BILAG 4

JUSTITSMINISTERIET
Lovafdelingen

Dato: 2. juni 2014
Kontor: EU-retskontoret
Sagsbeh: Nicholas Rahui Webster Rømer
Sagsnr.: 2014-6140-0620
Dok.: 1188632

Notat om betydningen af EU-Domstolens dom af 8. april 2014 i de forenede sager C-293/12 og C-594/12 (om logningsdirektivet) for de danske logningsregler

1. Indledning

EU-Domstolen har ved dom af 8. april 2014 i de forenede sager C-293/12 og C-594/12 erklæret direktiv 2006/24/EF af 15. marts 2006 (herefter logningsdirektivet) ugyldigt under henvisning til, at EU-lovgiver har overskredet de grænser, som overholdelsen af proportionalitetsprincippet kræver, henset til artikel 7, 8 og 52, stk. 1, i Den Europæiske Unions Charter om grundlæggende rettigheder (herefter Charteret).

Nedenfor under pkt. 2 redegøres for EU-Domstolens bemærkninger i dommen af 8. april 2014. Dernæst redegøres under pkt. 3 for gældende dansk ret for så vidt angår logning, øvrige regler, der angår registrering og opbevaring af personers tele- og internetkommunikation, og udvalgte bestemmelser i persondataloven. Pkt. 4 indeholder Justitsministeriets vurdering af dommens betydning for de danske logningsregler, herunder muligheden for at opretholde gældende lovgivning. Den samlede konklusion fremgår under pkt. 5.

2. EU-Domstolens bemærkninger i de forenede sager C-293/12 og C-594/12

EU-Domstolen fastslår indledningsvis, at den pligt, der i henhold til (det nu ugyldige) logningsdirektiv gælder med hensyn til at lagre de i direktivets artikel 5 nævnte data samt de kompetente nationale myndigheders adgang til dataene, udgør et indgreb i de rettigheder, der er sikret ved Charterets artikel 7 om retten til respekt for privat- og familieliv, jf. præmis 34-35. Domstolen fastslår endvidere, at direktivet ligeledes indebærer et indgreb i den grundlæggende ret til beskyttelse af personoplysninger, som er

Slotsholmsgade 10
1216 København K.

Telefon 7226 8400
Telefax 3393 3510

www.justitsministeriet.dk
jm@jm.dk

sikret ved Charterets artikel 8, eftersom det foreskriver en behandling af personoplysninger, jf. præmis 36. Domstolen bemærker på den baggrund, at det indgreb i de grundlæggende rettigheder, som direktivet herved indebærer, er meget vidtrækkende og må anses for at være af særligt alvorlig karakter. Den omstændighed, at lagringen af data og den efterfølgende anvendelse af dem finder sted, uden at abonnenten eller den registrerede bruger oplyses herom, er egnet til at skabe en følelse hos de berørte personer af, at deres privatliv er genstand for konstant overvågning, jf. præmis 37.

EU-Domstolen undersøger herefter, om indgrebet kan begrundes.

EU-Domstolen fastslår i den forbindelse, at den lagring af data, som kræves i henhold til direktivet, ikke er af en karakter, der kan krænke det væsentligste indhold af den grundlæggende ret til respekt for privatliv og beskyttelse af personoplysninger. Direktivet giver således ikke mulighed for at gøre sig bekendt med indholdet af den elektroniske kommunikation som sådan og bestemmer, at udbydere af tjenester eller telenet skal overholde visse principper om beskyttelse og sikkerhed vedrørende data, jf. præmis 38-40.

Endvidere fastslår EU-Domstolen, at lagring af data med henblik på en eventuel udlevering af disse til de kompetente nationale myndigheder i forbindelse med efterforskning, afsløring og retsforfølgning af grov kriminalitet i medlemsstaterne, forfølger et formål af almen interesse, nemlig bekæmpelse af grov kriminalitet samt i sidste ende at bidrage til den offentlige sikkerhed, jf. præmis 41-44.

EU-Domstolen undersøger dernæst, om EU-lovgiver ved at vedtage direktivet overskred de grænser, der følger af proportionalitetsprincippet, dvs. om direktivet er udfærdiget på en sådan måde, at det både er egnet til at nå det tilsigtede lovlige mål (bekæmpelse af grov kriminalitet og beskyttelse af den offentlige sikkerhed) og ikke går videre, end hvad der er nødvendigt og passende for at nå dette mål, jf. præmis 46. Domstolen bemærker i den forbindelse, at EU-lovgivers skønsbeføjelse – henset dels til den betydelige rolle, som beskyttelsen af personoplysninger spiller i forhold til den grundlæggende ret til respekt for privatliv, dels til rækkevidden og alvoren af det indgreb i denne ret, som direktivet indebærer – er begrænset, således at der skal foretages en streng efterprøvelse, jf. præmis 47-48.

Det er EU-Domstolens opfattelse, at den lagring af data, der kræves i henhold til direktivet, kan anses for *egnet* til at gennemføre det mål, som forfølges med det nævnte direktiv, jf. præmis 49.

