EuGH · Urteil vom 21. Dezember 2016 · Az. C-203/15, C-698/15

- **Gericht:**

  EuGH

- **Datum:**

  21. Dezember 2016

- **Aktenzeichen:**

  C-203/15, C-698/15

- **Typ:**

  Urteil

- **Fundstelle:**

  openJur 2016, 10221

- **Verfahrensgang:**

IT- und Medienrecht Internetrecht Europarecht Datenschutzrecht Öffentliches Recht Artt. 11, 52 Abs. 1, 7, 8 GrCH

Tenor

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 des Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union dahin auszulegen, dass er einer nationalen Regelung entgegensteht, die für Zwecke der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsieht.Art. 15 Abs. 1 der Richtlinie 2002/58 in der durch die Richtlinie 2009/136 geänderten Fassung ist im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta der Grundrechte dahin auszulegen, dass er einer nationalen Regelung entgegensteht, die den Schutz und die Sicherheit der Verkehrs- und Standortdaten, insbesondere den Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten zum Gegenstand hat, ohne im Rahmen der Bekämpfung von Straftaten diesen Zugang ausschließlich auf die Zwecke einer Bekämpfung schwerer Straftaten zu beschränken, ohne den Zugang einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsbehörde zu unterwerfen und ohne vorzusehen, dass die betreffenden Daten im Gebiet der Union auf Vorrat zu speichern sind. Die zweite Vorlagefrage des Court of Appeal (England & Wales) (Civil Division) (Berufungsgericht [England und Wales] [Abteilung für Zivilsachen], Vereinigtes Königreich) ist unzulässig.

Gründe

Die Vorabentscheidungsersuchen betreffen die Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. 2002, L 201, S. 37) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 (ABl.

2009, L 337, S. 11) geänderten Fassung (im Folgenden: Richtlinie 2002/58) im Licht der Art. 7 und 8 sowie des Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta).

Diese Ersuchen ergehen im Rahmen von zwei Rechtsstreitigkeiten; in der ersten streiten die Tele2 Sverige AB mit Post- och telestyrelsen (schwedische Überwachungsbehörde für Post und Telekommunikation, im Folgenden: PTS) über eine Anordnung der PTS gegenüber Tele2 Sverige zur Vorratsspeicherung von Verkehrsdaten und von Standortdaten ihrer Teilnehmer und registrierten Nutzer (Rechtssache C-203/15), in der zweiten Herr Tom Watson, Herr Peter Brice und Herr Geoffrey Lewis mit dem Secretary of State for the Home Department (Innenminister, Vereinigtes Königreich Großbritannien und Nordirland) über die Vereinbarkeit des Data Retention and Investigatory Powers Act 2014 (Gesetz von 2014 zur Vorratsdatenspeicherung und zu den Ermittlungsbefugnissen, im Folgenden: DRIPA) mit dem Unionsrecht (Rechtssache C-698/15).

Rechtlicher Rahmen

Unionsrecht

Richtlinie 2002/58

In den Erwägungsgründen 2, 6, 7, 11, 21, 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/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 Gemeinschaftsrecht fallen. Deshalb hat sie keine Auswirkungen auf das bestehende Gleichgewicht zwischen dem Recht des Einzelnen auf Privatsphäre und der Möglichkeit der Mitgliedstaaten, Maßnahmen nach Artikel 15 Absatz 1 dieser Richtlinie zu ergreifen, die für den Schutz der öffentlichen Sicherheit, für die Landesverteidigung, für die Sicherheit des Staates (einschließlich des wirtschaftlichen Wohls des Staates, soweit die Tätigkeiten die Sicherheit des Staates berühren) und für die Durchsetzung strafrechtlicher Bestimmungen erforderlich sind. Folglich betrifft diese Richtlinie nicht die Möglichkeit der Mitgliedstaaten zum rechtmäßigen Abfangen elektronischer Nachrichten oder zum Ergreifen anderer Maßnahmen, sofern dies erforderlich ist, um einen dieser Zwecke zu erreichen, und sofern dies im Einklang mit der 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.

...

(21) Es sollten Maßnahmen getroffen werden, um den unerlaubten Zugang zu Nachrichten – und zwar sowohl zu ihrem Inhalt als auch zu mit ihnen verbundenen Daten – zu verhindern und so die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen elektronischen Kommunikationsdiensten erfolgenden Nachrichtenübertragung zu schützen. Nach dem Recht einiger Mitgliedstaaten ist nur der absichtliche unberechtigte Zugriff auf die Kommunikation untersagt.

(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. ...

...

(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. ...

...

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

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 Gemeinschaft zu gewährleisten.

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

(3) Diese Richtlinie gilt nicht für Tätigkeiten, die nicht in den Anwendungsbereich des Vertrags zur Gründung der Europäischen Gemeinschaft 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.“

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

...

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;

...“

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 Gemeinschaft, einschließlich öffentlicher Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte unterstützen.“

In Art. 4 („Sicherheit der Verarbeitung“) dieser Richtlinie heißt es:

„(1) Der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes muss geeignete technische und organisatorische Maßnahmen ergreifen, um die Sicherheit seiner Dienste zu gewährleisten; die Netzsicherheit ist hierbei erforderlichenfalls zusammen mit dem Betreiber des öffentlichen Kommunikationsnetzes zu gewährleisten. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der Kosten ihrer Durchführung ein Sicherheitsniveau gewährleisten, das angesichts des bestehenden Risikos angemessen ist.

(1a) Unbeschadet der Richtlinie [95/46] ist durch die in Absatz 1 genannten Maßnahmen zumindest Folgendes zu erreichen:

– Sicherstellung, dass nur ermächtigte Personen für rechtlich zulässige Zwecke Zugang zu personenbezogenen Daten erhalten,

– Schutz gespeicherter oder übermittelter personenbezogener Daten vor unbeabsichtigter oder unrechtmäßiger Zerstörung, unbeabsichtigtem Verlust oder unbeabsichtigter Veränderung und unbefugter oder unrechtmäßiger Speicherung oder Verarbeitung, unbefugtem oder unberechtigtem Zugang oder unbefugter oder unrechtmäßiger Weitergabe und

– Sicherstellung der Umsetzung eines Sicherheitskonzepts für die Verarbeitung personenbezogener Daten.

...“

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."

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."

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. ..."

Art. 15 („Anwendung einzelner Bestimmungen der Richtlinie [95/46]“) bestimmt:

„(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 Gemeinschaftsrechts einschließlich den in Artikel 6 Absätze 1 und 2 des Vertrags über die Europäische Union niedergelegten Grundsätzen entsprechen.

...

(1b) Die Anbieter richten nach den gemäß Absatz 1 eingeführten nationalen Vorschriften interne Verfahren zur Beantwortung von Anfragen über den Zugang zu den personenbezogenen Daten der Nutzer ein. Sie stellen den zuständigen nationalen Behörden auf Anfrage Informationen über diese Verfahren, die Zahl der eingegangenen Anfragen, die vorgebrachten rechtlichen Begründungen und ihrer Antworten zur Verfügung.

(2) Die Bestimmungen des Kapitels III der Richtlinie [95/46] über Rechtsbehelfe, Haftung und Sanktionen gelten im Hinblick auf innerstaatliche Vorschriften, die nach der vorliegenden Richtlinie erlassen werden, und im Hinblick auf die aus dieser Richtlinie resultierenden individuellen Rechte.

...“

Richtlinie 95/46

Der in Kapitel III der Richtlinie 95/46 enthaltene Art. 22 hat folgenden Wortlaut:

„Unbeschadet des verwaltungsrechtlichen Beschwerdeverfahrens, das vor Beschreiten des Rechtsweges insbesondere bei der in Artikel 28 genannten Kontrollstelle eingeleitet werden kann, sehen die Mitgliedstaaten vor, dass jede Person bei der Verletzung der Rechte, die ihr durch die für die betreffende Verarbeitung geltenden einzelstaatlichen Rechtsvorschriften garantiert sind, bei Gericht einen Rechtsbehelf einlegen kann.“

Richtlinie 2006/24/EG

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 sah in ihrem Art. 1 („Gegenstand und Anwendungsbereich“) Abs. 2 vor:

„Diese Richtlinie gilt für Verkehrs- und Standortdaten sowohl von juristischen als auch von natürlichen Personen sowie für alle damit in Zusammenhang stehende Daten, die zur Feststellung des Teilnehmers oder registrierten Benutzers erforderlich sind. Sie gilt nicht für den Inhalt elektronischer Nachrichtenübermittlungen einschließlich solcher Informationen, die mit Hilfe eines elektronischen Kommunikationsnetzes abgerufen werden.“

Art. 3 der Richtlinie („Vorratsspeicherungspflicht“) lautete:

„(1) Abweichend von den Artikeln 5, 6 und 9 der Richtlinie [2002/58] tragen die Mitgliedstaaten durch entsprechende Maßnahmen dafür Sorge, dass die in Artikel 5 der vorliegenden Richtlinie genannten Daten, soweit sie im Rahmen ihrer Zuständigkeit im Zuge der Bereitstellung der betreffenden Kommunikationsdienste von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste

oder Betreibern eines öffentlichen Kommunikationsnetzes erzeugt oder verarbeitet werden, gemäß den Bestimmungen der vorliegenden Richtlinie auf Vorrat gespeichert werden.

(2) Die Verpflichtung zur Vorratsspeicherung nach Absatz 1 schließt die Vorratsspeicherung von in Artikel 5 genannten Daten im Zusammenhang mit erfolglosen Anrufversuchen ein, wenn diese Daten von den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder den Betreibern eines öffentlichen Kommunikationsnetzes im Rahmen der Zuständigkeit des betreffenden Mitgliedstaats im Zuge der Bereitstellung der betreffenden Kommunikationsdienste erzeugt oder verarbeitet und gespeichert (bei Telefoniedaten) oder protokolliert (bei Internetdaten) werden. Nach dieser Richtlinie ist die Vorratsspeicherung von Daten im Zusammenhang mit Anrufen, bei denen keine Verbindung zustande kommt, nicht erforderlich."

Schwedisches Recht

Aus der Vorlageentscheidung in der Rechtssache C-203/15 geht hervor, dass der schwedische Gesetzgeber zur Umsetzung der Richtlinie 2006/24 in nationales Recht das Lag (2003:389) om elektronisk kommunikation (Gesetz [2003:389] über die elektronische Kommunikation; im Folgenden: LEK) und die Förordning (2003:396) om elektronisk kommunikation (Verordnung [2003:396] über die elektronische Kommunikation) geändert hat. Beide Rechtstexte in ihrer auf das Ausgangsverfahren anwendbaren Fassung enthalten Vorschriften über die Vorratsspeicherung von Daten über elektronische Kommunikation und den Zugang der nationalen Behörden zu diesen Daten.

Der Zugang zu diesen Daten wird darüber hinaus geregelt durch das Lag (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (Gesetz [2012:278] über die Erfassung von Daten über die elektronische Kommunikation bei den Ermittlungstätigkeiten der Strafverfolgungsbehörden; im Folgenden: Gesetz 2012:278) und durch die Rättegångsbalk (Prozessordnung; im Folgenden: RB).

