Samling af Afgørelser

DOMSTOLENS DOM (Store Afdeling)

6. oktober 2020*

»Præjudiciel forelæggelse – behandling af personoplysninger i den elektroniske kommunikationssektor – udbydere af elektroniske kommunikationstjenester – generel og udifferentieret overføring af trafikdata og lokaliseringsdata – beskyttelse af den nationale sikkerhed – direktiv 2002/58/EF – anvendelsesområde – artikel 1, stk. 3, og artikel 3 – fortrolighed af elektronisk kommunikation – beskyttelse – artikel 5 og artikel 15, stk. 1 – Den Europæiske Unions charter om grundlæggende rettigheder – artikel 7, 8 og 11 samt artikel 52, stk. 1 – artikel 4, stk. 2, TEU«

I sag C-623/17,

angående en anmodning om præjudiciel afgørelse i henhold til artikel 267 TEUF, indgivet af Investigatory Powers Tribunal (domstol for efterforskningsbeføjelser, Det Forenede Kongerige) ved afgørelse af 18. oktober 2017, indgået til Domstolen den 31. oktober 2017, i sagen

Privacy International

mod

Secretary of State for Foreign and Commonwealth Affairs,

Secretary of State for the Home Department,

Government Communications Headquarters,

Security Service,

Secret Intelligence Service,

har

DOMSTOLEN (Store Afdeling),

sammensat af præsidenten, K. Lenaerts, vicepræsidenten, R. Silva de Lapuerta, afdelingsformændene J.-C. Bonichot, A. Arabadjiev, A. Prechal, M. Safjan, P.G. Xuereb og L.S. Rossi samt dommerne J. Malenovský, L. Bay Larsen, T. von Danwitz (refererende dommer), C. Toader, K. Jürimäe, C. Lycourgos og N. Piçarra,

generaladvokat: M. Campos Sánchez-Bordona,

justitssekretær: fuldmægtig C. Strömholm,

på grundlag af den skriftlige forhandling og efter retsmødet den 9. og den 10. september 2019,

* Processprog: engelsk.

efter at der er afgivet indlæg af:

– Privacy International ved B. Jaffey og T. de la Mare, QC, solicitor D. Cashman og avocat H. Roy,

– Det Forenede Kongeriges regering ved Z. Lavery, D. Guðmundsdóttir og S. Brandon, som befuldmægtigede, bistået af G. Facenna og D. Beard, QC, samt af barristers C. Knight og R. Palmer,

– den belgiske regering ved P. Cottin og J.-C. Halleux, som befuldmægtigede, bistået af advocaat J. Vanpraet og avocat E. de Lophem,

– den tjekkiske regering ved M. Smolek, J. Vláčil og O. Serdula, som befuldmægtigede,

– den tyske regering først ved M. Hellmann, R. Kanitz, D. Klebs og T. Henze, derefter ved J. Möller, M. Hellmann, R. Kanitz og D. Klebs, som befuldmægtigede,

– den estiske regering ved A. Kalbus, som befuldmægtiget,

– Irland ved M. Browne, G. Hodge og A. Joyce, som befuldmægtigede, bistået af barrister D. Fennelly,

– den spanske regering først ved L. Aguilera Ruiz og M.J. García-Valdecasas Dorrego, derefter ved L. Aguilera Ruiz, som befuldmægtigede,

– den franske regering først ved E. de Moustier, E. Armoët, A.-L. Desjonquères, F. Alabrune, D. Colas og D. Dubois, derefter ved E. de Moustier, E. Armoët, A.-L. Desjonquères, F. Alabrune og D. Dubois, som befuldmægtigede,

– den cypriotiske regering ved E. Symeonidou og E. Neofytou, som befuldmægtigede,

– den lettiske regering først ved V. Soņeca og I. Kucina, derefter ved V. Soņeca, som befuldmægtigede,

– den ungarske regering først ved G. Koós, M.Z. Fehér, G. Tornyai og Z. Wagner, derefter ved G. Koós og M.Z. Fehér, som befuldmægtigede,

– den nederlandske regering ved C.S. Schillemans og M. Bulterman, som befuldmægtigede,

– den polske regering ved B. Majczyna, J. Sawicka og M. Pawlicka, som befuldmægtigede,

– den portugisiske regering ved L. Inez Fernandes, M. Figueiredo og F. Aragão Homem, som befuldmægtigede,

– den svenske regering først ved A. Falk, H. Shev, C. Meyer-Seitz, L. Zettergren og A. Alriksson, derefter ved H. Shev, C. Meyer-Seitz, L. Zettergren og A. Alriksson, som befuldmægtigede,

– den norske regering ved T.B. Leming, M. Emberland og J. Vangsnes, som befuldmægtigede,

– Europa-Kommissionen først ved H. Kranenborg, M. Wasmeier, D. Nardi og P. Costa de Oliveira, derefter ved H. Kranenborg, M. Wasmeier og D. Nardi, som befuldmægtigede,

– Den Europæiske Tilsynsførende for Databeskyttelse ved T. Zerdick og A. Buchta, som befuldmægtigede,

og efter at generaladvokaten har fremsat forslag til afgørelse i retsmødet den 15. januar 2020,

afsagt følgende

Dom

1 Anmodningen om præjudiciel afgørelse vedrører fortolkningen af artikel 1, stk. 3, og artikel 15, stk. 1, i Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktiv om databeskyttelse inden for elektronisk kommunikation) (EFT 2002, L 201, s. 37), som ændret ved Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009 (EUT 2009, L 337, s. 11) (herefter »direktiv 2002/58«), sammenholdt med artikel 4, stk. 2, TEU og artikel 7 og 8 samt artikel 52, stk. 1, i Den Europæiske Unions charter om grundlæggende rettigheder (herefter »chartret«).

2 Denne anmodning er blevet indgivet i forbindelse med en tvist mellem Privacy International og Secretary of State for Foreign and Commonwealth Affairs (minister for udenrigs- og Commonwealth-anliggender, Det Forenede Kongerige), Secretary of State for the Home Departement (indenrigsministeren, Det Forenede Kongerige), Government Communications Headquarters (statens kommunikationshovedkvarter, Det Forenede Kongerige) (herefter »GCHQ«), Security Service (sikkerhedstjenesten, Det Forenede Kongerige, herefter »MI5«) og Secret Intelligence Service (efterretningstjenesten, Det Forenede Kongerige, herefter »MI6«) vedrørende lovligheden af en lovgivning, som tillader sikkerheds- og efterretningstjenesternes indsamling og brug af bulk-kommunikationsdata (*bulk communications data*).

Retsforskrifter

EU-retten

Direktiv 95/46

3 Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (EFT 1995, L 281, s. 31) blev ophævet med virkning fra den 25. maj 2018 ved Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (EUT 2016, L 119, s. 1). Det nævnte direktivs artikel 3 med overskriften »Anvendelsesområde« havde følgende ordlyd:

»1. Dette direktivs bestemmelser anvendes på behandling af personoplysninger, der helt eller delvis foretages ved hjælp af edb, samt på ikke-elektronisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

2. Dette direktiv gælder ikke for sådan behandling af personoplysninger,

– som iværksættes med henblik på udøvelse af aktiviteter, der ikke er omfattet af fællesskabsretten, som f.eks. de aktiviteter, der er fastsat i afsnit V og VI [TEU], og under ingen omstændigheder for behandling, der vedrører den offentlige sikkerhed, forsvar, statens sikkerhed (herunder statens økonomiske interesser, når behandlingen er forbundet med spørgsmål vedrørende statens sikkerhed) og statens aktiviteter på det strafferetlige område

– som foretages af en fysisk person med henblik på udøvelse af rent personlige eller familiemæssige aktiviteter.«

Direktiv 2002/58

4 2., 6., 7., 11., 22., 26. og 30. betragtning til direktiv 2002/58 har følgende ordlyd:

»(2) Dette direktiv søger at overholde de grundlæggende rettigheder og respektere de principper, der anerkendes i især [chartret]. Direktivet søger især at sikre fuld overholdelse af rettighederne i [chartrets] artikel 7 og 8.

[…]

(6) Internettet vender op og ned på de traditionelle markedsstrukturer, idet det udgør en fælles, global infrastruktur for fremføring af en lang række elektroniske kommunikationstjenester. Offentligt tilgængelige elektroniske kommunikationstjenester via internettet giver brugerne nye muligheder, men medfører også nye risikomomenter for deres personoplysninger og privatliv.

(7) Med hensyn til offentlige kommunikationsnet bør der træffes særlige foranstaltninger af lovgivningsmæssig, administrativ og teknisk art for at beskytte fysiske personers grundlæggende rettigheder og frihedsrettigheder og juridiske personers legitime interesser, navnlig mod den voksende risiko, der er forbundet med automatiseret opbevaring og behandling af oplysninger om abonnenter og brugere.

[…]

(11) Ligesom direktiv [95/46] finder dette direktiv ikke anvendelse på beskyttelse af grundlæggende rettigheder og frihedsrettigheder, der er forbundet med aktiviteter, der ikke er omfattet af [EU-]retten. Det ændrer derfor ikke den nuværende balance mellem enkeltpersoners ret til privatlivets fred og medlemsstaternes mulighed for, jf. artikel 15, stk. 1, i dette direktiv, at træffe de foranstaltninger, der er nødvendige til beskyttelse af den offentlige sikkerhed, forsvaret, statens sikkerhed (herunder statens økonomiske interesser, når disse aktiviteter er forbundet med spørgsmål vedrørende statens sikkerhed) og statens aktiviteter på det strafferetlige område. Dette direktiv berører derfor ikke medlemsstaternes mulighed for lovligt at opfange elektronisk kommunikation eller træffe andre foranstaltninger, hvis det er nødvendigt med et af disse formål for øje og i overensstemmelse med den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder[, undertegnet i Rom den 4. november 1950] som fortolket i Den Europæiske Menneskerettighedsdomstols retspraksis. Sådanne foranstaltninger skal være passende, stå i åbenbart rimeligt forhold til det mål, der forfølges, og være nødvendige i et demokratisk samfund, og foranstaltningerne bør omfattes af passende beskyttelsesordninger i overensstemmelse med den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder.

