Sammlung der Rechtsprechung

URTEIL DES GERICHTSHOFS (Große Kammer)

5. April 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 – Zugang zu auf Vorrat gespeicherten Daten – Nachträgliche gerichtliche Kontrolle – Richtlinie 2002/58/EG – Art. 15 Abs. 1 – Charta der Grundrechte der Europäischen Union – Art. 7, 8 und 11 sowie Art. 52 Abs. 1 – Möglichkeit für ein nationales Gericht, die zeitliche Wirkung einer Ungültigerklärung nationaler Rechtsvorschriften, die mit dem Unionsrecht unvereinbar sind, zu beschränken – Nichteinbeziehung“

In der Rechtssache C-140/20

betreffend ein Vorabentscheidungsersuchen nach Art. 267 AEUV, eingereicht vom Supreme Court (Oberster Gerichtshof, Irland) mit Entscheidung vom 25. März 2020, beim Gerichtshof eingegangen am selben Tag, in dem Verfahren

G. D.

gegen

Commissioner of An Garda Síochána,

Minister for Communications, Energy and Natural Resources,

Attorney General

erlässt

DER GERICHTSHOF (Große Kammer)

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

Generalanwalt: M. Campos Sánchez-Bordona,

Kanzler: D. Dittert, Referatsleiter,

* Verfahrenssprache: Englisch.

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

unter Berücksichtigung der Erklärungen

– von G. D., vertreten durch J. Dunphy, Solicitor, R. Kennedy und R. Farrell, SC, sowie K. McCormack, BL,

– des Commissioner of An Garda Síochána, des Minister for Communications, Energy and Natural Resources und des Attorney General, vertreten durch M. Browne, S. Purcell, C. Stone, J. Quaney und A. Joyce als Bevollmächtigte im Beistand von S. Guerin und P. Gallagher, SC, sowie von D. Fennelly und L. Dwyer, BL,

– der belgischen Regierung, vertreten durch P. Cottin und J.-C. Halleux als Bevollmächtigte im Beistand von J. Vanpraet, Advocaat,

– der tschechischen Regierung, vertreten durch M. Smolek, O. Serdula und J. Vláčil als Bevollmächtigte,

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

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

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

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

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

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

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

– der portugiesischen Regierung, vertreten durch L. Inez Fernandes, P. Barros da Costa und I. Oliveira als Bevollmächtigte,

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

– der schwedischen Regierung, vertreten durch O. Simonsson, J. Lundberg, H. Shev, C. Meyer-Seitz, A. Runeskjöld, M. Salborn Hodgson, R. Shahsavan Eriksson und H. Eklinder als Bevollmächtigte,

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

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

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

folgendes

Urteil

1 Das Vorabentscheidungsersuchen betrifft 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. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta).

2 Dieses Ersuchen ergeht im Rahmen eines Rechtsstreits zwischen G. D. auf der einen sowie dem Commissioner of An Garda Síochána (Leiter der Nationalpolizei, Irland), dem Minister for Communications, Energy and Natural Resources (Minister für Kommunikation, Energie und natürliche Ressourcen, Irland) und dem Attorney General auf der anderen Seite betreffend die Gültigkeit des Communications (Retention of Data) Act 2011 (Gesetz von 2011 über die Kommunikation [Vorratsdatenspeicherung], im Folgenden: Gesetz von 2011).

Rechtlicher Rahmen

Unionsrecht

3 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/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)] gilt auch die vorliegende Richtlinie nicht für Fragen des Schutzes der Grundrechte und Grundfreiheiten in Bereichen, die nicht unter das [Unionsrecht] 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.“

4 Art. 1 („Geltungsbereich und Zielsetzung“) der Richtlinie 2002/58 lautet:

„(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 [Europäischen Union] 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 Vertrags über die Europäische Union, 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.“

5 In Art. 2 („Begriffsbestimmungen“) der Richtlinie 2002/58 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;

…“

6 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 [Union], einschließlich öffentlicher Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte unterstützen.“

7 In Art. 5 („Vertraulichkeit der Kommunikation“) der Richtlinie 2002/58 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."

8 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.

…"

9 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. …“

10 Art. 15 („Anwendung einzelner Bestimmungen der Richtlinie [95/46]“) der Richtlinie 2002/58 sieht in Abs. 1 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 [Unionsrechts] einschließlich den in Artikel 6 Absätze 1 und 2 des Vertrags über die Europäische Union niedergelegten Grundsätzen entsprechen.“

Irisches Recht

11 Wie aus dem Vorabentscheidungsersuchen hervorgeht, wurde das Gesetz von 2011 erlassen, um 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) in irisches Recht umzusetzen.

12 Section 1 des Gesetzes von 2011 definiert den Begriff „Daten“ als „Verkehrs- oder Standortdaten und die damit in Zusammenhang stehenden Daten, die zur Feststellung des Teilnehmers oder Nutzers erforderlich sind“, und den Begriff „schwere Straftat“ als eine Straftat, die mit einer Freiheitsstrafe von mindestens fünf Jahren bedroht ist, oder eine der anderen in Anhang 1 dieses Gesetzes aufgeführten Straftaten.

13 Nach Section 3 Abs. 1 des genannten Gesetzes sind alle Betreiber elektronischer Kommunikationsdienste verpflichtet, die in Anhang 2 Teil 1 dieses Gesetzes genannten Daten für die Dauer von zwei Jahren und die in Anhang 2 Teil 2 des Gesetzes genannten Daten für die Dauer eines Jahres auf Vorrat zu speichern.

14 In Anhang 2 Teil 1 des Gesetzes werden u. a. Daten betreffend Festnetztelefonie und Mobilfunk genannt, mit denen die Quelle und der Adressat einer Nachricht identifiziert, Tag und Uhrzeit des Beginns und des Endes einer Nachricht bestimmt, die Art der betreffenden Kommunikation bestimmt sowie Art und geografische Lage des verwendeten Kommunikationsmaterials identifiziert werden können. Insbesondere sieht Anhang 2 Teil 1 Nr. 6 die Vorratsspeicherung der Daten vor, die erforderlich sind, um ein mobiles elektronisches Kommunikationsmittel zu lokalisieren. Bei diesen Daten handelt es sich zum einen um die Cell-ID und zum anderen um

Daten zur geografischen Ortung von Funkzellen durch Bezugnahme auf ihre Standortkennung (Cell-ID) während des Zeitraums, in dem die Vorratsspeicherung der Kommunikationsdaten erfolgt.

15 Anhang 2 Teil 2 des Gesetzes von 2011 bezieht sich auf Daten betreffend den Internetzugang, E-Mail und Internettelefonie und erfasst u. a. die Benutzerkennungen und die Telefonnummern, die IP-Adressen sowie den Tag und die Uhrzeit des Beginns und des Endes einer Kommunikation. Der Inhalt der Kommunikation fällt nicht unter diese Art von Daten.

16 Nach den Sections 4 und 5 des Gesetzes von 2011 haben die Betreiber elektronischer Kommunikationsdienste bestimmte Maßnahmen zu ergreifen, um sicherzustellen, dass die Daten vor unbefugten Zugriffen geschützt sind.

17 Section 6 dieses Gesetzes, die die Voraussetzungen für die Stellung eines Zugangsersuchens regelt, bestimmt in Abs. 1:

„Ein Beamter der Nationalpolizei, der mindestens den Dienstrang eines *chief superintendent* (Hauptkommissar) haben muss, kann einen Diensteanbieter ersuchen, ihm die von diesem Diensteanbieter gespeicherten Daten gemäß Section 3 zu übermitteln, wenn der Beamte die betreffenden Daten für erforderlich hält für:

a) die Verhütung, Feststellung, Ermittlung oder Verfolgung einer schweren Straftat,

b) den Schutz der Sicherheit des Staates,

c) die Rettung von Menschenleben.“

18 Section 7 des Gesetzes von 2011 verpflichtet die Betreiber elektronischer Kommunikationsdienste, den in Section 6 dieses Gesetzes genannten Ersuchen nachzukommen.

