Rättsfallssamlingen

DOMSTOLENS DOM (stora avdelningen)

den 21 december 2016*

[Texten ändrad genom beslut av den 16 mars 2017]

”Begäran om förhandsavgörande – Elektronisk kommunikation – Behandling av personuppgifter – Konfidentialitet vid elektronisk kommunikation – Skydd – Direktiv 2002/58/EG – Artiklarna 5, 6, 9 och 15.1 – Europeiska unionens stadga om de grundläggande rättigheterna – Artiklarna 7, 8, 11 och 52.1 – Nationell lagstiftning – Leverantörer av elektroniska kommunikationstjänster – Skyldighet som avser en generell och odifferentierad lagring av trafikuppgifter och lokaliseringsuppgifter – Nationella myndigheter – Tillgång till uppgifter – Ingen förhandskontroll av en domstol eller en oberoende förvaltningsmyndighet – Fråga om förenlighet med unionsrätten”

I de förenade målen C-203/15 och C-698/15,

angående beslut att begära förhandsavgörande enligt artikel 267 FEUF, från Kammarrätten i Stockholm (Sverige) och Court of Appeal (England & Wales) (Civil Division) (Appellationsdomstolen för England och Wales, avdelningen för tvistemål och förvaltningsmål, Förenade kungariket) av den 29 april 2015 respektive den 9 december 2015 som inkom till domstolen den 4 maj 2015 respektive den 28 december 2015, i målen

Tele2 Sverige AB (C-203/15)

mot

Post- och telestyrelsen,

och

Secretary of State for the Home Department (C-698/15)

mot

Tom Watson,

Peter Brice,

Geoffrey Lewis,

* Rättegångsspråk: svenska och engelska.

ytterligare deltagare i rättegången:

Open Rights Group,

Privacy International,

The Law Society of England and Wales,

meddelar

DOMSTOLEN (stora avdelningen)

sammansatt av ordföranden K. Lenaerts, vice ordföranden A. Tizzano, avdelningsordförandena R. Silva de Lapuerta, T. von Danwitz (referent), J.L. da Cruz Vilaça, E. Juhász och M. Vilaras samt domarna A. Borg Barthet, J. Malenovský, E. Levits, J.-C. Bonichot, A. Arabadjiev, S. Rodin, F. Biltgen och C. Lycourgos,

generaladvokat: H. Saugmandsgaard Øe,

justitiesekreterare: handläggaren C. Strömholm,

med hänsyn till beslutet av domstolens ordförande av den 1 februari 2016 att handlägga mål C-698/15 skyndsamt i enlighet med artikel 105.1 i domstolens rättegångsregler,

efter det skriftliga förfarandet och förhandlingen den 12 april 2016,

med beaktande av de yttranden som avgetts av:

– Tele2 Sverige AB, genom M. Johansson och N. Torgerzon, advokater, samt E. Lagerlöf och S. Backman,

– Tom Watson, genom J. Welch och E. Norton, solicitors, I. Steele, advocate, B. Jaffey, barrister, samt D. Rose, QC,

– Peter Brice och Geoffrey Lewis, genom A. Suterwalla och R. de Mello, barristers, R. Drabble, QC, samt S. Luke, solicitor,

– Open Rights Group och Privacy International, genom D. Carey, solicitor, samt R. Mehta och J. Simor, barristers,

– The Law Society of England and Wales, genom T. Hickman, barrister, samt N. Turner,

– Sveriges regering, genom A. Falk, C. Meyer-Seitz, U. Persson, N. Otte Widgren och L. Swedenborg, samtliga i egenskap av ombud,

– Förenade kungarikets regering, genom S. Brandon, L. Christie och V. Kaye, samtliga i egenskap av ombud, biträdda av D. Beard, G. Facenna och J. Eadie, QC, samt S. Ford, barrister,

– Belgiens regering, genom J.-C. Halleux, S. Vanrie och C. Pochet, samtliga i egenskap av ombud,

– Tjeckiens regering, genom M. Smolek och J. Vláčíl, båda i egenskap av ombud,

– Danmarks regering, genom C. Thorning och M. Wolff, båda i egenskap av ombud,

– Tysklands regering, genom T. Henze, M. Hellmann och J. Kemper, samtliga i egenskap av ombud, biträdda av M. Kottmann och U. Karpenstein, Rechtsanwälte,

– Estlands regering, genom K. Kraavi-Käerdi, i egenskap av ombud,

– Irland, genom E. Creedon, L. Williams och A. Joyce, samtliga i egenskap av ombud, biträdda av D. Fennelly, BL,

– Spaniens regering, genom A. Rubio González, i egenskap av ombud,

– Frankrikes regering, genom G. de Bergues, D. Colas, F.-X. Bréchot och C. David, samtliga i egenskap av ombud,

– Cyperns regering, genom K. Kleanthous, i egenskap av ombud,

– Ungerns regering, genom M. Fehér och G. Koós, båda i egenskap av ombud,

– Nederländernas regering, genom M. Bulterman, M. Gijzen och J. Langer, samtliga i egenskap av ombud,

– Polens regering, genom B. Majczyna, i egenskap av ombud,

– Finlands regering, genom J. Heliskoski, i egenskap av ombud,

– Europeiska kommissionen, genom H. Krämer, K. Simonsson, H. Kranenborg, D. Nardi, P. Costa de Oliveira och J. Vondung, samtliga i egenskap av ombud,

och efter att den 19 juli 2016 ha hört generaladvokatens förslag till avgörande,

följande

Dom

1 Respektive begäran om förhandsavgörande avser tolkningen av artikel 15.1 i Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 2002, s. 37), i dess lydelse enligt Europaparlamentets och rådets direktiv 2009/136/EG av den 25 november 2009 (EUT L 337, 2009, s. 11) (nedan kallat direktiv 2002/58), jämförd med artiklarna 7, 8 och 52.1 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad stadgan).

2 Den ena begäran har framställts i ett mål (C-203/15) mellan Tele2 Sverige AB och Post- och telestyrelsen (nedan kallad PTS), om ett föreläggande från PTS för Tele2 Sverige att lagra trafikuppgifter och lokaliseringsuppgifter avseende bolagets abonnenter och registrerade användare. Den andra begäran har framställts i ett mål (C-698/15) mellan Tom Watson, Peter

Brice och Geoffrey Lewis, å ena sidan, och Secretary of State for the Home Department (inrikesministern i Förenade konungariket Storbritannien och Nordirland), å andra sidan, om huruvida section 1 i Data Retention and Investigatory Powers Act 2014 (2014 års lag om datalagring och utredningsbefogenheter, nedan kallad Dripa) är förenlig med unionsrätten.

Tillämpliga bestämmelser

Unionsrätt

Direktiv 2002/58

3 I skälen 2, 6, 7, 11, 21, 22, 26 och 30 i direktiv 2002/58 anges följande:

”(2) I detta direktiv eftersträvas respekt för de grundläggande rättigheterna och iakttagande av de principer som erkänns i synnerhet i [stadgan]. I synnerhet eftersträvas i detta direktiv att säkerställa full respekt för rättigheterna i artiklarna 7 och 8 i … stadgan.

…

(6) Internet bryter upp traditionella marknadsstrukturer genom att tillhandahålla en gemensam, global infrastruktur för leverans av en mängd olika elektroniska kommunikationstjänster. Allmänt tillgängliga kommunikationstjänster via Internet öppnar nya möjligheter för användarna, men för även med sig nya risker för deras personuppgifter och integritet.

(7) När det gäller allmänna kommunikationsnät bör särskilda rättsliga och tekniska bestämmelser antas för att skydda fysiska personers grundläggande fri- och rättigheter samt juridiska personers berättigade intressen, särskilt med hänsyn till den ökade kapaciteten för automatisk lagring och behandling av uppgifter om abonnenter och användare.

…

(11) I likhet med [Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (EGT L 281, 1995, s. 31)] omfattar det här direktivet inte sådana frågor om skydd av grundläggande fri- och rättigheter som rör verksamhet som inte regleras av gemenskapslagstiftningen. Det ändrar därför inte den befintliga jämvikten mellan den enskildes rätt till integritet och medlemsstaternas möjligheter att vidta sådana åtgärder, enligt artikel 15.1 i det här direktivet, som krävs för att skydda allmän säkerhet, försvar, statens säkerhet (inbegripet statens ekonomiska välstånd när verksamheten rör statens säkerhet) och brottsbekämpning. Det här direktivet påverkar följaktligen inte medlemsstaternas möjlighet att utföra laglig avlyssning av elektronisk kommunikation eller att vidta andra åtgärder om det är nödvändigt för något av dessa ändamål och sker i enlighet med Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna i den tolkning dessa fått i rättspraxis från Europeiska domstolen för de mänskliga rättigheterna. Sådana åtgärder måste vara lämpliga, i strikt proportion till det avsedda ändamålet och nödvändiga i ett demokratiskt samhälle. De bör omfattas av lämpliga skyddsmekanismer i överensstämmelse med Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna.

…

(21) Åtgärder bör vidtas för att förhindra obehörig åtkomst av kommunikation, så att konfidentialiteten vid kommunikation via allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster skyddas såväl i fråga om innehåll som uppgifter som har samband med sådan kommunikation. Den nationella lagstiftningen i vissa medlemsstater förbjuder endast obehörig åtkomst av kommunikation om detta sker avsiktligen.

(22) Förbudet mot lagring av kommunikationer och tillhörande trafikuppgifter av andra än användarna eller utan deras samtycke är inte avsett att förbjuda någon automatisk, mellanliggande och tillfällig lagring av denna information, i den mån lagringen enbart görs för att utföra överföringen i det elektroniska kommunikationsnätet och under förutsättning att informationen inte lagras längre än vad som är nödvändigt för överföringen och trafikstyrningen och att konfidentialiteten förblir garanterad under lagringsperioden. …

…

(26) De uppgifter om abonnenter som behandlas inom elektroniska kommunikationsnät i samband med uppkoppling och överföring av information innehåller upplysningar om fysiska personers privatliv och gäller rätten till skydd för deras korrespondens eller omsorgen om juridiska personers berättigade intressen. Sådana uppgifter får endast lagras i den utsträckning det är nödvändigt för att tillhandahålla tjänsten när det gäller fakturering och betalning av samtrafikavgifter, och endast under en begränsad tid. [Ytterligare behandling av sådana uppgifter får] endast ske om abonnenten givit sitt samtycke till detta efter att ha erhållit korrekt och uttömmande information av den berörda leverantören om vilka typer av ytterligare behandling som denne avser att företa och om abonnentens rätt att inte ge sitt samtycke eller att återkalla sitt samtycke till en sådan behandling. …

…

(30) Systemen för tillhandahållande av elektroniska kommunikationsnät och elektroniska kommunikationstjänster bör utformas så att mängden nödvändiga personuppgifter begränsas till ett absolut minimum. …”

4 I artikel 1 i direktiv 2002/58, med rubriken ”Tillämpningsområde och syfte”, föreskrivs följande:

”1. Genom detta direktiv möjliggörs en harmonisering av nationella bestämmelser för att säkerställa ett likvärdigt skydd av de grundläggande fri- och rättigheterna, särskilt rätten till integritet och konfidentialitet, när det gäller behandling av personuppgifter inom sektorn för elektronisk kommunikation, samt för att säkerställa fri rörlighet för sådana uppgifter samt för utrustning och tjänster avseende elektronisk kommunikation inom gemenskapen.

2. Bestämmelserna i detta direktiv skall precisera och komplettera direktiv [95/46] för de ändamål som avses i punkt 1. Bestämmelserna är vidare avsedda att skydda berättigade intressen för de abonnenter som är juridiska personer.

3. Detta direktiv skall inte tillämpas på verksamheter som faller utanför tillämpningsområdet för Fördraget om upprättandet av Europeiska gemenskapen, t.ex. de som omfattas av avdelningarna V och VI i Fördraget om Europeiska unionen, och inte i något fall på verksamheter som avser allmän

säkerhet, försvar, statens säkerhet (inbegripet statens ekonomiska välstånd när verksamheten rör statens säkerhet) och statens verksamhet på straffrättens område.”

5 I artikel 2 i direktiv 2002/58, som har rubriken ”Definitioner”, anges följande:

”Om inte annat anges skall definitionerna i Europaparlamentets och rådets direktiv 95/46/EG och 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektiv) [(EGT L 108, 2002, s. 33)] gälla i detta direktiv.