For så vidt angår vurderingen af, om direktivet går videre, end hvad der er nødvendigt og passende for at nå det tilsigtede mål (dvs. om direktivet er proportionalt), udtaler EU-Domstolen, at selv om bekæmpelse af grov kriminalitet, navnlig organiseret kriminalitet og terrorisme, er af afgørende betydning for at beskytte den offentlige sikkerhed, kan et sådant mål af almen interesse, hvor grundlæggende det end er, ikke i sig selv begrunde, at en foranstaltning som den lagring, der finder sted efter direktivet, anses som nødvendig. Beskyttelsen af personoplysninger har en særlig betydning for retten til respekt for privatlivet, der efter EU-Domstolens faste praksis kræver, at undtagelser fra eller begrænsninger i beskyttelsen af personoplysninger skal holdes inden for det strengt nødvendige, jf. præmis 51-53.

EU-Domstolen anfører på den baggrund i præmis 54, at EU-lovgivningen skal fastsætte klare og præcise regler, som regulerer rækkevidden og anvendelsen af den omhandlede foranstaltning og opstiller en række mindstekrav, således at de personer, hvis data er blevet lagret, råder over tilstrækkelige garantier, der gør det muligt effektivt at beskytte deres personlige oplysninger mod risikoen for misbrug og mod ulovlig adgang til og anvendelse af disse oplysninger.

I forlængelse heraf understreger EU-Domstolen, at behovet for at råde over sådanne garantier er så meget desto større, når persondata er undergivet automatisk databehandling, og hvor der er en betydelig risiko for ulovlig adgang til disse data, jf. præmis 55.

Det er EU-Domstolens opfattelse, at direktivet ikke fastsætter klare og præcise regler, der regulerer rækkevidden af indgrebet i de grundlæggende rettigheder beskyttet i Charterets artikel 7 og 8, hvorfor direktivet indebærer et indgreb i disse grundlæggende rettigheder, som er meget vidtrækkende og af særligt alvorlig karakter i EU's retsorden, uden at dette indgreb er præcist afgrænset af bestemmelser, der gør det muligt at sikre, at det faktisk er begrænset til det strengt nødvendige. Domstolens begrundelse herfor er treleddet:

For det første omfatter direktivet generelt alle personer, alle elektroniske kommunikationsmidler og samtlige trafikdata, uden at der i direktivet fore-

tages nogen form for differentiering, begrænsning eller undtagelse under hensyn til målet om bekæmpelse af grov kriminalitet, jf. præmis 57.

Dels omfatter direktivet således generelt alle personer, der gør brug af elektroniske kommunikationstjenester, uden at de personer, hvis data lagres, dog – end ikke indirekte – befinder sig i en situation, der vil kunne give anledning til strafferetlig forfølgning, og indeholder endvidere ikke nogen undtagelsesbestemmelse og finder således anvendelse selv på personer, hvis kommunikation i henhold til nationale retsregler er omfattet af tavshedspligt. Dels kræver direktivet ikke nogen sammenhæng mellem de data, som foreskrives lagret, og en trussel mod den offentlige sikkerhed, og det er navnlig ikke begrænset til en lagring, som er rettet mod data vedrørende et bestemt tidsrum og/eller et bestemt geografisk område og/eller en given personkreds, der på den ene eller den anden måde vil kunne være indblandet i grov kriminalitet, eller mod personer, der af andre grunde gennem lagring af deres data ville kunne bidrage til forebyggelse, afsløring og retsforfølgning af grov kriminalitet, jf. præmis 58-59.

For det andet fastsætter direktivet ikke et objektivt kriterium, der gør det muligt at afgrænse de kompetente nationale myndigheders adgang til dataene og den efterfølgende anvendelse af disse med henblik på forebyggelse, afsløring eller strafferetlig retsforfølgning vedrørende kriminalitet, der – henset til rækkevidden og alvoren af indgrebet i rettighederne, der er beskyttet i Charterets artikel 7 og 8 – kan anses for tilstrækkeligt grov til at begrunde et sådant indgreb. I direktivets artikel 1, stk. 1, er der i stedet alene henvist til "grov kriminalitet" som defineret i national ret, jf. præmis 60.

Endvidere indeholder direktivet ingen materielle og processuelle betingelser for de kompetente nationale myndigheders adgang til dataene og efterfølgende anvendelse heraf. Direktivet foreskriver således ikke udtrykkeligt, at denne adgang og efterfølgende anvendelse skal være strengt begrænset til forebyggelse og afsløring af præcist afgrænsede strafbare handlinger eller strafferetlig retsforfølgning heraf, jf. præmis 61.

Navnlig fastsætter direktivet ikke noget objektivt kriterium, der gør det muligt at begrænse antallet af personer, der er bemyndigede til at få adgang til og efterfølgende anvende lagrede data til det strengt nødvendige henset til formålet. Særligt er myndighedernes adgang til lagrede data ikke undergivet en forudgående kontrol, der udøves enten af en retsinstans eller af en uafhængig administrativ enhed, jf. præmis 62.

For det tredje foreskriver direktivet, at dataene skal lagres i minimum 6 måneder og maksimum 2 år, uden at der på nogen måde foretages en sondring mellem de forskellige kategorier af data efter deres relevans for det mål, som forfølges, eller afhængigt af, hvilke personer der er berørt. Det er således ikke præciseret, at fastsættelsen af lagringsperioden skal være baseret på objektive kriterier for at sikre en begrænsning til det strengt nødvendige, jf. præmis 63-64.

