Rättsfallssamlingen

DOMSTOLENS DOM (stora avdelningen)

den 6 oktober 2020*

”Begäran om förhandsavgörande – Behandling av personuppgifter inom sektorn för elektronisk kommunikation – Leverantörer av elektroniska kommunikationstjänster – Generell och odifferentierad överföring av trafikuppgifter och lokaliseringsuppgifter – Skydd av nationell säkerhet – Direktiv 2002/58/EG – Tillämpningsområde – Artiklarna 1.3 och 3 – Konfidentialitet vid elektronisk kommunikation – Skydd – Artiklarna 5 och 15.1 – Stadgan om de grundläggande rättigheterna – Artiklarna 7, 8, 11 och 52.1 – Artikel 4.2 FEU”

I mål C-623/17,

angående en begäran om förhandsavgörande enligt artikel 267 FEUF, framställd av Investigatory Powers Tribunal (Domstolen för utredningsbefogenheter, Förenade kungariket) genom beslut av den 18 oktober 2017, som inkom till domstolen den 31 oktober 2017, i målet

Privacy International

mot

Secretary of State for Foreign and Commonwealth Affairs,

Secretary of State for the Home Department,

Government Communications Headquarters,

Security Service,

Secret Intelligence Service,

meddelar

DOMSTOLEN (stora avdelningen)

sammansatt av ordföranden K. Lenaerts, vice ordföranden R. Silva de Lapuerta, avdelningsordförandena J.-C. Bonichot, A. Arabadjiev, A. Prechal, M. Safjan, P.G. Xuereb och L.S. Rossi samt domarna J. Malenovský, L. Bay Larsen, T. von Danwitz (referent), C. Toader, K. Jürimäe, C. Lycourgos och N. Piçarra,

generaladvokat: M. Campos Sánchez-Bordona,

justitiesekreterare: handläggaren C. Strömholm,

efter det skriftliga förfarandet och förhandlingen den 9 och den 10 september 2019,

* Rättegångsspråk: engelska.

med beaktande av de yttranden som avgetts av:

– Privacy International, genom B. Jaffey och T. de la Mare, QC, genom D. Cashman, solicitor, samt genom H. Roy, avocat,

– Förenade kungarikets regering, genom Z. Lavery, D. Guðmundsdóttir och S. Brandon, samtliga i egenskap av ombud, biträdda av G. Facenna och D. Beard, QC, samt av C. Knight och R. Palmer, barristers,

– Belgiens regering, genom P. Cottin och J.-C. Halleux, båda i egenskap av ombud, biträdda av J. Vanpraet, advocaat, och E. de Lophem, avocat,

– Tjeckiens regering, genom M. Smolek, J. Vláčil och O. Serdula, samtliga i egenskap av ombud,

– Tysklands regering, inledningsvis genom M. Hellmann, R. Kanitz, D. Klebs och T. Henze, därefter genom J. Möller, M. Hellmann, R. Kanitz och D. Klebs, samtliga i egenskap av ombud,

– Estlands regering, genom A. Kalbus, i egenskap av ombud,

– Irland, genom M. Browne, G. Hodge och A. Joyce, samtliga i egenskap av ombud, biträdda av D. Fennelly, barrister,

– Spaniens regering, inledningsvis genom L. Aguilera Ruiz och M.J. García-Valdecasas Dorrego, därefter genom L. Aguilera Ruiz, samtliga i egenskap av ombud,

– Frankrikes regering, inledningsvis genom E. de Moustier, E. Armoët, A.-L. Desjonquères, F. Alabrune, D. Colas och D. Dubois, därefter genom E. de Moustier, E. Armoët, A.-L. Desjonquères, F. Alabrune och D. Dubois, samtliga i egenskap av ombud,

– Cyperns regering, genom E. Symeonidou och E. Neofytou, båda i egenskap av ombud,

– Lettlands regering, inledningsvis genom V. Soņeca och I. Kucina, därefter genom V. Soņeca, samtliga i egenskap av ombud,

– Ungerns regering, genom G. Koós, M.Z. Fehér, G. Tornyai och Z. Wagner, därefter genom G. Koós och M.Z. Fehér, samtliga i egenskap av ombud,

– Nederländernas regering, genom C.S. Schillemans och M.K. Bulterman, båda i egenskap av ombud,

– Polens regering, genom B. Majczyna, J. Sawicka och M. Pawlicka, samtliga i egenskap av ombud,

– Portugals regering, genom L. Inez Fernandes, M. Figueiredo och F. Aragão Homem, samtliga i egenskap av ombud,

– Sveriges regering, inledningsvis genom A. Falk, H. Shev, C. Meyer-Seitz, L. Zettergren och A. Alriksson, därefter genom H. Shev, C. Meyer-Seitz, L. Zettergren och A. Alriksson, samtliga i egenskap av ombud,

– Norges regering, genom T.B. Leming, M. Emberland och J. Vangsnes, samtliga i egenskap av ombud,

– Europeiska kommissionen, inledningsvis genom H. Kranenborg, M. Wasmeier, D. Nardi och P. Costa de Oliveira, därefter genom H. Kranenborg, M. Wasmeier och D. Nardi, samtliga i egenskap av ombud,

– Europeiska datatillsynsmannen, genom T. Zerdick och A. Buchta, båda i egenskap av ombud,

och efter att den 15 januari 2020 ha hört generaladvokatens förslag till avgörande,

följande

Dom

1 Begäran om förhandsavgörande avser tolkningen av artiklarna 1.3 och 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), jämförda med artikel 4.2 FEU samt artiklarna 7, 8 och 52.1 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad stadgan).

2 Begäran har framställts i ett mål mellan å ena sidan Privacy International och å andra sidan Secretary of State for Foreign and Commonwealth Affairs (utrikes- och samväldesministern, Förenade kungariket), Secretary of State for the Home Departement (inrikesministern, Förenade kungariket), Government Communications Headquarters (myndigheten för informationsinsamling genom signalspaning, Förenade kungariket) (nedan kallad GCHQ), Security Service (säkerhetstjänsten, Förenade kungariket) (nedan kallad MI5) och Secret Intelligence Service (hemliga underrättelsetjänsten, Förenade kungariket) (nedan kallad MI6). Målet rör lagenligheten av en lagstiftning som tillåter att säkerhets- och underrättelsetjänsterna inhämtar och använder så kallade *bulk communications data* (nedan kallade mängddata om kommunikation).

Tillämpliga bestämmelser

Unionsrätt

Direktiv 95/46

3 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) upphävdes med verkan från och med den 25 maj 2018 genom Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (EUT L 119, 2016, s. 1). I artikel 3 i direktiv 95/46, med rubriken ”Tillämpningsområde”, föreskrevs följande:

”1. Detta direktiv ska tillämpas på behandling av personuppgifter som helt eller delvis företas på automatiserad väg samt på annan behandling än automatiserad behandling av personuppgifter som ingår i eller kommer att ingå i ett register.

2. Detta direktiv gäller inte för sådan behandling av personuppgifter

– som utgör ett led i en verksamhet som inte omfattas av gemenskapsrätten, exempelvis sådan verksamhet som avses i avdelningarna V och VI [FEU], och inte under några omständigheter behandlingar som rör allmän säkerhet, försvar, statens säkerhet (inbegripet statens ekonomiska välstånd när behandlingen har samband med frågor om statens säkerhet) och statens verksamhet på straffrättens område,

– av en fysisk person som ett led i verksamhet av rent privat natur eller som har samband med hans hushåll.”

Direktiv 2002/58

4 I skälen 2, 6, 7, 11, 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 direktiv [95/46] omfattar det här direktivet inte sådana frågor om skydd av grundläggande fri- och rättigheter som rör verksamhet som inte regleras av [unionslagstiftningen]. 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 [som undertecknades i Rom den 4 november 1950] 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.

…

(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. Om det är nödvändigt för att effektivisera den fortsatta överföringen av allmänt tillgänglig information till andra mottagare av tjänsten på deras begäran, bör detta direktiv inte förhindra att sådan information får lagras

längre, förutsatt att informationen i alla händelser skulle vara tillgänglig för allmänheten utan begränsning och att alla uppgifter som hänvisar till vilka enskilda abonnenter eller användare som begär sådan information utplånas.

…

(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. Trafikuppgifter som används för marknadsföring av kommunikationstjänster … bör också utplånas eller avidentifieras …

…

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

5 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 [Europeiska unionen].