Dessutom skall följande definitioner gälla:

…

b) *trafikuppgifter*: alla uppgifter som behandlas i syfte att överföra en kommunikation via ett elektroniskt kommunikationsnät eller för att fakturera den.

c) *lokaliseringsuppgifter*: alla uppgifter som behandlas i ett elektroniskt kommunikationsnät eller av en elektronisk kommunikationstjänst och som visar den geografiska positionen för terminalutrustningen för en användare av en allmänt tillgänglig elektronisk kommunikationstjänst.”

d) *kommunikation*: all information som utbyts eller överförs mellan ett begränsat antal parter genom en allmänt tillgänglig elektronisk kommunikationstjänst. Detta inbegriper inte information som överförs som del av en sändningstjänst för rundradio eller TV till allmänheten via ett elektroniskt kommunikationsnät utom i den mån informationen kan sättas i samband med den enskilde abonnenten eller användaren av informationen.

…”

6 I artikel 3 i direktiv 2002/58, med rubriken ”Berörda tjänster”, föreskrivs följande:

”Detta direktiv ska tillämpas på behandling av personuppgifter i samband med att allmänt tillgängliga elektroniska kommunikationstjänster tillhandahålls i allmänna kommunikationsnät inom gemenskapen, inbegripet allmänna kommunikationsnät som stöder datainsamling och identifieringsutrustning.”

7 Artikel 4 i detta direktiv, med rubriken ”Säkerhet i samband med behandlingen av uppgifter”, har följande lydelse:

”1. Leverantören av en allmänt tillgänglig elektronisk kommunikationstjänst skall vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa säkerheten i sina tjänster, om nödvändigt tillsammans med leverantören av det allmänna kommunikationsnätet när det gäller nätsäkerhet. Dessa åtgärder skall säkerställa en säkerhetsnivå som är anpassad till den risk som föreligger, med beaktande av dagens tillgängliga teknik och kostnaderna för att genomföra åtgärderna.

1a. Utan att det påverkar tillämpningen av direktiv 95/46/EG ska de åtgärder som avses i punkt 1 minst

– säkerställa att endast auktoriserad personal, och endast i lagligen tillåtna syften, får tillgång till personuppgifter,

– skydda personuppgifter som lagrats eller överförts mot oavsiktlig eller olaglig förstörelse, oavsiktlig förlust eller ändring samt mot icke auktoriserad eller olaglig lagring och behandling eller icke auktoriserat eller olagligt tillträde eller offentliggörande, och

– säkerställa införandet av en säkerhetsstrategi för behandling av personuppgifter.

…”

8 I artikel 5 i direktiv 2002/58, som har rubriken ”Konfidentialitet vid kommunikation”, anges följande:

”1. Medlemsstaterna skall genom nationell lagstiftning säkerställa konfidentialitet vid kommunikation och därmed förbundna trafikuppgifter via allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster. De skall särskilt förbjuda avlyssning, uppfångande med tekniskt hjälpmedel, lagring eller andra metoder som innebär att kommunikationen och de därmed förbundna trafikuppgifterna kan fångas upp eller övervakas av andra personer än användarna utan de berörda användarnas samtycke, utom när de har laglig rätt att göra detta i enlighet med artikel 15.1. Denna punkt får inte förhindra teknisk lagring som är nödvändig för överföring av kommunikationen utan att det påverkar principen om konfidentialitet.

…

3. Medlemsstaterna ska se till att lagring av information eller tillgång till information som redan är lagrad i en abonnents eller användares terminalutrustning endast är tillåten på villkor att abonnenten eller användaren i fråga har gett sitt samtycke efter att ha fått tillgång till tydlig och fullständig information, i enlighet med direktiv [95/46/], bland annat om ändamålen med behandlingen av uppgifterna. Detta får inte förhindra någon teknisk lagring eller åtkomst som endast sker för att utföra överföringen av en kommunikation via ett elektroniskt kommunikationsnät eller det som är absolut nödvändigt för att leverantören ska kunna tillhandahålla en av informationssamhällets tjänster som användaren eller abonnenten uttryckligen har begärt.”

9 I artikel 6 i direktiv 2002/58, med rubriken ”Trafikuppgifter”, anges följande:

”1. Trafikuppgifter om abonnenter och användare som behandlas och lagras av leverantören av ett allmänt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst skall utplånas eller avidentifieras när de inte längre behövs för sitt syfte att överföra en kommunikation, utan att det påverkar tillämpningen av punkterna 2, 3 och 5 i den här artikeln samt artikel 15.1.

2. Trafikuppgifter som krävs för abonnentfakturering och betalning av samtrafikavgifter får behandlas. Sådan behandling är tillåten endast fram till utgången av den period under vilken det lagligen går att göra invändningar mot fakturan eller kräva betalning.

3. I syfte att saluföra elektroniska kommunikationstjänster eller i syfte att tillhandahålla mervärdestjänster får en leverantör av en allmänt tillgänglig elektronisk kommunikationstjänst behandla de uppgifter som avses i punkt 1 i den utsträckning och under den tidsperiod som är nödvändig för sådana tjänster eller sådan marknadsföring, om den abonnent eller användare som

uppgifterna gäller i förväg har samtyckt till detta. Användare eller abonnenter skall ha möjlighet att när som helst dra tillbaka sitt samtycke till behandling av trafikuppgifter.

…

5. Behandlingen av trafikuppgifter skall, i enlighet med punkterna 1, 2, 3 och 4, begränsas till sådana personer som av leverantören av allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster getts i uppdrag att sköta fakturering, trafikstyrning, kundförfrågningar, spårning av bedrägerier, marknadsföring av elektroniska kommunikationstjänster eller tillhandahållande av en mervärdestjänst, och behandlingen skall begränsas till sådant som är nödvändigt för dessa verksamheter.”

10 Artikel 9 i direktivet har rubriken ”Andra lokaliseringsuppgifter än trafikuppgifter”. Artikel 9.1 stadgar följande:

”Om andra lokaliseringsuppgifter än trafikuppgifter som rör användare eller abonnenter av allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster kan behandlas, får dessa uppgifter endast behandlas sedan de har avidentifierats eller om användarna eller abonnenterna givit sitt samtycke, i den utsträckning och för den tid som krävs för tillhandahållandet av en mervärdestjänst. Innan användaren eller abonnenten ger sitt samtycke skall tjänsteleverantören informera denne om vilken typ av andra lokaliseringsuppgifter än trafikuppgifter som kommer att behandlas, behandlingens syfte och varaktighet samt om uppgifterna kommer att vidarebefordras till tredje part för tillhandahållande av mervärdestjänsten. …”

11 Artikel 15 i direktivet, med rubriken ”Tillämpningen av vissa bestämmelser i direktiv [95/46]”, har följande lydelse:

”1. Medlemsstaterna får genom lagstiftning vidta åtgärder för att begränsa omfattningen av de rättigheter och skyldigheter som anges i artikel 5, artikel 6, artikel 8.1, 8.2, 8.3 och 8.4 och artikel 9 i detta direktiv när en sådan begränsning i ett demokratiskt samhälle är nödvändig, lämplig och proportionell för att skydda nationell säkerhet (dvs. statens säkerhet), försvaret och allmän säkerhet samt för förebyggande, undersökning, avslöjande av och åtal för brott eller vid obehörig användning av ett elektroniskt kommunikationssystem enligt artikel 13.1 i direktiv [95/46]. Medlemsstaterna får för detta ändamål bland annat vidta lagstiftningsåtgärder som innebär att uppgifter får bevaras under en begränsad period som motiveras av de skäl som fastställs i denna punkt. Alla åtgärder som avses i denna punkt skall vara i enlighet med de allmänna principerna i gemenskapslagstiftningen, inklusive principerna i artikel 6.1 och 6.2 i Fördraget om Europeiska unionen.

…

1b. Leverantörerna ska införa interna förfaranden för att besvara förfrågningar om tillgång till användarnas personuppgifter, på grundval av nationella bestämmelser som antagits i enlighet med punkt 1. De ska på begäran förse den behöriga nationella myndigheten med information om dessa förfaranden, antalet förfrågningar som mottagits, vilken juridisk motivering som framförts och vilket svar leverantören lämnat.

2. Bestämmelserna om rättslig prövning, ansvar och sanktioner i kapitel III i direktiv [95/46] skall gälla för de nationella bestämmelser som antas i enlighet med det här direktivet och för de individuella rättigheter som kan härledas från det här direktivet.

…”

Direktiv 95/46

12 Artikel 22 i direktiv 95/46, som ingår i direktivets kapitel III, har följande lydelse:

”Medlemsstaterna skall – utan att det påverkar möjligheten att utnyttja något administrativt förfarande, till exempel vid den tillsynsmyndighet som avses i artikel 28, som kan användas innan ett ärende anhängiggörs hos en rättslig instans – föreskriva att var och en har rätt att föra talan inför domstol om sådana kränkningar av rättigheter som skyddas av den nationella lagstiftning som är tillämplig på ifrågavarande behandling.”

Direktiv 2006/24/EG

13 Artikel 1 i Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG (EUT L 105, 2006, s. 54), med rubriken ”Syfte och tillämpningsområde”, föreskrev följande i punkt 2:

”Detta direktiv skall gälla trafik- och lokaliseringsuppgifter om såväl fysiska som juridiska personer och enheter, samt de uppgifter som är nödvändiga för att kunna identifiera abonnenten eller den registrerade användaren. Det skall inte vara tillämpligt på innehållet i elektronisk kommunikation, inklusive sådan information som användaren sökt med hjälp av ett elektroniskt kommunikationsnät.”

14 Artikel 3 i direktivet, med rubriken ”Skyldighet att lagra uppgifter”, hade följande lydelse:

”1. Genom avvikelse från artiklarna 5, 6 och 9 i direktiv [2002/58] skall medlemsstaterna anta åtgärder för att säkerställa lagring enligt bestämmelserna i det här direktivet av de uppgifter som specificeras i artikel 5 i detta, i den utsträckning som de genereras eller behandlas av leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät inom statens territorium i samband med att leverantörerna levererar de kommunikationstjänster som berörs.

2. Den lagringsskyldighet som anges i punkt 1 skall inbegripa lagring av sådana uppgifter som anges i artikel 5 rörande misslyckade uppringningsförsök där uppgifter genereras eller behandlas, och lagras (uppgifter rörande telefoni) eller loggas (uppgifter rörande Internet) av leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät inom den berörda medlemsstatens jurisdiktion i samband med att de levererar de berörda kommunikationstjänsterna. Detta direktiv skall inte innebära krav på lagring av uppgifter rörande samtal som inte kopplats fram.”

Svensk rätt

15 Det framgår av begäran om förhandsavgörande i mål C-203/15 att den svenska lagstiftaren, i syfte att införliva direktiv 2006/24 med nationell rätt, ändrade lagen (2003:389) om elektronisk kommunikation (nedan kallad LEK) och förordningen (2003:396) om elektronisk

kommunikation. Båda dessa författningar, i deras tillämpliga lydelse i det nationella målet, innehåller bestämmelser om lagring av uppgifter om elektronisk kommunikation och om de nationella myndigheternas tillgång till dessa uppgifter.

16 Tillgång till uppgifterna regleras även i lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (nedan kallad inhämtningslagen) och i rättegångsbalken (nedan kallad RB).

Skyldigheten att lagra uppgifter om elektronisk kommunikation

17 Enligt vad Kammarrätten i Stockholm (nedan kallad Kammarrätten) har uppgett föreskriver 6 kap. 16 a § jämförd med 2 kap. 1 § LEK att leverantörer av elektroniska kommunikationstjänster är skyldiga att lagra sådana uppgifter som skulle lagras enligt direktiv 2006/24. Det gäller sådana uppgifter om abonnemang och om all elektronisk kommunikation som är nödvändiga för att finna och identifiera kommunikationskällan, slutmålet för kommunikationen, datum, tidpunkt och varaktighet för kommunikationen, typen av kommunikation, kommunikationsutrustning samt lokalisering av mobil kommunikationsutrustning vid kommunikationens början och slut. Skyldigheten att lagra uppgifterna omfattar uppgifter som genereras eller behandlas vid telefonitjänst, telefonitjänst via mobil anslutningspunkt, meddelandehantering, internetåtkomst och tillhandahållande av kapacitet för att få internetåtkomst (anslutningsform). Denna skyldighet innefattar även uppgifter om misslyckad uppringning. Den gäller dock inte kommunikationens innehåll.

