Sammlung der Rechtsprechung

URTEIL DES GERICHTSHOFS (Große Kammer)

6. Oktober 2020*

„Vorlage zur Vorabentscheidung – Verarbeitung personenbezogener Daten in der elektronischen Kommunikation – Betreiber elektronischer Kommunikationsdienste – Allgemeine und unterschiedslose Übermittlung von Verkehrs- und Standortdaten – Schutz der nationalen Sicherheit – Richtlinie 2002/58/EG – Geltungsbereich – Art. 1 Abs. 3 und Art. 3 – Vertraulichkeit elektronischer Kommunikation – Schutz – Art. 5 und Art. 15 Abs. 1 – Charta der Grundrechte der Europäischen Union – Art. 7, 8 und 11 sowie Art. 52 Abs. 1 – Art. 4 Abs. 2 EUV“

In der Rechtssache C-623/17

betreffend ein Vorabentscheidungsersuchen nach Art. 267 AEUV, eingereicht vom Investigatory Powers Tribunal (Gericht für Ermittlungsbefugnisse, Vereinigtes Königreich) mit Entscheidung vom 18. Oktober 2017, beim Gerichtshof eingegangen am 31. Oktober 2017, in dem Verfahren

Privacy International

gegen

Secretary of State for Foreign and Commonwealth Affairs,

Secretary of State for the Home Department,

Government Communications Headquarters,

Security Service,

Secret Intelligence Service

erlässt

DER GERICHTSHOF (Große Kammer)

unter Mitwirkung des Präsidenten K. Lenaerts, der Vizepräsidentin R. Silva de Lapuerta, der Kammerpräsidenten J.-C. Bonichot und A. Arabadjiev, der Kammerpräsidentin A. Prechal, der Kammerpräsidenten M. Safjan und P. G. Xuereb, der Kammerpräsidentin L. S. Rossi, der Richter J. Malenovský, L. Bay Larsen und T. von Danwitz (Berichterstatter), der Richterinnen C. Toader und K. Jürimäe sowie der Richter C. Lycourgos und N. Piçarra,

Generalanwalt: M. Campos Sánchez-Bordona,

Kanzler: C. Strömholm, Verwaltungsrätin,

* Verfahrenssprache: Englisch.

aufgrund des schriftlichen Verfahrens und auf die mündliche Verhandlung vom 9. und 10. September 2019,

unter Berücksichtigung der Erklärungen

– von Privacy International, vertreten durch B. Jaffey und T. de la Mare, QC, D. Cashman, Solicitor, sowie H. Roy, avocat,

– der Regierung des Vereinigten Königreichs, vertreten durch Z. Lavery, D. Guðmundsdóttir und S. Brandon als Bevollmächtigte im Beistand von G. Facenna und D. Beard, QC, sowie von C. Knight und R. Palmer, Barristers,

– der belgischen Regierung, vertreten durch P. Cottin und J.-C. Halleux als Bevollmächtigte im Beistand von J. Vanpraet, advocaat, und E. de Lophem, avocat,

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

– der deutschen Regierung, zunächst vertreten durch M. Hellmann, R. Kanitz, D. Klebs und T. Henze, dann durch J. Möller, M. Hellmann, R. Kanitz und D. Klebs als Bevollmächtigte,

– der Regierung von Estland, vertreten durch A. Kalbus als Bevollmächtigte,

– der Regierung von Irland, vertreten durch M. Browne, G. Hodge und A. Joyce als Bevollmächtigte im Beistand von D. Fennelly, Barrister,

– der spanischen Regierung, zunächst vertreten durch L. Aguilera Ruiz und M. J. García-Valdecasas Dorrego, dann durch L. Aguilera Ruiz als Bevollmächtigte,

– der französischen Regierung, zunächst vertreten durch E. de Moustier, E. Armoët, A.-L. Desjonquères, F. Alabrune, D. Colas und D. Dubois, dann durch E. de Moustier, E. Armoët, A.-L. Desjonquères, F. Alabrune und D. Dubois als Bevollmächtigte,

– der zyprischen Regierung, vertreten durch E. Symeonidou und E. Neofytou als Bevollmächtigte,

– der lettischen Regierung, zunächst vertreten durch V. Soņeca und I. Kucina, dann durch V. Soņeca als Bevollmächtigte,

– der ungarischen Regierung, zunächst vertreten durch G. Koós, M. Z. Fehér, G. Tornyai und Z. Wagner, dann durch G. Koós und M. Z. Fehér als Bevollmächtigte,

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

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

– der portugiesischen Regierung, vertreten durch L. Inez Fernandes, M. Figueiredo und F. Aragão Homem als Bevollmächtigte,

– der schwedischen Regierung, zunächst vertreten durch A. Falk, H. Shev, C. Meyer-Seitz, L. Zettergren und A. Alriksson, dann durch H. Shev, C. Meyer-Seitz, L. Zettergren und A. Alriksson als Bevollmächtigte,

– der norwegischen Regierung, vertreten durch T. B. Leming, M. Emberland und J. Vangsnes als Bevollmächtigte,

– der Europäischen Kommission, zunächst vertreten durch H. Kranenborg, M. Wasmeier, D. Nardi und P. Costa de Oliveira, dann durch H. Kranenborg, M. Wasmeier und D. Nardi als Bevollmächtigte,

– des Europäischen Datenschutzbeauftragten, vertreten durch T. Zerdick und A. Buchta als Bevollmächtigte,

nach Anhörung der Schlussanträge des Generalanwalts in der Sitzung vom 15. Januar 2020

folgendes

Urteil

1 Das Vorabentscheidungsersuchen betrifft die Auslegung von Art. 1 Abs. 3 und 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 von Art. 4 Abs. 2 EUV sowie der Art. 7, 8 und 52 Abs. 1 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta).

2 Es ergeht im Rahmen eines Rechtsstreits zwischen Privacy International und dem Secretary of State for Foreign and Commonwealth Affairs (Minister für auswärtige Angelegenheiten und Commonwealth-Fragen, Vereinigtes Königreich), dem Secretary of State for the Home Departement (Minister des Innern, Vereinigtes Königreich), dem Government Communications Headquarters (Regierungskommunikationszentrale, Vereinigtes Königreich, im Folgenden: GCHQ), dem Security Service (Inlandsgeheimdienst, Vereinigtes Königreich, im Folgenden: MI5) und dem Secret Intelligence Service (Auslandsgeheimdienst, Vereinigtes Königreich, im Folgenden: MI6) wegen der Rechtmäßigkeit von Rechtsvorschriften, mit denen den Geheimdiensten gestattet wird, Massen-Kommunikationsdaten (bulk communications data) zu sammeln und zu nutzen.

Rechtlicher Rahmen

Unionsrecht

Richtlinie 95/46

3 Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. 1995, L 281, S. 31) wurde durch die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung

personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46 (Datenschutz-Grundverordnung) (ABl. 2016, L 119, S. 1) mit Wirkung vom 25. Mai 2018 aufgehoben. Art. 3 („Anwendungsbereich“) der Richtlinie lautete:

„(1) Diese Richtlinie gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

(2) Diese Richtlinie findet keine Anwendung auf die Verarbeitung personenbezogener Daten,

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

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

Richtlinie 2002/58

4 In den Erwägungsgründen 2, 6, 7, 11, 22, 26 und 30 der Richtlinie 2002/58 heißt es:

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

…

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

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

…

(11) Wie die Richtlinie [95/46] gilt auch die vorliegende Richtlinie nicht für Fragen des Schutzes der Grundrechte und Grundfreiheiten in Bereichen, die nicht unter das [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.

…

(22) Mit dem Verbot der Speicherung von Nachrichten und zugehörigen Verkehrsdaten durch andere Personen als die Nutzer oder ohne deren Einwilligung soll die automatische, einstweilige und vorübergehende Speicherung dieser Informationen insoweit nicht untersagt werden, als diese Speicherung einzig und allein zum Zwecke der Durchführung der Übertragung in dem elektronischen Kommunikationsnetz erfolgt und als die Information nicht länger gespeichert wird, als dies für die Übertragung und zum Zwecke der Verkehrsabwicklung erforderlich ist, und die Vertraulichkeit der Nachrichten gewahrt bleibt. Wenn dies für eine effizientere Weiterleitung einer öffentlich zugänglichen Information an andere Empfänger des Dienstes auf ihr Ersuchen hin erforderlich ist, sollte diese Richtlinie dem nicht entgegenstehen, dass die Information länger gespeichert wird, sofern diese Information der Öffentlichkeit auf jeden Fall uneingeschränkt zugänglich wäre und Daten, die einzelne, die Information anfordernde Teilnehmer oder Nutzer betreffen, gelöscht würden.