[…]

(22) Det er ikke tanken, at forbuddet mod, at der af andre end brugerne eller uden disses samtykke lagres oplysninger og de dertil hørende trafikdata, skal omfatte enhver automatisk, mellemliggende og kortvarig lagring af denne information, når blot lagringen udelukkende sker med henblik på gennemførelse af transmissionen i de elektroniske kommunikationsnet, og oplysningerne ikke lagres længere end det tidsrum, der er nødvendigt for transmissionen og af hensyn til trafikstyringen, forudsat at sikkerhedsbeskyttelsen af oplysningerne i lagringsperioden fortsat er garanteret. Hvis det er nødvendigt for at effektivisere den videre transmission af offentligt tilgængelige oplysninger til andre modtagere af tjenesten efter deres anmodning herom, bør dette direktiv ikke forhindre, at sådanne oplysninger lagres, forudsat at disse oplysninger i alle tilfælde er offentligt tilgængelige uden begrænsninger, og at alle data vedrørende de abonnenter eller brugere, der anmoder om disse oplysninger, slettes.

[…]

(26) Abonnentoplysninger, som behandles i elektroniske kommunikationsnet ved etablering af en kommunikationsforbindelse og fremføring af information, indeholder oplysninger om fysiske personers privatliv og vedrører retten til respekt for deres korrespondance eller vedrører juridiske personers legitime interesser. Sådanne data må kun lagres i det omfang, det er nødvendigt for tjenestens gennemførelse med henblik på debitering og afregning for samtrafik, og kun i et begrænset tidsrum. [Yderligere behandling af sådanne data må] kun ske, hvis abonnenten har givet sit samtykke hertil på grundlag af en nøjagtig og fuldstændig orientering fra udbyderen af de offentligt tilgængelige elektroniske kommunikationstjenester om arten af den yderligere behandling, han agter at foretage, og om abonnentens ret til at nægte eller tilbagekalde sit samtykke til denne behandling. Trafikdata, som anvendes til markedsføring af udbyderens egne kommunikationstjenester […], bør ligeledes slettes eller anonymiseres […]

[…]

(30) Systemer til levering af elektroniske kommunikationsnet og kommunikationstjenester bør konstrueres, så de begrænser mængden af nødvendige personoplysninger til et absolut minimum. […]«

5 Artikel 1 i direktiv 2002/58 med overskriften »Anvendelsesområde og formål« bestemmer:

»1. Dette direktiv tager sigte på en harmonisering af nationale bestemmelser, der er nødvendig for at sikre et ensartet niveau i beskyttelsen af de grundlæggende rettigheder og frihedsrettigheder og navnlig retten til privatliv og fortrolighed i forbindelse med behandling af personoplysninger inden for den elektroniske kommunikationssektor, og for at sikre fri omsætning af sådanne oplysninger og af elektronisk kommunikationsudstyr og elektroniske kommunikationstjenester i [Den Europæiske Union].

2. Med henblik på at nå de i stk. 1 omhandlede mål specificerer og supplerer dette direktivs bestemmelser direktiv [95/46]. Nærværende bestemmelser beskytter desuden legitime interesser hos abonnenter, der er juridiske personer.

3. Dette direktiv gælder ikke for aktiviteter, der ikke er omfattet af [TEUF], som f.eks. de aktiviteter, der er omfattet af afsnit V og VI i traktaten om Den Europæiske Union, og under ingen omstændigheder for aktiviteter, der vedrører den offentlige sikkerhed, forsvaret, statens sikkerhed (herunder statens økonomiske interesser, når disse aktiviteter er forbundet med spørgsmål vedrørende statens sikkerhed) og statens aktiviteter på det strafferetlige område.«

6 Dette direktivs artikel 2 med overskriften »Definitioner« er affattet således:

»Medmindre andet angives, gælder i dette direktiv de definitioner, der er fastsat i direktiv [95/46] og Europa-Parlamentets og Rådets direktiv 2002/21/EF af 7. marts 2002 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (rammedirektivet) [(EFT 2002, L 108, s. 33)].

Følgende definitioner anvendes også:

a) »bruger«: en fysisk person, som anvender en offentligt tilgængelig elektronisk kommunikationstjeneste i privat eller forretningsmæssigt øjemed, uden nødvendigvis at abonnere på den pågældende tjeneste

b) »trafikdata«: data, som behandles med henblik på overføring af kommunikation i et elektronisk kommunikationsnet eller debitering heraf

c) »lokaliseringsdata«: data, som behandles i et elektronisk kommunikationsnet eller af en elektronisk kommunikationstjeneste og angiver den geografiske placering af det terminaludstyr, som brugeren af en offentligt tilgængelig elektronisk kommunikationstjeneste anvender

d) »kommunikation«: oplysninger, som udveksles eller overføres mellem et begrænset antal parter via en offentligt tilgængelig elektronisk kommunikationstjeneste. Dette omfatter ikke oplysninger, der overføres som del af en radio- og fjernsynstransmissionstjeneste til offentligheden via et elektronisk kommunikationsnet, medmindre oplysningerne kan kædes sammen med en identificerbar abonnent eller bruger, der modtager oplysningerne

[…]«

7 Det nævnte direktivs artikel 3 med overskriften »Omfattede tjenester« fastsætter:

»Dette direktiv finder anvendelse på behandling af persondata i forbindelse med, at offentligt tilgængelige elektroniske kommunikationstjenester stilles til rådighed via offentlige kommunikationsnet i [EU], herunder offentlige kommunikationsnet med dataindsamlings- og identifikationsudstyr.«

8 Artikel 5 i direktiv 2002/58 med overskriften »Kommunikationshemmelighed« har følgende ordlyd:

»1. Medlemsstaterne sikrer kommunikationshemmeligheden ved brug af offentlige kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester, både for så vidt angår selve kommunikationen og de dermed forbundne trafikdata, via nationale forskrifter. De forbyder især aflytning, registrering, lagring og andre måder, hvorpå samtaler kan opfanges eller overvåges af andre end brugerne, uden at de pågældende brugere har indvilget heri, bortset fra tilfælde, hvor det er tilladt ifølge lovgivningen, jf. artikel 15, stk. 1. Dette stykke er ikke til hinder for teknisk lagring, som er nødvendig for overføring af en kommunikation, forudsat at princippet om kommunikationshemmelighed ikke berøres heraf.

[…]

3. Medlemsstaterne sikrer, at lagring af oplysninger eller opnåelse af adgang til oplysninger, der allerede er lagret i en abonnents eller brugers terminaludstyr, kun er tilladt på betingelse af, at abonnenten eller brugeren har givet sit samtykke hertil efter i overensstemmelse med direktiv [95/46] at have modtaget klare og fyldestgørende oplysninger, bl.a. om formålet med behandlingen. Dette er ikke til hinder for teknisk lagring eller adgang til oplysninger, hvis det alene sker med det formål at overføre kommunikation via et elektronisk kommunikationsnet eller er absolut påkrævet for at sætte udbyderen af en informationssamfundstjeneste, som abonnenten eller brugeren udtrykkelig har anmodet om, i stand til at levere denne tjeneste.«

9 Artikel 6 i direktiv 2002/58 med overskriften »Trafikdata« bestemmer:

»1. Trafikdata vedrørende abonnenter og brugere, som behandles og lagres af udbyderen af et offentligt kommunikationsnet eller en offentligt tilgængelig elektronisk kommunikationstjeneste, skal slettes eller gøres anonyme, når de ikke længere er nødvendige for fremføringen af kommunikationen, jf. dog stk. 2, 3 og 5, samt artikel 15, stk. 1.

2. Med henblik på debitering af abonnenten og afregning for samtrafik er det tilladt at behandle trafikdata. En sådan behandling er tilladt indtil udløbet af den lovbestemte forældelsesfrist for sådanne gældsforpligtelser eller fristen for anfægtelse af sådanne afregninger.

3. Med henblik på markedsføring af elektroniske kommunikationstjenester eller levering af værdiforøgende tjenester er det tilladt udbyderen af en offentligt tilgængelig elektronisk kommunikationstjeneste at behandle de i stk. 1 omtalte oplysninger i det omfang og tidsrum, som sådanne tjenester eller markedsføringen kræver, hvis den abonnent eller bruger, som oplysningerne vedrører, forudgående har givet sit samtykke hertil. Brugeren eller abonnenten skal på et hvilket som helst tidspunkt have mulighed for at trække sit samtykke til behandling af trafikdata tilbage.

[…]

5. Behandling af trafikdata i henhold til stk. 1, 2, 3 og 4 må kun foretages af personer, som handler efter bemyndigelse fra udbydere af de offentligt tilgængelige kommunikationsnet og -tjenester, og som er beskæftiget med debitering eller trafikstyring, kundeforespørgsler, afsløring af svig, markedsføring af elektroniske kommunikationstjenester eller levering af en tillægstjeneste, og skal begrænses til det for sådanne aktiviteter nødvendige.«

10 Dette direktivs artikel 9 med overskriften »Lokaliseringsdata, bortset fra trafikdata« bestemmer i stk. 1:

»Hvis lokaliseringsdata, bortset fra trafikdata, vedrørende brugere af eller abonnenter på de offentlige kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester, kan behandles, må disse data kun behandles, når de er gjort anonyme, eller når brugeren eller abonnenten har givet sit samtykke hertil, og da kun i det omfang og i det tidsrum, som er nødvendigt for levering af en tillægstjeneste. Tjenesteudbyderen skal, inden brugernes eller abonnenternes samtykke indhentes, underrette dem om, hvilken type lokaliseringsdata, bortset fra trafikdata, der behandles, hvorfor og hvor længe de behandles, og om de videregives til en tredjemand med henblik på levering af tillægstjenesten. […]«

11 Det nævnte direktivs artikel 15 med overskriften »Anvendelsesområdet for visse bestemmelser i direktiv [95/46]« fastsætter i stk. 1:

»Medlemsstaterne kan vedtage retsforskrifter med henblik på at indskrænke rækkevidden af de rettigheder og forpligtelser, der omhandles i artikel 5, artikel 6, artikel 8, stk. 1, 2, 3 og 4, og artikel 9, hvis en sådan indskrænkning er nødvendig, passende og forholdsmæssig i et demokratisk samfund af hensyn til den nationale sikkerhed (dvs. statens sikkerhed), forsvaret, den offentlige sikkerhed, eller forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager eller uautoriseret brug af det elektroniske kommunikationssystem efter artikel 13, stk. 1, i direktiv [95/46]. Med henblik herpå kan medlemsstaterne bl.a. vedtage retsforskrifter om lagring af data i en begrænset periode, som kan begrundes i et af de hensyn, der er nævnt i dette stykke. Alle i dette stykke omhandlede forskrifter skal være i overensstemmelse med [EU-]rettens generelle principper, herunder principperne i EU-traktatens artikel 6, stk. 1 og 2.«

Forordning 2016/679

12 Artikel 2 i forordning 2016/679 bestemmer følgende:

»1. Denne forordning finder anvendelse på behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling, og på anden ikkeautomatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

2. Denne forordning gælder ikke for behandling af personoplysninger:

a) under udøvelse af aktiviteter, der falder uden for EU-retten

b) som foretages af medlemsstaterne, når de udfører aktiviteter, der falder inden for rammerne af afsnit V, kapitel 2, i TEU

[…]

d) som foretages af kompetente myndigheder med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod og forebygge trusler mod den offentlige sikkerhed.