18 I 38–43 §§ i förordningen (2003:396) om elektronisk kommunikation preciseras vilka kategorier av uppgifter som ska lagras. Beträffande telefonitjänster ska bland annat uppringande och uppringt nummer samt datum och spårbar tid då kommunikationen påbörjades och avslutades lagras. När det gäller telefonitjänster via mobil anslutningspunkt framgår att ytterligare krav gäller, till exempel att även lokaliseringsuppgifter för kommunikationens början och slut ska lagras. När det gäller telefonitjänster som använder IP-paket ska utöver vad som anges ovan bland annat även den uppringandes och den uppringdes IP-adresser lagras. När det gäller meddelandehantering ska bland annat avsändares och mottagares nummer, IP-adress eller annan meddelandeadress lagras. När det gäller internetåtkomst ska exempelvis användares IP-adress samt datum och spårbar tid för på- och avloggning i den tjänst som ger internetåtkomst lagras.

Lagringstid för uppgifterna

19 Av 6 kap. 16 d § LEK framgår att leverantörer av elektroniska kommunikationstjänster ska lagra sådana uppgifter som avses i 6 kap. 16 a § LEK i sex månader räknat från den dag kommunikationen avslutades. Därefter ska uppgifterna genast utplånas, om inte annat följer av 6 kap. 16 d § andra stycket LEK.

Tillgång till lagrade uppgifter

20 Tillgång till uppgifter som har lagrats av nationella myndigheter regleras i bestämmelser i inhämtningslagen, LEK och RB.

– *Inhämtningslagen*

21 Polismyndigheten, Säkerhetspolisen och Tullverket får med stöd av 1 § inhämtningslagen, under de förutsättningar som anges i denna lag, i underrättelseverksamhet i hemlighet från den som enligt LEK tillhandahåller ett elektroniskt kommunikationsnät eller elektroniska kommunikationstjänster hämta in uppgifter om meddelanden som har överförts i ett elektroniskt kommunikationsnät, vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område, eller i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits.

22 Uppgifterna får enligt 2 och 3 §§ inhämtningslagen hämtas in om omständigheterna är sådana att åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år, eller sådana brott som omfattas av uppräkningen i 3 §, vilket inkluderar brott för vilka lindrigare straff än fängelse i två år kan utdömas. Skälen för åtgärden ska uppväga det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktar sig mot eller för något annat motstående intresse. Enligt 5 § inhämtningslagen får den tid som åtgärden avser inte överstiga en månad.

23 Beslut om en sådan åtgärd fattas av myndighetschefen eller en annan anställd vid myndigheten som myndighetschefen delegerar beslutanderätten till. Beslutet är inte underkastat förhandskontroll av en domstol eller oberoende förvaltningsmyndighet.

24 Säkerhets- och integritetsskyddsnämnden ska enligt 6 § inhämtningslagen underrättas om ett beslut om inhämtning av uppgifter. Enligt 1 § lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet ska Säkerhets- och integritetsskyddsnämnden utöva tillsyn över brottsbekämpande myndigheters tillämpning av lagen.

– *LEK*

25 Av 6 kap. 22 § första stycket 2 LEK framgår att en leverantör av elektroniska kommunikationstjänster på begäran ska lämna ut abonnemangsuppgifter till åklagarmyndighet, Polismyndigheten, Säkerhetspolisen eller någon annan myndighet som ska ingripa mot brott, om uppgifterna gäller misstanke om brott. Enligt de upplysningar som Kammarrätten har lämnat krävs det inte att det är fråga om ett allvarligt brott.

– *RB*

26 RB reglerar kommunikation av uppgifter som lagrats av nationella myndigheter inom ramen för förundersökningar. Enligt 27 kap. 19 § RB får hemlig ”övervakning av elektronisk kommunikation” i princip användas vid en förundersökning om bland annat brott för vilket det inte är föreskrivet lindrigare straff än fängelse i sex månader. ”Övervakning av elektronisk kommunikation” innebär enligt 27 kap. 19 § RB att uppgifter i hemlighet hämtas in om meddelanden som överförs eller har överförts i ett elektroniskt kommunikationsnät, om vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område eller om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits.

27 Enligt de upplysningar som Kammarrätten har lämnat i mål C-203/15, kan uppgifter om innehållet i meddelanden inte inhämtas med stöd av 27 kap. 19 § RB. Av 27 kap. 20 § RB framgår att hemlig övervakning av elektronisk kommunikation som huvudregel endast får ske om någon är skäligen misstänkt för brottet och åtgärden är av synnerlig vikt för utredningen. Utredningen ska avse brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år eller försök, förberedelse eller stämpling till sådant brott, om en sådan gärning är belagd med straff. Enligt 27 kap. 21 § RB måste åklagaren, utom i brådskande fall, först inhämta rättens tillstånd till hemlig övervakning av elektronisk kommunikation.

Säkerhet och skydd för lagrade uppgifter

28 Av 6 kap. 3 a § LEK framgår att leverantörer av elektroniska kommunikationstjänster som är skyldiga att lagra uppgifter ska vidta de särskilda tekniska och organisatoriska åtgärder som behövs för att skydda de lagrade uppgifterna vid behandling. Enligt de upplysningar som Kammarrätten har lämnat saknas emellertid i svensk rätt bestämmelser om var lagring av uppgifterna får ske.

Lagstiftningen i Förenade kungariket

Dripa

29 Section 1 i Dripa, med rubriken ”Befogenheter vad gäller lagring av uppgifter om kommunikation som omfattas av säkerhetsåtgärder”, stadgar följande:

”(1) Inrikesministern får genom beslut (nedan kallat föreläggande om lagring) förelägga en offentlig teleoperatör att lagra relevanta uppgifter om kommunikation om denne finner att detta är nödvändigt och proportionerligt mot bakgrund av ett eller flera av de syften som avses i punkterna a–h i section 22(2) i Regulation of Investigatory Powers Act 2000 (2000 års lag om utredningsbefogenheter) (syften för vilka uppgifter får inhämtas).

(2) Ett föreläggande om lagring får
(a) riktas mot en viss operatör eller en viss kategori av operatörer,
(b) avse samtliga uppgifter eller vissa kategorier av uppgifter,
(c) avse en specifikt angiven period under vilken uppgifter ska lagras,
(d) innehålla andra krav eller begränsningar avseende lagringen av uppgifter,
(e) innehålla olika föreskrifter för olika syften,
(f) avse uppgifter oberoende av huruvida de existerar när föreläggandet utfärdas eller träder i kraft.

(3) Inrikesministern får i förordning utfärda ytterligare föreskrifter om lagring av relevanta uppgifter om kommunikation.

(4) Sådana föreskrifter kan särskilt avse
(a) villkor som ska vara uppfyllda innan ett föreläggande om lagring får utfärdas,
(b) den längsta tid under vilken uppgifter ska lagras enligt ett föreläggande om lagring,
(c) innehållet i ett föreläggande om lagring samt utfärdande, ikraftträdande, omprövning, ändring eller återkallande av ett sådant föreläggande,

(d) integriteten hos, säkerheten för eller skydd av uppgifter som lagrats med stöd av förevarande section samt tillgång till, utlämnande eller utplånande av sådana uppgifter,
(e) genomförandet av relevanta krav eller begränsningar, eller kontrollen av detta genomförande,
(f) riktlinjer rörande relevanta krav, begränsningar eller befogenheter,
(g) återbetalning från inrikesministern (eventuellt underkastad villkor) av utgifter som offentliga teleoperatörer haft för att följa relevanta krav eller begränsningar, eller
(h) den omständigheten att [Data Retention (EC Directive) Regulations 2009 (2009 års förordning om datalagring (EG-direktiv))] upphör att gälla, samt övergången till lagring av uppgifter enligt förevarande section.

(5) Den längsta lagringstid som fastställs enligt punkt 4 b får inte överskrida 12 månader från och med den dag som anges i fråga om sådana uppgifter som avses med bestämmelserna i punkt 3.

…”

30 Section 2 i Dripa definierar begreppet ”relevanta uppgifter om kommunikation” som ”relevanta uppgifter om sådan kommunikation som avses i bilagan till 2009 års förordning om datalagring (EG-direktiv) i den utsträckning dessa uppgifter har genererats eller behandlats i Förenade kungariket av offentliga teleoperatörer i samband med tillhandahållandet av de berörda telekommunikationstjänsterna”.

Ripa

31 Section 21 i Regulation of Investigatory Powers Act 2000 (2000 års lag om utredningsbefogenheter, nedan kallad Ripa) ingår i kapitel II i den lagen och har rubriken ”Inhämtning och utlämnande av uppgifter om kommunikation”. Section 21.4 har följande lydelse:

”I detta kapitel avses med 'uppgifter om kommunikation’ något av följande:

(a) alla trafikuppgifter som ingår i eller bifogats en kommunikation (av avsändaren eller annan) i fråga om varje system för posttjänster eller telekommunikation genom vilket uppgifter överförs eller kan överföras,

(b) all information som inte innefattar något innehåll i en kommunikation (förutom information som avses i punkt a och som rör en persons användande av
(i) en post- eller telekommunikationstjänst, eller
(ii) någon del av ett telekommunikationssystem i samband med tillhandahållande till en person eller en persons användande av en telekommunikationstjänst,

(c) all information som inte omfattas av punkt a eller b som, i förhållande till tjänstemottagarna, innehas eller erhålls av en person som tillhandahåller en post- eller telekommunikationstjänst.”

32 Enligt upplysningarna i begäran om förhandsavgörande i mål C-698/15 omfattar dessa uppgifter lokaliseringsuppgifterna för en användare men däremot inte innehållet i en kommunikation.

33 Vad gäller tillgång till lagrade uppgifter föreskriver section 22 i Ripa följande:

”(1) Denna section gäller när en ansvarig person enligt detta kapitel finner det nödvändigt, av skäl som omfattas av punkt 2 i denna section, att inhämta uppgifter om kommunikation.

(2) Det är nödvändigt att inhämta uppgifter om kommunikation av skäl som omfattas av denna punkt, om de är nödvändiga med hänsyn till
(a) skyddet av nationell säkerhet,
(b) förebyggande och upptäckande av brott eller förebyggande av störningar av den allmänna ordningen,
(c) Förenade kungarikets ekonomiska välstånd,
(d) skyddet av allmän säkerhet,
(e) skyddet av folkhälsan,
(f) fastställande och uppbörd av skatter och andra avgifter till offentliga myndigheter,
(g) förebyggande, i en nödsituation, av fara för liv eller skada på en persons fysiska eller psykiska hälsa eller lindring av skada på en persons fysiska eller psykiska hälsa, eller
(h) varje annat syfte (utöver vad som anges i punkterna a–g) som inrikesministern fastställer i föreskrifter.

(4) Om inte annat följer av punkt 5 kan den ansvariga personen, när denne bedömer att en teleoperatör eller postoperatör innehar, skulle kunna inneha eller skulle kunna ha kapacitet att inneha uppgifter, framställa en begäran till operatören om att denne
(a) ska inhämta uppgifterna, om denne inte redan innehar dem, och
(b) i alla händelser ska utlämna alla uppgifter som denne innehar eller som denne sedermera har inhämtat.

(5) Den ansvariga personen får endast ge tillstånd enligt punkt 3 eller framställa en begäran enligt punkt 4 om denne anser att inhämtning av uppgifterna i fråga genom ett handlande som är godkänt eller som fordras enligt ett tillstånd eller en begäran är proportionerlig mot det mål som eftersträvas med inhämtning av uppgifterna.”

34 Enligt section 65 i Ripa kan klagomål ges in till Investigatory Powers Tribunal (domstol för utredningsbefogenheter, Förenade kungariket) om det finns misstanke om att uppgifter har inhämtats på felaktiga grunder.

Data Retention Regulations 2014

35 Data Retention Regulations 2014 (2014 års förordning om datalagring), som antagits med stöd av Dripa, är indelad i tre delar. Den andra delen omfattar sections 2–14 i förordningen. Section 4, med rubriken ”Föreläggande om lagring”, föreskriver följande:

”(1) Ett föreläggande om lagring ska ange
(a) den offentliga teleoperatör (eller en beskrivning av de operatörer) som föreläggandet är riktat till,
(b) de relevanta uppgifter om kommunikation som ska lagras,
(c) den period eller de perioder under vilken eller vilka uppgifterna ska lagras, och
(d) övriga krav eller begränsningar avseende lagringen av uppgifter.

(2) Ett föreläggande om lagring kan inte fordra att en uppgift lagras i mer än 12 månader, räknat från
   (a) dagen för den berörda kommunikationen, när det gäller trafikuppgifter eller uppgifter om användningen av tjänsten, och
   (b) den dag då den berörda personen avslutar kommunikationstjänsten i fråga, alternativt den dag då uppgiften ändras (om detta inträffar dessförinnan), när det gäller abonnentuppgifter.