2. Bestämmelserna i detta direktiv skall precisera och komplettera direktiv 95/46/EG 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 [FEUF], 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.”

6 I artikel 2 i direktiv 2002/58, med rubriken ”Definitioner”, föreskrivs följande:

”Om inte annat anges skall definitionerna i direktiv [95/46] och [i Europaparlamentets och rådets direktiv 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:

a) *användare*: en fysisk person som använder en allmänt tillgänglig elektronisk kommunikationstjänst för privat eller affärsmässigt bruk utan att nödvändigtvis ha abonnerat på denna tjänst.

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.

…”

7 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 {unionen], inbegripet allmänna kommunikationsnät som stöder datainsamling och identifieringsutrustning.”

8 I artikel 5 i direktiv 2002/58, med rubriken ”Konfidentialitet vid kommunikation”, föreskrivs 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”, föreskrivs 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 ska 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 direktiv 2002/58 har rubriken ”Andra lokaliseringsuppgifter än trafikuppgifter”, och där föreskrivs följande i punkt 1:

”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 direktiv 2002/58 har rubriken ”Tillämpningen av vissa bestämmelser i direktiv [95/46]”, och där föreskrivs följande i punkt 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 [unionslagstiftningen], inklusive principerna i artikel 6.1 och 6.2 i Fördraget om Europeiska unionen.”

Förordning 2016/679

12 I artikel 2 i förordning 2016/679 föreskrivs följande:

”1. Denna förordning ska tillämpas på sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register.

2. Denna förordning ska inte tillämpas på behandling av personuppgifter som

a) utgör ett led i en verksamhet som inte omfattas av unionsrätten,

b) medlemsstaterna utför när de bedriver verksamhet som omfattas av avdelning V kapitel 2 i [fördraget om Europeiska unionen],

…

d) behöriga myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, i vilket även ingår att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten.

…”

13 I artikel 4 i förordning 2016/679 föreskrivs följande:

”I denna förordning avses med

…

2) *behandling*: en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring,

…”

14 I artikel 23.1 i förordning 2016/679 föreskrivs följande:

”Det ska vara möjligt att i unionsrätten eller i en medlemsstats nationella rätt som den personuppgiftsansvarige eller personuppgiftsbiträdet omfattas av införa en lagstiftningsåtgärd som begränsar tillämpningsområdet för de skyldigheter och rättigheter som föreskrivs i artiklarna 12–22 och 34, samt artikel 5 i den mån dess bestämmelser motsvarar de rättigheter och skyldigheter som fastställs i artiklarna 12–22, om en sådan begränsning sker med respekt för andemeningen i de grundläggande rättigheterna och friheterna och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle i syfte att säkerställa

a) den nationella säkerheten,

b) försvaret,

c) den allmänna säkerheten,

d) förebyggande, förhindrande, utredning, avslöjande eller lagföring av brott eller verkställande av straffrättsliga sanktioner, inbegripet skydd mot samt förebyggande och förhindrande av hot mot den allmänna säkerheten,

e) andra av unionens eller en medlemsstats viktiga mål av generellt allmänt intresse, särskilt ett av unionens eller en medlemsstats viktiga ekonomiska eller finansiella intressen, däribland penning-, budget- eller skattefrågor, folkhälsa och social trygghet,

f) skydd av rättsväsendets oberoende och rättsliga åtgärder,

g) förebyggande, förhindrande, utredning, avslöjande och lagföring av överträdelser av etiska regler som gäller för lagreglerade yrken,

h) en tillsyns-, inspektions- eller regleringsfunktion som, även i enstaka fall, har samband med myndighetsutövning i fall som nämns i a–e och g,

i) skydd av den registrerade eller andras rättigheter och friheter,

j) verkställighet av civilrättsliga krav.”

15 I artikel 94.2 i förordning nr 2016/679 föreskrivs följande:

”Hänvisningar till det upphävda direktivet ska anses som hänvisningar till denna förordning. Hänvisningar till arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter, som inrättades genom artikel 29 i direktiv [95/46], ska anses som hänvisningar till Europeiska dataskyddsstyrelsen, som inrättas genom denna förordning.”

Lagstiftningen i Förenade kungariket

16 Section 94 i Telecommunications Act 1984 (1984 års lag om telekommunikation), i den lydelse som är tillämplig på omständigheterna i det nationella målet (nedan kallad 1984 års lag), har rubriken ”Anvisningar med hänsyn till den nationella säkerheten m.m.”, och där föreskrivs följande:

”1) Ministern får, efter samråd med personer på vilka denna section är tillämplig, ge dessa personer generella anvisningar i den mån som detta enligt ministern är nödvändigt med hänsyn till den nationella säkerheten eller till förbindelserna med regeringen i ett land eller område utanför Förenade kungariket.

2) Om ministern anser det nödvändigt med hänsyn till den nationella säkerheten eller till förbindelserna med regeringen i ett land eller område utanför Förenade kungariket, får ministern, efter samråd med personer på vilken denna artikel är tillämplig, anvisa dessa personer att (beroende på omständigheterna i det enskilda fallet) utföra eller underlåta att utföra en särskild åtgärd som anges i anvisningen.

2A) Ministern får endast ge anvisningar enligt punkt 1) eller 2) om denne anser att det handlande som krävs enligt anvisningen står i proportion till det mål som ska uppnås genom handlandet.

3) Personer på vilka denna section är tillämplig ska genomföra alla anvisningar som de får av ministern enligt denna section, utan hinder av andra skyldigheter som åligger dem enligt del 1 eller kapitel 1 i del 2 i Communications Act 2003 [2003 års lag om kommunikationer] och, när det gäller anvisningar som ges till operatörer av ett allmänt elektroniskt kommunikationsnät, utan hinder av att anvisningarna gäller för dem i en annan egenskap än den som operatör av ett sådant nät.

4) Ministern ska till var och en av parlamentets kammare ge in en kopia av alla anvisningar som ges enligt denna section, såvida inte ministern anser att ett utlämnande av dessa anvisningar skulle strida mot nationella säkerhetsintressen eller mot förbindelserna med regeringen i ett land eller område utanför Förenade kungariket eller mot en persons affärsintressen.

5) En person får inte lämna ut, eller enligt lag eller på annat sätt åläggas att lämna ut, någon information om åtgärder som vidtagits i enlighet med denna section, om ministern har underrättat vederbörande om att ministern anser att utlämnandet av sådan information skulle strida mot den nationella säkerheten eller mot förbindelserna med regeringen i ett land eller område utanför Förenade kungariket eller mot någon annan persons affärsintressen.

…

8) Denna section ska tillämpas på [Office of communications (OFCOM) (tillsynsmyndighet på teleområdet)] och på operatörer av allmänna elektroniska kommunikationsnät.”

17 I section 21 punkterna 4 och 6 i Regulation of Investigatory Powers Act 2000 (2000 års lag om utredningsbefogenheter) (nedan kallad Ripa) föreskrivs följande:

”4) [M]ed ’uppgifter om kommunikation’ [avses] 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.

…

6) Begreppet ’trafikuppgifter’, i samband med all kommunikation, avser följande:

a) varje uppgift som identifierar eller kan identifiera en person, apparat eller plats mot vilken, eller från vilken, en kommunikation överförs eller kan överföras,

b) varje uppgift som identifierar eller väljer ut, eller kan identifiera eller välja ut den utrustning genom vilken en kommunikation överförs eller kan överföras,

c) varje uppgift som omfattar signaler för manövrering av den apparat som i ett kommunikationssystem används för överföring av varje kommunikation, och

d) varje uppgift som identifierar de uppgifter som omfattas av eller fogas till en särskild kommunikation eller andra uppgifter som omfattas av eller fogas till en viss kommunikation.

…”

18 I sections 65–69 i Ripa finns bestämmelser om Investigatory Powers Tribunals (Domstolen för utredningsbefogenheter, Förenade kungariket) funktionssätt och behörighet. Enligt section 65 i Ripa får klagomål ges in till denna domstol om det finns skäl att anta att uppgifter har erhållits på ett olämpligt sätt.

Målet vid den nationella domstolen och tolkningsfrågorna

19 I början av år 2015 blev det känt, bland annat genom en rapport från Intelligence and Security Committee of Parliament (parlamentets kommitté för underrättelse- och säkerhetsfrågor, Förenade kungariket) att Förenade kungarikets olika säkerhets- och underrättelsetjänster, det vill säga GCHQ, MI5 och MI6, hade som praxis att samla in och använda mängddata om kommunikation. Den 5 juni 2015 väckte Privacy International, som är en icke-statlig organisation, talan vid den hänskjutande

domstolen, Investigatory Powers Tribunal (Domstolen för utredningsbefogenheter, Förenade kungariket) mot utrikes- och samväldesministern, inrikesministern samt säkerhets- och underrättelsetjänsterna och bestred lagenligheten av nyss nämnda praxis.