…

(26) Teilnehmerdaten, die in elektronischen Kommunikationsnetzen zum Verbindungsaufbau und zur Nachrichtenübertragung verarbeitet werden, enthalten Informationen über das Privatleben natürlicher Personen und betreffen ihr Recht auf Achtung ihrer Kommunikationsfreiheit, oder sie betreffen berechtigte Interessen juristischer Personen. Diese Daten dürfen nur für einen begrenzten Zeitraum und nur insoweit gespeichert werden, wie dies für die Erbringung des Dienstes, für die Gebührenabrechnung und für Zusammenschaltungszahlungen erforderlich ist. Jede weitere Verarbeitung solcher Daten … darf nur unter der Bedingung gestattet werden, dass der Teilnehmer dieser Verarbeitung auf der Grundlage genauer, vollständiger Angaben des Betreibers des öffentlich zugänglichen elektronischen Kommunikationsdienstes über die Formen der von ihm beabsichtigten weiteren Verarbeitung und über das Recht des Teilnehmers, seine Einwilligung zu dieser Verarbeitung nicht zu erteilen oder zurückzuziehen, zugestimmt hat. Verkehrsdaten, die für die Vermarktung von Kommunikationsdiensten … verwendet wurden, sollten ferner nach der Bereitstellung des Dienstes gelöscht oder anonymisiert werden. …

…

(30) Die Systeme für die Bereitstellung elektronischer Kommunikationsnetze und -dienste sollten so konzipiert werden, dass so wenig personenbezogene Daten wie möglich benötigt werden. …“

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

„(1) Diese Richtlinie sieht die Harmonisierung der Vorschriften der Mitgliedstaaten vor, die erforderlich sind, um einen gleichwertigen Schutz der Grundrechte und Grundfreiheiten, insbesondere des Rechts auf Privatsphäre und Vertraulichkeit, in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation sowie den freien Verkehr dieser Daten und von elektronischen Kommunikationsgeräten und -diensten in der [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."

6 Art. 2 („Begriffsbestimmungen") der Richtlinie 2002/58 sieht vor:

„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;

…"

7 Art. 3 („Betroffene Dienste") der Richtlinie 2002/58 lautet:

„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."

8 Art. 5 („Vertraulichkeit der Kommunikation") der Richtlinie 2002/58 sieht vor:

„(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."

9 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."

10 Art. 9 („Andere Standortdaten als Verkehrsdaten") der Richtlinie 2002/58 sieht in Abs. 1 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. …“

11 Art. 15 („Anwendung einzelner Bestimmungen der Richtlinie [95/46]“) der Richtlinie 2002/58 bestimmt in Abs. 1:

„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.“

Verordnung 2016/679

12 Art. 2 der Verordnung 2016/679 bestimmt:

„(1) Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

(2) Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten

a) im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt,

b) durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Titel V Kapitel 2 EUV fallen,

…

d) durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.

…“

13 Art. 4 der Verordnung 2016/679 sieht vor:

„Im Sinne dieser Verordnung bezeichnet der Ausdruck:

…

2. ‚Verarbeitung‘ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das

Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

…“

14 Art. 23 Abs. 1 der Verordnung 2016/679 lautet:

„Durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche oder der Auftragsverarbeiter unterliegt, können die Pflichten und Rechte gemäß den Artikeln 12 bis 22 und Artikel 34 sowie Artikel 5, insofern dessen Bestimmungen den in den Artikeln 12 bis 22 vorgesehenen Rechten und Pflichten entsprechen, im Wege von Gesetzgebungsmaßnahmen beschränkt werden, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt, die Folgendes sicherstellt:

a) die nationale Sicherheit;

b) die Landesverteidigung;

c) die öffentliche Sicherheit;

d) die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit;

e) den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit;

f) den Schutz der Unabhängigkeit der Justiz und den Schutz von Gerichtsverfahren;

g) die Verhütung, Aufdeckung, Ermittlung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe;

h) Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben a bis e und g genannten Zwecke verbunden sind;

i) den Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen;

j) die Durchsetzung zivilrechtlicher Ansprüche.“

15 Art. 94 Abs. 2 der Verordnung 2016/679 lautet:

„Verweise auf die [Richtlinie 95/46] gelten als Verweise auf die vorliegende Verordnung. Verweise auf die durch Artikel 29 der Richtlinie [95/46] eingesetzte Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten gelten als Verweise auf den kraft dieser Verordnung errichteten Europäischen Datenschutzausschuss.“

Recht des Vereinigten Königreichs

16 Section 94 („Weisungen im Interesse der nationalen Sicherheit etc.“) des Telecommunications Act 1984 (Gesetz über Telekommunikation von 1984) in seiner auf den Sachverhalt des Ausgangsverfahrens anwendbaren Fassung (im Folgenden: Gesetz von 1984) sieht vor:

„(1) Der Minister kann nach Konsultation einer Person, für die diese Section gilt, dieser Person Weisungen allgemeiner Art erteilen, die ihm im Interesse der nationalen Sicherheit oder der Beziehung zur Regierung eines Landes oder Gebiets außerhalb des Vereinigten Königreichs erforderlich erscheinen.

(2) Erscheint es dem Minister erforderlich, dies im Interesse der nationalen Sicherheit oder der Beziehung zur Regierung eines Landes oder Gebiets außerhalb des Vereinigten Königreichs zu tun, kann er nach Konsultation einer Person, für die diese Section gilt, dieser Person eine Weisung erteilen, mit der von ihr (je nach den Umständen des Falles) verlangt wird, etwas Bestimmtes, das in der Weisung spezifiziert wird, zu tun oder nicht zu tun.

(2A) Der Minister wird nur dann eine Weisung gemäß Subsection (1) oder (2) erteilen, wenn er der Ansicht ist, dass das mit der Weisung verlangte Verhalten in angemessenem Verhältnis zu dem steht, was mit diesem Verhalten erreicht werden soll.

(3) Eine Person, für die diese Section gilt, wird jede ihr vom Minister gemäß dieser Section erteilte Weisung umsetzen, ungeachtet jeder anderen ihr gemäß Teil 1 oder Kapitel 1 von Teil 2 des Communications Act 2003 [Gesetz von 2003 über die Kommunikation] obliegenden Pflicht und, im Fall einer an einen Betreiber eines öffentlichen elektronischen Kommunikationsnetzes gerichteten Weisung, unbeschadet dessen, dass sie sich auf ihn in einer anderen Eigenschaft als der des Betreibers eines solchen Netzes bezieht.

(4) Der Minister wird jeder der Kammern des Parlaments eine Kopie jeder gemäß dieser Section erteilte Weisung vorlegen, sofern er nicht der Meinung ist, dass die Offenlegung der Weisung den Interessen der nationalen Sicherheit oder den Beziehungen zur Regierung eines Landes oder Gebiets außerhalb des Vereinigten Königreichs oder den wirtschaftlichen Interessen einer Person abträglich ist.

(5) Eine Person wird nichts, was sie aufgrund dieser Section getan hat, offenlegen oder durch eine Rechtsnorm oder in anderer Weise zur Offenlegung verpflichtet werden, wenn der Minister ihr mitgeteilt hat, dass die Offenlegung seines Erachtens den Interessen der nationalen Sicherheit oder den Beziehungen zur Regierung eines Landes oder Gebiets außerhalb des Vereinigten Königreichs oder den wirtschaftlichen Interessen einer anderen Person abträglich wäre.

…

(8) Diese Section gilt für das [Office of communications (OFCOM)] und für die Betreiber öffentlicher elektronischer Kommunikationsnetze.“

17 Section 21(4) und (6) des Regulation of Investigatory Powers Act 2000 (Gesetz von 2000 zur Regelung von Ermittlungsbefugnissen, im Folgenden: RIPA) bestimmt:

„(4) … ‚Kommunikationsdaten‘ [bedeutet]

a) alle Verkehrsdaten, die in einer Nachricht für die Zwecke eines Postdienstes oder Telekommunikationssystems, über den oder das sie übermittelt wird oder übermittelt werden kann, enthalten oder ihr (vom Sender oder anderweitig) beigefügt sind;

b) jede nicht den Inhalt einer Nachricht betreffende Information (außer den unter Buchst. a fallenden Informationen) über die Nutzung durch irgendeine Person
   i) zu einer Post- oder Telekommunikationsdienstleistung oder
   ii) irgendeines Teils eines Telekommunikationssystems in Verbindung mit der Bereitstellung eines Telekommunikationsdienstes an eine Person oder dessen Nutzung durch diese;

c) jede nicht unter Buchst. a oder b fallende Information, über die der Erbringer einer Post- oder Telekommunikationsdienstleistung im Hinblick auf Personen, denen er die Dienstleistung erbringt, verfügt oder die er erhält.

