Sammlung der Rechtsprechung

URTEIL DES GERICHTSHOFS (Große Kammer)

20. September 2022*

[Berichtigt durch Beschluss vom 27. Oktober 2022]

„Vorlage zur Vorabentscheidung – Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation – Vertraulichkeit der Kommunikation – Betreiber elektronischer Kommunikationsdienste – Allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten – Richtlinie 2002/58/EG – Art. 15 Abs. 1 – Charta der Grundrechte der Europäischen Union – Art. 6, 7, 8 und 11 sowie Art. 52 Abs. 1 – Art. 4 Abs. 2 EUV“

In den verbundenen Rechtssachen C-793/19 und C-794/19

betreffend Vorabentscheidungsersuchen nach Art. 267 AEUV, eingereicht vom Bundesverwaltungsgericht (Deutschland) mit Entscheidungen vom 25. September 2019, beim Gerichtshof eingegangen am 29. Oktober 2019, in den Verfahren

Bundesrepublik Deutschland, vertreten durch die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen,

gegen

SpaceNet AG (C-793/19),

Telekom Deutschland GmbH (C-794/19)

erlässt

DER GERICHTSHOF (Große Kammer)

unter Mitwirkung des Präsidenten K. Lenaerts, des Kammerpräsidenten A. Arabadjiev, der Kammerpräsidentin A. Prechal, der Kammerpräsidenten S. Rodin und I. Jarukaitis, der Kammerpräsidentin I. Ziemele, der Richter T. von Danwitz, M. Safjan, F. Biltgen, P. G. Xuereb (Berichterstatter) und N. Piçarra sowie der Richterin L. S. Rossi und des Richters A. Kumin,

Generalanwalt: M. Campos Sánchez-Bordona,

Kanzler: D. Dittert, Referatsleiter,

* Verfahrenssprache: Deutsch.

aufgrund des schriftlichen Verfahrens und auf die mündliche Verhandlung vom 13. September 2021,

unter Berücksichtigung der Erklärungen

– der Bundesrepublik Deutschland, vertreten durch die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, diese wiederum vertreten durch C. Mögelin als Bevollmächtigten,

– [berichtigt durch Beschluss vom 27. Oktober 2022] der SpaceNet AG, vertreten durch M. Bäcker, Universitätsprofessor,

– der Telekom Deutschland GmbH, vertreten durch Rechtsanwalt T. Mayen,

– der deutschen Regierung, vertreten durch J. Möller, F. Halibi, M. Hellmann, D. Klebs und E. Lankenau als Bevollmächtigte,

– der dänischen Regierung, vertreten durch M. Jespersen, J. Nymann-Lindegren, V. Pasternak Jørgensen und M. Søndahl Wolff als Bevollmächtigte,

– der estnischen Regierung, vertreten durch A. Kalbus und M. Kriisa als Bevollmächtigte,

– Irlands, vertreten durch A. Joyce und J. Quaney als Bevollmächtigte im Beistand von D. Fennelly, BL, und P. Gallagher, SC,

– der spanischen Regierung, vertreten durch L. Aguilera Ruiz als Bevollmächtigten,

– der französischen Regierung, vertreten durch A. Daniel, D. Dubois, J. Illouz, E. de Moustier und T. Stéhelin als Bevollmächtigte,

– der zyprischen Regierung, vertreten durch I. Neophytou als Bevollmächtigte,

– der niederländischen Regierung, vertreten durch M. K. Bulterman, A. Hanje und C. S. Schillemans als Bevollmächtigte,

– der polnischen Regierung, vertreten durch B. Majczyna, D. Lutostańska und J. Sawicka als Bevollmächtigte,

– der finnischen Regierung, vertreten durch A. Laine und M. Pere als Bevollmächtigte,

– der schwedischen Regierung, vertreten durch H. Eklinder, A. Falk, J. Lundberg, C. Meyer-Seitz, R. Shahsavan Eriksson und H. Shev als Bevollmächtigte,

– der Europäischen Kommission, vertreten durch G. Braun, S. L. Kalėda, H. Kranenborg, M. Wasmeier und F. Wilman als Bevollmächtigte,

– des Europäischen Datenschutzbeauftragten, vertreten durch A. Buchta, D. Nardi, N. Stolič und K. Ujazdowski als Bevollmächtigte,

nach Anhörung der Schlussanträge des Generalanwalts in der Sitzung vom 18. November 2021

folgendes

Urteil

1 Die Vorabentscheidungsersuchen betreffen die Auslegung von 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) (ABl. 2002, L 201, S. 37) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 (ABl. 2009, L 337, S. 11) geänderten Fassung (im Folgenden: Richtlinie 2002/58) im Licht der Art. 6 bis 8 und 11 sowie von Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta) und von Art. 4 Abs. 2 EUV.

2 Diese Ersuchen ergehen im Rahmen von Rechtsstreitigkeiten zwischen der Bundesrepublik Deutschland, vertreten durch die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Deutschland), auf der einen Seite und der SpaceNet AG (Rechtssache C-793/19) sowie der Telekom Deutschland GmbH (Rechtssache C-794/19) auf der anderen Seite wegen der den Letztgenannten auferlegten Verpflichtung, Verkehrs- und Standortdaten betreffend die Telekommunikation ihrer Kunden auf Vorrat zu speichern.

Rechtlicher Rahmen

Unionsrecht

Richtlinie 95/46/EG

3 Die Richtlinie 95/46/EG 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) wurde durch die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46 (Datenschutz-Grundverordnung) (ABl. 2016, L 119, S. 1) mit Wirkung vom 25. Mai 2018 aufgehoben.

4 Art. 3 Abs. 2 der Richtlinie 95/46 bestimmte:

„Diese Richtlinie findet keine Anwendung auf die Verarbeitung personenbezogener Daten,

– die für die Ausübung von Tätigkeiten erfolgt, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des Vertrags über die Europäische Union, und auf keinen Fall auf Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Verarbeitung die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich;

– die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird.“

Richtlinie 2002/58

5 In den Erwägungsgründen 2, 6, 7 und 11 der Richtlinie 2002/58 heißt es:

„(2) Ziel dieser Richtlinie ist die Achtung der Grundrechte; sie steht insbesondere im Einklang mit den durch die [Charta] anerkannten Grundsätzen. Insbesondere soll mit dieser Richtlinie gewährleistet werden, dass die in den Artikeln 7 und 8 [der] Charta niedergelegten Rechte uneingeschränkt geachtet werden.

….

(6) Das Internet revolutioniert die herkömmlichen Marktstrukturen, indem es eine gemeinsame, weltweite Infrastruktur für die Bereitstellung eines breiten Spektrums elektronischer Kommunikationsdienste bietet. Öffentlich zugängliche elektronische Kommunikationsdienste über das Internet eröffnen neue Möglichkeiten für die Nutzer, bilden aber auch neue Risiken in Bezug auf ihre personenbezogenen Daten und ihre Privatsphäre.

(7) Für öffentliche Kommunikationsnetze sollten besondere rechtliche, ordnungspolitische und technische Vorschriften zum Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und der berechtigten Interessen juristischer Personen erlassen werden, insbesondere im Hinblick auf die zunehmenden Fähigkeiten zur automatischen Speicherung und Verarbeitung personenbezogener Daten über Teilnehmer und Nutzer.

….

(11) Wie die Richtlinie [95/46] gilt auch die vorliegende Richtlinie nicht für Fragen des Schutzes der Grundrechte und Grundfreiheiten in Bereichen, die nicht unter das Gemeinschaftsrecht fallen. Deshalb hat sie keine Auswirkungen auf das bestehende Gleichgewicht zwischen dem Recht des Einzelnen auf Privatsphäre und der Möglichkeit der Mitgliedstaaten, Maßnahmen nach Artikel 15 Absatz 1 dieser Richtlinie zu ergreifen, die für den Schutz der öffentlichen Sicherheit, für die Landesverteidigung, für die Sicherheit des Staates (einschließlich des wirtschaftlichen Wohls des Staates, soweit die Tätigkeiten die Sicherheit des Staates berühren) und für die Durchsetzung strafrechtlicher Bestimmungen erforderlich sind. Folglich betrifft diese Richtlinie nicht die Möglichkeit der Mitgliedstaaten zum rechtmäßigen Abfangen elektronischer Nachrichten oder zum Ergreifen anderer Maßnahmen, sofern dies erforderlich ist, um einen dieser Zwecke zu erreichen, und sofern dies im Einklang mit der [am 4. November 1950 in Rom unterzeichneten] Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten in ihrer Auslegung durch die Urteile des Europäischen Gerichtshofs für Menschenrechte erfolgt. Diese Maßnahmen müssen sowohl geeignet sein als auch in einem strikt angemessenen Verhältnis zum intendierten Zweck stehen und ferner innerhalb einer demokratischen Gesellschaft notwendig sein sowie angemessenen Garantien gemäß der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten entsprechen."

6 Art. 1 („Geltungsbereich und Zielsetzung") der Richtlinie bestimmt:

„(1) Diese Richtlinie sieht die Harmonisierung der Vorschriften der Mitgliedstaaten vor, die erforderlich sind, um einen gleichwertigen Schutz der Grundrechte und Grundfreiheiten,

insbesondere des Rechts auf Privatsphäre und Vertraulichkeit, in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation sowie den freien Verkehr dieser Daten und von elektronischen Kommunikationsgeräten und -diensten in der Gemeinschaft zu gewährleisten.

(2) Die Bestimmungen dieser Richtlinie stellen eine Detaillierung und Ergänzung der Richtlinie [95/46] im Hinblick auf die in Absatz 1 genannten Zwecke dar. Darüber hinaus regeln sie den Schutz der berechtigten Interessen von Teilnehmern, bei denen es sich um juristische Personen handelt.

(3) Diese Richtlinie gilt nicht für Tätigkeiten, die nicht in den Anwendungsbereich des [AEU-]Vertrags … fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des [EU-]Vertrags …, und auf keinen Fall für Tätigkeiten betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Tätigkeit die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich."

7 In Art. 2 („Begriffsbestimmungen") der Richtlinie heißt es:

„Sofern nicht anders angegeben, gelten die Begriffsbestimmungen der Richtlinie [95/46] und der Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (‚Rahmenrichtlinie') [ABl. 2002, L 108, S. 33] auch für diese Richtlinie.

Weiterhin bezeichnet im Sinne dieser Richtlinie der Ausdruck

a) ‚Nutzer' eine natürliche Person, die einen öffentlich zugänglichen elektronischen Kommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne diesen Dienst notwendigerweise abonniert zu haben;

b) ‚Verkehrsdaten' Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein elektronisches Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden;

c) ‚Standortdaten' Daten, die in einem elektronischen Kommunikationsnetz oder von einem elektronischen Kommunikationsdienst verarbeitet werden und die den geografischen Standort des Endgeräts eines Nutzers eines öffentlich zugänglichen elektronischen Kommunikationsdienstes angeben;

d) ‚Nachricht' jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlich zugänglichen elektronischen Kommunikationsdienst ausgetauscht oder weitergeleitet wird. Dies schließt nicht Informationen ein, die als Teil eines Rundfunkdienstes über ein elektronisches Kommunikationsnetz an die Öffentlichkeit weitergeleitet werden, soweit die Informationen nicht mit dem identifizierbaren Teilnehmer oder Nutzer, der sie erhält, in Verbindung gebracht werden können;

…"

8 Art. 3 („Betroffene Dienste“) der Richtlinie 2002/58 sieht vor:

„Diese Richtlinie gilt für die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Gemeinschaft, einschließlich öffentlicher Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte unterstützen.“

9 In Art. 5 („Vertraulichkeit der Kommunikation“) der Richtlinie heißt es:

„(1) 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.

