Samling af Afgørelser

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

Forenede sager C-511/18 og C-512/18

La Quadrature du Net,
French Data Network,
Fédération des fournisseurs d'accès à Internet associatifs,
Igwan.net (sag C-511/18)
mod
Premier ministre,
Garde des Sceaux, ministre de la Justice,
Ministre de l'Intérieur,
Ministre des Armées

(anmodning om præjudiciel afgørelse indgivet af Conseil d'État (øverste domstol i forvaltningsretlige sager, Frankrig))

»Præjudiciel forelæggelse – behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor – beskyttelse af den nationale sikkerhed og bekæmpelse af terrorisme – direktiv 2002/58/EF – anvendelsesområde – artikel 1, stk. 3 – artikel 15, stk. 3 – artikel 4, stk. 2, TEU – Den Europæiske Unions charter om grundlæggende rettigheder – artikel 6, 7, 8, 11 og 47 samt artikel 52, stk. 1 – generel og udifferentieret lagring af forbindelsesdata og af data, der gør det muligt at identificere ophavsmændene til indhold – indsamling af trafik- og lokaliseringsdata – adgang til de lagrede data«

1. Domstolen har de senere år opretholdt en fast praksis med hensyn til 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 den erklærede direktiv 2006/24/EF[3] 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 (herefter »chartret«)

– 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]

1 – Originalsprog: spansk.

2 – 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 – 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).

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

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 kriminalitet og 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 skal det undersøges, i hvilket omfang de forskellige nationale lovgivninger (Det Forenede Kongeriges[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

1. Direktiv 2002/58

5. Artikel 1 (»anvendelsesområde og formål«) har følgende ordlyd:

»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 Fællesskabet.

[…]

3. Dette direktiv gælder ikke for aktiviteter, der ikke er omfattet af traktaten om oprettelse af Det Europæiske Fællesskab, 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 – Sag C-207/16 (herefter »Ministerio Fiscal-dommen«) (EU:C:2018:788).

7 – Ud over disse to (sagerne C-511/18 og C-512/18) drejer det sig om sag C-623/17, Privacy International, 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 – Forenede sager C-511/18 og C-512/18, La Quadrature du Net m.fl.

6. Artikel 3 (»omfattede tjenester«) bestemmer:

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

7. Artikel 5 (»kommunikationshemmelighed«), stk. 1, er affattet som følger:

»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 indvilliget 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.«

8. Det bestemmes i artikel 6 (»trafikdata«):

»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.«

9. Artikel 15 (»anvendelsesområdet for visse bestemmelser i direktiv 95/46/EF«)[11], stk. 1, har følgende ordlyd:

»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/EF. 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 fællesskabsrettens generelle principper, herunder principperne i EU-traktatens artikel 6, stk. 1 og 2.«

11 – Europa-Parlamentet og Rådets direktiv af 24.10.1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (EFT 1995, L 281, s. 31).

2. Direktiv 2000/31/EF[12]

10. Artikel 14 bestemmer:

»1. Medlemsstaterne sikrer, at tjenesteyderen i tilfælde af levering af en informationssamfundstjeneste, som består i oplagring af information leveret af en tjenestemodtager, ikke pådrager sig ansvar for information oplagret på anmodning af en tjenestemodtager, forudsat:

[…]

3. Denne artikel berører ikke en domstols eller en administrativ myndigheds muligheder for i overensstemmelse med medlemsstaternes retssystemer at kræve, at en tjenesteyder bringer en overtrædelse til ophør eller forhindrer den, eller medlemsstaternes muligheder for at fastlægge procedurer for at fjerne information eller hindre adgangen til den.«

11. Artikel 15 fastsætter:

»1. Med hensyn til levering af de i artikel 12, 13 og 14 omhandlede tjenester må medlemsstaterne ikke pålægge tjenesteyderne en generel forpligtelse til at overvåge den information, de fremsender eller oplagrer, eller en generel forpligtelse til aktivt at undersøge forhold eller omstændigheder, der tyder på ulovlig virksomhed.

2. Medlemsstaterne kan kræve, at leverandører af informationssamfundstjenester straks underretter de kompetente offentlige myndigheder om påståede ulovlige aktiviteter, der udøves, eller information, der leveres af deres tjenestemodtagere, eller at de på anmodning giver de kompetente myndigheder oplysninger, som gør det muligt at identificere de tjenestemodtagere, de har oplagringsaftaler med.«

3. Forordning (EU) 2016/679[13]

12. Det bestemmes i artikel 2 (»materielt anvendelsesområde«):

»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

c) som foretages af en fysisk person som led i rent personlige eller familiemæssige aktiviteter

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.

12 – Europa-Parlamentets og Rådets direktiv af 8.6.2000 om visse retlige aspekter af informationssamfundstjenester, navnlig elektronisk handel, i det indre marked (»direktivet om elektronisk handel«) (EFT 2000, L 178, s. 1).

13 – Europa-Parlamentets og Rådets forordning af 27.4.2016 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 (generel forordning om databeskyttelse) (EUT 2016, L 119, s. 1).

[…]«

13. Artikel 23 (»begrænsninger«), stk. 1, har følgende ordlyd:

»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.«

14. Det hedder i artikel 95 (»forhold til direktiv 2002/58/EF«):

»Denne forordning indfører ikke yderligere forpligtelser for fysiske eller juridiske personer for så vidt angår behandling i forbindelse med levering af offentligt tilgængelige elektroniske kommunikationstjenester i offentlige kommunikationsnet i Unionen for så vidt angår spørgsmål, hvor de er underlagt specifikke forpligtelser med samme formål som det, der er fastsat i direktiv 2002/58/EF.«

B. National ret

1. Code de la sécurité intérieure (lov om indre sikkerhed)

15. Artikel L. 851-1 bestemmer:

»Under de betingelser, som er fastsat i kapitel 1 i denne bogs afsnit II, kan indsamling tillades fra operatører inden for elektronisk kommunikation og de personer, der henvises til i artikel L. 34-1 i code des postes et des communications électroniques (lov om postvæsen og elektronisk kommunikation), samt fra de personer, der henvises til i afsnit 1 og 2 i artikel 6, stk. I, i loi nº 2004-575 […] pour la confiance dans l'économie numérique (lov nr. 2004-575 […] om tillid til den digitale økonomi) af oplysninger eller dokumenter, der er behandlet eller lagret af deres elektroniske kommunikationsnetværk eller -tjenester, herunder tekniske data vedrørende identificering af abonnementsnumre eller forbindelsesnumre til elektroniske kommunikationstjenester, opgørelse af alle en bestemt persons abonnements- eller forbindelsesnumre, lokalisering af anvendt terminaludstyr samt en abonnents kommunikationer for så vidt angår oversigten over opkaldte og opkaldende numre, varigheden af og datoen for kommunikationerne […]«

16. Artikel L. 851-2 og L. 851-4 regulerer med henblik på de forskellige formål og efter de forskellige regler den administrative adgang i realtid til de således lagrede forbindelsesdata.

17. Artikel L. 851-2 tillader alene indsamling af de oplysninger eller dokumenter, som er fastsat i artikel L. 851-1, fra de samme personer med henblik på forebyggelse af terrorisme. Sådan indsamling, som alene vedrører en eller flere personer, der på forhånd er identificeret som personer, der kan have forbindelse til en terrortrussel, foretages i realtid. Det samme gælder artikel L. 851-4, hvorefter operatører i realtid alene kan overføre tekniske data vedrørende lokaliseringen af terminaludstyr [14].

18. Artikel L. 851-3 tillader, at operatører inden for elektronisk kommunikation og udbydere af tekniske tjenester pålægges »at anvende automatiseret behandling i deres netværk med henblik på i overensstemmelse med de parametre, som præciseres i tilladelsen, at opdage forbindelser, der vil kunne afsløre en terrortrussel« [15].

19. Det fastsættes i artikel L. 851-5, at der under bestemte forudsætninger »kan tillades anvendelse af en teknisk anordning, som gør det muligt at lokalisere en person, et køretøj eller et objekt i realtid«.

20. I henhold til artikel L. 851-6, stk. I, er det under bestemte forudsætninger muligt »ved hjælp af et af de apparater eller en af de tekniske anordninger, der er nævnt i artikel 226-3, stk. 1, i code pénal [(straffeloven)], at foretage en direkte […] indsamling af de tekniske forbindelsesdata, der gør det muligt at identificere et terminaludstyr eller dets brugers abonnementsnummer, samt data vedrørende lokaliseringen af det anvendte terminaludstyr«.

14 – Ifølge den forelæggende ret pålægger disse teknikker ikke de berørte udbydere et yderligere krav om lagring i forhold til, hvad der er nødvendigt for faktureringen af tjenesteydelserne, markedsføringen heraf og leveringen af tillægstjenester.

15 – Ifølge den forelæggende ret tager denne teknik, som ikke indebærer en generel og udifferentieret lagring, udelukkende sigte på, i et begrænset tidsrum og blandt samtlige forbindelsesdata, som behandles af disse personer, at indsamle de data, der vil kunne have forbindelse til en sådan alvorlig forbrydelse.

2. Lov om postvæsen og elektronisk kommunikation

21. Følgende bestemmes i artikel L. 34-1, i den affattelse, der var gældende på tidspunktet for de faktiske omstændigheder:

»I. Denne artikel finder anvendelse på behandling af personoplysninger i forbindelse med levering af elektroniske kommunikationstjenester til offentligheden, herunder navnlig i de net, der indeholder anordninger til indsamling af oplysninger og identifikation.

II. Operatører inden for elektronisk kommunikation, og navnlig personer, hvis virksomhed består i at tilbyde adgang til offentlige onlinekommunikationstjenester, skal slette eller anonymisere samtlige trafikdata, med forbehold af bestemmelserne i stk. III, IV, V og VI.

Leverandører af elektroniske kommunikationstjenester til offentligheden skal, under iagttagelse af bestemmelserne i foregående afsnit, fastlægge interne procedurer med henblik på at efterkomme de kompetente myndigheders krav.

Personer, som gennem en erhvervsmæssig hoved- eller bibeskæftigelse offentligt udbyder en forbindelse, der giver mulighed for onlinekommunikation via adgang til nettet, herunder også vederlagsfrit, har pligt til at overholde de gældende bestemmelser for operatører inden for elektronisk kommunikation, der er fastsat i denne artikel.

III. Med henblik på at efterforske, fastslå og retsforfølge strafbare handlinger eller manglende opfyldelse af den i artikel L. 336-3 i code de la propriété intellectuelle [(lov om intellektuelle ejendomsrettigheder)] fastsatte forpligtelse, eller med henblik på at forebygge de angreb på automatiserede databehandlingssystemer, som er omhandlet og sanktioneret i straffelovens artikel 323-1 – 323-3-1, og med det ene formål i givet fald at tillade en tilrådighedsstillelse for den retslige myndighed eller øverste myndighed, som er nævnt i artikel L. 331-12 i lov om intellektuelle ejendomsrettigheder, eller for den nationale sikkerhedsmyndighed på området for informationssystemer, som er nævnt i artikel L. 2321-1 i code de la défense [(forsvarsloven)], kan de transaktioner, der har til formål at slette eller anonymisere bestemte kategorier af tekniske data, udskydes i op til et år. Et dekret efter høring af Conseil d'État [(øverste domstol i forvaltningsretlige sager)], som vedtages efter indhentelse af en udtalelse fra Commission nationale de l'informatique et des libertés [(national kommission for databehandling og frihedsrettigheder)], fastlægger, inden for de grænser, som er fastsat i stk. VI, disse kategorier af data og varigheden af deres lagring, alt efter operatørernes virksomhed og kommunikationernes karakter, samt vilkårene for eventuel godtgørelse af identificerbare og specifikke meromkostninger forbundet med de tjenester, som i denne forbindelse leveres af operatørerne på statens anmodning.