…

(6) … ‚Verkehrsdaten' in Bezug auf eine Nachricht [bedeutet]

a) alle Daten, die eine Person, ein Gerät oder einen Ort identifizieren oder identifizieren können, zu oder von der bzw. dem die Nachricht übermittelt wird oder übermittelt werden kann;

b) alle Daten, die Geräte, durch die oder mittels derer die Nachricht übermittelt wird oder übermittelt werden kann, identifizieren oder wählen oder identifizieren oder wählen können;

c) alle Daten, die Signale für die Betätigung des Geräts enthalten, das in einem Telekommunikationssystem für die (vollständige oder teilweise) Übermittlung einer Nachricht verwendet wird, und

d) alle Daten, die Daten oder andere als die in einer bestimmten Nachricht enthaltenen oder dieser angehängten Daten identifizieren.

…"

18 Die Sections 65 bis 69 des RIPA enthalten die Regeln für die Funktionsweise und die Zuständigkeiten des Investigatory Powers Tribunal (Gericht für Ermittlungsbefugnisse, Vereinigtes Königreich). Nach Section 65 des RIPA kann beim Investigatory Powers Tribunal (Gericht für Ermittlungsbefugnisse) Beschwerde erhoben werden, wenn Grund zu der Annahme besteht, dass Daten auf unangemessene Weise erlangt wurden.

Ausgangsverfahren und Vorlagefragen

19 Zu Beginn des Jahres 2015 wurde, insbesondere durch einen Bericht des Intelligence and Security Committee of Parliament (Ausschuss des Parlaments für Nachrichtendienste und Sicherheit, Vereinigtes Königreich), öffentlich bekannt, dass es Praktiken für die Erlangung und Nutzung von Massen-Kommunikationsdaten durch die verschiedenen Sicherheits- und Nachrichtendienste des Vereinigten Königreichs (GCHQ, MI5 und MI6) gibt. Am 5. Juni 2015 befasste Privacy International, eine Nichtregierungsorganisation, das Investigatory Powers Tribunal (Gericht für Ermittlungsbefugnisse) mit einer gegen den Minister für auswärtige Angelegenheiten und Commonwealth-Fragen, den Minister des Innern und die genannten Sicherheits- und Nachrichtendienste gerichteten Beschwerde in Bezug auf die Rechtmäßigkeit dieser Praktiken.

20 Das vorlegende Gericht prüfte die Rechtmäßigkeit der fraglichen Praktiken zunächst anhand des nationalen Rechts und der Bestimmungen der am 4. November 1950 in Rom unterzeichneten Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK) und sodann anhand des Unionsrechts. Mit Urteil vom 17. Oktober 2016 stellte es fest, dass die Beklagten des Ausgangsverfahrens anerkannt hätten, dass die genannten Dienste im Rahmen ihrer Tätigkeiten große Mengen personenbezogener Daten (bulk personal data) erlangt und genutzt hätten, etwa biografische

Daten oder Reisedaten, finanzielle oder geschäftliche Informationen, Kommunikationsdaten, die vermutlich sensible, unter das Berufsgeheimnis fallende Daten enthielten, oder journalistisches Material. Diese durch verschiedene, möglicherweise geheime Mittel erlangten Daten würden gegeneinander abgeglichen und automatisch verarbeitet, und sie könnten anderen Personen und Behörden offengelegt und mit ausländischen Partnern geteilt werden. In diesem Kontext nutzten die Sicherheits- und Nachrichtendienste auch Massen-Kommunikationsdaten, die sie von Betreibern öffentlicher elektronischer Kommunikationsnetze u. a. aufgrund der von einem Minister gemäß Section 94 des Gesetzes von 1984 erteilten Weisungen erlangt haben. GCHQ und MI5 gingen seit den Jahren 2001 bzw. 2005 so vor.

21 Diese Maßnahmen zur Erlangung und Nutzung solcher Daten stünden mit dem nationalen Recht im Einklang, seit 2015 vorbehaltlich noch ungeklärter Fragen in Bezug auf ihre Verhältnismäßigkeit und den Datentransfer an Dritte im Hinblick auf Art. 8 der EMRK. Insoweit seien Belege für die einschlägigen Sicherheitsmaßnahmen vorgelegt worden, insbesondere hinsichtlich der Verfahren des Zugangs und der Offenlegung außerhalb der Sicherheits- und Nachrichtendienste und der Vorkehrungen für die Speicherung von Daten sowie für eine unabhängige Überwachung.

22 Was die Rechtmäßigkeit der im Ausgangsverfahren in Rede stehenden Maßnahmen zur Erlangung und Nutzung von Daten im Licht des Unionsrechts angeht, prüfte das vorlegende Gericht in einem Urteil vom 8. September 2017, ob diese Maßnahmen in den Geltungsbereich des Unionsrechts fallen und, wenn ja, ob sie mit dem Unionsrecht vereinbar sind. Es kam in Bezug auf die Massen-Kommunikationsdaten zu dem Ergebnis, dass die Betreiber elektronischer Kommunikationsnetze nach Section 94 des Gesetzes von 1984 bei entsprechenden Weisungen eines Ministers verpflichtet seien, den Sicherheits- und Nachrichtendiensten Daten zu liefern, die sie im Rahmen ihrer unter das Unionsrecht fallenden wirtschaftlichen Tätigkeit gesammelt hätten. Dies gelte jedoch nicht für die Erlangung anderer Daten, die diese Dienste erlangten, ohne von solchen Zwangsbefugnissen Gebrauch zu machen. Auf der Grundlage dieser Feststellung hat das vorlegende Gericht es für nötig erachtet, dem Gerichtshof Fragen vorzulegen, um zu klären, ob eine Regelung, wie sie sich aus Section 94 des Gesetzes von 1984 ergibt, unter das Unionsrecht fällt und, wenn ja, ob und inwiefern die Anforderungen, die in der auf das Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u. a. (C-203/15 und C-698/15, im Folgenden: Urteil Tele2, EU:C:2016:970), zurückgehenden Rechtsprechung aufgestellt wurden, für diese Regelung gelten.

23 Insoweit führt das vorlegende Gericht in seinem Vorabentscheidungsersuchen aus, nach Section 94 des Gesetzes von 1984 könne der Minister den Betreibern elektronischer Kommunikationsdienste allgemeine oder spezifische Weisungen erteilen, die er im Interesse der nationalen Sicherheit oder der Beziehungen zu einer ausländischen Regierung für erforderlich halte. Nach den Definitionen in Section 21(4) und (6) des RIPA gehörten zu den fraglichen Daten Verkehrsdaten und Informationen über die Dienstenutzung im Sinne dieser Bestimmung; nur der Inhalt der Nachrichten sei ausgenommen. Solche Daten und Informationen ermöglichten es insbesondere, das „Wer, wo, wann und wie“ einer Nachricht in Erfahrung zu bringen. Diese Daten würden den Sicherheits- und Nachrichtendiensten übermittelt und von ihnen für die Zwecke ihrer Tätigkeiten gespeichert.

24 Die im Ausgangsverfahren in Rede stehende Regelung unterscheide sich von der Regelung im Data Retention and Investigatory Powers Act 2014 (Gesetz von 2014 über die Speicherung von Daten und die Ermittlungsbefugnisse), die Gegenstand der Rechtssache gewesen sei, in der das Urteil vom 21. Dezember 2016, Tele2 (C-203/15 und C-698/15, EU:C:2016:970), ergangen sei, denn die letztgenannte Regelung sehe die Speicherung und Bereitstellung von Daten durch die Betreiber elektronischer Kommunikationsdienste nicht nur für Sicherheits- und Nachrichtendienste im Interesse der nationalen Sicherheit vor, sondern auch für andere Behörden, je nach deren Bedarf. In diesem Urteil sei es zudem um ein Strafverfahren gegangen und nicht um die nationale Sicherheit.

25 Zudem würden die Datenbanken der Sicherheits- und Nachrichtendienste in großem Umfang, unspezifisch und automatisiert verarbeitet, um unbekannte Bedrohungen aufzuspüren. Die dadurch erzeugten Metadatensätze sollten so umfassend wie möglich sein, um einen „Heuhaufen" zu haben, in dem die darin versteckte „Nadel" gefunden werden könne. Zum Nutzen der Erlangung von Massendaten durch diese Dienste und zu den Techniken für ihre Abfrage sei insbesondere auf die Feststellungen in dem Bericht zu verweisen, den David Anderson, QC, der damalige United Kingdom Independent Reviewer of Terrorism Legislation (Unabhängiger Prüfer der Rechtsvorschriften zum Terrorismus im Vereinigten Königreich), am 19. August 2016 erstellt habe. Bei der Erstellung seines Berichts habe er sich auf eine Prüfung durch ein Team von Nachrichtendienstspezialisten und die Aussagen von Beamten der Sicherheits- und Nachrichtendienste gestützt.

