

**Sag C-793/19****Sammendrag af anmodning om præjudiciel afgørelse i henhold til artikel 98, stk. 1, i Domstolens procesreglement****Dato for indlevering:**

29. oktober 2019

**Forelæggende ret:**

Bundesverwaltungsgericht (Tyskland)

**Afgørelse af:**

25. september 2019

**Sagsøger og revisionsinstævnt:**

SpaceNet AG

**Sagsøgt og revisionsappellant:**

Bundesrepublik Deutschland

**Hovedsagens genstand**

Søgsmål med påstand om, at det fastslås, at SpaceNet ikke er forpligtet til at lagre de i TKG's § 113b, stk. 3, nævnte telekommunikationstrafikdata vedrørende sine kunder, for hvem virksomheden formidler internetadgang.

**Genstand og retsgrundlag for forelæggelsen**

Fortolkning af EU-retten, navnlig artikel 15, stk. 1, i direktiv 2002/58, og af dommen Tele2 Sverige og Watson m.fl.; artikel 267 TEUF.

**Præjudicielt spørgsmål**

Skal artikel 15 i direktiv 2002/58/EF i lyset af artikel 7, 8 og 11 samt artikel 52, stk. 1, i Den Europæiske Unions charter om grundlæggende rettigheder på den ene side og artikel 6 i Den Europæiske Unions charter om grundlæggende rettigheder og artikel 4 i traktaten om Den Europæiske Union på den anden side fortolkes således, at den er til hinder for en national bestemmelse, som forpligter udbyderne

af offentligt tilgængelige elektroniske kommunikationstjenester til at lagre trafik- og lokaliseringsdata for slutbrugerne af disse tjenester, når

- denne forpligtelse ikke forudsætter nogen specifik anledning i lokal, tidsmæssig eller geografisk henseende
- genstanden for pligten til at lagre data i forbindelse med levering af offentligt tilgængelige telefontjenester – herunder formidling af sms-, multimedie- eller lignende beskeder samt ubesvarede eller forgæves opkald – er følgende data:
  - telefonnummeret eller en anden identitet for den, der ringer op, og den forbindelse, der ringes til, samt ved om- og viderestilling enhver anden involveret forbindelse
  - dato og klokkeslæt for begyndelse og afslutning af forbindelsen henholdsvis – i forbindelse med formidling af sms-, multimedie- eller lignende beskeder – tidspunkterne for afsendelse og modtagelse af beskeden med angivelse af den anvendte tidszone
  - oplysninger om den benyttede tjeneste, hvis der i forbindelse med telefontjenesten kan benyttes forskellige tjenester
  - for mobile telefontjenester endvidere
    - den internationale identitet for mobile abonnenter for den, der ringer op, og den forbindelse, der ringes til
    - den internationale identitet for det terminaludstyr, der ringer op, og som der ringes til
    - dato og klokkeslæt for den første aktivering af tjenesten under angivelse af den anvendte tidszone, hvis der er blevet betalt tjenester på forhånd
    - betegnelserne for de radioceller, som blev benyttet af den forbindelse, der ringer op, og den forbindelse, der ringes til, ved forbindelsens begyndelse
  - for internettelefontjenester tillige internetprotokoladresserne for den forbindelse, der ringer op, og den forbindelse, der ringes til, og tildelte brugeridentiteter
- genstanden for pligten til lagring i forbindelse med levering af offentligt tilgængelige internetadgangstjenester er følgende data:
  - den internetprotokoladresse, som er tildelt abonnenten til en internetbenyttelse

