Samling af Afgørelser

FORSLAG TIL AFGØRELSE FRA GENERALADVOKAT
M. CAMPOS SÁNCHEZ-BORDONA
fremsat den 15. januar 2020[1]

Sag C-623/17

Privacy International
mod
Secretary of State for Foreign and Commonwealth Affairs,
Secretary of State for the Home Department,
Government Communications Headquarters,
Security Service Srl,
Secret Intelligence Service

(anmodning om præjudiciel afgørelse indgivet af Investigatory Powers Tribunal (domstol for efterforskningsbeføjelser, Det Forenede Kongerige))

»Præjudiciel forelæggelse – behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor – direktiv 2002/58/EF – anvendelsesområde – artikel 1, stk. 3 – artikel 15, stk. 3 – Den Europæiske Unions charter om grundlæggende rettigheder – artikel 7, 8 og 51 samt artikel 52, stk. 1 – artikel 4, stk. 2, TEU – generel og udifferentieret overføring af forbindelsesdata for brugerne af en elektronisk kommunikationstjeneste til sikkerhedstjenesterne«

1. Domstolen har de senere år opretholdt en fast praksis om lagring af og adgang til personoplysninger, i hvilken forbindelse følgende domme fremhæves som milepæle:

– Dom af 8. april 2014, Digital Rights Ireland m.fl.[2], hvorved Domstolen fastslog, at direktiv 2006/24/EF[3] var ugyldigt, for så vidt som det tillod et uforholdsmæssigt indgreb i de rettigheder, som er sikret ved artikel 7 og 8 i Den Europæiske Unions charter om grundlæggende rettigheder.

– Dom af 21. december 2016, Tele2 Sverige og Watson m.fl.[4], hvorved Domstolen fortolkede artikel 15, stk. 1, i direktiv 2002/58/EF[5].

– Dom af 2. oktober 2018, Ministerio Fiscal[6], hvorved Domstolen bekræftede fortolkningen af førnævnte bestemmelse i direktiv 2002/58.

1 – Originalsprog: spansk.

2 – De forenede sager C-293/12 og C-594/12, herefter »Digital Rights-dommen«, EU:C:2014:238.

3 – Europa-Parlamentets og Rådets direktiv af 15.3.2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF (EUT 2006, L 105, s. 54).

4 – De forenede sager C-203/15 og C-698/15, herefter »dommen i sagen Tele2 Sverige og Watson«, EU:C:2016:970.

5 – Europa-Parlamentets og Rådets direktiv af 12.7.2002 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).

6 – Sag C-207/16, herefter »Ministerio Fiscal-dommen«, EU:C:2018:788.

2. Disse domme (især den anden) bekymrer myndighederne i visse medlemsstater, eftersom de efter disse myndigheders opfattelse fratager dem et instrument, som de anser for nødvendigt for at beskytte den nationale sikkerhed og bekæmpe terrorisme. Derfor har nogle af disse medlemsstater opfordret til, at denne retspraksis ændres eller nuanceres.

3. Visse af medlemsstaternes domstole har givet udtryk for samme bekymring i fire anmodninger om præjudiciel afgørelse[7], med hensyn til hvilke jeg også fremsætter mit forslag til afgørelse i dag.

4. De fire sager rejser først og fremmest en problemstilling i forbindelse med anvendelsen af direktiv 2002/58 på aktiviteter, der er forbundet med den nationale sikkerhed og bekæmpelsen af terrorisme. Hvis dette direktiv finder anvendelse i denne sammenhæng, må det i det følgende afklares, i hvilket omfang medlemsstaterne kan begrænse den ret til privatlivets fred, som direktivet beskytter. Endelig bør det undersøges, i hvilket omfang de forskellige nationale lovgivninger (den britiske[8], den belgiske[9] og den franske[10]) på dette område er i overensstemmelse med EU-retten som fortolket af Domstolen.

I. Retsforskrifter

A. EU-retten

5. Her henviser jeg til det tilsvarende afsnit i mit forslag til afgørelse i de forenede sager C-511/18 og C-512/18.

B. National ret (der finder anvendelse i denne tvist)

1. Telecommunications Act 1984[11]

6. I henhold til section 94 kan en minister (Secretary of State) udstede generelle eller specifikke påbud til en udbyder af et offentligt elektronisk kommunikationsnet, hvis de ifølge ministeren er nødvendige af hensyn til den nationale sikkerhed eller forbindelsen til en regering i et land eller et territorium, der befinder sig uden for Det Forenede Kongerige.