26 Privacy International halte die im Ausgangsverfahren in Rede stehende Regelung für unionsrechtswidrig, während die Beklagten des Ausgangsverfahrens der Ansicht seien, dass die in dieser Regelung aufgestellte Pflicht zur Datenübermittlung, der Zugang zu diesen Daten und ihre Nutzung nicht in die Zuständigkeiten der Union fielen, wie insbesondere aus Art. 4 Abs. 2 EUV hervorgehe, wonach die nationale Sicherheit weiterhin allein Sache jedes Mitgliedstaats sei.

27 Wie dem Urteil vom 30. Mai 2006, Parlament/Rat und Kommission (C-317/04 und C-318/04, EU:C:2006:346, Rn. 56 bis 59), das die Übermittlung von Passenger-Name-Record-Daten zum Schutz der öffentlichen Sicherheit betroffen habe, zu entnehmen sei, fielen die Tätigkeiten gewerblicher Unternehmen im Rahmen der Verarbeitung und Übermittlung von Daten zum Schutz der nationalen Sicherheit offenbar nicht in den Geltungsbereich des Unionsrechts. Es müsse nicht geprüft werden, ob die fragliche Tätigkeit eine Datenverarbeitung darstelle, sondern nur, ob der Zweck einer solchen Tätigkeit nach Inhalt und Wirkung darin bestehe, eine grundlegende Funktion des Staates im Sinne von Art. 4 Abs. 2 EUV durch einen Rahmen zu unterstützen, den die im Bereich der öffentlichen Sicherheit tätigen Behörden geschaffen hätten.

28 Sollten die im Ausgangsverfahren in Rede stehenden Maßnahmen hingegen in den Geltungsbereich des Unionsrechts fallen, erschienen die in den Rn. 119 bis 125 des Urteils vom 21. Dezember 2016, Tele2 (C-203/15 und C-698/15, EU:C:2016:970), aufgestellten Anforderungen im Kontext der nationalen Sicherheit unangemessen und würden die Fähigkeit der Sicherheits- und Nachrichtendienste zur Bewältigung einiger Bedrohungen der nationalen Sicherheit untergraben.

29 Unter diesen Umständen hat das Investigatory Powers Tribunal (Gericht für Ermittlungsbefugnisse) beschlossen, das Verfahren auszusetzen und dem Gerichtshof folgende Fragen zur Vorabentscheidung vorzulegen:

Wenn

a) die Fähigkeiten der Sicherheits- und Nachrichtendienste, ihnen zur Verfügung gestellte Massen-Telekommunikationsdaten zu nutzen, für den Schutz der nationalen Sicherheit des Vereinigten Königreichs, u. a. auf dem Gebiet der Terrorismusbekämpfung, der Spionagebekämpfung und der Bekämpfung der nuklearen Proliferation, wesentlich sind,

b) ein wesentliches Merkmal der Nutzung von Massen-Telekommunikationsdaten durch die Sicherheits- und Nachrichtendienste darin besteht, zuvor unbekannte Bedrohungen der nationalen Sicherheit mittels nicht-zielgerichteter Massentechniken aufzuspüren, die sich auf das Sammeln von Massen-Telekommunikationsdaten an einer einzigen Stelle stützen, wobei ihr Hauptnutzen in der schnellen Zielidentifizierung und -entwicklung und in der Bereitstellung einer Grundlage für das Tätigwerden im Fall einer unmittelbaren Bedrohung liegt,

c) der Betreiber eines elektronischen Kommunikationsnetzes danach nicht verpflichtet ist, Massen-Telekommunikationsdaten (über die Dauer der gewöhnlichen geschäftlichen Bedürfnisse hinaus) zu speichern, sondern sie allein vom Staat (den Sicherheits- und Nachrichtendiensten) gespeichert werden,

d) das nationale Gericht (vorbehaltlich bestimmter offener Fragestellungen) festgestellt hat, dass die Schutzmaßnahmen hinsichtlich der Nutzung von Massen-Telekommunikationsdaten durch die Sicherheits- und Nachrichtendienste mit den Anforderungen der EMRK im Einklang stehen, und

e) das nationale Gericht festgestellt hat, dass die Auferlegung der Anforderungen, die in den Rn. 119 bis 125 des Urteils vom 21. Dezember 2016, Tele2 (C-203/15 und C-698/15, EU:C:2016:970), spezifiziert werden – sollten sie anwendbar sein –, die von den Sicherheits- und Nachrichtendiensten zur Gewährleistung der nationalen Sicherheit ergriffenen Maßnahmen beeinträchtigen und dadurch die nationale Sicherheit des Vereinigten Königreichs gefährden würden,

1. fällt dann in Anbetracht von Art. 4 EUV und Art. 1 Abs. 3 der Richtlinie 2002/58 eine Verpflichtung in einer Weisung, mit der ein Minister einem Betreiber eines elektronischen Kommunikationsnetzes vorschreibt, den Sicherheits- und Nachrichtendiensten eines Mitgliedstaats Massen-Kommunikationsdaten zur Verfügung zu stellen, in den Geltungsbereich des Unionsrechts und der Richtlinie 2002/58?

2. Wenn die erste Frage bejaht wird: Ist eine der in den Rn. 119 bis 125 des Urteils vom 21. Dezember 2016, Tele2 (C-203/15 und C-698/15, EU:C:2016:970), aufgestellten Anforderungen oder irgendeine andere Anforderung neben den in der EMRK aufgestellten auf eine solche Weisung eines Ministers anwendbar? Und, wenn ja, wie und inwieweit sind solche Anforderungen anwendbar, berücksichtigt man das wesentliche Bedürfnis der Sicherheits- und Nachrichtendienste, mittels großer Datenmengen und automatisierter Verarbeitungstechniken die nationale Sicherheit zu schützen, und das Ausmaß, in dem solche Fähigkeiten, die im Übrigen mit der EMRK im Einklang stehen, durch die Auferlegung solcher Anforderungen entscheidend beeinträchtigt werden können?

Zu den Vorlagefragen

Zur ersten Frage

30 Mit seiner ersten Frage möchte das vorlegende Gericht wissen, ob Art. 1 Abs. 3 der Richtlinie 2002/58 im Licht von Art. 4 Abs. 2 EUV dahin auszulegen ist, dass eine nationale Regelung, die es einer staatlichen Stelle gestattet, den Betreibern elektronischer Kommunikationsdienste vorzuschreiben, zur Wahrung der nationalen Sicherheit den Sicherheits- und Nachrichtendiensten Verkehrs- und Standortdaten zu übermitteln, in den Geltungsbereich dieser Richtlinie fällt.

31 Insoweit trägt Privacy International im Wesentlichen vor, wie aus der Rechtsprechung des Gerichtshofs zum Geltungsbereich der Richtlinie 2002/58 hervorgehe, falle sowohl die Erlangung von Daten durch die Sicherheits- und Nachrichtendienste bei den genannten Betreibern gemäß Section 94 des Gesetzes von 1984 als auch ihre Nutzung seitens dieser Dienste in den Geltungsbereich der Richtlinie, unabhängig davon, ob die Daten im Wege einer Echtzeit-Übermittlung oder zeitversetzt erlangt würden. Insbesondere habe die Tatsache, dass das Ziel des Schutzes der nationalen Sicherheit in Art. 15 Abs. 1 der Richtlinie ausdrücklich aufgeführt sei, nicht zur Folge, dass sie auf solche Sachverhalte unanwendbar sei; Art. 4 Abs. 2 EUV ändere an dieser Beurteilung nichts.

32 Dagegen machen die Regierung des Vereinigten Königreichs, die tschechische und die estnische Regierung, Irland sowie die französische, die zyprische, die ungarische, die polnische und die schwedische Regierung im Wesentlichen geltend, die Richtlinie 2002/58 finde auf die im Ausgangsverfahren in Rede stehende nationale Regelung keine Anwendung, weil diese zur Wahrung der nationalen Sicherheit diene. Die Tätigkeiten der Sicherheits- und Nachrichtendienste gehörten zu den grundlegenden Funktionen der Mitgliedstaaten, da sie die Aufrechterhaltung der öffentlichen Ordnung sowie die Wahrung der inneren Sicherheit und der territorialen Unversehrtheit beträfen und infolgedessen in die alleinige Zuständigkeit der Mitgliedstaaten fielen, wie insbesondere Art. 4 Abs. 2 Satz 3 EUV zeige.

33 Sie fügen hinzu, die Richtlinie 2002/58 könne daher nicht in dem Sinne ausgelegt werden, dass nationale Maßnahmen zur Wahrung der nationalen Sicherheit in ihren Geltungsbereich fielen. In Art. 1 Abs. 3 der Richtlinie werde ihr Geltungsbereich abgegrenzt, wobei Tätigkeiten betreffend die öffentliche Sicherheit, die Landesverteidigung und die Sicherheit des Staates, wie schon in Art. 3 Abs. 2 erster Gedankenstrich der Richtlinie 95/46, ausgenommen würden. Diese Bestimmungen spiegelten die in Art. 4 Abs. 2 EUV vorgesehene Zuständigkeitsverteilung wider und verlören ihre praktische Wirksamkeit, wenn bei Maßnahmen, die zum Bereich der nationalen Sicherheit gehörten, die Anforderungen der Richtlinie 2002/58 eingehalten werden müssten. Überdies sei die auf das Urteil vom 30. Mai 2006, Parlament/Rat und Kommission (C-317/04 und C-318/04, EU:C:2006:346), zurückgehende Rechtsprechung zu Art. 3 Abs. 2 erster Gedankenstrich der Richtlinie 95/46 auf Art. 1 Abs. 3 der Richtlinie 2002/58 übertragbar.