- en entydig identitet for den forbindelse, gennem hvilken internetbenyttelsen sker, samt en tildelt brugeridentitet
- dato og klokkeslæt for internetbenyttelsens begyndelse og ophør under den tildelte internetprotokoladresse med angivelse af den anvendte tidszone
- for mobil benyttelse betegnelsen for den radiocelle, som benyttes ved internetforbindelsens begyndelse
- følgende data ikke må lagres:
  - kommunikationens indhold
  - data om besøgte internetsider
  - data fra elektroniske posttjenester
  - data, som er baseret på forbindelser til eller fra bestemte personer, myndigheders og organisationers forbindelser inden for sociale eller kirkelige områder
- lagringens varighed for lokaliseringsdata, dvs. betegnelsen for den benyttede radiocelle, udgør fire uger, og for de øvrige data ti uger
- der er sikret en effektiv beskyttelse af de lagrede data mod risici for misbrug samt mod enhver uberettiget adgang, og
- de lagrede data kun må anvendes til at forfølge særligt grove straffelovsovertrædelser og til at afværge en konkret fare for en persons liv og helbred eller frihed eller for forbundsstatens eller en delstats beståen, med undtagelse af den internetprotokoladresse, som er tildelt abonnenten til en internetbenyttelse, og som det er tilladt at anvende i forbindelse med en stamdataoplysning (»Bestandsdatenauskuft«) med henblik på forfølgelse af enhver form for strafbare handlinger, for at afværge en fare for den offentlige sikkerhed og orden samt for at opfylde efterretningstjenesternes opgaver?

### **Anførte EU-retlige bestemmelser**

Den Europæiske Unions charter om grundlæggende rettigheder (herefter »chartret«), artikel 6, 7, 8, 11 og 52

Traktaten om Den Europæiske Union (TEU), artikel 4 og 6

Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (Direktiv om databeskyttelse inden for

elektronisk kommunikation) som ændret ved Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009 (herefter »direktiv 2002/58«), artikel 5, 6, 8, 9, navnlig artikel 15; ellefte betragtning

### **Anførte nationale bestemmelser**

Telekommunikationsgesetz (telekommunikationsloven, herefter »TKG«), § 113a, stk. 1, første punktum (»Forpligtede«), § 113b (»Forpligtelser til at lagre trafikdata«), § 113c (»Anvendelse af dataene«), § 113d (»Sikring af dataenes sikkerhed«), § 113e (»Protokollering« (af adgang til lagrede data foretaget af den forpligtede)), § 113f (»Kravkatalog« (med hensyn til tekniske foranstaltninger og andre foranstaltninger)), § 99, stk. 2 (»Individuel forbrugsdokumentation«, om instanser, som er undtaget fra visning i individuelle forbrugsdokumentationer)

Strafprozessordnung (strafferetsplejeloven, herefter »StPO«), § 100g, stk. 2 (»Indsamling af trafikdata« i henhold til TKG's § 113b)

### **Anførte domme fra Domstolen**

Den Europæiske Unions Domstols dom af 21. december 2016, Tele2 Sverige AB og Watson m.fl., C-203/15 og C-698/15, EU:C:2016:970 (herefter »dommen i [de forenede sager] Tele2 Sverige og Watson m.fl.«)

Dom af 8. april 2014, Digital Rights Ireland og Seitlinger m.fl., C-293/12 og C-594/12, EU:C:2014:238 (herefter »dommen i [de forenede sager] Digital Rights Ireland m.fl.«)

Udtalelse 1/15 af 26. juli 2017, EU:C:2017:592

Desuden: Dom af 29. juli 2019, Funke Medien (C-469/17, EU:C:2019:623), af 9. marts 1978, Simmenthal (106/77, EU:C:1978:49), af 3. maj 2005, Berlusconi m.fl. (C-387/02, C-391/02 og C-403/02, EU:C:2005:270), af 22. juni 2010, Melki og Abdeli (C-188/10 og C-189/10, EU:C:2010:363), og af 18. september 2014, Vueling Airlines (C-487/12, EU:C: 2014: 2232).