EU-Domstolen anfører på den baggrund, at direktivet ikke fastsætter klare og præcise regler, der regulerer rækkevidden af indgrebet i de grundlæggende rettigheder, som er fastslået i Chartrets artikel 7 og 8. Derfor fastslås det, at direktivet indebærer et indgreb i disse grundlæggende rettigheder, som er meget vidtrækkende og af særligt alvorlig karakter i EU's retsorden, uden at dette indgreb er præcist afgrænset af bestemmelser, der gør det muligt at sikre, at det faktisk er begrænset til det strengt nødvendige, jf. præmis 65.

I de efterfølgende præmisser fastslår EU-Domstolen derudover, at direktivet ikke fastsætter tilstrækkelige garantier, der gør det muligt at sikre en effektiv beskyttelse af data – sådan som det er påkrævet efter artikel 8 i Charteret – mod risikoen for misbrug og mod enhver ulovlig adgang til og benyttelse af disse data. Der er således ikke fastsat regler, som er specifikke og tilpasset den meget store mængde data, til disse datas følsomme karakter samt til risikoen for ulovlig adgang til dataene, og som navnlig skulle udgøre en klar og streng regulering af beskyttelsen og sikkerheden af de omhandlede data med henblik på at sikre deres integritet og fortrolighed. Domstolen anfører endvidere, at direktivet sammenholdt med de relevante bestemmelser i direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (Direktiv om databeskyttelse inden for elektronisk kommunikation) (herefter e-data-beskyttelsesdirektivet) og direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (herefter databeskyttelsesdirektivet) ikke sikrer, at udbyderne anvender et særlig højt beskyttelses- og sikkerhedsniveau ved hjælp af tekniske og organisatoriske foranstaltninger, men bl.a. tillader disse at tage økonomiske hensyn i betragtning ved fastlæggelsen af det sikkerhedsniveau, de anvender. Navnlig sikrer direktivet ikke en irreversibel destruktion af dataene ved udløbet af lagringsperioden, jf. præmis 66-67.

Endelig bemærker EU-Domstolen, at direktivet ikke fastsætter krav om, at dataene skal lagres inden for EU's område. Domstolen konstaterer, at det derfor ikke kan antages, at det fuldt ud er sikret, at overholdelse af kravene om beskyttelse og sikkerhed kontrolleres af en uafhængig myndighed, således som det udtrykkeligt påkræves efter Charterets artikel 8, stk. 3, jf. præmis 68.

EU-Domstolen erklærer henset til samtlige ovenstående betragtninger logningsdirektivet ugyldigt med henvisning til, at EU-lovgiver med vedtagelsen af direktivet anses for ikke at have handlet i overensstemmelse med proportionalitetsprincippet i lyset af Charterets artikel 7, 8 og 52, stk. 1, jf. præmis 69.

3. Dansk ret

3.1. Nedenfor redegøres først for de danske regler om logning, jf. pkt. 3.2. Dernæst redegøres for reglerne i telelovgivningen, der regulerer teleudbyderes adgang til i visse nærmere bestemte situationer at registrere og opbevare personers tele- og internetkommunikation, jf. pkt. 3.3. Endelig redegøres for udvalgte bestemmelser i persondataloven, jf. pkt. 3.4.

3.2.1. Ved lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse af FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.) (anti-terrorpakke I), blev der indsat en bestemmelse i retsplejelovens § 786, stk. 4, om registrering og opbevaring af oplysninger om teletrafik samt om telenet- og teletjenesteudbyderes praktiske bistand til politiet.

Det fremgår af forarbejderne til denne lov (pkt. 3.1.1.1 i de almindelige bemærkninger til lovforslag nr. L 35 fremsat den 13. december 2001), at bestemmelsen er indsat på baggrund af et forslag fra Justitsministeriets udvalg om økonomisk kriminalitet og datakriminalitet (Brydensholt-udvalget) i betænkning nr. 1377/1999 om børnepornografi og IT-efterforskning.

3.2.2. Efter retsplejelovens § 786, stk. 4, påhviler det udbydere af telenet eller teletjenester at foretage registrering og opbevaring i 1 år af oplysnin-

ger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. Efter bestemmelsen fastsætter justitsministeren efter forhandling med (nu) erhvervs- og vækstministeren nærmere regler om denne registrering og opbevaring.

Det fremgår af forarbejderne til lov nr. 378 af 6. juni 2002 (bemærkningerne til § 2, nr. 2 og 3, i lovforslaget), at retsplejelovens § 786, stk. 4, indebærer pligt for udbydere af telenet og teletjenester til at registrere både tele- og internetkommunikation.

Det er endvidere i forarbejderne (pkt. 1.2 i de almindelige bemærkninger til lovforslaget) forudsat, at udbydere alene skal registrere og opbevare oplysninger om, hvem der har haft kontakt, men ikke oplysninger om, hvad indholdet af kommunikationen imellem de pågældende var.

Bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen) er udstedt med hjemmel i bl.a. retsplejelovens § 786, stk. 4.

Det fremgår af logningsbekendtgørelsens § 1, at udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal foretage registrering og opbevaring af oplysninger om teletrafik, der genereres eller behandles i deres net, således at disse oplysninger vil kunne anvendes som led i efterforskning og retsforfølgning af strafbare forhold.

Efter logningsbekendtgørelsens § 4 skal teleudbydere registrere en række nærmere angivne oplysninger om fastnet- og mobiltelefoni samt SMS-, EMS- og MMS-kommunikation, herunder oplysninger om det opkaldte og det opkaldende nummer og tidspunktet for kommunikationens start og afslutning.