…”

36 Enligt section 7 i förordningen, med rubriken ”Uppgifternas integritet och säkerhet”, gäller följande:

”(1) En offentlig teleoperatör som lagrar uppgifter i enlighet med section 1 i [Dripa] ska
   (a) säkerställa att de lagrade uppgifterna har samma integritet och ges samma säkerhet och skydd som uppgifterna i de system de härrör från,
   (b) säkerställa, genom lämpliga tekniska och organisatoriska åtgärder, att endast personal med särskilt tillstånd kan få tillgång till uppgifterna, och
   (c) genom lämpliga tekniska och organisatoriska åtgärder, skydda uppgifterna mot olaglig förstöring och oavsiktlig förlust eller ändring och mot otillåten eller olaglig lagring av, behandling av, tillgång till eller avslöjande av uppgifterna.

(2) En offentlig teleoperatör som lagrar uppgifter om kommunikation i enlighet med section 1 i [Dripa] måste förstöra uppgifterna om lagringen inte längre är tillåten enligt den bestämmelsen och inte heller i övrigt är tillåten enligt lag.

(3) Kravet i punkt 2 att förstöra uppgifter innebär att uppgifterna ska raderas på ett sådant sätt att det är omöjligt att få tillgång till dessa uppgifter.

(4) Det räcker för operatören att vidta åtgärder för att radera uppgifter månatligen eller med kortare mellanrum alltefter operatörens praktiska möjligheter.”

37 Section 8 i förordningen har rubriken ”Utlämnande av lagrade uppgifter” och föreskriver följande:

”(1) En offentlig teleoperatör ska inrätta lämpliga säkerhetssystem (inbegripet tekniska och organisatoriska åtgärder) för att bestämma tillgången till uppgifter om kommunikation som lagrats i enlighet med section 1 i [Dripa] för att förhindra att uppgifter lämnas ut om så inte föreskrivs i section 1.6 a i [Dripa].

(2) En offentlig teleoperatör som lagrar uppgifter i enlighet med section 1 i [Dripa] ska lagra uppgifterna på ett sådant sätt att operatören utan oskäligt dröjsmål kan föra över dem på begäran.”

38 I section 9 i samma förordning, under rubriken ”Datainspektionens tillsyn”, anges följande:

”Datainspektionen (*Information Commissioner*) ska tillse att de krav eller begränsningar som föreskrivs i denna del iakttas, rörande integriteten hos och säkerheten för samt förstörelse av lagrade uppgifter enligt section 1 i [Dripa].”

Riktlinjerna

39 Acquisition and Disclosure of Communications Data Code of Practice (riktlinjer för inhämtning och utlämnande av uppgifter om kommunikation, nedan kallade riktlinjerna) innehåller, i punkterna 2.5–2.9 och 2.36–2.45, hållpunkter rörande nödvändighet och proportionalitet vid inhämtning av uppgifter om kommunikation. Enligt de upplysningar som den hänskjutande domstolen i mål C-698/15 har lämnat, ska enligt punkterna 3.72–3.77 i riktlinjerna särskild vikt läggas vid kriterierna rörande nödvändighet och proportionalitet när de eftersökta uppgifterna avser en person som tillhör en yrkeskår som handhar information som erhållits under tystnadsplikt eller annan konfidentiell information.

40 För att inhämta uppgifter om kommunikation i syfte att identifiera en journalists källa krävs enligt punkterna 3.78–3.84 i riktlinjerna beslut av domstol. Enligt punkterna 3.85–3.87 i riktlinjerna krävs tillstånd av domstol i fråga om en ansökan om tillgång till uppgifter som inges av lokala myndigheter. Däremot finns det inte något krav på tillstånd från en domstol eller ett oberoende organ för tillgång till uppgifter om kommunikation som omfattas av advokatsekretess eller som rör läkare, parlamentsledamöter eller präster.

41 Enligt punkt 7.1 i riktlinjerna måste uppgifter om kommunikation som har inhämtats eller erhållits med stöd av Ripa samt alla kopior, utdrag och sammanfattningar av uppgifterna hanteras och förvaras på ett säkert sätt. Vidare måste kraven i Data Protection Act (dataskyddslagen) iakttas.

42 När en myndighet i Förenade kungariket överväger att lämna ut uppgifter om kommunikation till utländska myndigheter, ska den enligt punkt 7.18 i riktlinjerna bland annat pröva om uppgifterna kommer att få tillräckligt skydd. Det framgår dock av punkt 7.22 i riktlinjerna att uppgifter får föras över till ett tredjeland om det behövs med hänsyn till ett viktigt allmänt intresse, även när tredjelandet inte garanterar en lämplig skyddsnivå. Enligt de upplysningar som den hänskjutande domstolen i mål C-698/15 har lämnat, får inrikesministern utfärda ett nationellt säkerhetscertifikat som undantar vissa uppgifter från lagstiftningens krav.

43 I punkt 8.1 i riktlinjerna erinras om att det genom Ripa inrättats en tillsynsmyndighet för avlyssning av kommunikation (*Interception of Communications Commissioner*) i Förenade kungariket, som ska utöva oberoende tillsyn över utövandet och genomförandet av befogenheter och skyldigheter enligt kapitel II i del I i Ripa. Som framgår av punkt 8.3 i riktlinjerna, får den myndigheten underrätta en person om en misstänkt felaktig användning av befogenheter om myndigheten kan ”styrka att en enskild har lidit skada till följd av ett uppsåtligt eller grovt oaktsamt åsidosättande”.

Målen vid de nationella domstolarna och tolkningsfrågorna

Mål C-203/15

44 Den 9 april 2014 underrättade Tele2 Sverige – en leverantör av elektroniska kommunikationstjänster etablerad i Sverige – PTS om att bolaget, efter att direktiv 2006/24 förklarats ogiltigt genom dom av den 8 april 2014, Digital Rights Ireland m.fl. (C-293/12 och C-594/12, nedan kallad Digital Rights-domen, EU:C:2014:238), från den 14 april 2014 avsåg att upphöra med att lagra uppgifter om elektronisk kommunikation i enlighet med LEK samt radera de uppgifter som lagrats fram till den tidpunkten.

45 Den 15 april 2014 inkom Rikspolisstyrelsen med en anmälan till PTS av vilken det framgick att Tele2 Sverige hade upphört med leveranser av dessa uppgifter till polisen.

46 Den 29 april 2014 tillsatte justitieministern en särskild utredare som skulle granska de svenska reglernas tillämplighet mot bakgrund av Digital Rights-domen. I en promemoria av den 13 juni 2014 (”Datalagring, EU-rätten och svensk rätt”, Ds 2014:23) (nedan kallad promemorian) fann utredaren att det svenska regelverket avseende lagring enligt 6 kap. 16 a–f §§ LEK inte strider mot unionsrätten eller mot Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, som undertecknades i Rom den 4 november 1950 (nedan kallad Europakonventionen). Enligt den särskilda utredaren kunde Digital Rights-domen inte tolkas som att den kritiserade själva grundtanken med en generell och odifferentierad lagring av uppgifter. Domen skulle inte heller tolkas på så sätt att domstolen där presenterat en lista där alla punkter måste vara uppfyllda för att regleringen ska anses vara proportionerlig. Den svenska lagstiftningens förenlighet med unionsrätten kan avgöras först vid en sammantagen bedömning av alla omständigheter. Bland dessa omständigheter ingår lagringens omfattning i förhållande till bestämmelserna om tillgång till uppgifterna, lagringstiden samt skydd och säkerhet för uppgifterna.

47 Mot bakgrund av ovanstående underrättade PTS den 19 juni 2014 Tele2 Sverige om att bolaget inte uppfyllde skyldigheten enligt nationell lagstiftning att för brottsbekämpande ändamål lagra de uppgifter som avses i LEK i sex månader. PTS förelade den 27 juni 2014 bolaget att senast den 25 juli 2014 lagra dessa uppgifter.

48 Tele2 Sverige ansåg att promemorian grundade sig på en felaktig tolkning av Digital Rights-domen och att skyldigheten att lagra uppgifterna stred mot de grundläggande rättigheterna enligt stadgan. Bolaget överklagade därför föreläggandet av den 27 juni 2014 till Förvaltningsrätten i Stockholm. Förvaltningsrätten ogillade överklagandet genom dom av den 13 oktober 2014. Tele2 Sverige överklagade den domen till Kammarrätten.

49 Enligt Kammarrätten måste den svenska lagstiftningens förenlighet med unionsrätten prövas mot bakgrund av artikel 15.1 i direktiv 2002/58. Utgångspunkten enligt det direktivet är att trafikuppgifter och lokaliseringsuppgifter ska utplånas eller avidentifieras när de inte längre behövs för sitt syfte att överföra kommunikationen. Artikel 15.1 i direktivet innehåller emellertid ett undantag från den utgångspunkten, såtillvida att medlemsstaterna tillåts att begränsa ovan nämnda krav på utplåning eller avidentifiering eller rentav föreskriva att uppgifter måste lagras. Unionsrätten medger således att uppgifter om elektronisk kommunikation lagras i vissa fall.

50 Kammarrätten frågar sig emellertid om en generell och odifferentierad skyldighet att lagra uppgifter om elektronisk kommunikation, såsom den som är i fråga i det nationella målet, mot bakgrund av Digital Rights-domen är förenlig med artikel 15.1 i direktiv 2002/58 jämförd med artiklarna 7, 8 och 52.1 i stadgan. Med hänsyn till att parterna har olika uppfattningar i frågan, är det lämpligt att EU-domstolen uttalar sig entydigt om huruvida, som Tele2 Sverige anser, en generell och odifferentierad lagring av uppgifter om elektronisk kommunikation i sig är oförenlig med artiklarna 7, 8 och 52.1 i stadgan, eller huruvida, såsom anges i promemorian, förenligheten av en sådan lagring måste bedömas utifrån bestämmelserna om tillgång till uppgifterna, skydd och säkerhet för uppgifterna samt lagringstiden.

51 Mot denna bakgrund beslutade Kammarrätten att vilandeförklara målet och ställa följande frågor till EU-domstolen:

”1) Är en generell skyldighet att lagra trafikuppgifter som omfattar samtliga personer, samtliga elektroniska kommunikationsmedel och samtliga trafikuppgifter utan att det görs några åtskillnader, begränsningar eller undantag utifrån syftet att bekämpa brott … förenlig med artikel 15.1 i direktiv 2002/58 med beaktande av artiklarna 7, 8 och 52.1 i stadgan?

2) Om svaret på fråga 1 är nej, kan lagringen ändå vara tillåten
   a) om de nationella myndigheternas tillgång till de uppgifter som lagras är fastställd så som beskrivs i punkterna 19–36 [i begäran om förhandsavgörande], och
   b) om kraven på säkerhet regleras så som beskrivs i punkterna 38–43 [i begäran om förhandsavgörande], samt då
   c) samtliga aktuella uppgifter ska lagras i sex månader räknat från den dag kommunikationen avslutades och därefter utplånas så som beskrivs i punkt 37 [i begäran om förhandsavgörande]?”

Mål C-698/15

52 Tom Watson, Peter Brice och Geoffrey Lewis har var och en väckt talan vid High Court of Justice (England & Wales), Queens’ Bench Division (Divisional Court) (Överdomstolen för England och Wales, avdelningen för överprövning av rättsfrågor, Förenade kungariket) och begärt en laglighetsprövning av section 1 i Dripa. De har bland annat anfört att den bestämmelsen är oförenlig med artiklarna 7 och 8 i stadgan och med artikel 8 i Europakonventionen.

53 I dom av den 17 juli 2015 fann High Court of Justice (England & Wales), Queens’ Bench Division (Divisional Court) (Överdomstolen för England och Wales, avdelningen för överprövning av rättsfrågor) att Digital Rights-domen uppställde ”tvingande unionsrättsliga krav” som gäller medlemsstaternas bestämmelser om lagring av uppgifter om kommunikation och tillgången till sådana uppgifter. Enligt nämnda domstol kunde en nationell lagstiftning med samma innehåll som direktiv 2006/24 inte längre vara förenlig med proportionalitetsprincipen, eftersom EU-domstolen i Digital Rights-domen slagit fast att direktivet var oförenligt med den principen. Av den underliggande logiken i Digital Rights-domen följer att en lagstiftning som inrättar ett generellt system för lagring av uppgifter om kommunikation kränker de rättigheter som garanteras i artiklarna 7 och 8 i stadgan, såvida inte den lagstiftningen kompletteras med ett i nationell rätt definierat system för tillgång till uppgifter som ger tillräckliga garantier för skydd av dessa rättigheter. Section 1 i Dripa är således inte förenlig med artiklarna 7 och 8 i stadgan, då den inte innehåller tydliga och precisa bestämmelser om tillgång till och användning av lagrade uppgifter och då den inte villkorar tillgången till dessa uppgifter med en förhandskontroll av en domstol eller ett oberoende förvaltningsorgan.