….

(3) Die Mitgliedstaaten stellen sicher, dass die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn der betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er gemäß der Richtlinie [95/46] u. a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann.“

10 Art. 6 („Verkehrsdaten“) der Richtlinie 2002/58 bestimmt:

„(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.

(3) Der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes kann die in Absatz 1 genannten Daten zum Zwecke der Vermarktung elektronischer Kommunikationsdienste oder zur Bereitstellung von Diensten mit Zusatznutzen im dazu erforderlichen Maß und innerhalb des dazu oder zur Vermarktung erforderlichen Zeitraums verarbeiten, sofern der Teilnehmer oder der Nutzer, auf den sich die Daten beziehen, zuvor seine

Einwilligung gegeben hat. Der Nutzer oder der Teilnehmer hat die Möglichkeit, seine Einwilligung zur Verarbeitung der Verkehrsdaten jederzeit zu widerrufen.

….

(5) Die Verarbeitung von Verkehrsdaten gemäß den Absätzen 1, 2, 3 und 4 darf nur durch Personen erfolgen, die auf Weisung der Betreiber öffentlicher Kommunikationsnetze und öffentlich zugänglicher Kommunikationsdienste handeln und die für Gebührenabrechnungen oder Verkehrsabwicklung, Kundenanfragen, Betrugsermittlung, die Vermarktung der elektronischen Kommunikationsdienste oder für die Bereitstellung eines Dienstes mit Zusatznutzen zuständig sind; ferner ist sie auf das für diese Tätigkeiten erforderliche Maß zu beschränken.

…“

11 Art. 9 („Andere Standortdaten als Verkehrsdaten“) Abs. 1 dieser Richtlinie sieht vor:

„Können andere Standortdaten als Verkehrsdaten in Bezug auf die Nutzer oder Teilnehmer von öffentlichen Kommunikationsnetzen oder öffentlich zugänglichen Kommunikationsdiensten verarbeitet werden, so dürfen diese Daten nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Maß und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn die Nutzer oder Teilnehmer ihre Einwilligung gegeben haben. Der Diensteanbieter muss den Nutzern oder Teilnehmern vor Einholung ihrer Einwilligung mitteilen, welche Arten anderer Standortdaten als Verkehrsdaten verarbeitet werden, für welche Zwecke und wie lange das geschieht, und ob die Daten zum Zwecke der Bereitstellung des Dienstes mit Zusatznutzen an einen Dritten weitergegeben werden. …“

12 Art. 15 („Anwendung einzelner Bestimmungen der Richtlinie [95/46]“) Abs. 1 der Richtlinie 2002/58 sieht vor:

„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] 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 [EUV] niedergelegten Grundsätzen entsprechen.“

Deutsches Recht

TKG

13 § 113a Abs. 1 Satz 1 des Telekommunikationsgesetzes (TKG) vom 22. Juni 2004 (BGBl. 2004 I S. 1190) in seiner auf die Ausgangsverfahren anwendbaren Fassung lautet:

„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."

14 § 113b TKG sieht vor:

„(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 Internetznutzung 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.

…“

15 Bei den in § 99 Abs. 2 TKG genannten Verbindungen, auf die § 113b Abs. 6 TKG Bezug nimmt, handelt es sich um Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen, die grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit besonderen Verschwiegenheitsverpflichtungen unterliegen. Voraussetzung für die Ausnahme ist nach § 99 Abs. 2 Satz 2 und 4 TKG, dass die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen die angerufenen Anschlüsse auf Antrag in eine von ihr erstellte Liste aufgenommen hat, nachdem die Inhaber der Anschlüsse ihre Aufgabenbestimmung durch Bescheinigung einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts nachgewiesen haben.

16 In § 113c Abs. 1 und 2 TKG 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;

….

(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.“

17 § 113d TKG sieht vor:

„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.“

18 Art. 113e TKG lautet:

„(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.“

19 Zur Gewährleistung eines besonders hohen Standards der Datensicherheit und Datenqualität erstellt die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen nach § 113f Abs. 1 TKG einen Anforderungskatalog, der gemäß § 113f Abs. 2 TKG fortlaufend zu überprüfen und gegebenenfalls anzupassen ist. § 113g TKG verlangt die Aufnahme spezifischer Schutzmaßnahmen in das vom Verpflichteten vorzulegende Sicherheitskonzept.

StPO

20 § 100g Abs. 2 Satz 1 der Strafprozessordnung (StPO) lautet:

„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."

21 § 101a Abs. 1 StPO regelt für die Erhebung von Verkehrsdaten nach § 100g StPO einen Richtervorbehalt. Die Begründung des Beschlusses muss nach § 101a Abs. 2 StPO einzelfallbezogen die wesentlichen Erwägungen zur Erforderlichkeit und Angemessenheit der Maßnahme darlegen. § 101a Abs. 6 StPO sieht eine Pflicht zur Benachrichtigung der Beteiligten der betroffenen Telekommunikation vor.

Ausgangsverfahren und Vorlagefrage

22 SpaceNet und Telekom Deutschland erbringen in Deutschland öffentlich zugängliche Internetzugangsdienste. Telekom Deutschland erbringt darüber hinaus, ebenfalls in Deutschland, öffentlich zugängliche Telefondienste.

23 Diese Diensteanbieter fochten vor dem Verwaltungsgericht Köln (Deutschland) die ihnen durch § 113a Abs. 1 in Verbindung mit § 113b TKG auferlegte Pflicht an, ab dem 1. Juli 2017 Verkehrs- und Standortdaten betreffend die Telekommunikation ihrer Kunden auf Vorrat zu speichern.

24 Mit Urteilen vom 20. April 2018 entschied das Verwaltungsgericht Köln, dass SpaceNet und Telekom Deutschland nicht verpflichtet seien, die in § 113b Abs. 3 TKG genannten Verkehrsdaten in Bezug auf die Telekommunikation der Kunden, denen sie einen Internetzugang zur Verfügung stellten, auf Vorrat zu speichern, und dass Telekom Deutschland ferner nicht verpflichtet sei, die in § 113b Abs. 2 Satz 1 und 2 TKG genannten Verkehrsdaten in Bezug auf die Telekommunikation der Kunden, denen sie einen Zugang zu öffentlichen Telefondiensten zur Verfügung stelle, auf Vorrat zu speichern. Dieses Gericht war nämlich im Licht des Urteils vom 21. Dezember 2016, Tele2 Sverige und Watson u. a. (C-203/15 und C-698/15, EU:C:2016:970), der Auffassung, dass diese Pflicht zur Vorratsspeicherung gegen das Unionsrecht verstoße.

25 Die Bundesrepublik Deutschland legte beim Bundesverwaltungsgericht (Deutschland), dem vorlegenden Gericht, Revision gegen diese Urteile ein.

26 Das Bundesverwaltungsgericht ist der Ansicht, dass die Frage, ob die durch § 113a Abs. 1 in Verbindung mit § 113b TKG auferlegte Pflicht zur Vorratsspeicherung gegen das Unionsrecht verstoße, von der Auslegung der Richtlinie 2002/58 abhänge.

27 Insoweit weist das vorlegende Gericht darauf hin, dass der Gerichtshof bereits im Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u. a. (C-203/15 und C-698/15, EU:C:2016:970), abschließend geklärt habe, dass Regelungen über die Vorratsspeicherung von Verkehrs- und Standortdaten sowie über den Zugang der nationalen Behörden zu diesen Daten grundsätzlich in den Geltungsbereich der Richtlinie 2002/58 fielen.

28 Außerdem könne die in den Ausgangsverfahren in Rede stehende Pflicht zur Vorratsspeicherung, soweit sie die Rechte aus Art. 5 Abs. 1, Art. 6 Abs. 1 und Art. 9 Abs. 1 der Richtlinie 2002/58 beschränke, nur auf der Grundlage von Art. 15 Abs. 1 dieser Richtlinie gerechtfertigt werden.

29 Insoweit gehe aus dem Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u. a. (C-203/15 und C-698/15, EU:C:2016:970), hervor, dass Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta dahin auszulegen sei, dass er einer nationalen Regelung entgegenstehe, die für Zwecke der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsehe.

30 Nach Ansicht des vorlegenden Gerichts verlangt die in den Ausgangsverfahren in Rede stehende nationale Regelung jedoch wie die nationalen Regelungen, um die es in den Rechtssachen ging, in denen das genannte Urteil ergangen ist, weder einen Anlass für die Speicherung der Daten noch irgendeinen Zusammenhang zwischen den gespeicherten Daten und einer Straftat oder einer Gefahr für die öffentliche Sicherheit. Diese nationale Regelung schreibe nämlich eine anlasslose, flächendeckende und personell, zeitlich und geografisch undifferenzierte Speicherung eines Großteils der relevanten Telekommunikations-Verkehrsdaten vor.

31 Das vorlegende Gericht ist allerdings der Auffassung, dass nicht ausgeschlossen sei, dass die in den Ausgangsverfahren in Rede stehende Pflicht zur Vorratsspeicherung nach Art. 15 Abs. 1 der Richtlinie 2002/58 gerechtfertigt sein könne.

32 Erstens verlange die in den Ausgangsverfahren in Rede stehende nationale Regelung im Gegensatz zu den nationalen Regelungen, um die es in den Rechtssachen gegangen sei, in denen das Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u. a. (C-203/15 und C-698/15, EU:C:2016:970), ergangen sei, nicht die Vorratsspeicherung sämtlicher Verkehrsdaten bezüglich der Telekommunikation aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel. Von der Speicherpflicht ausgenommen sei nicht nur der Inhalt der Kommunikation, sondern es dürften auch Daten über aufgerufene Internetseiten, Daten von E-Mail-Diensten sowie Daten, die den Verbindungen zu oder von bestimmten Anschlüssen in sozialen oder kirchlichen Bereichen zugrunde lägen, nicht gespeichert werden, wie aus § 113b Abs. 5 und 6 TKG hervorgehe.

33 Zweitens weist das vorlegende Gericht darauf hin, dass § 113b Abs. 1 TKG eine Speicherungsfrist von vier Wochen für Standortdaten und von zehn Wochen für Verkehrsdaten vorsehe, während die Richtlinie 2006/24/EG 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), die den nationalen Regelungen zugrunde gelegen habe, um die es in den Rechtssachen gegangen sei,

in denen das Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u. a. (C-203/15 und C-698/15, EU:C:2016:970), ergangen sei, eine Speicherungsfrist zwischen sechs Monaten und zwei Jahren vorgesehen habe.

34 Zwar genügten die Ausnahme bestimmter Kommunikationsmittel oder Datenkategorien und die Begrenzung der Speicherungsfrist nicht, um jede Gefahr der Erstellung eines umfassenden Profils der betroffenen Personen zu beseitigen, jedoch sei diese Gefahr im Rahmen der Anwendung der in den Ausgangsverfahren in Rede stehenden nationalen Regelung zumindest erheblich verringert.

35 Drittens enthalte diese Regelung strenge Beschränkungen in Bezug auf den Schutz der gespeicherten Daten und den Zugang hierzu. Somit gewährleiste sie zum einen einen wirksamen Schutz der auf Vorrat gespeicherten Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang. Zum anderen dürften die auf Vorrat gespeicherten Daten nur zur Bekämpfung 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.