Efter logningsbekendtgørelsens § 5 skal teleudbydere registrere en række nærmere angivne oplysninger om internettrafik. Det gælder bl.a. oplysninger om en brugers adgang til internettet og tidspunktet for kommunikationens start og afslutning. Der skal endvidere registreres oplysninger om selve internetsessionen, dvs. kilden og endepunktet for en internetkommunikation (sessionslogning).

Efter logningsbekendtgørelsens § 6 skal teleudbydere registrere en række nærmere angivne oplysninger om brug af udbyderens egne e-mail- og in-

ternettelefonitjenester, herunder bl.a. oplysninger om modtagende og afsendende e-mail-adresser.

Det bemærkes i den forbindelse, at logningsbekendtgørelsen på enkelte punkter går videre end de forpligtigelser, der følger af logningsdirektivet, som er et minimumsdirektiv. Ifølge bekendtgørelsens § 4, stk. 1, nr. 6, skal der således registreres og opbevares oplysninger om den første og sidste mast, som en mobiltelefon er forbundet til som led i en kommunikation, mens direktivet kun stiller krav om, at der registreres og opbevares oplysninger om den første mast, jf. direktivets artikel 5, stk. 1, litra f, nr. 1.

For så vidt angår internetkommunikation går logningsbekendtgørelsen videre end direktivet, idet oplysninger om internetsessionen (også kaldet sessionslogning), dvs. kilden og endepunktet for en internetkommunikation, skal registreres og opbevares jf. § 5, stk. 1 og stk. 4. Der skal tillige logges oplysninger om trådløs adgang til internettet, herunder oplysninger om det lokale netværks geografiske placering samt identiteten på det benyttede kommunikationsudstyr.

3.2.3. Efter retsplejelovens § 786, stk. 4, og logningsbekendtgørelsens § 9 skal de registrerede oplysninger opbevares i 1 år.

For så vidt angår opbevaring af teletrafikdata fremgår det bl.a. af forarbejderne til lov nr. 378 af 6. juni 2002 (pkt. 3.1.3.1 i de almindelige bemærkninger til lovforslaget), at

> "Justitsministeriet foreslår, at opbevaringsperiodens varighed fastsættes til 1 år. Dette vil være i overensstemmelse med Europa-Parlamentet og Rådets direktiv om behandling af personoplysninger og beskyttelse af privatlivets fred inden for telesektoren (97/66/EF), jf. pkt. 2.1.2. ovenfor. I det omfang, der ikke er tale om oplysninger, der i henhold til direktivet kan opbevares med henblik på kundedebitering, kan opbevaringstiden ikke være længere end hensynet til "forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager" tilsiger, jf. direktivets artikel 14, stk. 1. Efter Justitsministeriets opfattelses går en opbevaringsperiode på 1 år ikke videre, end dette hensyn tilsiger."

For så vidt angår opbevaring af internettrafikdata fremgår det endvidere af de nævnte forarbejder (pkt. 3.1.3.2 i de almindelige bemærkninger til lovforslaget), at

> "[d]er er, som [Brydensholt-]udvalget ligeledes anfører, tale om en vanskelig afvejning mellem på den ene side hensynet til kriminalitetsbekæmpelse og på den anden side hensynet til både privatlivets

> fred og de omkostninger, der påføres udbyderne. Særligt vedrørende hensynet til privatlivets fred tilsiger dette hensyn, at der logges mindst muligt, og at loggen opbevares i så kort tid som muligt, idet risikoen for, at oplysningerne falder i de forkerte hænder, er større, jo længere opbevaringsperioden er.
>
> Imidlertid tager selv terrorhandlinger af væsentlig mindre omfang end de tragiske angreb på New York og Washington den 11. september 2001 normalt lang tid at planlægge. Justitsministeriet finder det i lyset heraf tvivlsomt, om en opbevaringsfrist på kun 6 måneder dækker det behov for adgang til oplysninger, som politiet måtte have i en konkret sag. Efter Justitsministeriets opfattelse bør der derfor lægges afgørende vægt på de efterforskningsmæssige hensyn, der som Brydensholt-udvalget påpeger taler for en frist på ikke under 1 år. Justitsministeriet stiller på den baggrund forslag om en lovfæstet opbevaringsperiode på 1 år."

3.2.4. Det følger af § 1 i logningsbekendtgørelsen, at de registrerede oplysninger skal opbevares med henblik på at kunne anvendes som led i efterforskning og retsforfølgning af strafbare forhold.

De nærmere betingelser for, hvornår udbydere af telenet og teletjenester skal udlevere oplysningerne, fremgår af retsplejelovens regler om indgreb i meddelelseshemmeligheden og edition.

3.2.4.1. De oplysninger om teletrafik, som teleudbydere ifølge logningsbekendtgørelsen skal registrere, udgør i vidt omfang historiske teleoplysninger i retsplejelovens forstand. Det betyder efter retspraksis, at indhentelse af oplysningerne kan finde sted efter reglerne om edition, hvis betingelserne for indgreb i meddelelseshemmeligheden samtidig er opfyldt.

Visse oplysninger, som er registreret hos en teleudbyder i henhold til logningsbekendtgørelsen, vil dog kunne indhentes alene efter reglerne om edition. Det drejer sig navnlig om oplysninger om de master, som en mobiltelefon er forbundet til som led i en kommunikation, samt oplysning om, hvem der på et givet tidspunkt har været bruger af en specifik internetprotokol-adresse.