20 Den hänskjutande domstolen gjorde en prövning av lagenligheten av säkerhets- och underrättelsetjänsternas praxis, först mot bakgrund av den nationella rätten och bestämmelserna i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, som undertecknades i Rom den 4 november 1950 (nedan kallad Europakonventionen) och därefter mot bakgrund av unionsrätten. I dom av den 17 oktober 2016 fann nämnda domstol att svarandena i det nationella målet hade medgett att säkerhets- och underrättelsetjänsterna inom ramen för sin verksamhet samlade in och använde samlingar av så kallade *bulk personal data* (nedan kallade mängddata om personuppgifter) inom olika kategorier, såsom biografiska uppgifter eller reseuppgifter, finansiell information eller affärsinformation, uppgifter som har samband med kommunikation och som kan innehålla känsliga uppgifter, som omfattas av tystnadsplikt, eller journalistiskt material. Den konstaterade att dessa uppgifter, som erhållits på olika sätt, i förekommande fall på hemlig väg, analyserades genom korskontroller och genom automatiserad behandling. De kunde vidare lämnas ut till andra personer och myndigheter och delas med utländska partner. I detta sammanhang använde säkerhets- och underrättelsetjänsterna även mängddata om kommunikation, vilka inhämtades från operatörer av allmänna elektroniska kommunikationsnät enligt bland annat ministeranvisningar som antagits med stöd av section 94 i 1984 års lag. GCHQ och MI5 hade gått till väga på detta sätt sedan år 2001 respektive år 2005.

21 Den hänskjutande domstolen fann att dessa åtgärder för insamling och användning av uppgifter var förenliga med nationell rätt och, sedan år 2015, med artikel 8 i Europakonventionen, dock med förbehåll för frågor som ännu inte prövats och som avsåg proportionaliteten av nämnda åtgärder och överföring av uppgifter till tredje parter. I det sistnämnda avseendet preciserade den hänskjutande domstolen att det i målet hade getts in bevisning om tillämpliga garantier, bland annat i fråga om förfaranden som reglerar åtkomst till uppgifter och hur uppgifter får spridas utanför säkerhets- och underrättelsetjänsterna, åtgärder för lagring av uppgifter och förekomsten av oberoende tillsyn.

22 Beträffande lagenligheten av de åtgärder som är aktuella i det nationella målet mot bakgrund av unionsrätten, prövade den hänskjutande domstolen i dom av den 8 september 2017 huruvida dessa åtgärder omfattades av unionsrättens tillämpningsområde och, om så var fallet, huruvida de var förenliga med unionsrätten. Den hänskjutande domstolen konstaterade, i fråga om mängddata om kommunikation, att operatörer av elektroniska kommunikationsnät var skyldiga enligt section 94 i 1984 års lag att vid anvisningar härom från en minister lämna ut uppgifter som samlats in inom ramen för deras ekonomiska verksamhet som omfattas av unionsrätten till säkerhets- och underrättelsetjänsterna. Så var däremot inte fallet i fråga om insamling av andra uppgifter som hade erhållits av säkerhets- och underrättelsetjänsterna utan att använda sig av sådana tvingande befogenheter. På grundval av det nyss anförda fann den hänskjutande domstolen att det var nödvändigt att begära ett förhandsavgörande från EU-domstolen för att få klarhet i huruvida ett system som det som följer av section 94 i 1984 års lag omfattas av unionsrätten och, om så är fallet, huruvida och på vilket sätt de krav som uppställs i den rättspraxis som följer av domen av den 21 december 2016, Tele2 Sverige och Watson m.fl. (C-203/15 och C-698/15, EU:C:2016:970) (nedan kallad domen Tele2) är tillämpliga på detta system.

23 I sin begäran om förhandsavgörande har den hänskjutande domstolen angett att ministern, enligt nämnda section 94, får ge leverantörer av elektroniska kommunikationstjänster de generella eller särskilda anvisningar som ministern anser vara nödvändiga med hänsyn till den nationella säkerheten eller till förbindelserna med en utländsk regering. Med hänvisning till definitionerna i section 21.4 och 21.6 i Ripa har den hänskjutande domstolen angett att de berörda uppgifterna innefattar trafikuppgifter och uppgifter om tjänsteanvändning, i den mening som avses i den sistnämnda bestämmelsen, och att det endast är innehållet i kommunikationen som inte omfattas. Dessa uppgifter

gör det bland annat möjligt att få kännedom om ”vem, var, när, hur?” när det gäller en kommunikation. Uppgifterna överförs till säkerhets- och underrättelsetjänsterna och lagras av dessa för deras verksamhet.

24 Enligt den hänskjutande domstolen skiljer sig det system som är aktuellt i det nationella målet från det som följer av Data Retention and Investigatory Powers Act 2014 (2014 års lag om datalagring och utredningsbefogenheter) (nedan kallad Dripa), som var i fråga i det mål som avgjordes genom domen av den 21 december 2016, Tele2 (C-203/15 och C-698/15, EU:C:2016:970). Enligt Dripa-systemet skulle nämligen uppgifter lagras av leverantörer av elektroniska kommunikationstjänster och göras tillgängliga inte bara för säkerhets- och underrättelsetjänsterna, med hänsyn till den nationella säkerheten, utan även för andra myndigheter efter deras behov. Tele2-domen avsåg dessutom en brottsutredning och inte nationell säkerhet.

25 Den hänskjutande domstolen har vidare anfört att de databaser som sammanställs av säkerhets- och underrättelsetjänsterna är föremål för en icke-konkret och automatiserad massdatabehandling, i syfte att påvisa förekomsten av eventuella okända hot. Den hänskjutande domstolen har i detta avseende anfört att de samlingar av metadata som sammanställts på detta sätt måste vara så fullständiga som möjligt för att säkerhets- och underrättelsetjänsterna ska kunna ha tillgång till en ”höstack” för att hitta ”nålen” som döljer sig där. När det gäller nyttan av säkerhets- och underrättelsetjänsternas massinsamling av uppgifter och teknikerna för att ta del av dessa uppgifter, har den hänskjutande domstolen särskilt hänvisat till slutsatserna i den rapport som David Anderson, QC, som då var United Kingdom Independent Reviewer of Terrorism Legislation (Förenade kungarikets oberoende utredare av terroristlagstiftningen), lämnade den 19 augusti 2016. Vid upprättandet av nämnda rapport grundade sig utredaren på en undersökning som utförts av en grupp underrättelsespecialister och på vittnesmål från anställda inom säkerhets- och underrättelsetjänsterna.

26 Den hänskjutande domstolen har även angett att Privacy International anser att det system som är aktuellt i det nationella målet är rättsstridigt enligt unionsrätten, medan svarandena i det nationella målet anser att skyldigheten enligt systemet att överföra uppgifter samt åtkomst till och användning av uppgifterna ligger utanför unionens befogenheter, i enlighet med bland annat artikel 4.2 FEU, enligt vilken nationell säkerhet också i fortsättningen ska vara varje medlemsstats eget ansvar.

27 I det avseendet har den hänskjutande domstolen hänvisat till domen av den 30 maj 2006, parlamentet/rådet och kommissionen (C-317/04 och C-318/04, EU:C:2006:346, punkterna 56–59), som rörde överföring av PNR-uppgifter (Passenger Name Record) i syfte att skydda allmän säkerhet, och anfört att affärsdrivande bolags verksamhet i samband med behandling och överföring av uppgifter i syfte att skydda nationell säkerhet inte förefaller omfattas av unionsrättens tillämpningsområde. Det som ska prövas är inte huruvida den aktuella verksamheten utgör behandling av uppgifter, utan enbart huruvida syftet med en sådan verksamhet, till sitt innehåll och sina verkningar, är att främja en väsentlig statlig funktion, i den mening som avses i artikel 4.2 FEU, med hjälp av en ram som inrättats av statsmakterna och som avser allmän säkerhet.