[…]

VI. De data, der lagres og behandles under de i stk. III, IV og V fastsatte betingelser, omfatter udelukkende identifikationen af brugerne af de af operatørerne leverede tjenester, de tekniske egenskaber for den kommunikation, der stilles til rådighed af sidstnævnte, og lokaliseringen af terminaludstyret.

De må i intet tilfælde omfatte indholdet af den udvekslede korrespondance eller de oplysninger, hvorom der er forespurgt – i en hvilken som helst form – i forbindelse med den pågældende kommunikation.

Lagringen og behandlingen af data skal ske under iagttagelse af bestemmelserne i lov nr. 78-17 af 6. januar 1978 om IT, arkiver og frihedsrettigheder.

Operatørerne træffer alle de nødvendige foranstaltninger med henblik på at forebygge, at disse data anvendes til andre formål end de i denne artikel fastsatte.«

22. I henhold til artikel R. 10-13, stk. I, skal operatørerne lagre følgende oplysninger af hensyn til efterforskning, afsløring og retsforfølgning af strafbare handlinger:

»a) oplysninger, der gør det muligt at fastslå brugerens identitet

b) oplysninger om det anvendte terminaludstyr

c) de tekniske kendetegn samt dato, tidspunkt og varighed af hver kommunikation

d) oplysninger vedrørende de supplerende tjenester, der er anmodet om eller anvendt, samt leverandørerne heraf

e) oplysninger, der gør det muligt at fastslå identiteten på den eller de modtagere, som kommunikationen er rettet til«.

23. I henhold til samme artikels stk. II skal operatøren i forbindelse med telefonitjenester endvidere lagre de oplysninger, der kan bidrage til at fastslå kommunikationens oprindelse og lokaliseringen heraf.

24. Det bestemmes i samme artikels stk. III, at de nævnte oplysninger skal lagres i et år, regnet fra den dato, hvor de er blevet registreret.

3. Loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (lov 2004-575 af 21.6.2004 om tillid til den digitale økonomi)

25. Det bestemmes i artikel 6, stk. II, første afsnit, i lov 2004-575 at personer, hvis virksomhed består i at tilbyde adgang til offentlige onlinekommunikationstjenester, og fysiske eller juridiske personer, der, selv vederlagsfrit, med henblik på tilrådighedsstillelse for offentligheden via offentlige onlinekommunikationstjenester varetager oplagring af signaler, skrift, billeder, lyd eller meddelelser af enhver art, der leveres af modtagere af disse tjenester, »skal lagre og opbevare oplysningerne på en sådan måde, at det er muligt at identificere enhver, der har bidraget til at skabe indholdet eller en del af indholdet af de tjenester, som de leverer«.

26. I henhold til samme artikels stk. II, tredje afsnit, kan den retslige myndighed kræve, at disse personer videregiver de i første afsnit nævnte oplysninger.

27. I henhold til sidste afsnit i stk. 2 »finder definitionen af de i første afsnit nævnte oplysninger og fastsættelsen af lagringens varighed og metode sted« ved dekret fra Conseil d'État (øverste domstol i forvaltningsretlige sager) [16].

II. De faktiske omstændigheder og de præjudicielle spørgsmål

A. Sag C-511/18

28. La Quadrature du Net, French Data Network, Igwan.net og Fédération des fournisseurs d'accès à internet associatifs (herefter »sagsøgerne«) anlagde sag ved Conseil d'État (øverste domstol i forvaltningsretlige sager) med påstand om annullation af flere forskellige gennemførelsesdekreter til visse bestemmelser i lov om indre sikkerhed [17].

29. Sagsøgerne gjorde i det væsentlige gældende, at såvel de anfægtede dekreter som de pågældende bestemmelser i lov om indre sikkerhed var i strid med retten til privatlivets fred, retten til beskyttelse af personoplysninger og retten til effektive retsmidler, som er sikret ved chartrets artikel 7, 8 og 47.

30. I denne forbindelse har Conseil d'État (øverste domstol i forvaltningsretlige sager) forelagt Domstolen følgende spørgsmål:

»1) Skal den forpligtelse til generel og udifferentieret lagring, som pålægges udbyderne på grundlag af bestemmelserne i artikel 15, stk. 1, i [direktiv 2002/58] […], i en situation, der er præget af alvorlige og vedvarende trusler mod den nationale sikkerhed og navnlig af risikoen for terror, anses for et indgreb, der er begrundet i retten til personlig sikkerhed, som er sikret ved [chartrets] artikel 6 […], og hensyn til den nationale sikkerhed, som medlemsstaterne er eneansvarlige for i medfør af artikel 4 [TEU]?

2) Skal [direktiv 2002/58] […] sammenholdt med [chartret] fortolkes således, at det tillader lovgivningsmæssige foranstaltninger, såsom foranstaltninger med henblik på indsamling i realtid af trafik- og lokaliseringsdata vedrørende bestemte personer, som ganske vist påvirker rettigheder og forpligtelser for udbydere af en elektronisk kommunikationstjeneste, men dog ikke pålægger dem en specifik forpligtelse til lagring af deres data?

16 – Definitionen blev fastsat ved décret nº 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne (dekret 2011-219 af 25.2.2011 om lagring af data, der gør det muligt at identificere enhver person, der har bidraget til at skabe indhold, der tilbydes online). Følgende kan fremhæves fra dette dekret: a) Artikel 1, stk. 1, hvorefter personer, der tilbyder adgang til onlinekommunikationstjenester, skal oplagre følgende oplysninger: forbindelsesidentifikatoren, den identifikator, der tildeles brugeren, identifikatoren for den terminal, der anvendes til forbindelsen, dato og tidspunkt for forbindelsens opstart og afslutning samt kendetegnene på abonnentlinjen. b) I henhold til artikel 1, stk. 2, skal personer, som, selv vederlagsfrit, med henblik på tilrådighedsstillelse for offentligheden via offentlige onlinekommunikationstjenester varetager oplagring af signaler, skrift, billeder, lyd eller meddelelser af enhver art, der leveres af modtagere af disse tjenester, lagre følgende data for hver transaktion: identifikatoren for forbindelsen på kommunikationens oprindelsessted, den tildelte identifikator på det indhold, der er genstand for transaktionen, de anvendte protokoltyper ved forbindelsen til tjenesten og ved overførsel af indhold, transaktionens art, dato og tidspunkt for transaktionen samt identifikatoren, som er anvendt af den, der har foretaget transaktionen. c) Endelig bestemmes det i artikel 1, stk. 3, at de i stk. 1 og 2 nævnte personer skal lagre følgende oplysninger, som er tilvejebragt af en bruger ved indgåelsen af en aftale eller oprettelsen af en konto: forbindelsesidentifikatoren ved oprettelsen af kontoen, for- og efternavne eller firmanavn, de tilknyttede postadresser, de anvendte pseudonymer, de tilknyttede e-mailadresser eller kontoadresser, telefonnumre, den opdaterede adgangskode, samt de oplysninger, der gør det muligt at kontrollere eller ændre denne.

17 – Følgende dekreter blev anfægtet: a) décret nº 2015-1885 du 28 septembre 2015 portant désignation des services spécialisés de renseignement (dekret 2015-1185 af 28.9.2015 om udpegning af specialiserede efterretningstjenester), b) décret n.º 2015-1211 du 1er octobre 2015 relatif au contentieux de la mise en oeuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État (dekret 2015-1211 af 1.10.2015 om retstvister vedrørende anvendelse af efterretningsteknikker, som kræver en tilladelse, og vedrørende datasæt af betydning for statens sikkerhed), c) décret nº 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du libre VIII du code de la sécurité intérieure (dekret 2015-1639 af 11.12.2015 om udpegelse af andre tjenester end specialiserede efterretningstjenester, som er godkendt til at anvende de teknikker, der er nævnt i afsnit V i bog VIII i lov om indre sikkerhed), og d) décret nº 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement (dekret 2016-67 af 29.1.2016 om teknikker til indsamling af efterretninger).

3) Skal [direktiv 2002/58] […] sammenholdt med [chartret] fortolkes således, at det i alle tilfælde gør retmæssigheden af procedurer til indsamling af forbindelsesdata betinget af opfyldelsen af et krav om underretning af de berørte personer, når en sådan underretning ikke længere kan skade de kompetente myndigheders efterforskning, eller kan sådanne procedurer anses for at være retmæssige, henset til samtlige øvrige eksisterende proceduremæssige garantier, idet disse sikrer, at adgangen til retsmidler er effektiv?«

B. Sag C-512/18

31. Sagsøgerne i den tvist, der ligger til grund for sag C-511/18, nedlagde, med undtagelse af Igwan.net, ligeledes påstand ved Conseil d'État (øverste domstol i forvaltningsretlige sager) om annullation af den stiltiende administrative afvisning af deres begæring om ophævelse af artikel R. 10-13 i code des postes et des communications électroniques (lov om postvæsen og elektronisk kommunikation) og af dekret 2011-219 af 25. februar 2011.

32. Efter sagsøgernes opfattelse indfører de anfægtede retsforskrifter en pligt til at lagre trafik-, lokaliserings- og forbindelsesdata, der som følge af dens generelle karakter udgør et uforholdsmæssigt indgreb i retten til respekt for privatliv og familieliv, retten til beskyttelse af personoplysninger samt ytringsfriheden, som er sikret ved chartrets artikel 7, 8 og 11, hvilket er i strid med artikel 15, stk. 1, i direktiv 2002/58.

33. I den nævnte sag har Conseil d'État (øverste domstol i forvaltningsretlige sager) forelagt følgende præjudicielle spørgsmål:

»1) Skal den forpligtelse til generel og udifferentieret lagring, som pålægges udbyderne på grundlag af bestemmelserne i artikel 15, stk. 1, i [direktiv 2002/58] […], navnlig henset til de garantier og den kontrol, som derefter er knyttet til indsamlingen og anvendelsen af disse forbindelsesdata, anses for et indgreb, der er begrundet i retten til personlig sikkerhed, som er sikret ved [chartrets] artikel 6 […], og hensyn til den nationale sikkerhed, som medlemsstaterne er eneansvarlige for i medfør af artikel 4 [TEU]?

2) Skal bestemmelserne i [direktiv 2000/31] sammenholdt med [chartrets] artikel 6, 7, 8, 11 og artikel 52, stk. 1, […] fortolkes således, at de tillader en stat at indføre en national lovgivning, der pålægger personer, hvis virksomhed består i at tilbyde adgang til offentlige onlinekommunikationstjenester, og fysiske eller juridiske personer, der, selv vederlagsfrit, med henblik på tilrådighedsstillelse for offentligheden via offentlige onlinekommunikationstjenester varetager oplagring af signaler, skrift, billeder, lyd eller meddelelser af enhver art, der leveres af modtagere af disse tjenester, at lagre data, som vil kunne gøre det muligt at identificere enhver, der har bidraget til at skabe indholdet eller en del af indholdet af de tjenester, som de leverer, for at den retslige myndighed i påkommende tilfælde kan kræve videregivelse heraf med henblik på at sikre overholdelsen af reglerne om civil- eller strafferetligt ansvar?«

III. Retsforhandlingerne for Domstolen og parternes standpunkter

34. De præjudicielle spørgsmål indgik til Domstolen den 3. august 2018.

35. Der er indgivet skriftlige indlæg af La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, French Data Network, den belgiske, den tjekkiske, den danske, den tyske og den estiske regering, Irland, den spanske, den franske, den cypriotiske, den ungarske, den polske, den svenske og Det Forenede Kongeriges regering samt Kommissionen.

