshof auf die Vorlagefragen zur Speicherung von IP-Adressen in Rn. 168 folgerichtig gegeben hat.

83. In der mündlichen Verhandlung wurden bestimmte Fragen im Zusammenhang mit der Speicherung der IP-Adressen hervorgehoben, die nach Ansicht einiger Beteiligter einer Klärung durch den Gerichtshof bedürfen. Die Entscheidung über diese Fragen (u. a. das Problem der Unterschiede zwischen dynamischen

und statischen IP-Adressen und die Auswirkungen des IPv6-Protokolls) geht nach meiner Auffassung über das hinaus, was das vorlegende Gericht wissen möchte; dieses geht auf diesen Punkt in seinen ursprünglichen Vorabentscheidungsersuchen(52) und in seinem Schreiben vom 13. Januar 2021 in wesentlich begrenzterem Umfang ein.

V. Ergebnis

84. Nach alledem schlage ich dem Gerichtshof vor, dem Bundesverwaltungsgericht (Deutschland) wie folgt zu antworten:

> 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 in Verbindung mit den Art. 7, 8, 11 und 52 Abs. 1 der Charta der Grundrechte der Europäischen Union und Art. 4 Abs. 2 EUV ist dahin auszulegen, dass er einer nationalen Regelung entgegensteht, die den Betreibern öffentlich zugänglicher elektronischer Kommunikationsdienste eine Pflicht zur präventiven, allgemeinen und unterschiedslosen Speicherung von Verkehrs- und Standortdaten der Endnutzer dieser Dienste für andere Zwecke als den Schutz der nationalen Sicherheit bei Vorliegen einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung auferlegt.

---

1 Originalsprache: Spanisch.

---

2 Rechtssache C-140/20, Commissioner of the Garda Síochána u. a., zu der ich am heutigen Tag ebenfalls meine Schlussanträge vortrage.

---

3 Im Folgenden: Schlussanträge La Quadrature du Net (EU:C:2020:6).

---

4 Im Folgenden: Schlussanträge Ordre des barreaux francophones et germanophone (EU:C:2020:7).

---

5 Rechtssachen C-293/12 und C-594/12 (EU:C:2014:238, im Folgenden: Urteil Digital Rights).

---

6 Richtlinie des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (ABl. 2006, L 105, S. 54).

---

7 Rechtssachen C-203/15 und C-698/15 (EU:C:2016:970, im Folgenden: Urteil Tele2 Sverige).

---

8 Richtlinie des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. 2002, L 201, S. 37) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 (ABl. 2009, L 337, S. 11) geänderten Fassung.

---

9 Rechtssache C-207/16 (EU:C:2018:788).

10 Rechtssache C-623/17 (EU:C:2020:790).

11 Rechtssachen C-511/18, C-512/18 und C-520/18 (EU:C:2020:791, im Folgenden: Urteil La Quadrature du Net).

12 Nr. 30 der vorliegenden Schlussanträge.

13 Richtlinie des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. 1995, L 281, S. 31).

14 § 99 Abs. 2 TKG betrifft Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen, die grundsätzlich anonym bleibenden Anrufern telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die insoweit besonderen Verschwiegenheitsverpflichtungen unterliegen. Voraussetzung für die Ausnahme ist nach § 99 Abs. 2 Satz 2 bis 4 TKG ist ihre Aufnahme in eine von der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (im Folgenden: Bundesnetzagentur) geführte Liste, nachdem sie ihre Aufgabenbestimmung durch Bescheinigung einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts nachgewiesen haben.

15 Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten.

16 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 (DE:BVerfG:2010:rs20100302.1bvr025608)

17 Das vorlegende Gericht vertritt den Standpunkt, die Rechtsprechung des Gerichtshofs schließe es nicht völlig aus, dass die nationalen Gesetzgeber aufgrund einer Gesamtabwägung eine – gegebenenfalls durch strenge Zugangsregelungen ergänzte – anlasslose Vorratsdatenspeicherung einführen könnten, um dem spezifischen Gefahrenpotenzial, das sich mit den neuen Telekommunikationsmitteln verbinde, Rechnung zu tragen.

18 Dies ist wörtlich der vom vorlegenden Gericht verwendete Ausdruck.

19 Urteil vom 27. Mai 2020, 1 BvR 1873/13, 1 BvR 2618/13 (DE:BVerfG:2020:rs20200527.1bvr187313). Diesem Urteil zufolge ist § 113 TKG nicht mit Art. 2 Abs. 1 sowie Art. 10 Abs. 1 des Grundgesetzes vereinbar und darf nur bis zum Erlass neuer Vorschriften, höchstens jedoch bis zum 31. Dezember 2021, angewandt werden.

20 Urteil La Quadrature du Net, Rn. 104.

21 Rn. 19 Buchst. a des Vorlagebeschlusses.

22 Schlussanträge La Quadrature du Net, Nrn. 40 bis 90.

23 Urteil La Quadrature du Net, Rn. 109.

24 Ebd., Rn. 111 bis 133.

25 Urteil La Quadrature du Net, Rn. 136.

26 Ebd., Rn. 137 (Hervorhebung nur hier). Der Gerichtshof führt weiter aus: „Auch wenn eine solche Maßnahme unterschiedslos alle Nutzer elektronischer Kommunikationsmittel erfasst, ohne dass *prima facie* ein Zusammenhang … zwischen ihnen und einer Bedrohung der nationalen Sicherheit dieses Mitgliedstaats zu bestehen scheint, ist gleichwohl davon auszugehen, dass das Vorliegen einer derartigen Bedrohung als solches geeignet ist, diesen Zusammenhang herzustellen“ (ebd.).