Zur Verpflichtung zur Vorratsspeicherung von Daten über elektronische Kommunikation

Nach den Angaben des vorlegenden Gerichts in der Rechtssache C-203/15 verpflichten die Bestimmungen des Kapitels 6 § 16a in Verbindung mit Kapitel 2 § 1 LEK die Anbieter elektronischer Kommunikationsdienste zur Vorratsspeicherung der Daten, für die dies in der Richtlinie 2006/24 vorgesehen war. Es handelt sich um Teilnehmeranschlussdaten und Daten in Bezug auf sämtliche elektronische Kommunikationen, die zur Rückverfolgung und Identifizierung der Quelle und des Adressaten einer Nachricht, zur Bestimmung von Datum, Uhrzeit und Dauer der Nachrichtenübermittlung, der Art einer Nachrichtenübermittlung sowie der Endeinrichtung und des Standorts mobiler Geräte bei Beginn und Ende der Nachrichtenübermittlung erforderlich sind. Die Pflicht zur Vorratsspeicherung erstreckt sich auf die Daten, die bei Telefoniediensten, bei der Mobilfunktelefonie, bei der elektronischen Nachrichtenübermittlung, beim Internetzugang und bei der Bereitstellung von Kapazität für den Internetzugang (Art der Verbindung) erzeugt oder verarbeitet werden. Diese Pflicht umfasst auch Daten über erfolglose Anrufe. Nicht eingeschlossen sind hingegen die übermittelten Inhalte.

In den §§ 38 bis 43 der Verordnung (2003:396) über die elektronische Kommunikation werden die Kategorien der zu speichernden Daten näher bestimmt. Bei Telefoniediensten müssen u. a. Daten über Anrufe und die Rufnummern sowie rückverfolgbar Datum und Uhrzeit von Beginn und Ende der Kommunikation gespeichert werden. Bei Mobiltelefonie gelten zusätzliche Pflichten, z. B. die Pflicht zur Vorratsspeicherung der Daten über den Standort zu Beginn und am Ende des Anrufs. Bei Telefoniediensten, die IP-Pakete umfassen, müssen außer den vorgenannten Daten u. a. auch die IP-Adressen des Anrufers und des Angerufenen gespeichert werden. Bei elektronischen Nachrichtenübermittlungssystemen sind u. a. die Nummern von Absender und Empfänger, die IP-Adressen oder sonstige Nachrichtenadressen zu speichern. Bei Internetzugangsdiensten müssen z. B. die IP-Adressen der Nutzer sowie rückverfolgbar Datum und Uhrzeit des Einloggens in und des Ausloggens aus dem betreffenden Dienst gespeichert werden.

Zur Dauer der Vorratsspeicherung der Daten

Nach Kapitel 6 § 16d LEK müssen die in § 16a dieses Kapitels genannten Daten von den Betreibern elektronischer Kommunikationsdienste sechs Monate ab dem Tag der Beendigung der Kommunikation auf Vorrat gespeichert werden. Danach sind sie unverzüglich zu löschen, sofern in Kapitel 6 § 16d Abs. 2 LEK nichts anderes bestimmt ist.

Zum Zugang zu den auf Vorrat gespeicherten Daten

Der Zugang zu den von den nationalen Behörden auf Vorrat gespeicherten Daten bestimmt sich nach den Vorschriften des Gesetzes 2012:278, des LEK und der RB.

– Das Gesetz 2012:278

Bei der Beschaffung von Informationen dürfen die nationale Polizeibehörde, die Säkerhetspolis (Sicherheitspolizei, Schweden) und die Tullverk (Zollbehörde, Schweden) nach § 1 des Gesetzes 2012:278 unter den in diesem Gesetz festgelegten Voraussetzungen bei einem nach dem LEK zugelassenen Betreiber elektronischer Kommunikationsnetze oder -dienste ohne dessen Wissen Daten über in einem elektronischen Kommunikationsnetz übermittelte Nachrichten, in einem bestimmten geografischen Gebiet befindliche elektronische Kommunikationsgeräte sowie das oder die geografischen Gebiete, in dem oder denen sich ein elektronisches Kommunikationsgerät befindet oder befunden hat, erfassen.

Nach den §§ 2 und 3 des Gesetzes 2012:278 dürfen die Daten grundsätzlich erfasst werden, wenn die Maßnahme nach den Umständen von besonderer Bedeutung ist für die Verhütung, Abwendung oder Feststellung krimineller Handlungen, bei denen es sich entweder um eine oder mehrere Straftaten handelt, die mit mindestens zweijährigem Freiheitsentzug geahndet werden, oder um eine der in § 3 dieses Gesetzes aufgeführten Taten, auch wenn die Strafdrohung unter zwei Jahre Freiheitsentzug beträgt. Die Gründe für die Anwendung der Maßnahme müssen schwerer wiegen als Erwägungen in Bezug auf die Beeinträchtigung oder den Schaden, die mit der Maßnahme für die Person, gegen die sie sich richtet, oder für ein entgegenstehendes Interesse verbunden sind. Nach § 5 des Gesetzes 2012:278 darf die Maßnahme nicht länger als einen Monat dauern.

Die Entscheidung über die Vornahme dieser Maßnahme wird von dem Leiter der betreffenden Behörde oder einer hierzu beauftragten Person getroffen. Sie unterliegt keiner vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsbehörde.

Nach § 6 des Gesetzes 2012:278 muss die Säkerhets och integritetsskyddsnämnd (Ausschuss für Sicherheits- und Integritätsschutz, Schweden) von jeder Entscheidung über die Erfassung von Daten in Kenntnis gesetzt werden. Nach § 1 des Lag (2007:980) om tillsyn över viss brottsbekämpande verksamhet (Gesetz [2007:980] über die Beaufsichtigung bestimmter Strafverfolgungshandlungen) hat dieser Ausschuss die Anwendung des Gesetzes durch die Strafverfolgungsbehörden zu beaufsichtigen.

– Das LEK

Nach Kapitel 6 § 22 Abs. 1 Nr. 2 des LEK hat jeder Betreiber elektronischer Kommunikationsdienste der Staatsanwaltschaft, der nationalen Polizeibehörde, der Sicherheitspolizei oder einer sonstigen mit der Kriminalitätsbekämpfung betrauten Behörde auf Verlangen Teilnehmeranschlussdaten zu übergeben, falls sich die Daten auf eine mutmaßliche Straftat beziehen. Nach den Angaben des vorlegenden Gerichts in der Rechtssache C-203/15 braucht es sich nicht um eine schwere Straftat zu handeln.

– Die RB

Die RB regelt die Übermittlung der auf Vorrat gespeicherten Daten an die nationalen Behörden im Rahmen von Voruntersuchungen. Nach Kapitel 27 § 19 der RB ist die heimliche „Überwachung elektronischer Kommunikationen“ bei Voruntersuchungen, u. a. bei solchen, die Straftaten zum Gegenstand haben, die mit einer Mindestfreiheitsstrafe von sechs Monaten bedroht sind, grundsätzlich zulässig. Unter „Überwachung elektronischer Kommunikationen“ ist nach Kapitel 27 § 19 der RB die heimliche Beschaffung von Daten zu verstehen, die sich auf Nachrichten, die über ein elektronisches Kommunikationsnetz übermittelt werden, elektronische Kommunikationsgeräte, die sich in einem bestimmten geografischen Gebiet befinden oder befunden haben, sowie das oder die geografischen

Gebiete beziehen, in dem oder denen sich ein bestimmtes elektronisches Kommunikationsgerät befindet oder befunden hat.

Nach den Angaben des vorlegenden Gerichts in der Rechtssache C-203/15 ist auf der Grundlage von Kapitel 27 § 19 der RB die Beschaffung von Informationen über den Inhalt einer Nachricht nicht möglich. Die Überwachung elektronischer Kommunikationen darf nach Kapitel 27 § 20 der RB grundsätzlich nur angeordnet werden, wenn der begründete Verdacht besteht, dass jemand eine Straftat begangen hat, und die Maßnahme für die Untersuchung von besonderer Bedeutung ist, wobei sich die Untersuchung auf eine mit einer Mindestfreiheitsstrafe von zwei Jahren bedrohte Straftat oder den Versuch, die Vorbereitung oder die Verabredung zur Begehung einer solchen Straftat beziehen muss. Nach Kapitel 27 § 21 RB hat die Staatsanwaltschaft außer bei Dringlichkeit beim zuständigen Gericht die Erlaubnis für die Überwachung der elektronischen Kommunikationsvorgänge einzuholen.

Zu Sicherheit und Schutz der auf Vorrat gespeicherten Daten

Nach Kapitel 6 § 3a des LEK müssen die zur Vorratsdatenspeicherung verpflichteten Betreiber elektronischer Kommunikationsdienste geeignete technische und organisatorische Maßnahmen treffen, um den Schutz der Daten während der Verarbeitung zu sichern. Nach den Angaben des vorlegenden Gerichts in der Rechtssache C-203/15 gibt es im schwedischen Recht jedoch keine Bestimmungen über den Ort, an dem die Daten auf Vorrat zu speichern sind.

Recht des Vereinigten Königreichs

Das DRIPA

Section 1 („Befugnis zur Schutzmaßnahmen unterliegender Vorratsspeicherung relevanter Kommunikationsdaten“) des DRIPA bestimmt:

„(1) Der [Minister des Innern] kann durch Anordnung (‚Vorratsspeicherungsanordnung‘) von einem Betreiber eines öffentlichen Telekommunikationsdienstes verlangen, relevante Kommunikationsdaten auf Vorrat zu speichern, wenn er dies für einen oder mehrere der unter Section 22(2)(a) bis (h) des Regulation of Investigatory Powers Act 2000 [Gesetz von 2000 zur Regelung von Ermittlungsbefugnissen] fallenden Zwecke für erforderlich und verhältnismäßig hält (Zwecke, für die Kommunikationsdaten beschafft werden dürfen).

(2) Eine Vorratsspeicherungsanordnung kann

(a) sich auf einen bestimmten Betreiber oder eine Kategorie von Betreibern beziehen;

(b) die Vorratsspeicherung aller Daten oder einer Kategorie von Daten vorschreiben;

(c) den Zeitraum oder Zeiträume angeben, für die Daten auf Vorrat gespeichert werden sollen;

(d) andere Erfordernisse oder Beschränkungen in Bezug auf die Vorratsdatenspeicherung enthalten;

(e) anderes für andere Zwecke vorsehen;

(f) sich auf Daten unabhängig davon beziehen, ob sie zum Zeitpunkt des Erlasses oder des Inkrafttretens der Anordnung vorhanden sind oder nicht.

(3) Der [Minister des Innern] kann durch Verordnung weitere Bestimmungen über die Vorratsspeicherung relevanter Kommunikationsdaten erlassen.

(4) Diese Bestimmungen können insbesondere Regelungen enthalten über:

(a) Voraussetzungen für den Erlass einer Vorratsspeicherungsanordnung;

(b) die Höchstdauer der auf eine Vorratsspeicherungsanordnung erfolgten Speicherung von Daten;

(c) Inhalt, Erlass, Inkrafttreten, Überprüfung, Änderung oder Aufhebung einer Vorratsspeicherungsanordnung;

(d) die Integrität, die Sicherheit oder den Schutz von, den Zugang zu oder die Offenlegung oder Zerstörung von nach dieser Section auf Vorrat gespeicherten Daten;

(e) die Durchsetzung oder Überprüfung der Einhaltung der einschlägigen Erfordernisse oder Beschränkungen;

(f) einen Verfahrenskodex bezüglich einschlägiger Erfordernisse oder Beschränkungen oder relevanter Befugnisse;

(g) die (an Bedingungen geknüpfte oder bedingungslose) Erstattung von Kosten, die Betreibern eines öffentlichen Telekommunikationsdienstes dadurch entstehen, dass sie sich an die einschlägigen Erfordernisse oder Beschränkungen halten, durch den [Minister des Innern];

(h) das Außerkrafttreten der [Data Retention (EC Directive) Regulations 2009 (Verordnung von 2009 zur Vorratsdatenspeicherung im Sinne der EG-Richtlinie)] und den Übergang zur Vorratsdatenspeicherung nach dieser Section.

(5) Die Höchstdauer nach Subsection (4)(b) darf zwölf Monate nicht überschreiten, beginnend mit dem Tag, der in Bezug auf die betreffenden Daten in der Verordnung nach Subsection (3) festgelegt ist.