36. Den 9. september 2019 blev der afholdt et offentligt retsmøde i fællesskab for den foreliggende sag, sag C-623/17, Privacy International, og sag C-520/18, Ordre des barreaux francophones et germanophone m.fl., med deltagelse af parterne i de fire præjudicielle procedurer, de ovennævnte regeringer og den nederlandske og den norske regering samt Kommissionen og Den Europæiske Tilsynsførende for Databeskyttelse.

IV. Bedømmelse

37. Spørgsmålene fra Conseil d'État (øverste domstol i forvaltningsretlige sager) kan inddeles i tre grupper:

– for det første, om en national lovgivning, hvorefter udbyderne af elektroniske kommunikationstjenester pålægges en forpligtelse til generel og udifferentieret lagring af forbindelsesdata (det første spørgsmål i sag C-511/18 og i sag C-512/18), og navnlig af de data, der gør det muligt at identificere ophavsmændene til det indhold, der leveres af disse udbydere (det andet spørgsmål i sag C-512/18), er forenelig med EU-retten

– for det andet, om retmæssigheden af procedurer til indsamling af forbindelsesdata i alle tilfælde er betinget af opfyldelsen af et krav om underretning af de berørte personer, når en sådan underretning ikke kan skade efterforskningen (det tredje spørgsmål i sag C-511/18)

– for det tredje, om indsamling i realtid af trafik- og lokaliseringsdata, uden pligt til lagring heraf, er forenelig – og under hvilke betingelser – med direktiv 2002/58 (det andet spørgsmål i sag C-511/18).

38. Det handler kort sagt om at fastslå, hvorvidt en national lovgivning er forenelig med EU-retten, når den pålægger udbyderne af elektroniske kommunikationstjenester to typer forpligtelser: a) dels *indsamling* af bestemte data, men ikke lagring heraf, og b) dels *lagring* af forbindelsesdata og af data, der gør det muligt at identificere ophavsmændene til indholdet af de tjenester, som de pågældende udbydere leverer.

39. Forud herfor er det nødvendigt at tage stilling til, om direktiv 2002/58 finder anvendelse, netop i betragtning af den situation [18], der ligger til grund for vedtagelsen af den pågældende nationale lovgivning (dvs. under omstændigheder, hvor den nationale sikkerhed kan være i fare).

A. Spørgsmålet, om direktiv 2002/58 finder anvendelse

40. Den forelæggende ret har antaget, at den omtvistede lovgivning er omfattet af anvendelsesområdet for direktiv 2002/58. Således fremgår det efter dens opfattelse af retspraksis fra dommen i sagen Tele2 Sverige og Watson, som blev bekræftet ved Ministerio Fiscal-dommen.

41. Nogle af de regeringer, som har indgivet indlæg i sagen, har derimod gjort gældende, at den omtvistede lovgivning ikke er omfattet af det nævnte anvendelsesområde. Til støtte for deres standpunkt har de, blandt andre argumenter, henvist til dom af 30. maj 2006, Parlamentet mod Rådet og Kommissionen [19].

18 – »En situation […] [med] alvorlige og vedvarende trusler mod den nationale sikkerhed og navnlig af risikoen for terror«, således som det er anført i det første spørgsmål i sag C-511/18.

19 – Forenede sager C-317/04 og C-318/04 (EU:C:2006:346) (herefter »dommen i sagen Parlamentet mod Rådet og Kommissionen«).

42. Jeg er enig med Conseil d'État (øverste domstol i forvaltningsretlige sager) i, at dommen i sagen Tele2 Sverige og Watson har afgjort denne del af debatten, for så vidt som den har bekræftet, at direktiv 2002/58 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.

43. Jeg skal allerede nu bemærke, at såfremt der måtte foreligge uoverensstemmelser mellem dommen i sagen Tele2 Sverige og Watson og de forudgående domme, vil førstnævnte dom have forrang, eftersom den er nyere og er blevet bekræftet ved Ministerio Fiscal-dommen. Jeg mener imidlertid ikke, at der foreligger en sådan uoverensstemmelse, således som jeg vil forsøge at gøre rede for i det følgende.

1. Dommen i sagen Parlamentet mod Rådet og Kommissionen

44. De sager, der blev afgjort ved dommen i sagen Parlamentet mod Rådet og Kommissionen, omhandlede følgende:

– aftalen mellem Det Europæiske Fællesskab og Amerikas Forenede Stater om luftfartsselskabers behandling og overførsel af PNR-oplysninger [Passenger Name Records (passageroplysninger)] til de amerikanske myndigheder [20]

– tilstrækkelig beskyttelse af personoplysninger, der er indeholdt i registre over flypassagerer, og som videregives til disse myndigheder [21].

45. Domstolen fastslog, at overførslen af disse oplysninger udgjorde en behandling, der vedrørte den offentlige sikkerhed og statens aktiviteter på det strafferetlige område. I henhold til artikel 3, stk. 2, første led, i direktiv 95/46 var de to omtvistede beslutninger ikke omfattet af anvendelsesområdet for direktiv 95/46.

46. Oplysningerne blev i første omgang indsamlet af luftfartsselskaberne som led i en aktivitet – salg af flybilletter – der er underlagt EU-retten. Behandlingen heraf som omhandlet i den omtvistede beslutning er imidlertid ikke nødvendig »for at levere en tjenesteydelse, men [en] behandling, som anses for nødvendig for at beskytte den offentlige sikkerhed og for at nå retshåndhævende mål« [22].

20 – Rådets afgørelse 2004/496/EF af 17.5.2004 om indgåelse af en aftale mellem Det Europæiske Fællesskab og Amerikas Forenede Stater om luftfartsselskabers behandling og overførsel af PNR-oplysninger til United States Department of Homeland Security, Bureau of Customs and Border Protection (EUT 2004, L 183, s. 83, berigtiget i EUT 2005, L 255, s. 168) (sag C-317/04).

21 – Kommissionens beslutning 2004/535/EF af 14.5.2004 om tilstrækkelig beskyttelse af personoplysninger, der er indeholdt i registre over flypassagerer, og som videregives til Amerikas Forenede Staters told- og grænsekontrolmyndighed (EUT 2004, L 235, s. 11) (sag C-318/04).

22 – Dommen i sagen Parlamentet mod Rådet og Kommissionen, præmis 57. Det bemærkes i præmis 58, at den »omstændighed, at […] oplysningerne er blevet indsamlet af private erhvervsdrivende til kommercielle formål, og at det er disse erhvervsdrivende, som forestår oplysningernes videregivelse til en tredjestat«, ikke indebærer, at denne overførsel ikke er omfattet af et af de undtagelsestilfælde for anvendelsen af direktiv 95/46, der er opregnet i direktivets artikel 3, stk. 2, første led, eftersom »[v]ideregivelsen sker […] inden for rammer, der er indført af de statslige myndigheder, og som vedrører den offentlige sikkerhed«.

47. Domstolen fulgte således en teleologisk fremgangsmåde, idet den tog udgangspunkt i det med databehandlingen forfulgte formål: Eftersom databehandlingen havde til formål at opnå beskyttelse af den offentlige sikkerhed, måtte den anses for at ligge uden for anvendelsesområdet for direktiv 95/46. Dette formål var imidlertid ikke det eneste afgørende kriterium [23], hvorfor det i dommen blev fremhævet, at det »sker nemlig inden for rammer, der er indført af de statslige myndigheder, og som vedrører den offentlige sikkerhed« [24].

48. Dommen i sagen Parlamentet mod Rådet og Kommissionen gør det således muligt at sondre mellem undtagelsesklausulen og begrænsningsklausulerne i direktiv 95/46 (som er analoge med klausulerne i direktiv 2002/58). Det er imidlertid korrekt, at begge disse typer af klausuler henviser til almene hensyn, som er ensartede, hvilket bidrager til, at deres rækkevidde sammenblandes med hinanden, således som generaladvokat Bot i sin tid bemærkede [25].

49. Denne sammenblanding ligger formentlig til grund for den antagelse, der forsvares af de medlemsstater, som taler for, at direktiv 2002/58 ikke finder anvendelse i denne sammenhæng. Efter deres opfattelse kan hensynet til national sikkerhed alene beskyttes gennem den undtagelse, der er omhandlet i artikel 1, stk. 3, i direktiv 2002/58. Det forholder sig imidlertid således, at dette hensyn ligeledes finder beskyttelse i de begrænsninger, der tillades i samme direktivs artikel 15, stk. 1, herunder begrænsningen vedrørende den nationale sikkerhed. Sidstnævnte bestemmelse ville være overflødig, hvis direktiv 2002/58 viste sig at være uanvendelig i forbindelse med en hvilken som helst påberåbelse af national sikkerhed.

2. Dommen i sagen Tele2 Sverige og Watson

50. I dommen i sagen Tele2 Sverige og Watson blev der taget stilling til, om visse nationale ordninger var forenelige med EU-retten, når de pålagde udbyderne af offentligt tilgængelige elektroniske kommunikationstjenester en generel forpligtelse til at lagre data vedrørende den pågældende kommunikation. Omstændighederne var således i det væsentlige identiske med de omstændigheder, der skal bedømmes i de nærværende anmodninger om præjudiciel afgørelse.

51. Efter atter at være blevet forelagt spørgsmålet om EU-rettens anvendelighed – denne gang blot med hensyn til anvendelsesområdet for direktiv 2002/58 – indledte Domstolen med at bemærke, at »rækkevidden af anvendelsesområdet for direktiv 2002/58 skal fastlægges under hensyntagen til bl.a. den generelle opbygning af direktivet« [26].

23 – Således bemærkede den savnede generaladvokat Bot sidenhen i sit forslag til afgørelse Irland mod Parlamentet og Rådet (C-301/06, EU:C:2008:558). Han bemærkede, at dommen i sagen Parlamentet mod Rådet og Kommissionen »ikke [kan] forstås på den måde, at kun en undersøgelse af det formål, der forfølges med behandling af personoplysninger, er relevant for, om en sådan behandling er omfattet af anvendelsesområdet for det system til beskyttelse af data, som er indført ved direktiv 95/46. Det må også undersøges, hvilken form for virksomhed behandlingen af data foretages inden for rammerne af. Kun såfremt denne behandling foretages med henblik på udøvelse af statens eller statslige myndigheders aktiviteter og ikke har noget at gøre med området for den enkelte borgers aktiviteter, er den udelukket fra det fællesskabssystem for beskyttelse af personoplysninger, som er indført ved direktiv 95/46, nemlig i medfør af dette direktivs artikel 3, stk. 2, første led« (punkt 122).

24 – Dommen i sagen Parlamentet mod Rådet og Kommissionen, præmis 58. Aftalen havde som hovedformål at stille krav til de luftfartsselskaber, der udøver passagerbefordring mellem Den Europæiske Union og USA, om at give de nordamerikanske myndigheder elektronisk adgang til de PNR-oplysninger, der findes i deres elektroniske reservations- og afgangskontrolsystemer. Den indførte således en metode til internationalt samarbejde mellem Den Europæiske Union og USA med henblik på bekæmpelse af terrorisme og andre alvorlige forbrydelser, i et forsøg på at forene dette formål med formålet om beskyttelse af passagerernes personlige oplysninger. I denne sammenhæng adskilte den forpligtelse, der pålagdes selskaberne, sig ikke væsentligt fra en direkte udveksling af oplysninger mellem offentlige myndigheder.

25 – Generaladvokat Bots forslag til afgørelse Irland mod Parlamentet og Rådet (C-301/06, EU:C:2008:558, punkt 127).