[…]«

13 Denne forordnings artikel 4 fastsætter følgende:

»I denne forordning forstås ved:

[…]

2) »behandling«: enhver aktivitet eller række af aktiviteter – med eller uden brug af automatisk behandling – som personoplysninger eller en samling af personoplysninger gøres til genstand for, f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse

[…]«

14 Følgende fremgår af samme forordnings artikel 23, stk. 1:

»EU-ret eller medlemsstaternes nationale ret, som den dataansvarlige eller databehandleren er underlagt, kan ved lovgivningsmæssige foranstaltninger begrænse rækkevidden af de forpligtelser og rettigheder, der er omhandlet i artikel 12-22 og 34 samt artikel 5, for så vidt bestemmelserne heri svarer til rettighederne og forpligtelserne i artikel 12-22, når en sådan begrænsning respekterer det væsentligste indhold af de grundlæggende rettigheder og frihedsrettigheder og er en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund af hensyn til:

a) statens sikkerhed

b) forsvaret

c) den offentlige sikkerhed

d) forebyggelse, efterforskning, afsløring eller retsforfølgning af strafbare handlinger eller fuldbyrdelse af strafferetlige sanktioner, herunder beskyttelse mod og forebyggelse af trusler mod den offentlige sikkerhed

e) andre vigtige målsætninger i forbindelse med beskyttelse af Unionens eller en medlemsstats generelle samfundsinteresser, navnlig Unionens eller en medlemsstats væsentlige økonomiske eller finansielle interesser, herunder valuta-, budget- og skatteanliggender, folkesundhed og social sikkerhed

f) beskyttelse af retsvæsenets uafhængighed og retssager

g) forebyggelse, efterforskning, afsløring og retsforfølgning i forbindelse med brud på etiske regler for lovregulerede erhverv

h) kontrol-, tilsyns- eller reguleringsfunktioner, herunder opgaver af midlertidig karakter, der er forbundet med offentlig myndighedsudøvelse i de tilfælde, der er omhandlet i litra a)-e) og g)

i) beskyttelse af den registrerede eller andres rettigheder og frihedsrettigheder

j) håndhævelse af civilretlige krav.«

15 Følgende er fastsat i artikel 94, stk. 2, i forordning 2016/679:

»Henvisninger til det ophævede direktiv gælder som henvisninger til denne forordning. Henvisninger til Gruppen vedrørende Beskyttelse af Personer i forbindelse med Behandling af Personoplysninger, der er nedsat ved artikel 29 i direktiv [95/46], gælder som henvisninger til Det Europæiske Databeskyttelsesråd oprettet ved denne forordning.«

Det Forenede Kongeriges lovgivning

16 Section 94 i Telecommunications Act 1984 (lov af 1984 om telekommunikation) i den affattelse, der finder anvendelse på tvisten i hovedsagen (herefter »lov af 1984«), med overskriften »Påbud af hensyn til den nationale sikkerhed osv.« bestemmer:

»(1) Ministeren kan efter høring af en person, der er omfattet af denne section, udstede generelle påbud til den pågældende, i det omfang det efter ministerens opfattelse er nødvendigt af hensyn til den nationale sikkerhed eller af hensyn til forbindelserne med regeringen i et land eller territorium uden for Det Forenede Kongerige.

(2) Såfremt ministeren finder det nødvendigt af hensyn til den nationale sikkerhed eller af hensyn til forbindelserne med regeringen i et land eller territorium beliggende uden for Det Forenede Kongerige, kan ministeren efter høring af en person, som denne section finder anvendelse på, udstede påbud (efter omstændighederne i det konkrete tilfælde) til denne person om at udføre eller undlade at udføre en bestemt handling, der beskrives nærmere i påbuddene.

(2A) Ministeren kan kun udstede påbud i henhold til subsection (1) eller (2), hvis ministeren finder, at den adfærd, der kræves i henhold til påbuddene, står i rimeligt forhold til det mål, der skal nås ved denne adfærd.

(3) Den person, som denne section finder anvendelse på, skal gennemføre alle de påbud, som ministeren udsteder til den pågældende i henhold til denne section, uanset de eventuelle andre forpligtelser, der påhviler den pågældende i henhold til Part 1 eller Chapter 1 i Part 2 i Communications Act 2003 [(lov af 2003 om kommunikation)], og i tilfælde af påbud til en udbyder af et offentligt elektronisk kommunikationsnet, selv om påbuddene finder anvendelse på den pågældende i medfør af en anden egenskab end udbyder af adgang til et sådant net.

(4) Ministeren indleverer til hvert parlamentskammer en kopi af eventuelle påbud, der er udstedt i medfør af denne artikel, medmindre en offentliggørelse af de nævnte påbud efter ministerens opfattelse strider mod de nationale sikkerhedsinteresser eller mod forbindelserne med regeringen i et land eller territorium beliggende uden for Det Forenede Kongerige eller en persons forretningsmæssige interesser.

(5) En person må ikke videregive eller i henhold til en lov eller på anden vis pålægges at videregive oplysninger om foranstaltninger, der er truffet i henhold til denne section, hvis ministeren har meddelt vedkommende, at videregivelse af disse oplysninger efter ministerens opfattelse strider mod de nationale sikkerhedsinteresser eller mod forbindelserne med regeringen i et land eller territorium beliggende uden for Det Forenede Kongerige eller en persons forretningsmæssige interesser.

[…]

(8) Denne section finder anvendelse på Office of communications [(telekommunikationsmyndighed, OFCOM)] og udbydere af offentlige elektroniske kommunikationsnet.«

17 Section 21 (4) og (6) i Regulation of Investigatory Powers Act 2000 (lov af 2000 om efterforskningsbeføjelser, herefter »RIPA«) bestemmer:

»(4) [V]ed »kommunikationsdata« forstås enhver af følgende:

(a) trafikdata indeholdt i eller vedføjet en kommunikation (enten af afsenderen eller på anden måde) i forbindelse med enhver posttjeneste eller ethvert telekommunikationssystem, hvorved den fremføres eller kan fremføres

(b) oplysninger, som ikke omfatter noget af indholdet af en kommunikation (bortset fra oplysninger, der er omfattet af paragraph (a)) og vedrører anvendelsen fra en persons side:
(i) af enhver posttjeneste eller telekommunikationstjeneste eller
(ii) i forbindelse med levering til en person eller en persons anvendelse af en telekommunikationstjeneste, af en del af et telekommunikationssystem

(c) oplysninger, der ikke er omfattet af paragraph (a) eller (b), og som en person, der leverer en posttjeneste eller telekommunikationstjeneste, har registreret eller indsamlet om personer, som tjenesten leveres til.

[…]

(6) [Ved]»trafikdata« i forbindelse med enhver kommunikation forstås:

(a) alle data, der identificerer eller kan identificere enhver person, anordning eller lokalisering, hvorfra en kommunikation overføres eller kan overføres

(b) data, der identificerer eller udpeger eller kan identificere eller udpege det udstyr, hvorfra en kommunikation overføres eller kan overføres

(c) alle data, der indeholder signaler til aktivering af den anvendte anordning i et kommunikationssystem med henblik på overføring af enhver kommunikation, og

(d) alle data, der identificerer data, der er indeholdt i eller ledsager en specifik kommunikation, eller andre data, for så vidt som de er indeholdt i eller ledsager en specifik kommunikation.

[…]«

18 RIPA's section 65-69 fastsætter reglerne om Investigatory Powers Tribunals (domstol for efterforskningsbeføjelser, Det Forenede Kongerige) virksomhed og kompetencer. I henhold til RIPA's section 65 kan der indgives klage til denne domstol, hvis der er grund til at antage, at data er blevet indsamlet med urette.

Tvisten i hovedsagen og de præjudicielle spørgsmål

19 I begyndelsen af 2015 blev oplysninger om den praksis, som Det Forenede Kongeriges forskellige sikkerheds- og efterretningstjenester, dvs. GCHQ, MI5 og MI6, fulgte med hensyn til indsamling og brug af bulk-kommunikationsdata, offentliggjort bl.a. i en rapport fra Intelligence and Security Committee of Parliament (Parlamentets efterretnings- og sikkerhedsudvalg, Det Forenede Kongerige).

Den 5. juni 2015 anlagde den ikke-statslige organisation Privacy International sag ved Investigatory Powers Tribunal (domstol for efterforskningsbeføjelser, Det Forenede Kongerige) mod Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Departement samt de nævnte sikkerheds- og efterretningstjenester, idet denne organisation anfægtede lovligheden af denne praksis.

20 Den forelæggende ret undersøgte lovligheden af den nævnte praksis i første omgang på grundlag af national ret og bestemmelserne i den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder, undertegnet i Rom den 4. november 1950 (herefter »EMRK«), og derefter EU-retten. I dom af 17. oktober 2016 fastslog denne ret, at de sagsøgte i hovedsagen havde anerkendt, at de nævnte sikkerheds- og efterretningstjenester i forbindelse med deres virksomhed havde indsamlet og anvendt samlinger af oplysninger om privatpersoner i forskellige kategorier (*bulk personal data*), såsom biografiske oplysninger eller oplysninger vedrørende rejser, finansielle eller kommercielle oplysninger, oplysninger i forbindelse med kommunikation, som kan indeholde følsomme oplysninger, der er omfattet af tavshedspligt, eller journalistisk materiale. Disse oplysninger, der var blevet indsamlet på forskellige – eventuelt hemmelige – måder, var blevet analyseret ved krydstjek og ved hjælp af automatiserede behandlinger, var blevet videregivet til andre personer og myndigheder og var blevet delt med udenlandske partnere. I denne forbindelse havde sikkerheds- og efterretningstjenesterne ligeledes anvendt bulk-kommunikationsdata, der var indsamlet hos udbydere af offentlige elektroniske kommunikationsnet, navnlig i henhold til ministerielle instrukser vedtaget på grundlag af section 94 i lov af 1984. GCHQ og MI5 havde anvendt denne fremgangsmåde siden henholdsvis 2001 og 2005.