28 För det fall de åtgärder som är aktuella i det nationella målet ändå skulle anses omfattas av unionsrätten, anser den hänskjutande domstolen att de krav som anges i punkterna 119–125 i domen av den 21 december 2016, Tele2 (C-203/15 och C-698/15, EU:C:2016:970), framstår som olämpliga med avseende på nationell säkerhet och skulle kunna undergräva säkerhets- och underrättelsetjänsternas förmåga att möta vissa hot mot den nationella säkerheten.

29 Mot denna bakgrund beslutade Investigatory Powers Tribunal (Domstolen för utredningsbefogenheter) att vilandeförklara målet och att ställa följande frågor till EU-domstolen:

”Nedanstående frågor ställs mot bakgrund av följande omständigheter:

a) [Säkerhets- och underrättelsetjänsternas] möjligheter att använda [mängddata om kommunikation] som lämnas ut till dem är nödvändiga för skyddet av Förenade kungarikets nationella säkerhet, vilket omfattar verksamhet inom kontraterrorism, kontraspionage och ickespridning av kärnvapen.

b) Ett centralt inslag i säkerhets- och underrättelseorganens användning av [mängddata om kommunikation] är att upptäcka tidigare okända hot mot nationell säkerhet genom olika tekniker för icke-riktad massinsamling av uppgifter, vilka är beroende av att mängddata samlas på ett och samma ställe. Den huvudsakliga nyttan med nämnda tekniker består i att de gör det möjligt att snabbt kunna identifiera och nå ökad förståelse om spaningsobjekt samt i att de ger en grund för åtgärder vid ett omedelbart hot.

c) En tillhandahållare av ett elektroniskt kommunikationsnät är inte därefter skyldig att lagra [mängddata om kommunikation] (längre än den tid som följer av deras ordinarie verksamhetskrav), vilka lagras enbart av staten (säkerhets- och underrättelsetjänsterna).

d) Den nationella domstolen har funnit (med vissa reservationer) att de garantier som omgärdar säkerhets- och underrättelsetjänsternas användning av mängddata är förenliga med kraven i Europakonventionen.

e) Den nationella domstolen har funnit att åläggandet av de krav som anges i punkterna 119–125 i domen [av den 21 december 2016, Tele2, C-203/15 och C-698/15 (EU:C:2016:970)], om de var tillämpliga, skulle omintetgöra de åtgärder som säkerhets- och underrättelsetjänsterna vidtagit för att skydda nationell säkerhet, och därigenom äventyra Förenade kungarikets nationella säkerhet.

1) Med beaktande av artikel 4 FEU och artikel 1.3 i direktiv [2002/58], ska ett krav i anvisningar som en minister lämnar till en tillhandahållare av ett elektroniskt kommunikationsnät och som innebär att tillhandahållaren måste lämna ut [mängddata om kommunikation] till en medlemsstats säkerhets- och underrättelsetjänster anses omfattas av tillämpningsområdet för unionsrätten och direktiv [2002/58]?

2) Om fråga 1 ska besvaras jakande, är något av kraven som [gäller för lagrade uppgifter om kommunikation och som anges i punkterna 119–125 i domen av den 21 december 2016, Tele2, C-203/15 och C-698/15 (EU:C:2016:970)] – eller några andra krav utöver de som följer av Europakonventionen – tillämpliga på sådana anvisningar som lämnas av en minister? Om så är fallet, hur och i vilken mån är då dessa krav tillämpliga, med beaktande av att det är absolut nödvändigt för säkerhets- och underrättelseorganen att använda inhämtning av mängddata och tekniker för automatiserad behandling för att skydda den nationella säkerheten och med beaktande av den utsträckning i vilken åläggandet av sådana krav allvarligt kan inskränka nyss nämnda möjligheter för dessa organ, om de i övrigt är förenliga med Europakonventionen?”

Prövning av tolkningsfrågorna

Den första frågan

30 Den hänskjutande domstolen har ställt den första frågan för att få klarhet i huruvida artikel 1.3 i direktiv 2002/58, jämförd med artikel 4.2 FEU, ska tolkas på så sätt att direktivets tillämpningsområde omfattar en nationell lagstiftning som ger en statlig myndighet rätt att ålägga leverantörer av elektroniska kommunikationstjänster att överföra trafikuppgifter och lokaliseringsuppgifter till säkerhets- och underrättelsetjänsterna i syfte att skydda nationell säkerhet.

31 Privacy International har i det avseendet i allt väsentligt gjort gällande att det följer av domstolens praxis avseende tillämpningsområdet för direktiv 2002/58 att både säkerhets- och underrättelsetjänsternas inhämtning av uppgifter från nämnda leverantörer enligt section 94 i 1984 års lag och säkerhets- och underrättelsetjänsternas användning av uppgifterna omfattas av direktivets tillämpningsområde, oberoende av om uppgifterna inhämtas genom en överföring i efterhand eller om detta sker i realtid. Privacy International anser i synnerhet att den omständigheten att målet att skydda den nationella säkerheten uttryckligen anges i artikel 15.1 i direktivet inte innebär att sådana situationer ligger utanför direktivets tillämpningsområde, och artikel 4.2 FEU föranleder inte någon annan bedömning.

32 Förenade kungarikets regering, den tjeckiska och den estniska regeringen, Irland samt den franska, den cypriotiska, den ungerska, den polska och den svenska regeringen har däremot gjort gällande att direktiv 2002/58 inte är tillämpligt på den nationella lagstiftning som är aktuell i det nationella målet, eftersom den syftar till att skydda den nationella säkerheten. Nämnda regeringar anser att säkerhets- och underrättelsetjänsternas verksamhet omfattas av medlemsstaternas väsentliga statliga funktioner, vilka består i att upprätthålla allmän ordning samt att skydda den inre säkerheten och den territoriella integriteten, och följaktligen av medlemsstaternas exklusiva befogenhet, vilket bland annat framgår av artikel 4.2 tredje meningen FEU.

33 Enligt dessa regeringar kan direktiv 2002/58 således inte tolkas på så sätt att nationella åtgärder som syftar till att skydda den nationella säkerheten omfattas av direktivets tillämpningsområde. Artikel 1.3 i direktiv 2002/58 avgränsar direktivets tillämpningsområde och innebär att verksamhet som avser allmän säkerhet, försvar och statens säkerhet inte omfattas av direktivets tillämpningsområde, i likhet med vad som redan föreskrevs i artikel 3.2 första strecksatsen i direktiv 95/46. Nyss nämnda bestämmelser avspeglar den befogenhetsfördelning som anges i artikel 4.2 FEU och de skulle förlora sin ändamålsenliga verkan om det krävdes att åtgärder inom det nationella säkerhetsområdet uppfyller kraven i direktiv 2002/58. Vidare anser regeringarna att den rättspraxis som bygger på domstolens dom av den 30 maj 2006, parlamentet/rådet och kommissionen (C-317/04 och C-318/04, EU:C:2006:346), som rör artikel 3.2 första strecksatsen i direktiv 95/46, kan överföras på artikel 1.3 i direktiv 2002/58.

34 Domstolen gör i denna del följande bedömning. Enligt lydelsen i artikel 1.1 i direktiv 2002/58 möjliggörs genom direktivet 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.

35 I artikel 1.3 i nämnda direktiv utesluts ”statens verksamheter” på vissa angivna områden från direktivets tillämpningsområde, bland annat statens verksamheter på straffrättens område liksom verksamheter som avser allmän säkerhet, försvar, statens säkerhet, inbegripet statens ekonomiska välstånd när verksamheten rör statens säkerhet. De verksamheter som nämns som exempel är i samtliga fall verksamheter som endast kan bedrivas av staten eller statliga myndigheter och som inte kan bedrivas av enskilda (dom av den 2 oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punkt 32 och där angiven rättspraxis).

36 I artikel 3 i direktiv 2002/58 anges dessutom 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 (dom av den 2 oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punkt 33 och där angiven rättspraxis).

37 I detta sammanhang låter artikel 15.1 i direktiv 2002/58 medlemsstaterna, på de villkor som föreskrivs i den artikeln, ”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” (dom av den 21 december 2016, Tele2, C-203/15 och C-698/15, EU:C:2016:970, punkt 71).

38 Artikel 15.1 i direktiv 2002/58 förutsätter emellertid med nödvändighet att den nationella lagstiftning som avses i den bestämmelsen omfattas av direktivets tillämpningsområde, eftersom direktivet uttryckligen tillåter medlemsstaterna att vidta sådana åtgärder endast om de däri angivna villkoren är uppfyllda. Sådan lagstiftning reglerar dessutom, för de ändamål som anges i bestämmelsen, verksamheten för leverantörer av elektroniska kommunikationstjänster (dom av den 2 oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punkt 34 och där angiven rättspraxis).