26 – Dommen i sagen Tele2 Sverige og Watson, præmis 67.

52. I denne sammenhæng bemærkede Domstolen, at »[d]e i artikel 15, stk. 1, i direktiv 2002/58 fastsatte retsforskrifter vedrører ganske vist statens eller statslige myndigheders aktiviteter og har ikke noget at gøre med området for den enkelte borgers aktiviteter […] De formål, som sådanne foranstaltninger skal opfylde i medfør af denne bestemmelse – i det foreliggende tilfælde beskyttelse af den nationale sikkerhed […], kan endvidere i det væsentlige sammenholdes med de formål, der forfølges med de i direktivets artikel 1, stk. 3, omhandlede aktiviteter« [27].

53. Formålet med de foranstaltninger, som medlemsstaterne i henhold til artikel 15, stk. 1, i direktiv 2002/58 kan iværksætte med henblik på at begrænse retten til privatlivets fred, kan således (på dette punkt) sammenholdes med det formål, der kan begrunde fritagelsen af bestemte statslige aktiviteter fra direktivets anvendelsesområde, jf. direktivets artikel 1, stk. 3.

54. Domstolen fandt imidlertid, at dette forhold, »[h]enset til den generelle opbygning af direktiv 2002/58«, ikke gjorde det muligt »at fastslå, at de retsforskrifter, som er omhandlet i artikel 15, stk. 1, i direktiv 2002/58, er udelukket fra direktivets anvendelsesområde, idet denne bestemmelse ellers ville blive frataget enhver effektiv virkning. Den nævnte bestemmelse forudsætter nemlig nødvendigvis, at de heri omhandlede nationale foranstaltninger […] er omfattet af direktivets anvendelsesområde, idet det udtrykkeligt fremgår af direktivet, at medlemsstaterne kun må vedtage dem under iagttagelse af de i direktivet fastsatte betingelser« [28].

55. Endvidere blev det tilføjet, at de begrænsninger, der tillades ved artikel 15, stk. 1, i direktiv 2002/58, regulerer »den virksomhed, som udøves af udbydere af elektroniske kommunikationstjenester«, »med de i bestemmelsen fastsatte formål for øje«. Nævnte bestemmelse, sammenholdt med direktivets artikel 3, »skal derfor fortolkes således, at sådanne retsforskrifter er omfattet af direktivets anvendelsesområde« [29].

56. Følgelig fastslog Domstolen, at anvendelsesområdet for direktiv 2002/58 omfatter såvel en retsforskrift, der pålægger udbyderne »at lagre trafikdata og lokaliseringsdata, idet en sådan virksomhed nødvendigvis indebærer, at udbyderne behandler personoplysninger« [30], som en retsforskrift, der vedrører myndighedernes adgang til de data, der lagres af disse udbydere [31].

57. Domstolens fortolkning af direktiv 2002/58 i dommen i sagen Tele2 Sverige og Watson blev gentaget i Ministerio Fiscal-dommen.

58. Kan det fastslås, at dommen i sagen Tele2 Sverige og Watson afspejler et – mere eller mindre implicit – vendepunkt i forhold til retspraksis fra dommen i sagen Parlamentet mod Rådet og Kommissionen? Denne antagelse deles f.eks. af Irland, idet det efter denne medlemsstats opfattelse kun er retspraksis fra sidstnævnte dom, som er forenelig med retsgrundlaget for direktiv 2002/58, og som er i overensstemmelse med artikel 4, stk. 2, TEU [32].

59. Den franske regering er af den opfattelse, at modsætningsforholdet vil kunne undgås, hvis man betænker, at retspraksis fra dommen i sagen Tele2 Sverige og Watson omhandler medlemsstaternes aktiviteter inden for det strafferetlige område, mens retspraksis fra dommen i sagen Parlamentet mod Rådet og Kommissionen vedrører statens sikkerhed og forsvaret. Dermed ville retspraksis fra dommen i sagen Tele2 Sverige og Watson ikke finde anvendelse på det foreliggende tilfælde, hvor der i stedet ville skulle henses til resultatet fra dommen i sagen Parlamentet mod Rådet og Kommissionen [33].

27 – Ibidem, præmis 72.

28 – Ibidem, præmis 73.

29 – Ibidem, præmis 74.

30 – Ibidem, præmis 75.

31 – Ibidem, præmis 76.

32 – Punkt 15 og 16 i Irlands skriftlige indlæg.

33 – Punkt 34-50 i den franske regerings skriftlige indlæg.

60. Som jeg allerede har bemærket, er det efter min opfattelse muligt at finde en anden metode til integration mellem de to domme end den af den franske regering foreslåede. Jeg er ikke enig i den sidstnævnte antagelse, eftersom de betragtninger i dommen i sagen Tele2 Sverige og Watson, som specifikt omhandler bekæmpelsen af terrorisme [34], efter min opfattelse kan overføres på en hvilken som helst anden trussel mod den nationale sikkerhed (hvoraf terrorisme blot er én ud af flere).

3. Muligheden for at foretage en helhedsfortolkning af dommen i sagen Parlamentet mod Rådet og Kommissionen og dommen i sagen Tele2 Sverige og Watson

61. Efter min opfattelse tog Domstolen i dommen i sagen Tele2 Sverige og Watson og Ministerio Fiscal-dommen hensyn til undtagelsesklausulernes og begrænsningsklausulernes eksistensgrundlag samt det systematiske forhold mellem de to typer klausuler.

62. Når Domstolen i dommen i sagen Parlamentet mod Rådet og Kommissionen fastslog, at databehandlingen lå uden for anvendelsesområdet for direktiv 95/46, skyldtes dette som nævnt, at det i forbindelse med samarbejdet mellem Den Europæiske Union og USA, dvs. inden for en typisk international ramme, bør være aktivitetens statslige dimension, der har forrang i forhold til den omstændighed, at den pågældende behandling ligeledes omfatter en erhvervsmæssig eller privat dimension. Et af de rejste spørgsmål i den pågældende sag omhandlede netop den rette hjemmel for den omtvistede beslutning.

63. Med hensyn til de nationale foranstaltninger, der blev undersøgt i dommen i sagen Tele2 Sverige og Watson og i Ministerio Fiscal-dommen, fokuserede Domstolen derimod på den interne rækkevidde af databehandlingen: Behandlingen fandt sted inden for rent nationale lovgivningsmæssige rammer, og derfor savnedes den eksterne dimension, som kendetegnede genstanden for dommen i sagen Parlamentet mod Rådet og Kommissionen.

64. Den forskellige vægtning af den internationale og den nationale (erhvervsmæssige og private) dimension af databehandlingen resulterede i, at den EU-retlige undtagelsesklausul i det førstnævnte tilfælde blev anset for at være bedst egnet til at beskytte den almene interesse bestående i den nationale sikkerhed. I det andet tilfælde kunne den samme interesse derimod beskyttes effektivt ved hjælp af begrænsningsklausulen i artikel 15, stk. 1, i direktiv 2002/58.

65. Der skulle ligeledes tages stilling til en anden uoverensstemmelse i forbindelse med de forskellige lovgivningsmæssige sammenhænge: Der blev i disse domme foretaget en fortolkning af to retsforskrifter, som på trods af deres umiddelbare lighed ikke er identiske.

66. I dommen i sagen Parlamentet mod Rådet og Kommissionen tog Domstolen således stilling til fortolkningen af artikel 3, stk. 2, i direktiv 95/46, mens den i dommen i sagen Tele2 Sverige og Watson udtalte sig om artikel 1, stk. 3, i direktiv 2002/58. Efter en nærlæsning af disse bestemmelser står det klart, at der er tilstrækkelige forskelle til at begrunde Domstolens forskelligrettede udtalelser i de to domme.

67. I henhold til artikel 3, stk. 2, i direktiv 95/46 gælder »[d]ette direktiv […] *ikke for sådan behandling af personoplysninger* […] som iværksættes med henblik på udøvelse af aktiviteter, der ikke er omfattet af fællesskabsretten […] 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« [35].

34 – Dommen i sagen Tele2 Sverige og Watson, præmis 103 og 119.

35 – Min fremhævelse.

68. I henhold til artikel 1, stk. 3, i direktiv 2002/58 gælder dette direktiv derimod »*ikke for aktiviteter*, der ikke er omfattet af traktaten om oprettelse af Det Europæiske Fællesskab […], 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« [36].

69. Mens artikel 3, stk. 2, i direktiv 95/46 udelukker den *behandling af oplysninger*, som – for så vidt det er relevant for denne sag – vedrører statens sikkerhed, vedrører artikel 1, stk. 3, i direktiv 2002/58 de *aktiviteter*, der – ligeledes af interesse for denne sag – har til formål at beskytte statens sikkerhed.

70. Forskellen er ikke ubetydelig. Direktiv 95/46 udelod en aktivitet, som enhver kan udføre, fra sit anvendelsesområde (»behandling af personoplysninger«). Behandlinger, som bl.a. vedrørte statens sikkerhed, blev udtrykkeligt undtaget fra denne aktivitet. Karakteren af det *subjekt*, der måtte udføre behandlingen af oplysningerne, havde derimod ingen betydning. Den fremgangsmåde, der blev anvendt til at identificere de udelukkede aktiviteter, var således teleologisk eller formålsbestemt, uden sondring mellem personer for så vidt angik deres aktører.

71. Det vil altså sige, at Domstolen i sagen Parlamentet mod Rådet og Kommissionen først og fremmest beskæftigede sig med formålet med behandlingen af oplysninger. »[D]en omstændighed, at […] oplysningerne er blevet indsamlet af private erhvervsdrivende til kommercielle formål, og at det er disse erhvervsdrivende, som forestår oplysningernes videregivelse til en tredjestat«, havde ingen betydning, eftersom det afgørende var, at »[v]ideregivelsen sker […] inden for rammer, der er indført af de statslige myndigheder, og som vedrører den offentlige sikkerhed« [37].

72. Derimod kan »aktiviteter, der vedrører den offentlige sikkerhed«, og som ligger uden for anvendelsesområdet for direktiv 2002/58, som blev undersøgt i sagen Tele2 Sverige og Watson, ikke udføres af et hvilket som helst subjekt, men derimod alene af selve staten. Endvidere omfatter disse aktiviteter ikke statens lovgivningsmæssige eller regeludstedende funktioner, men alene de offentlige myndigheders materielle handlinger.

73. De *aktiviteter*, der er opregnet i artikel 1, stk. 3, i direktiv 2002/58, er under alle omstændigheder »statens eller statslige myndigheders aktiviteter og har ikke noget at gøre med området for den enkelte borgers aktiviteter« [38]. Disse »aktiviteter« kan imidlertid ikke være af lovgivningsmæssig art. Hvis dette var tilfældet, ville ingen af de retsforskrifter, der vedtages af medlemsstaterne i forbindelse med behandling af personoplysninger, være omfattet af direktiv 2002/58, uanset om de blev begrundet i hensynet til statens sikkerhed.

74. Dels ville det indebære en betydelig svækkelse af direktivets effektive virkning, eftersom påberåbelsen af et så ubestemt retligt begreb som den nationale sikkerhed ville være tilstrækkelig til, at de af EU-lovgiver udtænkte foranstaltninger til beskyttelse af borgernes personoplysninger ikke ville kunne anvendes over for medlemsstaterne. En sådan beskyttelse er praktisk umulig uden medlemsstaternes medvirken, og borgerens garanti herfor sikres ligeledes over for de nationale offentlige myndigheder.

36 – Min fremhævelse.

37 – Dommen i sagen Parlamentet mod Rådet og Kommissionen, præmis 58.