19 Zu den Mechanismen zur Kontrolle der Entscheidung des Beamten der Nationalpolizei im Sinne von Section 6 des Gesetzes von 2011 gehören das in Section 10 dieses Gesetzes vorgesehene Beschwerdeverfahren und das Verfahren vor dem *designated judge* (benannter Richter) im Sinne von Section 12 des Gesetzes, der die Anwendung der Bestimmungen des genannten Gesetzes zu prüfen hat.

Ausgangsverfahren und Vorlagefragen

20 Im März 2015 wurde G. D. wegen Mordes an einer Person, die im August 2012 verschwunden war und deren Leiche erst im September 2013 entdeckt worden war, zu einer lebenslangen Freiheitsstrafe verurteilt. In der Berufung gegen seine Verurteilung warf der Betroffene dem erstinstanzlichen Gericht u. a. vor, es habe zu Unrecht Verkehrs- und Standortdaten im Zusammenhang mit Telefonanrufen als Beweismittel zugelassen, da das Gesetz von 2011, das die Speicherung dieser Daten regele und auf dessen Grundlage die Ermittler der Nationalpolizei Zugang zu diesen Daten gehabt hätten, seine Rechte aus dem Unionsrecht verletze. Diese Berufung ist derzeit anhängig.

21 Um im Rahmen des Strafverfahrens die Zulässigkeit dieser Beweise in Abrede stellen zu können, leitete G. D. beim High Court (Hoher Gerichtshof, Irland) ein Zivilverfahren mit dem Ziel ein, die Ungültigkeit bestimmter Vorschriften des Gesetzes von 2011 feststellen zu lassen. Mit Entscheidung vom 6. Dezember 2018 gab dieses Gericht dem Vorbringen von G. D. statt und stellte fest, dass Section 6 Abs. 1 Buchst. a dieses Gesetzes mit Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und Art. 52 Abs. 1 der Charta unvereinbar sei. Irland legte gegen diese Entscheidung ein Rechtsmittel beim Supreme Court (Oberster Gerichtshof, Irland), dem vorlegenden Gericht, ein.

22 Das beim Court of Appeal (Berufungsgericht, Irland) anhängige Strafverfahren wurde bis zur Verkündung der Entscheidung des vorlegenden Gerichts im Zivilverfahren ausgesetzt.

23 Vor dem vorlegenden Gericht machte Irland geltend, dass für die Feststellung, ob der Eingriff in das in Art. 7 der Charta verankerte Recht auf Achtung des Privatlebens, der sich aus der Speicherung von Verkehrs- und Standortdaten gemäß dem Gesetz von 2011 ergebe, verhältnismäßig sei, die Ziele der durch dieses Gesetz eingeführten Regelung in ihrer Gesamtheit geprüft werden müssten. Außerdem habe dieses Gesetz einen detaillierten Rahmen für den Zugang zu auf Vorrat gespeicherten Daten geschaffen, wonach die Stelle, die innerhalb der Nationalpolizei mit der vorherigen Prüfung von Zugangsersuchen betraut sei, bei der Wahrnehmung ihrer Aufgaben von der Nationalpolizei funktional unabhängig sei und damit dem Erfordernis einer vorherigen Kontrolle durch eine unabhängige Verwaltungsstelle genüge. Dieses Kontrollsystem werde durch ein Beschwerdeverfahren und eine gerichtliche Kontrolle ergänzt. Schließlich dürfe, sollte das Gesetz von 2011 letztlich als unionsrechtswidrig angesehen werden, jede Feststellung, die daraus vom vorlegenden Gericht abgeleitet werde, unter dem Gesichtspunkt ihrer zeitlichen Wirkungen nur für die Zukunft gelten.

24 G. D. machte seinerseits geltend, dass die durch das Gesetz von 2011 eingeführte Regelung der allgemeinen und unterschiedslosen Vorratsspeicherung von Daten sowie die in diesem Gesetz vorgesehene Regelung über den Zugang zu diesen Daten mit dem Unionsrecht, wie es insbesondere vom Gerichtshof in Rn. 120 des Urteils vom 21. Dezember 2016, Tele2 Sverige und Watson u. a. (C-203/15 und C-698/15, EU:C:2016:970), ausgelegt worden sei, unvereinbar seien.

25 Das vorlegende Gericht stellt zunächst klar, dass es nur zu beurteilen habe, ob der High Court (Hoher Gerichtshof) zu Recht entschieden habe, dass Section 6 Abs. 1 Buchst. a des Gesetzes von 2011 mit dem Unionsrecht unvereinbar sei, die Frage der Zulässigkeit der im Rahmen des Strafverfahrens erhobenen Beweise hingegen in die alleinige Zuständigkeit des Court of Appeal (Berufungsgericht) falle, bei dem die gegen die Verurteilung eingelegte Berufung anhängig sei.

26 In diesem Zusammenhang fragt sich das vorlegende Gericht zunächst nach den Anforderungen des Unionsrechts hinsichtlich der Vorratsdatenspeicherung zum Zweck der Bekämpfung schwerer Kriminalität. Hierzu vertritt es im Wesentlichen die Auffassung, dass nur eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten eine wirksame Bekämpfung schwerer Kriminalität ermögliche, was bei einer gezielten Vorratsspeicherung und einer umgehenden Sicherung (*quick freeze*) nicht möglich sei. Hinsichtlich der gezielten Vorratsspeicherung fragt sich das vorlegende Gericht, ob für die Zwecke der Bekämpfung schwerer Kriminalität bestimmte Gruppen oder geografische Gebiete erfasst werden können, da bestimmte schwere Straftaten selten mit Umständen verbunden seien, die den zuständigen nationalen Behörden bekannt seien und die es ihnen ermöglichen würden, die Begehung einer Straftat im Voraus zu vermuten. Außerdem könne eine gezielte

Vorratsspeicherung zu Diskriminierungen führen. Was die umgehende Sicherung betrifft, so ist das vorlegende Gericht der Ansicht, dass diese nur in Situationen sinnvoll sei, in denen es in einem frühen Stadium der Ermittlungen einen identifizierbaren Verdächtigen gebe.

27 Was sodann den Zugang zu den von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten Daten betrifft, weist das vorlegende Gericht darauf hin, dass die Nationalpolizei bei sich ein System der Selbstzertifizierung der an diese Betreiber gerichteten Zugangsersuchen eingeführt habe. Aus den dem High Court (Hoher Gerichtshof) vorgelegten Unterlagen gehe hervor, dass der Leiter der Nationalpolizei als interne Maßnahme entschieden habe, dass Zugangsersuchen, die nach dem Gesetz von 2011 gestellt würden, von einem einzigen Beamten der Nationalpolizei zentral bearbeitet werden müssten, der die Eigenschaft eines *chief superintendent* (Hauptkommissar) habe, nämlich dem Leiter der Abteilung Sicherheit und Aufklärung. Wenn dieser der Ansicht sei, dass die betreffenden Daten u. a. zur Verhütung, Ermittlung, Feststellung oder Verfolgung einer schweren Straftat erforderlich seien, könne er ein Zugangsersuchen an die Betreiber elektronischer Kommunikationsdienste richten. Im Übrigen habe der Leiter der Nationalpolizei bei dieser eine selbständige Einheit namens *Telecommunications Liaison Unit* (Koordinationsstelle für Telekommunikation, im Folgenden: TLU) eingerichtet, um den Leiter der Abteilung Sicherheit und Aufklärung bei der Ausübung seiner Aufgaben zu unterstützen und als einzige Stelle für den Kontakt zu eben diesen Diensteanbietern zu dienen.