2. Data Retention and Investigatory Powers Act 2014[12]

7. Section 1 fastsætter:

»(1) Secretary of State kan ved en lagringsmeddelelse pålægge en offentlig teleoperatør at lagre relevante kommunikationsdata, hvis Secretary of State er af den opfattelse, at kravet er nødvendigt og forholdsmæssigt for et eller flere af de formål, der er omfattet af section 22(2)(a)-(h) i Regulation of Investigatory Powers Act 2000 [lov af 2000 om efterforskningsbeføjelser, herefter »RIPA«].

(2) En lagringsmeddelelse kan:

(a) vedrøre en bestemt operatør eller enhver kategori af operatører

7 – Ud over den foreliggende anmodning drejer det sig om de forenede sager C-511/18 og C-512/18, La Quadrature du Net m.fl., og sag C-520/18, Ordre des barreaux francophones et germanophone m.fl.

8 – Sag C-623/17, Privacy International.

9 – Sag C-520/18, Ordre des barreaux francophones et germanophone m.fl.

10 – De forenede sager C-511/18 og C-512/18, La Quadrature du Net m.fl.

11 – Lov af 1984 om telekommunikation, herefter »lov af 1984«.

12 – Lov af 2014 om lagring af data og undersøgelsesbeføjelser, herefter »DRIPA«.

(b) kræve lagring af alle data eller enhver kategori af data

(c) fastsætte den eller de perioder, hvori data skal lagres

(d) medføre andre krav eller begrænsninger med hensyn til lagring af data

(e) fastsætte forskellige bestemmelser for forskellige formål

(f) vedrøre data, uanset om de eksisterer på det tidspunkt, hvor meddelelsen udstedes eller træder i kraft.

(3) Secretary of State kan ved bekendtgørelse fastsætte nærmere bestemmelser om lagringen af relevante kommunikationsdata.

(4) Sådanne bestemmelser kan navnlig omfatte bestemmelser om:

(a) krav inden udstedelse af en lagringsmeddelelse

(b) den maksimale periode, hvori data skal lagres i henhold til en lagringsmeddelelse

(c) indhold, vedtagelse, ikrafttræden, revision, ændring eller tilbagekaldelse af en lagringsmeddelelse

(d) integritet eller sikkerhed i forbindelse med, beskyttelse af, adgang til eller videregivelse eller tilintetgørelse af data, der lagres i medfør af denne section

(e) overholdelse af relevante krav eller begrænsninger eller efterprøvelse af overholdelsen

(f) en praksiskodeks med hensyn til relevante krav eller begrænsninger eller relevante beføjelser

(g) Secretary of States godtgørelse (med eller uden betingelser) af udgifter afholdt af offentlige teleoperatører i forbindelse med overholdelsen af relevante krav eller begrænsninger

[…]

(5) Den maksimale periode, der er fastsat i medfør af subsection (4)(b), må ikke overstige 12 måneder fra den dato, der er fastsat med hensyn til de data, som er omfattet af de i subsection (3) omhandlede bekendtgørelser.

(6) En offentlig teleoperatør, der lagrer relevante kommunikationsdata i medfør af denne section, må ikke videregive disse data undtagen:

(a) i overensstemmelse med:

(i) del 1, kapitel 2, i [RIPA]

(ii) en retsafgørelse eller anden retlig afgørelse eller retskendelse, eller

(b) som fastsat i de i subsection (3) omhandlede bekendtgørelser.

(7) Secretary of State kan i regler fastsætte bestemmelser med hensyn til enhver bestemmelse, der er fastsat (eller kan fastsættes) i medfør af subsection (4)(d)-(g) eller subsection (6), med hensyn til kommunikationsdata, som lagres af udbydere af telekommunikationstjenester i medfør af en praksiskodeks i henhold til section 102 i Anti-terrorism, Crime and Security Act 2001 [lov om terrorbekæmpelse, kriminalitet og sikkerhed af 2001].«

3. RIPA

8. Section 21 bestemmer:

»[…]

(4) I dette kapitel forstås ved »kommunikationsdata« 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) I denne afdeling forstås der ved »trafikdata« i forbindelse med enhver kommunikation:

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

(b) alle 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.