38 – Ministerio Fiscal-dommen, præmis 32. Jf. i samme retning dommen i sagen Tele2 Sverige og Watson, præmis 72.

75. Dels ville en fortolkning af begrebet »statslige aktiviteter«, som omfattede de aktiviteter, der fører til vedtagelsen af retlige bestemmelser og regler, berøve meningen med artikel 15 i direktiv 2002/58, som netop giver medlemsstaterne beføjelse til – af hensyn til beskyttelsen af bl.a. den nationale sikkerhed – at vedtage »retsforskrifter« med det formål at begrænse rækkevidden af visse af de af samme direktiv omfattede rettigheder og forpligtelser [39].

76. Som Domstolen bemærkede i sagen Tele2 Sverige og Watson, skal »rækkevidden af anvendelsesområdet for direktiv 2002/58 […] fastlægges under hensyntagen til bl.a. den generelle opbygning af direktivet« [40]. Ud fra dette perspektiv er en fortolkning af artikel 1, stk. 3, og artikel 15, stk. 1, i direktiv 2002/58, som giver disse bestemmelser mening, uden at de mister deres effektive virkning, en fortolkning, hvorved der – for så vidt angår den første af disse bestemmelser – identificeres en materiel undtagelse med hensyn til de af medlemsstaterne udførte *aktiviteter* på området for national sikkerhed (og tilsvarende områder), og – i det andet tilfælde – en beføjelse til at vedtage *retsforskrifter* (dvs. lovbestemmelser med generel virkning), som ud fra et hensyn til den nationale sikkerhed har indvirkning på de aktiviteter, der udføres af borgere, der er underlagt medlemsstaternes lovgivning, og dermed indskrænker de ved direktiv 2002/58 sikrede rettigheder.

4. Udelukkelse af den nationale sikkerhed i direktiv 2002/58

77. Den nationale sikkerhed (eller det synonyme udtryk »statens sikkerhed«, der anvendes i direktivets artikel 15, stk. 1) 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 [41].

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« [42].

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.

39 – Det vil således vanskeligt kunne anføres, at artikel 15, stk. 1, i direktiv 2002/58 tillader en begrænsning af de fastsatte rettigheder og forpligtelser, som direktivet sikrer, på et område, der – som det er tilfældet med den nationale sikkerhed – i princippet ligger uden for dets anvendelsesområde i henhold til samme direktivs artikel 1, stk. 3. Domstolen fastslog således i dommen i sagen Tele2 Sverige og Watson, præmis 73, at artikel 15, stk. 1, i direktiv 2002/58 »nødvendigvis [forudsætter], at de heri omhandlede nationale foranstaltninger […] er omfattet af direktivets anvendelsesområde, idet det udtrykkeligt fremgår af direktivet, at medlemsstaterne kun må vedtage dem under iagttagelse af de i direktivet fastsatte betingelser«.

40 – Dommen i sagen Tele2 Sverige og Watson, præmis 67.

41 – Som generaladvokat Saugmandsgaard Øe tilfældigt bemærkede i sit forslag til afgørelse Ministerio Fiscal (C-207/16, EU:C:2018:300, punkt 47), er det »vigtigt ikke at forveksle dels de personoplysninger, der behandles *direkte* som et led i de statslige aktiviteter, som en stat udøver inden for det strafferetlige område, dels de personoplysninger, der behandles som et led i kommercielle aktiviteter, der udøves af en udbyder af elektroniske kommunikationstjenester, som de kompetente statslige myndigheder *efterfølgende* anvender«.

42 – Præmis 18 og 21 i forelæggelsesafgørelsen i sag C-511/18.

81. Da der i de foreliggende præjudicielle sager er tale om borgeres medvirken (dvs. dem, der udbyder elektroniske kommunikationstjenester til brugerne), og der således ikke blot er tale om statslige myndigheders handlinger, er det ikke nødvendigt at tage stilling til afgrænsningen af den nationale sikkerhed i snæver forstand.

82. Jeg mener imidlertid, at kriteriet i rammeafgørelse 2006/960/RIA [43] 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 [44].

83. Det bemærkes i 11. betragtning til direktiv 2002/58, at direktivet »[l]igesom direktiv 95/46/EF […] ikke [finder] anvendelse på beskyttelse af grundlæggende rettigheder og frihedsrettigheder, der er forbundet med aktiviteter, der ikke er omfattet af [EU-]retten«. Direktiv 2002/58 »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 […] statens sikkerhed […]«.

84. Der findes således 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 ovennævnte betragtning, 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.

87. For så vidt angår forordning 2016/679, hvorved der indføres (nye) generelle rammebestemmelser for beskyttelse af personoplysninger, fastsættes det i artikel 2, stk. 2, at forordningen ikke gælder for »behandling af personoplysninger«, når medlemsstaterne »udfører aktiviteter, der falder inden for rammerne af afsnit V, kapitel 2, i TEU«.

43 – Rådets rammeafgørelse af 18.12.2016 om forenkling af udvekslingen af oplysninger og efterretninger mellem medlemsstaternes retshåndhævende myndigheder (EUT 2006, L 386, s. 89).

44 – På linje hermed blev det i artikel 1, stk. 4, i Rådets rammeafgørelse 2008/977/RIA af 27.11.2008 om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager (EUT 2008, L 350, s. 60) fastsat, at rammeafgørelsen »ikke [berører] væsentlige nationale sikkerhedsinteresser og specifikke efterretningsaktiviteter vedrørende national sikkerhed«.

88. På samme måde som behandlingen af personoplysninger i direktiv 95/46 alene blev kvalificeret ud fra dens formål, uden at tage hensyn til hvem der foretog behandlingen, identificeres de behandlinger, der udelukkes, i forordning 2016/679 både ud fra deres formål og ud fra, hvem der foretager dem: Forordningen udelukker de behandlinger, der foretages af medlemsstaterne under udøvelse af *aktiviteter*, der falder uden for EU-retten [artikel 2, stk. 2, litra a) og b)], og dem, der foretages af myndighederne *med henblik på bekæmpelse af strafbare handlinger samt forebyggelse* af trusler mod den offentlige sikkerhed[45].

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.

90. Ligesom det er tilfældet med direktiv 2002/58, ville det ikke være sammenhængende, at de i artikel 23 i forordning 2016/679 omhandlede lovgivningsmæssige foranstaltninger (der som nævnt tillader statslige begrænsninger af borgernes ret til privatlivets fred af hensyn til statens sikkerhed) falder ind under forordningens anvendelsesområde, og at beskyttelsen af statens sikkerhed samtidig og uden videre gør samme forordning uanvendelig, hvilket ville indebære en mangel på anerkendelse af enhver subjektiv rettighed.

B. Bekræftelse og muligheder for udvikling af retspraksis fra dommen i sagen Tele2 Sverige og Watson

91. I mit forslag til afgørelse i sag C-520/18 har jeg foretaget en detaljeret analyse[46] af Domstolens praksis på dette område, på baggrund af hvilken jeg foreslår en bekræftelse heraf, samtidig med at jeg foreslår en fortolkning, der kan bidrage til en nuancering af dens indhold.

92. Jeg henviser til denne analyse, som jeg af rent pladsmæssige hensyn ikke finder tvingende nødvendig at gengive her. De betragtninger, som jeg vil fremsætte nedenfor vedrørende de af Conseil d'Etat (øverste domstol i forvaltningsretlige sager) rejste præjudicielle spørgsmål, skal således læses under iagttagelse af de tilsvarende afsnit i forslag til afgørelse i sag C-520/18.

C. Besvarelse af de præjudicielle spørgsmål

1. Pligten til at lagre data (det første præjudicielle spørgsmål i sagerne C-511/18 og C-512/18 og det andet præjudicielle spørgsmål i sag C-512/18)

93. Med hensyn til den pligt til at lagre data, som pålægges udbyderne af elektroniske kommunikationstjenester, ønsker den forelæggende ret konkret oplyst,

45 – Forordning 2016/679 udelukker således de behandlinger af oplysninger, der foretages af medlemsstaterne under udøvelse af *aktiviteter*, der falder uden for EU-retten, samt dem, der foretages af myndighederne *med henblik på beskyttelse* af den offentlige sikkerhed.

46 – Punkt 27-68.

– om denne forpligtelse, som pålægges i henhold til artikel 15, stk. 1, i direktiv 2002/58, udgør et indgreb, der er begrundet i »retten til personlig sikkerhed«, som er sikret ved chartrets artikel 6, og hensyn til den nationale sikkerhed (det første spørgsmål i sagerne C-511/18 og C-512/18 samt det tredje spørgsmål i sag C-511/18)

– om direktiv 2000/31 tillader en lagring af data, som vil kunne gøre det muligt at identificere enhver, der har bidraget til at skabe det offentligt tilgængelige onlineindhold (det andet spørgsmål i sag C-512/18).

a) Indledende betragtning

94. Conseil d'État (øverste domstol i forvaltningsretlige sager) har henvist til de grundlæggende rettigheder, som er sikret ved chartrets artikel 7 (respekt for privatliv og familieliv), artikel 8 (beskyttelse af personoplysninger) og artikel 11 (ytrings- og informationsfrihed). Det er netop disse rettigheder, der efter Domstolens opfattelse kan blive påvirket af den pligt til at lagre trafikdata, som de nationale myndigheder pålægger udbyderne af elektroniske kommunikationstjenester [47].

95. Den forelæggende ret har ligeledes henvist til den ved chartrets artikel 6 sikrede ret til sikkerhed. Snarere end som en ret, der muligvis bliver påvirket, har den gjort den gældende som en faktor, der vil kunne begrunde pålæggelsen af den pågældende forpligtelse.

96. Jeg er enig med Kommissionen i, at en påberåbelse af artikel 6 under disse omstændigheder kan vise sig at være tvivlsom. Jeg er ligesom Kommissionen af den opfattelse, at bestemmelsen ikke skal fortolkes således, at den er egnet »til at pålægge Unionen en positiv forpligtelse til at træffe foranstaltninger til beskyttelse af befolkningen mod kriminelle handlinger« [48].

97. Den sikkerhed, der garanteres ved den pågældende bestemmelse i chartret, er ikke identisk med den offentlige sikkerhed. Sagt på en anden måde har den lige så meget at gøre med sidstnævnte sikkerhed som en hvilken som helst anden grundlæggende rettighed, eftersom den offentlige sikkerhed er en uomgængelig betingelse for at kunne nyde godt af de grundlæggende rettigheder og frihedsrettigheder.

98. Som Kommissionen har bemærket, svarer chartrets artikel 6 til artikel 5 i Den Europæiske Menneskerettighedskonvention (herefter »EMRK«), således som det bekræftes i de ledsagende forklaringer. Det fremgår af EMRK's artikel 5, at den »sikkerhed«, der garanteres ved denne bestemmelse, alene er den personlige sikkerhed, forstået som sikring af retten til fysisk frihed over for ubegrundet anholdelse eller frihedsberøvelse. Kort sagt sikkerheden for, at ingen kan berøves deres frihed, bortset fra i de tilfælde, under de forudsætninger og i overensstemmelse med de procedurer, som foreskrives ved lov.

99. Der er således tale om den *personlige sikkerhed*, set i forhold til de betingelser, hvorunder personers fysiske frihed kan begrænses [49], og ikke den *offentlige sikkerhed*, der er knyttet til eksistensen af en stat, hvilket i et udviklet samfund er en uomgængelig forudsætning for at kunne forene udøvelsen af de offentlige beføjelser med udøvelsen af de individuelle rettigheder.

47 – Jf. dommen i sagen Tele2 Sverige og Watson, præmis 92, hvori der er en analog henvisning til Digital Rights-dommen, præmis 25 og 70.