34 Hierzu ist festzustellen, dass die Richtlinie 2002/58 nach ihrem Art. 1 Abs. 1 u. a. eine Harmonisierung der Vorschriften der Mitgliedstaaten vorsieht, 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 zu gewährleisten.

35 Nach Art. 1 Abs. 3 der Richtlinie 2002/58 sind von ihrem Geltungsbereich die „Tätigkeiten des Staates“ in den dort vorgesehenen Bereichen ausgeschlossen, zu denen die Tätigkeiten im strafrechtlichen Bereich sowie die Tätigkeiten betreffend die öffentliche Sicherheit, die Landesverteidigung und die Sicherheit des Staates einschließlich seines wirtschaftlichen Wohls, wenn die Tätigkeit die Sicherheit des Staates berührt, gehören. Die dort beispielhaft aufgeführten Tätigkeiten sind allesamt spezifische Tätigkeiten der Staaten oder staatlicher Stellen, die nichts mit den Tätigkeitsbereichen von Privatpersonen zu tun haben (Urteil vom 2. Oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, Rn. 32 und die dort angeführte Rechtsprechung).

36 Nach ihrem Art. 3 gilt die Richtlinie 2002/58 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 (im Folgenden: elektronische Kommunikationsdienste). Folglich ist davon auszugehen, dass diese Richtlinie die Tätigkeiten der Betreiber solcher Dienste regelt (Urteil vom 2. Oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, Rn. 33 und die dort angeführte Rechtsprechung).

37 In diesem Rahmen können die Mitgliedstaaten nach Art. 15 Abs. 1 der Richtlinie 2002/58 unter den dort angegebenen Voraussetzungen „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“ (Urteil vom 21. Dezember 2016, Tele2, C-203/15 und C-698/15, EU:C:2016:970, Rn. 71).

38 Art. 15 Abs. 1 der Richtlinie 2002/58 setzt nämlich zwangsläufig voraus, dass die dort genannten nationalen Rechtsvorschriften in den Geltungsbereich der Richtlinie fallen, da sie die Mitgliedstaaten zum Erlass solcher Vorschriften ausdrücklich nur dann ermächtigt, wenn die in dieser Bestimmung vorgesehenen Voraussetzungen eingehalten werden. Außerdem regeln solche Rechtsvorschriften – zu

den in dieser Bestimmung genannten Zwecken – die Tätigkeit der Betreiber elektronischer Kommunikationsdienste (Urteil vom 2. Oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, Rn. 34 und die dort angeführte Rechtsprechung).

39 Vor allem anhand dieser Erwägungen ist der Gerichtshof zu dem Schluss gelangt, dass Art. 15 Abs. 1 der Richtlinie 2002/58 in Verbindung mit ihrem Art. 3 dahin auszulegen ist, dass in den Geltungsbereich der Richtlinie nicht nur eine Rechtsvorschrift fällt, die den Betreibern elektronischer Kommunikationsdienste vorschreibt, die Verkehrs- und Standortdaten zu speichern, sondern auch eine Rechtsvorschrift, die ihnen vorschreibt, den zuständigen nationalen Behörden Zugang zu diesen Daten zu gewähren. Solche Vorschriften haben nämlich zwangsläufig eine Verarbeitung der betreffenden Daten durch die Betreiber zur Folge und können, da sie die Tätigkeiten dieser Betreiber regeln, den in Art. 1 Abs. 3 der Richtlinie genannten spezifischen Tätigkeiten der Staaten nicht gleichgestellt werden (vgl. in diesem Sinne Urteil vom 2. Oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, Rn. 35 und 37 sowie die dort angeführte Rechtsprechung).

40 In Bezug auf eine Rechtsvorschrift wie Section 94 des Gesetzes von 1984, auf deren Grundlage die zuständige Behörde den Betreibern elektronischer Kommunikationsdienste die Weisung erteilen kann, den Sicherheits- und Nachrichtendiensten große Datenmengen zu übermitteln, ist festzustellen, dass der Begriff „Verarbeitung personenbezogener Daten“ nach der Definition in Art. 4 Nr. 2 der Verordnung 2016/679, die gemäß Art. 2 der Richtlinie 2002/58 in Verbindung mit deren Art. 94 Abs. 2 anwendbar ist, „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, … die Speicherung, … das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung …“ bezeichnet.

41 Folglich stellt eine Offenlegung personenbezogener Daten durch Übermittlung ebenso wie eine Speicherung von Daten oder eine andere Form der Bereitstellung eine Verarbeitung im Sinne von Art. 3 der Richtlinie 2002/58 dar und fällt somit in den Geltungsbereich der Richtlinie (vgl. in diesem Sinne Urteil vom 29. Januar 2008, Promusicae, C-275/06, EU:C:2008:54, Rn. 45).

42 Außerdem würde in Anbetracht der Erwägungen in Rn. 38 des vorliegenden Urteils und der Systematik der Richtlinie 2002/58 eine Auslegung, wonach die Rechtsvorschriften, auf die sich ihr Art. 15 Abs. 1 bezieht, von ihrem Geltungsbereich ausgeschlossen sind, weil sich die Zweckbestimmungen, denen solche Rechtsvorschriften entsprechen müssen, im Wesentlichen mit den Zielen decken, die mit den in Art. 1 Abs. 3 der Richtlinie genannten Tätigkeiten verfolgt werden, Art. 15 Abs. 1 jede praktische Wirksamkeit nehmen (vgl. in diesem Sinne Urteil vom 21. Dezember 2016, Tele2, C-203/15 und C-698/15, EU:C:2016:970, Rn. 72 und 73).

43 Der Begriff „Tätigkeiten“ in Art. 1 Abs. 3 der Richtlinie 2002/58 kann daher, wie der Generalanwalt in Nr. 75 seiner Schlussanträge in den verbundenen Rechtssachen La Quadrature du Net u. a. (C-511/18 und C-512/18, EU:C:2020:6), auf die er in Nr. 24 seiner Schlussanträge in der vorliegenden Rechtssache Bezug nimmt, im Wesentlichen ausgeführt hat, nicht so ausgelegt werden, dass er sich auf die Rechtsvorschriften im Sinne von Art. 15 Abs. 1 der Richtlinie erstreckt.

44 Die Bestimmungen von Art. 4 Abs. 2 EUV, auf die die in Rn. 32 des vorliegenden Urteils genannten Regierungen verwiesen haben, können diese Auslegung nicht in Frage stellen. Denn nach ständiger Rechtsprechung des Gerichtshofs ist es zwar Sache der Mitgliedstaaten, ihre wesentlichen Sicherheitsinteressen festzulegen und die geeigneten Maßnahmen zu ergreifen, um ihre innere und äußere Sicherheit zu gewährleisten, doch kann die bloße Tatsache, dass eine nationale Maßnahme zum Schutz der nationalen Sicherheit getroffen wurde, nicht dazu führen, dass das Unionsrecht unanwendbar ist und die Mitgliedstaaten von der erforderlichen Beachtung dieses Rechts entbunden werden (vgl. in diesem Sinne Urteile vom 4. Juni 2013, ZZ, C-300/11, EU:C:2013:363, Rn. 38 und die dort angeführte Rechtsprechung, vom 20. März 2018, Kommission/Österreich [Staatsdruckerei],

C-187/16, EU:C:2018:194, Rn. 75 und 76, sowie vom 2. April 2020, Kommission/Polen, Ungarn und Tschechische Republik [Vorübergehender Umsiedlungsmechanismus für internationalen Schutz beantragende Personen], C-715/17, C-718/17 und C-719/17, EU:C:2020:257, Rn. 143 und 170).

45 Es trifft zu, dass der Gerichtshof im Urteil vom 30. Mai 2006, Parlament/Rat und Kommission (C-317/04 und C-318/04, EU:C:2006:346, Rn. 56 bis 59), entschieden hat, dass die Übermittlung personenbezogener Daten durch Fluggesellschaften an die Behörden eines Drittstaats zur Verhütung und Bekämpfung des Terrorismus und anderer schwerer Straftaten nach Art. 3 Abs. 2 erster Gedankenstrich der Richtlinie 95/46 nicht in deren Anwendungsbereich fiel, weil sie in einem von staatlichen Stellen geschaffenen Rahmen stattfand und der öffentlichen Sicherheit diente.