[…]«

9. Section 22 bestemmer:

»(1) Nærværende section finder anvendelse, når en person, der er ansvarlig i henhold til dette kapitel, finder det nødvendigt at indsamle kommunikationsdata af de grunde, som er anført i subsection (2).

(2) Det er nødvendigt at indsamle kommunikationsdata af grunde henhørende under nærværende subsection, såfremt disse kommunikationsdata er nødvendige:

(a) af hensyn til den nationale sikkerhed

(b) med henblik på forebyggelse eller afsløring af forbrydelser eller forebyggelse af forstyrrelse af den offentlige orden

(c) af hensyn til Det Forenede Kongeriges økonomiske velfærd, såfremt disse interesser ligeledes er relevante med hensyn til den nationale sikkerhed

(d) af hensyn til den offentlige tryghed

(e) med henblik på beskyttelse af den offentlige sundhed

(f) med henblik på fastsættelse eller opkrævning af enhver form for skat, told, afgift eller andet bidrag eller gebyr, der skal betales til en offentlig myndighed

(g) med henblik på i nødstilfælde at forebygge dødsfald eller legemsbeskadigelse eller enhver skade på en persons fysiske eller mentale sundhed eller afhjælpe enhver skade på en persons fysiske eller mentale sundhed

(h) i henhold til ethvert andet formål (der ikke er omfattet af paragraph (a)-(g)), der er fastsat i en afgørelse truffet af Secretary of State i henhold til section 22(2)(h) i [DRIPA].

(4) Med forbehold af subsection (5) kan den ansvarlige person, når denne finder, at en postoperatør eller en teleoperatør er eller kan være i besiddelse af eller er i stand til at indsamle kommunikationsdata, ved meddelelse til postoperatøren eller teleoperatøren anmode operatøren om:

(a) at indsamle disse data, såfremt den pågældende ikke allerede er i besiddelse heraf, og

(b) under alle omstændigheder at videregive samtlige data i den pågældendes besiddelse, eller som den pågældende har indsamlet efterfølgende.

(5) Den ansvarlige person skal ikke meddele tilladelse i henhold til subsection (3) eller indgive en anmodning i henhold til subsection (4), medmindre den pågældende er af den opfattelse, at en indsamling af de omhandlede data, der sker ved en tilladt eller krævet adfærd i medfør af tilladelsen eller anmodningen, står i forhold til det mål, der forfølges med en sådan indsamling af disse data.«

10. I henhold til section 65 kan der indgives klage til Investigatory Powers Tribunal (domstol for efterforskningsbeføjelser, Det Forenede Kongerige), hvis der er en formodning om, at data er blevet indsamlet med urette.

II. De faktiske omstændigheder og de præjudicielle spørgsmål

11. Ifølge den forelæggende ret omhandler hovedsagen Det Forenede Kongeriges sikkerheds- og efterretningsagenturers (Security and Intelligence Agencies, herefter »agenturerne«) indsamling og brug af bulk-kommunikationsdata (Bulk Communications Data, herefter »BCD«).

12. Sådanne data omfatter oplysninger om »hvem, hvornår, hvor, hvordan og med hvem« i forbindelse med brug af både telefon og internet. De omfatter lokalisering af mobil- og fastnettelefoner, hvorfra der foretages eller modtages opkald, og lokalisering af computere, der bruges til at få adgang til internettet. De omfatter ikke indholdet af kommunikation, hvilket kræver en retskendelse.

13. Sagsøgeren i hovedsagen (Privacy International, en ikkestatslig menneskerettighedsorganisation) har anlagt sag ved den forelæggende ret med påstand om, at agenturernes brug af BCD udgør en krænkelse af retten til privatlivets fred i henhold til artikel 8 i den europæiske menneskerettighedskonvention (herefter »EMRK«) og er i strid med EU-retten.

14. De sagsøgte myndigheder[13] har gjort gældende, at deres brug af sådanne beføjelser er lovlig og afgørende for bl.a. beskyttelsen af den nationale sikkerhed.

15. Ifølge forelæggelsesafgørelsens oplysninger modtager agenturerne bulk-kommunikationsdata fra operatørerne af offentlige elektroniske kommunikationsnet i medfør af en afgørelse truffet af Secretary of State i overensstemmelse med section 94 i lov af 1984.