36 Viertens könnte nach Ansicht des vorlegenden Gerichts der Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58 dahin, dass jede anlasslose Vorratsdatenspeicherung mit dem Unionsrecht allgemein unvereinbar wäre, die Handlungspflicht der Mitgliedstaaten entgegenstehen, die sich aus dem in Art. 6 der Charta verankerten Recht auf Sicherheit ergebe.

37 Fünftens würde nach Auffassung des vorlegenden Gerichts eine Auslegung von Art. 15 der Richtlinie 2002/58 dahin, dass er einer allgemeinen Vorratsspeicherung der Daten entgegensteht, den Handlungsspielraum des nationalen Gesetzgebers in einem Bereich der Strafverfolgung und der öffentlichen Sicherheit, der nach Art. 4 Abs. 2 EUV weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten fällt, erheblich einschränken.

38 Sechstens ist das vorlegende Gericht der Ansicht, dass die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte zu berücksichtigen sei und weist darauf hin, dass dieser entschieden habe, dass Art. 8 Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK) nationalen Bestimmungen, die eine Massenüberwachung des grenzüberschreitenden Datenverkehrs vorsähen, angesichts der Bedrohungen, denen zahlreiche Staaten derzeit ausgesetzt seien, und den technologischen Instrumenten, auf die sich Terroristen und Kriminelle nunmehr zur Begehung strafbarer Handlungen stützen könnten, nicht entgegenstehe.

39 Vor diesem Hintergrund hat das Bundesverwaltungsgericht beschlossen, die Verfahren auszusetzen und dem Gerichtshof 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

1. diese Verpflichtung keinen spezifischen Anlass in örtlicher, zeitlicher oder räumlicher Hinsicht voraussetzt,

2. 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:
   a) die Rufnummer oder eine andere Kennung des anrufenden und des angerufenen Anschlusses sowie bei Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses,
   b) 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,
   c) Angaben zu dem genutzten Dienst, wenn im Rahmen des Telefondienstes unterschiedliche Dienste genutzt werden können,
   d) im Fall mobiler Telefondienste ferner
      i) die internationale Kennung mobiler Teilnehmer für den anrufenden und den angerufenen Anschluss,
      ii) die internationale Kennung des anrufenden und des angerufenen Endgerätes,
      iii) Datum und Uhrzeit der ersten Aktivierung des Dienstes unter Angabe der zugrunde liegenden Zeitzone, wenn Dienste im Voraus bezahlt wurden,
      iv) die Bezeichnungen der Funkzellen, die durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzt wurden,
   e) im Fall von Internet-Telefondiensten auch die Internetprotokoll-Adressen des anrufenden und des angerufenen Anschlusses und zugewiesene Benutzerkennungen,

3. Gegenstand der Pflicht zur Speicherung bei der Erbringung öffentlich zugänglicher Internetzugangsdienste folgende Daten sind:
   a) die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse,
   b) eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt, sowie eine zugewiesene Benutzerkennung,
   c) Datum und Uhrzeit von Beginn und Ende der Internetnutzung unter der zugewiesenen Internetprotokoll-Adresse unter Angabe der zugrunde liegenden Zeitzone,
   d) im Fall der mobilen Nutzung die Bezeichnung der bei Beginn der Internetverbindung genutzten Funkzelle,

4. folgende Daten nicht gespeichert werden dürfen:
   a) der Inhalt der Kommunikation,
   b) Daten über aufgerufene Internetseiten,
   c) Daten von Diensten der elektronischen Post,
   d) Daten, die den Verbindungen zu oder von bestimmten Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen zugrunde liegen,

5. 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,

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

7. 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?

Verfahren vor dem Gerichtshof

40 Mit Beschluss des Präsidenten des Gerichtshofs vom 3. Dezember 2019 sind die Rechtssachen C-793/19 und C-794/19 zu gemeinsamem schriftlichen und mündlichen Verfahren sowie zu gemeinsamer Entscheidung verbunden worden.

41 Mit Beschluss des Präsidenten des Gerichtshofs vom 14. Juli 2020 ist das Verfahren in den verbundenen Rechtssachen C-793/19 und C-794/19 gemäß Art. 55 Abs. 1 Buchst. b der Verfahrensordnung des Gerichtshofs bis zur Verkündung des Urteils in der Rechtssache La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18) ausgesetzt worden.

42 Nachdem der Gerichtshof am 6. Oktober 2020 sein Urteil in der Rechtssache La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791) erlassen hatte, hat der Präsident des Gerichtshofs am 8. Oktober 2020 die Fortsetzung des Verfahrens in den verbundenen Rechtssachen C-793/19 und C-794/19 angeordnet.

43 Das vorlegende Gericht, dem die Kanzlei dieses Urteil übermittelt hatte, hat mitgeteilt, dass es sein Vorabentscheidungsersuchen aufrechterhalte.

44 Insoweit hat das vorlegende Gericht zunächst darauf hingewiesen, dass die in der in den Ausgangsverfahren in Rede stehenden Regelung vorgesehene Speicherpflicht weniger Daten und eine kürzere Speicherungsfrist betreffe, als sie die nationalen Regelungen vorgesehen hätten, um die es in den Rechtssachen gegangen sei, in denen das Urteil vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791), ergangen sei. Diese Besonderheiten verringerten die Möglichkeit, dass aus den gespeicherten Daten sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten auf Vorrat gespeichert worden seien, gezogen würden.

45 Sodann hat das vorlegende Gericht erneut darauf hingewiesen, dass die in den Ausgangsverfahren in Rede stehende nationale Regelung gewährleiste, dass die auf Vorrat gespeicherten Daten wirksam vor den Risiken eines Missbrauchs und eines unberechtigten Zugangs geschützt seien.

46 Schließlich hat es hervorgehoben, dass weiterhin Unsicherheiten hinsichtlich der Frage bestünden, ob die in der in den Ausgangsverfahren in Rede stehenden nationalen Regelung vorgesehene Speicherung der IP-Adressen mit dem Unionsrecht vereinbar sei, weil zwischen den Rn. 155 und 168 des Urteils vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791), eine Inkohärenz bestehe. So ergebe sich aus diesem Urteil eine Unsicherheit hinsichtlich der Frage, ob der Gerichtshof für die Vorratsspeicherung der IP-Adressen einen mit dem Ziel des Schutzes der nationalen Sicherheit, der Bekämpfung schwerer Kriminalität oder der Verhütung schwerer Bedrohungen der öffentlichen Sicherheit zusammenhängenden Anlass verlange, wie sich aus Rn. 168 des genannten Urteils ergebe, oder ob die Vorratsspeicherung der IP-Adressen auch bei Fehlen eines konkreten Anlasses zulässig sei und lediglich die Verwendung der gespeicherten Daten durch diese Ziele begrenzt werde, wie sich aus Rn. 155 des genannten Urteils ergebe.

Zur Vorlagefrage

47 Mit seiner Vorlagefrage möchte das vorlegende Gericht im Wesentlichen wissen, ob Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 6 bis 8 und 11 sowie des Art. 52 Abs. 1 der Charta und des Art. 4 Abs. 2 EUV dahin auszulegen ist, dass er einer nationalen Rechtsvorschrift entgegensteht, die – von bestimmten Ausnahmen abgesehen – die Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste für die in Art. 15 Abs. 1 der genannten Richtlinie aufgeführten Zwecke, insbesondere zur Verfolgung schwerer Straftaten oder zur Abwehr einer konkreten Gefahr für die nationale Sicherheit, zu einer allgemeinen und unterschiedslosen Vorratsspeicherung eines Großteils der Verkehrs- und Standortdaten der Endnutzer dieser Dienste verpflichtet und eine Speicherungsfrist von mehreren Wochen sowie Regeln vorsieht, die einen wirksamen Schutz der auf Vorrat gespeicherten Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang gewährleisten sollen.

Zur Anwendbarkeit der Richtlinie 2002/58

48 Was das Vorbringen Irlands sowie der französischen, der niederländischen, der polnischen und der schwedischen Regierung anbelangt, die in den Ausgangsverfahren in Rede stehende nationale Regelung falle nicht in den Geltungsbereich der Richtlinie 2002/58, da sie insbesondere zum Schutz der nationalen Sicherheit erlassen worden sei, genügt der Hinweis, dass eine nationale Regelung, die wie die in den Ausgangsverfahren in Rede stehende 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 fällt (Urteil vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 104).

Zur Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58

Hinweis auf die sich aus der Rechtsprechung des Gerichtshofs ergebenden Grundsätze

49 Nach ständiger Rechtsprechung ist bei der Auslegung einer unionsrechtlichen Vorschrift nicht nur ihr Wortlaut zu berücksichtigen, sondern auch ihr Kontext und die Ziele, die mit der Regelung, zu der sie gehört, verfolgt werden, und insbesondere deren Entstehungsgeschichte (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 32 und die dort angeführte Rechtsprechung).

50 Bereits aus dem Wortlaut von Art. 15 Abs. 1 der Richtlinie 2002/58 geht hervor, dass die Rechtsvorschriften, zu deren Erlass die Richtlinie die Mitgliedstaaten unter den in der Richtlinie festgelegten Voraussetzungen ermächtigt, lediglich darauf abzielen können, die u. a. in den Art. 5, 6 und 9 der Richtlinie 2002/58 vorgesehenen Rechte und Pflichten zu „beschränken“ (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 33).

51 Was das durch diese Richtlinie eingeführte System betrifft, in das sich ihr Art. 15 Abs. 1 einfügt, ist darauf hinzuweisen, dass die Mitgliedstaaten nach Art. 5 Abs. 1 Sätze 1 und 2 der Richtlinie verpflichtet sind, 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 (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 34).

52 Insoweit hat der Gerichtshof bereits entschieden, dass in Art. 5 Abs. 1 der Richtlinie 2002/58 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 (Urteile vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 107, sowie vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 35).

53 Diese Bestimmung spiegelt das vom Unionsgesetzgeber beim Erlass der Richtlinie 2002/58 verfolgte Ziel wider. Aus der Begründung des Vorschlags für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (KOM[2000] 385 endg.), aus dem die Richtlinie 2002/58 hervorgegangen ist, ergibt sich nämlich, dass der Unionsgesetzgeber sicherstellen wollte, „dass für alle elektronischen Kommunikationsdienste unabhängig von der zugrunde liegenden Technologie weiterhin ein hochgradiger Schutz personenbezogener Daten und der Privatsphäre gewährleistet bleibt“. Die genannte Richtlinie soll somit, wie sich u. a. aus ihren Erwägungsgründen 6 und 7 ergibt, die Nutzer elektronischer Kommunikationsdienste vor den Risiken für ihre personenbezogenen Daten und ihre Privatsphäre schützen, die sich aus den neuen Technologien und vor allem den zunehmenden Fähigkeiten zur automatisierten Speicherung und Verarbeitung von Daten ergeben. Insbesondere ist es, wie im zweiten Erwägungsgrund der Richtlinie zum Ausdruck kommt, der Wille des Unionsgesetzgebers, die uneingeschränkte Achtung der in den die Achtung des Privatlebens bzw. den Schutz personenbezogener Daten garantierenden Art. 7 und 8 der Charta niedergelegten Rechte zu gewährleisten (vgl. in diesem Sinne Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 36 und die dort angeführte Rechtsprechung).