39 Det är bland annat mot bakgrund av dessa överväganden som domstolen har slagit fast att artikel 15.1 i direktiv 2002/58, jämförd med artikel 3 i samma direktiv, ska tolkas så, att tillämpningsområdet för direktivet inte bara omfattar lagstiftning som ålägger leverantörer av elektroniska kommunikationstjänster att lagra trafik- och lokaliseringsuppgifter, utan även lagstiftning som ålägger dessa leverantörer att ge de behöriga nationella myndigheterna åtkomst till dessa uppgifter. Sådan lagstiftning medför nämligen med nödvändighet behandling av nämnda uppgifter från leverantörernas sida och kan, i den mån de reglerar dessa leverantörers verksamhet, inte likställas med sådana staten förbehållna verksamheter som avses i artikel 1.3 i nämnda direktiv (se, för ett liknande resonemang, dom av den 2 oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punkterna 35 och 37 och där angiven rättspraxis).

40 När det gäller en sådan lagstiftningsåtgärd som section 94 i 1984 års lag, med stöd av vilken den behöriga myndigheten får ge leverantörer av elektroniska kommunikationstjänster anvisningar om att lämna ut mängddata till säkerhets- och underrättelsetjänsterna genom överföring ska följande påpekas. Enligt definitionen i artikel 4.2 i förordning 2016/679, som enligt artikel 2 i direktiv 2002/58 jämförd med artikel 94.2 i förordning 2016/679 är tillämplig, avses med ”behandling” av personuppgifter ”en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling …, lagring …, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt …”.

41 Av detta följer att utlämnande av personuppgifter genom överföring, liksom lagring eller tillhandahållande på annat sätt av sådana uppgifter, utgör behandling i den mening som avses i artikel 3 i direktiv 2002/58 och omfattas följaktligen av tillämpningsområdet för det direktivet (se, för ett liknande resonemang, dom av den 29 januari 2008, Promusicae, C-275/06, EU:C:2008:54, punkt 45).

42 Mot bakgrund av övervägandena i punkt 38 ovan och systematiken i direktiv 2002/58 skulle en tolkning av detta direktiv, enligt vilken sådan lagstiftning som avses i artikel 15.1 i direktivet skulle vara undantagen från direktivets tillämpningsområde på grund av att de syften som denna lagstiftning måste eftersträva i materiellt hänseende väsentligen överlappar med syftena med de verksamheter som avses i artikel 1.3 i direktivet, innebära att nämnda artikel 15.1 helt fråntogs sin ändamålsenliga verkan (se, för ett liknande resonemang, dom av den 21 december 2016, Tele2, C-203/15 och C-698/15, EU:C:2016:970, punkterna 72 och 73).

43 Begreppet ”verksamheter” i artikel 1.3 i direktiv 2002/58 kan således inte, såsom generaladvokaten i huvudsak fann i punkt 75 i sitt förslag till avgörande i de förenade målen La Quadrature du Net m.fl. (C-511/18 och C-512/18, EU:C:2020:6), tolkas på så sätt att det omfattar sådan lagstiftning som den som avses i artikel 15.1 i detta direktiv.

44 Denna slutsats påverkas inte av artikel 4.2 FEU som de regeringar som nämns i punkt 32 ovan har hänvisat till. Enligt domstolens fasta praxis kan den omständigheten att en åtgärd har vidtagits för att skydda nationell säkerhet nämligen inte, trots att det ankommer på medlemsstaterna att definiera sina väsentliga säkerhetsintressen och att vidta de åtgärder som är nödvändiga för att säkerställa inre och yttre säkerhet, leda till att unionsrätten inte är tillämplig och befria medlemsstaterna från skyldigheten att iaktta unionsrätten (se, för ett liknande resonemang, dom av den 4 juni 2013, ZZ, C-300/11, EU:C:2013:363, punkt 38, dom av den 20 mars 2018, kommissionen/Österrike (Statstryckeri), C-187/16, EU:C:2018:194, punkterna 75 och 76, och dom av den 2 april 2020, kommissionen/Polen, Ungern och Tjeckien (Tillfällig mekanism för omplacering av personer som ansöker om internationellt skydd), C-715/17, C-718/17 och C-719/17, EU:C:2020:257, punkterna 143 och 170).

45 Det är riktigt att domstolen i domen av den 30 maj 2006, parlamentet/rådet och kommissionen (C-317/04 och C-318/04, EU:C:2006:346, punkterna 56–59), slog fast att lufttrafikföretags överföring av personuppgifter till myndigheter i tredjeland i syfte att förebygga och bekämpa terrorism och andra grova brott i kraft av artikel 3.2 första strecksatsen i direktiv 95/46 inte omfattades av tillämpningsområdet för detta direktiv, eftersom denna överföring sker inom en ram som inrättats av statsmakterna och som avser allmän säkerhet.

46 Med beaktande av övervägandena i punkterna 36, 38 och 39 ovan kan denna rättspraxis emellertid inte överföras på tolkningen av artikel 1.3 i direktiv 2002/58. Såsom generaladvokaten i huvudsak anförde i punkterna 70–72 i sitt förslag till avgörande i de förenade målen La Quadrature du Net m.fl. (C-511/18 och C-512/18, EU:C:2020:6), utesluter artikel 3.2 första strecksatsen i direktiv 95/46, vilken är den bestämmelse som avses i nämnda rättspraxis, nämligen från sitt tillämpningsområde generellt ”behandlingar som rör allmän säkerhet, försvar, statens säkerhet” utan att någon åtskillnad görs med avseende på vem som behandlar uppgifterna i fråga. En sådan åtskillnad måste däremot göras vid tolkningen av artikel 1.3 i direktiv 2002/58. Såsom framgår av punkterna 37–39 och 42 ovan omfattas nämligen all behandling av personuppgifter som utförs av leverantörer av elektroniska kommunikationstjänster av detta direktivs tillämpningsområde, inbegripet den behandling som följer av skyldigheter som ålagts dem av statsmakten. Den sistnämnda behandlingen kunde emellertid, i förekommande fall, omfattas av undantaget i artikel 3.2 första strecksatsen i direktiv 95/46, med hänsyn till den mer vidsträckta utformningen av den bestämmelsen, vilken avsåg all behandling, oavsett vem som är uppgiftsbehandlare och oavsett om den avser allmän säkerhet, försvar eller statens säkerhet.

47 Det ska dessutom påpekas att direktiv 95/46 som var i fråga i det mål som avgjordes genom domen av den 30 maj 2006, parlamentet/rådet och kommissionen (C-317/04 och C-318/04, EU:C:2006:346), enligt artikel 94.1 i förordning 2016/679 upphävdes och ersattes av denna förordning, med verkan från och med den 25 maj 2018. Även om det i artikel 2.2 d i nämnda förordning anges att den inte ska tillämpas på behandling som utförs av ”behöriga myndigheter” i syfte att bland annat förebygga och avslöja brott, i vilket även ingår att förhindra hot mot allmän säkerhet och förebygga sådana hot, framgår det av artikel 23.1 d och h i samma förordning att förordningen är tillämplig på behandling av personuppgifter som utförs av enskilda för samma ändamål. Härav följer att ovannämnda tolkning av artikel 1.3, artikel 3 och artikel 15.1 i direktiv 2002/58 är förenlig med den avgränsning av tillämpningsområdet för förordning 2016/679 som direktivet kompletterar och preciserar.

48 När medlemsstaterna däremot direkt genomför åtgärder som innebär undantag från konfidentialiteten vid elektronisk kommunikation, utan att ålägga tjänsteleverantörer av sådan kommunikation någon skyldighet att behandla uppgifter, omfattas skyddet av de berörda personernas uppgifter inte av direktiv 2002/58, utan enbart av nationell rätt, med förbehåll för tillämpningen av Europaparlamentets

och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (EUT L 119, 2016, s. 89), vilket innebär att åtgärderna i fråga bland annat måste vara förenliga med nationell rätt på grundlagsnivå och kraven i Europakonventionen.

49 Mot bakgrund av det ovan anförda ska den första frågan besvaras enligt följande. Artiklarna 1.3, 3 och 15.1 i direktiv 2002/58, jämförda med artikel 4.2 FEU, ska tolkas på så sätt att direktivets tillämpningsområde omfattar en nationell lagstiftning som ger en statlig myndighet rätt att ålägga leverantörer av elektroniska kommunikationstjänster att överföra trafikuppgifter och lokaliseringsuppgifter till säkerhets- och underrättelsetjänsterna i syfte att skydda nationell säkerhet.