46 Angesichts der Erwägungen in den Rn. 36, 38 und 39 des vorliegenden Urteils ist diese Rechtsprechung jedoch nicht auf die Auslegung von Art. 1 Abs. 3 der Richtlinie 2002/58 übertragbar. Wie der Generalanwalt in den Nrn. 70 bis 72 seiner Schlussanträge in den verbundenen Rechtssachen La Quadrature du Net u. a. (C-511/18 und C-512/18, EU:C:2020:6) im Wesentlichen ausgeführt hat, nahm Art. 3 Abs. 2 erster Gedankenstrich der Richtlinie 95/46, auf den sich die genannte Rechtsprechung bezieht, nämlich „Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung [und] die Sicherheit des Staates“ generell vom Anwendungsbereich dieser Richtlinie aus, ohne anhand des Urhebers der betreffenden Verarbeitung von Daten zu unterscheiden. Dagegen erweist sich eine solche Unterscheidung im Rahmen der Auslegung von Art. 1 Abs. 3 der Richtlinie 2002/58 als erforderlich. Wie aus den Rn. 37 bis 39 und 42 des vorliegenden Urteils hervorgeht, fallen in ihren Geltungsbereich nämlich alle Verarbeitungen personenbezogener Daten durch Betreiber elektronischer Kommunikationsdienste, einschließlich Verarbeitungen aufgrund von Verpflichtungen, die ihnen von den Behörden auferlegt wurden. Die letztgenannten Verarbeitungen konnten hingegen gegebenenfalls unter die in Art. 3 Abs. 2 erster Gedankenstrich der Richtlinie 95/46 vorgesehene Ausnahme fallen, da diese Bestimmung weiter gefasst ist und sich auf alle die öffentliche Sicherheit, die Landesverteidigung oder die Sicherheit des Staates betreffenden Verarbeitungen erstreckt, unabhängig von ihrem Urheber.

47 Überdies ist festzustellen, dass die Richtlinie 95/46, um die es in der Rechtssache ging, in der das Urteil vom 30. Mai 2006, Parlament/Rat und Kommission (C-317/04 und C-318/04, EU:C:2006:346), ergangen ist, gemäß Art. 94 Abs. 1 der Verordnung 2016/679 mit Wirkung vom 25. Mai 2018 durch diese Verordnung aufgehoben und ersetzt wurde. Die Verordnung findet zwar nach ihrem Art. 2 Abs. 2 Buchst. d keine Anwendung auf Verarbeitungen „durch die zuständigen Behörden“ u. a. zum Zweck der Verhütung und Feststellung von Straftaten, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Wie aus Art. 23 Abs. 1 Buchst. d und h der Verordnung hervorgeht, fallen aber Verarbeitungen personenbezogener Daten, die zu diesem Zweck von Privatpersonen vorgenommen werden, in ihren Anwendungsbereich. Daraus folgt, dass die vorstehende Auslegung von Art. 1 Abs. 3, Art. 3 und Art. 15 Abs. 1 der Richtlinie 2002/58 im Einklang mit der Abgrenzung des Anwendungsbereichs der Verordnung 2016/679 steht, die diese Richtlinie ergänzt und präzisiert.

48 Wenn die Mitgliedstaaten unmittelbar Maßnahmen umsetzen, mit denen von der Vertraulichkeit elektronischer Kommunikationen abgewichen wird, ohne den Betreibern elektronischer Kommunikationsdienste Verarbeitungspflichten aufzuerlegen, fällt der Schutz der Daten der Betroffenen hingegen nicht unter die Richtlinie 2002/58, sondern allein unter das nationale Recht, vorbehaltlich der Anwendung der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. 2016, L 119, S. 89), so dass die fraglichen Maßnahmen insbesondere mit nationalem Recht von Verfassungsrang und den Anforderungen der EMRK im Einklang stehen müssen.

49 Nach alledem ist auf die erste Frage zu antworten, dass Art. 1 Abs. 3, Art. 3 und Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht von Art. 4 Abs. 2 EUV dahin auszulegen sind, dass eine nationale Regelung, die es einer staatlichen Stelle gestattet, den Betreibern elektronischer Kommunikationsdienste vorzuschreiben, zur Wahrung der nationalen Sicherheit den Sicherheits- und Nachrichtendiensten Verkehrs- und Standortdaten zu übermitteln, in den Geltungsbereich dieser Richtlinie fällt.

Zur zweiten Frage

50 Mit seiner zweiten Frage möchte das vorlegende Gericht wissen, ob Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht von Art. 4 Abs. 2 EUV sowie der Art. 7, 8 und 11 der Charta und ihres Art. 52 Abs. 1 dahin auszulegen ist, dass er einer nationalen Regelung entgegensteht, die es einer staatlichen Stelle gestattet, zur Wahrung der nationalen Sicherheit den Betreibern elektronischer Kommunikationsdienste vorzuschreiben, den Sicherheits- und Nachrichtendiensten allgemein und unterschiedslos Verkehrs- und Standortdaten zu übermitteln.

51 Zunächst ist darauf hinzuweisen, dass Section 94 des Gesetzes von 1984 nach den Angaben im Vorabentscheidungsersuchen dem Minister gestattet, den Betreibern elektronischer Kommunikationsdienste durch Weisungen vorzuschreiben, den Sicherheits- und Nachrichtendiensten Massen-Kommunikationsdaten, zu denen Verkehrs- und Standortdaten sowie Informationen über die genutzten Dienste im Sinne von Section 21(4) und (6) des RIPA gehören, zu übermitteln, wenn er dies im Interesse der nationalen Sicherheit oder der Beziehungen zu einer ausländischen Regierung für erforderlich hält. Die letztgenannte Bestimmung erfasst u. a. die Daten, die notwendig sind, um die Quelle und den Adressaten einer Kommunikation aufzuspüren, Datum, Uhrzeit, Dauer und Art der Kommunikation zu ermitteln, das verwendete Kommunikationsmaterial zu identifizieren sowie den Standort der Endgeräte und der Kommunikationen zu bestimmen. Zu diesen Daten gehören u. a. Name und Adresse des Nutzers, die Telefonnummern des Anrufers und des Angerufenen, die IP-Adressen der Quelle und des Adressaten der Kommunikation sowie die Adressen der besuchten Websites.

52 Eine solche Offenlegung durch Übermittlung der Daten betrifft alle Nutzer elektronischer Kommunikationsmittel, ohne dass näher angegeben wird, ob die Übermittlung in Echtzeit oder zeitversetzt erfolgen muss. Im Anschluss an ihre Übermittlung werden diese Daten nach den Angaben im Vorabentscheidungsersuchen von den Sicherheits- und Nachrichtendiensten gespeichert und stehen ihnen für ihre Tätigkeiten ebenso zur Verfügung wie ihre übrigen Datenbanken. Insbesondere können die auf diese Weise gesammelten Daten, die automatisierten Massenverarbeitungen und -analysen unterzogen werden, mit anderen Datenbanken, die andere Kategorien personenbezogener Massendaten enthalten, abgeglichen oder an Stellen außerhalb dieser Dienste und an Drittstaaten weitergegeben werden. Schließlich bedürfen diese Vorgänge keiner vorherigen Genehmigung durch ein Gericht oder eine unabhängige Verwaltungsstelle, und die Betroffenen werden nicht davon unterrichtet.

53 Die Richtlinie 2002/58 soll, 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 soll mit der Richtlinie nach ihrem zweiten Erwägungsgrund gewährleistet werden, dass die in den Art. 7 und 8 der Charta niedergelegten Rechte uneingeschränkt geachtet werden. Insoweit ergibt sich 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, 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“.

54 Zu diesem Zweck sieht Art. 5 Abs. 1 der Richtlinie 2002/58 vor, dass die Mitgliedstaaten „durch innerstaatliche Vorschriften die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten sicher[stellen]“. Weiter heißt es dort: „Insbesondere untersagen [die Mitgliedstaaten] 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.“ Art. 5 Abs. 1 „steht – unbeschadet des Grundsatzes der Vertraulichkeit – der für die Weiterleitung einer Nachricht erforderlichen technischen Speicherung nicht entgegen.“

55 In Art. 5 Abs. 1 der Richtlinie 2002/58 wird somit der Grundsatz der Vertraulichkeit sowohl elektronischer Nachrichten als auch der damit verbundenen Verkehrsdaten aufgestellt, der u. a. das grundsätzliche Verbot für jede andere Person als die Nutzer impliziert, ohne deren Einwilligung solche Nachrichten und Daten auf Vorrat zu speichern. In Anbetracht ihres allgemein gehaltenen Wortlauts gilt diese Bestimmung notwendigerweise für jeden Vorgang, der es Dritten erlaubt, zu anderen Zwecken als der Weiterleitung einer Nachricht Kenntnis von Nachrichten und den damit verbundenen Daten zu erlangen.