16. Disse data omfatter trafik- og lokalitetsdata med oplysninger om brugernes sociale, kommercielle og finansielle aktiviteter, kommunikation og rejseaktivitet. Agenturerne lagrer disse data, når de modtager dem, på en sikker måde ved hjælp af teknikker (f.eks. filtrering og sammenholdelse), som er generelle, dvs. ikke rettet mod specifikke, kendte mål.

17. Den forelæggende ret anser det for godtgjort, at disse teknikker er afgørende for agenturernes arbejde med at bekæmpe alvorlige trusler mod den offentlige sikkerhed, navnlig terrorisme, kontraspionage og spredningen af atomvåben. Agenturernes beføjelse til at indsamle og anvende dataene er afgørende for beskyttelsen af Det Forenede Kongeriges nationale sikkerhed.

18. Ifølge den forelæggende ret er de omtvistede foranstaltninger i overensstemmelse med national ret og EMRK's artikel 8. Den nærer imidlertid tvivl om, hvorvidt de er forenelige med EU-retten, henset til dommen i sagen Tele2 Sverige og Watson.

19. På denne baggrund har den forelæggende ret forelagt Domstolen følgende præjudicielle spørgsmål:

»1) [Idet] der henvises til artikel 4 TEU og artikel 1, stk. 3, i direktiv 2002/58/EF […], gælder det da, at et krav i en afgørelse truffet af en Secretary of State om, at en udbyder af et elektronisk kommunikationsnetværk skal udlevere bulk-kommunikationsdata til en medlemsstats sikkerheds- og efterretningsagenturer, er omfattet af EU-retten og [direktiv 2002/58]?

2) Hvis [det] første spørgsmål besvares bekræftende: Finder nogen af Watson-kravene [14], eller eventuelle andre krav ud over kravene i EMRK, anvendelse på en sådan afgørelse truffet af en Secretary of State? 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 efterretningsagenturerne 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?«

20. Den forelæggende ret har præciseret sine spørgsmål som følger:

»a) [Agenturernes] mulighed for at bruge [bulk-kommunikationsdata] indgivet til agenturerne 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 [agenturernes] brug af [disse data] er at afdække hidtil ukendte trusler mod den nationale sikkerhed ved hjælp af ikkemålrettede bulk-teknikker, der afhænger af, at [disse data] 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.

13 – Secretary of State for Foreign and Commonwealth Affairs (minister for udenrigs- og Commonwealth-anliggender), Secretary of State for the Home Department (indenrigsministeren) og Det Forenede Kongeriges tre sikkerheds- og efterretningsagenturer, dvs. Government Communications Headquarters (statens kommunikationshovedkvarter, GCHQ), Security Service (sikkerhedstjenesten, MI5) og Secret Intelligence Service (den oversøiske efterretningstjeneste, MI6).

14 – Dvs. praksis efter dommen i sagen Tele2 Sverige og Watson.

c) Udbyderen af et elektronisk kommunikationsnetværk […] er [ikke efterfølgende] forpligtet til at lagre BCD (efter det tidsrum, der stilles krav om i forbindelse med deres almindelige virksomhed), som opbevares af de offentlige myndigheder ([agenturerne]) alene.

d) Den nationale domstol [har] (med nogle få forbehold) […] fastslået, at de sikkerhedsforanstaltninger, der er forbundet med [agenturernes] brug af [disse data], er i overensstemmelse med kravene i EMRK.

e) Den nationale domstol har fastslået, at fastsættelsen af de krav, der fremgår af [dommen i sagen] Tele2 Sverige og Watson […][,] i givet fald ville begrænse de foranstaltninger, som agenturerne træffer for at beskytte den nationale sikkerhed, og dermed bringe Det Forenede Kongeriges nationale sikkerhed i fare.«

III. Retsforhandlingerne for Domstolen

21. Det præjudicielle spørgsmål indgik til Domstolen den 31. oktober 2017.

22. Den belgiske, den tjekkiske og den tyske regering, Irland, den spanske, den estiske, den franske, den cypriotiske, den ungarske, den lettiske, den nederlandske, den polske, den portugisiske, den svenske, Det Forenede Kongeriges og den norske regering samt Kommissionen har afgivet skriftlige indlæg.