...“

Section 2 des DRIPA definiert „relevante Kommunikationsdaten“ als „Kommunikationsdaten der im Anhang der Verordnung von 2009 [zur Vorratsdatenspeicherung im Sinne der EG-Richtlinie] genannten Art, soweit solche Daten im Vereinigten Königreich von Betreibern eines öffentlichen Telekommunikationsdienstes bei der Bereitstellung der betroffenen Telekommunikationsdienste erzeugt oder verarbeitet werden“.

Das RIPA

Section 21 („Rechtmäßige Erlangung und Offenlegung von Kommunikationsdaten“) in Kapitel II des Gesetzes von 2000 zur Regelung von Ermittlungsbefugnissen (im Folgenden: RIPA) sieht in Subsection (4) vor:

„In diesem Kapitel werden vom Begriff ‚Kommunikationsdaten‘ erfasst:

(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

(i) eines Post- oder Telekommunikationsdienstes durch eine Person oder

(ii) irgendeines Teils eines Telekommunikationssystems durch eine Person 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.“

Nach den Angaben in der Vorlageentscheidung in der Rechtssache C-698/15 schließen diese Daten die „Standortdaten eines Nutzers“ ein, nicht aber Daten über den Inhalt einer Kommunikation.

Bezüglich des Zugangs zu den auf Vorrat gespeicherten Daten sieht Section 22 RIPA vor:

„(1) Die vorliegende Section findet Anwendung, wenn eine für die Zwecke dieses Kapitels benannte Person aus unter Subsection (2) fallenden Gründen die Beschaffung von Kommunikationsdaten für erforderlich hält.

(2) Die Beschaffung von Kommunikationsdaten ist aus unter diese Subsection fallenden Gründen erforderlich, wenn dies erforderlich ist

(a) im Interesse der nationalen Sicherheit;

(b) zur Vorbeugung oder Aufdeckung von Straftaten oder zur Verhütung von Störungen der öffentlichen Ordnung;

(c) im Interesse des wirtschaftlichen Wohls des Vereinigten Königreichs;

(d) im Interesse der öffentlichen Sicherheit;

(e) zum Schutz der öffentlichen Gesundheit;

(f) zur Festsetzung oder Erhebung von Steuern, Zöllen, Abgaben oder anderen Lasten, Beiträgen oder Gebühren, die an eine staatliche Stelle zu entrichten sind;

(g) um im Notfall den Tod oder eine Verletzung oder jegliche Schädigung der physischen oder psychischen Gesundheit einer Person zu verhindern oder eine Verletzung oder Schädigung der physischen oder psychischen Gesundheit einer Person zu lindern;

(h) zu jedem (nicht unter die vorstehenden Buchst. a bis g fallenden) Zweck, der in einer Verordnung des [Ministers der Innern] eigens aufgeführt wird.

(4) Vorbehaltlich Subsection (5) kann die benannte Person, wenn sie meint, dass der Betreiber eines Post- oder Telekommunikationsdienstes im Besitz von Kommunikationsdaten ist oder sein kann oder sich diese beschaffen kann, von diesem Betreiber durch eine an ihn gerichtete Anordnung verlangen, dass er

(a) – wenn er noch nicht im Besitz der Daten ist – sich diese Daten beschafft und

(b) in jedem Fall sämtliche sich in seinem Besitz befindlichen oder von ihm später beschafften Daten offenlegt.

(5) Die benannte Person darf nur dann eine Erlaubnis nach Subsection (3) erteilen oder eine Anordnung nach Subsection (4) erlassen, wenn sie der Auffassung ist, dass die Beschaffung der betreffenden Daten durch das erlaubte oder mit der Erlaubnis oder Anordnung verlangte Vorgehen zu dem Ziel, das mit dieser Beschaffung der Daten erreicht werden soll, im Verhältnis steht.“

Nach Section 65 RIPA kann beim Investigatory Powers Tribunal (Gericht für Ermittlungsbefugnisse, Vereinigtes Königreich) Beschwerde erhoben werden, wenn Grund zur Annahme besteht, dass Daten auf unangemessene Weise beschafft wurden.

Die Data Retention Regulations 2014

Die auf der Grundlage des DRIPA erlassenen Data Retention Regulations 2014 (Verordnung von 2014 über die Vorratsdatenspeicherung) bestehen aus drei Teilen. Der zweite Teil umfasst die Regulations (2) bis (14). In Regulation (4) („Vorratsspeicherungsanordnungen“) heißt es:

„(1) In einer Vorratsspeicherungsanordnung sind anzugeben:

(a) der Betreiber des öffentlichen Kommunikationsdienstes (oder eine Kategorie von Betreibern), an den (oder die) die Anordnung gerichtet ist;

(b) die relevanten Kommunikationsdaten, die auf Vorrat gespeichert werden sollen;

(c) der Zeitraum oder die Zeiträume, für die die Daten auf Vorrat gespeichert werden sollen;

(d) andere Erfordernisse oder Beschränkungen in Bezug auf die Vorratsspeicherung der Daten.

(2) Mit einer Vorratsspeicherungsanordnung kann keine über einen Zeitraum von als zwölf Monaten hinausgehende Speicherung verlangt werden; dieser Zeitraum beginnt

(a) bei Verkehrsdaten oder Daten in Bezug auf die Nutzung des Dienstes mit dem Tag der betreffenden Kommunikation und

(b) bei Teilnehmerdaten mit dem Tag, an dem die betreffende Person den in Rede stehenden Kommunikationsdienst verlässt, oder (wenn früher der Fall) mit dem Tag, an dem die Daten geändert werden.

...“

Regulation (7) („Integrität und Sicherheit von Daten“) der Verordnung sieht vor:

„(1) Der Betreiber eines öffentlichen Kommunikationsdienstes, der nach Section 1 des [DRIPA] Kommunikationsdaten auf Vorrat speichert, muss

(a) sicherstellen, dass die Daten dieselbe Integrität aufweisen und denselben Sicherheits- und Schutzstandards unterworfen sind wie die Daten in dem System, aus dem sie stammen;

(b) durch geeignete technische und organisatorische Maßnahmen sicherstellen, dass nur eigens ermächtigte Personen Zugang zu den Daten haben, und

(c) die Daten durch geeignete technische und organisatorische Maßnahmen vor versehentlicher oder rechtswidriger Zerstörung, vor versehentlichem Verlust oder versehentlicher Veränderung und vor unerlaubter oder rechtswidriger Vorratsspeicherung, Verarbeitung, Zugänglichmachung oder Offenlegung schützen.

(2) Der Betreiber eines öffentlichen Kommunikationsdienstes, der nach Section 1 des [DRIPA] Kommunikationsdaten auf Vorrat speichert, muss die Daten vernichten, wenn deren Vorratsspeicherung nach dieser Section nicht mehr gestattet und nicht anderweitig durch Gesetz erlaubt ist.

(3) Das in Subsection (2) vorgesehene Erfordernis einer Vernichtung der Daten ist ein Erfordernis, die Daten in der Weise zu löschen, dass kein Zugang zu ihnen mehr möglich ist.

(4) Es reicht aus, wenn der Betreiber Vorkehrungen trifft, dass die Daten monatlich oder in kürzeren Zeitabständen gelöscht werden, wie es dem Betreiber praktikabel erscheint.“

Regulation (8) („Offenlegung von auf Vorrat gespeicherten Daten“) der Verordnung bestimmt:

„(1) Der Betreiber eines öffentlichen Kommunikationsdienstes muss angemessene Sicherheitssysteme (einschließlich technischer und organisatorischer Maßnahmen) zur Regelung des Zugangs zu den auf Vorrat gespeicherten Kommunikationsdaten einrichten, um eine nicht unter Section 1(6)(a) des [DRIPA] fallende Offenlegung der Daten zu verhindern.

(2) Der Betreiber eines öffentlichen Kommunikationsdienstes, der nach Section 1 des [DRIPA] Kommunikationsdaten auf Vorrat speichert, muss die Daten in der Weise auf Vorrat speichern, dass er sie auf Verlangen unverzüglich übermitteln kann.“

Regulation (9) („Überwachung durch den Datenschutzbeauftragten“) der Verordnung lautet:

„Der Datenschutzbeauftragte muss die Einhaltung der in diesem Teil in Bezug auf die Integrität, Sicherheit oder Vernichtung von nach Section 1 des [DRIPA] auf Vorrat gespeicherten Daten kontrollieren."

Der Verfahrenskodex

Der Acquisition and Disclosure of Communications Data Code of Practice (Verfahrenskodex für die Beschaffung und Offenlegung von Kommunikationsdaten; im Folgenden: Verfahrenskodex) enthält in den Abschnitten 2.5 bis 2.9 und 2.36 bis 2.45 Hinweise zur Erforderlichkeit und Verhältnismäßigkeit der Beschaffung von Kommunikationsdaten. Nach den Erläuterungen des vorlegenden Gerichts in der Rechtssache C-698/15 muss gemäß den Abschnitten 3.72 bis 3.77 des Verfahrenskodexes besondere Aufmerksamkeit der Erforderlichkeit und der Verhältnismäßigkeit gelten, wenn sich die angefragten Daten auf eine Person beziehen, die Mitglied eines Berufsstands ist, der mit unter dem Schutz des Berufsgeheimnisses stehenden oder anderweitig vertraulichen Informationen umgeht.

In dem besonderen Fall, dass ein Antrag in Bezug auf Kommunikationsdaten gestellt wird, um die Quelle von Journalisten herauszufinden, ist nach den Abschnitten 3.78 bis 3.84 des Verfahrenskodexes ein Gerichtsbeschluss erforderlich. Gemäß den Abschnitten 3.85 bis 3.87 des Kodexes ist eine gerichtliche Genehmigung erforderlich, wenn Kommunalbehörden den Zugang beantragen. Hingegen ist keine Genehmigung durch ein Gericht oder eine unabhängige Stelle für den Zugang zu Kommunikationsdaten erforderlich, die unter dem Schutz eines gesetzlichen Berufsgeheimnisses stehen oder sich auf Ärzte, Mitglieder des Parlaments oder Geistliche beziehen.

Gemäß Abschnitt 7.1 des Verfahrenskodexes müssen nach den Bestimmungen des RIPA erlangte oder beschaffte Kommunikationsdaten sowie sämtliche Auszüge, Zusammenfassungen und Kopien dieser Daten auf sichere Weise verarbeitet und gespeichert werden. Zudem müssen die Erfordernisse des Data Protection Act (Datenschutzgesetz) beachtet werden.

Nach Abschnitt 7.18 des Verfahrenskodexes muss eine Behörde des Vereinigten Königreichs, wenn sie eine Offenlegung von Kommunikationsdaten an ausländische Behörden erwägt, u. a. prüfen, ob diese Daten dort angemessen geschützt werden. Nach Abschnitt 7.22 des Verfahrenskodexes dürfen Daten in Drittstaaten übermittelt werden, sofern dies aus Gründen, die mit einem wichtigen öffentlichen Interesse in Zusammenhang stehen, erforderlich ist, selbst wenn der Drittstaat kein angemessenes Schutzniveau gewährleistet. Nach den Angaben des vorlegenden Gerichts in der Rechtssache C-698/15 kann der Minister des Innern eine nationale Sicherheitsbescheinigung ausstellen, aufgrund deren bei bestimmten Daten von der Einhaltung der gesetzlichen Bestimmungen abgesehen werden kann.

In Abschnitt 8.1 des Verfahrenskodexes wird darauf hingewiesen, dass mit dem RIPA das Amt des Interception of Communications Commissioner (Beauftragter für das Abfangen von Nachrichten, Vereinigtes Königreich) geschaffen wurde, zu dessen Aufgabe u. a. die unabhängige Überwachung der Ausübung und Durchführung der in Kapitel II von Teil I des DRIPA vorgesehenen Befugnisse und Pflichten gehört. Wie aus Abschnitt 8.3 des Verfahrenskodexes hervorgeht, darf der Beauftragte, wenn er „feststellen sollte, dass eine Person durch ein vorsätzliches oder fahrlässiges Fehlverhalten ... beeinträchtigt worden ist", den Betroffenen davon in Kenntnis setzen, dass der Verdacht eines Missbrauchs von Befugnissen besteht.