54 Durch den Erlass der Richtlinie 2002/58 hat der Unionsgesetzgeber somit diese Rechte konkretisiert, so dass die Nutzer elektronischer Kommunikationsmittel grundsätzlich erwarten dürfen, dass ihre Nachrichten und die damit verbundenen Verkehrsdaten anonym bleiben und nicht gespeichert werden dürfen, es sei denn, sie haben darin eingewilligt (Urteile vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 109, sowie vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 37).

55 Was die Verarbeitung und Speicherung von sich auf Teilnehmer und Nutzer beziehenden Verkehrsdaten durch die Betreiber elektronischer Kommunikationsdienste anbelangt, sieht Art. 6 der Richtlinie 2002/58 in Abs. 1 vor, dass diese Daten zu löschen oder zu anonymisieren sind, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden, und stellt in Abs. 2 klar, 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.

56 Folglich beschränkt sich die Richtlinie 2002/58 nicht darauf, den Zugang zu solchen Daten durch Garantien zu regeln, die Missbrauch verhindern sollen, sondern sie regelt insbesondere auch den Grundsatz des Verbots der Speicherung dieser Daten durch Dritte (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 39).

57 Indem Art. 15 Abs. 1 der Richtlinie 2002/58 den Mitgliedstaaten gestattet, Rechtsvorschriften zu erlassen, die die Rechte und Pflichten gemäß u. a. den Art. 5, 6 und 9 dieser Richtlinie – wie sie sich aus den in Rn. 52 des vorliegenden Urteils angeführten Grundsätzen der Vertraulichkeit der Kommunikation und dem Verbot der Speicherung der damit verbundenen Daten ergeben – „beschränken“, sieht diese Bestimmung eine Ausnahme von der allgemeinen Regel vor, die u. a. in den Art. 5, 6 und 9 vorgesehen ist, und ist daher nach ständiger Rechtsprechung eng auszulegen. Eine solche Bestimmung vermag es daher nicht zu rechtfertigen, dass 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 vorgesehenen Verbot, diese Daten zu speichern, zur Regel wird, soll die letztgenannte Vorschrift nicht weitgehend ausgehöhlt werden (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 40 und die dort angeführte Rechtsprechung).

58 Hinsichtlich der Zwecke, die eine Beschränkung der insbesondere in den Art. 5, 6 und 9 der Richtlinie 2002/58 vorgesehenen Rechte und Pflichten rechtfertigen können, hat der Gerichtshof bereits entschieden, dass die Aufzählung der in Art. 15 Abs. 1 Satz 1 der Richtlinie genannten Zwecke abschließend ist, so dass eine aufgrund dieser Bestimmung erlassene Rechtsvorschrift tatsächlich strikt einem von ihnen dienen muss (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 41 und die dort angeführte Rechtsprechung).

59 Außerdem geht aus Art. 15 Abs. 1 Satz 3 der Richtlinie 2002/58 hervor, dass die nach dieser Vorschrift von den Mitgliedstaaten erlassenen Vorschriften die allgemeinen Grundsätze des Unionsrechts beachten müssen, zu denen der Grundsatz der Verhältnismäßigkeit gehört, und die Achtung der durch die Charta garantierten Grundrechte gewährleisten müssen. Hierzu hat der Gerichtshof bereits entschieden, dass die den Betreibern elektronischer Kommunikationsdienste durch nationale Rechtsvorschriften auferlegte Pflicht, Verkehrsdaten auf Vorrat zu speichern, um sie gegebenenfalls den zuständigen nationalen Behörden zugänglich zu machen, Fragen aufwirft, die nicht nur die Einhaltung der Art. 7 und 8 der Charta betreffen, sondern auch die in Art. 11 der Charta gewährleistete Freiheit der Meinungsäußerung, und dass diese Freiheit eine der wesentlichen Grundlagen einer demokratischen und pluralistischen Gesellschaft darstellt, die zu den Werten gehört, auf die sich die Europäische Union nach Art. 2 EUV gründet (vgl. in diesem Sinne Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 42 und 43 sowie die dort angeführte Rechtsprechung).

60 Insoweit ist darauf hinzuweisen, dass die Speicherung der Verkehrs- und Standortdaten als solche zum einen eine Abweichung von dem nach Art. 5 Abs. 1 der Richtlinie 2002/58 für alle anderen Personen als die Nutzer geltenden Verbot der Speicherung dieser Daten darstellt und zum anderen einen Eingriff in die Grundrechte auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten, die in den Art. 7 und 8 der Charta 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 (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 44 und die dort angeführte Rechtsprechung).

61 Dieser Schluss erscheint umso gerechtfertigter, als die Verkehrs- und Standortdaten Informationen über eine Vielzahl von Aspekten des Privatlebens der Betroffenen enthalten können, 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 (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 45 und die dort angeführte Rechtsprechung).

62 Daher kann die Vorratsspeicherung von Verkehrs- und Standortdaten zu polizeilichen Zwecken zum einen das in Art. 7 der Charta verankerte Recht auf Achtung der Kommunikation beeinträchtigen und die Nutzer elektronischer Kommunikationsmittel von der Ausübung ihrer durch Art. 11 der Charta gewährleisteten Freiheit der Meinungsäußerung abhalten; diese Wirkungen sind umso stärker, je größer die Menge und die Vielfalt der auf Vorrat gespeicherten Daten sind. Zum anderen birgt die bloße Vorratsspeicherung durch die Betreiber elektronischer Kommunikationsdienste 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, Gefahren des Missbrauchs und des rechtswidrigen Zugangs (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 46 und die dort angeführte Rechtsprechung).

63 In Art. 15 Abs. 1 der Richtlinie 2002/58, der es den Mitgliedstaaten gestattet, die in den Rn. 51 bis 54 des vorliegenden Urteils angesprochenen Rechte und Pflichten zu beschränken, kommt allerdings zum Ausdruck, dass die in den Art. 7, 8 und 11 der Charta verankerten Rechte keine uneingeschränkte Geltung beanspruchen können, sondern im Hinblick auf ihre gesellschaftliche Funktion gesehen werden müssen. Nach Art. 52 Abs. 1 der Charta sind nämlich 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 im Licht der Charta muss somit auch berücksichtigt werden, welche Bedeutung den in den Art. 3, 4, 6 und 7 der Charta 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 (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 48 und die dort angeführte Rechtsprechung).

64 Somit ist in Bezug insbesondere auf die wirksame Bekämpfung von Straftaten, deren Opfer u. a. Minderjährige und andere schutzbedürftige Personen sind, zu berücksichtigen, dass sich aus Art. 7 der Charta positive Verpflichtungen der Behörden im Hinblick auf den Erlass rechtlicher Maßnahmen zum Schutz des Privat- und Familienlebens ergeben können. Solche Verpflichtungen können sich aus Art. 7 auch in Bezug auf den Schutz der Wohnung und der Kommunikation sowie aus den Art. 3 und 4 hinsichtlich des Schutzes der körperlichen und geistigen Unversehrtheit der Menschen sowie des Verbots der Folter und unmenschlicher oder erniedrigender Behandlung ergeben (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 49 und die dort angeführte Rechtsprechung).

65 Angesichts dieser verschiedenen positiven Verpflichtungen müssen die verschiedenen betroffenen berechtigten Interessen und Rechte somit miteinander in Einklang gebracht werden, und es ist ein rechtlicher Rahmen zu schaffen, der diesen Einklang ermöglicht (vgl. in diesem Sinne Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 50 und die dort angeführte Rechtsprechung).

66 In diesem Rahmen ergibt sich bereits aus dem Wortlaut von Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58, dass die Mitgliedstaaten eine Vorschrift erlassen können, die von dem in Rn. 52 des vorliegenden Urteils genannten Grundsatz der Vertraulichkeit abweicht, wenn eine solche Vorschrift „in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig“ ist, wobei es im elften Erwägungsgrund der Richtlinie heißt, dass eine derartige Maßnahme in einem „strikt“ angemessenen Verhältnis zum intendierten Zweck stehen muss.

67 Insoweit ist darauf hinzuweisen, dass der Schutz des Grundrechts auf Achtung des Privatlebens nach ständiger Rechtsprechung des Gerichtshofs verlangt, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken. Außerdem kann eine dem Gemeinwohl dienende Zielsetzung nicht verfolgt werden, ohne den Umstand zu berücksichtigen, dass sie mit den von der Maßnahme betroffenen Grundrechten in Einklang gebracht werden muss, indem eine ausgewogene Gewichtung der dem Gemeinwohl dienenden Zielsetzung und der fraglichen Rechte vorgenommen wird (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 52 und die dort angeführte Rechtsprechung).

68 Insbesondere geht aus der Rechtsprechung des Gerichtshofs hervor, dass die Möglichkeit für die Mitgliedstaaten, eine Beschränkung der u. a. in den Art. 5, 6 und 9 der Richtlinie 2002/58 vorgesehenen Rechte und Pflichten zu rechtfertigen, zu beurteilen ist, indem die Schwere des mit einer solchen Beschränkung verbundenen Eingriffs bestimmt und geprüft wird, ob die verfolgte dem Gemeinwohl dienende Zielsetzung in angemessenem Verhältnis zur Schwere des Eingriffs steht (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 53 und die dort angeführte Rechtsprechung).

69 Um dem Erfordernis der Verhältnismäßigkeit zu genügen, müssen nationale Rechtsvorschriften klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindesterfordernisse aufstellen, so dass 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. Das Erfordernis, über solche Garantien zu verfügen, ist umso bedeutsamer, wenn die

personenbezogenen Daten automatisiert verarbeitet werden, vor allem wenn eine erhebliche Gefahr des unberechtigten Zugangs zu ihnen besteht. Diese Erwägungen gelten in besonderem Maß, wenn es um den Schutz der besonderen Kategorie sensibler personenbezogener Daten geht (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 54 und die dort angeführte Rechtsprechung).

70 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 (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 55 und die dort angeführte Rechtsprechung).

71 Was die dem Gemeinwohl dienenden Ziele anbelangt, die eine nach Art. 15 Abs. 1 der Richtlinie 2002/58 erlassene Vorschrift rechtfertigen können, geht aus der Rechtsprechung des Gerichtshofs, insbesondere aus dem Urteil vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791), hervor, dass nach dem Grundsatz der Verhältnismäßigkeit eine Hierarchie zwischen diesen Zielen entsprechend ihrer jeweiligen Bedeutung besteht und dass die Bedeutung des mit einer solchen Vorschrift verfolgten Ziels im Verhältnis zur Schwere des daraus resultierenden Eingriffs stehen muss (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 56).

72 Daher hat der Gerichtshof, was den Schutz der nationalen Sicherheit anbelangt, dessen Bedeutung die der übrigen von Art. 15 Abs. 1 der Richtlinie 2002/58 erfassten Ziele übersteigt, festgestellt, dass diese Bestimmung im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta 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 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 (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 58 und die dort angeführte Rechtsprechung).

73 Was das Ziel der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten anbelangt, hat der Gerichtshof festgestellt, 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, die in den Art. 7 und 8 der Charta verankert sind, zu rechtfertigen. Daher können nur Eingriffe in die genannten Grundrechte, die nicht schwer sind, durch das Ziel der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten im Allgemeinen gerechtfertigt sein (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 59 und die dort angeführte Rechtsprechung).

