ENTSCHEIDUNGEN

Vorratsdatenspeicherung ohne Anlass unzulässig

EuGH, Urt. v. 21.12.2016
in den verbundenen Rechtssachen C-203/15 und C-698/15*

1. **Art. 15 Abs. 1 der Richtlinie 2002/58/EG in der durch die Richtlinie 2009/136 geänderten Fassung steht einer nationalen Regelung entgegen, 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. Nationale Regelungen, die den Schutz und die Sicherheit der Verkehrs- und Standortdaten sowie insbesondere auch den Zugang der zuständigen nationalen Behörden zu diesen Daten zum Gegenstand haben, sind darauf zu beschränken, dass Zugang ausschließlich zur Bekämpfung schwerer Straftaten erfolgt, dieser einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsbehörde unterliegt und die betreffenden Daten im Gebiet der Union auf Vorrat zu speichern sind.**
2. **Bei der Begrenzung der Eingriffsmaßnahme 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. (Leitsätze der Schriftleitung)**

1 Die Vorabentscheidungsersuchen betreffen die Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.7.2002 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 25.12.2009 (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).

2 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 W., B. und L. 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

(wird ausgeführt...)

Ausgangsverfahren und Vorlagefragen

Rechtssache C-203/15

44 Am 9.4.2014 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 8.4.2014, Digital Rights Ireland u. a. (C-293/12 und C-594/12, im Folgenden: Urteil Digital Rights, EU:C:2014:238) ab dem 14.4. 2014 die vom LEK erfassten elektronischen Kommunikationsdaten nicht mehr auf Vorrat speichern und die bis dahin gespeicherten Daten löschen werde.

45 Am 15.4.2014 beschwerte sich die Rikspolisstyrels (Reichspolizeidirektion, Schweden) bei der PTS darüber, dass Tele2 Sverige ihr die betreffenden Daten nicht mehr mitteile.

* Das Urteil ist vollständig abrufbar unter: http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1&cid=601733 (zuletzt abgerufen am 16.1.2017).

46 Am 29.4.2014 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 13.6.2014 („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 4.12.1950 in Rom unterzeichnete Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK) verstoße (*wird ausgeführt*).

47 Aufgrund dessen teilte die PTS am 19.6.2014 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 27.6.2014 gab die PTS ihr auf, diese Daten spätestens ab dem 25.7.2014 auf Vorrat zu speichern.

48 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. 6.2014 Klage beim *Förvaltningsrätt i Stockholm* (Verwaltungsgericht Stockholm, Schweden). Nachdem die Klage mit Urteil vom 13.10.2014 abgewiesen worden war, legte Tele2 Sverige Berufung beim vorlegenden Gericht ein.

49 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.

50 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.

51 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

52 W., B. und L. 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.

53 Mit Urteil vom 17.7.2015 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.

54 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.

55 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.

56 Das vorlegende Gericht ging in der Vorlageentscheidung und in seinem im Rahmen des Rechtsmittelverfahrens erlassenen Urteil vom 20.11.2015, 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.

57 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.

58 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.

59 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

60 Mit Beschluss vom 1.2.2016, D. 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.

61 Mit Beschluss des Präsidenten des Gerichtshofs vom 10. 3.2016 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

62 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.

63 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.

64 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

65 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.

66 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.

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

68 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.

69 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 6.11.2003, Lindqvist, C-101/01, EU:C:2003:596, Rn. 43, sowie vom 16.12.2008, Satakunnan Markkinapörssi und Satamedia, C-73/07, EU:C:2008:727, Rn. 41).

70 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.

71 Nach Art. 15 Abs. 1 der Richtlinie 2002/58 können die Mitgliedstaaten unter den angegebenen Voraussetzungen „Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Art. 5, Art. 6, Art. 8 Abs. 1, 2, 3 und 4 sowie Art. 9 dieser Richtlinie beschränken“. Art. 15 Abs. 1 S. 2 der Richtlinie nennt als Beispiel für Vorschriften, die so von den Mitgliedstaaten erlassen werden können, Vorschriften, die „vorsehen, dass Daten … aufbewahrt werden“.

72 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 29.1.2008, 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.

73 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 i.S.d. 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.

74 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 i.V.m. Art. 3 der Richtlinie 2002/58 dahin auszulegen, dass diese Rechtsvorschriften in den Geltungsbereich dieser Richtlinie fallen.

75 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.

76 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.

77 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.

78 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.

79 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.

80 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.

81 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

82 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".

83 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.

84 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.

85 Der mit der Richtlinie 2002/58 eingeführte Grundsatz der Vertraulichkeit von Kommunikationen bedeutet u. a., dass – wie aus Art. 5 Abs. 1 S. 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 gem. Art. 15 Abs. 1 dieser Richtlinie gesetzlich dazu ermächtigten Personen sowie die für die Weiterleitung einer Nachricht erforderliche technische Speicherung (vgl. in diesem Sinne Urt. vom 29.1.2008, Promusicae, C-275/06, EU:C:2008:54, Rn. 47).