54 Inrikesministern överklagade den domen till Court of Appeal (England & Wales) (Civil Division) (Appellationsdomstolen för England och Wales, avdelningen för tvistemål och förvaltningsmål, Förenade kungariket) (nedan kallad Court of Appeal).

55 Den domstolen har anfört att inrikesministern enligt section 1.1 i Dripa utan förhandstillstånd från en domstol eller ett oberoende förvaltningsorgan får föreskriva en allmän ordning som ålägger offentliga teleoperatörer att lagra alla uppgifter i fråga om varje system för posttjänster eller telekommunikationer under högst 12 månader, om ministern bedömer att ett sådant krav är

nödvändigt och proportionerligt för att uppnå de mål som anges i Förenade kungarikets lagstiftning. Även om dessa uppgifter inte innefattar innehållet i en kommunikation, skulle de kunna vara särskilt ingripande i privatlivet för kommunikationstjänsternas användare.

56 Den hänskjutande domstolen har i beslutet om hänskjutande och i sitt avgörande av den 20 november 2015, som meddelades inom ramen för målet om överklagande och där den beslutade att begära förhandsavgörande från EU-domstolen anfört att de nationella bestämmelserna om lagring av uppgifter med nödvändighet omfattas av artikel 15.1 i direktiv 2002/58 och således måste iaktta de krav som följer av stadgan. Enligt artikel 1.3 i direktivet har unionslagstiftaren emellertid inte harmoniserat bestämmelserna om tillgång till lagrade uppgifter.

57 Vad gäller Digital Rights-domens inverkan på de frågor som aktualiserats i det nationella målet, har den hänskjutande domstolen anfört att EU-domstolen i det mål som avgjordes genom Digital Rights-domen hade att pröva giltigheten av direktiv 2006/24, inte giltigheten av den nationella lagstiftningen. Med hänsyn bland annat till det nära sambandet mellan lagring av uppgifter och tillgång till uppgifterna, var det nödvändigt att direktivet åtföljdes av en rad garantier och att EU-domstolen i Digital Rights-domen, som ett led i prövningen av lagenligheten av direktivets bestämmelser om lagring av uppgifter, även bedömde bestämmelserna om tillgången till dessa uppgifter. Domstolen hade således i den domen inte i åtanke att formulera några tvingande krav på nationell lagstiftning rörande tillgång till uppgifter som inte genomför unionsrätten. Domstolens resonemang var vidare nära kopplat till direktivets syfte. En nationell lagstiftning måste dock bedömas utifrån syftena med den lagstiftningen och det sammanhang den ingår i.

58 Vad gäller behovet av att begära ett förhandsavgörande från EU-domstolen, har den hänskjutande domstolen betonat att vid den tidpunkt då den fattade beslut om hänskjutande, hade sex domstolar i andra medlemsstater, däribland fem i högsta instans, ogiltigförklarat nationell lagstiftning med stöd av Digital Rights-domen. Svaret på de frågor som aktualiseras är således inte uppenbart, och det är nödvändigt att besvara dem för att kunna avgöra de nationella målen.

59 Mot denna bakgrund beslutade Court of Appeal (England & Wales) (Civil Division) (Appellationsdomstolen för England och Wales, avdelningen för tvistemål och förvaltningsmål) att vilandeförklara målen och ställa följande frågor till EU-domstolen:

”1) Innebär Digital Rights-domen (särskilt punkterna 60–62) att det i unionsrätten uppställs tvingande krav som en medlemsstats nationella bestämmelser om tillgång till uppgifter som lagrats i enlighet med nationell lagstiftning måste uppfylla för att vara förenliga med artiklarna 7 och 8 i stadgan?

2) Innebär Digital Rights-domen att artikel 7 och/eller artikel 8 i stadgan ges ett mer vidsträckt tillämpningsområde än artikel 8 i Europakonventionen såsom den bestämmelsens tillämpningsområde har fastställts i praxis från Europeiska domstolen för de mänskliga rättigheterna (Europadomstolen)?”

Förfarandet vid domstolen

60 Genom beslut av den 1 februari 2016, Davis m.fl. (C-698/15, ej publicerat, EU:C:2016:70) biföll domstolens ordförande begäran från Court of Appeal (England & Wales) (Civil Division) (Appellationsdomstolen för England och Wales, avdelningen för tvistemål och förvaltningsmål) om att mål C-698/15 skulle handläggas skyndsamt i enlighet med artikel 105.1 i domstolens rättegångsregler.

61 Genom beslut av domstolens ordförande av den 10 mars 2016 förenades målen C-203/15 och C-698/15 vad gäller det muntliga förfarandet och domen.

Prövning av tolkningsfrågorna

Den första frågan i mål C-203/15

62 Kammarrätten har ställt den första frågan i mål C-203/15 för att få klarhet i huruvida artikel 15.1 i direktiv 2002/58 jämförd med artiklarna 7, 8 och 52.1 i stadgan ska tolkas på så sätt att den utgör hinder för en nationell lagstiftning – som den i det nationella målet – som i brottsbekämpande syfte föreskriver en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter avseende samtliga abonnenter och registrerade användare och samtliga elektroniska kommunikationsmedel.

63 Frågan har uppkommit bland annat av den anledningen att direktiv 2006/24, som den berörda svenska lagstiftningen syftade till att införliva, förklarades ogiltigt genom Digital Rights-domen, men parterna är oense om räckvidden av den domen och dess inverkan på nämnda lagstiftning, vilken reglerar lagring av trafikuppgifter och lokaliseringsuppgifter samt de nationella myndigheternas tillgång till dessa uppgifter.

64 Domstolen ska inledningsvis pröva om sådan nationell lagstiftning som den som är i fråga i målet omfattas av unionsrättens tillämpningsområde.

Tillämpningsområdet för direktiv 2002/58

65 De medlemsstater som har yttrat sig skriftligen till domstolen har uttryckt skilda meningar om huruvida, och i så fall i vilken utsträckning, nationell lagstiftning som reglerar lagring av trafikuppgifter och lokaliseringsuppgifter samt nationella myndigheters tillgång till sådana uppgifter, i brottsbekämpande syfte, omfattas av tillämpningsområdet för direktiv 2002/58. Enligt den belgiska, den danska, den tyska, den estniska regeringen och Irland samt den nederländska regeringen bör denna fråga besvaras jakande, medan den tjeckiska regeringen har föreslagit att den ska besvaras nekande, eftersom sådan lagstiftning har brottsbekämpning som enda syfte. Förenade kungarikets regering har gjort gällande att endast lagstiftning om lagring av uppgifter, men däremot inte lagstiftning om behöriga nationella brottsbekämpande myndigheters tillgång till sådana uppgifter, omfattas av direktivets tillämpningsområde.

66 Slutligen har kommissionen, i sitt skriftliga yttrande till domstolen i mål C-203/15, hävdat att den svenska lagstiftning som är i fråga i det målet omfattas av tillämpningsområdet för direktiv 2002/58. Samtidigt har den i sitt skriftliga yttrande i mål C-698/15 anfört att direktivets tillämpningsområde endast omfattar nationella bestämmelser som reglerar lagring av uppgifter,

och inte bestämmelser som reglerar nationella myndigheters tillgång till uppgifterna. De sistnämnda bestämmelserna ska dock enligt kommissionen beaktas vid bedömningen av om en nationell lagstiftning som reglerar lagring av uppgifter hos leverantörer av elektroniska kommunikationstjänster utgör ett proportionerligt ingrepp i de grundläggande rättigheter som garanteras i artiklarna 7 och 8 i stadgan.

67 Domstolen vill i det sammanhanget påpeka att tillämpningsområdet för direktiv 2002/58 ska bedömas med hänsyn bland annat till direktivets allmänna systematik.

68 Enligt lydelsen i artikel 1.1 i direktiv 2002/58 harmoniserar direktivet bland annat medlemsstaternas bestämmelser för att säkerställa ett likvärdigt skydd av de grundläggande fri- och rättigheterna, i synnerhet rätten till integritet och konfidentialitet, när det gäller behandling av personuppgifter inom sektorn för elektronisk kommunikation.

69 Enligt artikel 1.3 i direktiv 2002/58 ska direktivet inte tillämpas på ”statens verksamhet” på de områden som avses här, det vill säga bland annat statens verksamhet på straffrättens område och verksamheter som avser allmän säkerhet, försvar och statens säkerhet, inbegripet statens ekonomiska välstånd när verksamheten rör statens säkerhet (se analogt, beträffande artikel 3.2 första strecksatsen i direktiv 95/46, dom av den 6 november 2003, Lindqvist, C-101/01, EU:C:2003:596, punkt 43, och dom av den 16 december 2008, Satakunnan Markkinapörssi och Satamedia, C-73/07, EU:C:2008:727, punkt 41).

70 Artikel 3 i direktiv 2002/58 anger att direktivet ska tillämpas på behandling av personuppgifter i samband med att allmänt tillgängliga elektroniska kommunikationstjänster tillhandahålls i allmänna kommunikationsnät inom unionen, inbegripet allmänna kommunikationsnät som stöder datainsamling och identifieringsutrustning (nedan kallade elektroniska kommunikationstjänster). Direktivet ska därför anses reglera verksamheten för leverantörer av sådana tjänster.

71 Artikel 15.1 i direktiv 2002/58 låter medlemsstaterna, på de villkor den föreskriver, ”genom lagstiftning vidta åtgärder för att begränsa omfattningen av de rättigheter och skyldigheter som anges i artikel 5, artikel 6, artikel 8.1, 8.2, 8.3 och 8.4 och artikel 9 i detta direktiv”. Artikel 15.1 andra meningen i samma direktiv nämner, som exempel på åtgärder som medlemsstaterna får vidta, åtgärder ”som innebär att uppgifter får bevaras”.

72 De lagstiftningsåtgärder som avses i artikel 15.1 i direktiv 2002/58 avser förvisso sådan verksamhet som endast kan bedrivas av staten eller statliga myndigheter och som inte kan bedrivas av enskilda personer (se, för ett liknande resonemang, dom av den 29 januari 2008, Promusicae, C-275/06, EU:C:2008:54, punkt 51). De syften som dessa åtgärder ska ha enligt nämnda bestämmelse, det vill säga att skydda nationell säkerhet, försvaret och allmän säkerhet samt att förebygga, undersöka, avslöja och väcka åtal för brott eller vid obehörig användning av ett elektroniskt kommunikationssystem, sammanfattar också väsentligen syftena med de verksamheter som avses i artikel 1.3 i direktivet.

73 Sett till den allmänna systematiken i direktiv 2002/58 betyder dock inte de omständigheter som nämns i föregående punkt att de lagstiftningsåtgärder som avses i artikel 15.1 i direktivet ska anses uteslutna från direktivets tillämpningsområde. Det skulle helt frånta den bestämmelsen dess ändamålsenliga verkan. Nämnda bestämmelse förutsätter nämligen med nödvändighet att de där avsedda nationella åtgärderna, såsom de om lagring av uppgifter i brottsbekämpande syfte,

omfattas av direktivets tillämpningsområde, eftersom direktivet uttryckligen tillåter medlemsstaterna att vidta sådana åtgärder endast under förutsättning att de däri angivna villkoren är uppfyllda.

74 De lagstiftningsåtgärder som avses i artikel 15.1 i direktiv 2002/58 reglerar dessutom – för de syften som anges i bestämmelsen – verksamheten för leverantörer av elektroniska kommunikationstjänster. Den bestämmelsen, jämförd med artikel 3 i samma direktiv, ska därför tolkas på så sätt att sådana lagstiftningsåtgärder omfattas av direktivets tillämpningsområde.

75 I tillämpningsområdet ingår i synnerhet en lagstiftningsåtgärd, såsom den som är i fråga i det nationella målet, som ålägger sådana leverantörer en skyldighet att lagra trafikuppgifter och lokaliseringsuppgifter. Deras verksamhet innebär nämligen med nödvändighet att de behandlar personuppgifter.

76 Tillämpningsområdet inkluderar även en lagstiftningsåtgärd som, såsom i det nationella målet, innebär att nationella myndigheter får tillgång till uppgifter som lagrats av leverantörer av elektroniska kommunikationstjänster.