56 Das Verbot in Art. 5 Abs. 1 der Richtlinie 2002/58, Nachrichten und die damit verbundenen Daten abzufangen, erfasst deshalb jede Form der Bereitstellung von Verkehrs- und Standortdaten durch die Betreiber elektronischer Kommunikationsdienste für Behörden wie Sicherheits- und Nachrichtendienste sowie die Speicherung solcher Daten durch diese Behörden, unabhängig von einer späteren Verwendung dieser Daten.

57 Durch den Erlass dieser Richtlinie hat der Unionsgesetzgeber somit die in den Art. 7 und 8 der Charta verankerten Rechte konkretisiert, so dass die Nutzer elektronischer Kommunikationsmittel grundsätzlich erwarten dürfen, dass ihre Nachrichten und die damit verbundenen Daten 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, Rn. 109).

58 Art. 15 Abs. 1 der Richtlinie 2002/58 gestattet es den Mitgliedstaaten jedoch, Ausnahmen von der in Art. 5 Abs. 1 der Richtlinie aufgestellten grundsätzlichen Pflicht zur Sicherstellung der Vertraulichkeit personenbezogener Daten sowie den entsprechenden, u. a. in den Art. 6 und 9 der Richtlinie genannten Pflichten zu schaffen, sofern eine solche Beschränkung für die nationale Sicherheit, die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs elektronischer Kommunikationssysteme in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zweck können die Mitgliedstaaten u. a. durch Rechtsvorschriften vorsehen, dass Daten aus einem dieser Gründe für begrenzte Zeit aufbewahrt werden.

59 Die Befugnis, von den Rechten und Pflichten, wie sie die Art. 5, 6 und 9 der Richtlinie 2002/58 vorsehen, abzuweichen, kann es aber nicht rechtfertigen, dass die Ausnahme von dieser grundsätzlichen Pflicht zur Sicherstellung der Vertraulichkeit elektronischer Kommunikationen und der damit verbundenen Daten und insbesondere von dem in Art. 5 der Richtlinie ausdrücklich vorgesehenen Verbot, solche Daten zu speichern, zur Regel wird (vgl. in diesem Sinne Urteile vom 21. Dezember 2016, Tele2, C-203/15 und C-698/15, EU:C:2016:970, Rn. 89 und 104, sowie vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, Rn. 111).

60 Außerdem geht aus Art. 15 Abs. 1 Satz 3 der Richtlinie 2002/58 hervor, dass die Mitgliedstaaten Rechtsvorschriften, die die Tragweite der Rechte und Pflichten gemäß den Art. 5, 6 und 9 dieser Richtlinie beschränken sollen, nur unter Beachtung der allgemeinen Grundsätze des Unionsrechts, zu denen der Grundsatz der Verhältnismäßigkeit gehört, und der durch die Charta garantierten Grundrechte erlassen dürfen. Hierzu hat der Gerichtshof bereits entschieden, dass die den Betreibern

elektronischer Kommunikationsdienste durch eine nationale Regelung auferlegte Pflicht, Verkehrsdaten auf Vorrat zu speichern, um sie gegebenenfalls den zuständigen nationalen Behörden zugänglich zu machen, Fragen aufwirft, die die Einhaltung nicht nur 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 (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. 25 und 70, sowie vom 21. Dezember 2016, Tele2, C-203/15 und C-698/15, EU:C:2016:970, Rn. 91 und 92 sowie die dort angeführte Rechtsprechung).

61 Die gleichen Fragen stellen sich auch für andere Arten der Verarbeitung von Daten, wie ihre Übermittlung an andere Personen als die Nutzer oder den Zugang zu ihnen im Hinblick auf ihre Nutzung (vgl. entsprechend Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26. Juli 2017, EU:C:2017:592, Rn. 122 und 123 sowie die dort angeführte Rechtsprechung).

62 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 (vgl. in diesem Sinne Urteile vom 6. März 2001, Connolly/Kommission, C-274/99 P, EU:C:2001:127, Rn. 39, und vom 21. Dezember 2016, Tele2, C-203/15 und C-698/15, EU:C:2016:970, Rn. 93 und die dort angeführte Rechtsprechung).

63 Die in den Art. 7, 8 und 11 der Charta verankerten Rechte können jedoch keine uneingeschränkte Geltung beanspruchen, sondern müssen im Hinblick auf ihre gesellschaftliche Funktion gesehen werden (vgl. in diesem Sinne Urteil vom 16. Juli 2020, Facebook Ireland und Schrems, C-311/18, EU:C:2020:559, Rn. 172 und die dort angeführte Rechtsprechung).

64 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.

65 Hinzuzufügen ist, dass das Erfordernis, dass jede Einschränkung der Ausübung von Grundrechten gesetzlich vorgesehen sein muss, bedeutet, dass die gesetzliche Grundlage für den Eingriff in die Grundrechte den Umfang, in dem die Ausübung des betreffenden Rechts eingeschränkt wird, selbst festlegen muss (Urteil vom 16. Juli 2020, Facebook Ireland und Schrems, C-311/18, EU:C:2020:559, Rn. 175 und die dort angeführte Rechtsprechung).

66 In Bezug auf die Beachtung des Grundsatzes der Verhältnismäßigkeit sieht Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 vor, dass die Mitgliedstaaten eine Vorschrift erlassen können, die vom Grundsatz der Vertraulichkeit von Kommunikationen und der damit verbundenen Verkehrsdaten abweicht, sofern dies in Anbetracht der dort genannten Zwecke „in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig“ ist. Im elften Erwägungsgrund der Richtlinie wird klargestellt, dass eine derartige Maßnahme in einem „strikt“ angemessenen Verhältnis zum intendierten Zweck stehen muss.

67 Insoweit ist darauf hinzuweisen, dass der Schutz des Grundrechts auf Achtung des Privatlebens nach ständiger Rechtsprechung des Gerichtshofs verlangt, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken. Außerdem kann eine dem Gemeinwohl dienende Zielsetzung nicht verfolgt werden, ohne den Umstand zu berücksichtigen, dass sie mit den von der Maßnahme betroffenen Grundrechten in

Einklang gebracht werden muss, indem eine ausgewogene Gewichtung der Zielsetzung und der fraglichen Rechte und Pflichten vorgenommen wird (vgl. in diesem Sinne Urteile vom 16. Dezember 2008, Satakunnan Markkinapörssi und Satamedia, C-73/07, EU:C:2008:727, Rn. 56, vom 9. November 2010, Volker und Markus Schecke und Eifert, C-92/09 und C-93/09, EU:C:2010:662, Rn. 76, 77 und 86, sowie vom 8. April 2014, Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 52; Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26. Juli 2017, EU:C:2017:592, Rn. 140).

68 Um dem Erfordernis der Verhältnismäßigkeit zu genügen, muss eine Regelung 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 ihrer Daten vor Missbrauchsrisiken ermöglichen. Die Regelung muss 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 speziellen Kategorie sensibler personenbezogener Daten geht (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. 54 und 55, sowie vom 21. Dezember 2016, Tele2, C-203/15 und C-698/15, EU:C:2016:970, Rn. 117; Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26. Juli 2017, EU:C:2017:592, Rn. 141).

69 Zu der Frage, ob eine nationale Regelung wie die im Ausgangsverfahren in Rede stehende im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta den Anforderungen von Art. 15 Abs. 1 der Richtlinie 2002/58 genügt, ist festzustellen, dass die Übermittlung von Verkehrs- und Standortdaten an andere Personen als die Nutzer, etwa an die Sicherheits- und Nachrichtendienste, vom Grundsatz der Vertraulichkeit abweicht. Geschieht dies, wie hier, in allgemeiner und unterschiedsloser Weise, wird die Abweichung von der grundsätzlichen Pflicht zur Gewährleistung der Vertraulichkeit der Daten zur Regel, obwohl das durch die Richtlinie 2002/58 geschaffene System verlangt, dass eine solche Abweichung die Ausnahme bleibt.

70 Zudem stellt nach ständiger Rechtsprechung des Gerichtshofs die Übermittlung von Verkehrs- und Standortdaten an einen Dritten einen Eingriff in die Grundrechte dar, die in den Art. 7 und 8 der Charta verankert sind, unabhängig davon, wie diese Daten später genutzt werden. 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 (vgl. in diesem Sinne Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26. Juli 2017, EU:C:2017:592, Rn. 124 und 126 sowie die dort angeführte Rechtsprechung, und Urteil vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, Rn. 115 und 116).

71 Der mit der Übermittlung von Verkehrs- und Standortdaten an die Sicherheits- und Nachrichtendienste verbundene Eingriff in das in Art. 7 der Charta verankerte Recht ist insbesondere angesichts des sensiblen Charakters der Informationen, die diese Daten liefern können, und vor allem angesichts der Möglichkeit, anhand von ihnen ein Profil der Betroffenen zu erstellen, als besonders schwer anzusehen, da eine solche Information ebenso sensibel ist wie der Inhalt der Kommunikationen selbst. Überdies ist er geeignet, bei den Betroffenen das Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist (vgl. entsprechend Urteile vom 8. April 2014, Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 27 und 37, sowie vom 21. Dezember 2016, Tele2, C-203/15 und C-698/15, EU:C:2016:970, Rn. 99 und 100).