86 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 Urt. v. 29.1.2008, 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.

87 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".

88 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 Urt. v. 29.1.2008, Promusicae, C-275/06, EU:C:2008:54, Rn. 50).

89 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 Urt. v. 22.11.2012, 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.

90 Insoweit ist darauf hinzuweisen, dass Art. 15 Abs. 1 S. 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 S. 1 der Richtlinie 2002/58 verweist, genannt sind (vgl. in diesem Sinne Urt. v. 29.1.2008, 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 S. 2 der Richtlinie 2002/58 hervorgeht, wonach die Rechtsvorschriften aus den in Art. 15 Abs. 1 S. 1 dieser Richtlinie „aufgeführten Gründen" gerechtfertigt sein müssen. Die Mitgliedstaaten dürfen demnach solche Vorschriften nicht zu anderen als den in Art. 15 Abs. 1 S. 1 der Richtlinie 2002/58 aufgezählten Zwecken erlassen.

91 Außerdem müssen nach Art. 15 Abs. 1 S. 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 Art. 6 Abs. 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, Urt. v. 20.5.2003, Österreichischer Rundfunk u. a., C-465/00, C-138/01 und C-139/01, EU:C:2003:294, Rn. 68, v. 13.5.2014, Google Spain und Google, C-131/12, EU:C:2014:317, Rn. 68, sowie v. 6.10.2015, Schrems, C-362/14, EU:C:2015:650, Rn. 38).

92 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).

93 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 Urt. v. 6.10.2015, 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 Urt. v. 12.6.2003, Schmidberger, C-112/00, EU:C:2003:333, Rn. 79, und vom 6.9.2011, Patriciello, C-163/10, EU:C:2011:543, Rn. 31).

94 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 (Urt. v. 15.2.2016, N., C-601/15 PPU, EU:C:2016:84, Rn. 50).

95 Was den letztgenannten Gesichtspunkt betrifft, sieht Art. 15 Abs. 1 S. 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 S. 2 der Richtlinie 2002/58, dass diese nur „während einer begrenzten Zeit“ und „aus den“ in Art. 15 Abs. 1 S. 1 der Richtlinie aufgeführten Gründen erfolgen darf.

96 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 (Urt. v. 16.12.2008, Satakunnan Markkinapörssi und Satamedia, C-73/07, EU:C:2008:727, Rn. 56, v. 9.11.2010, 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 6.10.2015, Schrems, C-362/14, EU:C:2015:650, Rn. 92).

97 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.

98 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).

99 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.

100 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).

101 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).

102 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).

103 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).

104 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.

105 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).

106 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).

107 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.

108 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.

109 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).

110 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.

111 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.

112 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

113 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.

114 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.

115 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 S. 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.

116 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.

117 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.

118 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).

119 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 *EGMR* v. 4.12.2015, 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.

120 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 *EGMR* v. 12.1.2016, Szabó und Vissy/Ungarn CE:ECHR:2016:0112JUD003713814, Rn. 77 und 80).

121 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 i.V.m. Art. 22 der Richtlinie 95/46 für den Fall einer Verletzung ihrer Rechte ausdrücklich vorgesehen ist (vgl. entsprechend Urteile v. 7.5.2009, Rijkeboer, C-553/07, EU:C:2009:293, Rn. 52, sowie v. 6.10.2015, Schrems, C-362/14, EU:C:2015:650, Rn. 95).

122 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).

123 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 v. 6.10.2015, Schrems, C-362/14, EU:C:2015:650, Rn. 41 und 58).

124 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.

125 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

126 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 *EGMR* gegeben wurde.

127 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 Urt. v. 15.2.2016, N., C-601/15 PPU, EU:C:2016:84, Rn. 45 und die dort angeführte Rechtsprechung).

128 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 Urt. v. 15.2.2016, N., C-601/15 PPU, EU:C:2016:84, Rn. 46 und die dort angeführte Rechtsprechung).

129 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 Urt. v. 15.2.2016, N., C-601/15 PPU, EU:C:2016:84, Rn. 47). Insbesondere steht, wie aus Art. 52 Abs. 3 S. 2 der Charta hervorgeht, Art. 52 Abs. 3 S. 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.

130 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 v. 24.4.2012, Kamberaj, C-571/10, EU:C:2012:233, Rn. 41, v. 26.2.2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, Rn. 42, sowie v. 27.2. 2014, Pohotovosť, C-470/12, EU:C:2014:101, Rn. 29).

131 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.

132 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.

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

Kosten (*wird ausgeführt*). …

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

Art. 15 Abs. 1 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.7.2002 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 25.11.2009 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.