23. Den 9. september 2019 blev der afholdt et retsmøde, som blev afholdt samtidig med retsmøderne i sag C-511/18, C-512/18 og C-520/18, med deltagelse af parterne i de fire præjudicielle procedurer, de ovennævnte regeringer, Kommissionen og Den Europæiske Tilsynsførende for Databeskyttelse.

IV. Bedømmelse

A. Anvendelsesområdet for direktiv 2002/58 og udelukkelsen af den nationale sikkerhed (det første præjudicielle spørgsmål)

24. I det forslag til afgørelse, som jeg i dag fremsætter i de forenede sager C-511/18 og C-512/18, forklarer jeg grundene til, at direktiv 2002/58 efter min opfattelse »som udgangspunkt finder anvendelse, når udbydere af elektroniske tjenester ved lov er forpligtede til at lagre oplysninger om deres abonnenter og at tillade de offentlige myndigheder adgang hertil. Det ændrer ikke ved denne antagelse, at forpligtelserne pålægges udbyderne af nationale sikkerhedshensyn« [15].

25. I forbindelse med min argumentation ser jeg nærmere på indvirkningen af Domstolens dom af 30. maj 2006, Parlamentet mod Rådet [16], og dommen i sagen Tele2 Sverige og Watson og foreslår en helhedsfortolkning af disse to domme [17].

26. I samme forslag til afgørelse undersøger jeg efter en bekræftelse af, at direktiv 2002/58 finder anvendelse, udelukkelsen af den nationale sikkerhed, der fremgår heraf, og indvirkningen af artikel 4, stk. 2, TEU [18].

15 – Forslag til afgørelse i de forenede sager C-511/18 og C-512/18, punkt 42.

16 – De forenede sager C-317/04 og C-318/04, EU:C:2006:346.

17 – Forslag til afgørelse i de forenede sager C-511/18 og C-512/18, punkt 44-76.

18 – Ibidem, punkt 77-90.

27. Med forbehold af det nedenstående henviser jeg til mine betragtninger i ovennævnte forslag til afgørelse samt i mit forslag til afgørelse i sag C-520/18.

1. Anvendelsen af direktiv 2002/58 i denne sag

28. I henhold til de omtvistede bestemmelser i denne sag pålægges udbydere af elektroniske kommunikationstjenester en forpligtelse, der ud over lagring indebærer en behandling af de data, som er i deres besiddelse på grund af de tjenester, som de leverer til brugere af offentlige kommunikationsnet i Unionen [19].

29. De nævnte operatører har nærmere bestemt pligt til at overføre de pågældende data til agenturerne. Her rejses spørgsmålet, om artikel 15, stk. 1, i direktiv 2002/58 tillader, at denne overføring, på grund af dens formål, uden videre udelukkes fra EU-retten.

30. Dette er efter min opfattelse ikke tilfældet. Lagringen af de pågældende data og den efterfølgende overføring kan kvalificeres som en behandling af personoplysninger forestået af udbyderne af elektroniske kommunikationstjenester og er således naturligt omfattet af anvendelsesområdet for direktiv 2002/58.

31. Hensynet til den nationale sikkerhed kan ikke gå forud for denne konstatering, således som den forelæggende ret har foreslået, med den følge, at den omtvistede forpligtelse ikke omfattes af EU-rettens anvendelsesområde. Efter min opfattelse pålægges udbyderne som nævnt en behandling af data i forbindelse med, at offentligt tilgængelige elektroniske kommunikationstjenester stilles til rådighed via offentlige kommunikationsnet i Unionen, hvilket netop er anvendelsesområdet for direktiv 2002/58, jf. dets artikel 3, stk. 1.

32. På denne baggrund drejer diskussionen sig ikke længere om agenturernes virksomhed (der som nævnt kan befinde sig uden for EU-retten, hvis den ikke berører operatører inden for elektronisk kommunikation), men derimod lagring og efterfølgende overføring af de data, som er i disse operatørers besiddelse. Efter disse betragtninger drejer spørgsmålet sig om de grundlæggende rettigheder, som sikres af Unionen.

33. Nøglen til at afgøre denne diskussion er atter pligten til generel og udifferentieret lagring af data, som de offentlige myndigheder har adgang til.