74 Was das Ziel der Bekämpfung schwerer Kriminalität anbelangt, hat der Gerichtshof entschieden, dass nationale Rechtsvorschriften, die zu diesem Zweck die allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen, die Grenzen des absolut Notwendigen überschreiten und nicht als in einer demokratischen Gesellschaft gerechtfertigt

angesehen werden können. Angesichts des sensiblen Charakters der Informationen, die sich aus den Verkehrs- und Standortdaten ergeben können, ist deren Vertraulichkeit nämlich von entscheidender Bedeutung für das Recht auf Achtung des Privatlebens. In Anbetracht zum einen der in Rn. 62 des vorliegenden Urteils angesprochenen abschreckenden Wirkungen, die die Speicherung dieser Daten auf die Ausübung der in den Art. 7 und 11 der Charta verankerten Grundrechte haben kann, und zum anderen der Schwere des mit ihr verbundenen Eingriffs muss eine solche Speicherung in einer demokratischen Gesellschaft, wie es das durch die Richtlinie 2002/58 geschaffene System vorsieht, die Ausnahme und nicht die Regel sein, und solche Daten dürfen nicht Gegenstand einer systematischen und kontinuierlichen Speicherung sein. Dies gilt auch in Anbetracht der Ziele der Bekämpfung schwerer Kriminalität und der Verhütung ernster Bedrohungen der öffentlichen Sicherheit sowie der Bedeutung, die ihnen beizumessen ist (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 65 und die dort angeführte Rechtsprechung).

75 Dagegen hat der Gerichtshof klargestellt, 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 Rechtsvorschriften nicht entgegensteht, die 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;

– für einen auf das absolut Notwendige begrenzten Zeitraum eine allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, vorsehen;

– eine allgemeine und unterschiedslose Vorratsspeicherung der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten vorsehen;

– 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)*.

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 (Urteile vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 168, sowie vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 67).

Zu einer Maßnahme, die für eine Dauer von mehreren Wochen eine allgemeine und unterschiedslose Vorratsspeicherung eines Großteils der Verkehrs- und Standortdaten vorsieht

76 Anhand dieser grundsätzlichen Erwägungen sind die vom vorlegenden Gericht hervorgehobenen Merkmale der in den Ausgangsverfahren in Rede stehenden nationalen Regelung zu prüfen.

77 Was erstens den Umfang der auf Vorrat gespeicherten Daten anbelangt, geht aus der Vorlageentscheidung hervor, dass im Rahmen der Erbringung von Telefondiensten die durch diese Regelung auferlegte Pflicht zur Vorratsspeicherung 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. Im Rahmen der Bereitstellung von Internetzugangsdiensten bezieht sich die Pflicht zur Vorratsspeicherung 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. Die Daten, aus denen sich die geografische Lage und die Hauptstrahlrichtungen der die jeweilige Funkzelle versorgenden Funkantennen ergeben, werden ebenfalls gespeichert.

78 Zwar nimmt die in den Ausgangsverfahren in Rede stehende nationale Regelung den Inhalt der Kommunikation sowie die Daten über aufgerufene Internetseiten von der Speicherpflicht aus und schreibt die Speicherung der Funkzellenkennung lediglich zu Beginn der Kommunikation vor, jedoch ist darauf hinzuweisen, dass dies im Wesentlichen auch für die nationalen Regelungen zur Umsetzung der Richtlinie 2006/24 galt, um die es in den Rechtssachen ging, in denen das Urteil vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791), ergangen ist. Trotz dieser Beschränkungen hat der Gerichtshof in diesem Urteil aber entschieden, dass die Kategorien der nach der genannten Richtlinie und diesen nationalen Regelungen auf Vorrat gespeicherten Daten sehr genaue Schlüsse auf das Privatleben der betroffenen Personen – 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 – und insbesondere die Erstellung eines Profils dieser Personen ermöglichen konnten.

79 Darüber hinaus ist festzustellen, dass die in den Ausgangsverfahren in Rede stehende Regelung zwar nicht die Daten über die aufgerufenen Internetseiten erfasst, wohl aber die Speicherung der IP-Adressen vorsieht. Diese Adressen können jedoch insbesondere zur umfassenden Nachverfolgung der von einem Internetnutzer besuchten Internetseiten und infolgedessen seiner Online-Aktivität genutzt werden, so dass diese Daten die Erstellung eines detaillierten Profils dieses Nutzers ermöglichen. Die für eine solche Nachverfolgung erforderliche Vorratsspeicherung und Analyse der IP-Adressen stellen daher schwere Eingriffe in die Grundrechte des Internetnutzers aus den Art. 7 und 8 der Charta dar (vgl. in diesem Sinne Urteil vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 153).

80 Außerdem stellen, wie SpaceNet in ihren schriftlichen Erklärungen ausgeführt hat, die Daten betreffend E-Mail-Dienste, auch wenn sie nicht von der in der in den Ausgangsverfahren in Rede stehenden Regelung vorgesehenen Pflicht zur Vorratsspeicherung erfasst werden, nur einen Bruchteil der in Rede stehenden Daten dar.

81 Wie der Generalanwalt in Nr. 60 seiner Schlussanträge im Kern ausgeführt hat, erstreckt sich die in der in den Ausgangsverfahren in Rede stehenden nationalen Regelung vorgesehene Pflicht zur Vorratsspeicherung somit auf einen umfangreichen Satz von Verkehrs- und Standortdaten, der im Wesentlichen denjenigen entspricht, die zu der ständigen Rechtsprechung geführt haben, auf die in Rn. 78 des vorliegenden Urteils hingewiesen worden ist.

82 Des Weiteren hat die deutsche Regierung in Beantwortung einer in der mündlichen Verhandlung gestellten Frage ausgeführt, dass in der Liste der Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen lediglich 1 300 Stellen aufgeführt seien, deren Daten betreffend die elektronische Kommunikation nicht nach § 99 Abs. 2 und § 113b Abs. 6 TKG auf Vorrat gespeichert würden, was offensichtlich einen geringen Teil aller Nutzer von Telekommunikationsdiensten in Deutschland darstellt, deren Daten unter die in der in den Ausgangsverfahren in Rede stehenden nationalen Regelung vorgesehene Pflicht zur Vorratsspeicherung fallen. So werden u. a. Daten von Nutzern gespeichert, die dem Berufsgeheimnis unterliegen, wie beispielsweise Rechtsanwälte, Ärzte und Journalisten.

83 Aus der Vorlageentscheidung geht somit hervor, dass die in dieser nationalen Regelung 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, deren Umfang im Wesentlichen dem der Daten entspricht, die in den Rechtssachen gespeichert wurden, die zu der in Rn. 78 des vorliegenden Urteils angeführten Rechtsprechung geführt haben.

84 In Anbetracht der in Rn. 75 des vorliegenden Urteils angeführten Rechtsprechung kann daher eine Verpflichtung zur Vorratsdatenspeicherung wie die in den Ausgangsverfahren in Rede stehende entgegen dem Vorbringen der deutschen Regierung nicht als gezielte Vorratsdatenspeicherung angesehen werden.

85 Zweitens ergibt sich, was die Vorratsspeicherungsfrist anbelangt, aus Art. 15 Abs. 1 Satz 2 der Richtlinie 2002/58, dass die Vorratsspeicherungsfrist, die eine nationale Maßnahme vorsieht, die eine allgemeine und unterschiedslose Vorratsdatenspeicherung vorschreibt, zwar ein relevanter Faktor unter anderen ist, um zu bestimmen, ob das Unionsrecht einer solchen Maßnahme entgegensteht, wobei der genannte Satz 2 verlangt, dass diese Frist „begrenzt“ sein muss.

86 Im vorliegenden Fall sind diese Fristen, die gemäß § 113b Abs. 1 TKG vier Wochen für Standortdaten und zehn Wochen für sonstige Daten betragen, zwar deutlich kürzer als die Fristen, die in den nationalen Regelungen, die eine Pflicht zur allgemeinen und unterschiedslosen Vorratsspeicherung vorschreiben, vorgesehen sind, die der Gerichtshof in seinen Urteilen vom 21. Dezember 2016, Tele2 Sverige und Watson u. a. (C-203/15 und C-698/15, EU:C:2016:970), vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791), sowie vom 5. April 2022, Commissioner of An Garda Síochána u. a. (C-140/20, EU:C:2022:258), geprüft hat.

87 Wie aus der in Rn. 61 des vorliegenden Urteils angeführten Rechtsprechung hervorgeht, ergibt sich die Schwere des Eingriffs jedoch aus der Gefahr, dass die auf Vorrat gespeicherten Daten insbesondere in Anbetracht ihrer Menge und Vielfalt es in ihrer Gesamtheit ermöglichen, sehr genaue Schlüsse auf das Privatleben der Person bzw. der Personen zu ziehen, deren Daten gespeichert wurden, und insbesondere die Erstellung eines Profils der betroffenen Person bzw.

der betroffenen Personen ermöglichen, das im Hinblick auf das Recht auf Achtung des Privatlebens eine ebenso sensible Information darstellt wie der Inhalt der Kommunikationen selbst.

88 Folglich ist 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, 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 (vgl. zum Zugang zu solchen Daten 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).

89 Insoweit können selbst die Speicherung einer begrenzten Menge von Verkehrs- oder Standortdaten oder die Speicherung dieser Daten über einen kurzen Zeitraum geeignet sein, sehr genaue Informationen über das Privatleben des Nutzers eines elektronischen Kommunikationsmittels zu liefern. Außerdem können die Menge der verfügbaren Daten und die daraus resultierenden sehr genauen Informationen über das Privatleben des Betroffenen erst nach Konsultation der fraglichen Daten beurteilt werden. Der sich aus der Speicherung der genannten Daten ergebende Eingriff erfolgt aber notwendigerweise, bevor die Daten und die daraus resultierenden Informationen konsultiert werden können. Somit erfolgt die Beurteilung der Schwere des in der Speicherung bestehenden Eingriffs notwendigerweise anhand der mit der Kategorie gespeicherter Daten allgemein verbundenen Gefahr für das Privatleben der Betroffenen, ohne dass es überdies darauf ankommt, ob die daraus resultierenden Informationen über das Privatleben im konkreten Fall sensiblen Charakter haben (vgl. in diesem Sinne Urteil vom 2. März 2021, Prokuratuur [Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation], C-746/18, EU:C:2021:152, Rn. 40).

90 Im vorliegenden Fall kann, wie aus Rn. 77 des vorliegenden Urteils hervorgeht und in der mündlichen Verhandlung bestätigt worden ist, ein Satz von Verkehrs- und Standortdaten, die zehn Wochen bzw. vier Wochen lang gespeichert werden, sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten gespeichert wurden – 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 –, und insbesondere die Erstellung eines Profils dieser Personen ermöglichen.

91 Drittens ist in Bezug auf die in der in den Ausgangsverfahren in Rede stehenden nationalen Regelung vorgesehenen Garantien, die die gespeicherten Daten gegen Missbrauchsrisiken und vor jedem unberechtigten Zugang schützen sollen, festzustellen, dass die Vorratsspeicherung dieser Daten und der Zugang zu ihnen, wie sich aus der in Rn. 60 des vorliegenden Urteils angeführten Rechtsprechung ergibt, unterschiedliche Eingriffe in die in den Art. 7 und 11 der Charta garantierten Grundrechte darstellen, die eine gesonderte Rechtfertigung nach Art. 52 Abs. 1 der Charta erfordern. Daraus folgt, dass 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 ergeben, naturgemäß den schwerwiegenden Eingriff weder beschränken noch beseitigen können, der sich aus der nach diesen nationalen Rechtsvorschriften vorgesehenen allgemeinen Vorratsspeicherung dieser Daten in die Rechte ergeben würde, die in den Art. 5 und 6 dieser

Richtlinie und in den durch diese Vorschriften konkretisierten Grundrechten garantiert werden (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 47).