Ausgangsverfahren und Vorlagefragen

Rechtssache C-203/15

Am 9. April 2014 teilte Tele2 Sverige, ein in Schweden ansässiger Betreiber elektronischer Kommunikationsdienste, der PTS mit, dass sie infolge 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, im Folgenden: Urteil Digital Rights, EU:C:2014:238) ab dem 14. April 2014 die vom LEK erfassten elektronischen Kommunikationsdaten nicht mehr auf Vorrat speichern und die bis dahin gespeicherten Daten löschen werde.

Am 15. April 2014 beschwerte sich die Rikspolisstyrels (Reichspolizeidirektion, Schweden) bei der PTS darüber, dass Tele2 Sverige ihr die betreffenden Daten nicht mehr mitteile.

Am 29. April 2014 beauftragte der Justitieminister (Minister der Justiz, Schweden) einen Sondergutachter damit, die einschlägige schwedische Regelung im Hinblick auf das Urteil Digital Rights zu prüfen. In einem Bericht Ds 2014:23 vom 13. Juni 2014 („Datalagring, EU-rätten och svensk rätt“ [Vorratsdatenspeicherung, Unionsrecht und schwedisches Recht], im Folgenden: Bericht von 2014) gelangte der Sondergutachter zu dem Schluss, dass die nationale Regelung über die Vorratsdatenspeicherung in den §§ 16 bis 16f des LEK weder gegen das Unionsrecht noch gegen die am 4. November 1950 in Rom unterzeichnete Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK) verstoße. Nach Auffassung des Sondergutachters kann das Urteil Digital Rights nicht dahin ausgelegt werden, dass es einer allgemeinen und unterschiedslosen Vorratsdatenspeicherung grundsätzlich entgegenstehe. Es dürfe auch nicht dahin verstanden werden, dass der Gerichtshof darin eine Reihe von Kriterien aufgestellt habe, die alle erfüllt sein müssten, damit eine Regelung als verhältnismäßig angesehen werden könne. Bei der Feststellung, ob die schwedische Regelung mit dem Unionsrecht vereinbar sei, müssten alle Umstände berücksichtigt werden, wie der Umfang der Vorratsdatenspeicherung im Hinblick auf die Bestimmungen über den Zugang zu den Daten, über die Dauer ihrer Speicherung, über ihren Schutz sowie über ihre Sicherheit.

Aufgrund dessen teilte die PTS am 19. Juni 2014 Tele2 Sverige mit, dass sie gegen ihre Pflichten aus der nationalen Regelung verstoße, indem sie die unter das LEK fallenden Daten nicht für Zwecke der Kriminalitätsbekämpfung für sechs Monate auf Vorrat speichere. Mit Verfügung vom 27. Juni 2014 gab die PTS ihr auf, diese Daten spätestens ab dem 25. Juli 2014 auf Vorrat zu speichern.

Da Tele2 Sverige der Ansicht war, dass dem Bericht von 2014 eine unzutreffende Lesart des Urteils Digital Rights zugrunde liege und die Pflicht zur Vorratsspeicherung der Daten gegen die durch die Charta gewährleisteten Grundrechte verstoße, erhob sie gegen die Verfügung vom 27. Juni 2014 Klage beim Förvaltningsrätt i Stockholm (Verwaltungsgericht Stockholm, Schweden). Nachdem die Klage mit Urteil vom 13. Oktober 2014 abgewiesen worden war, legte Tele2 Sverige Berufung beim vorlegenden Gericht ein.

Nach Ansicht des vorlegenden Gerichts ist die Vereinbarkeit der schwedischen Regelung mit dem Unionsrecht anhand von Art. 15 Abs. 1 der Richtlinie 2002/58 zu beurteilen. Denn diese Richtlinie stelle zwar den Grundsatz auf, dass Verkehrs- und Standortdaten zu löschen oder zu anonymisieren seien, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt würden. Ihr Art. 15 Abs. 1 schaffe aber eine Ausnahme von diesem Grundsatz, da er die Mitgliedstaaten ermächtige, die Pflicht zur Löschung oder Anonymisierung zu beschränken oder sogar eine Vorratsdatenspeicherung vorzusehen, wenn dies aus den in dieser Bestimmung genannten Gründen gerechtfertigt sei. Nach dem Unionsrecht sei somit in bestimmten Fällen die Vorratsspeicherung elektronischer Kommunikationsdaten zulässig.

Dem vorlegenden Gericht stellt sich jedoch die Frage, ob eine allgemeine und unterschiedslose Pflicht zur Vorratsspeicherung elektronischer Kommunikationsdaten, wie sie im Ausgangsverfahren in Rede steht, mit Rücksicht auf das Urteil Digital Rights mit Art. 15 Abs. 1 der Richtlinie 2002/58, im Licht der Art. 7 und 8 sowie des Art. 52 Abs. 1 der Charta betrachtet, vereinbar ist. Im Hinblick auf die insoweit divergierenden Ansichten der Parteien wäre es angebracht, dass der Gerichtshof in eindeutiger Weise darüber befinde, ob – wie Tele2 Sverige meine – die allgemeine und unterschiedslose Vorratsspeicherung elektronischer Kommunikationsdaten als solche mit den Art. 7 und 8 sowie Art. 52 Abs. 1 der Charta unvereinbar sei oder aber ob, wie sich aus dem Bericht von 2014 ergebe, die Vereinbarkeit einer solchen Vorratsdatenspeicherung nach den Bestimmungen über den Zugang zu den Daten, über ihren Schutz, über ihre Sicherheit sowie über die Dauer ihrer Speicherung beurteilt werden müsse.

Unter diesen Umständen hat das vorlegende Gericht beschlossen, das Verfahren auszusetzen und dem Gerichtshof folgende Fragen zur Vorabentscheidung vorzulegen:

1. Ist eine generelle Verpflichtung zur Vorratsspeicherung von Verkehrsdaten, die sich auf alle Personen und alle elektronischen Kommunikationsmittel sowie auf sämtliche Verkehrsdaten erstreckt, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des Ziels der Bekämpfung von Straftaten vorzusehen, mit Art. 15 Abs. 1 der Richtlinie 2002/58 unter Berücksichtigung der Art. 7, 8 und 52 Abs. 1 der Charta vereinbar?

2. Falls die erste Frage zu verneinen ist, kann die Vorratsspeicherung dennoch zulässig sein, wenn

a) der Zugang der nationalen Behörden zu den gespeicherten Daten wie in den Nrn. 19 bis 36 der Vorlageentscheidung beschrieben festgelegt ist und

b) die Sicherheitsanforderungen wie in den Nrn. 38 bis 43 der Vorlageentscheidung beschrieben geregelt sind und

c) sämtliche relevanten Daten wie in Nr. 37 der Vorlageentscheidung beschrieben für einen Zeitraum von sechs Monaten ab dem Tag, an dem die Kommunikation beendet wird, gespeichert und anschließend gelöscht werden müssen?

Rechtssache C-698/15

Herr Watson, Herr Brice und Herr Lewis erhoben beim High Court of Justice (England & Wales), Queens' Bench Division (Divisional Court) (Hoher Gerichtshof [England und Wales], Abteilung Queen's Bench, Vereinigtes Königreich) jeweils Klage auf Überprüfung der Rechtmäßigkeit von Section 1 des DRIPA und machten insbesondere geltend, dass diese Section mit den Art. 7 und 8 der Charta sowie mit Art. 8 EMRK unvereinbar sei.

Mit Urteil vom 17. Juli 2015 stellte der High Court of Justice (England & Wales), Queens' Bench Division (Divisional Court) (Hoher Gerichtshof [England und Wales], Abteilung Queen's Bench) fest, dass das Urteil Digital Rights „verbindliche unionsrechtliche Voraussetzungen" für die Regelungen der Mitgliedstaaten über die Vorratsspeicherung von Kommunikationsdaten und den Zugang zu solchen Daten festlege. Da der Gerichtshof in diesem Urteil angenommen habe, dass die Richtlinie 2006/24 mit dem Grundsatz der Verhältnismäßigkeit unvereinbar sei, lasse sich eine nationale Regelung gleichen Inhalts wie diese Richtlinie ebenfalls nicht mit dem Verhältnismäßigkeitsgrundsatz vereinbaren. Aus der dem Urteil Digital Rights zugrunde liegenden Logik ergebe sich, dass Rechtsvorschriften, mit denen eine allgemeine Regelung für die Vorratsspeicherung von Kommunikationsdaten geschaffen werde, gegen die in den Art. 7 und 8 der Charta gewährleisteten Rechte verstoße, sofern diese Rechtsvorschriften nicht durch eine im nationalen Recht festgelegte Regelung über den Zugang zu den Daten ergänzt werde, die ausreichende Garantien für die Wahrung dieser Rechte vorsehe. Section 1 des DRIPA sei folglich nicht mit den Art. 7 und 8 der Charta vereinbar, da sie keine klaren und präzisen Regeln für den Zugang zu den auf Vorrat gespeicherten Daten und über deren Nutzung aufstelle und den Zugang zu diesen Daten nicht von einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle abhängig mache.

Der Minister des Innern legte gegen dieses Urteil Rechtsmittel beim Court of Appeal (England & Wales) (Civil Division) (Berufungsgericht [England und Wales] [Abteilung für Zivilsachen], Vereinigtes Königreich) ein.

Dieses Gericht weist darauf hin, dass Section 1(1) des DRIPA den Minister des Innern ermächtige, ohne jede vorherige Genehmigung durch ein Gericht oder eine unabhängige Verwaltungsstelle eine allgemeine Regelung zu erlassen, die den Betreibern öffentlicher Kommunikationsdienste vorschreibe, alle Daten in Bezug auf sämtliche Post- oder Telekommunikationsdienste für längstens zwölf Monate auf Vorrat zu speichern, sofern er dies zur Verfolgung der in der Regelung des Vereinigten Königreichs genannten Ziele für erforderlich und verhältnismäßig halte. Auch wenn diese Daten nicht den Inhalt einer Kommunikation einschlössen, könnten sie doch einen erheblichen Eingriff in die Privatsphäre der Nutzer von Kommunikationsdienstleistungen darstellen.

Das vorlegende Gericht ging in der Vorlageentscheidung und in seinem im Rahmen des Rechtsmittelverfahrens erlassenen Urteil vom 20. November 2015, mit dem es beschlossen hat, das vorliegende Vorabentscheidungsersuchen an den Gerichtshof zu richten, davon aus, dass die nationalen Vorschriften über die Vorratsdatenspeicherung zwangsläufig unter Art. 15 Abs. 1 der Richtlinie 2002/58 fielen und daher die sich aus der Charta ergebenden Erfordernisse beachten müssten. Allerdings habe nach Art. 1 Abs. 3 der Richtlinie der Unionsgesetzgeber die Regeln für den Zugang zu den auf Vorrat gespeicherten Daten nicht harmonisiert.