28 Das vorlegende Gericht führt weiter aus, dass während des Zeitraums, auf den sich die gegen G. D. eingeleitete strafrechtliche Untersuchung beziehe, alle Zugangsersuchen zunächst von einem Oberkommissar oder einem die Aufgaben eines Oberkommissars wahrnehmenden Kommissar hätten genehmigt werden müssen, bevor sie zur Bearbeitung an die TLU weitergeleitet worden seien, und dass die Ermittler angewiesen gewesen seien, ihre Zugangsersuchen mit ausreichend detaillierten Informationen zu versehen, um eine fundierte Entscheidung zu ermöglichen. Außerdem seien die TLU und der Leiter der Abteilung Sicherheit und Aufklärung verpflichtet gewesen, die Rechtmäßigkeit, die Erforderlichkeit und die Verhältnismäßigkeit der Zugangsersuchen zu prüfen, wobei zu berücksichtigen sei, dass dieser Leiter habe aufgefordert werden können, seine Entscheidung vor einem vom High Court (Hoher Gerichtshof) benannten Richter zu rechtfertigen. Die TLU unterliege außerdem der Prüfung durch den Data Protection Commissioner (Datenschutzbeauftragter, Irland).

29 Schließlich fragt das vorlegende Gericht nach der Tragweite und den zeitlichen Wirkungen einer etwaigen Feststellung der Unvereinbarkeit des Gesetzes von 2011 mit dem Unionsrecht. Eine solche Feststellung könne nur für die Zukunft gelten, da die im Strafverfahren gegen G. D. als Beweise verwendeten Daten Ende 2013 gespeichert und zugänglich gemacht worden seien, d. h. zu einer Zeit, als Irland verpflichtet gewesen sei, die Bestimmungen des Gesetzes von 2011, mit dem die Richtlinie 2006/24 umgesetzt worden sei, anzuwenden. Eine solche Lösung sei auch insoweit angemessen, als andernfalls die Ermittlung und Verfolgung schwerer Straftaten in Irland sowie die Situation bereits verurteilter Personen ernsthaft beeinträchtigt sein könnten.

30 Unter diesen Umständen hat der Supreme Court (Oberster Gerichtshof) beschlossen, das Verfahren auszusetzen und dem Gerichtshof folgende Fragen zur Vorabentscheidung vorzulegen:

1. Verstößt eine allgemeine/universelle Regelung über die Vorratsdatenspeicherung – auch wenn die Speicherung und der Zugang strengen Beschränkungen unterliegen – *per se* gegen Art. 15 der Richtlinie 2002/58, ausgelegt im Licht der Charta?

2. Darf ein nationales Gericht bei der Prüfung der Frage, ob eine gemäß der Richtlinie 2006/24 umgesetzte nationale Maßnahme, die eine allgemeine Regelung für die Vorratsspeicherung von Daten vorsieht (mit den notwendigen strengen Kontrollen in Bezug auf die Vorratsspeicherung und/oder den Zugang), für mit dem Unionsrecht unvereinbar zu erklären ist, und insbesondere bei der Beurteilung der Verhältnismäßigkeit einer solchen Regelung berücksichtigen, dass Diensteanbieter Daten für ihre eigenen kommerziellen Zwecke rechtmäßig auf Vorrat speichern dürfen und aus Gründen der nationalen Sicherheit, die nicht unter die Richtlinie 2002/58 fallen, möglicherweise auf Vorrat speichern müssen?

3. Welche Kriterien muss ein nationales Gericht bei der Beurteilung der Vereinbarkeit einer nationalen Regelung über den Zugang zu auf Vorrat gespeicherten Daten mit dem Unionsrecht und insbesondere mit den in der Charta verankerten Rechten anwenden, wenn es prüft, ob eine solche Zugangsregelung die erforderliche unabhängige vorherige Kontrolle, wie sie der Gerichtshof in seiner Rechtsprechung festgelegt hat, vorsieht? Kann ein nationales Gericht in diesem Zusammenhang bei einer solchen Beurteilung das Vorhandensein einer nachträglichen gerichtlichen oder unabhängigen Kontrolle berücksichtigen?

4. Ist jedenfalls ein nationales Gericht verpflichtet, die Unvereinbarkeit einer nationalen Maßnahme mit Art. 15 der Richtlinie 2002/58 festzustellen, wenn die nationale Maßnahme eine allgemeine Regelung für die Vorratsspeicherung von Daten zum Zwecke der Bekämpfung schwerer Straftaten vorsieht und das nationale Gericht anhand aller verfügbaren Beweise zu dem Schluss gelangt ist, dass eine solche Vorratsspeicherung für die Erreichung des Ziels der Bekämpfung schwerer Straftaten sowohl wesentlich als auch zwingend erforderlich ist?

5. Wenn ein nationales Gericht feststellen muss, dass eine nationale Maßnahme mit Art. 15 der Richtlinie 2002/58, ausgelegt im Licht der Charta, unvereinbar ist, darf es dann die zeitliche Wirkung einer solchen Feststellung beschränken, wenn es sich davon überzeugt hat, dass es andernfalls zu „daraus resultierendem Chaos und einer Schädigung des öffentlichen Interesses“ käme (im Einklang mit dem Ansatz, der etwa im Urteil R [National Council for Civil Liberties] v Secretary of State for Home Department und Secretary of State for Foreign Affairs [2018] EWHC 975, Rn. 46, verfolgt wurde)?

6. Darf ein nationales Gericht, bei dem im Rahmen eines Verfahrens, das eingeleitet wurde, um Argumente zur Frage der Zulässigkeit von Beweisen in einem Strafverfahren zu stützen, oder in einem anderen Zusammenhang beantragt wird, die Unvereinbarkeit nationaler Rechtsvorschriften mit Art. 15 der Richtlinie 2002/58 festzustellen und/oder diese Rechtsvorschriften unangewendet zu lassen und/oder festzustellen, dass die Rechte eines Einzelnen durch die Anwendung dieser Rechtsvorschriften verletzt wurden, einen solchen Antrag in Bezug auf Daten zurückweisen, die gemäß der nationalen Bestimmung, die aufgrund der Verpflichtung nach Art. 288 AEUV zur getreuen Umsetzung der Bestimmungen einer Richtlinie in nationales Recht erlassen wurde, auf Vorrat gespeichert wurden, oder die Wirkung einer solchen Feststellung auf die Zeit nach der Ungültigerklärung der Richtlinie 2006/24 durch das Urteil vom 8. April 2014, Digital Rights Ireland u. a. (C-293/12 und C-594/12, EU:C:2014:238), beschränken?

Zu den Vorlagefragen

Zu den Fragen 1, 2 und 4

31 Mit seinen Fragen 1, 2 und 4, die zusammen zu prüfen sind, möchte das vorlegende Gericht wissen, ob Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. l der Charta dahin auszulegen ist, dass er nationalen Rechtsvorschriften entgegensteht, die eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten zu Zwecken der Bekämpfung schwerer Kriminalität vorsehen.