77 Skyddet för konfidentialitet vid elektronisk kommunikation och för därmed förbundna trafikuppgifter, som säkerställs i artikel 5.1 i direktiv 2002/58, gäller för åtgärder som vidtas av andra personer än användarna, oavsett om de är privatpersoner eller privata enheter eller om de är statliga enheter. Som bekräftas av skäl 21 i samma direktiv, syftar direktivet till att hindra obehörig åtkomst av kommunikation, inbegripet ”uppgifter som har samband med sådan kommunikation”, för att skydda konfidentialiteten vid elektronisk kommunikation.

78 En lagstiftningsåtgärd genom vilken en medlemsstat med stöd av artikel 15.1 i direktiv 2002/58 ålägger leverantörer av elektronisk kommunikation att, för de syften som nämns i denna bestämmelse, ge de nationella myndigheterna tillgång till uppgifter som leverantörerna lagrat, på de villkor som föreskrivs genom åtgärden, rör följaktligen behandling av personuppgifter från leverantörernas sida, och denna behandling omfattas av direktivets tillämpningsområde.

79 Då datalagringen endast sker för att i förekommande fall ge behöriga nationella myndigheter tillgång till uppgifterna, måste dessutom en nationell lagstiftning som föreskriver att uppgifter ska lagras i princip innehålla bestämmelser om behöriga nationella myndigheters tillgång till de uppgifter som lagrats av leverantörer av elektroniska kommunikationstjänster.

80 Den tolkningen får också stöd av artikel 15.1b i direktiv 2002/58, enligt vilken leverantörerna ska införa interna förfaranden för att besvara förfrågningar om tillgång till användarnas personuppgifter, på grundval av nationella bestämmelser som antagits med stöd av artikel 15.1 i direktivet.

81 Av vad som anförts följer att nationell lagstiftning av det slag som är i fråga i de båda nationella målen omfattas av tillämpningsområdet för direktiv 2002/58.

Tolkningen av artikel 15.1 i direktiv 2002/58, mot bakgrund av artiklarna 7, 8, 11 och 52.1 i stadgan

82 Enligt artikel 1.2 i direktiv 2002/58 ska bestämmelserna i detta direktiv ”precisera och komplettera” direktiv 95/46. Som framgår av skäl 2 i direktiv 2002/58, eftersträvas i detta direktiv i synnerhet att säkerställa full respekt för rättigheterna i artiklarna 7 och 8 i stadgan. Det

framgår av redogörelsen för skälen i förslaget till Europaparlamentets och rådets direktiv om behandling av personuppgifter och skydd för privatlivet inom sektorn för elektronisk kommunikation (KOM/2000/385 slutlig), som låg till grund för direktiv 2002/58, att unionslagstiftaren avsett att ”garantera en fortsatt hög skyddsnivå för personuppgifter och privatliv för alla elektroniska kommunikationstjänster, oavsett vilken teknik som används”.

83 Direktiv 2002/58 innehåller specifika bestämmelser för detta ändamål, vilka – såsom framgår av bland annat skälen 6 och 7 – syftar till att skydda användarna av elektroniska kommunikationstjänster mot de risker för deras personuppgifter och integritet som ny teknik och den ökade kapaciteten för automatisk lagring och behandling av uppgifter medför.

84 Enligt artikel 5.1 i direktiv 2002/58 ska medlemsstaterna genom nationell lagstiftning säkerställa konfidentialitet vid kommunikation via allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster liksom för därmed förbundna trafikuppgifter.

85 Principen om konfidentialitet vid kommunikation som infördes genom direktiv 2002/58 innebär bland annat, som framgår av artikel 5.1 andra meningen i direktivet, i princip förbud för andra personer än användarna att utan användarnas samtycke lagra trafikuppgifter avseende elektronisk kommunikation. Undantag gäller endast för personer som har laglig rätt att göra detta i enlighet med artikel 15.1 i direktivet, samt för teknisk lagring som är nödvändig för överföring av kommunikationen (se, för ett liknande resonemang, dom av den 29 januari 2008, Promusicae, C-275/06, EU:C:2008:54, punkt 47).

86 Enligt artikel 6 i direktiv 2002/58, och som också framgår av skälen 22 och 26 i direktivet, får trafikuppgifter behandlas och lagras i den utsträckning och under den tid som krävs för att kunna fakturera för tjänster, marknadsföra tjänster eller tillhandahålla kringtjänster (se, för ett liknande resonemang, dom av den 29 januari 2008, Promusicae, C-275/06, EU:C:2008:54, punkterna 47 och 48). Vad specifikt gäller fakturering för tjänster, är sådan behandling endast tillåten fram till utgången av den period under vilken det lagligen går att göra invändningar mot fakturan eller kräva betalning. När den perioden har löpt ut, ska de behandlade och lagrade uppgifterna utplånas eller avidentifieras. Vad gäller andra lokaliseringsuppgifter än trafikuppgifter, föreskriver artikel 9.1 i direktivet att de endast får behandlas på vissa villkor och sedan de har avidentifierats eller om användarna eller abonnenterna gett sitt samtycke.

87 Räckvidden av bestämmelserna i artiklarna 5, 6 och 9.1 i direktiv 2002/58, som syftar till att säkerställa konfidentialitet vid kommunikation och därmed förbundna trafikuppgifter och minimera riskerna för missbruk, ska vidare bedömas mot bakgrund av skäl 30 i direktivet. Där anges att ”[s]ystemen för tillhandahållande av elektroniska kommunikationsnät och elektroniska kommunikationstjänster bör utformas så att mängden nödvändiga personuppgifter begränsas till ett absolut minimum”.

88 Artikel 15.1 i direktiv 2002/58 ger förvisso medlemsstaterna möjlighet att föreskriva undantag från deras principiella skyldighet enligt artikel 5.1 i samma direktiv att garantera konfidentialiteten för personuppgifter liksom från motsvarande skyldigheter enligt bland annat artiklarna 6 och 9 i direktivet (se, för ett liknande resonemang, dom av den 29 januari 2008, Promusicae, C-275/06, EU:C:2008:54, punkt 50).

89 I och med att artikel 15.1 i direktiv 2002/58 ger medlemsstaterna möjlighet att begränsa omfattningen av den principiella skyldigheten att säkerställa konfidentialiteten för kommunikation och därmed förbundna trafikuppgifter, ska denna artikel emellertid enligt

domstolens fasta praxis tolkas strikt (se, analogt, dom av den 22 november 2012, Probst, C-119/12, EU:C:2012:748, punkt 23). En sådan bestämmelse kan alltså inte motivera att undantaget från denna principiella skyldighet, i synnerhet förbudet i artikel 5 i direktivet mot att lagra dessa uppgifter, görs till huvudregel. Det skulle i stor utsträckning förta verkan av sistnämnda bestämmelse.

90 Artikel 15.1 första meningen i direktiv 2002/58 föreskriver att de lagstiftningsåtgärder som den bestämmelsen avser och som avviker från principen om konfidentialitet för kommunikationer och därmed förbundna trafikuppgifter ska syfta till att ”skydda nationell säkerhet (dvs. statens säkerhet), försvaret och allmän säkerhet samt för förebyggande, undersökning, avslöjande av och åtal för brott eller vid obehörig användning av ett elektroniskt kommunikationssystem” eller ha ett annat syfte enligt artikel 13.1 i direktiv 95/46, som artikel 15.1 första meningen i direktiv 2002/58 hänvisar till (se, för ett liknande resonemang, dom av den 29 januari 2008, Promusicae, C-275/06, EU:C:2008:54, punkt 53). Denna uppräkning av syftena är uttömmande, vilket också framgår av artikel 15.1 andra meningen i direktivet, enligt vilken lagstiftningsåtgärder ska vara motiverade av ”de skäl” som fastställs i artikel 15.1 första meningen. Medlemsstaterna kan alltså inte anta sådana åtgärder för andra syften än de som räknas upp i artikel 15.1 första meningen i direktiv 2002/58.

91 Vidare föreskrivs i artikel 15.1 tredje meningen i direktiv 2002/58 att ”[a]lla åtgärder som avses i [artikel 15.1 i direktivet] skall vara i enlighet med de allmänna principerna i [union]slagstiftningen, inklusive principerna i artikel 6.1 och 6.2 [FEU]”. Bland dessa ingår de allmänna principer och grundläggande rättigheter som numera garanteras i stadgan. Nämnda artikel 15.1 ska alltså tolkas mot bakgrund av de grundläggande rättigheter som garanteras i stadgan (se, analogt, beträffande direktiv 95/46, dom av den 20 maj 2003, Österreichischer Rundfunk m.fl., C-465/00, C-138/01 och C-139/01, EU:C:2003:294, punkt 68, dom av den 13 maj 2014, Google Spain och Google, C-131/12, EU:C:2014:317, punkt 68, och dom av den 6 oktober 2015, Schrems, C-362/14, EU:C:2015:650, punkt 38).

92 Skyldigheten, enligt nationell lagstiftning av nu aktuellt slag, för leverantörer av elektroniska kommunikationstjänster att lagra trafikuppgifter i syfte att vid behov göra dem tillgängliga för behöriga nationella myndigheter väcker frågor om sådan lagstiftnings förenlighet inte bara med artiklarna 7 och 8 i stadgan, som uttryckligen nämns i tolkningsfrågorna, utan även med yttrandefriheten, som garanteras i artikel 11 i stadgan (se, analogt, beträffande direktiv 2006/24, Digital Rights-domen, punkterna 25 och 70).

93 Betydelsen av såväl rätten till respekt för privatlivet, vilken garanteras i artikel 7 i stadgan, som rätten till skydd för personuppgifter, vilken garanteras i artikel 8 i stadgan, framgår av domstolens praxis (se, för ett liknande resonemang, dom av den 6 oktober 2015, Schrems, C-362/14, EU:C:2015:650, punkt 39 och där angiven rättspraxis) och ska beaktas vid tolkningen av artikel 15.1 i direktiv 2002/58. Detsamma gäller yttrandefriheten, med tanke på den särskilda betydelse den har i varje demokratiskt samhälle. Denna grundläggande rättighet, som garanteras i artikel 11 i stadgan, utgör en av grundvalarna för ett demokratiskt och pluralistiskt samhälle och ingår i de värden som unionen enligt artikel 2 FEU bygger på (se, för ett liknande resonemang, dom av den 12 juni 2003, Schmidberger, C-112/00, EU:C:2003:333, punkt 79, och dom av den 6 september 2011, Patriciello, C-163/10, EU:C:2011:543, punkt 31).

94 Enligt artikel 52.1 i stadgan ska varje begränsning i utövandet av de rättigheter och friheter som erkänns i stadgan vara föreskriven i lag och vara förenlig med deras väsentliga innehåll. Begränsningar får, med beaktande av proportionalitetsprincipen, endast göras om de är

nödvändiga och faktiskt svarar mot mål av allmänt intresse som erkänns av unionen eller mot behovet av skydd för andra människors rättigheter och friheter (dom av den 15 februari 2016, N., C-601/15 PPU, EU:C:2016:84, punkt 50).

95 Artikel 15.1 första meningen i direktiv 2002/58 föreskriver att medlemsstaterna får vidta en åtgärd som avviker från principen om konfidentialitet vid kommunikation och därmed förbundna trafikuppgifter om åtgärden ”i ett demokratiskt samhälle är nödvändig, lämplig och proportionell” för de syften som anges i den bestämmelsen. Skäl 11 i direktivet preciserar att en åtgärd av sådant slag måste stå i ”strikt” proportion till det avsedda ändamålet. Vad särskilt gäller lagring av uppgifter kräver artikel 15.1 andra meningen i direktivet att uppgifter endast bevaras ”under en begränsad period” och att lagringen ”motiveras” av de skäl som fastställs i artikel 15.1 första meningen i direktivet.

96 Att proportionalitetsprincipen ska iakttas framgår även av domstolens fasta praxis, enligt vilken skyddet av den grundläggande rätten till respekt för privatlivet på unionsnivå kräver att undantag från och begränsningar av skyddet för personuppgifter ska inskränkas till vad som är strängt nödvändigt (dom av den 16 december 2008, Satakunnan Markkinapörssi och Satamedia, C-73/07, EU:C:2008:727, punkt 56, dom av den 9 november 2010, Volker und Markus Schecke och Eifert, C-92/09 och C-93/09, EU:C:2010:662, punkt 77, Digital Rights-domen, punkt 52, och dom av den 6 oktober 2015, Schrems, C-362/14, EU:C:2015:650, punkt 92).