Hinsichtlich der Auswirkungen des Urteils Digital Rights auf die im Ausgangsverfahren aufgeworfenen Fragen weist das vorlegende Gericht darauf hin, dass der Gerichtshof in der Rechtssache, die zu diesem Urteil geführt habe, mit der Gültigkeit der Richtlinie 2006/24 und nicht mit der Gültigkeit einer nationalen

Regelung befasst gewesen sei. In Anbetracht u. a. des engen Zusammenhangs zwischen der Vorratsspeicherung von Daten und dem Zugang zu diesen Daten wäre es unbedingt erforderlich gewesen, dass die Richtlinie mit einer Reihe von Garantien einhergegangen wäre und das Urteil Digital Rights bei der Prüfung der Rechtmäßigkeit der mit der Richtlinie geschaffenen Regelung zur Vorratsdatenspeicherung auf die Regeln für den Zugang zu diesen Daten eingegangen wäre. Der Gerichtshof habe daher nicht beabsichtigt, in diesem Urteil zwingende Erfordernisse für nationale Regelungen über den Zugang zu Daten aufzustellen, mit denen nicht Unionsrecht umgesetzt werde. Außerdem hätten die Erwägungen des Gerichtshofs in engem Zusammenhang mit dem Ziel gestanden, das mit der Richtlinie selbst verfolgt worden sei. Eine nationale Regelung müsse jedoch im Hinblick auf die mit ihr verfolgten Ziele und ihren Kontext beurteilt werden.

Hinsichtlich der Erforderlichkeit eines Vorabentscheidungsersuchens an den Gerichtshof hebt das vorlegende Gericht hervor, dass zum Zeitpunkt des Erlasses der Vorlageentscheidung sechs Gerichte anderer Mitgliedstaaten, darunter fünf letztinstanzliche Gerichte, nationale Rechtsvorschriften gestützt auf das Urteil Digital Rights für nichtig erklärt hätten. Die Antwort auf die aufgeworfenen Fragen sei daher nicht offensichtlich, während sie für die Entscheidung der bei diesem Gericht anhängigen Rechtssachen erforderlich sei.

Daher hat der Court of Appeal (England & Wales) (Civil Division) (Berufungsgericht [England und Wales] [Abteilung für Zivilsachen], Vereinigtes Königreich) beschlossen, das Verfahren auszusetzen und dem Gerichtshof folgende Fragen zur Vorabentscheidung vorzulegen:

1. Legt das Urteil Digital Rights (einschließlich insbesondere seiner Rn. 60 bis 62) verbindliche, für die nationale Regelung eines Mitgliedstaats über den Zugang zu gemäß den nationalen Rechtsvorschriften auf Vorrat gespeicherten Daten geltende Voraussetzungen für die Vereinbarkeit mit den Art. 7 und 8 der Charta fest?

2. Erweitert das Urteil Digital Rights die Reichweite von Art. 7 und/oder Art. 8 der Charta über die von Art. 8 EMRK, wie sie in der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte festgestellt ist, hinaus?

Zum Verfahren vor dem Gerichtshof

Mit Beschluss vom 1. Februar 2016, Davis u. a. (C-698/15, nicht veröffentlicht, EU:C:2016:70), hat der Präsident des Gerichtshofs dem Antrag des Court of Appeal (England & Wales) (Civil Division) (Berufungsgericht [England und Wales] [Abteilung für Zivilsachen]) stattgegeben, die Rechtssache C-698/15 dem beschleunigten Verfahren des Art. 105 Abs. 1 der Verfahrensordnung des Gerichtshofs zu unterwerfen.

Mit Beschluss des Präsidenten des Gerichtshofs vom 10. März 2016 sind die Rechtssachen C-203/15 und C-698/15 zu gemeinsamem mündlichen Verfahren und zu gemeinsamer Entscheidung verbunden worden.

Zu den Vorlagefragen

Zur ersten Frage in der Rechtssache C-203/15

Mit der ersten Frage in der Rechtssache C-203/15 möchte der Kammarrätt i Stockholm (Oberverwaltungsgericht Stockholm) wissen, ob Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7 und 8 sowie des Art. 52 Abs. 1 der Charta dahin auszulegen ist, dass er einer nationalen Regelung wie der im Ausgangsverfahren streitigen entgegensteht, die für Zwecke der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsieht.

Diese Frage geht u. a. darauf zurück, dass die Richtlinie 2006/24, die mit der im Ausgangsverfahren in Rede stehenden nationalen Regelung umgesetzt werden sollte, mit dem Urteil Digital Rights für ungültig erklärt wurde, die Parteien aber uneins sind über die Tragweite dieses Urteils und seine Auswirkungen auf die nationale Regelung, die für die Vorratsspeicherung von Verkehrs- und Standortdaten sowie für den Zugang der nationalen Behörden zu diesen Daten gilt.

Zunächst ist zu prüfen, ob eine nationale Regelung wie die im Ausgangsverfahren in Rede stehende in den Anwendungsbereich des Unionsrechts fällt.

Zum Geltungsbereich der Richtlinie 2002/58

Die Mitgliedstaaten, die beim Gerichtshof schriftliche Erklärungen eingereicht haben, vertreten unterschiedliche Standpunkte zu der Frage, ob und inwieweit nationale Regelungen über die Vorratsspeicherung von Verkehrs- und Standortdaten sowie den Zugang der nationalen Behörden zu diesen Daten für Zwecke der Kriminalitätsbekämpfung in den Geltungsbereich der Richtlinie 2002/58 fallen. Während namentlich die belgische, die dänische, die deutsche und die estnische Regierung, Irland und die niederländische Regierung sich dafür ausgesprochen haben, diese Frage zu bejahen, hat die tschechische Regierung vorgeschlagen, sie zu verneinen, weil alleiniger Zweck dieser Regelungen die Kriminalitätsbekämpfung sei. Die Regierung des Vereinigten Königreichs macht geltend, dass in den Geltungsbereich dieser Richtlinie nur Regelungen über die Vorratsdatenspeicherung fielen, nicht aber Regelungen über den Zugang zu den gespeicherten Daten durch die nationalen Strafverfolgungsbehörden.

Die Kommission schließlich hat zwar in ihren schriftlichen Erklärungen, die sie beim Gerichtshof in der Rechtssache C-203/15 eingereicht hat, die Ansicht vertreten, dass die im Ausgangsverfahren streitige nationale Regelung in den Geltungsbereich der Richtlinie 2002/58 falle. In ihren schriftlichen Erklärungen in der Rechtssache C-698/15 hingegen hat sie vorgetragen, dass nur nationale Vorschriften über die Vorratsspeicherung von Daten, nicht aber solche über den Zugang der nationalen Behörden zu diesen Daten in den Geltungsbereich der Richtlinie fielen. Diese letztgenannten Vorschriften müssten gleichwohl berücksichtigt werden, um zu beurteilen, ob eine nationale Regelung über die Vorratsdatenspeicherung durch Betreiber elektronischer Kommunikationsdienste einen unverhältnismäßigen Eingriff in die durch die Art. 7 und 8 der Charta gewährleisteten Grundrechte darstelle.

Insoweit ist darauf hinzuweisen, dass für die Bestimmung der Reichweite des Geltungsbereichs der Richtlinie 2002/58 insbesondere deren Systematik zu berücksichtigen ist.

Die Richtlinie 2002/58 sieht nach ihrem Art. 1 Abs. 1 u. a. 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 zu gewährleisten.

Art. 1 Abs. 3 dieser Richtlinie schließt von ihrem Geltungsbereich die „Tätigkeiten des Staates“ in den dort genannten Bereichen aus, d. h. namentlich die Tätigkeiten des Staates im strafrechtlichen Bereich sowie Tätigkeiten betreffend die öffentliche Sicherheit, die Landesverteidigung und die Sicherheit des Staates, einschließlich seines wirtschaftlichen Wohls, wenn die Tätigkeit die Sicherheit des Staates berührt (vgl. entsprechend, zu Art. 3 Abs. 2 erster Gedankenstrich der Richtlinie 95/46, Urteile vom 6. November 2003, Lindqvist, C-101/01, EU:C:2003:596, Rn. 43, sowie vom 16. Dezember 2008, Satakunnan Markkinapörssi und Satamedia, C-73/07, EU:C:2008:727, Rn. 41).

Nach Art. 3 der Richtlinie 2002/58 gilt diese 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.

Nach Art. 15 Abs. 1 der Richtlinie 2002/58 können die Mitgliedstaaten unter den 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“. Art. 15 Abs. 1 Satz 2 der Richtlinie nennt als Beispiel für Vorschriften, die so von den Mitgliedstaaten erlassen werden können, Vorschriften, die „vorsehen, dass Daten ... aufbewahrt werden“.

Zwar beziehen sich die Rechtsvorschriften, um die es in Art. 15 Abs. 1 der Richtlinie 2002/58 geht, auf spezifische Tätigkeiten der Staaten oder der staatlichen Stellen, die mit den Tätigkeitsbereichen von Einzelpersonen nichts zu tun haben (vgl. in diesem Sinne Urteil vom 29. Januar 2008, Promusicae,

C-275/06, EU:C:2008:54, Rn. 51). Zudem decken sich die Zweckbestimmungen, denen die Rechtsvorschriften nach dieser Bestimmung entsprechen müssen – Schutz der nationalen Sicherheit, der Landesverteidigung und der öffentlichen Sicherheit sowie Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen –, im Wesentlichen mit den Zielen, die mit den in Art. 1 Abs. 3 der Richtlinie genannten Tätigkeiten verfolgt werden.

In Anbetracht der Systematik der Richtlinie 2002/58 erlauben jedoch die in der vorstehenden Randnummer dieses Urteils genannten Gesichtspunkte nicht den Schluss, dass die Rechtsvorschriften im Sinne des Art. 15 Abs. 1 dieser Richtlinie von deren Geltungsbereich ausgeschlossen sind, da dieser Bestimmung damit jede praktische Wirksamkeit genommen würde. Art. 15 Abs. 1 der Richtlinie 2002/58 setzt nämlich zwangsläufig voraus, dass die dort genannten nationalen Vorschriften, wie Vorschriften über die Aufbewahrung von Daten für Zwecke der Kriminalitätsbekämpfung, in den Geltungsbereich der Richtlinie fallen, da diese Richtlinie die Mitgliedstaaten zum Erlass solcher Vorschriften ausdrücklich nur dann ermächtigt, wenn die darin vorgesehenen Voraussetzungen eingehalten werden.

Außerdem regeln die in Art. 15 Abs. 1 der Richtlinie 2002/58 genannten Rechtsvorschriften – zu den in dieser Bestimmung genannten Zwecken – die Tätigkeit der Betreiber elektronischer Kommunikationsdienste. Demnach ist Art. 15 Abs. 1 in Verbindung mit Art. 3 der Richtlinie 2002/58 dahin auszulegen, dass diese Rechtsvorschriften in den Geltungsbereich dieser Richtlinie fallen.

In ihren Geltungsbereich fällt insbesondere eine Rechtsvorschrift wie die im Ausgangsverfahren in Rede stehende, die den Betreibern elektronischer Kommunikationsdienste vorschreibt, die Verkehrs- und Standortdaten auf Vorrat zu speichern, da damit zwangsläufig eine Verarbeitung personenbezogener Daten durch die Betreiber verbunden ist.

Ebenfalls in ihren Geltungsbereich fällt eine Rechtsvorschrift, die, wie im Ausgangsverfahren, den Zugang der nationalen Behörden zu den von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten Daten betrifft.

Der in Art. 5 Abs. 1 der Richtlinie 2002/58 garantierte Schutz der Vertraulichkeit elektronischer Kommunikationen und der damit verbundenen Verkehrsdaten gilt nämlich für Maßnahmen sämtlicher anderer Personen als der Nutzer, unabhängig davon, ob es sich um private Personen oder Einrichtungen oder um staatliche Einrichtungen handelt. Wie ihr 21. Erwägungsgrund bestätigt, soll die Richtlinie 2002/58 jeden unerlaubten Zugang zu Nachrichten einschließlich zu „mit ihnen verbundenen Daten“ verhindern, um die Vertraulichkeit elektronischer Kommunikationen zu schützen.