Retsplejelovens regler om indgreb i meddelelseshemmeligheden og edition gennemgås nærmere nedenfor.

3.2.4.2. Det er alene politiet, der efter retsplejelovens § 780 kan foretage indgreb i meddelelseshemmeligheden, herunder få udleveret registrerede historiske teleoplysninger.

De nærmere betingelser for at foretage indgreb i meddelelseshemmeligheden fremgår navnlig af retsplejelovens §§ 781-783.

Retsplejelovens § 781 opstiller særlige krav til mistankegrundlaget (mistankekravet), behovet for at foretage indgrebet (indikationskravet) samt til grovheden af den kriminalitet, som efterforskningen angår (kriminalitetskravet). Således kræves det, at der foreligger bestemte grunde til at antage, at der på den pågældende måde gives meddelelser eller foretages forsendelser til eller fra en mistænkt, ligesom indgrebet må antages at være af afgørende betydning for efterforskningen. Det er endvidere et krav, at efterforskningen angår en lovovertrædelse, som efter loven kan straffes med fængsel i 6 år eller derover, en forsætlig overtrædelse af f.eks. straffelovens kapitel 12 (forbrydelser mod statens selvstændighed og sikkerhed) og 13 (forbrydelser mod statsforfatningen og de øverste statsmyndigheder, terrorisme m.v.), eller en række særligt oplistede bestemmelser i straffeloven og særlovgivningen, herunder bl.a. udlændingeloven.

Fælles for disse særligt oplistede bestemmelser, jf. retsplejelovens § 781, stk. 1, nr. 3, sidste led, stk. 2 og stk. 3, er, at de alle har en lavere strafferamme end 6 års fængsel, jf. det generelle strafferammekrav i retsplejelovens § 781, stk. 1, nr. 3.

Bestemmelserne om indgreb i meddelelseshemmeligheden har i det væsentligste fået deres nuværende udformning ved lov nr. 227 af 6. juni 1985, der er udarbejdet på grundlag af Strafferetsplejeudvalgets betænkning nr. 1023/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter.

Straffelovens § 124, stk. 2 (ændret fra stk. 1 til stk. 2 ved lov nr. 382 af 6. juni 2002), og §§ 125, 127, stk. 1, 266 og 281 blev indsat i retsplejelovens § 781, stk. 1, nr. 3, ved denne lov. Det fremgår i den forbindelse af pkt. 2.4 i de almindelige bemærkninger til lovforslaget, at de nævnte bestemmelser blev taget med under henvisning til betænkning nr. 1023/1984.

Det fremgår af betænkningen s. 51, at der i udvalget var enighed om, at der generelt bør sættes snævre grænser for politiets indgreb i meddelelseshemmeligheden. Samtidig påpegede udvalget, at der i det moderne samfund findes nye kriminalitetsformer, der er kendetegnet ved, at sædvanlige efterforskningsmetoder ikke er tilstrækkelige.

Det fremgår nærmere af betænkning nr. 1023/1984, s. 91f, at udvalget har fundet det nødvendigt at føje enkelte bestemmelser til hovedreglen om et kriminalitetskrav på 6 års fængsel i strafferammen. Indføjelse af straffelovens §§ 124, 125 og 127, stk. 1, begrundes med, at de har karakter af komplot, og at telefonaflytning kan være en hensigtsmæssig foranstaltning til at hindre eller opklare fangeflugt. For så vidt angår straffelovens § 281 fremgår det, at telefonaflytning og teleoplysninger her er helt relevante efterforskningsmidler. Vedrørende straffelovens § 266 lægger udvalget vægt på, at telefonkommunikation netop er et særligt egnet middel til at fremsætte trusler, hvorfor telefonaflytning kan være nødvendig for at afsløre den truendes identitet.

Straffelovens § 235 om børnepornografi blev indsat i retsplejelovens § 781, stk. 1, nr. 3, ved lov nr. 441 af 31. maj 2000. Det fremgår bl.a. af pkt. 8.3.2 i de almindelige bemærkninger til lovforslaget, at det fortsat er Justitsministeriets principielle synspunkt, at der generelt bør sættes snævre grænser for politiets adgang til at foretage indgreb i meddelelseshemmeligheden, men at der imidlertid kan være særlige kriminalitetsformer, hvor sædvanlige efterforskningsmetoder ikke er tilstrækkelige. Justitsministeriet finder derfor, at der løbende på baggrund af udviklingen i kriminalitetsformerne må tages stilling til, om der – på enkelte områder – er særlige behov for at udvide adgangen til at foretage indgreb i meddelelseshemmeligheden. Der må i den forbindelse foretages en overordnet afvejning mellem på den ene side hensynet til en effektiv kriminalitetsbekæmpelse og på den anden side hensynet til borgernes privatliv. Det fremgår endvidere, at Justitsministeriet på det foreliggende grundlag kun har overvejet, om der bør være adgang til at foretage indgreb i meddelelseshemmeligheden ved efterforskning af sager om udbredelse og besiddelse af børnepornografi, da denne kriminalitet i høj grad begås ad elektronisk vej, hvor mere traditionelle efterforskningsmetoder ikke er tilstrækkelige, hvorfor der i sager af denne karakter skal være mulighed for at foretage indgreb i meddelelseshemmeligheden, uanset at det almindelige krav om mindst 6 års fængsel i strafferammen ikke er opfyldt.