97 Vad gäller frågan huruvida en nationell lagstiftning som den som är i fråga i mål C-203/15 uppfyller de villkoren, påpekar domstolen att den lagstiftningen föreskriver en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter för samtliga abonnenter och registrerade användare avseende samtliga elektroniska kommunikationsmedel och ålägger leverantörer av elektroniska kommunikationstjänster att systematiskt och kontinuerligt lagra dessa uppgifter, utan undantag. Som framgår av begäran om förhandsavgörande, motsvarar de kategorier av uppgifter som avses med denna lagstiftning väsentligen dem för vilka lagring föreskrevs i direktiv 2006/24.

98 De uppgifter som leverantörer av elektroniska kommunikationstjänster således är skyldiga att lagra är sådana som gör det möjligt att spåra och identifiera en kommunikationskälla, identifiera slutmålet för en kommunikation, identifiera en kommunikations datum, tidpunkt, varaktighet och typ, identifiera användarnas kommunikationsutrustning och identifiera lokaliseringen av mobil kommunikationsutrustning. Bland dessa uppgifter ingår abonnentens eller den registrerade användarens namn och adress, det uppringande telefonnumret, det uppringda numret och IP-adressen för internettjänster. Dessa uppgifter gör det möjligt att få kännedom om med vilken person en abonnent eller registrerad användare har kommunicerat och på vilket sätt, hur länge kommunikationen varat och från vilken plats kommunikationen skett. Uppgifterna gör det dessutom möjligt att få kännedom om hur ofta abonnenten eller den registrerade användaren kommunicerat med vissa personer under en viss tidsperiod (se analogt, beträffande direktiv 2006/24, Digital Rights-domen, punkt 26).

99 Dessa uppgifter kan sammantagna göra det möjligt att dra mycket precisa slutsatser om privatlivet för de personer vilkas uppgifter har lagrats, såsom deras vanor i vardagslivet, deras stadigvarande och tillfälliga uppehållsorter, deras dagliga förflyttningar och förflyttningar i övrigt, de aktiviteter de utövar, deras sociala relationer och de umgängeskretsar de rör sig i (se analogt, beträffande direktiv 2006/24, Digital Rights-domen, punkt 27). Dessa uppgifter gör det möjligt att, som

generaladvokaten påpekat i punkterna 253, 254 och 257–259 i sitt förslag till avgörande, kartlägga de berörda personerna på ett sätt som är lika känsligt ur integritetssynpunkt som själva innehållet i kommunikationerna.

100 Det ingrepp som en sådan lagstiftning utgör i de grundläggande rättigheter som är stadfästa i artiklarna 7 och 8 i stadgan är långtgående och måste betraktas som synnerligen allvarligt. Den omständigheten att lagringen av uppgifterna och den senare användningen av dem sker utan att abonnenten eller den registrerade användaren är underrättad om detta kan ge de berörda personerna en känsla av att deras privatliv står under ständig övervakning (se analogt, beträffande direktiv 2006/24, Digital Rights-domen, punkt 37).

101 Även om en sådan lagstiftning inte medger lagring av innehållet i en kommunikation, och därför inte kan kränka det väsentliga innehållet i dessa grundläggande rättigheter (se analogt, beträffande direktiv 2006/24, Digital Rights-domen, punkt 39), skulle lagringen av trafikuppgifter och lokaliseringsuppgifter emellertid kunna inverka på användningen av de elektroniska kommunikationsmedlen och följaktligen på användarnas utövande av sin i artikel 11 i stadgan garanterade yttrandefrihet (se analogt, beträffande direktiv 2006/24, Digital Rights-domen, punkt 28).

102 Med hänsyn till det allvarliga ingrepp i de berörda grundläggande rättigheterna som en nationell lagstiftning som i brottsbekämpande syfte föreskriver lagring av trafikuppgifter och lokaliseringsuppgifter utgör, kan endast bekämpning av grov brottslighet motivera en sådan åtgärd (se analogt, angående direktiv 2006/24, Digital Rights-domen, punkt 60).

103 En effektiv bekämpning av grov brottslighet och särskilt av organiserad brottslighet och terrorism kan förvisso i stor utsträckning vara beroende av användningen av moderna utredningstekniker. Fastän det syftet är av allmänt samhällsintresse kan det emellertid inte, trots sin grundläggande betydelse, i sig ensamt motivera att en nationell lagstiftning som föreskriver en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter ska anses vara nödvändig för detta ändamål (se analogt, beträffande direktiv 2006/24, Digital Rights-domen, punkt 51).

104 För det första får en sådan lagstiftning till följd, sett till dess särdrag såsom de beskrivits i punkt 97 ovan, att lagring av trafikuppgifter och lokaliseringsuppgifter blir huvudregeln, trots att det system som inrättats genom direktiv 2002/58 kräver att sådan lagring ska vara ett undantag.

105 För det andra innebär en nationell lagstiftning som den som är i fråga i det nationella målet, som på ett generellt sätt omfattar samtliga abonnenter och registrerade användare och avser samtliga elektroniska kommunikationsmedel och samtliga trafikuppgifter, att det inte görs några åtskillnader, begränsningar eller undantag utifrån det eftersträvade syftet. Den berör på ett allomfattande sätt samtliga personer som använder elektroniska kommunikationstjänster, utan att dessa personer ens indirekt befinner sig i en situation som kan föranleda lagföring. Den är således även tillämplig på personer beträffande vilka det inte föreligger något indicium som ger anledning att tro att deras beteende ens kan ha ett indirekt eller avlägset samband med grov brottslighet. Den föreskriver inte heller några undantag, vilket innebär att den även är tillämplig på personer vilkas kommunikationer enligt nationell rätt omfattas av tystnadsplikt (se analogt, beträffande direktiv 2006/24, Digital Rights-domen, punkterna 57 och 58).

106 En sådan lagstiftning kräver inte något samband mellan de uppgifter som ska lagras och ett hot mot den allmänna säkerheten. Den är inte begränsad till lagring av uppgifter avseende en viss tidsperiod och/eller ett visst geografiskt område och/eller en viss krets av personer som på något sätt kan vara inblandade i ett allvarligt brott eller till personer beträffande vilka lagringen av uppgifter av andra skäl skulle kunna bidra till bekämpningen av brott (se analogt, beträffande direktiv 2006/24, Digital Rights-domen, punkt 59).

107 En nationell lagstiftning som den som är i fråga i det nationella målet överskrider således gränserna för vad som är strängt nödvändigt och kan inte anses motiverad i ett demokratiskt samhälle, såsom krävs enligt artikel 15.1 i direktiv 2002/58 jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan.

108 Artikel 15.1 i direktiv 2002/58 jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan hindrar däremot inte att en medlemsstat antar lagstiftning som i förebyggande syfte tillåter en riktad lagring av trafikuppgifter och lokaliseringsuppgifter, i syfte att bekämpa grov brottslighet, förutsatt att lagringen av uppgifterna, vad gäller vilka slags uppgifter som ska lagras, vilka kommunikationsmedel som avses, vilka personer som berörs och hur länge lagringen ska ske, begränsas till vad som är strängt nödvändigt.

109 För att uppfylla kraven i föregående punkt måste den nationella lagstiftningen för det första föreskriva tydliga och precisa bestämmelser som reglerar omfattningen och tillämpligheten av en sådan lagringsåtgärd och som slår fast minimikrav, så att de personer vars uppgifter har lagrats har tillräckliga garantier som möjliggör ett effektivt skydd av deras personuppgifter mot riskerna för missbruk. Den måste särskilt precisera under vilka omständigheter och villkor en sådan lagringsåtgärd får vidtas i förebyggande syfte, vilket säkerställer att lagringen begränsas till vad som är strängt nödvändigt (se analogt, beträffande direktiv 2006/24, Digital Rights-domen, punkt 54 och där angiven rättspraxis).

110 Vad för det andra gäller de materiella villkor som en nationell lagstiftning som inom ramen för brottsbekämpning tillåter lagring i förebyggande syfte av trafikuppgifter och lokaliseringsuppgifter måste uppfylla för att säkerställa att den är begränsad till vad som är strängt nödvändigt, påpekar domstolen att även om de villkoren kan variera utifrån vilka åtgärder som vidtas för att förebygga, undersöka, avslöja och väcka åtal för grov brottslighet, måste lagringen av uppgifterna alltid uppfylla objektiva kriterier, som fastställer ett samband mellan de uppgifter som ska lagras och det eftersträvade syftet. I synnerhet måste villkoren vara sådana att de klart avgränsar åtgärdens omfattning och följaktligen den berörda personkretsen.

111 [Texten ändrad genom beslut av den 16 mars 2017] Vad gäller avgränsningen av en sådan åtgärd beträffande den personkrets och de situationer som kan komma att beröras gör domstolen följande bedömning. Den nationella lagstiftningen ska grunda sig på objektiva omständigheter som gör det möjligt att ta sikte på en personkrets vars uppgifter kan avslöja en, åtminstone indirekt, koppling till grov brottslighet, på ett eller annat sätt bidra till att bekämpa grov brottslighet eller förhindra en allvarlig risk för den allmänna säkerheten. En sådan avgränsning kan säkerställas genom ett geografiskt kriterium när de behöriga nationella myndigheterna på grundval av objektiva omständigheter bedömer att det i ett eller flera geografiska områden finns en förhöjd risk för förberedelse eller genomförande av sådana handlingar.

112 Den första frågan i mål C-203/15 ska mot denna bakgrund besvaras på följande sätt. Artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan, ska tolkas på så sätt att den utgör hinder för en nationell lagstiftning som i brottsbekämpande syfte föreskriver en generell

och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter avseende samtliga abonnenter och registrerade användare och samtliga elektroniska kommunikationsmedel.

Den andra frågan i mål C-203/15 och den första frågan i mål C-698/15

113 Kammarrätten i Stockholm har ställt sin andra fråga, i mål C-203/15, endast för det fall att den första frågan i målet besvaras nekande. Denna andra fråga är dock oberoende av om en lagring av uppgifter är generell eller riktad, i den mening som avses i punkterna 108–111 ovan. Den andra frågan i mål C-203/15 ska därför besvaras gemensamt med den första frågan i mål C-698/15, vilken ställts oberoende av omfattningen av den skyldighet att lagra uppgifter som ålagts leverantörer av elektroniska kommunikationstjänster.

114 De hänskjutande domstolarna har ställt den andra frågan i mål C-203/15 respektive den första frågan i mål C-698/15 för att få klarhet i huruvida artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8 och 52.1 i stadgan, ska tolkas på så sätt att den utgör hinder för en nationell lagstiftning som reglerar skydd och säkerhet för trafikuppgifter och lokaliseringsuppgifter samt, i synnerhet, behöriga nationella myndigheters tillgång till lagrade uppgifter och som inte begränsar denna tillgång till enbart syftet att bekämpa grov brottslighet, inte föreskriver att tillgången ska vara underkastad förhandskontroll av en domstol eller en oberoende förvaltningsmyndighet och inte kräver att uppgifterna ska lagras inom unionen.

115 Vad gäller de syften som kan motivera en nationell lagstiftning som avviker från principen om konfidentialitet vid elektronisk kommunikation vill domstolen anföra följande. Såsom konstaterats i punkterna 90 och 102 ovan är uppräkningen av syftena i artikel 15.1 första meningen i direktiv 2002/58 uttömmande. Därför måste tillgång till lagrade uppgifter vara faktiskt och strikt begränsad till de fall då tillgången krävs för ett av dessa syften. Då syftet med lagstiftningen måste stå i proportion till hur allvarligt ingrepp i de grundläggande rättigheterna det innebär att ge tillgång till de lagrade uppgifterna, är det vid förebyggande, undersökning, avslöjande av och åtal för brott endast bekämpning av grov brottslighet som kan motivera en sådan tillgång.

116 Vad gäller proportionalitetsprincipen, måste en nationell lagstiftning som reglerar på vilka villkor en leverantör av elektronisk kommunikation ska ge behöriga nationella myndigheter tillgång till lagrade uppgifter garantera – i enlighet med vad domstolen konstaterat i punkterna 95 och 96 ovan – att tillgång inte ges utöver vad som är strängt nödvändigt.

117 Eftersom de lagstiftningsåtgärder som avses i artikel 15.1 i direktiv 2002/58 enligt skäl 11 i direktivet ska ”omfattas av lämpliga skyddsmekanismer”, måste en sådan åtgärd dessutom, som framgår av ovan i punkt 109 angiven rättspraxis, föreskriva klara och precisa bestämmelser som anger under vilka omständigheter och på vilka villkor leverantörer av elektroniska kommunikationstjänster måste ge behöriga nationella myndigheter tillgång till uppgifterna. En åtgärd av detta slag måste också vara rättsligt bindande i nationell rätt.