2. Henvisningen til den nationale sikkerhed

34. Eftersom den forelæggende ret har lagt særlig vægt på den del af agenturernes virksomhed, der berører den nationale sikkerhed, tillader jeg mig at gengive nogle af punkterne fra mit forslag til afgørelse af samme dato i de forenede sager C-511/18 og C-512/18 om dette emne:

»77. Den nationale sikkerhed […] er genstand for en dobbelt behandling i direktiv 2002/58. Dels udgør den en udelukkelsesgrund (med hensyn til direktivets anvendelse) for alle de af medlemsstaterne udførte aktiviteter, som specifikt »vedrører« denne. Dels udgør den en begrundelse for begrænsning – som skal gennemføres ved lov – af de i direktiv 2002/58 fastsatte rettigheder og forpligtelser, dvs. i forbindelse med aktiviteter af privat eller erhvervsmæssig art, som ikke udgør statslige aktiviteter.

19 – I henhold til artikel 2 i direktiv 2002/58 gælder i dette direktiv de definitioner, der er fastsat i direktiv 95/46. I henhold til artikel 2, litra b), i sidstnævnte direktiv forstås der ved »behandling af personoplysninger« »enhver operation eller række af operationer – med eller uden brug af elektronisk databehandling – som personoplysninger gøres til genstand for, f.eks. indsamling, registrering, systematisering, opbevaring, tilpasning eller ændring, selektion, søgning, brug, *videregivelse ved transmission*, formidling eller enhver anden *form for overladelse*, sammenstilling eller samkøring samt blokering, slettelse eller tilintetgørelse« (min fremhævelse).

78. Hvilke aktiviteter vedrører artikel 1, stk. 3, i direktiv 2002/58? Conseil d'État (øverste domstol i forvaltningsretlige sager) har efter min opfattelse givet et godt eksempel ved at nævne artikel L. 851-5 og L. 851-6 i lov om indre sikkerhed, som omhandler »teknikker til indsamling af efterretninger, som anvendes direkte af staten og ikke regulerer den virksomhed, der udøves af udbydere af elektroniske kommunikationstjenester ved at pålægge dem specifikke forpligtelser«. […]

79. Efter min opfattelse skal nøglen til at fastlægge rækkevidden af udelukkelsen fra artikel 1, stk. 3, i direktiv 2002/58 findes heri. Ordningen omfatter ikke de *aktiviteter*, der sigter mod at beskytte den nationale sikkerhed, og som de offentlige myndigheder udfører for egen regning uden behov for borgernes medvirken, og dermed uden at pålægge disse en forpligtelse i forbindelse med deres virksomhedsdrift.

80. Listen over offentlige myndigheders aktiviteter, som er undtaget fra den almindelige ordning for behandling af personoplysninger, skal imidlertid fortolkes snævert. Nærmere bestemt kan begrebet *national sikkerhed*, for hvilket den enkelte medlemsstat er eneansvarlig, jf. artikel 4, stk. 2, TEU, ikke overføres til andre mere eller mindre beslægtede områder af det offentlige liv.

[…]

82. Jeg mener […], at kriteriet i rammeafgørelse 2006/960/RIA […] kan anvendes som vejledning, for så vidt som dens artikel 2, litra a), sondrer mellem retshåndhævende myndigheder i bred forstand – idet de omfatter »en national politimyndighed, toldmyndighed eller anden myndighed, der i henhold til national lovgivning har beføjelse til at afsløre, forebygge og efterforske lovovertrædelser og kriminelle aktiviteter, udøve myndighed og foretage tvangsindgreb i forbindelse med sådanne aktiviteter« – på den ene side, og »kontorer eller enheder, der specifikt tager sig af nationale sikkerhedsspørgsmål«, på den anden. […]

[…]

84. Der findes […] en kontinuitet mellem direktiv 95/46 og direktiv 2002/58 for så vidt angår medlemsstaternes kompetencer vedrørende den nationale sikkerhed. Ingen af de to direktiver har til formål at beskytte de grundlæggende rettigheder på dette specifikke område, hvor medlemsstaternes aktiviteter ikke er »omfattet af [EU]-retten«.

85. Den »balance«, der nævnes i [11.] betragtning [til direktiv 2002/58], opstår ud fra nødvendigheden af at respektere medlemsstaternes kompetencer på området for national sikkerhed, når de udøver disse *direkte og for egen regning*. Når der derimod – selv på grundlag af de samme nationale sikkerhedshensyn – kræves medvirken fra borgere, som pålægges bestemte forpligtelser, indebærer denne omstændighed, at man begiver sig ind på et område (kravet om beskyttelse af privatlivets fred, som pålægges disse private aktører), der er omfattet af EU-retten.