### **Kort fremstilling af de faktiske omstændigheder og retsforhandlingerne i hovedsagen**

- 1 Sagsøgeren, SpaceNetAG (herefter »sagsøgeren« eller »SpaceNet«) leverer offentligt tilgængelige internetadgangstjenester. Sagsøgeren anfægter den pligt, der ved TKG's § 113a, stk. 1, sammenholdt med § 113b i den affattelse, der følger af lov af 10. december 2015, er pålagt virksomheden til fra den 1. juli 2017 at lagre telekommunikationstrafikdata vedrørende virksomhedens kunder.
- 2 I første instans fastslog Verwaltungsgericht (forvaltningsdomstol), at SpaceNet ikke er forpligtet til at lagre de i TKG's § 113b, stk. 3, nævnte

telekommunikationstrafikdata vedrørende sine kunder, for hvem virksomheden formidler internetadgang. Sagsøgte, Forbundsrepublikken Tyskland (herefter »sagsøgte«), har iværksat revisionsappel direkte (»Sprungrevision«) til Bundesverwaltungsgericht (forbundsdomstol i forvaltningsretlige sager) til prøvelse af Verwaltungsgerichts (forvaltningsdomstol) dom.

- 3 Revisionsappellen kan kun tages til følge, hvis den pligt til at lagre telekommunikationstrafikdata, der ved de nævnte bestemmelser i TKG pålægges leverandørerne af offentligt tilgængelige telekommunikationstjenester (herefter »telekommunikationsudbydere«), er forenelig med EU-retten.
- 4 Bestemmelserne om denne pligt for telekommunikationsudbydere til at lagre bestemte trafikdata i en begrænset periode blev ændret ved Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 (lov om indførelse af en lagringspligt og en maksimal lagringsperiode for trafikdata af 10.12.2015, herefter »lov af 10. december 2015«)
- 5 En ændring var nødvendig, efter at en dom fra Bundesverfassungsgericht (forbundsdomstol i forfatningsretlige sager) fra 2010 havde erklæret de tidligere bestemmelser, som regulerede lagring af data, for ugyldige på grund af tilsidesættelse af grundlæggende rettigheder, og efter at direktiv 2006/24, som disse tidligere bestemmelser tjente til gennemførelse af, i 2014 desuden var blevet erklæret ugyldigt ved dommen i [de forenede sager] Digital Rights Ireland m.fl. Lov af 10. december 2015 skal afhjælpe mangler i forbindelse med strafforfølgelse og afværgelse af risici og samtidig tage højde for de forfatnings- og EU-retlige krav, der følger af de nævnte afgørelser.
- 6 For at kunne besvare spørgsmålet om, hvorvidt den lagringspligt, der er fastsat i TKG's § 113a, stk. 1, sammenholdt med § 113b, er i strid med EU-retten, er der behov for, at Domstolen fortolker direktiv 2002/58 og navnlig præciserer, hvordan dommen i sagen Tele2 Sverige og Watson m.fl. skal forstås.

### **Kort fremstilling af begrundelsen for forelæggelsen**

- 7 Pligten til at lagre telekommunikationstrafikdata, som er fastsat i TKG's § 113a, stk. 1, første punktum, sammenholdt med § 113b, begrænser rettighederne i henhold til artikel 5, stk. 1, artikel 6, stk. 1, og artikel 9, stk. 1, i direktiv 2002/58.
- 8 Den udgør et indgreb i den elektroniske kommunikationshemmelighed, som er beskyttet ved direktivets artikel 5, stk. 1, første punktum, og er i strid med princippet om, at det principielt er forbudt enhver anden person end brugeren uden dennes samtykke at lagre trafikdata i forbindelse med elektronisk kommunikation.
- 9 Desuden overholder den ikke bestemmelsen i direktivets artikel 6 om, at trafikdata kun må behandles og lagres med henblik på debitering af abonnenten for tjenesterne, med henblik på markedsføring og med henblik på levering af tillægstjenester i det hertil fornødne omfang og tidsrum.