32 Zunächst ist darauf hinzuweisen, dass nach ständiger Rechtsprechung bei der Auslegung einer unionsrechtlichen Vorschrift nicht nur ihr Wortlaut zu berücksichtigen ist, sondern auch ihr Kontext und die Ziele, die mit der Regelung, zu der sie gehört, verfolgt werden, und insbesondere deren Entstehungsgeschichte (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. 105 und die dort angeführte Rechtsprechung).

33 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“.

34 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.

35 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 (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. 107).

36 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 Art. 7 und 8 der Charta niedergelegten Rechte zu gewährleisten (vgl. in diesem Sinne Urteile vom 21. Dezember 2016, Tele2 Sverige und Watson u. a., C-203/15 und C-698/15, EU:C:2016:970, Rn. 83, sowie 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. 106).

37 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 (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. 109).

38 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.

39 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.

40 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. 35 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 (vgl. in diesem Sinne Urteile vom 21. Dezember 2016, Tele2 Sverige und Watson u. a., C-203/15 und C-698/15, EU:C:2016:970, Rn. 89, sowie 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. 111).

41 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 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 112 und die dort angeführte Rechtsprechung).

42 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 die Achtung des Privatlebens und den Schutz personenbezogener Daten garantierenden Art. 7 und 8 der Charta betreffen, sondern auch der in Art. 11 der Charta gewährleisteten Freiheit der Meinungsäußerung (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. 113 und die dort angeführte Rechtsprechung).

43 Bei der Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58 muss somit die Bedeutung sowohl des in Art. 7 der Charta gewährleisteten Rechts auf Achtung des Privatlebens als auch des in Art. 8 der Charta gewährleisteten Rechts auf den Schutz personenbezogener Daten, wie sie sich aus der Rechtsprechung des Gerichtshofs ergibt, berücksichtigt werden sowie das in Art. 11 der Charta gewährleistete Grundrecht auf freie Meinungsäußerung, das eine der wesentlichen Grundlagen einer demokratischen und pluralistischen Gesellschaft darstellt, die zu den Werten gehört, auf die sich die Union nach Art. 2 EUV gründet (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. 114 und die dort angeführte Rechtsprechung).

44 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 (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. 115 und 116 sowie die dort angeführte Rechtsprechung).

45 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 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 117 und die dort angeführte Rechtsprechung).

46 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 (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. 118 und 119 sowie die dort angeführte Rechtsprechung).

47 Insoweit ist hervorzuheben, dass die Vorratsspeicherung dieser Daten und der Zugang zu ihnen, wie sich aus der in Rn. 44 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.

48 In Art. 15 Abs. 1 der Richtlinie 2002/58, der es den Mitgliedstaaten gestattet, die in den Rn. 34 bis 37 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 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 120 bis 122 und die dort angeführte Rechtsprechung).

49 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 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 126 und die dort angeführte Rechtsprechung).

50 Angesichts dieser verschiedenen positiven Verpflichtungen müssen die verschiedenen betroffenen berechtigten Interessen und Rechte miteinander in Einklang gebracht werden. Der Europäische Gerichtshof für Menschenrechte hat nämlich entschieden, dass die den Art. 3 und 8 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten zu entnehmenden positiven Verpflichtungen, denen die Garantien in den Art. 4 und 7 der Charta entsprechen, u. a. bedeuten, dass materielle und prozedurale Vorschriften zu erlassen sowie praktische Maßnahmen zu treffen sind, die eine wirksame Bekämpfung von Straftaten gegen Personen mittels effektiver Ermittlungen und Verfolgung gestatten. Diese Verpflichtung ist umso wichtiger, wenn das körperliche und geistige Wohlergehen eines Kindes bedroht ist. Die von den zuständigen Behörden zu treffenden Maßnahmen müssen aber den Rechtsschutzmöglichkeiten und übrigen Garantien, die geeignet sind, den Umfang der strafrechtlichen Ermittlungsbefugnisse zu begrenzen, sowie den sonstigen Freiheiten und Rechten umfassend Rechnung tragen. Insbesondere ist ein rechtlicher Rahmen zu schaffen, der es erlaubt, die verschiedenen zu schützenden berechtigten Interessen und Rechte miteinander in Einklang zu bringen (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. 127 und 128 und die dort angeführte Rechtsprechung).

51 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. 35 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 (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. 129).

52 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 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 130 und die dort angeführte Rechtsprechung).

53 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 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 131 und die dort angeführte Rechtsprechung).

54 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 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 132 und die dort angeführte Rechtsprechung).

55 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. Was konkret die Bekämpfung schwerer Kriminalität betrifft, müssen die Daten, deren Vorratsspeicherung vorgesehen ist, geeignet sein, zur Verhütung, Feststellung oder Verfolgung schwerer Straftaten beizutragen (vgl. in diesem Sinne Urteile vom 8. April 2014, Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 59, sowie 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. 133).

56 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.

57 Insoweit hat der Gerichtshof entschieden, dass die Bedeutung des Ziels des Schutzes der nationalen Sicherheit im Licht von Art. 4 Abs. 2 EUV, wonach der Schutz der nationalen Sicherheit weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten fällt, die der übrigen von Art. 15 Abs. 1 der Richtlinie 2002/58 erfassten Ziele, insbesondere der Ziele, die Kriminalität im Allgemeinen, auch schwere Kriminalität, zu bekämpfen und die öffentliche Sicherheit zu schützen, übersteigt. Vorbehaltlich der Erfüllung der übrigen Anforderungen von Art. 52 Abs. 1 der Charta ist das Ziel des Schutzes der nationalen Sicherheit daher geeignet, Maßnahmen zu rechtfertigen, die schwerere Grundrechtseingriffe enthalten als solche, die mit den übrigen Zielen gerechtfertigt werden könnten (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. 135 und 136).

58 Aus diesem Grund hat der Gerichtshof festgestellt, 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 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 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).

59 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 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 140 und die dort angeführte Rechtsprechung).

60 In der mündlichen Verhandlung hat die Europäische Kommission vorgetragen, dass besonders schwere Kriminalität einer Bedrohung der nationalen Sicherheit gleichgestellt werden könne.

61 Der Gerichtshof hat aber 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 insbesondere terroristische Aktivitäten (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. 135).

62 Außerdem ist festzustellen, dass im Unterschied zur Kriminalität – auch besonders schwerer Kriminalität – eine Bedrohung für die nationale Sicherheit real und aktuell, zumindest aber vorhersehbar sein muss, 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 (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. 136 und 137).

63 Somit kann Kriminalität – auch besonders schwere Kriminalität – nicht mit einer Bedrohung der nationalen Sicherheit gleichgesetzt werden. Wie der Generalanwalt in den Nrn. 49 und 50 seiner Schlussanträge ausgeführt hat, könnte eine solche Gleichstellung nämlich eine Zwischenkategorie zwischen der nationalen Sicherheit und der öffentlichen Sicherheit einführen, um auf die zweite Kategorie die Voraussetzungen der ersten Kategorie anzuwenden.

64 Daraus folgt auch, dass der in der zweiten Vorlagefrage erwähnte Umstand, dass die Verkehrs- und Standortdaten rechtmäßig zum Zweck des Schutzes der nationalen Sicherheit auf Vorrat gespeichert wurden, keinen Einfluss auf die Rechtmäßigkeit ihrer Speicherung zum Zweck der Bekämpfung schwerer Kriminalität hat.

65 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. Aus diesem Grund und angesichts des sensiblen Charakters der Informationen, die sich aus den Verkehrs- und Standortdaten ergeben können, ist deren Vertraulichkeit von entscheidender Bedeutung für das Recht auf Achtung des Privatlebens. In Anbetracht zum einen der in Rn. 46 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 (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. 141 und 142 sowie die dort angeführte Rechtsprechung).