92 Viertens und letztens hat der Gerichtshof, was das Vorbringen der Europäischen Kommission anbelangt, wonach besonders schwere Kriminalität einer Bedrohung der nationalen Sicherheit gleichgestellt werden könne, bereits entschieden, 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 Bevölkerung oder den Staat als solchen unmittelbar zu bedrohen, wie etwa terroristische Aktivitäten (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 61 und die dort angeführte Rechtsprechung).

93 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 (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 62 und die dort angeführte Rechtsprechung).

94 Somit kann Kriminalität – auch besonders schwere Kriminalität – nicht mit einer Bedrohung der nationalen Sicherheit gleichgesetzt werden. Eine solche Gleichstellung könnte nämlich eine Zwischenkategorie zwischen der nationalen Sicherheit und der öffentlichen Sicherheit einführen, um auf die zweite Kategorie die Voraussetzungen der ersten Kategorie anzuwenden (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 63).

Zu den Maßnahmen, die eine gezielte Vorratsspeicherung, eine umgehende Sicherung oder eine Speicherung der IP-Adressen vorsehen

95 Mehrere Regierungen, darunter die französische Regierung, betonen, dass nur eine allgemeine und unterschiedslose Vorratsspeicherung die wirksame Verwirklichung der mit den Speicherungsmaßnahmen verfolgten Ziele ermögliche; die deutsche Regierung führt im Wesentlichen aus, dass diese Schlussfolgerung nicht dadurch entkräftet werde, dass die Mitgliedstaaten auf die in Rn. 75 des vorliegenden Urteils genannten Maßnahmen der gezielten Vorratsspeicherung und umgehenden Sicherung zurückgreifen könnten.

96 Hierzu ist erstens festzustellen, dass die Wirksamkeit der Strafverfolgung im Allgemeinen nicht von einem einzigen Ermittlungsinstrument abhängt, sondern von allen Ermittlungsinstrumenten, über die die zuständigen nationalen Behörden zu diesem Zweck verfügen (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 69).

97 Zweitens gestattet Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta in seiner Auslegung durch die in Rn. 75 des vorliegenden Urteils angeführte Rechtsprechung es den Mitgliedstaaten, zur Bekämpfung schwerer Kriminalität und

zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit nicht nur Rechtsvorschriften zur Einführung einer gezielten Vorratsspeicherung und einer umgehenden Sicherung zu erlassen, sondern auch Rechtsvorschriften, die eine allgemeine und unterschiedslose Vorratsspeicherung von zum einen der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten und zum anderen der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, vorsehen (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 70).

98 Insoweit steht fest, dass die Vorratsspeicherung der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten zur Bekämpfung schwerer Kriminalität beitragen kann, sofern diese Daten es ermöglichen, die Personen zu identifizieren, die solche Kommunikationsmittel im Zusammenhang mit der Vorbereitung oder Begehung einer zur schweren Kriminalität zählenden Tat verwendet haben (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 71).

99 Die Richtlinie 2002/58 steht aber einer allgemeinen Vorratsspeicherung der die Identität betreffenden Daten für die Zwecke der Bekämpfung der Kriminalität im Allgemeinen nicht entgegen. Unter diesen Umständen ist klarzustellen, dass weder diese Richtlinie noch irgendein anderer Unionsrechtsakt nationalen Rechtsvorschriften entgegenstehen, die die Bekämpfung schwerer Kriminalität zum Gegenstand haben und nach denen der Erwerb eines elektronischen Kommunikationsmittels wie einer vorausbezahlten SIM-Karte von der Überprüfung amtlicher Dokumente, die die Identität des Käufers belegen, und der Erfassung der sich daraus ergebenden Informationen durch den Verkäufer abhängig ist, wobei der Verkäufer gegebenenfalls verpflichtet ist, den zuständigen nationalen Behörden Zugang zu diesen Informationen zu gewähren (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 72).

100 Außerdem ist darauf hinzuweisen, dass die allgemeine Speicherung der IP-Adressen der Quelle der Verbindung einen schweren Eingriff in die in den Art. 7 und 8 der Charta verankerten Grundrechte darstellt, da diese IP-Adressen es ermöglichen können, genaue Schlüsse auf das Privatleben des Nutzers des betreffenden elektronischen Kommunikationsmittels zu ziehen, und abschreckende Wirkung in Bezug auf die Ausübung der in Art. 11 der Charta garantierten Freiheit der Meinungsäußerung haben kann. Allerdings hat der Gerichtshof in Bezug auf eine solche Speicherung festgestellt, dass, um die widerstreitenden Rechte und berechtigten Interessen miteinander in Einklang zu bringen, wie es die in den Rn. 65 bis 68 des vorliegenden Urteils angeführte Rechtsprechung verlangt, zu berücksichtigen ist, dass im Fall einer im Internet begangenen Straftat und insbesondere im Fall des Erwerbs, der Verbreitung, der Weitergabe oder der Bereitstellung im Internet von Kinderpornografie im Sinne von Art. 2 Buchst. c der Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates (ABl. 2011, L 335, S. 1, berichtigt in ABl. 2012, L 18, S. 7) die IP-Adresse der einzige Anhaltspunkt sein kann, der es ermöglicht, die Identität der Person zu ermitteln, der diese Adresse zugewiesen war, als die Tat begangen wurde (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 73).

101 Unter diesen Umständen trifft es zwar zu, dass eine Rechtsvorschrift, die eine Vorratsspeicherung der IP-Adressen aller natürlichen Personen vorsieht, denen ein Endgerät gehört, von dem aus ein Internetzugang möglich ist, Personen erfassen würde, die *prima facie* keinen Zusammenhang mit den verfolgten Zielen im Sinne der in Rn. 70 des vorliegenden Urteils angeführten Rechtsprechung aufweisen, und dass die Internetnutzer nach der Feststellung in Rn. 54 des

vorliegenden Urteils aufgrund der Art. 7 und 8 der Charta erwarten dürfen, dass ihre Identität grundsätzlich nicht preisgegeben wird. Gleichwohl verstößt eine Rechtsvorschrift, die eine allgemeine und unterschiedslose Vorratsspeicherung allein der IP-Adressen der Quelle einer Verbindung vorsieht, grundsätzlich nicht gegen Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta, sofern diese Möglichkeit von der strikten Einhaltung der materiellen und prozeduralen Voraussetzungen abhängig gemacht wird, die die Nutzung dieser Daten regeln müssen (Urteil vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 155).

102 Angesichts der Schwere des mit dieser Vorratsdatenspeicherung verbundenen Eingriffs in die Grundrechte, die in den Art. 7 und 8 der Charta verankert sind, sind neben dem Schutz der nationalen Sicherheit nur die Bekämpfung schwerer Kriminalität und die Verhütung schwerer Bedrohungen der öffentlichen Sicherheit geeignet, diesen Eingriff zu rechtfertigen. Außerdem darf die Dauer der Speicherung das im Hinblick auf das verfolgte Ziel absolut Notwendige nicht überschreiten. Schließlich muss eine derartige Maßnahme strenge Voraussetzungen und Garantien hinsichtlich der Auswertung dieser Daten, insbesondere in Form einer Nachverfolgung, in Bezug auf die Online-Kommunikationen und -Aktivitäten der Betroffenen vorsehen (Urteil vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 156).

103 Entgegen den Ausführungen des vorlegenden Gerichts besteht somit kein Spannungsverhältnis zwischen den Rn. 155 und 168 des Urteils vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791). Wie der Generalanwalt in den Nrn. 81 und 82 seiner Schlussanträge im Kern ausgeführt hat, geht nämlich aus dieser Rn. 155 in Verbindung mit Rn. 156 und Rn. 168 dieses Urteils klar hervor, dass neben dem Schutz der nationalen Sicherheit nur die Bekämpfung schwerer Kriminalität und die Verhütung schwerer Bedrohungen der öffentlichen Sicherheit geeignet sind, die allgemeine Vorratsspeicherung der der Quelle einer Verbindung zugewiesenen IP-Adressen zu rechtfertigen, unabhängig davon, ob die betroffenen Personen einen zumindest mittelbaren Zusammenhang mit den verfolgten Zielen aufweisen.

104 Was drittens die Rechtsvorschriften betrifft, die eine gezielte Vorratsspeicherung und eine umgehende Sicherung der Verkehrs- und Standortdaten vorsehen, lassen bestimmte, von den Mitgliedstaaten in Bezug auf solche Maßnahmen dargelegte Erwägungen ein engeres Verständnis der Tragweite dieser Vorschriften erkennen als das, das der in Rn. 75 des vorliegenden Urteils angeführten Rechtsprechung zugrunde liegt. Denn auch wenn diese Maßnahmen der Speicherung, wie in Rn. 57 des vorliegenden Urteils ausgeführt worden ist, in dem durch die Richtlinie 2002/58 geschaffenen System Ausnahmecharakter haben müssen, so macht diese Richtlinie im Licht der in den Art. 7, 8 und 11 sowie in Art. 52 Abs. 1 der Charta verankerten Grundrechte die Möglichkeit, eine Anordnung zur gezielten Vorratsspeicherung zu erlassen, gleichwohl nicht von den Voraussetzungen abhängig, dass im Voraus bekannt ist, an welchen Orten eine schwere Straftat begangen werden könnte oder welche Personen verdächtigt werden, an einer solchen Tat beteiligt zu sein. Ebenso wenig verlangt die Richtlinie, dass die Anordnung, mit der eine umgehende Sicherung angeordnet wird, auf Verdächtige beschränkt wird, die vor einer solchen Anordnung identifiziert wurden (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 75).

105 Was erstens die gezielte Vorratsspeicherung anbelangt, so hat der Gerichtshof entschieden, dass Art. 15 Abs. 1 der Richtlinie 2002/58 auf objektiven Kriterien beruhenden nationalen Rechtsvorschriften nicht entgegensteht, mit denen zum einen Personen erfasst werden können,

deren Verkehrs- und Standortdaten geeignet sind, einen zumindest mittelbaren Zusammenhang mit schweren Straftaten zu offenbaren, zur Bekämpfung schwerer Kriminalität beizutragen oder eine schwerwiegende Gefahr für die öffentliche Sicherheit oder eine Gefahr für die nationale Sicherheit zu verhüten (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 76 und die dort angeführte Rechtsprechung).

106 Der Gerichtshof hat insoweit klargestellt, dass diese objektiven Kriterien zwar je nach den zur Verhütung, Ermittlung, Feststellung und Verfolgung schwerer Straftaten getroffenen Maßnahmen unterschiedlich sein können, zu den erfassten Personen aber insbesondere diejenigen gehören können, die zuvor im Rahmen der einschlägigen nationalen Verfahren und auf der Grundlage objektiver und nicht diskriminierender Kriterien als Bedrohung der öffentlichen Sicherheit oder der nationalen Sicherheit des betreffenden Mitgliedstaats eingestuft wurden (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 77).

107 Die Mitgliedstaaten haben somit u. a. die Möglichkeit, Maßnahmen zur Speicherung zu ergreifen, die Personen betreffen, die aufgrund einer solchen Einstufung Gegenstand aktueller Ermittlungen oder anderer Überwachungsmaßnahmen sind oder zu denen im nationalen Strafregister eine frühere Verurteilung wegen schwerer Straftaten vermerkt ist, die ein hohes Rückfallrisiko bedeuten können. Beruht eine solche Einstufung aber auf objektiven und nicht diskriminierenden Kriterien, die im nationalen Recht festgelegt sind, so ist die gezielte Vorratsspeicherung in Bezug auf so eingestufte Personen gerechtfertigt (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 78).