Den andra frågan

50 Den hänskjutande domstolen har ställt den andra frågan för att få klarhet i huruvida artikel 15.1 i direktiv 2002/58, jämförd med artikel 4.2 FEU samt artiklarna 7, 8, 11 och 52.1 i stadgan, ska tolkas på så sätt att den utgör hinder för en nationell lagstiftning som ger en statlig myndighet rätt att ålägga leverantörer av elektroniska kommunikationstjänster att på ett generellt och odifferentierat sätt överföra trafikuppgifter och lokaliseringsuppgifter till säkerhets- och underrättelsetjänsterna i syfte att skydda nationell säkerhet.

51 Domstolen erinrar inledningsvis om att det framgår av uppgifterna i begäran om förhandsavgörande att section 94 i 1984 års lag innebär att ministern, när denne anser det vara nödvändigt med hänsyn till den nationella säkerheten eller till förbindelserna med en utländsk regering, genom anvisningar får ålägga leverantörer av elektroniska kommunikationstjänster att till säkerhets- och underrättelsetjänsterna överföra mängddata om kommunikation. Sådana data omfattar trafik- och lokaliseringsuppgifter samt uppgifter om tjänsteanvändning, i den mening som avses i section 21.4 och 21.6 i Ripa. Den nyss nämnda bestämmelsen omfattar bland annat uppgifter som behövs för att identifiera kommunikationskällan och slutmålet för kommunikationen, fastställa datum, tidpunkt och varaktighet för kommunikationen samt typen av kommunikation och för att lokalisera terminalutrustning och kommunikationer. Bland dessa uppgifter återfinns bland annat användarens namn och adress, telefonnummer och uppringt nummer, ip-adresser för kommunikationskällan och mottagaren av kommunikationen samt adressen till de besökta webbplatserna.

52 Sådant utlämnande av uppgifter genom överföring avser samtliga användare av elektroniska kommunikationsmedel, utan att det preciseras huruvida överföringen ska ske i realtid eller i efterhand. När uppgifterna väl har överförts lagras de – enligt uppgifterna i begäran om förhandsavgörande – av säkerhets- och underrättelsetjänsterna och förblir tillgängliga för dem i deras verksamhet, i likhet med andra databaser som de har. I synnerhet kan uppgifter som samlas in på detta sätt och som är föremål för icke-konkret och automatiserad behandling och analys korskontrolleras mot andra databaser som innehåller olika kategorier av mängddata om personuppgifter eller lämnas ut utanför säkerhets- och underrättelsetjänsterna och till tredjeländer. Till sist kan det konstateras att nyss nämnda åtgärder inte kräver förhandstillstånd från en domstol eller en oberoende förvaltningsmyndighet och de föranleder inte heller någon information till berörda personer.

53 Syftet med direktiv 2002/58 är, såsom framgår av bland annat skälen 6 och 7 i direktivet, att skydda användarna av elektroniska kommunikationstjänster mot de faror för deras personuppgifter och deras privatliv som följer av ny teknik och särskilt den ökade kapaciteten för automatiserad lagring och behandling av uppgifter. Direktivet syftar särskilt, såsom anges i dess skäl 2, till att säkerställa full respekt för de rättigheter som anges i artiklarna 7 och 8 i stadgan. Det framgår av motiveringen till förslaget till Europaparlamentets och rådets direktiv om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (COM(2000) 385 final), som ligger till

grund för direktiv 2002/58, att unionslagstiftaren avsåg att ”garantera en fortsatt hög skyddsnivå för personuppgifter och privatliv för alla elektroniska kommunikationstjänster, oavsett vilken teknik som används”.

54 I detta syfte anges i artikel 5.1 i direktiv 2002/58 att ”medlemsstaterna genom nationell lagstiftning [ska] säkerställa konfidentialitet vid kommunikation och därmed förbundna trafikuppgifter via allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster”. I samma bestämmelse anges även att ”[medlemsstaterna] särskilt [ska] 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” och att ”[d]enna punkt [inte får] förhindra teknisk lagring som är nödvändig för överföring av kommunikationen utan att det påverkar principen om konfidentialitet”.

55 I artikel 5.1 stadfästs således principen om konfidentialitet för såväl elektronisk kommunikation som därmed förbundna trafikuppgifter. Detta innebär bland annat ett principiellt förbud för andra personer än användarna att, utan användarnas samtycke, lagra sådan kommunikation och sådana uppgifter. Mot bakgrund av bestämmelsens generella ordalydelse ska den anses omfatta varje åtgärd som gör det möjligt för tredje man att få kännedom om kommunikationer och därmed förbundna uppgifter för andra ändamål än överföring av en kommunikation.

56 Förbudet i artikel 5.1 i direktiv 2002/58 mot att fånga upp kommunikationer och därmed förbundna uppgifter omfattar således alla former genom vilka leverantörer av elektroniska kommunikationstjänster gör trafik- och lokaliseringsuppgifter tillgängliga för statliga myndigheter, såsom säkerhets- och underrättelsetjänster, samt sådana myndigheters lagring av trafik- och lokaliseringsuppgifter, oberoende av hur dessa uppgifter senare används.

57 Genom att anta detta direktiv har unionslagstiftaren således konkretiserat de rättigheter som är stadfästa i artiklarna 7 och 8 i stadgan, vilket innebär att användarna av elektroniska kommunikationsmedel i princip har rätt att förvänta sig att deras kommunikationer och därmed förbundna uppgifter förblir anonyma och inte kan registreras, såvida de inte har samtyckt till detta (dom av den 6 oktober 2020, La Quadrature du Net m.fl., C-511/18, C-512/18 och C-520/18, punkt 109).

58 Enligt artikel 15.1 i direktiv 2002/58 får medlemsstaterna emellertid införa undantag från den principiella skyldigheten enligt artikel 5.1 i direktivet att garantera konfidentialiteten för personuppgifter och från motsvarande skyldigheter, vilka nämns bland annat i artiklarna 6 och 9 i direktivet, när en sådan begränsning i ett demokratiskt samhälle är nödvändig, lämplig och proportionell för att skydda nationell säkerhet, försvaret och allmän säkerhet samt för förebyggande, undersökning, avslöjande av och åtal för brott eller vid obehörig användning av ett elektroniskt kommunikationssystem. Medlemsstaterna får för detta ändamål bland annat vidta lagstiftningsåtgärder som innebär att uppgifter får bevaras under en begränsad period när det är motiverat av ett av dessa skäl.

59 Möjligheten att göra undantag från de rättigheter och skyldigheter som föreskrivs i artiklarna 5, 6 och 9 i direktiv 2002/58 kan emellertid inte motivera att ett undantag från den principiella skyldigheten att säkerställa konfidentialiteten för elektronisk kommunikation och därmed tillhörande uppgifter, och i synnerhet från det förbud mot lagring av sådana uppgifter som uttryckligen föreskrivs i artikel 5 i direktivet, blir huvudregeln (se, för ett liknande resonemang, dom av den 21 december 2016, Tele2, C-203/15 och C-698/15, EU:C:2016:970, punkterna 89 och 104, och dom av den 6 oktober 2020, La Quadrature du Net m.fl., C-511/18, C-512/18 och C-520/18, punkt 111).

60 Det framgår dessutom av artikel 15.1 tredje meningen i direktiv 2002/58 att medlemsstaterna endast får vidta lagstiftningsåtgärder för att begränsa omfattningen av de rättigheter och skyldigheter som avses i artiklarna 5, 6 och 9 i direktivet i enlighet med de allmänna principerna i unionsrätten, däribland proportionalitetsprincipen, och de grundläggande rättigheter som garanteras i stadgan. Domstolen har redan slagit fast att när en medlemsstat i nationell lagstiftning ålägger leverantörer av elektroniska kommunikationstjänster en skyldighet att lagra trafikuppgifter i syfte att, i förekommande fall, göra dem tillgängliga för behöriga nationella myndigheter väcker detta frågor om en sådan lagstiftnings förenlighet inte bara med artiklarna 7 och 8 i stadgan, vilka rör skyddet för privatlivet respektive skyddet av personuppgifter, utan även med artikel 11 i stadgan, som rör yttrandefriheten (se, för ett liknande resonemang, dom av den 8 april 2014, Digital Rights Ireland m.fl., C-293/12 och C-594/12, EU:C:2014:238, punkterna 25 och 70, samt dom av den 21 december 2016, Tele2, C-203/15 och C-698/15, EU:C:2016:970, punkterna 91 och 92 och där angiven rättspraxis).