Daher betrifft eine Rechtsvorschrift, mit der ein Mitgliedstaat den Betreibern elektronischer Kommunikationsdienste auf der Grundlage von Art. 15 Abs. 1 der Richtlinie 2002/58 zu den in dieser Bestimmung genannten Zwecken vorschreibt, den nationalen Behörden unter in der betreffenden Rechtsvorschrift vorgesehenen Voraussetzungen den Zugang zu den von ihnen gespeicherten Daten zu gewähren, die Verarbeitung personenbezogener Daten durch die Betreiber, und eine solche Verarbeitung fällt in den Geltungsbereich dieser Richtlinie.

Grundsätzlich setzt eine nationale Regelung über die Vorratsdatenspeicherung, da diese allein zu dem Zweck erfolgt, die Daten gegebenenfalls den zuständigen nationalen Behörden zugänglich zu machen, zwangsläufig voraus, dass es Bestimmungen über den Zugang dieser Behörden zu den von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten Daten gibt.

Diese Auslegung wird durch Art. 15 Abs. 1b der Richtlinie 2002/58 gestützt, wonach die Betreiber nach den gemäß Art. 15 Abs. 1 der Richtlinie eingeführten nationalen Vorschriften interne Verfahren zur Beantwortung von Anfragen über den Zugang zu den personenbezogenen Daten der Nutzer einrichten.

Nach alledem fällt eine nationale Regelung, wie sie in den Ausgangsverfahren der Rechtssachen C-203/15 und C-698/15 in Rede steht, in den Geltungsbereich der Richtlinie 2002/58.

Zur Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58 im Hinblick auf die Art. 7, 8 und 11 sowie Art. 52 Abs. 1 der Charta

Nach Art. 1 Abs. 2 der Richtlinie 2002/58 stellen ihre Bestimmungen eine „Detaillierung und Ergänzung“ der Richtlinie 95/46 dar. Wie in ihrem zweiten Erwägungsgrund zum Ausdruck gebracht wird, soll mit der Richtlinie 2002/58 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 endgültig), aus dem die Richtlinie 2002/58 hervorgegangen ist, dass der Unionsgesetzgeber beabsichtigte, „sicher[zu]stellen, dass für alle elektronischen Kommunikationsdienste unabhängig von der zugrunde liegenden Technologie weiterhin ein hochgradiger Schutz personenbezogener Daten und der Privatsphäre gewährleistet bleibt“.

Zu diesem Zweck enthält die Richtlinie 2002/58 spezielle Vorschriften, die – wie sich u. a. aus ihren Erwägungsgründen 6 und 7 ergibt – die Nutzer elektronischer Kommunikationsdienste vor den sich aus den neuen Technologien und den zunehmenden Fähigkeiten zur automatischen Speicherung und Verarbeitung von Daten ergebenden Risiken für personenbezogene Daten und die Privatsphäre schützen sollen.

Insbesondere sieht Art. 5 Abs. 1 der Richtlinie 2002/58 vor, dass die Mitgliedstaaten die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten durch ihre innerstaatlichen Vorschriften sicherzustellen haben.

Der mit der Richtlinie 2002/58 eingeführte Grundsatz der Vertraulichkeit von Kommunikationen bedeutet u. a., dass – wie aus Art. 5 Abs. 1 Satz 2 der Richtlinie hervorgeht – es jeder anderen Person als dem Nutzer grundsätzlich untersagt ist, ohne dessen Einwilligung mit elektronischen Kommunikationen verbundene Verkehrsdaten zu speichern. Ausgenommen sind lediglich die gemäß Art. 15 Abs. 1 dieser Richtlinie gesetzlich dazu ermächtigten Personen sowie die für die Weiterleitung einer Nachricht erforderliche technische Speicherung (vgl. in diesem Sinne Urteil vom 29. Januar 2008, Promusicae, C-275/06, EU:C:2008:54, Rn. 47).

Wie die Erwägungsgründe 22 und 26 der Richtlinie 2002/58 bestätigen, dürfen Verkehrsdaten nach Art. 6 der Richtlinie nur zur Gebührenabrechnung für die Dienste, zu deren Vermarktung und zur Bereitstellung von Diensten mit Zusatznutzen im dazu erforderlichen Maß und innerhalb des dazu erforderlichen Zeitraums verarbeitet und gespeichert werden (vgl. in diesem Sinne Urteil vom 29. Januar 2008, Promusicae, C-275/06, EU:C:2008:54, Rn. 47 und 48). Was speziell die Gebührenabrechnung für die Dienste betrifft, ist diese Verarbeitung nur bis zum Ende des Zeitraums zulässig, in dem die Rechnung rechtlich angefochten oder der Anspruch auf Zahlung geltend gemacht werden kann. Danach sind die verarbeiteten und gespeicherten Daten zu löschen oder zu anonymisieren. Andere Standortdaten als Verkehrsdaten dürfen nach Art. 9 Abs. 1 der Richtlinie 2002/58 nur unter bestimmten Voraussetzungen und nur dann verarbeitet werden, wenn sie anonymisiert wurden oder wenn die Nutzer oder Teilnehmer ihre Einwilligung gegeben haben.

Die Tragweite der Bestimmungen der Art. 5, 6 und 9 Abs. 1 der Richtlinie 2002/58, die die Vertraulichkeit von Kommunikationen und der damit verbundenen Daten gewährleisten und Missbrauchsrisiken verringern sollen, beurteilt sich außerdem unter Berücksichtigung des 30. Erwägungsgrundes der Richtlinie, wonach „[d]ie Systeme für die Bereitstellung elektronischer Kommunikationsnetze und -dienste ... so konzipiert werden [sollten], dass so wenig personenbezogene Daten wie möglich benötigt werden“.

Zwar erlaubt Art. 15 Abs. 1 der Richtlinie 2002/58 den Mitgliedstaaten, Ausnahmen von der in Art. 5 Abs. 1 der Richtlinie aufgestellten grundsätzlichen Pflicht zur Sicherstellung der Vertraulichkeit personenbezogener Daten und den entsprechenden, u. a. in den Art. 6 und 9 der Richtlinie genannten Pflichten vorzusehen (vgl. in diesem Sinne Urteil vom 29. Januar 2008, Promusicae, C-275/06, EU:C:2008:54, Rn. 50).

Gleichwohl ist Art. 15 Abs. 1 der Richtlinie 2002/58, da er den Mitgliedstaaten erlaubt, die Tragweite der grundsätzlichen Verpflichtung, die Vertraulichkeit elektronischer Kommunikationen und der damit verbundenen Verkehrsdaten zu gewährleisten, einzuschränken, nach der ständigen Rechtsprechung des Gerichtshofs eng auszulegen (vgl. entsprechend Urteil vom 22. November 2012, Probst, C-119/12, EU:C:2012:748, Rn. 23). Eine solche Bestimmung vermag es daher nicht zu rechtfertigen, dass die

Ausnahme von dieser grundsätzlichen Verpflichtung 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.

Insoweit ist darauf hinzuweisen, dass Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 vorsieht, dass die in dieser Bestimmung genannten Rechtsvorschriften, die vom Grundsatz der Vertraulichkeit von Kommunikationen und der damit verbundenen Verkehrsdaten abweichen, „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“ zum Ziel haben müssen oder einen der anderen Zwecke verfolgen müssen, die in Art. 13 Abs. 1 der Richtlinie 95/46, auf den Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 verweist, genannt sind (vgl. in diesem Sinne Urteil vom 29. Januar 2008, Promusicae, C-275/06, EU:C:2008:54, Rn. 53). Hierbei handelt es sich um eine abschließende Aufzählung der Zwecke, wie aus Art. 15 Abs. 1 Satz 2 der Richtlinie 2002/58 hervorgeht, wonach die Rechtsvorschriften aus den in Art. 15 Abs. 1 Satz 1 dieser Richtlinie „aufgeführten Gründen“ gerechtfertigt sein müssen. Die Mitgliedstaaten dürfen demnach solche Vorschriften nicht zu anderen als den in Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 aufgezählten Zwecken erlassen.

Außerdem müssen nach Art. 15 Abs. 1 Satz 3 der Richtlinie 2002/58 „[a]lle in [Art. 15 Abs. 1 dieser Richtlinie] genannten Maßnahmen ... den allgemeinen Grundsätzen des [Unions]rechts einschließlich den in Artikel 6 Absätze 1 und 2 [EU] niedergelegten Grundsätzen entsprechen“, zu denen die allgemeinen Grundsätze und die Grundrechte gehören, die nunmehr durch die Charta gewährleistet werden. Art. 15 Abs. 1 der Richtlinie 2002/58 muss somit im Licht der von der Charta garantierten Grundrechte ausgelegt werden (vgl. entsprechend, zur Richtlinie 95/46, Urteile vom 20. Mai 2003, Österreichischer Rundfunk u. a., C-465/00, C-138/01 und C-139/01, EU:C:2003:294, Rn. 68, vom 13. Mai 2014, Google Spain und Google, C-131/12, EU:C:2014:317, Rn. 68, sowie vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 38).

In diesem Zusammenhang ist hervorzuheben, dass die den Betreibern elektronischer Kommunikationsdienste durch eine nationale Regelung, wie sie im Ausgangsverfahren in Rede steht, auferlegte Pflicht, Verkehrsdaten auf Vorrat zu speichern, um diese gegebenenfalls den zuständigen nationalen Behörden zugänglich zu machen, Fragen aufwirft, die nicht nur die Einhaltung der in den Vorlagefragen ausdrücklich erwähnten Art. 7 und 8 der Charta, sondern auch die Einhaltung der in Art. 11 der Charta gewährleisteten Freiheit der Meinungsäußerung betreffen (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 25 und 70).

Folglich muss die Bedeutung sowohl des in Art. 7 der Charta gewährleisteten Grundrechts auf Achtung des Privatlebens als auch des in Art. 8 der Charta gewährleisteten Grundrechts auf Schutz personenbezogener Daten, wie sie sich aus der Rechtsprechung des Gerichtshofs ergibt (vgl. in diesem Sinne Urteil vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 39 und die dort angeführte Rechtsprechung), bei der Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58 berücksichtigt werden. Das Gleiche gilt in Anbetracht der besonderen Bedeutung, die der Freiheit der Meinungsäußerung in jeder demokratischen Gesellschaft zukommt, für das Recht auf freie Meinungsäußerung. Dieses in Art. 11 der Charta gewährleistete Grundrecht stellt eine der wesentlichen Grundlagen einer demokratischen und pluralistischen Gesellschaft dar, die zu den Werten gehört, auf die sich die Union nach Art. 2 EUV gründet (vgl. in diesem Sinne Urteile vom 12. Juni 2003, Schmidberger, C-112/00, EU:C:2003:333, Rn. 79, und vom 6. September 2011, Patriciello, C-163/10, EU:C:2011:543, Rn. 31).

Insoweit ist darauf hinzuweisen, dass nach Art. 52 Abs. 1 der Charta jede Einschränkung der Ausübung der in der Charta anerkannten Rechte und Freiheiten gesetzlich vorgesehen sein und Wesensgehalt dieser Rechte und Freiheiten achten muss. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen der Ausübung dieser Rechte und Freiheiten nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen (Urteil vom 15. Februar 2016, N., C-601/15 PPU, EU:C:2016:84, Rn. 50).

Was den letztgenannten Gesichtspunkt betrifft, sieht Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 vor, dass die Mitgliedstaaten eine Vorschrift erlassen können, die von dem 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 dieser Richtlinie wird klargestellt, dass eine derartige Maßnahme in einem „strikt“ angemessenen Verhältnis zum intendierten Zweck stehen muss. Was speziell die Vorratsspeicherung von Daten betrifft, verlangt Art. 15 Abs. 1 Satz 2 der Richtlinie 2002/58, dass diese nur „während einer begrenzten Zeit“ und „aus den“ in Art. 15 Abs. 1 Satz 1 der Richtlinie aufgeführten Gründen erfolgen darf.