27 CE:ECHR:2021:0525JUD005817013.

28 CE:ECHR:2021:0525JUD003525208.

29 CE:ECHR:2015:1204JUD004714306.

30 Urteil La Quadrature du Net, Rn. 147: „… Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta [untersagt] es einem Mitgliedstaat … nicht, eine Regelung zu erlassen, die zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit sowie zum Schutz der nationalen Sicherheit präventiv eine *gezielte Vorratsspeicherung* von Verkehrs- und Standortdaten ermöglicht, sofern ihre Speicherung hinsichtlich der Kategorien der zu speichernden Daten, der erfassten Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer der Vorratsspeicherung auf das absolut Notwendige beschränkt ist.“ Hervorhebung nur hier.

31 Urteil La Quadrature du Net, Rn. 148 und 149.

32 Urteil La Quadrature du Net, Rn. 150.

33 Schlussanträge Ordre des barreaux francophones et germanophone, Nrn. 88 und 89.

34 Eine Identifizierung aufgrund solcher Kriterien ist nicht nur unzureichend, sondern kann auch zu einem Generalverdacht gegenüber bestimmten Bevölkerungsgruppen und zur Stigmatisierung bestimmter geografischer Gebiete führen.

35 Ebd., Nr. 90.

36 Rn. 47 ihrer schriftlichen Erklärungen. Eine Auffassung, die auch einige Regierungen in der mündlichen Verhandlung betont haben.

37 Groupe Échange d’informations et protection des données (DAPIX). Den gleichen Standpunkt vertritt die schwedische Regierung in Rn. 21 ihrer schriftlichen Erklärungen.

38 In Nr. 92 der Schlussanträge Ordre des barreaux francophones et germanophone weise ich darauf hin, dass diese Arbeitsgruppen folgende Möglichkeiten in Betracht gezogen haben: die Beschränkung der Kategorien der gespeicherten Daten, die Pseudonymisierung der Daten, die Begrenzung der Aufbewahrungsfristen, den Ausschluss bestimmter Kategorien von Betreibern elektronischer Kommunikationsdienste, die Erneuerung der Genehmigung zur Speicherung, die Verpflichtung zur Aufbewahrung der gespeicherten Daten an einem Ort innerhalb der Union oder die systematische und regelmäßige Kontrolle durch eine unabhängige Verwaltungsbehörde der von den Betreibern elektronischer Kommunikationsdienste gebotenen Garantien gegen den Datenmissbrauch.

39 Schlussanträge Ordre des barreaux francophones et germanophone, Nrn. 93 und 94.

40 Ebd., Nr. 95.

41 Ebd., Nr. 104.

42 Rn. 25 Buchst. bb der deutschen Originalfassung des Vorlagebeschlusses.

43 In der mündlichen Verhandlung hat die deutsche Regierung die Anzahl der Anschlüsse von Personen bzw. Stellen, deren Verbindungen von der Speicherpflicht ausgenommen sind, auf 1 300 beziffert und klargestellt, dass die Ausnahme für die Angehörigen von Berufsgruppen, die dem Berufsgeheimnis unterliegen (z. B. Rechtsanwälte oder Ärzte), aufgrund ihrer großen Anzahl nicht gelten kann.

44 Schlussanträge Ordre des barreaux francophones et germanophone, Nr. 96. So wird sichergestellt, dass „aus ihnen kein detailliertes Abbild vom Leben der betroffenen Personen abgeleitet werden kann. Die Aufbewahrungsfrist ist außerdem an die Art der Daten anzupassen, d. h., die Daten, die genauere Informationen über den Lebensstil und die Gewohnheiten dieser Personen liefern, dürfen nur für einen kürzeren Zeitraum gespeichert werden."

45 Ebd., Nr. 97. „Mit anderen Worten sollte die Möglichkeit einer Differenzierung der Aufbewahrungsfristen der einzelnen Datenkategorien entsprechend ihrer Zweckmäßigkeit für die Erreichung der Sicherheitsziele geprüft werden. Indem die Zeit, in der die jeweiligen Datenkategorien gleichzeitig gespeichert (und somit zur Feststellung von Zusammenhängen, die den Lebensstil der Betroffenen offenbaren, verwendet) werden, begrenzt wird, erweitert sich der Schutz des in Art. 8 der Charta verankerten Rechts."

46 Urteil La Quadrature du Net, Rn. 117.

47 Wie sich in der mündlichen Verhandlung gezeigt hat, kann schon ein Zeitraum von zehn Wochen für die Sammlung von Metadaten (Verkehrs- und Standortdaten) ausreichen, um Verhaltensmuster des Teilnehmers erkennen zu lassen, die durch ihre Wiederholung sensible Eigenschaften seiner Persönlichkeit und seines Lebens offenbaren.

48 Urteil vom 2. März 2021, Prokuratuur (Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation) (C-746/18, EU:C:2021:152, Rn. 39). Hervorhebung nur hier.

49 Urteil La Quadrature du Net, Rn. 115.

50 Ebd., Rn. 116. Hervorhebung nur hier.

51 Vgl. Fn. 19 der vorliegenden Schlussanträge.

52 Rn. 30 der Vorlagebeschlüsse.