66 Außerdem hat der Gerichtshof betont, dass nationale Rechtsvorschriften, die eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen, die elektronischen Kommunikationen fast der gesamten Bevölkerung erfassen, ohne jede Differenzierung, Einschränkung oder Ausnahme anhand des verfolgten Ziels. Solche Rechtsvorschriften betreffen pauschal sämtliche Personen, die elektronische Kommunikationsdienste nutzen, ohne dass sich diese Personen auch nur mittelbar in einer Lage befinden, die Anlass zur Strafverfolgung geben könnte. Sie gilt somit auch für Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit dem Ziel der Bekämpfung schwerer Straftaten stehen könnte, und setzt insbesondere keinen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit voraus. Insbesondere beschränken solche Rechtsvorschriften, wie der Gerichtshof bereits entschieden hat, die Vorratsspeicherung weder auf die Daten eines Zeitraums und/oder eines geografischen Gebiets und/oder eines Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, noch auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Bekämpfung schwerer Kriminalität beitragen könnten (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. 143 und 144 und die dort angeführte Rechtsprechung).

67 Dagegen hat der Gerichtshof in Rn. 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), 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.

68 Im vorliegenden Vorabentscheidungsersuchen, das vor der Verkündung der 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), und vom 2. März 2021, Prokuratuur (Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation) (C-746/18, EU:C:2021:152), beim Gerichtshof eingegangen ist, hat das vorlegende Gericht jedoch die Auffassung vertreten, dass nur eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten eine wirksame Bekämpfung schwerer Kriminalität ermöglichen würde. In der mündlichen Verhandlung vom 13. September 2021 haben u. a. Irland und die französische Regierung vorgetragen, dass diese Schlussfolgerung nicht dadurch entkräftet werde, dass die Mitgliedstaaten auf die in der vorstehenden Randnummer genannten Maßnahmen zurückgreifen könnten.

69 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.

70 Zweitens ist hervorzuheben, 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 in seiner Auslegung durch die in Rn. 67 des vorliegenden Urteils angeführte Rechtsprechung es den Mitgliedstaaten gestattet, 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.

71 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.

72 Wie sich aus der in Rn. 67 des vorliegenden Urteils zusammenfassend dargestellten Rechtsprechung ergibt, steht die Richtlinie 2002/58 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.

73 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. 50 bis 53 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) 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 (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 und 154).

74 Der Gerichtshof hat daher entschieden, dass eine solche allgemeine und unterschiedslose Vorratsspeicherung allein der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, grundsätzlich nicht gegen Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 der Charta verstößt, sofern diese Möglichkeit von der strikten Einhaltung der in den Rn. 155 und 156 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), genannten materiellen und prozeduralen Voraussetzungen abhängig gemacht wird, die die Nutzung dieser Daten regeln müssen.

75 Was drittens die Rechtsvorschriften betrifft, die eine gezielte Vorratsspeicherung und eine umgehende Sicherung der Verkehrs- und Standortdaten vorsehen, lassen die Angaben im Vorabentscheidungsersuchen ein engeres Verständnis der Tragweite dieser Vorschriften erkennen als das, das der in Rn. 67 des vorliegenden Urteils angeführten Rechtsprechung zugrunde liegt. Denn auch wenn diese Maßnahmen der Speicherung, wie in Rn. 40 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.

76 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 (vgl. in diesem Sinne Urteile vom 21. Dezember 2016, Tele2 Sverige und Watson u. a., C-203/15 und C-698/15, EU:C:2016:970, Rn. 111, sowie 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. 148).

77 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 (vgl. in diesem Sinne Urteile vom 21. Dezember 2016, Tele2 Sverige und Watson u. a., C-203/15 und C-698/15, EU:C:2016:970, Rn. 110, sowie 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. 149).

78 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.

79 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 (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. 150 sowie die dort angeführte Rechtsprechung).

80 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.

81 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.

82 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. 76 bis 81 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 (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. 151).

83 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.

84 Wie Generalanwalt Campos Sánchez-Bordona in Nr. 50 seiner Schlussanträge in den verbundenen Rechtssachen SpaceNet und Telekom Deutschland (C-793/19 und C-794/19, EU:C:2021:939) 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.

85 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 (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. 160 und 161).

86 In einer solchen Situation steht es den Mitgliedstaaten angesichts dessen, dass nach den Ausführungen in den Rn. 50 bis 53 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 (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. 163).

87 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.

88 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. 55 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 (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. 165).

89 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.

90 Eine solche umgehende Sicherung kann nach der in Rn. 88 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.

91 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.

92 Was die Vielfalt der in Rn. 67 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.

93 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.

94 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.

95 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. 49 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.

96 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.

97 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.

98 Wie der Gerichtshof bereits entschieden hat, kann der Zugang zu von Betreibern 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 der Richtlinie 2002/58 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 (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. 165 und 166).

99 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. 53, 56, 57 und 59 dieses Urteils hingewiesen worden ist.

100 Außerdem und vor allem dürfen nach der in Rn. 65 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. 58 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. 65 genannte Verbot einer solchen Speicherung zum Zweck der Bekämpfung schwerer Straftaten seine praktische Wirksamkeit verlieren würde.

101 Nach alledem ist auf die Fragen 1, 2 und 4 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 Rechtsvorschriften entgegensteht, die präventiv zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit eine allgemeine und unterschiedslose Vorratsspeicherung der Verkehrs- und der Standortdaten vorsehen. Dagegen steht der genannte Art. 15 Abs. 1 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta Rechtsvorschriften nicht entgegen, 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.

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.

Zur dritten Frage

102 Mit seiner dritten Frage möchte das vorlegende Gericht wissen, ob Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8, 11 und von Art. 52 Abs. 1 der Charta dahin auszulegen ist, dass er nationalen Rechtsvorschriften entgegensteht, nach denen die zentralisierte Bearbeitung von Ersuchen um Zugang zu auf Vorrat gespeicherten Daten, die von der Polizei im Rahmen der Ermittlung und Verfolgung schwerer Straftaten gestellt werden, einem Polizeibeamten obliegt, der von einer innerhalb der Polizei eingerichteten Einheit, die bei der Wahrnehmung ihrer Aufgaben über einen gewissen Grad an Autonomie verfügt, unterstützt wird und dessen Entscheidungen später gerichtlich überprüft werden können.

103 Zunächst ist darauf hinzuweisen, dass zwar die Voraussetzungen, unter denen die Betreiber elektronischer Kommunikationsdienste den zuständigen nationalen Behörden Zugang zu den Daten gewähren müssen, über die sie verfügen, im nationalen Recht festzulegen sind, nationale Rechtsvorschriften jedoch, um dem Erfordernis der Verhältnismäßigkeit, auf das in Rn. 54 des vorliegenden Urteils hingewiesen worden ist, zu genügen, klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindesterfordernisse aufstellen müssen, damit die Personen, deren personenbezogene Daten betroffen sind, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer Daten vor Missbrauchsrisiken ermöglichen (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. 48 und die dort angeführte Rechtsprechung).

104 Insbesondere dürfen sich nationale Rechtsvorschriften über den Zugang der zuständigen Behörden zu gespeicherten Verkehrs- und Standortdaten, die aufgrund von Art. 15 Abs. 1 der Richtlinie 2002/58 erlassen wurden, nicht darauf beschränken, dass der behördliche Zugang zu den Daten dem mit diesen Rechtsvorschriften verfolgten Zweck zu entsprechen hat, sondern müssen auch die materiellen und prozeduralen Voraussetzungen für die Verwendung der Daten vorsehen (Urteil vom 2. März 2021, Prokuratuur [Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation], C-746/18, EU:C:2021:152, Rn. 49 und die dort angeführte Rechtsprechung).