61 Samma frågor uppkommer även för andra typer av behandling av uppgifter, såsom överföring av uppgifterna till andra personer än användarna eller åtkomst till uppgifterna i avsikt att de ska användas (se, analogt, yttrande 1/15 (PNR-avtalet mellan EU och Kanada) av den 26 juli 2017, EU:C:2017:592, punkt 122 och där angiven rättspraxis)

62 Vid tolkningen av artikel 15.1 i direktiv 2002/58 ska således 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, såsom denna betydelse framgår av domstolens praxis, samt betydelsen av rätten till yttrandefrihet beaktas. Denna grundläggande rättighet, som garanteras i artikel 11 i stadgan, utgör nämligen 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 6 mars 2001, Connolly/kommissionen, C-274/99 P, EU:C:2001:127, punkt 39, och dom av den 21 december 2016, Tele2, C-203/15 och C-698/15, EU:C:2016:970, punkt 93 och där angiven rättspraxis).

63 De rättigheter som är stadfästa i artiklarna 7, 8 och 11 i stadgan är emellertid inte några absoluta rättigheter, utan måste bedömas utifrån deras funktion i samhället (se, för ett liknande resonemang, dom av den 16 juli 2020, Facebook Ireland och Schrems, C-311/18, EU:C:2020:559, punkt 172 och där angiven rättspraxis).

64 Såsom framgår av artikel 52.1 i stadgan är det nämligen enligt stadgan tillåtet att begränsa utövandet av dessa rättigheter, under förutsättning att begränsningarna föreskrivs i lag, att de är förenliga med det väsentliga innehållet i dessa rättigheter och att de, med beaktande av proportionalitetsprincipen, är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller mot behovet av skydd för andra människors rättigheter och friheter

65 Det ska tilläggas att kravet på att samtliga begränsningar i utövandet av grundläggande rättigheter ska vara föreskrivna i lag innebär att räckvidden av begränsningen i utövandet av den aktuella rättigheten ska vara definierad i själva den rättsliga grund som tillåter ingreppet (dom av den 16 juli 2020, Facebook Ireland och Schrems, C-311/18, EU:C:2020:559, punkt 175 och där angiven rättspraxis).

66 Vad gäller iakttagandet av proportionalitetsprincipen föreskrivs i artikel 15.1 första meningen i direktiv 2002/58 att medlemsstaterna får vidta en åtgärd som avviker från principen om konfidentialitet vid kommunikation och därmed tillhörande trafikuppgifter, när en sådan åtgärd är ”nödvändig, lämplig och proportionerlig” ”i ett demokratiskt samhälle”, med hänsyn till de mål som anges i denna bestämmelse. I skäl 11 i direktivet anges att en åtgärd av detta slag ska vara i ”strikt” proportion till det avsedda ändamålet.

67 Det ska i detta avseende erinras om att skyddet för den grundläggande rätten till respekt för privatlivet enligt domstolens fasta praxis kräver att undantag från och begränsningar av skyddet för personuppgifter ska inskränkas till vad som är strängt nödvändigt. Uppnåendet ett mål av allmänt

samhällsintresse kan dessutom inte ske utan att det beaktas att detta mål måste vara förenligt med de grundläggande rättigheter som berörs av åtgärden, varvid en balanserad avvägning ska göras mellan, å ena sidan, målet av allmänt samhällsintresse, och, å andra sidan, rättigheterna i fråga (se, för ett liknande resonemang, 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, punkterna 76, 77 och 86, samt dom av den 8 april 2014, Digital Rights Ireland m.fl., C-293/12 och C-594/12, EU:C:2014:238, punkt 52, yttrande 1/15 (PNR-avtalet mellan EU och Kanada) av den 26 juli 2017, EU:C:2017:592, punkt 140).

68 För att kravet på proportionalitet ska vara uppfyllt måste det i lagstiftning föreskrivas klara och precisa bestämmelser som reglerar räckvidden och tillämpningen av den aktuella åtgärden samt anges minimikrav, så att de personer vars personuppgifter berörs har tillräckliga garantier för att uppgifterna på ett effektivt sätt är skyddade mot riskerna för missbruk. Denna lagstiftning ska vara rättsligt bindande enligt nationell rätt och i synnerhet ange under vilka omständigheter och på vilka villkor en åtgärd avseende behandling av sådana uppgifter får vidtas, vilket säkerställer att ingreppet begränsas till vad som är strängt nödvändigt. Behovet av sådana garantier är särskilt stort när personuppgifter är föremål för automatiserad behandling, särskilt när det föreligger en betydande risk för otillåten åtkomst till uppgifterna. Dessa överväganden äger särskild giltighet när det är fråga om skyddet av den särskilda kategori av personuppgifter som utgörs av känsliga uppgifter (se, för ett liknande resonemang, dom av den 8 april 2014, Digital Rights Ireland m.fl., C-293/12 och C-594/12, EU:C:2014:238, punkterna 54 och 55, och dom av den 21 december 2016, Tele2, C-203/15 och C-698/15, EU:C:2016:970, punkt 117, yttrande 1/15 (PNR-avtalet mellan EU och Kanada) av den 26 juli 2017, EU:C:2017:592, punkt 141).

69 Domstolen ska nu pröva frågan huruvida en nationell lagstiftning, som den som är aktuell i det nationella målet, uppfyller kraven i artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11 och artikel 52.1 i stadgan. I det avseendet ska det påpekas att överföring av trafik- och lokaliseringsuppgifter till andra personer än användarna, som till exempel säkerhets- och underrättelsetjänster, avviker från principen om konfidentialitet. När sådan överföring sker – som i det nu aktuella fallet – på ett generellt och odifferentierat sätt får detta till följd att undantaget från den principiella skyldigheten att garantera konfidentialitet för uppgifterna görs till huvudregel, medan det system som inrättats genom direktiv 2002/58 däremot kräver att ett sådant undantag förblir just ett undantag.

70 Enligt domstolens fasta praxis utgör dessutom överföring av trafik- och lokaliseringsuppgifter till tredje man ett ingrepp i de grundläggande rättigheter som stadfästs i artiklarna 7 och 8 i stadgan, oavsett hur dessa uppgifter senare används. Det saknar härvidlag betydelse om de uppgifter som avser privatlivet är av känslig art eller om de berörda har fått utstå eventuella olägenheter på grund av ingreppet (se, för ett liknande resonemang, yttrande 1/15 (PNR-avtalet mellan EU och Kanada), av den 26 juli 2017, EU:C:2017:592, punkterna 124 och 126 och där angiven rättspraxis, och dom av den 6 oktober 2020, La Quadrature du Net m.fl., C-511/18, C-512/18 och C-520/18, punkterna 115 och 116).

71 Det ingrepp som överföring av trafik- och lokaliseringsuppgifter till säkerhets- och underrättelsetjänsterna utgör i den rätt som är stadfäst i artikel 7 i stadgan måste betraktas som synnerligen allvarligt, bland annat med hänsyn till att den information som dessa uppgifter kan innehålla är känslig och i synnerhet till att det utifrån uppgifterna är möjligt att kartlägga de berörda personerna, då sådan information är lika känslig som själva innehållet i kommunikationerna. Det kan dessutom ge de berörda personerna en känsla av att deras privatliv står under ständig övervakning (se, analogt, dom av den 8 april 2014, Digital Rights Ireland m.fl., C-293/12 och C-594/12, EU:C:2014:238, punkterna 27 och 37, och dom av den 21 december 2016, Tele2, C-203/15 och C-698/15, EU:C:2016:970, punkterna 99 och 100).