108 Zum anderen kann eine Maßnahme gezielter Vorratsspeicherung von Verkehrs- und Standortdaten nach Wahl des nationalen Gesetzgebers und unter strikter Beachtung des Grundsatzes der Verhältnismäßigkeit auch auf ein geografisches Kriterium gestützt werden, wenn die zuständigen nationalen Behörden aufgrund objektiver und nicht diskriminierender Anhaltspunkte davon ausgehen, dass in einem oder mehreren geografischen Gebieten eine durch ein erhöhtes Risiko der Vorbereitung oder Begehung schwerer Straftaten gekennzeichnete Situation besteht. Dabei kann es sich insbesondere um Orte handeln, die durch eine erhöhte Zahl schwerer Straftaten gekennzeichnet sind, um Orte, an denen die Gefahr, dass schwere Straftaten begangen werden, besonders hoch ist, wie Orte oder Infrastrukturen, die regelmäßig von einer sehr hohen Zahl von Personen aufgesucht werden, oder um strategische Orte wie Flughäfen, Seehäfen, Bahnhöfe oder Mautstellen (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 79 und die dort angeführte Rechtsprechung).

109 Es ist hervorzuheben, dass nach dieser Rechtsprechung die zuständigen nationalen Behörden für die in der vorstehenden Randnummer genannten Gebiete eine Maßnahme der gezielten Vorratsspeicherung auf der Grundlage eines geografischen Kriteriums wie u. a. der durchschnittlichen Kriminalitätsrate in einem geografischen Gebiet treffen können, ohne dass sie zwingend über konkrete Anhaltspunkte für die Vorbereitung oder die Begehung schwerer Straftaten in den betreffenden Gebieten verfügen müssten. Da eine gezielte Vorratsspeicherung, die auf einem solchen Kriterium beruht, je nach den betreffenden schweren Straftaten und der den jeweiligen Mitgliedstaaten eigenen Situation sowohl Orte betreffen kann, die durch eine erhöhte Zahl schwerer Straftaten gekennzeichnet sind, als auch Orte, die für die Begehung solcher Straftaten besonders anfällig sind, kann sie grundsätzlich auch nicht zu Diskriminierungen führen, da das Kriterium der durchschnittlichen Rate schwerer Straftaten als solches keine Verbindung zu potenziell diskriminierenden Elementen aufweist (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 80).

110 Außerdem und vor allem ermöglicht eine gezielte Vorratsspeicherung in Bezug auf Orte oder Infrastrukturen, die regelmäßig von einer sehr großen Zahl von Personen frequentiert werden, oder auf strategische Orte wie Flughäfen, Bahnhöfe, Seehäfen oder Mautstellen den zuständigen Behörden, Verkehrsdaten und insbesondere Standortdaten aller Personen zu sammeln, die zu einem bestimmten Zeitpunkt an einem dieser Orte ein elektronisches Kommunikationsmittel benutzen. Eine solche Maßnahme der gezielten Vorratsspeicherung kann es diesen Behörden somit ermöglichen, durch den Zugang zu den so gespeicherten Daten Informationen über die Anwesenheit dieser Personen an den Orten oder in den geografischen Gebieten, auf die sich diese Maßnahme bezieht, sowie über ihre Bewegungen zwischen oder innerhalb dieser Orte oder geografischen Gebiete zu erhalten und daraus zum Zweck der Bekämpfung schwerer Kriminalität Schlüsse über ihre Anwesenheit und ihre Tätigkeit an diesen Orten oder in diesen geografischen Gebieten zu einem bestimmten Zeitpunkt während des Speicherungszeitraums zu ziehen (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 81).

111 Ferner ist darauf hinzuweisen, dass die geografischen Gebiete, auf die sich eine solche gezielte Vorratsspeicherung bezieht, geändert werden können und gegebenenfalls müssen, wenn sich die Bedingungen, die ihre Auswahl gerechtfertigt haben, ändern, so dass insbesondere auf die Entwicklungen bei der Bekämpfung schwerer Kriminalität reagiert werden kann. Der Gerichtshof hat nämlich bereits entschieden, dass die Dauer der in den Rn. 105 bis 110 des vorliegenden Urteils beschriebenen Maßnahmen gezielter Speicherung das im Hinblick auf das verfolgte Ziel sowie die sie rechtfertigenden Umstände absolut Notwendige nicht überschreiten darf, unbeschadet einer etwaigen Verlängerung wegen des fortbestehenden Erfordernisses einer solchen Speicherung (Urteile vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 151, sowie vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 82).

112 Was die Möglichkeit betrifft, andere Unterscheidungskriterien als ein persönliches oder geografisches Kriterium für die Durchführung einer gezielten Vorratsspeicherung von Verkehrs- und Standortdaten vorzusehen, so kann nicht ausgeschlossen werden, dass andere objektive und nicht diskriminierende Kriterien in Betracht kommen, um sicherzustellen, dass der Umfang einer gezielten Vorratsspeicherung auf das absolut Notwendige beschränkt wird, und um eine zumindest indirekte Verbindung zwischen den schweren Straftaten und den Personen, deren Daten auf Vorrat gespeichert werden, herzustellen. Da sich Art. 15 Abs. 1 der Richtlinie 2002/58 auf Rechtsvorschriften der Mitgliedstaaten bezieht, obliegt es allerdings diesen und nicht dem Gerichtshof, solche Kriterien zu bestimmen, wobei es nicht darum gehen kann, auf diesem Weg wieder eine allgemeine und unterschiedslose Vorratsspeicherung der Verkehrs- und Standortdaten einzuführen (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 83).

113 Wie der Generalanwalt in Nr. 50 seiner Schlussanträge ausgeführt hat, kann jedenfalls das etwaige Bestehen von Schwierigkeiten bei der genauen Bestimmung der Fälle und Bedingungen, in bzw. unter denen eine gezielte Vorratsspeicherung durchgeführt werden kann, nicht rechtfertigen, dass Mitgliedstaaten, indem sie die Ausnahme zur Regel machen, eine allgemeine und unterschiedslose Speicherung von Verkehrs- und Standortdaten vorsehen (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 84).

114 Was zweitens die umgehende Sicherung der von den Betreibern elektronischer Kommunikationsdienste auf der Grundlage der Art. 5, 6 und 9 der Richtlinie 2002/58 oder auf der Grundlage von Rechtsvorschriften, die gemäß Art. 15 Abs. 1 dieser Richtlinie erlassen wurden, verarbeiteten und gespeicherten Verkehrs- und Standortdaten anbelangt, ist darauf

hinzuweisen, dass solche Daten grundsätzlich nach Ablauf der gesetzlichen Fristen, innerhalb deren sie gemäß den nationalen Bestimmungen zur Umsetzung der Richtlinie verarbeitet und gespeichert werden müssen, je nach Fall, entweder gelöscht oder anonymisiert werden müssen. Allerdings hat der Gerichtshof entschieden, dass während dieser Verarbeitung und Speicherung Situationen auftreten können, die es erforderlich machen, die betreffenden Daten zur Aufklärung schwerer Straftaten oder von Beeinträchtigungen der nationalen Sicherheit über diese Fristen hinaus zu speichern, und zwar sowohl dann, wenn die Taten oder Beeinträchtigungen bereits festgestellt werden konnten, als auch dann, wenn nach einer objektiven Prüfung aller relevanten Umstände der begründete Verdacht besteht, dass sie vorliegen (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 85).

115 In einer solchen Situation steht es den Mitgliedstaaten angesichts dessen, dass nach den Ausführungen in den Rn. 65 bis 68 des vorliegenden Urteils die widerstreitenden Rechte und berechtigten Interessen miteinander in Einklang gebracht werden müssen, frei, in Rechtsvorschriften, die sie gemäß Art. 15 Abs. 1 der Richtlinie 2002/58 erlassen, vorzusehen, dass den Betreibern elektronischer Kommunikationsdienste mittels einer Entscheidung der zuständigen Behörde, die einer wirksamen gerichtlichen Kontrolle unterliegt, aufgegeben wird, für einen festgelegten Zeitraum die ihnen zur Verfügung stehenden Verkehrs- und Standortdaten umgehend zu sichern (Urteile vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 163, sowie vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 86).

116 Da die Zielsetzung einer solchen umgehenden Sicherung nicht mehr den Zielsetzungen entspricht, aufgrund deren die Daten ursprünglich gesammelt und gespeichert wurden, und da nach Art. 8 Abs. 2 der Charta jede Datenverarbeitung für festgelegte Zwecke zu erfolgen hat, müssen die Mitgliedstaaten in ihren Rechtsvorschriften angeben, mit welcher Zielsetzung die umgehende Sicherung der Daten vorgenommen werden kann. Angesichts der Schwere des Eingriffs in die in den Art. 7 und 8 der Charta verankerten Grundrechte, der mit einer solchen Speicherung verbunden sein kann, sind nur die Bekämpfung schwerer Kriminalität und, *a fortiori*, der Schutz der nationalen Sicherheit geeignet, diesen Eingriff zu rechtfertigen, sofern diese Maßnahme sowie der Zugang zu den auf Vorrat gespeicherten Daten die Grenzen des absolut Notwendigen, wie sie in den Rn. 164 bis 167 des Urteils vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791), dargelegt sind, einhalten (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 87).

117 Der Gerichtshof hat klargestellt, dass sich eine derartige Maßnahme der Vorratsspeicherung nicht auf die Daten der Personen beschränken muss, die zuvor als Bedrohung für die öffentliche oder nationale Sicherheit des betreffenden Mitgliedstaats identifiziert wurden, oder von Personen, die konkret im Verdacht stehen, eine schwere Straftat begangen oder die nationale Sicherheit beeinträchtigt zu haben. Nach Auffassung des Gerichtshofs kann nämlich unter Beachtung des durch Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta vorgegebenen Rahmens und angesichts der Erwägungen in Rn. 70 des vorliegenden Urteils eine solche Maßnahme nach Wahl des nationalen Gesetzgebers, unter Einhaltung der Grenzen des absolut Notwendigen, auf die Verkehrs- und Standortdaten anderer als der Personen erstreckt werden, die im Verdacht stehen, eine schwere Straftat oder eine Beeinträchtigung der nationalen Sicherheit geplant oder begangen zu haben, sofern diese Daten auf der Grundlage objektiver und nicht diskriminierender Kriterien zur Aufdeckung einer solchen Straftat oder einer solchen Beeinträchtigung der nationalen Sicherheit beitragen können. Dazu gehören die Daten des Opfers sowie seines sozialen oder beruflichen Umfelds (Urteile vom

6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 165, sowie vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 88).

118 Somit kann eine Rechtsvorschrift es gestatten, gegenüber den Betreibern elektronischer Kommunikationsdienste anzuordnen, die Verkehrs- und Standortdaten u. a. von Personen, mit denen ein Opfer vor dem Auftreten einer schweren Bedrohung der öffentlichen Sicherheit oder der Begehung einer schweren Straftat unter Verwendung seiner elektronischen Kommunikationsmittel in Kontakt gestanden hat, umgehend zu sichern (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 89).