105 Infolgedessen, und weil ein allgemeiner Zugang zu allen gespeicherten Daten unabhängig davon, ob irgendein – zumindest mittelbarer – Zusammenhang mit dem verfolgten Ziel besteht, nicht als auf das absolut Notwendige beschränkt angesehen werden kann, müssen sich die betreffenden nationalen Rechtsvorschriften bei der Festlegung der Umstände und Voraussetzungen, unter denen den zuständigen nationalen Behörden Zugang zu den fraglichen Daten zu gewähren ist, auf objektive Kriterien stützen. Insoweit darf im Zusammenhang mit dem Ziel, die Kriminalität zu bekämpfen, ein solcher Zugang grundsätzlich nur zu den Daten von Personen gewährt werden, die im Verdacht stehen, eine schwere Straftat zu planen, zu begehen oder begangen zu haben oder auf irgendeine Weise in eine solche Straftat verwickelt zu sein. Allerdings kann in besonderen Situationen wie etwa solchen, in denen vitale Interessen der nationalen Sicherheit, der Landesverteidigung oder der öffentlichen Sicherheit durch terroristische Aktivitäten bedroht sind, auch Zugang zu Daten anderer Personen gewährt werden, wenn es objektive Anhaltspunkte dafür gibt, dass diese Daten in einem konkreten Fall einen wirksamen Beitrag zur Bekämpfung

derartiger Aktivitäten leisten könnten (Urteil vom 2. März 2021, Prokuratuur [Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation], C-746/18, EU:C:2021:152, Rn. 50 und die dort angeführte Rechtsprechung).

106 Um in der Praxis die vollständige Einhaltung dieser Voraussetzungen zu gewährleisten, ist es unabdingbar, dass der Zugang der zuständigen nationalen Behörden zu den gespeicherten Daten einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen wird und dass dessen oder deren Entscheidung auf einen mit Gründen versehenen, von den zuständigen nationalen Behörden insbesondere im Rahmen von Verfahren zur Verhütung, Feststellung oder Verfolgung von Straftaten gestellten Antrag ergeht (Urteil vom 2. März 2021, Prokuratuur [Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation], C-746/18, EU:C:2021:152, Rn. 51 und die dort angeführte Rechtsprechung).

107 Diese vorherige Kontrolle setzt u. a. voraus, dass das mit ihr betraute Gericht oder die mit ihr betraute unabhängige Verwaltungsstelle über alle Befugnisse verfügt und alle Garantien aufweist, die erforderlich sind, um zu gewährleisten, dass die verschiedenen einander gegenüberstehenden berechtigten Interessen und Rechte in Einklang gebracht werden. Im Fall strafrechtlicher Ermittlungen verlangt eine solche Kontrolle, dass dieses Gericht oder diese Stelle in der Lage ist, für einen gerechten Ausgleich zwischen den berechtigten Interessen, die sich aus den Erfordernissen der Ermittlungen im Rahmen der Kriminalitätsbekämpfung ergeben, und den Grundrechten auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten der Personen, auf deren Daten zugegriffen wird, zu sorgen (Urteil vom 2. März 2021, Prokuratuur [Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation], C-746/18, EU:C:2021:152, Rn. 52).

108 Wird die Kontrolle nicht von einem Gericht, sondern von einer unabhängigen Verwaltungsstelle wahrgenommen, muss diese über eine Stellung verfügen, die es ihr erlaubt, bei der Wahrnehmung ihrer Aufgaben objektiv und unparteiisch vorzugehen, ohne jede Einflussnahme von außen. Das Erfordernis, wonach die mit der Wahrnehmung der vorherigen Kontrolle betraute Stelle unabhängig sein muss, gebietet es somit, dass es sich bei ihr um eine andere Stelle als die den Zugang zu den Daten begehrende Behörde handelt, damit diese Stelle in der Lage ist, diese Kontrolle objektiv und unparteiisch, vor jeder Einflussnahme von außen geschützt, auszuüben. Im strafrechtlichen Bereich impliziert das Erfordernis der Unabhängigkeit insbesondere, dass die mit der vorherigen Kontrolle betraute Behörde zum einen nicht an der Durchführung des fraglichen Ermittlungsverfahrens beteiligt ist und zum anderen eine Position der Neutralität gegenüber den Beteiligten am Strafverfahren hat (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. 53 und 54).

109 So hat der Gerichtshof u. a. festgestellt, dass einer Staatsanwaltschaft, die das Ermittlungsverfahren leitet und gegebenenfalls die öffentliche Klage vertritt, nicht die Eigenschaft eines Dritten bezüglich der betreffenden berechtigten Interessen zuerkannt werden kann, da ihre Aufgabe nicht darin besteht, über eine Rechtssache in voller Unabhängigkeit zu entscheiden, sondern darin, sie gegebenenfalls als Beteiligte am Strafprozess dem zuständigen Gericht zu unterbreiten. Folglich ist eine solche Staatsanwaltschaft nicht in der Lage, die vorherige Kontrolle der Ersuchen um Zugang zu den auf Vorrat gespeicherten Daten wahrzunehmen (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. 55 und 57).

110 Schließlich muss die nach Art. 15 Abs. 1 der Richtlinie 2002/58 erforderliche unabhängige Kontrolle vor jedem Zugang zu den betreffenden Daten erfolgen, außer in hinreichend begründeten Eilfällen, in denen die Kontrolle kurzfristig erfolgen muss. Eine spätere Kontrolle würde es nämlich nicht ermöglichen, das Ziel der vorherigen Kontrolle zu erreichen, das darin besteht, zu verhindern, dass ein über das absolut Notwendige hinausgehender Zugang zu den fraglichen Daten genehmigt wird (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. 189, sowie vom 2. März 2021, Prokuratuur [Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation], C-746/18, EU:C:2021:152, Rn. 58).

111 Im vorliegenden Fall geht aus dem Vorabentscheidungsersuchen zunächst hervor, dass das Gesetz von 2011 einem Polizeibeamten, der mindestens den Dienstrang eines *chief superintendent* (Hauptkommissar) haben muss, die Befugnis verleiht, die vorherige Kontrolle bezüglich der Anträge von Ermittlungsdienststellen der Polizei auf Zugang zu Daten auszuüben und die Betreiber elektronischer Kommunikationsdienste um Übermittlung der von ihnen gespeicherten Daten zu ersuchen. Da dieser Beamte in Bezug auf diese Dienststellen nicht die Eigenschaft eines Dritten hat, erfüllt er nicht die in Rn. 108 des vorliegenden Urteils genannten Erfordernisse der Unabhängigkeit und Unparteilichkeit, ungeachtet dessen, dass er bei dieser Aufgabe von einer Polizeieinheit, hier der TLU, unterstützt wird, die bei der Wahrnehmung ihrer Aufgabe über einen gewissen Grad an Autonomie verfügt.

112 Sodann sieht das Gesetz von 2011 zwar Mechanismen zur nachträglichen Kontrolle der Entscheidung des zuständigen Polizeibeamten in Form eines Beschwerdeverfahrens und eines Verfahrens vor einem Richter vor, der mit der Prüfung der Anwendung der Bestimmungen dieses Gesetzes betraut ist, doch geht aus der in Rn. 110 des vorliegenden Urteils angeführten Rechtsprechung hervor, dass eine nachträgliche Kontrolle nicht das in Rn. 106 des vorliegenden Urteils angeführte Erfordernis einer unabhängigen und – mit Ausnahme von hinreichend begründeten Eilfällen – vorherigen Kontrolle ersetzen kann.