48 – Punkt 37 i Kommissionens skriftlige indlæg.

49 – Således er det blevet fortolket af Menneskerettighedsdomstolen. Jf. dom af 5.7.2016, Buzadji mod Republikken Moldova (CE:ECHR:2016:0705JUD002375507), hvor det i § 84 blev fastslået, at den grundlæggende målsætning med den ved EMRK's artikel 5 sikrede rettighed er at forebygge ubegrundet eller uberettiget personlig frihedsberøvelse.

100. Nogle af regeringerne har imidlertid anført, at der bør tages mere hensyn til retten til sikkerhed i sidstnævnte forstand. I virkeligheden har Domstolen ikke set bort herfra, men har faktisk nævnt det udtrykkeligt i sine domme [50] og udtalelser [51]. Den har aldrig afvist betydningen af de almennyttige mål om beskyttelse af den nationale sikkerhed og offentlige orden [52], om bekæmpelse af international terrorisme med henblik på opretholdelse af international fred og sikkerhed og om bekæmpelse af grov kriminalitet med henblik på at sikre den offentlige sikkerhed [53], som den med rette har kvalificeret som værende »af afgørende betydning« [54]. Som den i sin tid bemærkede, bidrager »[b]eskyttelse af den offentlige sikkerhed […] desuden ligeledes til beskyttelsen af andres rettigheder og friheder« [55].

101. Man kunne med fordel udnytte den mulighed, som disse præjudicielle forespørgsler giver, til tydeligere at slå til lyd for, at der skal forsøges at finde en balance mellem retten til sikkerhed på den ene side, samt retten til privatliv og retten til beskyttelse af personoplysninger på den anden. Dermed ville kritikken af, at de sidstnævnte rettigheder bliver favoriseret på bekostning af den førstnævnte, kunne undgås.

102. I 11. betragtning til og artikel 15, stk. 1, i direktiv 2002/58 henvises der efter min opfattelse til denne balance, når der tales om, at foranstaltningerne *i et demokratisk samfund* skal være nødvendige og forholdsmæssige. Retten til sikkerhed er som nævnt tæt forbundet med selve eksistensen af et demokrati og dets muligheder for at bestå, hvorfor det er berettiget, at der i fuldt omfang tages hensyn hertil i forbindelse med bedømmelsen af den nævnte forholdsmæssighed. Det vil med andre ord sige, at hvis beskyttelsen af princippet om datafortrolighed er af afgørende betydning i et demokratisk samfund, bør betydningen af dets sikkerhed ej heller undervurderes.

103. Situationen med alvorlige og vedvarende trusler mod den nationale sikkerhed, og navnlig risikoen for terror, bør derfor tages i betragtning, således som det blev bemærket i sidste sætning af præmis 119 i dommen i sagen Tele2 Sverige og Watson. Et nationalt system kan reagere forholdsmæssigt på arten og intensiteten af de trusler, som den står over for, uden at denne løsning nødvendigvis behøver at være identisk med andre medlemsstaters løsninger.

104. Endelig skal jeg tilføje, at ovenstående betragtninger ikke er til hinder for, at den nationale lovgivning i helt *særlige* tilfælde, hvor der er en umiddelbar trussel eller en usædvanlig risiko, som kan berettige en officiel erklæring om nødsituation i en medlemsstat, i en begrænset periode kan tillade indførelsen af en pligt til lagring af data, som er så omfattende og generel, som det anses for at være nødvendigt [56].

105. Følgelig bør det første spørgsmål i begge præjudicielle forespørgsler omformuleres, således at det snarere omhandler muligheden for at begrunde indgrebet i nationale sikkerhedshensyn. Tvivlen ville dermed dreje sig om, hvorvidt den forpligtelse, der pålægges udbyderne af elektroniske kommunikationstjenester, er forenelig med artikel 15, stk. 1, i direktiv 2002/58.

50 – Digital Rights-dommen, præmis 42.

51 – Udtalelse 1/15 (PNR-aftale mellem EU og Canada) af 26.7.2017 (herefter »udtalelse 1/15«, EU:C:2017:592, præmis 149 og den deri nævnte retspraksis).

52 – Dom af 15.2.2016, N. (C-601/15 PPU, EU:C:2016:84, præmis 53).

53 – Digital Rights-dommen, præmis 42 og den deri nævnte retspraksis.

54 – Ibidem, præmis 51.

55 – Udtalelse 1/15, præmis 149.

56 – Jf. punkt 105-107 i mit forslag til afgørelse i sag C-520/18.

b) Bedømmelse

1) Karakterisering af de nationale retsforskrifter, således som der redegøres herfor i de to præjudicielle forespørgsler, set i lyset af Domstolens faste praksis

106. Det fremgår af forelæggelsesafgørelserne, at den omtvistede lovgivning i hovedsagerne indfører en forpligtelse til at lagre data for:

– operatører inden for elektronisk kommunikation, navnlig dem, der tilbyder adgang til offentlige onlinekommunikationstjenester, og

– fysiske eller juridiske personer, der, selv vederlagsfrit, med henblik på tilrådighedsstillelse for offentligheden online varetager oplagring af signaler, skrift, lyd, billeder eller meddelelser af enhver art, der leveres af modtagere af disse tjenester [57].

107. Operatørerne skal i et år, regnet fra den dato, hvor registreringen har fundet sted, lagre de oplysninger, der gør det muligt at fastslå brugerens identitet, oplysninger om det anvendte terminaludstyr, de tekniske kendetegn, dato, tidspunkt og varighed af hvert opkald, oplysninger vedrørende de supplerende tjenester, der er anmodet om eller anvendt, samt leverandørerne heraf, og de oplysninger, der gør det muligt at fastslå identiteten på den modtager, som kommunikationen er rettet til, samt i forbindelse med telefonitjenester kommunikationens oprindelse og lokaliseringen heraf [58].

108. Navnlig når der er tale om internetadgang og lagringstjenester, indfører den nationale lovgivning tilsyneladende en forpligtelse til at lagre IP-adresser [59], adgangskoder og, såfremt der er underskrevet en kontrakt eller indgået aftale om en betalingskonto, den afstedfundne betalingsform samt betalingsreferencen og transaktionens beløb, dato og klokkeslæt [60].

109. Denne forpligtelse til lagring pålægges af hensyn til efterforskning, afsløring og retsforfølgning af strafbare handlinger [61]. Til forskel fra pligten til at *indsamle* trafik- og lokaliseringsdata er forebyggelsen af terrorisme således ikke det eneste formål med pligten til at *lagre* disse data [62], hvilket der vil blive redegjort for nedenfor.

110. For så vidt angår betingelserne for *adgang* til de lagrede data fremgår det af sagens akter, at det enten er dem, der gælder for den fælles ordning (domsmyndighedens indgriben), eller at en sådan adgang begrænses til individuelt udpegede og bemyndigede agenter, efter forudgående tilladelse fra premierministeren udstedt på grundlag af en ikke-bindende udtalelse fra en uafhængig administrativ myndighed [63].

57 – Således fremgår det af artikel L. 851-1 i lov om indre sikkerhed, hvori der henvises til artikel L. 34-1 i lov om postvæsen og elektronisk kommunikation og artikel 6 i lov nr. 2004-575 om tillid til den digitale økonomi.

58 – Således fastsættes det i artikel R. 10-13 i lov om postvæsen og elektronisk kommunikation.

59 – Det tilkommer den forelæggende ret at efterprøve dette punkt, som var genstand for uenighed i retsmødet.

60 – Artikel 1 i dekret 2011-219.

61 – Artikel R. 10-13 i lov om postvæsen og elektronisk kommunikation.

62 – Såvel La Quadrature du Net som Fédération des founisseurs d'accès à Internet associatifs har henledt opmærksomheden på oplagringens mange formål, de skønsbeføjelser, som myndighederne tillægges, de manglende objektive kriterier i forbindelse med definitionen heraf og den betydning, som tillægges de former for kriminalitet, der ikke kan kvalificeres som alvorlige.

63 – Commission nationale de contrôle des techniques de renseignement (den nationale tilsynsmyndighed for efterretningsteknikker). Jf. i denne forbindelse punkt 145-148 i den franske regerings skriftlige indlæg.

111. Det kan uden videre konstateres, således som Kommissionen har bemærket [64], at de oplysninger, som skal lagres i henhold til de nationale bestemmelser, i det væsentlige svarer til dem, der blev undersøgt af Domstolen i Digital Rights-dommen og dommen i sagen Tele2 Sverige og Watson [65]. Ligesom det var tilfældet dengang, er disse oplysninger genstand for en »forpligtelse til generel og udifferentieret lagring«, således som Conseil d'État (øverste domstol i forvaltningsretlige sager) helt åbent har bemærket i begyndelsen af sine præjudicielle spørgsmål.

112. Såfremt dette er tilfældet, hvilket det i sidste ende tilkommer den forelæggende ret at vurdere, er der ingen tvivl om, at den omhandlede lovgivning udgør et »indgreb […] i de grundlæggende rettigheder fastslået i chartrets artikel 7 og 8, [som] er meget vidtrækkende og må anses for at være særligt alvorligt« [66].

113. Ingen af de fremmødte parter har bestridt, at en lovgivning med disse kendetegn indebærer et indgreb i disse rettigheder. Det er ikke nødvendigt at dvæle ved dette punkt her, end ikke for at erindre om, at indskrænkningen af disse rettigheder uvægerligt vil være til skade for selve grundlaget for et samfund, der sigter mod – blandt andre værdier – at respektere privatlivets fred som sikret ved chartret.

114. En anvendelse af retspraksis fra dommen i sagen Tele2 Sverige og Watson, som blev bekræftet ved Ministerio Fiscal-dommen, vil af naturlige årsager lede til den konklusion, at en lovgivning som den her omhandlede »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 chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1« [67].

115. Ligesom den undersøgte lovgivning i dommen i sagen Tele2 Sverige og Watson omfatter den her omhandlede lovgivning ligeledes »alle abonnenter og registrerede brugere generelt, og […] er rettet mod alle elektroniske kommunikationsmidler og samtlige trafikdata, [og foreskriver] ingen form for differentiering, begrænsning eller undtagelse under hensyn til det forfulgte mål« [68]. Følgelig »finder [den] 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 grove straffelovsovertrædelser«, og endvidere indeholder den ikke nogen undtagelsesbestemmelse, »således at den finder anvendelse endog på personer, hvis kommunikation i henhold til nationale retsregler er omfattet af tavshedspligt« [69].

116. Endvidere kræver den omtvistede lovgivning »ikke nogen sammenhæng mellem de data, som foreskrives lagret, og en trussel mod den offentlige sikkerhed. Den er navnlig ikke begrænset til en lagring, som er rettet mod data vedrørende et tidsrum og/eller et geografisk område og/eller en personkreds, der på den ene eller anden måde vil kunne være indblandet i alvorlige lovovertrædelser, eller mod personer, der af andre grunde gennem lagring af deres data ville kunne bidrage til bekæmpelse af kriminalitet« [70].

64 – Punkt 60 i Kommissionens skriftlige indlæg.

65 – Faktisk rækker de lidt videre, eftersom de i forbindelse med internetadgang ligeledes lader til at omfatte lagring af IP-adresser og adgangskoder.

66 – Dommen i sagen Tele2 Sverige og Watson, præmis 100.

67 – Ibidem, præmis 107.

68 – Ibidem, præmis 105.

69 – Ibidem.

70 – Dommen i sagen Tele2 Sverige og Watson, præmis 106.

117. Det fremgår af det ovenstående, at en sådan lovgivning »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 chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1« [71].