118 För att säkerställa att behöriga nationella myndigheters tillgång till lagrade uppgifter begränsas till vad som är strängt nödvändigt, ankommer det förvisso på nationell rätt att fastställa på vilka villkor leverantörer av elektroniska kommunikationstjänster ska ge sådan tillgång. Det räcker dock inte att den berörda nationella lagstiftningen stadgar att tillgång enbart ska medges för något av de syften som avses i artikel 15.1 i direktiv 2002/58, även om det gäller bekämpning av

grov brottslighet. Den måste även ange de materiella och formella villkoren för de behöriga nationella myndigheternas tillgång till de lagrade uppgifterna (se analogt, beträffande direktiv 2006/24, Digital Rights-domen, punkt 61).

119 Eftersom en allmän tillgång till samtliga lagrade uppgifter, oberoende av om det finns någon koppling, ens indirekt, till det eftersträvade syftet, inte kan anses vara begränsad till vad som är strängt nödvändigt, måste den berörda nationella lagstiftningen således vara grundad på objektiva kriterier som avgör under vilka omständigheter och på vilka villkor behöriga nationella myndigheter ska ges tillgång till uppgifter om abonnenter eller registrerade användare. Tillgång kan i princip bara beviljas, i samband med bekämpning av brott, till uppgifter om personer som misstänks planera, begå eller ha begått ett allvarligt brott eller på något sätt vara inblandade i ett sådant brott (se, analogt, Europadomstolens dom av den 4 december 2015, Zakharov mot Ryssland, CE:ECHR:2015:1204JUD004714306, § 260). I särskilda fall, som när vitala intressen för nationell säkerhet, försvar eller allmän säkerhet hotas av terrorism, skulle dock tillgång kunna ges även till uppgifter om andra personer när det finns objektiva omständigheter som ger skäl att anta att de uppgifterna i ett konkret fall effektivt skulle kunna bidra till att bekämpa terrorism.

120 För att säkerställa att dessa villkor uppfylls fullt ut i praktiken, är det väsentligt att behöriga nationella myndigheters tillgång till de lagrade uppgifterna i princip, utom i vederbörligen motiverade brådskande fall, är underkastad förhandskontroll av en domstol eller en oberoende myndighet och att domstolen meddelar sitt avgörande eller myndigheten fattar sitt beslut efter det att de behöriga nationella myndigheterna framställt en motiverad ansökan, vilket kan ske bland annat inom ramen för ett förfarande för förebyggande, avslöjande eller lagföring av brott (se analogt, beträffande direktiv 2006/24, Digital Rights-domen, punkt 62; se även analogt, vad gäller artikel 8 i Europakonventionen, Europadomstolen, 12 januari 2016, Szabó och Vissy mot Ungern, CE:ECHR:2016:0112JUD003713814, §§ 77 och 80).

121 Vidare krävs att de behöriga nationella myndigheter som beviljats tillgång till lagrade uppgifter informerar de berörda personerna om detta, enligt tillämpliga nationella förfaranden, så snart en sådan upplysning inte längre riskerar att skada myndigheternas utredningar. Den informationen är i själva verket nödvändig bland annat för att dessa personer ska kunna utöva sin rätt till rättslig prövning vid kränkning av deras rättigheter, såsom uttryckligen stadgas i artikel 15.2 i direktiv 2002/58, jämförd med artikel 22 i direktiv 95/46 (se, analogt, dom av den 7 maj 2009, Rijkeboer, C-553/07, EU:C:2009:293, punkt 52, och dom av den 6 oktober 2015, Schrems, C-362/14, EU:C:2015:650, punkt 95).

122 Vad gäller bestämmelserna om skydd av och säkerhet för de uppgifter som lagras av leverantörer av elektroniska kommunikationstjänster, konstaterar domstolen att artikel 15.1 i direktiv 2002/58 inte medger att medlemsstaterna avviker från artikel 4.1 eller 4.1a i direktivet. De sistnämnda bestämmelserna kräver att leverantörerna vidtar lämpliga tekniska och organisatoriska åtgärder för att säkerställa ett effektivt skydd av de lagrade uppgifterna mot riskerna för missbruk och otillåten tillgång till uppgifterna. Med hänsyn till att det är fråga om en stor mängd uppgifter och att dessa är av känslig natur samt att det finns en risk för otillåten tillgång till uppgifterna, måste leverantörerna av elektroniska kommunikationstjänster, för att säkerställa fullständig integritet och konfidentialitet för uppgifterna, garantera en särskilt hög skydds- och säkerhetsnivå genom lämpliga tekniska och organisatoriska åtgärder. Den nationella lagstiftningen måste i synnerhet föreskriva att lagringen sker inom unionen och att uppgifterna oåterkalleligen förstörs när deras lagringstid gått ut (se analogt, beträffande direktiv 2006/24, Digital Rights-domen, punkterna 66–68).

123 Medlemsstaterna måste i alla händelser garantera att en oberoende myndighet kontrollerar att den skyddsnivå som säkerställs i unionsrätten iakttas vad gäller skyddet för fysiska personer vid behandlingen av personuppgifter. En sådan kontroll krävs uttryckligen enligt artikel 8.3 i stadgan och utgör enligt domstolens fasta praxis en grundläggande beståndsdel i skyddet för enskilda i samband med behandlingen av personuppgifter. Annars skulle de personer vars personuppgifter har lagrats berövas sin rätt enligt artikel 8.1 och 8.3 i stadgan att vända sig till de nationella tillsynsmyndigheterna med begäran om skydd för sina personuppgifter (se, för ett liknande resonemang, Digital Rights-domen, punkt 68, och dom av den 6 oktober 2015, Schrems, C-362/14, EU:C:2015:650, punkterna 41 och 58).

124 Det ankommer på de hänskjutande domstolarna att pröva huruvida och i så fall i vilken utsträckning de nu aktuella nationella lagstiftningarna uppfyller kraven enligt artikel 15.1 i direktiv 2002/58 jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan, såsom de preciserats i punkterna 115–123 ovan, vad gäller såväl behöriga nationella myndigheters tillgång till lagrade uppgifter som skyddet och säkerhetsnivån för dessa uppgifter.

125 Den andra frågan i mål C-203/15 och den första frågan i mål C-698/15 ska mot denna bakgrund besvaras på följande sätt. Artikel 15.1 i direktiv 2002/58 jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan ska tolkas på så sätt att den utgör hinder för en nationell lagstiftning som reglerar skydd och säkerhet för trafikuppgifter och lokaliseringsuppgifter och, i synnerhet, behöriga nationella myndigheters tillgång till lagrade uppgifter och som inte – inom ramen för brottsbekämpning – begränsar denna tillgång till enbart åtgärder som syftar till att bekämpa grov brottslighet, inte föreskriver att tillgången ska vara underkastad förhandskontroll av en domstol eller en oberoende förvaltningsmyndighet och inte kräver att uppgifterna ska lagras inom unionen.

Den andra frågan i mål C-698/15

126 Court of Appeal (England & Wales) (Civil Division) (Appellationsdomstolen för England och Wales, avdelningen för tvistemål och förvaltningsmål) har ställt sin andra fråga för att få klarhet i huruvida domstolen i Digital Rights-domen tolkade artikel 7 och/eller artikel 8 i stadgan på så sätt att de bestämmelserna anses gå längre än artikel 8 i Europakonventionen enligt Europadomstolens tolkning.

127 Domstolen erinrar inledningsvis om att de grundläggande rättigheter som erkänns i Europakonventionen ingår i unionsrätten som allmänna principer, såsom bekräftas i artikel 6.3 FEU. Europakonventionen utgör emellertid inte något rättsligt instrument som formellt har införlivats med unionens rättsordning, så länge som unionen inte har anslutit sig till denna konvention (se, för ett liknande resonemang, dom av den 15 februari 2016, N., C-601/15 PPU, EU:C:2016:84, punkt 45 och där angiven rättspraxis).

128 Tolkningen av direktiv 2002/58, som är i fråga här, ska följaktligen göras enbart utifrån de grundläggande rättigheter som garanteras i stadgan (se, för ett liknande resonemang, dom av den 15 februari 2016, N., C-601/15 PPU, EU:C:2016:84, punkt 46 och där angiven rättspraxis).

129 I förklaringarna avseende artikel 52 i stadgan anges att artikel 52.3 syftar till att trygga det nödvändiga sammanhanget mellan stadgan och Europakonventionen ”utan att detta inkräktar på unionsrättens och Europeiska unionens domstols autonomi” (dom av den 15 februari 2016, N., C-601/15 PPU, EU:C:2016:84, punkt 47). Som uttryckligen anges i artikel 52.3 andra meningen, hindrar inte första meningen i den bestämmelsen unionsrätten från att tillförsäkra ett mer

långtgående skydd än Europakonventionen. Till detta kommer slutligen att artikel 8 i stadgan rör en grundläggande rättighet som är skild från den som slås fast i artikel 7 i stadgan och som saknar motsvarighet i Europakonventionen.

130 Enligt domstolens fasta praxis är domstolens uppgift rörande en begäran om förhandsavgörande att bidra till den faktiska lösningen av en tvist som rör unionsrätten och inte att uttala sig om allmänna eller hypotetiska frågor (se, för ett liknande resonemang, dom av den 24 april 2012, Kamberaj, C-571/10, EU:C:2012:233, punkt 41, dom av den 26 februari 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, punkt 42, och dom av den 27 februari 2014, Pohotovost', C-470/12, EU:C:2014:101, punkt 29).

131 I förevarande fall finner domstolen mot bakgrund av övervägandena i bland annat punkterna 128 och 129 ovan att frågan huruvida skyddet enligt artiklarna 7 och 8 i stadgan går längre än det enligt artikel 8 i Europakonventionen inte påverkar tolkningen av direktiv 2002/58, jämförd med stadgan, vilket är vad den nationella domstolen har att ta ställning till i mål C-698/15.

132 Att besvara den andra frågan i mål C-698/15 tycks således inte bidra till tolkningen av unionsrätten på ett sätt som är nödvändigt för att, i unionsrättsligt avseende, avgöra tvisten i det nationella målet.

133 Den andra frågan i mål C-698/15 kan därför inte tas upp till prövning.

Rättegångskostnader

134 Eftersom förfarandet i förhållande till parterna i de nationella målen utgör ett led i beredningen av samma mål, ankommer det på de hänskjutande domstolarna att besluta om rättegångskostnaderna. De kostnader för att avge yttrande till domstolen som andra än nämnda parter har haft är inte ersättningsgilla.

Mot denna bakgrund beslutar domstolen (stora avdelningen) följande:

1) **Artikel 15.1 i Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation), i dess lydelse enligt Europaparlamentets och rådets direktiv 2009/136/EG av den 25 november 2009, jämförd med artiklarna 7, 8, 11 och 52.1 i Europeiska unionens stadga om de grundläggande rättigheterna, ska tolkas på så sätt att den utgör hinder för en nationell lagstiftning som i brottsbekämpande syfte föreskriver en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter avseende samtliga abonnenter och registrerade användare och samtliga elektroniska kommunikationsmedel.**

2) **Artikel 15.1 i direktiv 2002/58, i dess lydelse enligt direktiv 2009/136, jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan om de grundläggande rättigheterna ska tolkas på så sätt att den utgör hinder för en nationell lagstiftning som reglerar skydd och säkerhet för trafikuppgifter och lokaliseringsuppgifter och, i synnerhet, behöriga nationella myndigheters tillgång till lagrade uppgifter och som inte – inom ramen för brottsbekämpning – begränsar denna tillgång till enbart åtgärder som syftar till att**

bekämpa grov brottslighet, inte föreskriver att tillgången ska vara underkastad förhandskontroll av en domstol eller en oberoende förvaltningsmyndighet och inte kräver att uppgifterna ska lagras inom unionen.

3) **Den andra frågan från Court of Appeal (England & Wales) (Civil Division) (Appellationsdomstolen för England och Wales, avdelningen för tvistemål och förvaltningsmål) avvisas.**

Lenaerts	Tizzano	Silva de Lapuerta
von Danwitz	Da Cruz Vilaça	Juhász
Vilaras	Borg Barthet	Malenovský
Levits	Bonichot	Arabadjiev
Rodin	Biltgen	Lycourgos

Avkunnad vid offentligt sammanträde i Luxemburg den 21 december 2016.

A. Calot Escobar	K. Lenaerts
Justitiesekreterare	Ordförande