113 Schließlich sieht das Gesetz von 2011 keine objektiven Kriterien vor, die genau festlegen würden, unter welchen Voraussetzungen und unter welchen Umständen den nationalen Behörden Zugang zu Daten zu gewähren ist, da, wie Irland in der mündlichen Verhandlung bestätigt hat, allein der mit der Bearbeitung von Ersuchen um Zugang zu den gespeicherten Daten betraute Polizeibeamte dafür zuständig ist, den Verdacht gegen die betroffenen Personen und die Notwendigkeit eines Zugangs zu den sie betreffenden Daten zu beurteilen.

114 Folglich ist auf die dritte Frage zu antworten dass Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8, 11 und von Art. 52 Abs. 1 der Charta dahin auszulegen ist, dass er nationalen Rechtsvorschriften entgegensteht, nach denen die zentralisierte Bearbeitung von Ersuchen um Zugang zu von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten Daten, die von der Polizei im Rahmen der Ermittlung und Verfolgung schwerer Straftaten gestellt werden, einem Polizeibeamten obliegt, der von einer innerhalb der Polizei eingerichteten Einheit, die bei der Wahrnehmung ihrer Aufgaben über einen gewissen Grad an Autonomie verfügt, unterstützt wird und dessen Entscheidungen später gerichtlich überprüft werden können.

Zu den Fragen 5 und 6

115 Mit seinen Fragen 5 und 6, die zusammen zu prüfen sind, möchte das vorlegende Gericht wissen, ob das Unionsrecht dahin auszulegen ist, dass ein nationales Gericht die Wirkungen einer ihm nach nationalem Recht in Bezug auf nationale Rechtsvorschriften, die den Betreibern

elektronischer Kommunikationsdienste eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorschreiben, obliegenden Ungültigerklärung wegen Unvereinbarkeit dieser Rechtsvorschriften mit Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Charta zeitlich begrenzen kann.

116 Aus den vom vorlegenden Gericht erteilten Informationen geht hervor, dass die im Ausgangsverfahren in Rede stehenden nationalen Rechtsvorschriften, nämlich das Gesetz von 2011, erlassen wurden, um die Richtlinie 2006/24 – die der Gerichtshof danach mit Urteil vom 8. April 2014, Digital Rights Ireland u. a. (C-293/12 und C-594/12, EU:C:2014:238), für ungültig erklärt hat – in nationales Recht umzusetzen.

117 Außerdem weist das vorlegende Gericht darauf hin, dass die Prüfung der Zulässigkeit der Beweise, die auf nach dem Gesetz von 2011 gespeicherte Daten gestützt seien und die im Rahmen des Strafverfahrens gegen G. D. geltend gemacht worden seien, zwar Sache des Strafgerichts sei, es im Rahmen des Zivilverfahrens aber seine Aufgabe sei, über die Gültigkeit der in Rede stehenden Bestimmungen dieses Gesetzes und über die zeitlichen Wirkungen einer Feststellung ihrer Ungültigkeit zu entscheiden. Auch wenn die einzige Frage, die sich vor dem vorlegenden Gericht stellt, die nach der Gültigkeit der Bestimmungen des Gesetzes von 2011 ist, hält es dieses Gericht gleichwohl für erforderlich, den Gerichtshof nach den Auswirkungen einer möglichen Feststellung der Ungültigkeit auf die Zulässigkeit von Beweismitteln zu fragen, die durch die allgemeine und unterschiedslose Vorratsspeicherung von Daten, die dieses Gesetz gestattete, gewonnen wurden.

118 Zunächst ist darauf hinzuweisen, dass der Grundsatz des Vorrangs des Unionsrechts besagt, dass das Unionsrecht dem Recht der Mitgliedstaaten vorgeht. Dieser Grundsatz verpflichtet daher alle mitgliedstaatlichen Stellen, den verschiedenen Bestimmungen des Unionsrechts volle Wirksamkeit zu verschaffen, wobei das Recht der Mitgliedstaaten die diesen Bestimmungen zuerkannte Wirkung im Hoheitsgebiet dieser Staaten nicht beeinträchtigen darf. Nach diesem Grundsatz ist ein nationales Gericht, das im Rahmen seiner Zuständigkeit die Bestimmungen des Unionsrechts anzuwenden hat und nationale Rechtsvorschriften nicht im Einklang mit den Anforderungen des Unionsrechts auslegen kann, verpflichtet, für die volle Wirksamkeit dieser Bestimmungen Sorge zu tragen, indem es erforderlichenfalls jede – auch spätere – entgegenstehende Bestimmung des nationalen Rechts aus eigener Entscheidungsbefugnis unangewendet lässt, ohne dass es die vorherige Beseitigung dieser Bestimmung auf gesetzgeberischem Weg oder durch irgendein anderes verfassungsrechtliches Verfahren beantragen oder abwarten müsste (vgl. in diesem Sinne Urteile vom 15. Juli 1964, Costa, 6/64, EU:C:1964:66, S. 1270 und 1271, vom 19. November 2019, A. K. u. a. [Unabhängigkeit der Disziplinarkammer des Obersten Gerichts], C-585/18, C-624/18 und C-625/18, EU:C:2019:982, Rn. 157, 158 und 160, sowie 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. 214 und 215).

119 Nur der Gerichtshof kann in Ausnahmefällen und aus zwingenden Erwägungen der Rechtssicherheit eine vorübergehende Aussetzung der Verdrängungswirkung herbeiführen, die eine unionsrechtliche Vorschrift gegenüber mit ihr unvereinbarem nationalem Recht ausübt. Eine solche zeitliche Beschränkung der Wirkungen einer Auslegung des Unionsrechts durch den Gerichtshof kann nur in dem Urteil vorgenommen werden, in dem über die begehrte Auslegung entschieden wird. Der Vorrang und die einheitliche Anwendung des Unionsrechts würden beeinträchtigt, wenn nationale Gerichte befugt wären, nationalen Bestimmungen, sei es auch nur

vorübergehend, Vorrang vor dem Unionsrecht einzuräumen, gegen das sie verstoßen (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. 216 und 217 und die dort angeführte Rechtsprechung).

120 Zwar hat der Gerichtshof in einer Rechtssache betreffend die Rechtmäßigkeit von Maßnahmen, die unter Verstoß gegen die durch das Unionsrecht auferlegte Pflicht zur Durchführung einer vorherigen Prüfung der Umweltverträglichkeit eines Projekts und seiner Verträglichkeit mit einem geschützten Gebiet ergangen waren, entschieden, dass ein nationales Gericht, wenn das innerstaatliche Recht es gestattet, die Wirkungen solcher Maßnahmen ausnahmsweise aufrechterhalten kann, sofern dies durch zwingende Erwägungen gerechtfertigt ist, die im Zusammenhang mit der Notwendigkeit stehen, die tatsächliche und schwerwiegende Gefahr einer Unterbrechung der Stromversorgung im betreffenden Mitgliedstaat abzuwenden, der nicht mit anderen Mitteln und Alternativen, insbesondere im Rahmen des Binnenmarkts, entgegengetreten werden kann. Ihre Aufrechterhaltung darf aber nur für den Zeitraum gelten, der absolut notwendig ist, um die Rechtswidrigkeit zu beseitigen (Urteil vom 29. Juli 2019, Inter-Environnement Wallonie und Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, Rn. 175, 176, 179 und 181).

121 Jedoch kann im Gegensatz zu dem Versäumnis, einer prozeduralen Pflicht wie der vorherigen Prüfung der Auswirkungen eines Projekts, die sich in den speziellen Bereich des Umweltschutzes einfügt, nachzukommen, ein Verstoß 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 nicht durch ein Verfahren wie das in der vorstehenden Randnummer erwähnte geheilt werden (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. 219).