21 Den nævnte ret fandt, at disse foranstaltninger med henblik på indsamling og brug af oplysninger var i overensstemmelse med national ret, og at disse foranstaltninger siden 2015 med forbehold af de endnu ikke undersøgte spørgsmål om forholdsmæssigheden af de nævnte foranstaltninger og om videregivelse af oplysninger til tredjeparter, havde været i overensstemmelse med EMRK's artikel 8. I sidstnævnte henseende præciserede den forelæggende ret, at den havde fået forelagt beviser vedrørende de gældende garantier, bl.a. for så vidt angår procedurerne for adgang og videregivelse uden for sikkerheds- og efterretningstjenesterne, metoderne for lagring af oplysninger og eksistensen af uafhængige kontroller.

22 Hvad angår lovligheden af de i hovedsagen omhandlede foranstaltninger med henblik på indsamling og brug i forhold til EU-retten undersøgte den forelæggende ret i dom af 8. september 2017, om disse foranstaltninger var omfattet af EU-rettens anvendelsesområde, og i bekræftende fald, om de var forenelige med EU-retten. Denne ret fastslog for så vidt angår bulk-kommunikationsdata, at udbydere af elektroniske kommunikationsnet i henhold til section 94 i lov af 1984 i tilfælde af et påbud fra en minister var forpligtet til at udlevere de data, der var indsamlet i forbindelse med deres økonomiske virksomhed, der var omfattet af EU-retten, til sikkerheds- og efterretningstjenesterne. Dette var derimod ikke tilfældet for så vidt angår indsamlingen af andre data, der blev indsamlet af disse tjenester uden at gøre brug af sådanne bindende beføjelser. På grundlag af denne konstatering har den forelæggende ret fundet det nødvendigt at forelægge Domstolen en række spørgsmål med henblik på at få fastslået, om en ordning som den, der følger af denne section 94, er omfattet af EU-retten, og i bekræftende fald, om og i givet fald på hvilken måde kravene ifølge den retspraksis, der følger af dom af 21. december 2016, Tele2 Sverige og Watson m.fl. (C-203/15 og C-698/15, herefter »Tele2-dommen«, EU:C:2016:970), finder anvendelse på denne ordning.

23 I denne henseende har den forelæggende ret i anmodningen om præjudiciel afgørelse anført, at en minister i henhold til den nævnte section 94 kan udstede generelle eller specifikke påbud til udbydere af elektroniske kommunikationstjenester, hvis sådanne påbud efter ministerens opfattelse er nødvendige af hensyn til den nationale sikkerhed eller forbindelserne til en udenlandsk regering. Denne ret har under henvisning til definitionerne i RIPA's section 21 (4) og (6), præciseret, at de omhandlede data omfatter trafikdata og oplysninger om de anvendte tjenester som omhandlet i denne sidstnævnte bestemmelse, idet kun indholdet af kommunikationen er udelukket. Disse data og

oplysninger gør det navnlig muligt at få kendskab til, »hvem, hvor, hvornår og hvordan« en kommunikation finder sted. De nævnte data videregives til sikkerheds- og efterretningstjenesterne og lagres af disse i forbindelse med deres aktiviteter.

24 Ifølge den forelæggende ret adskiller den i hovedsagen omhandlede ordning sig fra den, der følger af Data Retention and Investigatory Powers Act 2014 (lov af 2014 om lagring af data og undersøgelsesbeføjelser), der var omhandlet i den sag, som gav anledning til dom af 21. december 2016, Tele2 (C-203/15 og C-698/15, EU:C:2016:970), eftersom det med sidstnævnte ordning blev fastsat, at udbydere af elektroniske kommunikationstjenester skulle lagre data og stille dem til rådighed ikke blot for sikkerheds- og efterretningstjenester af hensyn til den nationale sikkerhed, men ligeledes andre offentlige myndigheder på baggrund af deres behov. Denne dom vedrørte i øvrigt en strafferetlig efterforskning og ikke den nationale sikkerhed.

25 Den forelæggende ret har tilføjet, at sikkerheds- og efterretningstjenesternes databaser er genstand for en automatiseret og ikke-specifik massebehandling med henblik på at afsløre, om der foreligger eventuelle ukendte trusler. I denne forbindelse har den nævnte ret anført, at de således oprettede metadatasæt bør være så fuldstændige som muligt, således at man skal lede i en »høstak« for at finde den deri skjulte »nål«. Hvad angår nytten af de nævnte tjenesters indsamling af massedata og af mulighederne for søgning i disse oplysninger har den forelæggende ret navnlig henvist til konklusionerne i den rapport, der blev udarbejdet den 19. august 2016 af David Anderson, QC, som var den daværende United Kingdom Independent Reviewer of Terrorism Legislation (Det Forenede Kongeriges uafhængige tilsynsførende i forbindelse med terrorlovgivningen), som med henblik på udarbejdelsen af denne rapport støttede sig på en undersøgelse foretaget af et hold efterretningsspecialister og på vidneforklaringer fra ansatte i sikkerheds- og efterretningstjenesterne.

26 Den forelæggende ret har endvidere præciseret, at den i hovedsagen omhandlede ordning ifølge Privacy International er ulovlig i henhold til EU-retten, mens de sagsøgte i hovedsagen er af den opfattelse, at den i henhold til denne ordning fastsatte forpligtelse til at foretage overføring af data, adgangen til disse data samt brugen heraf ikke er omfattet af Den Europæiske Unions kompetencer i overensstemmelse med bl.a. artikel 4, stk. 2, TEU, hvorefter den nationale sikkerhed forbliver den enkelte medlemsstats eneansvar.

27 I denne henseende har den forelæggende ret med henvisning til dom af 30. maj 2006, Parlamentet mod Rådet og Kommissionen (C-317/04 og C-318/04, EU:C:2006:346, præmis 56-59), der vedrørte videregivelse af PNR-oplysninger (*Passenger Name Record*) med henblik på at beskytte den offentlige sikkerhed, fundet, at handelsselskabers aktiviteter i forbindelse med behandling og videregivelse af data med henblik på at beskytte den nationale sikkerhed ikke forekommer at være omfattet af EU-rettens anvendelsesområde. Det skal ikke undersøges, om den omhandlede aktivitet udgør databehandling, men kun, om formålet med en sådan aktivitet efter sit indhold og virkninger er at støtte en central statslig funktion som omhandlet i artikel 4, stk. 2, TEU inden for en ramme, der af de offentlige myndigheder er fastlagt med hensyn til den offentlige sikkerhed.

28 Såfremt de i hovedsagen omhandlede foranstaltninger ikke desto mindre er omfattet af EU-retten, er den forelæggende ret af den opfattelse, at kravene i præmis 119-125 i dom af 21. december 2016, Tele2 (C-203/15 og C-698/15, EU:C:2016:970), forekommer irrelevante i forbindelse med den nationale sikkerhed og kan hindre sikkerheds- og efterretningstjenesternes evne til at begrænse visse trusler mod den nationale sikkerhed.

29 På denne baggrund har Investigatory Powers Tribunal (domstol for efterforskningsbeføjelser) besluttet at udsætte sagen og at forelægge Domstolen følgende præjudicielle spørgsmål:

»I en situation, hvor

a) [sikkerheds- og efterretningstjenesterne]s mulighed for at bruge [bulk-kommunikationsdata] indgivet til [disse tjenester] er afgørende for beskyttelsen af den nationale sikkerhed i Det Forenede Kongerige, herunder som led i bekæmpelse af terrorisme, kontraspionage og bekæmpelse af spredningen af atomvåben

b) et grundlæggende formål med sikkerheds- og efterretnings[tjenesternes] brug af [bulk-kommunikationsdata] er at afdække hidtil ukendte trusler mod den nationale sikkerhed ved hjælp af ikkemålrettede bulk-teknikker, der afhænger af, at [bulk-kommunikationsdata] er samlet på ét sted, idet dataene primært bidrager til hurtig identifikation og udvikling af mål og danner grundlag for handling i tilfælde af overhængende fare, idet dataene primært bidrager til hurtig identifikation og udvikling af mål og danner grundlag for handling i tilfælde af overhængende fare

c) udbyderen af et elektronisk kommunikationsnet[…] ikke efterfølgende er forpligtet til at lagre [bulk-kommunikationsdata] (efter det tidsrum, der stilles krav om i forbindelse med deres almindelige virksomhed), som opbevares af de offentlige myndigheder (sikkerheds- og efterretnings[tjenesterne]) alene

d) den nationale domstol (med nogle få forbehold) har fastslået, at de sikkerhedsforanstaltninger, der er forbundet med sikkerheds- og efterretnings[tjenesternes] brug af [bulk-kommunikationsdata], er i overensstemmelse med kravene i EMRK, og

e) den nationale domstol har fastslået, at fastsættelsen af de krav, der fremgår af præmis 119-125 i dom [af 21. december 2016, Tele2 (C-203/15 og C-698/15 (EU:C:2016:970)], i givet fald ville begrænse de foranstaltninger, som [sikkerheds- og efterretningstjenesterne] træffer for at beskytte den nationale sikkerhed, og dermed bringe Det Forenede Kongeriges nationale sikkerhed i fare

1) og idet der henvises til artikel 4 TEU og artikel 1, stk. 3, i direktiv [2002/58], gælder det da, at et krav i en afgørelse truffet af en [minister] om, at en udbyder af et elektronisk kommunikationsnet[…] skal udlevere bulk-kommunikationsdata til en medlemsstats sikkerheds- og efterretnings[tjenester], er omfattet af EU-retten og [direktiv 2002/58]?