72 Hinzuzufügen ist, dass eine Übermittlung von Verkehrs- und Standortdaten an Behörden zu Sicherheitszwecken für sich genommen 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 kann. Solche abschreckenden Wirkungen können in besonderem Maß Personen treffen, deren Kommunikationen nach den nationalen Vorschriften dem Berufsgeheimnis unterliegen, sowie Whistleblower, deren Aktivitäten durch die Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (ABl. 2019, L 305, S. 17), geschützt werden. Außerdem sind diese Wirkungen umso stärker, je größer die Menge und die Vielfalt der auf Vorrat gespeicherten Daten sind (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. 28, vom 21. Dezember 2016, Tele2, C-203/15 und C-698/15, EU:C:2016:970, Rn. 101, und vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, Rn. 118).

73 Schließlich birgt die bloße Vorratsspeicherung durch die Betreiber elektronischer Kommunikationsdienste angesichts der großen Menge von Verkehrs- und Standortdaten, die durch eine Maßnahme allgemeiner Vorratsspeicherung kontinuierlich gespeichert werden können, sowie des sensiblen Charakters der Informationen, die diese Daten liefern können, Gefahren des Missbrauchs und des rechtswidrigen Zugangs.

74 Zu den Zielen, die solche Eingriffe rechtfertigen können, und insbesondere zu dem im Ausgangsverfahren in Rede stehenden Ziel der Wahrung der nationalen Sicherheit ist zunächst festzustellen, dass nach Art. 4 Abs. 2 EUV die nationale Sicherheit weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten fällt. Diese Verantwortung entspricht dem zentralen Anliegen, die wesentlichen Funktionen des Staates und die grundlegenden Interessen der Gesellschaft zu schützen, und umfasst die Verhütung und Repression von Tätigkeiten, 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 (Urteil vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, Rn. 135).

75 Die Bedeutung des Ziels, die nationale Sicherheit zu wahren, übersteigt im Licht von Art. 4 Abs. 2 EUV 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. Bedrohungen wie die in der vorstehenden Randnummer genannten unterscheiden sich nämlich aufgrund ihrer Art und ihrer besonderen Schwere von der allgemeinen Gefahr des Auftretens selbst schwerer Spannungen oder Störungen im Bereich der öffentlichen Sicherheit. Vorbehaltlich der Erfüllung der übrigen Anforderungen von Art. 52 Abs. 1 der Charta ist das Ziel, die nationale Sicherheit zu wahren, daher geeignet, Maßnahmen zu rechtfertigen, die schwerere Grundrechtseingriffe enthalten als solche, die mit den übrigen Zielen gerechtfertigt werden könnten (Urteil vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, Rn. 136).

76 Um dem in Rn. 67 des vorliegenden Urteils angesprochenen Erfordernis der Verhältnismäßigkeit, wonach Ausnahmen vom Schutz personenbezogener Daten und dessen Beschränkungen nicht über das absolut Notwendige hinausgehen dürfen, zu genügen, muss eine nationale Regelung, die mit einem Eingriff in die in den Art. 7 und 8 der Charta verankerten Grundrechte verbunden ist, jedoch den Anforderungen entsprechen, die sich aus der in den Rn. 65, 67 und 68 des vorliegenden Urteils angeführten Rechtsprechung ergeben.

77 Eine solche Regelung darf sich insbesondere hinsichtlich des Zugangs einer Behörde zu personenbezogenen Daten nicht darauf beschränken, dass der behördliche Zugang zu den Daten dem mit der Regelung verfolgten Zweck zu entsprechen hat, sondern muss auch die materiellen und prozeduralen Voraussetzungen für die Verwendung der Daten vorsehen (vgl. entsprechend Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26. Juli 2017, EU:C:2017:592, Rn. 192 und die dort angeführte Rechtsprechung).

78 Infolgedessen, und weil ein allgemeiner Zugang zu allen auf Vorrat gespeicherten Daten ohne jeden – auch nur mittelbaren – Zusammenhang mit dem verfolgten Ziel nicht als auf das absolut Notwendige beschränkt angesehen werden kann, muss sich eine nationale Regelung des Zugangs zu Verkehrs- und Standortdaten 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 (vgl. in diesem Sinne Urteil vom 21. Dezember 2016, Tele2, C-203/15 und C-698/15, EU:C:2016:970, Rn. 119 und die dort angeführte Rechtsprechung).

79 Diese Anforderungen gelten erst recht für eine Rechtsvorschrift wie die im Ausgangsverfahren in Rede stehende, auf deren Grundlage die zuständige nationale Behörde den Betreibern elektronischer Kommunikationsdienste vorschreiben kann, den Sicherheits- und Nachrichtendiensten Verkehrs- und Standortdaten durch eine allgemeine und unterschiedslose Übermittlung offenzulegen. Eine solche Übermittlung hat nämlich zur Folge, dass diese Daten den Behörden zur Verfügung gestellt werden (vgl. entsprechend Gutachten 1/15 [PNR-Abkommen EU–Kanada] vom 26. Juli 2017, EU:C:2017:592, Rn. 212).

80 Da die Verkehrs- und Standortdaten allgemein und unterschiedslos übermittelt werden, betrifft ihre Übermittlung pauschal sämtliche Personen, die elektronische Kommunikationsdienste nutzen. 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 Wahrung der nationalen Sicherheit stehen könnte, und setzt insbesondere keinen Zusammenhang zwischen den Daten, deren Übermittlung vorgesehen ist, und einer Bedrohung der nationalen Sicherheit voraus (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. 57 und 58, sowie vom 21. Dezember 2016, Tele2, C-203/15 und C-698/15, EU:C:2016:970, Rn. 105). Angesichts dessen, dass die Übermittlung solcher Daten an die Behörden nach den in Rn. 79 des vorliegenden Urteils getroffenen Feststellungen einem Zugang gleichkommt, ist davon auszugehen, dass eine Regelung, die eine allgemeine und unterschiedslose Übermittlung der Daten an die Behörden gestattet, einen allgemeinen Zugang impliziert.

81 Daraus folgt, dass eine nationale Regelung, die den Betreibern elektronischer Kommunikationsdienste vorschreibt, den Sicherheits- und Nachrichtendiensten Verkehrs- und Standortdaten durch eine allgemeine und unterschiedslose Übermittlung offenzulegen, die Grenzen des absolut Notwendigen überschreitet und nicht als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden kann, wie es Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht von Art. 4 Abs. 2 EUV sowie der Art. 7, 8 und 11 der Charta und ihres Art. 52 Abs. 1 verlangt.

82 Nach alledem ist auf die zweite Frage zu antworten, dass Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht von Art. 4 Abs. 2 EUV sowie der Art. 7, 8 und 11 der Charta und ihres Art. 52 Abs. 1 dahin auszulegen ist, dass er einer nationalen Regelung entgegensteht, die es einer staatlichen Stelle gestattet, zur Wahrung der nationalen Sicherheit den Betreibern elektronischer Kommunikationsdienste vorzuschreiben, den Sicherheits- und Nachrichtendiensten allgemein und unterschiedslos Verkehrs- und Standortdaten zu übermitteln.

Kosten

83 Für die Parteien des Ausgangsverfahrens ist das Verfahren ein Zwischenstreit in dem beim vorlegenden Gericht anhängigen Rechtsstreit; 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. 1 Abs. 3, Art. 3 und 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 sind im Licht von Art. 4 Abs. 2 EUV dahin auszulegen, dass eine nationale Regelung, die es einer staatlichen Stelle gestattet, den Betreibern elektronischer Kommunikationsdienste vorzuschreiben, zur Wahrung der nationalen Sicherheit den Sicherheits- und Nachrichtendiensten Verkehrs- und Standortdaten zu übermitteln, in den Geltungsbereich dieser Richtlinie fällt.**

2. **Art. 15 Abs. 1 der Richtlinie 2002/58 in der durch die Richtlinie 2009/136 geänderten Fassung ist im Licht von Art. 4 Abs. 2 EUV sowie der Art. 7, 8 und 11 der Charta der Grundrechte der Europäischen Union und ihres Art. 52 Abs. 1 dahin auszulegen, dass er einer nationalen Regelung entgegensteht, die es einer staatlichen Stelle gestattet, zur Wahrung der nationalen Sicherheit den Betreibern elektronischer Kommunikationsdienste vorzuschreiben, den Sicherheits- und Nachrichtendiensten allgemein und unterschiedslos Verkehrs- und Standortdaten zu übermitteln.**

Unterschriften