122 Würden die Wirkungen nationaler Rechtsvorschriften wie des Gesetzes von 2011 aufrechterhalten, würde dies nämlich bedeuten, dass durch die betreffenden Rechtsvorschriften den Betreibern elektronischer Kommunikationsdienste weiterhin Verpflichtungen auferlegt würden, die gegen das Unionsrecht verstoßen und mit schwerwiegenden Eingriffen in die Grundrechte der Personen verbunden sind, deren Daten gespeichert wurden (vgl. entsprechend 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. 219).

123 Das vorlegende Gericht darf somit die ihm nach nationalem Recht obliegende Feststellung der Ungültigkeit der im Ausgangsverfahren in Rede stehenden nationalen Rechtsvorschriften nicht in ihren zeitlichen Wirkungen beschränken (vgl. entsprechend 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. 220).

124 Insoweit ist, wie der Generalanwalt in Nr. 75 seiner Schlussanträge im Kern ausgeführt hat, der Umstand, dass diese nationalen Rechtsvorschriften erlassen wurden, um die Richtlinie 2006/24 in nationales Recht umzusetzen, unerheblich, da das vorlegende Gericht wegen der Ungültigerklärung dieser Richtlinie durch den Gerichtshof, die auf den Zeitpunkt des Inkrafttretens der Richtlinie zurückwirkt (vgl. in diesem Sinne Urteil vom 8. Februar 1996, FMC u. a., C-212/94, EU:C:1996:40, Rn. 55), die Gültigkeit dieser nationalen Rechtsvorschriften im Licht der Richtlinie 2002/58 und der Charta in ihrer Auslegung durch den Gerichtshof zu beurteilen hat.

125 Was insbesondere die Auslegung der Richtlinie 2002/58 und der Charta durch den Gerichtshof u. a. in den Urteilen vom 21. Dezember 2016, Tele2 Sverige und Watson u. a. (C-203/15 und C-698/15, EU:C:2016:970), und vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791), anbelangt, ist darauf hinzuweisen, dass nach ständiger Rechtsprechung durch die Auslegung einer Vorschrift des Unionsrechts, die der Gerichtshof in Ausübung seiner Befugnisse aus Art. 267 AEUV vornimmt, erläutert und verdeutlicht wird, in welchem Sinne und mit welcher Tragweite die Vorschrift seit ihrem Inkrafttreten zu verstehen und anzuwenden ist oder gewesen wäre. Daraus folgt, dass die Gerichte die Vorschrift in dieser Auslegung auch auf Rechtsverhältnisse anwenden können und müssen, die vor dem Erlass des auf das Ersuchen um Auslegung ergangenen Urteils entstanden sind, wenn alle sonstigen Voraussetzungen für die Anrufung der zuständigen Gerichte in einem die Anwendung der Vorschrift betreffenden Streit vorliegen (Urteil vom 16. September 2020, Romenergo und Aris Capital, C-339/19, EU:C:2020:709, Rn. 47 und die dort angeführte Rechtsprechung).

126 Insoweit ist außerdem klarzustellen, dass in den Urteilen vom 21. Dezember 2016, Tele2 Sverige und Watson u. a. (C-203/15 und C-698/15, EU:C:2016:970), und vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791), die Wirkungen der vorgenommenen Auslegung nicht zeitlich begrenzt wurden, so dass nach der in Rn. 119 des vorliegenden Urteils angeführten Rechtsprechung eine solche Begrenzung nicht in einem nach diesen Urteilen ergangenen Urteil des Gerichtshofs erfolgen kann.

127 Was schließlich die Auswirkungen der Feststellung einer etwaigen Unvereinbarkeit des Gesetzes von 2011 mit der Richtlinie 2002/58 im Licht der Charta auf die Zulässigkeit der gegen G. D. im Rahmen des Strafverfahrens vorgebrachten Beweise anbelangt, genügt es, auf die diesbezügliche Rechtsprechung des Gerichtshofs zu verweisen, insbesondere auf die in den Rn. 41 bis 44 des Urteils vom 2. März 2021, Prokuratuur (Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation) (C-746/18, EU:C:2021:152), angeführten Grundsätze, aus denen sich ergibt, dass diese Zulässigkeit gemäß dem Grundsatz der Verfahrensautonomie der Mitgliedstaaten vorbehaltlich der Beachtung u. a. der Grundsätze der Äquivalenz und der Effektivität dem nationalen Recht unterliegt.

128 Nach alledem ist auf die Fragen 5 und 6 zu antworten, dass das Unionsrecht dahin auszulegen ist, dass es dem entgegensteht, dass ein nationales Gericht die Wirkungen einer ihm nach nationalem Recht in Bezug auf nationale Rechtsvorschriften, die den Betreibern elektronischer Kommunikationsdienste eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorschreiben, obliegenden Ungültigerklärung wegen Unvereinbarkeit dieser Rechtsvorschriften mit Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Charta zeitlich begrenzt. Die Zulässigkeit der durch eine solche Vorratsspeicherung erlangten Beweismittel unterliegt nach dem Grundsatz der Verfahrensautonomie der Mitgliedstaaten vorbehaltlich der Beachtung u. a. der Grundsätze der Äquivalenz und der Effektivität dem nationalen Recht.

Kosten

129 Für die Beteiligten des Ausgangsverfahrens ist das Verfahren Teil des beim vorlegenden Gericht anhängigen Verfahrens; 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:

1. **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 Rechtsvorschriften entgegensteht, die präventiv zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit eine allgemeine und unterschiedslose Vorratsspeicherung der Verkehrs- und der Standortdaten vorsehen. Dagegen steht der genannte Art. 15 Abs. 1 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta der Grundrechte Rechtsvorschriften nicht entgegen, 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.**

   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.

2. **Art. 15 Abs. 1 der Richtlinie 2002/58 in der durch die Richtlinie 2009/136 geänderten Fassung ist im Licht der Art. 7, 8, 11 und von Art. 52 Abs. 1 der Charta der Grundrechte dahin auszulegen, dass er nationalen Rechtsvorschriften entgegensteht, nach denen die zentralisierte Bearbeitung von Ersuchen um Zugang zu von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten Daten, die von der Polizei im Rahmen der Ermittlung und Verfolgung schwerer Straftaten gestellt werden, einem Polizeibeamten obliegt, der von einer innerhalb der Polizei eingerichteten Einheit, die bei der Wahrnehmung ihrer Aufgaben über einen gewissen Grad an Autonomie verfügt, unterstützt wird und dessen Entscheidungen später gerichtlich überprüft werden können.**

3. Das Unionsrecht ist dahin auszulegen, dass es dem entgegensteht, dass ein nationales Gericht die Wirkungen einer ihm nach nationalem Recht in Bezug auf nationale Rechtsvorschriften, die den Betreibern elektronischer Kommunikationsdienste eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorschreiben, obliegenden Ungültigerklärung wegen Unvereinbarkeit dieser Rechtsvorschriften mit Art. 15 Abs. 1 der Richtlinie 2002/58 in der durch die Richtlinie 2009/136 geänderten Fassung im Licht der Charta der Grundrechte zeitlich begrenzt. Die Zulässigkeit der durch eine solche Vorratsspeicherung erlangten Beweismittel unterliegt nach dem Grundsatz der Verfahrensautonomie der Mitgliedstaaten vorbehaltlich der Beachtung u. a. der Grundsätze der Äquivalenz und der Effektivität dem nationalen Recht.

Unterschriften