86. Såvel direktiv 95/46 som direktiv 2002/58 sigter mod at opnå en sådan balance ved at tillade, at borgernes rettigheder kan begrænses ved lovgivningsmæssige foranstaltninger truffet af medlemsstaterne i henhold til henholdsvis artikel 13, stk. 1, og artikel 15, stk. 1, i de to direktiver. Der er på dette punkt ingen forskel mellem de to direktiver.

[…]

89. Identifikationen af disse offentlige myndighedsaktiviteter skal nødvendigvis være snæver, idet EU-lovgivningen på området for beskyttelse af privatlivets fred ellers vil miste sin effektive virkning. Forordning 2016/679 omhandler i sin artikel 23 – på linje med artikel 15, stk. 1, i direktiv 2002/58 – en begrænsning, *gennem lovgivningsmæssige foranstaltninger*, af de i forordningen fastsatte rettigheder og forpligtelser, når dette er nødvendigt af hensyn til bl.a.

statens sikkerhed, forsvaret eller den offentlige sikkerhed. Hvis beskyttelsen af disse målsætninger var tilstrækkelig til at fastslå en udelukkelse fra anvendelsesområdet for forordning 2016/679, ville det også her være overflødigt at påberåbe sig statens sikkerhed som begrundelse for at begrænse de ved den pågældende forordning sikrede rettigheder gennem lovgivningsmæssige foranstaltninger.«

3. Konsekvenserne af at anvende dommen i sagen Tele2 Sverige og Watson på denne sag

35. Den forelæggende ret har fokuseret på Domstolens fortolkning i dommen i sagen Tele2 Sverige og Watson og har gjort rede for de vanskeligheder, som anvendelsen af denne fortolkning på den foreliggende sag efter denne rets opfattelse medfører.

36. Dommen i sagen Tele2 Sverige og Watson angav de betingelser, som skal opfyldes af en national lovgivning, der indfører en pligt til at lagre trafik- og lokaliseringsdata med henblik på, at de offentlige myndigheder efterfølgende får adgang til dem.

37. Ligesom i de forenede sager C-511/18 og C-512/18 og af tilsvarende grunde er jeg af den opfattelse, at de nationale bestemmelser, som denne forelæggelse omhandler, ikke opfylder betingelserne efter dommen i sagen Tele2 Sverige og Watson, eftersom de indebærer en generel og udifferentieret lagring af personoplysninger, som skaber et detaljeret billede af de berørte personers liv over en længere periode.

38. I forslaget til afgørelse i disse to sager overvejer jeg, om det ville være muligt at nuancere eller supplere retspraksis efter førnævnte dom i lyset af dens konsekvenser for bekæmpelsen af terrorisme eller for beskyttelsen af staten mod andre tilsvarende trusler mod den nationale sikkerhed.

39. Jeg tillader mig også at gengive nogle af punkterne i det pågældende forslag til afgørelse, hvori jeg i det væsentlige anfører, at den nævnte retspraksis bør bekræftes i det væsentlige, selv om det er muligt at nuancere den.

»135. Om end det er vanskeligt, er det dog ikke umuligt at foretage en præcis fastlæggelse – som er i overensstemmelse med objektive kriterier – af såvel de kategorier af data, hvis lagring skønnes strengt nødvendig, som kredsen af de derved berørte personer. Det ville ganske vist være mest *praktisk og effektivt* at foretage en generel og udifferentieret lagring af alle de data, som udbyderne af elektroniske kommunikationstjenester har mulighed for at indsamle, men […] spørgsmålet [kan] ikke løses ud fra en bedømmelse af den *praktiske virkning*, men derimod *retsvirkningen* og inden for rammerne af en retsstat.

136. En sådan fastlæggelse er typisk en lovgivningsmæssig opgave inden for de rammer, der er fastsat i Domstolens praksis. […]

137. Med udgangspunkt i den forudsætning, at operatørerne har indsamlet oplysningerne på en måde, der respekterer bestemmelserne i direktiv 2002/58, og at lagringen heraf har fundet sted i overensstemmelse med direktivets artikel 15, stk. 1 […], skal de kompetente myndigheders adgang til disse oplysninger finde sted på de betingelser, som Domstolen har opstillet, og som jeg har gennemgået i forslag til afgørelse i sag C-520/18, hvortil jeg henviser.