- 10 Hvis lokaliseringsdata, bortset fra trafikdata, vedrørende brugere af eller abonnenter på de offentlige kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester, kan behandles, fastsætter artikel 9, stk. 1, første punktum, i direktiv 2002/58, at disse data kun må behandles, når de er gjort anonyme, eller når brugeren eller abonnenten har givet sit samtykke hertil, og da kun i det omfang og i det tidsrum, som er nødvendigt for levering af en tillægstjeneste. Også dette krav fraviger lovens bestemmelse, for så vidt som også de dér nævnte lokaliseringsdata skal lagres i henhold til TKG's § 113b, stk. 1, nr. 2, sammenholdt med stk. 4.
- 11 Begrænsningen af rettighederne i henhold til artikel 5, stk. 1, artikel 6, stk. 1, og artikel 9, stk. 1, i direktiv 2002/58 er kun begrundet, hvis bestemmelsen i TKG's § 113a, stk. 1, første punktum, sammenholdt med § 113b, kan støttes på artikel 15, stk. 1, i direktiv 2002/58.
- 12 Ifølge denne bestemmelse kan medlemsstaterne vedtage retsfor skrifter 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 retsfor skrifter 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 for skrifter skal være i overensstemmelse med fællesskabsrettens generelle principper, herunder principperne i EU-traktatens artikel 6, stk. 1 og 2.
- 13 I henhold til det af Domstolen anførte i dommen i [de forenede sager] Tele2 Sverige og Watson m.fl., navnlig i denne doms præmis 82 ff. og 108 ff., er det en forudsætning for lovligheden af en national bestemmelse om lagring af data i henhold til artikel 15, stk. 1, i direktiv 2002/58, at der foreligger en tilstrækkelig anledning. Det betyder, at kun de personer er omfattet, for hvem der foreligger et indicium for en forbindelse til en grov straffelovsovertrædelse, at der sker en begrænsning til den region, det tidsrum samt de kommunikationsmidler, som er relevante for anledningen, og at kun de data omfattes, som er nødvendige for at opklare den nævnte straffelovsovertrædelse.
- 14 Sagsøgtes opfattelse, at allerede den omstændighed, at der benyttes internetadgangs- eller telefontjenester, skal anses for en tilstrækkelig anledning til lagring, er åbenlyst ikke i overensstemmelse med dette. Heller ikke sagsøgtes henvisning til Domstolens udtalelse af 26. juli 2017 om aftalen mellem Canada og Den Europæiske Union om overførsel af passagerlisteoplysninger kan rokke ved den antagelse, som kommer til udtryk i dommen i [de forenede sager] Tele2 Sverige og Watson m.fl., nemlig at enhver lagring af data uden anledning generelt er i strid med EU-retten. Domstolen fremhævede ganske vist i forbindelse med

nødvendigheden af de indgreb i de grundlæggende rettigheder om ret til privatliv og beskyttelse af personoplysninger, som er forbundet med aftalen, at PNR-oplysningerne formidles til Canada uafhængigt af, om der foreligger objektive indikationer af, at flypassagererne udgør en risiko for den offentlige sikkerhed i Canada. Der er imidlertid ikke tale om en lagring af data uden anledning, idet lagringen og formidlingen er knyttet til de grænsekontroller, som alle flypassagerer, der ønsker at indrejse til Canada eller udrejse fra Canada, er underlagt i henhold til gældende canadisk ret. Når flypassagererne udrejser, bortfalder denne anledning til lagringen. Den fortsatte lagring efter dette tidspunkt forudsætter derfor – som en ny anledning – at der foreligger objektive indicier for, at de pågældende flypassagerer udgør en risiko i forbindelse med terrorbekæmpelse og grænseoverskridende alvorlig kriminalitet.