119 Eine solche umgehende Sicherung kann nach der in Rn. 117 des vorliegenden Urteils angeführten Rechtsprechung des Gerichtshofs unter den in dieser Randnummer genannten Voraussetzungen auch auf bestimmte geografische Gebiete wie die Orte der Begehung und Vorbereitung der Straftat oder der betreffenden Beeinträchtigung der nationalen Sicherheit ausgedehnt werden. Es ist klarzustellen, dass Gegenstand einer solchen Maßnahme auch die Verkehrs- und Standortdaten sein können, die sich auf den Ort beziehen, an dem eine Person, die möglicherweise Opfer einer schweren Straftat ist, verschwunden ist, sofern diese Maßnahme sowie der Zugang zu den auf diese Weise auf Vorrat gespeicherten Daten die Grenzen des für die Bekämpfung schwerer Straftaten oder den Schutz der nationalen Sicherheit absolut Notwendigen, wie sie in den Rn. 164 bis 167 des Urteils vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791), dargelegt sind, einhalten (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 90).

120 Außerdem ist klarzustellen, dass Art. 15 Abs. 1 der Richtlinie 2002/58 die zuständigen nationalen Behörden nicht daran hindert, bereits im ersten Stadium der Ermittlungen bezüglich einer schweren Bedrohung der öffentlichen Sicherheit oder einer möglichen schweren Straftat, d. h. ab dem Zeitpunkt, zu dem diese Behörden nach den einschlägigen Bestimmungen des nationalen Rechts solche Ermittlungen einleiten können, eine umgehende Sicherung anzuordnen (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 91).

121 Was des Weiteren die Vielfalt der in Rn. 75 des vorliegenden Urteils genannten Maßnahmen der Vorratsspeicherung der Verkehrs- und Standortdaten betrifft, ist klarzustellen, dass diese verschiedenen Maßnahmen nach der Wahl des nationalen Gesetzgebers und unter Einhaltung der Grenzen des absolut Notwendigen zusammen Anwendung finden können. Unter diesen Umständen steht Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta in der Auslegung durch die auf das Urteil vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791), zurückgehende Rechtsprechung einer Kombination dieser Maßnahmen nicht entgegen (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 92).

122 Viertens und letztens ist darauf hinzuweisen, dass, wie sich aus dem die ständige Rechtsprechung des Gerichtshofs zusammenfassenden Urteil vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791), ergibt, die Verhältnismäßigkeit der nach Art. 15 Abs. 1 der Richtlinie 2002/58 getroffenen Maßnahmen die Einhaltung nicht nur der Erfordernisse der Geeignetheit und der Erforderlichkeit verlangt, sondern auch des Erfordernisses, dass diese Maßnahmen in einem angemessenen Verhältnis zum verfolgten Ziel stehen müssen (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 93).

123 In diesem Zusammenhang ist darauf hinzuweisen, dass der Gerichtshof in Rn. 51 des Urteils vom 8. April 2014, Digital Rights Ireland u. a. (C-293/12 und C-594/12, EU:C:2014:238), entschieden hat, dass zwar die Bekämpfung schwerer Kriminalität von größter Bedeutung für die Gewährleistung der öffentlichen Sicherheit ist und dass ihre Wirksamkeit in hohem Maß von der Nutzung moderner Ermittlungstechniken abhängen kann; eine solche dem Gemeinwohl dienende Zielsetzung kann aber, so grundlegend sie auch sein mag, für sich genommen die Erforderlichkeit einer Maßnahme der allgemeinen und unterschiedslosen Vorratsspeicherung von Verkehrs- und Standortdaten – wie sie die Richtlinie 2006/24 vorsieht – nicht rechtfertigen (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 94).

124 Im selben Sinne hat der Gerichtshof in Rn. 145 des Urteils vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791), klargestellt, dass selbst die positiven Verpflichtungen der Mitgliedstaaten – die sich, je nach Fall, aus den Art. 3, 4 und 7 der Charta ergeben können und, wie in Rn. 64 des vorliegenden Urteils ausgeführt worden ist, die Schaffung von Regeln für eine wirksame Bekämpfung von Straftaten betreffen – keine so schwerwiegenden Eingriffe rechtfertigen können, wie sie mit nationalen Rechtsvorschriften, die eine Speicherung von Verkehrs- und Standortdaten vorsehen, für die in den Art. 7 und 8 der Charta verankerten Grundrechte fast der gesamten Bevölkerung verbunden sind, ohne dass die Daten der Betroffenen einen zumindest mittelbaren Zusammenhang mit dem verfolgten Ziel aufweisen (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 95).

125 Im Übrigen sind die Urteile des EGMR vom 25. Mai 2021, Big Brother Watch u. a./Vereinigtes Königreich (CE:ECHR:2021:0525JUD005817013), und vom 25. Mai 2021, Centrum för Rättvisa/Schweden (CE:ECHR:2021:0525JUD003525208), die von einigen Regierungen in der mündlichen Verhandlung angeführt worden sind, um geltend zu machen, dass die EMRK nationalen Regelungen, die im Wesentlichen eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsähen, nicht entgegenstehe, nicht geeignet, die Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58, die sich aus den vorstehenden Ausführungen ergibt, in Frage zu stellen. In diesen Urteilen ging es nämlich um das massenhafte Abfangen von Daten betreffend internationale Kommunikationen. Somit hat der Europäische Gerichtshof für Menschenrechte, wie die Kommission in der mündlichen Verhandlung ausgeführt hat, in den genannten Urteilen weder über die Vereinbarkeit einer allgemeinen und unterschiedslosen Vorratsspeicherung von Verkehrs- und Standortdaten im Inland noch auch nur über ein Abfangen dieser Daten in großem Umfang zur Verhütung, Feststellung und Ermittlung schwerer Straftaten mit der EMRK entschieden. Jedenfalls ist darauf hinzuweisen, dass mit Art. 52 Abs. 3 der Charta die notwendige Kohärenz zwischen den in der Charta enthaltenen Rechten und den entsprechenden durch die EMRK garantierten Rechten gewährleistet werden soll, ohne dass dadurch die Eigenständigkeit des Unionsrechts und des Gerichtshofs der Europäischen Union berührt wird, so dass die entsprechenden Rechte der EMRK bei der Auslegung der Charta nur als Mindestschutzstandard zu berücksichtigen sind (Urteil vom 17. Dezember 2020, Centraal Israëlitisch Consistorie van België u. a., C-336/19, EU:C:2020:1031, Rn. 56).

Zum Zugang zu Daten, die allgemein und unterschiedslos auf Vorrat gespeichert wurden

126 In der mündlichen Verhandlung hat die dänische Regierung vorgebracht, dass die zuständigen nationalen Behörden zum Zweck der Bekämpfung schwerer Kriminalität Zugang zu Verkehrs- und Standortdaten haben müssten, die gemäß der aus dem Urteil vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 135 bis 139),

hervorgegangenen Rechtsprechung allgemein und unterschiedslos auf Vorrat gespeichert worden seien, um einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit zu begegnen.

127 Zunächst ist festzustellen, dass die Gestattung des Zugangs zu allgemein und unterschiedslos auf Vorrat gespeicherten Verkehrs- und Standortdaten zum Zweck der Bekämpfung schwerer Kriminalität diesen Zugang von Umständen abhängig machen würde, die mit diesem Ziel nichts zu tun haben – je nachdem, ob in dem betreffenden Mitgliedstaat eine ernste Bedrohung für die nationale Sicherheit im Sinne der vorstehenden Randnummer besteht oder nicht –, während im Hinblick auf das alleinige Ziel der Bekämpfung schwerer Kriminalität, das die Speicherung dieser Daten und den Zugang zu ihnen rechtfertigen soll, nichts eine unterschiedliche Behandlung insbesondere zwischen den Mitgliedstaaten rechtfertigen würde (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 97).

128 Wie der Gerichtshof bereits entschieden hat, kann der Zugang zu von Betreibern elektronischer Kommunikationsdienste in Anwendung einer gemäß Art. 15 Abs. 1 der Richtlinie 2002/58 erlassenen Rechtsvorschrift auf Vorrat gespeicherten Verkehrs- und Standortdaten, der unter vollständiger Beachtung der sich aus der Rechtsprechung zur Auslegung dieser Richtlinie ergebenden Voraussetzungen zu erfolgen hat, grundsätzlich nur mit dem dem Gemeinwohl dienenden Ziel gerechtfertigt werden, zu dem die Speicherung den Betreibern auferlegt wurde. Etwas anderes gilt nur, wenn die Bedeutung des mit dem Zugang verfolgten Ziels die Bedeutung des Ziels, das die Speicherung gerechtfertigt hat, übersteigt (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 98).

129 Das Vorbringen der dänischen Regierung bezieht sich aber auf eine Situation, in der das Ziel des beabsichtigten Zugangsersuchens, nämlich die Bekämpfung schwerer Kriminalität, in der Hierarchie der dem Gemeinwohl dienenden Ziele von geringerer Bedeutung ist als das Ziel, das die Speicherung rechtfertigte, nämlich der Schutz der nationalen Sicherheit. In einer solchen Situation Zugang zu den auf Vorrat gespeicherten Daten zu gewähren, würde gegen die Hierarchie der dem Gemeinwohl dienenden Ziele verstoßen, auf die in der vorstehenden Randnummer sowie in den Rn. 68, 71, 72 und 73 dieses Urteils hingewiesen worden ist (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 99).

130 Außerdem und vor allem dürfen nach der in Rn. 74 des vorliegenden Urteils angeführten Rechtsprechung Verkehrs- und Standortdaten für die Zwecke der Bekämpfung schwerer Kriminalität nicht allgemein und unterschiedslos auf Vorrat gespeichert werden, so dass auch der Zugang zu diesen Daten zu diesen Zwecken nicht gerechtfertigt sein kann. Wenn diese Daten ausnahmsweise allgemein und unterschiedslos zum Schutz der nationalen Sicherheit vor einer Bedrohung, die als real und aktuell oder vorhersehbar einzustufen ist, unter den in Rn. 71 des vorliegenden Urteils genannten Voraussetzungen gespeichert wurden, dürfen die für strafrechtliche Ermittlungen zuständigen nationalen Behörden im Rahmen der Strafverfolgung nicht auf diese Daten zugreifen, da sonst das in Rn. 74 genannte Verbot einer solchen Speicherung zum Zweck der Bekämpfung schwerer Straftaten seine praktische Wirksamkeit verlieren würde (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 100).

131 Nach alledem ist auf die Vorlagefrage zu antworten, 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 dahin auszulegen ist, 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. Dagegen ist der genannte Art. 15 Abs. 1 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta dahin auszulegen, dass 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 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 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.

Kosten

132 Für die Beteiligten der Ausgangsverfahren ist das Verfahren Teil der bei dem vorlegenden Gericht anhängigen Verfahren; die Kostenentscheidung ist daher Sache dieses Gerichts. Die Auslagen anderer Beteiligter für die Abgabe von Erklärungen vor dem Gerichtshof sind nicht erstattungsfähig.

Aus diesen Gründen hat der Gerichtshof (Große Kammer) für Recht erkannt:

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 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 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.

Lenaerts	Arabadjiev	Prechal
Rodin	Jarukaitis	Ziemele
von Danwitz	Safjan	Biltgen
Xuereb	Piçarra	Rossi
	Kumin	

Verkündet in öffentlicher Sitzung in Luxemburg am 20. September 2022.

Der Kanzler	Der Präsident
A. Calot Escobar	K. Lenaerts