2) Hvis [det] første spørgsmål besvares bekræftende: Finder nogen af [de krav, der gælder for lagrede kommunikationsdata, og som fremgår af præmis 119-125 i dom af 21. december 2016, Tele2 (C-203/15 og C-698/15 (EU:C:2016:970)] eller eventuelle andre krav ud over kravene i EMRK, anvendelse på en sådan afgørelse truffet af en [minister]? Hvis det er tilfældet, hvordan og i hvilket omfang finder de pågældende krav da anvendelse, idet der tages højde for, at det er tvingende nødvendigt, at sikkerheds- og efterretnings[tjenesterne] kan indsamle bulk-kommunikationsdata og bruge automatiserede behandlingsteknikker for at beskytte den nationale sikkerhed, og for, i hvor høj grad denne mulighed, såfremt den i øvrigt er i overensstemmelse med EMRK, risikerer at blive begrænset i kritisk omfang ved indførelsen af sådanne krav?«

De præjudicielle spørgsmål

Det første spørgsmål

30 Med det første spørgsmål ønsker den forelæggende ret nærmere bestemt oplyst, om artikel 1, stk. 3, i direktiv 2002/58, sammenholdt med artikel 4, stk. 2, TEU, skal fortolkes således, at en national lovgivning, hvorefter en statslig myndighed kan pålægge udbydere af elektroniske kommunikationstjenester at overføre trafikdata og lokaliseringsdata til sikkerheds- og efterretningstjenesterne med henblik på at beskytte den nationale sikkerhed, er omfattet af dette direktivs anvendelsesområde.

31 I denne henseende har Privacy International i det væsentlige anført, at henset til den lære, som kan drages af Domstolens praksis vedrørende anvendelsesområdet for direktiv 2002/58, er både sikkerheds- og efterretningstjenesternes indsamling af data hos disse udbydere i henhold til section 94 i lov af 1984, og de nævnte tjenesters anvendelse heraf omfattet af dette direktivs anvendelsesområde, uanset om de nævnte oplysninger indsamles ved overføring med forsinkelse eller i realtid. Navnlig det forhold, at formålet om beskyttelse af den nationale sikkerhed udtrykkeligt er anført i det nævnte direktivs artikel 15, stk. 1, indebærer ikke, at dette direktiv ikke finder anvendelse på sådanne situationer, og artikel 4, stk. 2, TEU påvirker ikke denne bedømmelse.

32 Det Forenede Kongeriges regering, den tjekkiske og den estiske regering, Irland samt den franske, den cypriotiske, den ungarske, den polske og den svenske regering har derimod i det væsentlige gjort gældende, at direktiv 2002/58 ikke finder anvendelse på den i hovedsagen omhandlede nationale lovgivning, for så vidt som denne lovgivning har til formål at beskytte den nationale sikkerhed. Efterretningstjenesternes aktiviteter henhører under medlemsstaternes centrale funktioner vedrørende opretholdelse af lov og orden samt beskyttelse af den interne sikkerhed og den territoriale integritet, og dermed under medlemsstaternes enekompetence, således som det bl.a. fremgår af artikel 4, stk. 2, tredje punktum, TEU.

33 Ifølge disse regeringer kan direktiv 2002/58 derfor ikke fortolkes således, at nationale foranstaltninger til beskyttelse af den nationale sikkerhed er omfattet af dets anvendelsesområde. Dette direktivs artikel 1, stk. 3, afgrænser dette anvendelsesområde og udelukker i lighed med, hvad der allerede fremgik af artikel 3, stk. 2, første led, i direktiv 95/46, de aktiviteter, der vedrører den offentlige sikkerhed, forsvaret og statens sikkerhed herfra. Disse bestemmelser afspejler den i artikel 4, stk. 2, TEU, fastsatte kompetencefordeling, og ville miste deres effektive virkning, hvis foranstaltninger vedrørende beskyttelse af den nationale sikkerhed skulle overholde kravene i direktiv 2002/58. I øvrigt kan den praksis fra Domstolen, der følger af dom af 30. maj 2006, Parlamentet mod Rådet og Kommissionen (C-317/04 og C-318/04, EU:C:2006:346), og som vedrørte artikel 3, stk. 2, første led, i direktiv 95/46, overføres på artikel 1, stk. 3, i direktiv 2002/58.

34 Det skal i denne henseende bemærkes, at det af artikel 1, stk. 1, i direktiv 2002/58 fremgår, at dette direktiv bl.a. tager sigte på en harmonisering af nationale bestemmelser, der er nødvendig for at sikre et ensartet niveau i beskyttelsen af de grundlæggende rettigheder og frihedsrettigheder og navnlig retten til privatliv og fortrolighed i forbindelse med behandling af personoplysninger inden for den elektroniske kommunikationssektor.

35 Dette direktivs artikel 1, stk. 3, udelukker fra sit anvendelsesområde »statens aktiviteter« på de områder, som er nævnt deri, herunder statens aktiviteter på det strafferetlige område og aktiviteter, der vedrører den offentlige sikkerhed, forsvaret, statens sikkerhed, herunder statens økonomiske interesser, når disse aktiviteter er forbundet med spørgsmål vedrørende statens sikkerhed. De aktiviteter, der er nævnt som eksempler heri, er under alle omstændigheder statens eller statslige myndigheders aktiviteter, der ikke har noget at gøre med området for den enkelte borgers aktiviteter (dom af 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, præmis 32 og den deri nævnte retspraksis).

36 Det fremgår endvidere af artikel 3 i direktiv 2002/58, at dette direktiv finder anvendelse på behandling af personoplysninger i forbindelse med, at offentligt tilgængelige elektroniske kommunikationstjenester stilles til rådighed via offentlige kommunikationsnet i Unionen, herunder offentlige kommunikationsnet med dataindsamlings- og identifikationsudstyr (herefter »de elektroniske kommunikationstjenester«). Det nævnte direktiv skal derfor anses for at regulere den virksomhed, som udbydere af sådanne tjenester udøver (dom af 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, præmis 33 og den deri nævnte retspraksis).

37 I denne henseende gør artikel 15, stk. 1, i direktiv 2002/58 det muligt for medlemsstaterne under iagttagelse af de i direktivet fastsatte betingelser at vedtage »retsforskrifter med henblik på at indskrænke rækkevidden af de rettigheder og forpligtelser, der omhandles i [dette direktivs] artikel 5, artikel 6, artikel 8, stk. 1, 2, 3 og 4, og artikel 9« (dom af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 71).

38 Artikel 15, stk. 1, i direktiv 2002/58 forudsætter imidlertid nødvendigvis, at de heri omhandlede nationale retsforskrifter er omfattet af det nævnte direktivs anvendelsesområde, idet det af direktivet udtrykkeligt fremgår, at medlemsstaterne kun må vedtage sådanne retsforskrifter under iagttagelse af de i direktivet fastsatte betingelser. Sådanne retsforskrifter regulerer desuden med de i bestemmelsen fastsatte formål for øje den virksomhed, som udøves af udbydere af elektroniske kommunikationstjenester (dom af 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, præmis 34 og den deri nævnte retspraksis).

39 Domstolen fastslog bl.a. ud fra disse betragtninger, at artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med dette direktivs artikel 3, skal fortolkes således, at det ikke kun er en retsforskrift, der pålægger udbyderne af elektroniske kommunikationstjenester at lagre trafikdata og lokaliseringsdata, der er omfattet af dette direktivs anvendelsesområde, men også en retsforskrift, der pålægger disse udbydere at give de kompetente nationale myndigheder adgang til disse data. Sådanne retsforskrifter indebærer nemlig nødvendigvis, at de nævnte udbydere behandler de nævnte oplysninger, og kan, for så vidt som de regulerer de nævnte udbyderes virksomhed, ikke sidestilles med statens aktiviteter, der er omfattet af det nævnte direktivs artikel 1, stk. 3 (jf. i denne retning dom af 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, præmis 35 og 37 og den deri nævnte retspraksis).

40 For så vidt angår en retsforskrift som section 94 i lov af 1984, på grundlag af hvilken den kompetente myndighed kan pålægge udbydere af elektroniske kommunikationstjenester et påbud om at videregive massedata ved overføring til sikkerheds- og efterretningstjenesterne, skal det bemærkes, at begrebet »behandling af personoplysninger« i henhold til definitionen i artikel 4, nr. 2), i forordning 2016/679, der finder anvendelse i medfør af artikel 2 i direktiv 2002/58, sammenholdt med den nævnte forordnings artikel 94, stk. 2, omfatter »enhver aktivitet eller række af aktiviteter – med eller uden brug af automatisk behandling – som personoplysninger eller en samling af personoplysninger gøres til genstand for, f.eks. indsamling, […] opbevaring, […] søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse […]«.

41 Det følger heraf, at videregivelse af personoplysninger ved transmission, ligesom opbevaring af oplysninger eller enhver anden form for overladelse, udgør en behandling som omhandlet i artikel 3 i direktiv 2002/58, og følgelig henhører under dette direktivs anvendelsesområde (jf. i denne retning dom af 29.1.2008, Promusicae, C-275/06, EU:C:2008:54, præmis 45).

42 Henset til de betragtninger, der fremgår af denne doms præmis 38, og til den generelle opbygning af direktiv 2002/58 ville en fortolkning af dette direktiv, hvorefter de retsforskrifter, der er nævnt i dets artikel 15, stk. 1, er udelukket fra det nævnte direktivs anvendelsesområde som følge af, at de formål, som sådanne retsforskrifter skal opfylde, i det væsentlige kan sammenholdes med de formål, der forfølges med de i dette samme direktivs artikel 1, stk. 3, omhandlede aktiviteter, endvidere fratage denne artikel 15, stk. 1, enhver effektiv virkning (jf. i denne retning dom af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 72 og 73).

43 Begrebet »aktiviteter«, der er anvendt i artikel 1, stk. 3, i direktiv 2002/58, kan, således som generaladvokaten i det væsentlige har anført i punkt 75 i forslag til afgørelse La Quadrature du Net m.fl. (C-511/18 og C-512/18, EU:C:2020:6), hvortil generaladvokaten har henvist i punkt 24 i forslaget til afgørelse i den foreliggende sag, derfor ikke fortolkes således, at det omfatter de retsforskrifter, der er omhandlet i dette direktivs artikel 15, stk. 1.

44 Artikel 4, stk. 2, TEU, som de regeringer, der er nævnt i denne doms præmis 32, har henvist til, kan ikke rejse tvivl om denne konklusion. Det fremgår nemlig af Domstolens faste praksis, at selv om det tilkommer medlemsstaterne at fastsætte deres væsentlige sikkerhedsinteresser og at træffe de nødvendige foranstaltninger til at opretholde deres indre og ydre sikkerhed, kan alene den omstændighed, at en national foranstaltning er blevet truffet med henblik på at beskytte den nationale sikkerhed, ikke medføre, at EU-retten ikke finder anvendelse, og fritage medlemsstaterne fra at sikre den nødvendige overholdelse af denne ret (jf. i denne retning dom af 4.6.2013, ZZ, C-300/11, EU:C:2013:363, præmis 38 og den deri nævnte retspraksis, af 20.3.2018, Kommissionen mod Østrig (Statstrykkeri), C-187/16, EU:C:2018:194, præmis 75 og 76, og af 2.4.2020, Kommissionen mod Polen, Ungarn og Den Tjekkiske Republik (Midlertidig flytningsordning for ansøgere om international beskyttelse), C-715/17, C-718/17 og C-719/17, EU:C:2020:257, præmis 143 og 170).