138. En sådan national lovgivning skal således også i dette tilfælde fastsætte de materielle og processuelle betingelser for de kompetente myndigheders adgang til de lagrede data […]. I forbindelse med de foreliggende anmodninger om præjudiciel afgørelse vil det under disse betingelser være tilladt at opnå adgang til data vedrørende personer, der er mistænkt for at planlægge, ville begå, have begået eller være involveret i en terrorhandling […].

139. Det er imidlertid afgørende, at adgangen til de omhandlede data, undtagen i behørigt begrundede hastende tilfælde, er undergivet en forudgående kontrol, der foretages af enten en domstol eller en uafhængig administrativ myndighed, hvis afgørelse træffes på grundlag af en begrundet anmodning fra de kompetente myndigheder […]. I de situationer, hvor det ikke er muligt for den uafhængige myndighed at foretage en abstrakt vurdering af loven, sikres det på denne måde, at den kan foretage en *konkret* bedømmelse, hvor sikringen af statens sikkerhed og beskyttelsen af borgernes grundlæggende rettigheder iagttages på lige fod.«

B. Det andet præjudicielle spørgsmål

40. Den forelæggende ret har forelagt det andet spørgsmål i det tilfælde, at det første spørgsmål besvares bekræftende. I så fald ønsker den oplyst, hvilke »andre krav ud over kravene i EMRK« eller kravene efter dommen i sagen Tele2 Sverige og Watson der finder anvendelse.

41. Den forelæggende ret har i denne retning fastslået, at fastsættelsen af de krav, der følger af dommen i sagen Tele2 Sverige og Watson, »ville begrænse de foranstaltninger, som agenturerne træffer for at beskytte den nationale sikkerhed«.

42. Eftersom det svar, jeg foreslår med hensyn til det første spørgsmål, er benægtende, er det ikke nødvendigt at behandle det andet spørgsmål. Sidstnævnte er, således som den forelæggende ret har fremhævet, betinget af, at »[indsamlingen af] bulk-kommunikationsdata og bruge[n af] automatiserede behandlingsteknikker« med hensyn til personoplysningerne for alle brugerne i Det Forenede Kongerige, som udbyderne af elektroniske kommunikationstjenester skal overføre til agenturerne, fastslås at være forenelige med EU-retten.

43. Såfremt Domstolen anser det for nødvendigt at besvare det andet spørgsmål, bør den efter min opfattelse bekræfte de nævnte betingelser efter dommen i sagen Tele2 Sverige og Watson med hensyn til:

– forbuddet mod generel adgang til data

– kravet om en forudgående tilladelse fra en dommer eller en uafhængig myndighed for at legitimere denne adgang

– forpligtelsen til at underrette de berørte personer, medmindre dette skader effektiviteten af foranstaltningen

– lagringen af data på Unionens område.

44. Det er som nævnt tilstrækkeligt at bekræfte disse betingelser, som er ufravigelige, af de grunde, som jeg har anført i forslagene til afgørelse i de forenede sager C-511/18 og C-512/18 og i sag C-520/18, og det er ikke nødvendigt at opstille eventuelle »andre« krav, således som den forelæggende ret har nævnt.

V. Forslag til afgørelse

45. På baggrund af det ovenstående foreslår jeg, at Domstolen svarer Investigatory Powers Tribunal (domstol for efterforskningsbeføjelser, Det Forenede Kongerige) således:

»Artikel 4 TEU og artikel 1, stk. 3, 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) skal fortolkes således, at de er til hinder for en national lovgivning, der pålægger en udbyder af elektroniske kommunikationsnet en pligt til at udlevere »bulk-kommunikationsdata« til en medlemsstats sikkerheds- og efterrefatningsagenturer, som indebærer en forudgående generel og udifferentieret indsamling«.

Subsidiært:

»En medlemsstats sikkerheds- og efterretningsagenturers adgang til de data, som udbydere af elektronisk kommunikationsnet overfører, skal opfylde de betingelser, der er fastsat i dom af 21. december 2016, Tele2 Sverige og Watson (C-203/15 og C-698/15, EU:C:2016:970).«