Straffelovens § 233, stk. 1, (tidligere § 228) om rufferi blev indsat i retsplejelovens § 781, stk. 1, nr. 3, ved lov nr. 436 af 10. juni 2003. Der henvises i pkt. 6.2 i de almindelige bemærkninger til lovforslaget på ny til, at der generelt bør sættes snævre grænser for politiets adgang til at foretage indgreb i meddelelseshemmeligheden, og at der i forbindelse med overvejelser om, at udvide adgangen hertil foretages en overordnet afvejning af på den ene side hensynet til en effektiv kriminalitetsbekæmpelse og på den

anden side hensynet til borgernes privatliv, men at der imidlertid kan være særlige kriminalitetsformer, hvor sædvanlige efterforskningsmetoder ikke er tilstrækkelige. Det fremgår i den forbindelse bl.a., at udviklingen i det danske prostitutionsmiljø, herunder den mere organiserede måde prostitution drives på i dag, har medført, at politiet har fået stadig vanskeligere ved at efterforske og opklare bagmandsvirksomhed i forbindelse med prostitution, og at frygten for repressalier afholder de prostituerede, der udnyttes ved bagmændenes virksomhed, fra at medvirke til sagens opklaring.

Muligheden for at foretage indgreb i meddelelseshemmeligheden ved mistanke om overtrædelse af udlændingelovens § 59, stk. 7, nr. 1-5 (dengang § 59, stk. 3, og senere § 59, stk. 5), om forsætlig bistand til udlændinge med ulovlig indrejse, ophold, arbejde samt vidererejse blev indsat i retsplejelovens § 781, stk. 1, nr. 3, ved lov nr. 411 af 6. oktober 1997.

Det fremgår af pkt. 3.3 i de almindelige bemærkninger til lovforslaget fra 1997, at indgreb i meddelelseshemmeligheden i mange tilfælde vil være et relevant efterforskningsmiddel i forhold til kriminalitet, som er kendetegnet ved, at den begås af flere personer i forening, og at der på den baggrund bør være adgang til indgreb i meddelelseshemmeligheden for kriminalitetsformer, der ofte begås af en flerhed af personer, i det omfang, der er tale om kriminalitet af en sådan alvorlig karakter, at sådanne indgreb er velbegrundede.

Det fremgår endvidere af Retsudvalgets betænkning over lovforslaget, at baggrunden for ændringsforslaget, hvorefter en overtrædelse af udlændingelovens § 59, stk. 7, nr. 1-5, blev indsat i retsplejelovens § 781, stk. 1, nr. 3, var, at udviklingen i den internationale menneskesmugling i stadig stigende omfang bar præg af professionel planlægning, at en meget stor andel af asylansøgerne var kommet til Danmark illegalt, bistået af personer, der mod betaling havde hjulpet de pågældende hertil, at menneskesmugling udgjorde en grov kriminalitetsform, og at det således var af afgørende betydning at styrke politiets muligheder for at optrevle den professionelle menneskesmugling ved at give politiet adgang til at foretage indgreb i meddelelseshemmeligheden som led i efterforskningen af sager om menneskesmugling. Det fremgår endvidere, at de almindelige betingelser for at foretage indgreb i meddelelseshemmeligheden, herunder mistankekravet (§ 781, stk. 1, nr. 1) og indikationskravet (retsplejelovens § 781, stk. 1, nr. 2) også gælder i disse sager. Herudover gælder kravet om proportionalitet i retsplejelovens § 782.

Efter retsplejelovens § 782 må indgrebet ikke være uforholdsmæssigt i forhold til indgrebets formål, sagens betydning og den krænkelse og ulempe, som indgrebet må antages at forvolde den eller de personer, som det rammer.

Endvidere foreskriver retsplejelovens § 783, at indgreb i meddelelseshemmeligheden alene kan ske efter indhentelse af en retskendelse, medmindre indgrebets øjemed ville forspildes, hvis retskendelse skulle afventes. I så fald skal indgrebet forelægges for retten senest 24 timer fra indgrebets iværksættelse.

Det følger af retsplejelovens § 784, stk. 1, at der – inden retten træffer afgørelse efter § 783 – skal beskikkes en advokat for den, som indgrebet vedrører, og at advokaten skal have lejlighed til at udtale sig.

Endelig følger det af retsplejelovens § 788, at der efter afslutningen af et indgreb i meddelelseshemmeligheden skal gives underretning om indgrebet til bl.a. indehaveren af den pågældende telefon ved telefonaflytning og teleoplysning, medmindre underretning eksempelvis vil være til skade for efterforskningen i en anden verserende sag om en lovovertrædelse, som efter loven kan danne grundlag for et indgreb i meddelelseshemmeligheden, jf. retsplejelovens § 788, stk. 4.

3.2.4.3. For så vidt angår reglerne om edition fremgår det af retsplejelovens § 804, at retten som led i efterforskningen af en lovovertrædelse, der er undergivet offentlig påtale, kan meddele en person, der ikke er mistænkt, pålæg om at forevise eller udlevere genstande, hvis der er grund til at antage, at en genstand, som den pågældende har rådighed over, kan tjene som bevis, bør konfiskeres eller ved lovovertrædelsen er fravendt nogen, som kan kræve den tilbage. I modsætning til reglerne om indgreb i meddelelseshemmeligheden indeholder reglerne om edition – bortset fra kravet om, at der skal være tale om lovovertrædelse, der er undergivet offentlig påtale – ikke noget krav om, at lovovertrædelserne skal være af en særlig art eller grovhed.