45 Det er korrekt, at Domstolen i dom af 30. maj 2006, Parlamentet mod Rådet og Kommissionen (C-317/04 og C-318/04, EU:C:2006:346, præmis 56-59), fastslog, at luftfartsselskabers videregivelse af personoplysninger til offentlige myndigheder i et tredjeland med henblik på at forebygge og bekæmpe terrorisme og andre alvorlige forbrydelser i henhold til artikel 3, stk. 2, første led, i direktiv 95/46 ikke var omfattet af dette direktivs anvendelsesområde, eftersom denne en sådan videregivelse skete inden for rammer, der var indført af de offentlige myndigheder, og som vedrørte den offentlige sikkerhed.

46 Henset til de betragtninger, der fremgår af denne doms præmis 36, 38 og 39, kan denne retspraksis imidlertid ikke overføres på fortolkningen af artikel 1, stk. 3, i direktiv 2002/58. Således som generaladvokaten i det væsentlige har anført i punkt 70-72 i forslag til afgørelse La Quadrature du Net m.fl. (C-511/18 og C-512/18, EU:C:2020:6), udelukkede artikel 3, stk. 2, første led, i direktiv 95/46, som den nævnte retspraksis omhandlede, nemlig generelt »behandling, der vedrører den offentlige sikkerhed, forsvar, statens sikkerhed«, fra dette sidstnævnte direktivs anvendelsesområde, uden at foretage en sondring ud fra, hvem der havde behandlet de pågældende data. Det er i forbindelse med fortolkningen af artikel 1, stk. 3, i direktiv 2002/58, til gengæld nødvendigt at foretage en sådan sondring. Som det fremgår af denne doms præmis 37-39 og 42, henhører al behandling af personoplysninger, der foretages af udbydere af elektroniske kommunikationstjenester, nemlig under det nævnte direktivs anvendelsesområde, herunder de behandlinger, der følger af de forpligtelser, som disse udbydere er pålagt af de offentlige myndigheder, selv om disse sidstnævnte behandlinger i givet fald kunne være omfattet af anvendelsesområdet for den undtagelse, der er fastsat i artikel 3, stk. 2, første led, i direktiv 95/46, som følge af den bredere formulering af denne bestemmelse, der omhandler alle behandlinger, uanset hvem der foretager dem, og som vedrører den offentlige sikkerhed, forsvaret eller statens sikkerhed.

47 Det skal i øvrigt bemærkes, at direktiv 95/46, der var genstand for den sag, der gav anledning til dom af 30. maj 2006, Parlamentet mod Rådet og Kommissionen (C-317/04 og C-318/04, EU:C:2006:346), i henhold til artikel 94, stk. 1, i forordning 2016/679 blev ophævet og erstattet af denne sidstnævnte forordning med virkning fra den 25. maj 2018. Selv om det af den nævnte forordnings artikel 2, stk. 2, litra d), fremgår, at denne forordning ikke gælder for behandlinger, som foretages af »kompetente myndigheder« med henblik på bl.a. at forebygge og afsløre strafbare handlinger, herunder beskytte og forebygge trusler mod den offentlige sikkerhed, fremgår det af samme forordnings artikel 23, stk. 1, litra d) og h), at behandling af personoplysninger, der af privatpersoner foretages med henblik på de samme formål, er omfattet af forordningens anvendelsesområde. Det følger heraf, at den ovenfor anførte fortolkning af artikel 1, stk. 3, artikel 3 og artikel 15, stk. 1, i direktiv 2002/58 er i overensstemmelse med den afgrænsning af anvendelsesområdet for forordning 2016/679, som dette direktiv supplerer og præciserer.

48 Når medlemsstaterne direkte vedtager foranstaltninger, der fraviger kravet om fortrolighed i forbindelse med elektronisk kommunikation uden at pålægge de udbydere, der tilbyder denne form for kommunikation, behandlingsforpligtelser, henhører beskyttelsen af de pågældende personoplysninger til gengæld ikke under direktiv 2002/58, men udelukkende under national ret, dog med forbehold af anvendelsen af Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse

af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA (EUT 2016, L 119, s. 89), hvilket indebærer, at de omhandlede foranstaltninger skal overholde bl.a. de nationale regler, der har forfatningsrang, og de krav, der følger af EMRK.

49 Henset til ovenstående betragtninger skal det første spørgsmål besvares med, at artikel 1, stk. 3, artikel 3 og artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med artikel 4, stk. 2, TEU, skal fortolkes således, at en national lovgivning, hvorefter en statslig myndighed kan pålægge udbydere af elektroniske kommunikationstjenester at overføre trafikdata og lokaliseringsdata til sikkerheds- og efterretningstjenesterne med henblik på at beskytte den nationale sikkerhed, er omfattet af dette direktivs anvendelsesområde.

Det andet spørgsmål

50 Med det andet spørgsmål ønsker den forelæggende ret nærmere bestemt oplyst, om artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med artikel 4, stk. 2, TEU og chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, skal fortolkes således, at denne bestemmelse er til hinder for en national lovgivning, hvorefter en statslig myndighed kan pålægge udbydere af elektroniske kommunikationstjenester at foretage generel og udifferentieret overføring af trafikdata og lokaliseringsdata til sikkerheds- og efterretningstjenesterne med henblik på at beskytte den nationale sikkerhed.

51 Indledningsvis bemærkes, at ifølge oplysningerne i anmodningen om præjudiciel afgørelse giver section 94 i lov af 1984 ministeren mulighed for, hvis det efter dennes opfattelse er nødvendigt af hensyn til den nationale sikkerhed eller forbindelserne til en udenlandsk regering, ved påbud at pålægge udbydere af elektroniske kommunikationstjenester at overføre bulk-kommunikationsdata til sikkerheds- og efterretningstjenesterne, idet disse data omfatter trafikdata og lokaliseringsdata samt oplysninger om de anvendte tjenester som omhandlet i RIPA's section 21 (4) og (6). Sidstnævnte bestemmelse omfatter bl.a. de data, der er nødvendige for at spore kilden til en kommunikation og dens bestemmelsessted, fastslå en kommunikations dato, tidspunkt, varighed og type, identificere det anvendte kommunikationsudstyr samt foretage lokalisering af terminaludstyret og kommunikationerne, dvs. de data, der navnlig omfatter navn og adresse på brugeren, telefonnummer på den, der foretager opkaldet, og det kaldte nummer, IP-adresserne på kilden til og modtageren af kommunikationen samt adresserne for besøgte websteder.

52 En sådan videregivelse ved overføring af data vedrører alle brugere af elektroniske kommunikationsmidler, uden at det præciseres, om denne overføring skal ske i realtid eller med forsinkelse. Efter overføringen lagres disse oplysninger ifølge oplysningerne i anmodningen om præjudiciel afgørelse af sikkerheds- og efterretningstjenesterne og står fortsat til rådighed for disse tjenester i forbindelse med deres aktiviteter i lighed med de andre databaser, som disse tjenester råder over. De således indsamlede data, der undergives automatiseret massebehandling og analyse, kan især krydstjekkes med andre databaser, der indeholder forskellige kategorier af massepersonoplysninger, eller videregives uden for disse tjenester og til tredjelande. Endelig kræver disse aktiviteter ikke forudgående tilladelse fra en domstol eller en uafhængig administrativ enhed og giver ikke anledning til at foretage underretning af de berørte personer.

53 Som det bl.a. fremgår af sjette og syvende betragtning til direktiv 2002/58, har dette direktiv til formål at beskytte brugerne af elektroniske kommunikationstjenester mod de risikomomenter for deres personoplysninger og privatliv, der følger af anvendelsen af ny teknologi, og navnlig den øgede mulighed for at foretage automatiseret opbevaring og behandling af oplysninger. Det nævnte direktiv søger, således som det fremgår af anden betragtning hertil, især at sikre fuld overholdelse af de rettigheder, der er nævnt i chartrets artikel 7 og 8. Det fremgår i denne henseende af begrundelsen til

forslaget til Europa-Parlamentets og Rådets direktiv om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (KOM(2000) 385 endelig), der lå til grund for direktiv 2002/58, at EU-lovgiver ønskede »at sikre, at der fortsat garanteres en høj grad af beskyttelse af personoplysninger og privatlivets fred i forbindelse med alle elektroniske kommunikationstjenester, uanset hvilken teknologi der anvendes«.

54 Det fremgår i denne henseende af artikel 5, stk. 1, i direktiv 2002/58, at »[m]edlemsstaterne sikrer kommunikationshemmeligheden ved brug af offentlige kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester, både for så vidt angår selve kommunikationen og de dermed forbundne trafikdata, via nationale forskrifter«. Det anføres ligeledes i denne bestemmelse, at »[medlemsstaterne] især [forbyder] aflytning, registrering, lagring og andre måder, hvorpå samtaler kan opfanges eller overvåges af andre end brugerne, uden at de pågældende brugere har indvilget heri, bortset fra tilfælde, hvor det er tilladt ifølge lovgivningen, jf. artikel 15, stk. 1«, og det præciseres, at »[d]ette stykke [ikke er] til hinder for teknisk lagring, som er nødvendig for overføring af en kommunikation, forudsat at princippet om kommunikationshemmelighed ikke berøres heraf«.

55 Denne artikel 5, stk. 1, i direktiv 2002/58 fastsætter således princippet om fortrolighed i forbindelse med såvel elektronisk kommunikation som de dermed forbundne trafikdata og indebærer navnlig, at det for andre end brugerne principielt er forbudt for enhver at lagre denne kommunikation og disse data, uden at disse brugere har givet samtykke hertil. Henset til den generelle karakter af denne bestemmelses ordlyd omfatter den nødvendigvis enhver handling, som giver tredjemand mulighed for at få kendskab til kommunikationen og de dermed forbundne data til andre formål end overføring af en kommunikation.

56 Det i artikel 5, stk. 1, i direktiv 2002/58 anførte forbud mod at registrere kommunikation og de dermed forbundne data omfatter derfor alle de situationer, hvor udbydere af elektroniske kommunikationstjenester stiller trafikdata og lokaliseringsdata til rådighed for offentlige myndigheder, såsom sikkerheds- og efterretningstjenester, og hvor disse myndigheder foretager lagring af de nævnte data, uanset hvorledes disse data efterfølgende anvendes.