118. Ovenstående var tilstrækkeligt til, at Domstolen kunne fastslå, at de pågældende nationale retsforskrifter ikke var forenelige med artikel 15, stk. 1, i direktiv 2002/58, for så vidt som de »med henblik på bekæmpelse af kriminalitet [fastsatte] en generel og udifferentieret lagring af samtlige trafikdata og lokaliseringsdata vedrørende samtlige abonnenter og registrerede brugere i forbindelse med samtlige midler til elektronisk kommunikation« [72].

119. Det spørgsmål, der rejses her, handler om, hvorvidt Domstolens faste praksis på området for lagring af personoplysninger kan, om ikke tages op til fornyet overvejelse, så i det mindste nuanceres, når formålet med en sådan »generel og udifferentieret« lagring er bekæmpelsen af terrorisme. Det første spørgsmål i sag C-511/18 rejses netop i »en situation, der er præget af alvorlige og vedvarende trusler mod den nationale sikkerhed og navnlig af risikoen for terror«.

120. Mens dette er den *faktiske sammenhæng*, hvori forpligtelsen til lagring af data pålægges, forholder det sig imidlertid således, at denne forpligtelse i en *normativ sammenhæng* ikke alene er begrundet i terrorisme. I den ordning for lagring af og adgang til data, som er genstand for sagen ved Conseil d'État (øverste domstol i forvaltningsretlige sager), gøres denne forpligtelse betinget af et generelt hensyn til efterforskning, afsløring og retsforfølgning af strafbare handlinger.

121. Jeg skal i alle tilfælde erindre om, at bekæmpelsen af terrorisme ikke blev ignoreret i forbindelse med argumentationen i dommen i sagen Tele2 Sverige og Watson, men at Domstolen ikke fandt, at denne form for kriminalitet gjorde det nødvendig at ændre dens faste praksis [73].

122. Således finder jeg som udgangspunkt, at den forelæggende rets spørgsmål, som er centreret omkring terrortruslen, bør besvares i samme retning som Domstolens besvarelse i dommen i sagen Tele2 Sverige og Watson.

123. Som jeg bemærkede i mit forslag til afgørelse i Stichting Brein-sagen, forholder det sig således, at »[s]elv om retsinstanserne ikke skal anvende princippet om stare decisis kategorisk, skal de af hensyn til sikkerheden i forbindelse med anvendelsen af retten udvise forsigtighed og holde sig til det, som de efter moden overvejelse selv har besluttet i forbindelse med en forelagt retlig problemstilling« [74].

2) Begrænset lagring af data set i forhold til truslerne mod statens sikkerhed, herunder terrortruslen

124. Ville det imidlertid være muligt at præcisere eller supplere denne retspraksis, i lyset af dens konsekvenser for bekæmpelsen af terrorisme eller for beskyttelsen af staten mod andre tilsvarende trusler mod den nationale sikkerhed?

71 – Ibidem, præmis 107.

72 – Ibidem, præmis 112.

73 – Ibidem, præmis 103.

74 – Sag C-527/15, EU:C:2016:938, punkt 41.

125. Jeg har allerede bemærket, at lagringen af personoplysninger i sig selv udgør et indgreb i de ved chartrets artikel 7, 8 og 11 sikrede rettigheder[75]. Uanset om formålet med denne lagring i sidste ende er at sikre muligheden for en efterfølgende eller samtidig *adgang* til oplysningerne på et givent tidspunkt[76], udgør den blotte lagring af data, som rækker ud over, hvad der er strengt nødvendigt for at fremføre en kommunikation eller fakturere for de af udbyderen leverede ydelser, en overskridelse af de i artikel 5 og 6 i direktiv 2002/58 fastsatte begrænsninger.

126. Brugerne af disse tjenester (hvilket i realiteten vil sige stor set alle borgere i de mest udviklede samfund) har, eller bør have, en berettiget forventning om, at der ikke opbevares flere oplysninger om dem end de oplysninger, der oplagres i medfør af de nævnte bestemmelser, medmindre de har givet deres samtykke hertil. Undtagelserne i artikel 15, stk. 1, i direktiv 2002/58 skal læses ud fra denne forudsætning.

127. Som jeg tidligere har redegjort for, afviste Domstolen i dommen i sagen Tele2 Sverige og Watson en generel og udifferentieret lagring af personoplysninger, også i forbindelse med bekæmpelsen af terrorisme[77].

128. Over for den fremsatte kritik mener jeg ikke, at retspraksis fra den pågældende dom undervurderer terrortruslen med hensyn til, at der er tale om en særlig alvorlig kriminalitet, der indebærer en klar hensigt om at angribe statens autoritet og destabilisere eller ødelægge dens institutioner. Bekæmpelsen af terrorisme er bogstavelig talt altafgørende for staten, og dens succes er et uomgængeligt mål af almen interesse for en retsstat.

129. Stort set alle de regeringer, der har afgivet indlæg i sagen, samt Kommissionen, er enige om, at en delvis og differentieret lagring af personoplysninger – ud over de tekniske vanskeligheder, der er forbundet hermed – vil fratage de nationale efterretningstjenester muligheden for at få adgang til oplysninger, som er nødvendige for at kunne identificere trusler mod den offentlige sikkerhed og statens forsvar og for at kunne retsforfølge gerningsmændene bag terrorangreb[78].

130. Over for denne antagelse finder jeg det nødvendigt at bemærke, at bekæmpelsen af terrorisme ikke udelukkende bør vurderes med tanke på dens effektivitet. Dette er årsagen til dens vanskeligheder, men også til dens betydningsfuldhed, når dens midler og metoder tilpasses de retsstatslige krav, som først og fremmest går ud på, at magten og styrken skal gøres betinget af rettighedernes begrænsninger, og navnlig af en retsorden, hvis eksistensgrundlag er baseret på beskyttelsen af de grundlæggende rettigheder.

75 – Som Domstolen bemærkede i udtalelse 1/15, præmis 124, »udgør videregivelsen af personoplysninger til en tredjemand såsom en offentlig myndighed et indgreb i den grundlæggende rettighed, der er sikret ved chartrets artikel 7, uanset hvad de videregivne oplysninger efterfølgende bruges til. Det samme gælder opbevaringen af personoplysninger og de offentlige myndigheders adgang hertil med henblik på brug heraf. I denne henseende er det uden betydning, om de pågældende oplysninger vedrørende privatlivet er følsomme oplysninger, eller om indgrebet har medført eventuelle ubehageligheder for de berørte«.

76 – Som generaladvokat Cruz Villalón bemærkede i sit forslag til afgørelse Digital Rights (C-293/12 og C-594/12, EU:C:2013:845, punkt 72), forholder det sig således, at »indsamling og særligt lagring i meget store databaser af store mængder data, der genereres eller behandles i forbindelse med størstedelen af unionsborgernes almindelige elektroniske kommunikation, udgør et alvorligt indgreb i privatlivet, selv om denne lagring kun skaber betingelser, der gør det muligt at foretage en efterfølgende kontrol af unionsborgernes såvel personlige som arbejdsmæssige aktiviteter. Indsamling af sådanne oplysninger skaber betingelserne for at foretage overvågning, der, selv om den kun foretages efterfølgende i forbindelse med udnyttelse af oplysningerne, dog udgør en konstant trussel under hele lagringsperioden mod unionsborgernes ret til at hemmeligholde deres privatliv. Den vage følelse af at blive overvåget, der opstår derved, gør spørgsmålet om varigheden af det tidsrum, i hvilket oplysningerne lagres, særlig relevant«.

77 – Dommen i sagen Tele2 Sverige og Watson, præmis 103: »[D]et [kan] ikke i sig selv begrunde, at en national lovgivning, der foreskriver en generel og udifferentieret lagring af samtlige trafik- og lokaliseringsdata, kan anses for nødvendig med henblik på den pågældende bekæmpelse.«

78 – Dette er bl.a. den franske regerings fortolkning, idet den har illustreret denne påstand med konkrete eksempler på nytteværdien af en generel lagring af data, som gav staten mulighed for at reagere på de alvorlige terrorangreb, som landet har været udsat for i de senere år (punkt 107 og 122-126 i den franske regerings skriftlige indlæg).

131. Mens de midler, der anvendes i forbindelse med terrorisme, alene efterlever kriteriet om at opnå fuld (og maksimal) effektivitet af angrebene på den etablerede orden, måles effektiviteten for retsstatens vedkommende ud fra kriterier, hvorefter det i forbindelse med forsvaret heraf ikke er tilladt at fravige de procedurer og garantier, som er medvirkende til at kvalificere retsstaten som en legitim orden. Tages der udelukkende hensyn til effektiviteten, vil retsstaten miste den egenskab, hvorved den udmærker sig, og vil dermed, i ekstreme tilfælde, selv kunne udgøre en trussel mod borgerne. Såfremt de offentlige myndigheder var udrustet med uforholdsmæssige instrumenter til retsforfølgelse af strafbare handlinger, hvorved de kunne se bort fra eller forringe de grundlæggende rettigheder, ville der ikke være nogen sikkerhed for, at deres ukontrollerede og fuldstændig frie handlinger i sidste ende ikke kunne være til skade for alle borgeres frihed.

132. De offentlige myndigheders effektivitet støder som nævnt på en uoverstigelig hindring i form af borgernes grundlæggende rettigheder, for hvilke der i henhold til chartrets artikel 52, stk. 1, alene kan fastlægges begrænsninger ved lov og under iagttagelse af deres væsentligste indhold, »såfremt disse 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« [79].

133. For så vidt angår de forudsætninger, hvorunder det i henhold til dommen i sagen Tele2 Sverige og Watson vil være tilstedeligt at foretage en *målrettet* lagring af data, skal jeg henvise til mit forslag til afgørelse i sag C-520/18 [80].

134. Omstændigheder, hvorunder den information, som er til rådighed for de retshåndhævende myndigheder, gør det muligt at fremsætte en begrundet mistanke om forberedelse af et terrorangreb, kan udgøre en legitim begrundelse for at pålægge en pligt til at lagre bestemte data. Den reelle gennemførelse af et attentat kan i endnu højere grad udgøre en legitim begrundelse. Såfremt det at begå en strafbar handling i sidstnævnte tilfælde i sig selv kan udgøre en omstændighed, der kan begrunde iværksættelsen af den pågældende foranstaltning, vil det ved den blotte mistanke om et muligt attentat være en forudsætning, at de tilgrundliggende omstændigheder tilbyder en vis grad af sandsynlighed, hvilket er strengt nødvendigt for at kunne foretage en objektiv afvejning af de indicier, der kan lægges til grund herfor.

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 som jeg allerede har bemærket, kan spørgsmålet 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. Jeg skal atter henvise til mine bemærkninger vedrørende dette spørgsmål i forslag til afgørelse i sag C-520/18 [81].

79 – Dom af 15.2.2016, N. (C-601/15 PPU, EU:C:2016:84, præmis 50). Det drejer sig således om den vanskelige balancegang mellem de grundlæggende retsprincipper og frihedsrettighederne, som jeg tidligere har redegjort for, og som hele EU-lovgivningen som udgangspunkt forfølger. Et eksempel herpå er Europa-Parlamentets og Rådets direktiv (EU) 2017/541 af 15.3.2017 om bekæmpelse af terrorisme og om erstatning af Rådets rammeafgørelse 2002/475/RIA og ændring af Rådets afgørelse 2005/671/RIA (EUT 2017, L 88, s. 6). Samtidig med, at det i direktivets artikel 20, stk. 1, bestemmes, at medlemsstaterne skal sikre, at de ansvarlige for efterforskning eller retsforfølgning af terrorhandlinger »råder over effektive efterforskningsmidler«, bemærkes det i 21. betragtning til direktivet, at brugen af sådanne effektive midler »bør være målrettet og ske under hensyntagen til proportionalitetsprincippet og karakteren og alvoren af de lovovertrædelser, der efterforskes, og bør respektere retten til beskyttelse af personoplysninger«.