Det fremgår af retsplejelovens § 806, stk. 2, at afgørelse om pålæg om edition træffes af retten ved kendelse. Såfremt indgrebets øjemed ville forspildes, hvis retskendelse skulle afventes, kan politiet dog i medfør af § 806, stk. 4, træffe beslutning om edition. Fremsætter den, som indgrebet retter sig mod, anmodning herom, skal politiet snarest muligt og senest in-

den 24 timer forelægge sagen for retten, der ved kendelse afgør, om indgrebet kan godkendes.

3.2.4.4. For så vidt angår politiets, herunder PET's, erfaringer med anvendelsen af logningsreglerne henvises der til pkt. 5 og 6 i Justitsministeriets redegørelse af 21. december 2012 til Folketingets Retsudvalg om diverse spørgsmål vedrørende logningsreglerne og Justitsministeriets svar af 28. maj 2014 på spørgsmål nr. 942 (Alm. del) fra Folketingets Retsudvalg.

3.2.5. For så vidt angår anden hjemmel end retsplejeloven til udlevering af oplysninger, der registreres og opbevares i henhold til logningsbekendtgørelsen, kan det om Justitsministeriets område oplyses, at Datatilsynet efter persondatalovens § 62, stk. 1, kan kræve enhver oplysning, der er af betydning for dets virksomhed, herunder til afgørelse af, om et forhold falder ind under persondatalovens bestemmelser.

Baggrunden for bestemmelsen, der udspringer af persondatadirektivets artikel 28, stk. 3, er, at Datatilsynet som tilsynsmyndighed skal have mulighed for at kræve oplysninger udleveret af både den offentlige forvaltning og private dataansvarlige.

Bestemmelsen omfatter – jf. udtrykket "enhver oplysning" – i princippet også oplysninger registreret efter logningsbekendtgørelsen, men det må antages, at det kun i helt særlige tilfælde vil være relevant for Datatilsynet at indhente sådanne oplysninger.

Efter § 73 i lov om elektroniske kommunikationsnet og -tjenester, jf. lovbekendtgørelse nr. 128 af 7. februar 2014 (herefter teleloven), som hører under Erhvervs- og Vækstministeriet, kan Erhvervsstyrelsen kræve alle oplysninger og alt materiale, som Erhvervsstyrelsen skønner relevant i forbindelse med tilsyn med overholdelse af lovens regler eller regler fastsat i medfør heraf og i forbindelse med administration, undersøgelser og konkrete afgørelser, der gennemføres og træffes efter lovens bestemmelser herom, af blandt andre udbydere af elektroniske kommunikationsnet eller -tjenester og udbydere af teleterminaludstyr, der anvendes til mobilkommunikationstjenester.

Erhvervs- og Vækstministeriet har oplyst, at bestemmelsen efter sin ordlyd principielt kunne omfatte de i logningsbekendtgørelsen anførte oplysninger, men at indhentelse mv. af sådanne oplysninger ville forudsætte, at dette kunne betragtes som relevant i forhold til de pågældende bestemmelsers

formål, hvilket er usandsynligt.

Ifølge skattekontrollovens § 8 D, som hører under Skatteministeriet, skal blandt andre bestyrelser eller lignende øverste ledelser for private juridiske personer efter anmodning meddele told- og skatteforvaltningen oplysninger, der af myndighederne skønnes at være af væsentlig betydning for skatteligningen.

Bestemmelsen blev i sin nuværende form indsat i skattekontrolloven ved lov nr. 1113 af 21. december 1994. Det fremgår af lovforslagets specielle bemærkninger om bestemmelsen, at skattemyndighedernes adgang efter skattekontrollovens § 8 D, stk. 1, til at rekvirere oplysninger til brug for skattemyndighedernes virksomhed fra juridiske personer mv. begrænses til kun at omfatte oplysninger, der skønnes at ville være af væsentlig betydning for skattemyndighedernes virksomhed. I væsentlighedskriteriet ligger bl.a., at skattemyndighederne skal være tilbageholdende med at kræve nødvendige oplysninger direkte fra juridiske personer mv., hvis oplysningerne lige så vel kan kræves af den skattepligtige selv eller gennem denne.

Skatteministeriet har oplyst, at SKAT med hjemmel i den nævnte bestemmelse i forbindelse med ligning af en skattepligtig kan anmode teleselskaberne om at oplyse den skattepligtiges brug af telefon, typisk ved fremsendelse af specificeret faktura. Skatteministeriet har endvidere oplyst, at der i praksis er tale om oplysninger, der registreres i henhold til bekendtgørelse nr. 715 af 23. juni 2011 om udbud af elektroniske kommunikationsnet og -tjenester (herefter udbudsbekendtgørelsen, jf. nærmere nedenfor). Skatteministeriet har i samarbejde med Erhvervsstyrelsen rettet henvendelse til Europa-Kommissionen for at få afklaret, om der eventuelt er regelkonflikt mellem skattekontrolloven og e-data-beskyttelsesdirektivet (2002/58/EF). Skatteministeriet har oplyst, at de oplysninger, der i praksis indhentes, er oplysninger, der registreres i henhold til udbudsbekendtgørelsen, og at det er usandsynligt, at SKAT skulle få behov for at indhente oplysninger registreret i henhold til logningsbekendtgørelsen. Efter det oplyste har Skatteministeriet ikke taget stilling til, om sådanne oplysninger i givet fald ville kunne indhentes med hjemmel i skattekontrollovens § 8 D.