Dass der Grundsatz der Verhältnismäßigkeit zu beachten ist, ergibt sich ebenfalls aus der ständigen Rechtsprechung des Gerichtshofs, wonach der Schutz des Grundrechts auf Achtung des Privatlebens auf Unionsebene verlangt, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken (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. 77, Digital Rights, Rn. 52, sowie vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 92).

Hinsichtlich der Frage, ob eine nationale Regelung wie die in der Rechtssache C-203/15 in Rede stehende diesen Voraussetzungen genügt, ist festzustellen, dass sie eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsieht und die Betreiber elektronischer Kommunikationsdienste verpflichtet, diese Daten systematisch und kontinuierlich auf Vorrat zu speichern, und zwar ausnahmslos. Wie aus der Vorlageentscheidung hervorgeht, entsprechen die von dieser Regelung erfassten Datenkategorien im Wesentlichen denen, deren Vorratsspeicherung nach der Richtlinie 2006/24 vorgesehen war.

Die Daten, die somit von den Betreibern elektronischer Kommunikationsdienste auf Vorrat zu speichern sind, ermöglichen die Rückverfolgung und Identifizierung der Quelle und des Adressaten einer Nachricht sowie die Bestimmung von Datum, Uhrzeit, Dauer und Art einer Nachrichtenübermittlung, der Endeinrichtung von Benutzern und des Standorts mobiler Geräte. Zu diesen Daten gehören Name und Anschrift des Teilnehmers oder registrierten Benutzers, die Rufnummer des anrufenden und des angerufenen Anschlusses sowie bei Internetdiensten eine IP-Adresse. Aus diesen Daten geht insbesondere hervor, mit welcher Person ein Teilnehmer oder registrierter Benutzer auf welchem Weg kommuniziert hat, wie lange die Kommunikation gedauert hat und von welchem Ort aus sie stattfand. Ferner ist ihnen zu entnehmen, wie häufig der Teilnehmer oder registrierte Benutzer in einem bestimmten Zeitraum mit bestimmten Personen kommuniziert hat (vgl. entsprechend, in Bezug auf die Richtlinie 2006/24, Urteil Digital Rights, Rn. 26).

Aus der Gesamtheit dieser Daten können sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten auf Vorrat 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 (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 27). Diese Daten ermöglichen insbesondere – wie der Generalanwalt in den Nrn. 253, 254 und 257 bis 259 seiner Schlussanträge ausgeführt hat – die Erstellung des Profils der betroffenen Personen, das im Hinblick auf das Recht auf Achtung der Privatsphäre eine genauso sensible Information darstellt wie der Inhalt der Kommunikationen selbst.

Der mit einer solchen Regelung verbundene Eingriff in die in den Art. 7 und 8 der Charta verankerten Grundrechte ist von großem Ausmaß und als besonders schwerwiegend anzusehen. Der Umstand, dass die Vorratsspeicherung der Daten vorgenommen wird, ohne dass die Nutzer der elektronischen Kommunikationsdienste darüber informiert werden, ist geeignet, bei den Betroffenen das Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 37).

Auch wenn eine solche Regelung nicht die Vorratsspeicherung des Inhalts einer Kommunikation erlaubt und folglich nicht den Wesensgehalt der vorgenannten Grundrechte antastet (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 39), könnte die Vorratsspeicherung der Verkehrs- und Standortdaten jedoch Auswirkungen auf die Nutzung der elektronischen Kommunikationsmittel und infolgedessen auf die Ausübung der in Art. 11 der Charta gewährleisteten Freiheit der Meinungsäußerung durch die Nutzer dieser Mittel haben (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 28).

In Anbetracht der Schwere des Eingriffs in die betreffenden Grundrechte durch eine nationale Regelung, die für Zwecke der Kriminalitätsbekämpfung die Vorratsspeicherung von Verkehrs- und Standortdaten vorsieht, vermag allein die Bekämpfung der schweren Kriminalität eine solche Maßnahme zu rechtfertigen (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 60).

Zudem kann zwar die Wirksamkeit der Bekämpfung schwerer Kriminalität, insbesondere der organisierten Kriminalität und des Terrorismus, in hohem Maß von der Nutzung moderner Ermittlungstechniken abhängen; eine solche dem Gemeinwohl dienende Zielsetzung kann jedoch, so grundlegend sie auch sein mag, für sich genommen die Erforderlichkeit einer nationalen Regelung, die die allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten vorsieht, für die Kriminalitätsbekämpfung nicht rechtfertigen (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 51).

Eine solche Regelung hat zum einen in Anbetracht ihrer in Rn. 97 des vorliegenden Urteils beschriebenen charakteristischen Merkmale zur Folge, dass die Vorratsspeicherung der Verkehrs- und Standortdaten die Regel ist, obwohl nach dem mit der Richtlinie 2002/58 geschaffenen System die Vorratsspeicherung von Daten die Ausnahme zu sein hat.

Zum anderen sieht eine nationale Regelung wie die im Ausgangsverfahren, die sich allgemein auf alle Teilnehmer und registrierten Nutzer erstreckt und alle elektronischen Kommunikationsmittel sowie sämtliche Verkehrsdaten erfasst, keine Differenzierung, Einschränkung oder Ausnahme in Abhängigkeit von dem verfolgten Ziel vor. Sie betrifft 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 also auch für Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte. Zudem sieht sie keine Ausnahme vor, so dass sie auch für Personen gilt, deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 57 und 58).

Eine solche Regelung verlangt keinen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit. Insbesondere beschränkt sie 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 von Straftaten beitragen könnten (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 59).

Eine nationale Regelung wie die im Ausgangsverfahren in Rede stehende überschreitet somit die Grenzen des absolut Notwendigen und kann nicht als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden, wie es Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta verlangt.

Hingegen untersagt Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta einem Mitgliedstaat nicht, eine Regelung zu erlassen, die zur Bekämpfung schwerer Straftaten vorbeugend die gezielte Vorratsspeicherung von Verkehrs- und Standortdaten ermöglicht, sofern die Vorratsdatenspeicherung hinsichtlich Kategorien der zu speichernden Daten, der erfassten elektronischen Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer der Vorratsspeicherung auf das absolut Notwendige beschränkt ist.

Um den in der vorstehenden Randnummer des vorliegenden Urteils genannten Erfordernissen zu genügen, muss die betreffende nationale Regelung erstens klare und präzise Regeln über die Tragweite und die Anwendung einer solchen Maßnahme der Vorratsdatenspeicherung vorsehen und Mindesterfordernisse aufstellen, so dass die Personen, deren Daten auf Vorrat gespeichert wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken ermöglichen. Sie muss insbesondere angeben, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme der Vorratsdatenspeicherung vorbeugend getroffen werden darf, um so zu gewährleisten, dass eine derartige Maßnahme auf das absolut Notwendige beschränkt wird (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 54 und die dort angeführte Rechtsprechung).

Zweitens können sich die materiellen Voraussetzungen, die eine nationale Regelung, die im Rahmen der Bekämpfung von Straftaten vorbeugend die Vorratsspeicherung von Verkehrs- und Standortdaten ermöglicht, erfüllen muss, um zu gewährleisten, dass sie auf das absolut Notwendige beschränkt wird, zwar je nach den zur Verhütung, Ermittlung, Feststellung und Verfolgung schwerer Straftaten getroffenen Maßnahmen unterscheiden, doch muss die Vorratsspeicherung der Daten stets objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen. Diese Voraussetzungen müssen insbesondere in der Praxis geeignet sein, den Umfang der Maßnahme und infolgedessen die betroffenen Personenkreise wirksam zu begrenzen.

Bei der Begrenzung einer solchen Maßnahme im Hinblick auf die potenziell betroffenen Personenkreise und Situationen muss sich die nationale Regelung auf objektive Anknüpfungspunkte stützen, die es ermöglichen, Personenkreise zu erfassen, deren Daten geeignet sind, einen zumindest mittelbaren Zusammenhang mit schweren Straftaten sichtbar zu machen, auf irgendeine Weise zur Bekämpfung schwerer Kriminalität beizutragen oder eine schwerwiegende Gefahr für die öffentliche Sicherheit zu verhindern. Eine solche Begrenzung lässt sich durch ein geografisches Kriterium gewährleisten, wenn die zuständigen nationalen Behörden aufgrund objektiver Anhaltspunkte annehmen, dass in einem oder mehreren geografischen Gebieten ein erhöhtes Risiko besteht, dass solche Taten vorbereitet oder begangen werden.

In Anbetracht all dessen ist auf die erste Frage in der Rechtssache C-203/15 zu antworten, dass Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta dahin auszulegen ist, dass er einer nationalen Regelung entgegensteht, die für Zwecke der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsieht.

Zur zweiten Frage in der Rechtssache C-203/15 und zur ersten Frage in der Rechtssache C-698/15

Vorab ist darauf hinzuweisen, dass der Kammarrätt i Stockholm (Oberverwaltungsgericht Stockholm) die zweite Frage in der Rechtssache C-203/15 nur für den Fall gestellt hat, dass die erste Frage in dieser Rechtssache verneint wird. Diese zweite Frage ist jedoch unabhängig davon, ob eine Vorratsspeicherung von Daten in dem in den Rn. 108 bis 111 des vorliegenden Urteils in Betracht gezogenen Sinne allgemein oder gezielt erfolgt. Daher sind die zweite Frage in der Rechtssache C-203/15 und die erste Frage in der Rechtssache C-698/15, die unabhängig vom Umfang der den Betreibern elektronischer Kommunikationsdienste auferlegten Pflicht zur Vorratsspeicherung von Daten gestellt ist, gemeinsam zu beantworten.

Mit der zweiten Frage in der Rechtssache C-203/15 und der ersten Frage in der Rechtssache C-698/15 möchten die vorlegenden Gerichte wissen, ob Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7 und 8 sowie des Art. 52 Abs. 1 der Charta dahin auszulegen ist, dass er einer nationalen Regelung entgegensteht, die den Schutz und die Sicherheit der Verkehrs- und Standortdaten, insbesondere den Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten, zum Gegenstand hat, ohne diesen Zugang ausschließlich auf die Zwecke einer Bekämpfung schwerer Straftaten zu beschränken, ohne ihn einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsbehörde zu unterwerfen und ohne das Erfordernis vorzusehen, dass die betreffenden Daten im Gebiet der Union auf Vorrat zu speichern sind.

Hinsichtlich der Zwecke, die eine vom Grundsatz der Vertraulichkeit elektronischer Kommunikationen abweichende nationale Regelung rechtfertigen können, ist darauf hinzuweisen, dass, da die Aufzählung der in Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 genannten Zwecke – wie in den Rn. 90 und 102 des vorliegenden Urteils festgestellt – abschließend ist, der Zugang zu den auf Vorrat gespeicherten Daten tatsächlich strikt einem dieser Zwecke dienen muss. Da außerdem der mit der Regelung verfolgte Zweck im Verhältnis zur Schwere des mit dem Zugang einhergehenden Eingriffs in die Grundrechte stehen muss, vermag folglich im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten nur die Bekämpfung schwerer Straftaten einen solchen Zugang zu den auf Vorrat gespeicherten Daten zu rechtfertigen.

Was die Einhaltung des Grundsatzes der Verhältnismäßigkeit anbelangt, muss eine nationale Regelung über die Voraussetzungen, unter denen die Betreiber elektronischer Kommunikationsdienste den

zuständigen nationalen Behörden Zugang zu den auf Vorrat gespeicherten Daten zu gewähren haben, nach den in den Rn. 95 und 96 des vorliegenden Urteils getroffenen Feststellungen sicherstellen, dass ein solcher Zugang nur innerhalb der Schranken des absolut Notwendigen stattfindet.