80 – Punkt 87-95.

81 – Punkt 100-107.

3) Adgang til de lagrede data

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[82], 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[83].

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[84]. 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[85].

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[86]. 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.

4) Pligten til at lagre data, der gør det muligt at identificere ophavsmændene til indhold, i lyset af direktiv 2000/31 (det andet præjudicielle spørgsmål i sag C-512/18)

140. Den forelæggende ret har henvist til direktiv 2000/31 som referencepunkt i forbindelse med bedømmelsen af, om det er muligt at forpligte bestemte personer[87] og operatører, der tilbyder offentlige onlinekommunikationstjenester, til at lagre data, »som vil kunne gøre det muligt at identificere enhver, der har bidraget til at skabe indholdet eller en del af indholdet af de tjenester, som de leverer, for at den retslige myndighed i påkommende tilfælde kan kræve videregivelse heraf med henblik på at sikre overholdelsen af reglerne om civil- eller strafferetligt ansvar«.

141. Jeg er enig med Kommissionen i, at der ikke er grundlag for at undersøge denne forpligtelses forenelighed med direktiv 2000/31[88], for så vidt som direktivets anvendelsesområde i henhold til artikel 1, stk. 5, litra b), ikke omfatter »spørgsmål, der vedrører informationssamfundstjenester omfattet af direktiv 95/46/EF og 97/66/EF«, retsforskrifter, som i dag er omfattet af forordning 2006/679 og direktiv 2002/58[89], hvis artikel 23, stk. 1, henholdsvis artikel 15, stk. 1, efter min opfattelse bør fortolkes således, som jeg har redegjort for ovenfor.

82 – Forstået således, at de i præmis 122 i dommen i sagen Tele2 Sverige og Watson nævnte krav skal opfyldes: Domstolen har bemærket, at artikel 15, stk. 1, i direktiv 2002/58 ikke gør det muligt at fravige direktivets artikel 4, stk. 1 eller stk. 1a, som pålægger udbyderne at træffe foranstaltninger, der gør det muligt at sikre beskyttelsen af de lagrede data mod risikoen for misbrug og mod ulovlig adgang hertil. Den fastslog i denne forbindelse, at »[h]enset til mængden af lagrede data, den følsomme karakter af disse data og risikoen for ulovlig adgang til disse skal udbyderne af elektroniske kommunikationstjenester med henblik på at sikre de pågældende datas fulde integritet og fortrolighed sikre et særligt højt niveau for beskyttelse og sikkerhed gennem passende tekniske og organisatoriske foranstaltninger. Særligt skal den nationale lovgivning foreskrive en lagring på EU's område og en irreversibel destruktion af disse data ved udløbet af lagringsperioden«.

83 – Punkt 52-60.

84 – Dommen i sagen Tele2 Sverige og Watson, præmis 118.

85 – Ibidem, præmis 119.

86 – Ibidem, præmis 120.

87 – Dem, som »med henblik på tilrådighedsstillelse for offentligheden via offentlige onlinekommunikationstjenester varetager oplagring af signaler, skrift, billeder, lyd eller meddelelser af enhver art […]«.

88 – Den forelæggende ret nævner dette direktiv i generelle vendinger og uden at henvise til nogen konkrete bestemmelser i det andet spørgsmål i sag C-512/18.

89 – Punkt 112 og 113 i Kommissionens skriftlige indlæg.

2. Pligten til at indsamle trafik- og lokaliseringsdata i realtid (det andet præjudicielle spørgsmål i sag C-511/18)

142. Efter den forelæggende rets opfattelse tillader artikel L. 851-2 i lov om indre sikkerhed alene med henblik på forebyggelse af terrorisme at indsamle oplysninger i realtid vedrørende personer, der i forvejen er mistænkt for at have forbindelse til en terrortrussel. På samme måde tillader lovens artikel L. 851-4, at operatører i realtid kan overføre tekniske data vedrørende lokaliseringen af terminaludstyr.

143. Det er den forelæggende rets opfattelse, at disse teknikker ikke pålægger udbyderne et yderligere krav om lagring i forhold til, hvad der er nødvendigt for debiteringen af tjenesteydelserne og markedsføringen heraf.

144. I henhold til artikel L. 851-3 i lov om indre sikkerhed kan operatører inden for elektronisk kommunikation og udbydere af tekniske tjenester endvidere pålægges at »anvende automatiseret behandling i deres netværk med henblik på i overensstemmelse med de parametre, som præciseres i tilladelsen, at opdage forbindelser, der vil kunne afsløre en terrortrussel«. Denne teknik udgør ikke en generel og udifferentieret lagring af data, men sigter mod, i et begrænset tidsrum, at indsamle de forbindelsesdata, der kan have tilknytning til udøvelsen af en terrorhandling.

145. Efter min opfattelse skal de opstillede betingelser i forbindelse med adgangen til lagrede personoplysninger ligeledes finde anvendelse på adgangen i realtid til de data, der genereres i løbet af den elektroniske kommunikation. Jeg skal således henvise til min redegørelse på dette punkt. Det er uden betydning, om der er tale om lagrede data eller data, som tilgås øjeblikkeligt, eftersom der i begge tilfælde opnås kendskab til personoplysninger, uanset om der er tale om historiske eller aktuelle data.

146. Det vil nærmere bestemt sige, at såfremt adgangen i realtid er en følge af forbindelser, som er konstateret i forbindelse med en automatiseret databehandling som den i artikel L. 851-3 i lov om indre sikkerhed omhandlede, kræves det, at de forud fastsatte modeller og kriterier for denne behandling skal være specifikke, pålidelige og ikke-diskriminerende, således at de kan lette identificeringen af personer, for hvis vedkommende der kan være en rimelig mistanke om deltagelse i terrorhandlinger [90].

3. Pligten til at underrette de berørte personer (det tredje præjudicielle spørgsmål i sag C-511/18)

147. Domstolen har fastslået, at de myndigheder, som får adgang til de lagrede data, skal underrette de berørte personer herom, så snart det ikke kan skade disse myndigheders efterforskning. Begrundelsen for denne pligt er, at den pågældende underretning er nødvendig for at gøre det muligt for disse personer at udøve den adgang til retsmidler, som udtrykkeligt er fastsat i artikel 15, stk. 2, i direktiv 2002/58, i tilfælde af, at deres rettigheder er blevet tilsidesat [91].

148. Conseil d'État (øverste domstol i forvaltningsretlige sager) ønsker med sit tredje spørgsmål i sag C-511/18 oplyst, om dette krav om underretning i alle tilfælde er ufravigeligt, eller om det er muligt af dispensere herfra, når der foreligger andre garantier, som f.eks. de i forelæggelsesafgørelsen beskrevne.

90 – Digital Rights-dommen, præmis 59.

91 – Dommen i sagen Tele2 Sverige og Watson, præmis 121.

149. Ifølge den forelæggende rets fremstilling [92] består de nævnte garantier af muligheden for, at enhver person, der ønsker en efterprøvelse af, at ingen efterretningsteknik bliver anvendt uretmæssigt, kan indbringe et søgsmål for Conseil d'État (øverste domstol i forvaltningsretlige sager). Dette organ kan i givet fald ophæve tilladelsen til foranstaltningen og anordne tilintetgørelse af de indsamlede oplysninger inden for rammerne af en procedure, som ikke er bundet af det kontradiktionsprincip, der almindeligvis er gældende i forbindelse med retslige procedurer.

150. Efter den forelæggende rets opfattelse krænker denne lovgivning ikke retten til effektive retsmidler. Jeg mener imidlertid, at denne antagelse i teorien kan godtages for så vidt angår dem, der beslutter sig for at efterprøve, om de er genstand for en efterretningsoperation. Derimod respekteres denne rettighed ikke, når personer, som er eller har været genstand for en sådan operation, ikke bliver underrettet om dette forhold, og derfor end ikke overvejer muligheden for, at deres rettigheder er blevet krænket.

151. De retlige garantier, som den forelæggende ret henviser til, lader til at være betingede af, at de personer, som mistænker, at de er genstand for en indsamling af personoplysninger, selv tager initiativ. Adgangen til domstolsprøvelse med henblik på beskyttelse af sine rettigheder skal imidlertid være effektiv for alle, hvilket indebærer, at den, der har været genstand for en behandling af sine personoplysninger, skal have mulighed for at sætte spørgsmålstegn ved lovligheden af denne behandling ved domstolene, og derfor skal vedkommende nødvendigvis underrettes om eksistensen heraf.

152. Som det fremgår af de tilvejebragte oplysninger, kan retshåndhævelsen ganske vist iværksættes ex officio eller ved administrativ anmeldelse, men den berørte person bør i alle tilfælde gives mulighed for selv at anlægge sagen, og derfor er det nødvendigt at gøre vedkommende bekendt med, at hans personoplysninger har været genstand for den pågældende behandling. Beskyttelsen af hans rettigheder kan ikke baseres på den forudsætning, at han eventuelt opnår kendskab til den pågældende behandling fra tredjemand eller af egen kraft.

153. Det vil således sige, at for så vidt som det ikke er til fare for den efterforskning, i forbindelse med hvilken der er givet adgang til de lagrede data, skal den berørte person underrettes om denne adgang.

154. Noget andet er, at når den berørte person har givet udtryk for sit ønske om retshåndhævelse efter at være blevet gjort bekendt med adgangen til oplysningerne, skal den efterfølgende retslige procedure overholde kravene om tavshed og fortrolighed i forbindelse med undersøgelsen af de offentlige myndigheders handlinger på følsomme områder som statens sikkerhed og forsvar. Dette spørgsmål ligger imidlertid uden for rammerne af disse anmodninger om præjudiciel afgørelse, hvorfor der efter min opfattelse ikke er belæg for, at Domstolen udtaler sig herom.

92 – Forelæggelsesafgørelsens præmis 8-11.

V. Forslag til afgørelse

155. På baggrund af det ovenstående foreslår jeg, at Domstolen besvarer de af Conseil d'État (øverste domstol i forvaltningsretlige sager, Frankrig) forelagte spørgsmål således:

»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 (direktivet om privatliv og elektronisk kommunikation), sammenholdt med artikel 7, 8 og 11 samt artikel 52, stk. 1, i Den Europæiske Unions charter om grundlæggende rettigheder, skal fortolkes således, at:

1) Bestemmelsen er til hinder for en national lovgivning, som i en situation, der er præget af alvorlige og vedvarende trusler mod den nationale sikkerhed og navnlig af risikoen for terror, forpligter operatørerne og udbyderne af elektroniske kommunikationstjenester til at foretage en generel og udifferentieret lagring af samtlige trafikdata og lokaliseringsdata vedrørende samtlige abonnenter, samt af de data, der gør det muligt at identificere skaberne af det indhold, der leveres af udbyderne af disse tjenester.

2) Bestemmelsen er til hinder for en national lovgivning, som ikke fastsætter en pligt til at underrette de berørte personer om de kompetente myndigheders behandling af deres personoplysninger, medmindre en sådan underretning er til fare for de pågældende myndigheders efterforskning.

3) Bestemmelsen er ikke til hinder for en national lovgivning, hvorefter det er tilladt at indsamle specifikke personers trafik- og lokaliseringsdata i realtid, for så vidt som disse handlinger udføres i overensstemmelse med de fastsatte procedurer for adgang til lovligt lagrede personoplysninger og med samme garantier.«