57 EU-lovgiver har således med vedtagelsen af dette direktiv konkretiseret de rettigheder, der er sikret ved chartrets artikel 7 og 8, hvilket indebærer, at brugerne af elektroniske kommunikationsmidler principielt med rette kan forvente, at deres kommunikation og de dermed forbundne data forbliver anonyme, så længe de ikke har givet deres samtykke og ikke kan gøres til genstand for registrering (dom af 6.10.2020, La Quadrature du Net m.fl., forenede sager C-511/18, C-512/18 og C-520/18, præmis 109).

58 Artikel 15, stk. 1, i direktiv 2002/58 gør det imidlertid muligt for medlemsstaterne at indføre undtagelser til såvel den i dette direktivs artikel 5, stk. 1, fastsatte principielle forpligtelse til at sikre fortroligheden af personoplysninger som til de tilsvarende forpligtelser, der bl.a. er anført i det nævnte direktivs artikel 6 og 9, hvis en sådan indskrænkning er nødvendig, passende og forholdsmæssig i et demokratisk samfund af hensyn til den nationale sikkerhed, forsvaret, den offentlige sikkerhed, eller forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager eller uautoriseret brug af det elektroniske kommunikationssystem. Med henblik herpå kan medlemsstaterne bl.a. vedtage retsforskrifter om lagring af data i en begrænset periode, som kan begrundes i et af disse hensyn.

59 Når dette er sagt, kan den mulighed for at fravige de rettigheder og forpligtelser, der er fastsat i artikel 5, 6 og 9 i direktiv 2002/58, ikke begrunde, at en fravigelse af den principielle pligt til at sikre fortroligheden af elektronisk kommunikation og de dermed forbundne data og navnlig af det forbud mod at lagre disse data, der udtrykkeligt er fastsat i dette direktivs artikel 5, bliver hovedreglen (jf. i denne retning dom af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 89 og 104, og af 6.10.2020, La Quadrature du Net m.fl., forenede sager C-511/18, C-512/18 og C-520/18, præmis 111).

60 Det fremgår endvidere af artikel 15, stk. 1, tredje punktum, i direktiv 2002/58, at medlemsstaterne kun har mulighed for at vedtage retsforskrifter med henblik på at indskrænke rækkevidden af de rettigheder og forpligtelser, der er omhandlet i dette direktivs artikel 5, 6 og 9, såfremt dette sker i overensstemmelse med EU-rettens generelle principper, som bl.a. omfatter proportionalitetsprincippet, og de grundlæggende rettigheder, der er sikret ved chartret. Domstolen har i denne henseende allerede fastslået, at den pligt, som en medlemsstat i henhold til en national lovgivning har pålagt udbydere af elektroniske kommunikationstjenester, til at lagre trafikdata med henblik på i påkommende tilfælde at gøre dem tilgængelige for de kompetente nationale myndigheder, ikke blot rejser en række spørgsmål vedrørende overholdelsen af chartrets artikel 7 og 8, der vedrører henholdsvis respekten for privatlivet og beskyttelsen af personoplysninger, men ligeledes vedrørende artikel 11, der omhandler ytringsfriheden (jf. i denne retning dom af 8.4.2014, Digital Rights Ireland m.fl., C-293/12 og C-594/12, EU:C:2014:238, præmis 25 og 70, og af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 91 og 92 og den deri nævnte retspraksis).

61 Disse spørgsmål opstår ligeledes i forbindelse med andre former for databehandling, såsom overføring til andre end brugerne eller adgang til disse data med henblik på at anvende dem (jf. analogt udtalelse 1/15 (PNR-aftalen mellem EU og Canada) af 26.7.2017, EU:C:2017:592, præmis 122 og 123 og den deri nævnte retspraksis).

62 I forbindelse med fortolkningen af artikel 15, stk. 1, i direktiv 2002/58 skal der således tages hensyn til betydningen af såvel retten til respekt for privatlivet, der er sikret ved chartrets artikel 7, som retten til beskyttelse af personoplysninger, der er sikret ved dette charters artikel 8, således som denne betydning fremgår af Domstolens praksis, og retten til ytringsfrihed, idet denne grundlæggende rettighed, der er sikret ved chartrets artikel 11, udgør et af de væsentlige grundlag for et demokratisk og pluralistisk samfund, og er en del af de værdier, som Unionen i overensstemmelse med artikel 2 TEU er støttet på (jf. i denne retning dom af 6.3.2001, Connolly mod Kommissionen, C-274/99 P, EU:C:2001:127, præmis 39, og af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 93 og den deri nævnte retspraksis).

63 De rettigheder, der er sikret ved chartrets artikel 7, 8 og 11, er imidlertid ikke absolutte rettigheder, men skal ses i sammenhæng med deres funktion i samfundet (jf. i denne retning dom af 16.7.2020, Facebook Ireland og Schrems, C-311/18, EU:C:2020:559, præmis 172 og den deri nævnte retspraksis).

64 Som det fremgår af chartrets artikel 52, stk. 1, tillader dette charter nemlig begrænsninger i udøvelsen af disse rettigheder, for så vidt som disse begrænsninger er fastlagt i lovgivningen og respekterer de nævnte rettigheders væsentligste indhold, og for så vidt som disse begrænsninger under iagttagelse af proportionalitetsprincippet er nødvendige og faktisk svarer til mål af almen interesse, der er anerkendt af Unionen, eller et behov for beskyttelse af andres rettigheder og friheder.

65 Det skal tilføjes, at kravet om, at enhver begrænsning af udøvelsen af de grundlæggende rettigheder skal være fastlagt i lovgivningen, indebærer, at det retsgrundlag, som tillader et indgreb i disse rettigheder, selv skal definere rækkevidden af begrænsningen af udøvelsen af den pågældende rettighed (dom af 16.7.2020, Facebook Ireland og Schrems, C-311/18, EU:C:2020:559, præmis 175 og den deri nævnte retspraksis).

66 Hvad angår overholdelsen af proportionalitetsprincippet bestemmer artikel 15, stk. 1, første punktum, i direktiv 2002/58, at medlemsstaterne kan vedtage en foranstaltning, der fraviger princippet om fortroligheden af kommunikation og de dermed forbundne trafikdata, når en sådan foranstaltning er »nødvendig, passende og forholdsmæssig i et demokratisk samfund« af hensyn til de formål, der er nævnt i denne bestemmelse. Det fremgår af 11. betragtning til dette direktiv, at en foranstaltning af denne art skal stå i »åbenbart« rimeligt forhold til det mål, der forfølges.

67 Det skal i denne henseende bemærkes, at det af Domstolens faste praksis fremgår, at beskyttelsen af den grundlæggende ret til respekt for privatlivet kræver, at undtagelserne til og begrænsningerne af beskyttelsen af personoplysninger holdes inden for det strengt nødvendige. Desuden kan et mål af almen interesse ikke forfølges uden hensyntagen til den omstændighed, at dette mål skal forenes med de grundlæggende rettigheder, der er berørt af foranstaltningen, ved at foretage en rimelig afvejning mellem målet og de pågældende interesser og rettigheder (jf. i denne retning dom af 16.12.2008, Satakunnan Markkinapörssi og Satamedia, C-73/07, EU:C:2008:727, præmis 56, og af 9.11.2010, Volker und Markus Schecke og Eifert, C-92/09 og C-93/09, EU:C:2010:662, præmis 76, 77 og 86, og af 8.4.2014, Digital Rights Ireland m.fl., C-293/12 og C-594/12, EU:C:2014:238, præmis 52, samt udtalelse 1/15 (PNR-aftalen mellem EU og Canada) af 26.7.2017, EU:C:2017:592, præmis 140).

68 For at opfylde kravet om proportionalitet skal en lovgivning fastsætte klare og præcise regler, der regulerer rækkevidden og anvendelsen af den pågældende foranstaltning, og som opstiller en række mindstekrav, således at de personer, hvis personoplysninger er berørt, råder over tilstrækkelige garantier, der gør det muligt effektivt at beskytte disse oplysninger mod risikoen for misbrug. Denne lovgivning skal være retligt bindende i national ret og navnlig angive, under hvilke omstændigheder og på hvilke betingelser der kan vedtages en foranstaltning om behandling af sådanne oplysninger, hvorved det sikres, at indgrebet begrænses til det strengt nødvendige. Nødvendigheden af at råde over sådanne garantier er så meget desto større, når personoplysningerne er undergivet en automatiseret behandling, navnlig når der eksisterer en betydelig risiko for ulovlig adgang til disse oplysninger. Disse betragtninger gør sig især gældende, når der er tale om beskyttelse af den særlige kategori af personoplysninger, som følsomme oplysninger udgør (jf. i denne retning dom af 8.4.2014, Digital Rights Ireland m.fl., C-293/12 og C-594/12, EU:C:2014:238, præmis 54 og 55, og af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 117, samt udtalelse 1/15 (PNR-aftalen mellem EU og Canada) af 26.7.2017, EU:C:2017:592, præmis 141).

69 Hvad angår spørgsmålet om, hvorvidt en national lovgivning som den i hovedsagen omhandlede opfylder kravene i artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, skal det bemærkes, at overføring af trafikdata og lokaliseringsdata til andre end brugerne, såsom sikkerheds- og efterretningstjenester, fraviger princippet om fortrolighed. Da denne aktivitet som i det foreliggende tilfælde foretages generelt og udifferentieret, bevirker den, at undtagelsen fra den principielle forpligtelse til at sikre datafortroligheden gøres til hovedreglen, mens den ved direktiv 2002/58 indførte ordning opstiller et krav om, at en sådan fravigelse forbliver undtagelsen.

70 Dertil kommer, at overføring af trafikdata og lokaliseringsdata til en tredjemand ifølge Domstolens faste praksis udgør et indgreb i de grundlæggende rettigheder, der er sikret ved chartrets artikel 7 og 8, uanset hvad disse data efterfølgende bruges til. I denne henseende er det ikke afgørende, om de pågældende oplysninger vedrørende privatlivet er følsomme, eller om dette indgreb har medført eventuelle ubehageligheder for de berørte (jf. i denne retning udtalelse 1/15 (PNR-aftalen mellem EU og Canada) af 26.7.2017, EU:C:2017:592, præmis 124 og 126 og den deri nævnte retspraksis, og dom af 6.10.2020, La Quadrature du Net m.fl., forenede sager C-511/18, C-512/18 og C-520/18, præmis 115 og 116).