- 15 Såfremt Domstolens praksis skal forstås således, at lagring af data uden anledning under ingen omstændigheder er forenelig med EU-retten, kan sagsøgte revisionsappel til prøvelse af Verwaltungsgerichts (forvaltningsdomstolens) dom ikke tages til følge. Ligesom de svenske og Det Forenede Kongeriges bestemmelser om lagring af data, som var genstand for dommen i [de forenede sager] Tele2 Sverige og Watson m.fl., kræver TKG's § 113a, stk. 1, første punktum, sammenholdt med § 113b, nemlig hverken en anledning til lagringen – ud over den blotte benyttelse af internetadgangs- eller telefontjenester – eller en sammenhæng mellem de lagrede data og en strafbar handling, henholdsvis en risiko for den offentlige sikkerhed. Der er tværtimod tale om en bestemmelse, som foreskriver en lagring af størstedelen af alle relevante telekommunikationstrafikdata, som er uden anledning, landsdækkende og personligt, tidsmæssigt og geografisk udifferentieret.
- 16 Uanset det i dommen i [de forenede sager] Tele2 Sverige og Watson m.fl. anførte anser den forelæggende ret det imidlertid ikke for udelukket, at den i TKG's § 113a, stk. 1, første punktum, sammenholdt med § 113b, regulerede pligt til at lagre telekommunikationstrafikdata uden anledning kan støttes på artikel 15, stk. 1, i direktiv 2002/58, af følgende grunde:
- 17 For det første kræver de pågældende bestemmelser i TKG ikke lagring af samtlige telekommunikationstrafikdata for alle abonnenter og registrerede brugere med hensyn til alle elektroniske kommunikationsmidler. Det er ikke kun kommunikationens indhold, der er undtaget fra lagringspligten; der må heller ikke lagres data om besøgte internetsider, data fra e-mailtjenester eller data, som er baseret på forbindelserne til eller fra visse forbindelser inden for sociale eller kirkelige områder (jf. TKG's § 113b, stk. 5 og 6). Når visse kommunikationsmidler eller kategorier af data undtages fra lagringspligten, kan dette ganske vist ikke fjerne risikoen for, at der kan udarbejdes en omfattende profil af de pågældende personer, men det kan i det mindste reducere den væsentligt.
- 18 En endnu mere tungtvejende forskel mellem de i den foreliggende sag omhandlede bestemmelser i TKG og den tidligere bestemmelse i direktiv 2006/24,

henholdsvis de svenske og Det Forenede Kongeriges bestemmelser, der var støttet på dette direktiv, og som var genstand for dommen i [de forenede sager] *Tele2 Sverige og Watson m.fl.*, ser den forelæggende ret for det andet deri, at lagringsperioden på seks måneder til to år (jf. artikel 6 i direktiv 2006/24) i henhold til TKG's artikel 113b, stk. 1, er forkortet markant til fire henholdsvis ti uger.

- 19 Risikoen for at udarbejde en omfattende profil af de pågældende personer må anses for at være mindre, jo kortere de perioder er, hvor trafikdataene lagres. Jo kortere lagringsperioden er, desto mere mangelfuld bliver personlighedsprofilen nødvendigvis, og desto mindre intenst bliver indgrebet i grundlæggende rettigheder.
- 20 For det tredje er de her omhandlede bestemmelser i TKG underlagt strenge begrænsninger med hensyn til beskyttelsen af de lagrede data og adgangen til dem. For det første sikrer bestemmelserne i TKG's §§ 113d ff. en effektiv beskyttelse af de lagrede data mod risiko for misbrug og mod enhver uberettiget adgang. For det andet må de lagrede data i henhold til TKG's § 113c, stk. 1, kun anvendes til bekæmpelse af grove straffelovsovertrædelser eller til at afværge en konkret risiko for en persons liv, helbred eller frihed eller for forbundsstatens eller en delstats beståen.
- 21 Indsamling af trafikdata med henblik på strafforfølgelse forudsætter i henhold til StPO's § 100g, stk. 2, at der er mistanke om, at der foreligger en af de særligt grove straffelovsovertrædelser, som er opregnet udtømmende i loven, at gerningen også i det konkrete tilfælde vejer særligt tungt, at det ville være væsentligt vanskeligere eller udsigtsløst at efterforske de faktiske omstændigheder eller fastslå den mistænkte opholdssted på anden måde, og at indsamlingen af dataene står i et rimeligt forhold til sagens betydning. I henhold til StPO's § 100g, stk. 4, er det ikke tilladt at indsamle eller anvende trafikdata for personer, som i henhold til StPO's § 53, stk. 1, første punktum, nr. 1-5, er pålagt professionel tavshedspligt, herunder bl.a. advokater, læger eller journalister. StPO's § 101a, stk. 1, kræver desuden en retsligt indgriben, for at der kan ske indsamling af trafikdata i henhold til StPO's § 100g.
- 22 Disse begrænsende adgangsbestemmelser gælder ganske vist ikke for en internetprotokoladresse, som er tildelt abonnenten til en internetbenyttelse. Denne må nemlig i henhold til TKG's § 113c, stk. 1, nr. 3, også anvendes i forbindelse med en stamdataoplysning med henblik på forfølgelse af enhver form for strafbare handlinger, for at afværge farer for den offentlige sikkerhed og orden samt for at opfylde efterretningstjenesternes opgaver. Imidlertid må det lægges til grund, at oplysningen om, hvilken abonnent der var anmeldt på internettet under en allerede kendt internetprotokoladresse, ikke tillader udarbejdelse af personligheds- og bevægelsesprofiler.
- 23 Selv hvis SpaceNets anbringende følges, og det lægges til grund, at der i stigende omfang anvendes tekniske procedurer, hvor en internetprotokoladresse ikke