Da zudem die in Art. 15 Abs. 1 der Richtlinie 2002/58 genannten Rechtsvorschriften nach dem elften Erwägungsgrund der Richtlinie „angemessenen Garantien ... entsprechen“ müssen, muss eine solche Rechtsvorschrift – wie sich aus der in Rn. 109 des vorliegenden Urteils angeführten Rechtsprechung ergibt – klare und präzise Regeln aufstellen, in denen angegeben ist, unter welchen Umständen und unter welchen Voraussetzungen die Betreiber elektronischer Kommunikationsdienste den zuständigen nationalen Behörden Zugang zu den Daten zu gewähren haben. Außerdem muss eine derartige Vorschrift im innerstaatlichen Recht verbindlich sein.

Es ist zwar Sache des nationalen Rechts, die Voraussetzungen festzulegen, unter denen die Betreiber elektronischer Kommunikationsdienste den zuständigen nationalen Behörden den Zugang zu den auf Vorrat gespeicherten Daten gewähren müssen, damit gewährleistet ist, dass dieser Zugang auf das absolut Notwendige beschränkt ist. Die betreffende nationale Regelung darf sich jedoch nicht darauf beschränken, dass der Zugang einem der in Art. 15 Abs. 1 der Richtlinie 2002/58 genannten Zwecke zu entsprechen hat, auch wenn es sich dabei um die Bekämpfung schwerer Straftaten handelt. Denn eine solche nationale Regelung muss auch die materiell- und verfahrensrechtlichen Voraussetzungen für den Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten festlegen (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 61).

Infolgedessen, und weil ein allgemeiner Zugang zu allen auf Vorrat gespeicherten Daten unabhängig davon, ob irgendein – zumindest mittelbarer – Zusammenhang mit dem verfolgten Ziel besteht, nicht als auf das absolut Notwendige beschränkt angesehen werden kann, muss sich die betreffende nationale Regelung bei der Festlegung der Umstände und Voraussetzungen, unter denen den zuständigen nationalen Behörden Zugang zu den Daten von Teilnehmern oder registrierten Nutzern zu gewähren ist, auf objektive Kriterien stützen. Insoweit darf im Zusammenhang mit dem Zweck der Bekämpfung von Straftaten 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 (vgl. entsprechend Urteil des Europäischen Gerichtshofs für Menschenrechte vom 4. Dezember 2015, Zakharov/Russland, CE:ECHR:2015:1204JUD004714306, Rn. 260). Allerdings könnte in besonderen Situationen wie etwa solchen, in denen vitale Interessen der nationalen Sicherheit, der Landesverteidigung oder der öffentlichen Sicherheit durch terroristische Aktivitäten bedroht sind, der Zugang zu Daten anderer Personen ebenfalls gewährt werden, wenn es objektive Anhaltspunkte dafür gibt, dass diese Daten in einem konkreten Fall einen wirksamen Beitrag zur Bekämpfung solcher Aktivitäten leisten könnten.

Damit in der Praxis die vollständige Einhaltung dieser Voraussetzungen gewährleistet ist, ist es unabdingbar, dass der Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten grundsätzlich – außer in hinreichend begründeten Eilfällen – einer vorherigen Kontrolle entweder durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen wird und deren Entscheidung auf einen mit Gründen versehenen Antrag ergeht, der von den zuständigen nationalen Behörden u. a. im Rahmen von Verfahren zur Verhütung, Feststellung oder Verfolgung von Straftaten gestellt wird (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 62; vgl. auch entsprechend, zu Art. 8 EMRK, Urteil des Europäischen Gerichtshofs für Menschenrechte vom 12. Januar 2016, Szabó und Vissy/Ungarn CE:ECHR:2016:0112JUD003713814, Rn. 77 und 80).

Außerdem ist es wichtig, dass die zuständigen nationalen Behörden, denen Zugang zu den auf Vorrat gespeicherten Daten gewährt worden ist, die betroffenen Personen im Rahmen der einschlägigen nationalen Verfahren davon in Kenntnis setzen, sobald die Mitteilung die behördlichen Ermittlungen nicht mehr beeinträchtigen kann. Diese Information ist nämlich der Sache nach erforderlich, damit die betroffenen Personen u. a. das Recht auf Einlegung eines Rechtsbehelfs ausüben können, das in Art. 15 Abs. 2 der Richtlinie 2002/58 in Verbindung mit Art. 22 der Richtlinie 95/46 für den Fall einer Verletzung ihrer Rechte ausdrücklich vorgesehen ist (vgl. entsprechend Urteile vom 7. Mai 2009, Rijkeboer, C-553/07, EU:C:2009:293, Rn. 52, sowie vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 95).

Bezüglich der Vorschriften zur Sicherheit und zum Schutz der von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten Daten ist festzustellen, dass Art. 15 Abs. 1 der

Richtlinie 2002/58 den Mitgliedstaaten nicht erlaubt, von Art. 4 Abs. 1 und Art. 4 Abs. 1a der Richtlinie abzuweichen. Nach diesen Bestimmungen haben die Betreiber geeignete technische und organisatorische Maßnahmen zu ergreifen, um zu gewährleisten, dass die auf Vorrat gespeicherten Daten wirksam vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang geschützt sind. Unter Berücksichtigung der Menge an gespeicherten Daten, ihres sensiblen Charakters und der Gefahr eines unberechtigten Zugangs zu ihnen müssen die Betreiber elektronischer Kommunikationsdienste, um die Unversehrtheit und Vertraulichkeit der Daten in vollem Umfang zu sichern, durch geeignete technische und organisatorische Maßnahmen ein besonders hohes Schutz- und Sicherheitsniveau gewährleisten. Die nationale Regelung muss insbesondere vorsehen, dass die Daten im Unionsgebiet zu speichern und nach Ablauf ihrer Speicherungsfrist unwiderruflich zu vernichten sind (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 66 bis 68).

Jedenfalls müssen die Mitgliedstaaten gewährleisten, dass die Einhaltung des Schutzniveaus, das das Unionsrecht im Rahmen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten garantiert, durch eine unabhängige Stelle überwacht wird, da eine solche Überwachung in Art. 8 Abs. 3 der Charta ausdrücklich gefordert wird und nach ständiger Rechtsprechung des Gerichtshofs ein wesentlicher Bestandteil der Wahrung des Schutzes der Betroffenen bei der Verarbeitung personenbezogener Daten ist. Anderenfalls würde den Personen, deren personenbezogene Daten gespeichert wurden, das durch Art. 8 Abs. 1 und 3 der Charta garantierte Recht vorenthalten, sich zum Schutz ihrer Daten mit einer Eingabe an die nationalen Kontrollstellen zu wenden (vgl. in diesem Sinne Urteile Digital Rights, Rn. 68, und vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 41 und 58).

Es ist Sache der vorlegenden Gerichte, zu prüfen, ob und inwieweit die in den Ausgangsverfahren in Rede stehenden nationalen Regelungen die sich aus Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta ergebenden Erfordernisse beachten, wie sie in den Rn. 115 bis 123 des vorliegenden Urteils ausdrücklich benannt sind, sowohl was den Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten als auch was den Schutz dieser Daten und das Sicherheitsniveau betrifft.

Aufgrund all dessen ist auf die zweite Frage in der Rechtssache C-203/15 und die erste Frage in der Rechtssache C-698/15 zu antworten, dass Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta dahin auszulegen ist, dass er einer nationalen Regelung entgegensteht, die den Schutz und die Sicherheit der Verkehrs- und Standortdaten, insbesondere den Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten zum Gegenstand hat, ohne im Rahmen der Bekämpfung von Straftaten diesen Zugang ausschließlich auf die Zwecke einer Bekämpfung schwerer Straftaten zu beschränken, ohne den Zugang einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsbehörde zu unterwerfen und ohne vorzusehen, dass die betreffenden Daten im Gebiet der Union auf Vorrat zu speichern sind.

Zur zweiten Frage in der Rechtssache C-698/15

Mit der zweiten Frage in der Rechtssache C-698/15 möchte der Court of Appeal (England & Wales) (Civil Division) (Berufungsgericht [England und Wales] [Abteilung für Zivilsachen]) wissen, ob der Gerichtshof im Urteil Digital Rights die Art. 7 und 8 der Charta in einem Sinne ausgelegt hat, der über den hinausgeht, der Art. 8 EMRK vom Europäischen Gerichtshof für Menschenrechte gegeben wurde.

Zunächst ist darauf hinzuweisen, dass die in der EMRK anerkannten Grundrechte zwar, wie Art. 6 Abs. 3 EUV bestätigt, als allgemeine Grundsätze Teil des Unionsrechts sind, die EMRK jedoch, solange die Union ihr nicht beigetreten ist, kein Rechtsinstrument darstellt, das förmlich in die Unionsrechtsordnung übernommen wurde (vgl. in diesem Sinne Urteil vom 15. Februar 2016, N., C-601/15 PPU, EU:C:2016:84, Rn. 45 und die dort angeführte Rechtsprechung).

Daher ist die Richtlinie 2002/58, um die es vorliegend geht, einzig und allein anhand der durch die Charta garantierten Grundrechte auszulegen (vgl. in diesem Sinne Urteil vom 15. Februar 2016, N., C-601/15 PPU, EU:C:2016:84, Rn. 46 und die dort angeführte Rechtsprechung).

Außerdem heißt es in den Erläuterungen zu Art. 52 der Charta, dass mit ihrem Art. 52 Abs. 3 die notwendige Kohärenz zwischen der Charta und der EMRK geschaffen werden soll, „ohne dass dadurch

die Eigenständigkeit des Unionsrechts und des Gerichtshofs der Europäischen Union berührt wird“ (vgl. in diesem Sinne Urteil vom 15. Februar 2016, N., C-601/15 PPU, EU:C:2016:84, Rn. 47). Insbesondere steht, wie aus Art. 52 Abs. 3 Satz 2 der Charta hervorgeht, Art. 52 Abs. 3 Satz 1 der Charta dem nicht entgegen, dass das Recht der Union einen weiter gehenden Schutz gewährt als die EMRK. Zudem betrifft Art. 8 der Charta ein anderes als das in ihrem Art. 7 verankerte Grundrecht, für das es in der EMRK keine Entsprechung gibt.

Nach ständiger Rechtsprechung des Gerichtshofs liegt die Rechtfertigung für ein Vorabentscheidungsersuchen jedoch nicht in der Abgabe von Gutachten zu allgemeinen oder hypothetischen Fragen, sondern darin, dass das Ersuchen für die tatsächliche Entscheidung eines Rechtsstreits über das Unionsrecht erforderlich ist (vgl. in diesem Sinne Urteile vom 24. April 2012, Kamberaj, C-571/10, EU:C:2012:233, Rn. 41, vom 26. Februar 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, Rn. 42, sowie vom 27. Februar 2014, Pohotovosť, C-470/12, EU:C:2014:101, Rn. 29).

Im vorliegenden Fall ist in Anbetracht der insbesondere in den Rn. 128 und 129 des vorliegenden Urteils enthaltenen Erwägungen die Frage, ob der in den Art. 7 und 8 der Charta verliehene Schutz über den in Art. 8 EMRK garantierten hinausgeht, nicht geeignet, die Auslegung der Richtlinie 2002/58 im Licht der Charta, um die es in der Rechtssache C-698/15 im Ausgangsverfahren geht, zu beeinflussen.

Es ist somit nicht ersichtlich, dass die Antwort auf die zweite Frage in der Rechtssache C-698/15 Hinweise zur Auslegung des Unionsrechts liefern könnte, die für die Entscheidung des betreffenden Rechtsstreits im Hinblick auf das Unionsrecht erforderlich sind.

Folglich ist die zweite Frage in der Rechtssache C-698/15 unzulässig.

Kosten

Für die Parteien der Ausgangsverfahren ist das Verfahren ein Zwischenstreit in den bei den vorlegenden Gerichten anhängigen Rechtsstreitigkeiten; die Kostenentscheidung ist daher Sache dieser Gerichte. Die Auslagen anderer Beteiligter für die Abgabe von Erklärungen vor dem Gerichtshof sind nicht erstattungsfähig.