71 Det indgreb, som overføring af trafikdata og lokaliseringsdata til sikkerheds- og efterretningstjenesterne indebærer i den rettighed, som er fastsat i chartrets artikel 7, skal anses for at være særligt alvorligt, henset til bl.a. den følsomme karakter af de oplysninger, som disse data kan give adgang til, og navnlig muligheden for på grundlag heraf at lave en profil af de berørte personer, idet en sådan oplysning er lige så følsom som selve indholdet af kommunikationen. Den er i øvrigt egnet til at skabe en følelse hos de berørte personer af, at deres privatliv er genstand for konstant overvågning (jf. analogt dom af 8.4.2014, Digital Rights Ireland m.fl., C-293/12 og C-594/12, EU:C:2014:238, præmis 27 og 37, og af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 99 og 100).

72 Det skal endvidere bemærkes, at overføring af trafikdata og lokaliseringsdata til offentlige myndigheder med henblik på sikkerhedsmæssige formål i sig selv kan medføre et indgreb i retten til respekt for kommunikation, der er sikret ved chartrets artikel 7, og have afskrækkende virkninger, der kan afholde brugerne af elektroniske kommunikationsmidler fra at udøve deres ret til ytringsfrihed, der er sikret ved chartrets artikel 11. Sådanne afskrækkende virkninger kan navnlig påvirke de personer, hvis kommunikation i henhold til nationale bestemmelser er undergivet tavshedspligt, og de whistleblowere, hvis aktiviteter er beskyttet i henhold til Europa-Parlamentets og Rådets direktiv (EU) 2019/1937 af 23. oktober 2019 om beskyttelse af personer, der indberetter overtrædelser af EU-retten (EUT 2019, L 305, s. 17). Disse virkninger er desuden så meget desto mere alvorlige i betragtning af, at der er tale om store mængder af lagrede data af meget forskellig art (jf. i denne retning dom af 8.4.2014, Digital Rights Ireland m.fl., C-293/12 og C-594/12, EU:C:2014:238, præmis 28, af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 101, og af 6.10.2020, La Quadrature du Net m.fl., forenede sager C-511/18, C-512/18 og C-520/18, præmis 118).

73 Henset endelig til den store mængde trafikdata og lokaliseringsdata, der løbende kan lagres ved hjælp af en generel og udifferentieret lagringsforanstaltning, og den følsomme karakter af de oplysninger, som disse data kan give adgang til, medfører alene den omstændighed, at udbyderne af elektroniske kommunikationstjenester lagrer de nævnte data, en risiko for misbrug og ulovlig adgang.

74 Hvad angår de formål, som kan begrunde sådanne indgreb, nærmere bestemt det i hovedsagen omhandlede formål om at beskytte den nationale sikkerhed, skal det indledningsvis bemærkes, at det af artikel 4, stk. 2, TEU fremgår, at den nationale sikkerhed forbliver den enkelte medlemsstats eneansvar. Dette ansvar svarer til den primære interesse i at beskytte statens væsentlige funktioner og grundlæggende samfundsinteresser og omfatter forebyggelse og bekæmpelse af aktiviteter, der alvorligt kan destabilisere et lands grundlæggende forfatningsmæssige, politiske, økonomiske eller sociale strukturer og navnlig direkte true samfundet, befolkningen eller staten som sådan, såsom bl.a. terrorvirksomhed (dom af 6.10.2020, La Quadrature du Net m.fl., forenede sager C-511/18, C-512/18 og C-520/18, præmis 135).

75 Formålet om beskyttelse af den nationale sikkerhed, sammenholdt med artikel 4, stk. 2, TEU, vejer tungere end de andre formål, der er indeholdt i artikel 15, stk. 1, i direktiv 2002/58, bl.a. formålet om bekæmpelse af kriminalitet i almindelighed, herunder også grov kriminalitet og om beskyttelse af den offentlige sikkerhed. Trusler som dem, der er nævnt i den foregående præmis, adskiller sig nemlig på grund af deres art og særligt alvorlige karakter fra den generelle risiko for, selv alvorlige, spændinger eller forstyrrelser for den offentlige sikkerhed. Med forbehold for overholdelsen af de øvrige krav, der er fastsat i chartrets artikel 52, stk. 1, kan formålet om beskyttelse af den nationale sikkerhed derfor begrunde foranstaltninger, der indebærer indgreb i de grundlæggende rettigheder, som er mere alvorlige end dem, som disse andre formål kan begrunde (dom af 6.10.2020, La Quadrature du Net m.fl., forenede sager C-511/18, C-512/18 og C-520/18, præmis 136).

76 For at opfylde kravet om proportionalitet, der er nævnt i denne doms præmis 67, ifølge hvilket undtagelserne fra og begrænsningerne af beskyttelsen af personoplysninger skal holdes inden for det strengt nødvendige, skal en national lovgivning, som indebærer et indgreb i de grundlæggende rettigheder, der er sikret ved chartrets artikel 7 og 8, overholde de krav, der følger af den retspraksis, der er nævnt i denne doms præmis 65, 67 og 68.

77 Hvad særligt angår en myndigheds adgang til personoplysninger kan en lovgivning ikke begrænse sig til at opstille et krav om, at myndighedernes adgang til oplysningerne opfylder formålet med denne lovgivning, men skal tillige fastsætte de materielle og processuelle betingelser for denne brug (jf. analogt udtalelse 1/15 (PNR-aftalen mellem EU og Canada) af 26.7.2017, EU:C:2017:592, præmis 192 og den deri nævnte retspraksis).

78 For så vidt som en generel adgang til samtlige lagrede data – når der ikke foreligger nogen forbindelse, selv indirekte, til det forfulgte mål – ikke kan anses for at være begrænset til det strengt nødvendige, skal en national lovgivning, der regulerer adgang til trafikdata og lokaliseringsdata, således være baseret på objektive kriterier med henblik på fastlæggelsen af de omstændigheder og betingelser, hvorunder de kompetente nationale myndigheder skal gives adgang til de pågældende data (jf. i denne retning dom af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 119 og den deri nævnte retspraksis).

79 Disse krav gælder så meget desto mere for en lovgivningsmæssig foranstaltning som den i hovedsagen omhandlede, på grundlag af hvilken den kompetente nationale myndighed kan pålægge udbydere af elektroniske kommunikationstjenester at foretage generel og udifferentieret overføring af trafikdata og lokaliseringsdata til sikkerheds- og efterretningstjenesterne. En sådan overføring bevirker nemlig, at disse data stilles til rådighed for de offentlige myndigheder (jf. analogt udtalelse 1/15 (PNR-aftalen mellem EU og Canada) af 26.7.2017, EU:C:2017:592, præmis 212).

80 Eftersom overføringen af trafikdata og lokaliseringsdata sker på en generel og udifferentieret måde, vedrører den generelt alle personer, der gør brug af elektroniske kommunikationstjenester. Den finder dermed anvendelse selv på personer, for hvis vedkommende der ikke findes noget som helst indicium for, at deres adfærd kan have – selv en indirekte eller fjern – forbindelse til formålet om beskyttelse af den nationale sikkerhed, og navnlig uden at det er godtgjort, at der er en forbindelse mellem de data, der skal overføres, og en trussel mod den offentlige sikkerhed (jf. i denne retning dom af 8.4.2014, Digital Rights Ireland m.fl., C-293/12 og C-594/12, EU:C:2014:238, præmis 57 og 58, og af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 105). Henset til den omstændighed, at overføringen af sådanne oplysninger til de offentlige myndigheder i overensstemmelse med, hvad der er konstateret i denne doms præmis 79, svarer til en adgang, skal det fastslås, at en lovgivning, der tillader en generel og udifferentieret overføring af data til de offentlige myndigheder, indebærer en generel adgang.

81 Heraf følger, at en national lovgivning, der pålægger udbydere af elektroniske kommunikationstjenester at foretage generel og udifferentieret overføring af trafikdata og lokaliseringsdata til sikkerheds- og efterretningstjenesterne, overskrider det strengt nødvendige og kan i et demokratisk samfund ikke anses for at være begrundet, således som det er påkrævet i henhold til artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med artikel 4, stk. 2, TEU, og chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1.

82 Henset til samtlige ovenstående betragtninger skal det andet spørgsmål besvares med, at artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med artikel 4, stk. 2, TEU og chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, skal fortolkes således, at bestemmelsen er til hinder for en national lovgivning, hvorefter en statslig myndighed kan pålægge udbydere af elektroniske kommunikationstjenester at foretage generel og udifferentieret overføring af trafikdata og lokaliseringsdata til sikkerheds- og efterretningstjenesterne med henblik på at beskytte den nationale sikkerhed.

Sagsomkostninger

83 Da sagens behandling i forhold til hovedsagens parter udgør et led i den sag, der verserer for den forelæggende ret, tilkommer det denne at træffe afgørelse om sagsomkostningerne. Bortset fra de nævnte parters udgifter kan de udgifter, som er afholdt i forbindelse med afgivelse af indlæg for Domstolen, ikke erstattes.

På grundlag af disse præmisser kender Domstolen (Store Afdeling) for ret:

1) **Artikel 1, stk. 3, artikel 3 og artikel 15, stk. 1, i Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktiv om databeskyttelse inden for elektronisk kommunikation), som ændret ved Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009, sammenholdt med artikel 4, stk. 2, TEU, skal fortolkes således, at en national lovgivning, hvorefter en statslig myndighed kan pålægge udbydere af elektroniske kommunikationstjenester at overføre trafikdata og lokaliseringsdata til sikkerheds- og efterretningstjenesterne med henblik på at beskytte den nationale sikkerhed, er omfattet af dette direktivs anvendelsesområde.**

2) **Artikel 15, stk. 1, i direktiv 2002/58, som ændret ved direktiv 2009/136, sammenholdt med artikel 4, stk. 2, TEU og artikel 7, 8 og 11 samt artikel 52, stk. 1, i Den Europæiske Unions charter om grundlæggende rettigheder, skal fortolkes således, at bestemmelsen er til hinder for en national lovgivning, hvorefter en statslig myndighed kan pålægge udbydere af elektroniske kommunikationstjenester at foretage generel og udifferentieret overføring af trafikdata og lokaliseringsdata til sikkerheds- og efterretningstjenesterne med henblik på at beskytte den nationale sikkerhed.**

Underskrifter