72 Det ska vidare påpekas att en överföring av trafik- och lokaliseringsuppgifter till statliga myndigheter för säkerhetsändamål i sig kan utgöra ett åsidosättande av rätten till respekt för kommunikationer, vilken är stadfäst i artikel 7 i stadgan, och ha en avhållande inverkan på användarna av elektroniska kommunikationsmedels utövande av sin yttrandefrihet, vilken garanteras i artikel 11 i stadgan. En sådan avhållande inverkan kan särskilt påverka personer vars kommunikationer enligt nationella regler omfattas av tystnadsplikt och visselblåsare, vilkas verksamhet skyddas av Europaparlamentets och rådets direktiv (EU) 2019/1937 av den 23 oktober 2019 om skydd för personer som avslöjar överträdelser av unionsrätten (EUT L 305, 2019, s. 17). Den omständigheten att antalet lagrade uppgifter är stort och att det rör sig om många olika slags uppgifter förstärker dessutom allvaret av dessa effekter (se, för ett liknande resonemang, dom av den 8 april 2014, Digital Rights Ireland m.fl., C-293/12 och C-594/12, EU:C:2014:238, punkt 28, dom av den 21 december 2016, Tele2, C-203/15 och C-698/15, EU:C:2016:970, punkt 101, och dom av den 6 oktober 2020, La Quadrature du Net m.fl., C-511/18, C-512/18 och C-520/18, punkt 118).

73 Med hänsyn till den stora mängd trafik- och lokaliseringsuppgifter som kan bli föremål för fortlöpande lagring genom en generell och odifferentierad lagringsåtgärd och till att den information som dessa uppgifter kan innehålla är känslig, medför den omständigheten att leverantörer av elektroniska kommunikationstjänster lagrar dessa uppgifter i sig en risk för missbruk och olovlig åtkomst.

74 När det gäller de mål som kan motivera sådana ingrepp, närmare bestämt målet att skydda den nationella säkerheten, vilket är aktuellt i det nationella målet, ska det inledningsvis påpekas att det i artikel 4.2 FEU anges att nationell säkerhet också i fortsättningen ska vara varje medlemsstats eget ansvar. Detta ansvar motsvarar det grundläggande intresset av att skydda statens väsentliga funktioner och samhällets grundläggande intressen och inbegriper förebyggande och beivrande av verksamhet som allvarligt kan störa de grundläggande konstitutionella, politiska, ekonomiska eller sociala strukturerna i ett land och i synnerhet direkt hota samhället, befolkningen eller staten som sådan, såsom bland annat terrorverksamhet (dom av den 6 oktober 2020, La Quadrature du Net m.fl., C-511/18, C-512/18 och C-520/18, punkt 135).

75 Betydelsen av målet att skydda nationell säkerhet, tolkad mot bakgrund av artikel 4.2 FEU, är dock mer omfattande än betydelsen av de övriga mål som anges i artikel 15.1 i direktiv 2002/58, bland annat målen att bekämpa brottslighet i allmänhet, även grov brottslighet, och att skydda allmän säkerhet. Sådana hot som avses i föregående punkt skiljer sig nämligen, till sin art och på grund av sitt särskilda allvar, från risken i allmänhet för oroligheter eller störningar, även allvarliga sådana, av den allmänna säkerheten. Under förutsättning att övriga krav i artikel 52.1 i stadgan iakttas, kan målet att skydda nationell säkerhet således motivera åtgärder som innebär mer långtgående ingrepp i de grundläggande rättigheterna än dem som dessa övriga mål skulle kunna motivera (dom av den 6 oktober 2020, La Quadrature du Net m.fl., C-511/18, C-512/18 och C-520/18, punkt 136).

76 För att uppfylla det krav på proportionalitet som det erinrats om i punkt 67 ovan, enligt vilket undantag från och begränsningar av skyddet för personuppgifter ska inskränkas till vad som är strängt nödvändigt, måste en nationell lagstiftning som innebär ett ingrepp i de grundläggande rättigheter som är stadfästa i artiklarna 7 och 8 i stadgan uppfylla de krav som följer av den rättspraxis som anges i punkterna 65, 67 och 68 ovan.

77 Vad särskilt beträffar en myndighets åtkomst till personuppgifter finner domstolen att en lagstiftning inte kan vara begränsad till att kräva att myndigheternas åtkomst till uppgifterna svarar mot det ändamål som eftersträvas med lagstiftningen, utan den måste även fastställa de materiella och formella villkor som gäller för sådan användning (se, analogt, yttrande 1/15 (PNR-avtalet mellan EU och Kanada) av den 26 juli 2017, EU:C:2017:592, punkt 192 och där angiven rättspraxis).

78 Eftersom en heltäckande 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 en nationell lagstiftning som reglerar tillgång till trafik- och lokaliseringsuppgifter

således vara grundad på objektiva kriterier som avgör under vilka omständigheter och på vilka villkor behöriga nationella myndigheter ska ges tillgång till de aktuella uppgifterna (se, för ett liknande resonemang, dom av den 21 december 2016, Tele2, C-203/15 och C-698/15, EU:C:2016:970, punkt 119 och där angiven rättspraxis).

79 Nyss nämnda krav gäller i ännu högre grad för en lagstiftningsåtgärd, som den som är aktuell i det nationella målet, enligt vilken den behöriga nationella myndigheten får ålägga leverantörer av elektroniska kommunikationstjänster att genom generell och odifferentierad överföring lämna ut trafik- och lokaliseringsuppgifter till säkerhets- och underrättelsetjänsterna. Sådan överföring får nämligen till följd att nämnda uppgifter görs tillgängliga för myndigheterna (se, analogt, yttrande 1/15 (PNR-avtalet mellan EU och Kanada) av den 26 juli 2017, EU:C:2017:592, punkt 212).

80 Eftersom överföringen av trafik- och lokaliseringsuppgifter sker på ett generellt och odifferentierat sätt berör den på ett allomfattande sätt samtliga personer som använder elektroniska kommunikationstjänster. Den är således även tillämplig på personer beträffande vilka det inte finns något indicium som ger anledning att tro att deras beteende skulle kunna ha ett samband, inte ens indirekt eller avlägset, med målet att skydda den nationella säkerheten och, i synnerhet, utan att det har visats att det finns ett samband mellan de uppgifter som ska överföras och ett hot mot den nationella säkerheten (se, för ett liknande resonemang, dom av den 8 april 2014, Digital Rights Ireland m.fl., C-293/12 och C-594/12, EU:C:2014:238, punkterna 57 och 58, och dom av den 21 december 2016, Tele2, C-203/15 och C-698/15, EU:C:2016:970, punkt 105). Med hänsyn till att överföring av trafik- och lokaliseringsuppgifter till statliga myndigheter motsvarar – i enlighet med vad som anförts i punkt 79 ovan – åtkomst till uppgifterna, finner domstolen att en lagstiftning som tillåter en generell och odifferentierad överföring av uppgifter till statliga myndigheter innebär en allmän åtkomst till uppgifterna.

81 Härav följer att en nationell lagstiftning som ålägger leverantörer av elektroniska kommunikationstjänster att genom generell och odifferentierad överföring lämna ut trafik- och lokaliseringsuppgifter till säkerhets- och underrättelsetjänsterna går utöver vad som är strängt nödvändigt och inte kan anses vara motiverad i ett demokratiskt samhälle, såsom krävs enligt artikel 15.1 i direktiv 2002/58, jämförd med artikel 4.2 FEU samt artiklarna 7, 8, 11 och 52.1 i stadgan.

82 Mot bakgrund av det ovan anförda ska den andra frågan besvaras enligt följande. Artikel 15.1 i direktiv 2002/58, jämförd med artikel 4.2 FEU samt 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 ger en statlig myndighet rätt att ålägga leverantörer av elektroniska kommunikationstjänster att på ett generellt och odifferentierat sätt överföra trafikuppgifter och lokaliseringsuppgifter till säkerhets- och underrättelsetjänsterna i syfte att skydda nationell säkerhet.

Rättegångskostnader

83 Eftersom förfarandet i förhållande till parterna i det nationella målet utgör ett led i beredningen av samma mål, ankommer det på den hänskjutande domstolen 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) **Artiklarna 1.3, 3 och 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, jämförda med artikel 4.2 FEU, ska tolkas på så sätt att direktivets**

tillämpningsområde omfattar en nationell lagstiftning som ger en statlig myndighet rätt att ålägga leverantörer av elektroniska kommunikationstjänster att överföra trafikuppgifter och lokaliseringsuppgifter till säkerhets- och underrättelsetjänsterna i syfte att skydda nationell säkerhet.

2) **Artikel 15.1 i direktiv 2002/58, i dess lydelse enligt direktiv 2009/136, jämförd med artikel 4.2 FEU samt 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 ger en statlig myndighet rätt att ålägga leverantörer av elektroniska kommunikationstjänster att på ett generellt och odifferentierat sätt överföra trafikuppgifter och lokaliseringsuppgifter till säkerhets- och underrättelsetjänsterna i syfte att skydda nationell säkerhet.**

Underskrifter