længere entydigt kan henføres til en bestemt telekommunikationsforbindelse, men kun til en større gruppe af forbindelser, og stamdataoplysningen derfor har udviklet sig til en foranstaltning med en betragtelig spredning, er en sådan stamdataoplysning fortsat et betydeligt mindre intensivt indgreb end indsamling og anvendelse af telekommunikationstrafikdata.

- 24 For det fjerde taler det også til fordel for, at pligten til uden anledning at lagre telekommunikationstrafikdata, som er reguleret i TKG's § 113a, stk. 1, første punktum, sammenholdt med § 113b, kan støttes på artikel 15, stk. 1, i direktiv 2002/58, at den nationale lovgiver dermed er efterkommet den pligt til at handle, som for medlemsstaterne følger af retten til sikkerhed, som er garanteret ved chartrets artikel 6. I dommen i [de forenede sager] Digital Rights Ireland m.fl. nævnte Domstolen udtrykkeligt chartrets artikel 6 og påpegede i denne forbindelse, at bekæmpelsen af international terrorisme med henblik på opretholdelse af international fred og sikkerhed udgør et mål for EU af almen interesse, og at det samme gælder for bekæmpelsen af grov kriminalitet med henblik på at sikre den offentlige sikkerhed.
- 25 På denne baggrund er den forelæggende ret i tvivl om, hvorvidt Domstolens hidtidige praksis skal forstås således, at lagring af data uden anledning ikke kun i den konkrete udformning, den fandt i direktiv 2006/24, og i bestemmelserne i Sverige og Det Forenede Kongerige, der var støttet herpå, men generelt ikke kan støttes på artikel 15, stk. 1, i direktiv 2002/58. Det grundlæggende koncept i forbindelse med lagring af data kan nemlig ikke forenes med Domstolens krav – som er formuleret uden begrænsninger – om, at der i forbindelse med lagring af data skal differentieres efter personer, perioder og geografiske områder.
- 26 Efter den forelæggende rets opfattelse taler også kravet om at etablere en balance mellem på den ene side medlemsstaternes forpligtelse til at garantere sikkerheden for de personer, der opholder sig på deres område, og på den anden side overholdelsen af de grundlæggende rettigheder, der er forankret i chartrets artikel 7 og 8, imod at lægge til grund, at lagring af trafikdata uden anledning *per se* er uforenelig med chartret.
- 27 Den forelæggende ret kan derfor ikke udlede entydigt af Domstolens praksis, at de nationale lovgivere ikke længere skal have mulighed for på grundlag af en samlet afvejning at indføre en lagring af data uden anledning, eventuelt suppleret med strenge adgangsregler, for at tage højde for det specifikke risikopotentiale, som er knyttet til de nye telekommunikationsmidler.
- 28 For det femte gør den forelæggende ret opmærksom på, at i tilfælde af, at en lagring af data uden anledning generelt ikke kan støttes på artikel 15, stk. 1, i direktiv 2002/58, og at det følger ikke kommer an på de konkrete ordninger vedrørende de omfattede kommunikationsmidler, kategorierne af lagrede data, lagringens varighed, betingelserne for adgang til de lagrede data og beskyttelsen mod risici for misbrug, er de nationale lovgiveres handlemuligheder væsentligt begrænset på et område inden for strafforfølgelse og offentlig sikkerhed, som i

henhold til artikel 4, stk. 2, tredje punktum, TEU i hvert fald principielt fortsat hører under de enkelte medlemsstaters enekompetence.

- 29 For det sjette står det, bl.a. på baggrund af den nyere praksis fra Den Europæiske Menneskerettighedsdomstol (herefter »EMD«), ikke klart for den forelæggende ret, om det af Domstolen anførte i dommen i [de forenede sager] Tele2 Sverige og Watson m.fl. skal forstås som et forbud rettet til medlemsstaterne mod at støtte indførelse af en pligt til at lagre telekommunikationstrafikdata uden anledning på artikel 15, stk. 1, i direktiv 2002/58.
- 30 EMD har senest i en dom af 19. juni 2018 udtalt, at de svenske bestemmelser om masseovervågning af den grænseoverskridende datatrafik er i overensstemmelse med artikel 8 i Den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder (EMRK). I betragtning af de trusler, som stater aktuelt er udsat for, herunder den globale terrorismes svøbe og andre grove forbrydelser såsom narkotikahandel, menneskehandel, seksuel udnyttelse af børn og internetkriminalitet, samt på grund af de tekniske fremskridt, som gør det lettere for terrorister og kriminelle at undgå at blive opdaget på internettet, og de uforudsigelige transmissionsveje for elektroniske data, hører beslutningen om at etablere et masseovervågningssystem med henblik på at opdage hidtil ukendte trusler mod den nationale sikkerhed fortsat under statens skønsbeføjelse (EMD, dom af 19.6.2018, nr. 35252/08 (ECLI: CE:ECHR:2018:0619JUD003525208), Centrum för Rättvisa mod Sverige, § 112). Når EMD henviser til de uforudsigelige transmissionsveje for elektroniske data og til de tekniske fremskridt, som gør det lettere for terrorister og kriminelle at undgå at blive opdaget på internettet, fremhæver den tydeligere end Den Europæiske Unions Domstol det specifikke risikopotentiale, som er forbundet med de nye telekommunikationsmidler.
- 31 Den forelæggende ret henviser til ellefte betragtning til direktiv 2002/58 og chartrets artikel 52, stk. 3, hvoraf det følger, at der skal skabes den nødvendige sammenhæng mellem de rettigheder, der er forankret i chartret, og de tilsvarende rettigheder, som er garanteret ved EMRK, uden at dette berører EU-rettens og Den Europæiske Unions Domstols selvstændighed.
- 32 Afslutningsvis nævner den forelæggende ret andre verserende præjudicielle sager, som drejer sig om fortolkningen af dommen i [de forenede sager] Tele2 Sverige og Watson m.fl., altså spørgsmålet om, hvorvidt der af denne kan udledes et generelt forbud mod at lagre data uden anledning, som hverken kan overvindes af hensyn til alvoren af de risici for den offentlige sikkerhed, der skal bekæmpes, eller i forbindelse med en »kompensation« i form af restriktive adgangsregler og høje sikkerhedskrav.
- 33 Den forelæggende ret nævner de præjudicielle anmodninger indgivet af Investigatory Powers Tribunal, London (Det Forenede Kongerige) (C-623/17), de præjudicielle anmodninger indgivet af Conseil d'État (Frankrig) (C-511/18 og C-

512/18) og den præjudicielle anmodning indgivet af den belgiske forfatningsdomstol (C-520/18).

ARBEJDS  
DOKUMENT