3.3. Lov om elektroniske kommunikationsnet og -tjenester (teleloven) indeholder regler, hvis formål er at fremme et velfungerende og innovationspræget marked for elektroniske kommunikationsnet og -tjenester til gavn for slutbrugerne. Loven indeholder regler, der bl.a. gennemfører e-data-beskyttelsesdirektivet.

I medfør af bl.a. telelovens § 8, stk. 1, 2 og 4, jf. § 20, stk. 1, har erhvervs- og vækstministeren udstedt udbudsbekendtgørelsen. Ifølge bekendtgørelsens § 19 skal teleudbydere, hvis deres opkrævning er afhængig af forbruget, tilbyde kunden specificeret regning. Til brug for dette registrerer og opbevarer teleudbyderen oplysninger, sådan at kunden kan identificere forbruget af tjenesten. De oplysninger, teleudbyderen skal registrere, er blandt andet tidspunkt, varighed og opkaldt nummer.

Formålet med bestemmelsen er at give kunderne mulighed for at kontrollere, at teleudbyderens opkrævning for forbrug af teletjenesten er korrekt.

Efter § 23 i udbudsbekendtgørelsen skal udbydere af offentlige elektroniske kommunikationsnet eller -tjenester sikre, at trafikdata vedrørende abonnenter eller brugere slettes eller anonymiseres, når de ikke længere er nødvendige for fremføringen af kommunikationen. Det fremgår dog samtidig af bestemmelsen, at det er tilladt for en udbyder at opbevare trafikdata til visse nærmere angivne formål, herunder bl.a. til debitering af abonnenter samt til opfyldelsen af de forpligtelser, der påhviler dem i medfør af logningsbekendtgørelsen.

Erhvervsstyrelsen under Erhvervs- og Vækstministeriet har oplyst, at sletningsreglen i udbudsbekendtgørelsens § 23 bl.a. gælder for oplysninger, der er logget efter logningsbekendtgørelsen. Oplysninger, som teleudbyderne registrerer og opbevarer *alene* med det formål at opfylde logningsforpligtelsen i henhold til logningsbekendtgørelsen, vil således ikke efter de gældende regler kunne opbevares i mere end 1 år, jf. den 1-årige opbevaringspligt i logningsbekendtgørelsens § 9.

Erhvervsstyrelsen har over for Justitsministeriet på spørgsmålet om, hvilke sikkerhedskrav til teleudbyderne der gælder på telelovgivningens område, herunder hvilke garantier der i denne lovgivning er fastsat for at sikre en effektiv beskyttelse af data mod risiko for misbrug samt ulovlig adgang til og benyttelse af data, endvidere oplyst følgende:

> "Erhvervsstyrelsen kan som uafhængig telemyndighed oplyse, at opbevaring eller lagring af data, som er logget efter Justitsministeriets logningsbekendtgørelse er underlagt reglerne i bekendtgørelse nr. 445 af 11. maj 2011 om informationssikkerhed og beredskab for elektroniske kommunikationsnet og -tjenester. Bekendtgørelsen er udstedt med hjemmel i § 8, stk. 1 og 8, stk. 4 i lov 169 af 3. marts 2011 om elektroniske kommunikationsnet og -tjenester.
>
> Reglerne om persondatasikkerhed følger af bekendtgørelsens § 7. Efter denne bestemmelse skal net- og tjenesteudbyderne jf. § 5 gennemføre en risikovurdering og udarbejde en sikkerhedspolitik

for persondatasikkerheden i forbindelse med net- og tjenesteudbuddet og i relevant omfang sikringsplaner omfattende foranstaltninger til beskyttelse heraf. Sådanne foranstaltninger skal leve op til kravene i kap. 4 i bekendtgørelse nr. 715 af 23. juni 2011 om udbud af elektroniske kommunikationsnet- og tjenester – herunder kravene til behandling (navnlig sletning og anonymisering) af trafik- og lokaliseringsdata.

Herudover skal foranstaltningerne som minimum:

1. Sikre at kun autoriserede personer får adgang til persondata til lovlige formål
2. Beskytte lagrede persondata og persondata under transmission mod hændelig eller ulovlig tilintetgørelse, hændeligt tab eller ændring og ubeføjet eller ulovlig lagring, behandling, adgang eller videregivelse.

Erhvervsstyrelsen kan desuden oplyse, at der på myndighedens område ikke findes specifikke regler, der regulerer overførsel af data til lande uden for EU."

Erhvervsstyrelsen fører som telemyndighed tilsyn med, at teleudbyderne overholder reglerne i udbudsbekendtgørelsen og bekendtgørelse nr. 445 af 11. maj 2011 om informationssikkerhed og beredskab for elektroniske kommunikationsnet og -tjenester (herefter sikkerhedsbekendtgørelsen), jf. den generelle tilsynspligt i telelovens § 20.

3.4. Persondataloven indeholder regler om persondatabeskyttelse. Loven gennemfører databeskyttelsesdirektivet.

Persondataloven gælder bl.a. for behandling af personoplysninger, som helt eller delvis foretages ved hjælp af elektronisk databehandling, jf. lovens § 1, stk. 1.

Teleudbyderes behandling af personoplysninger er ud over reglerne i telelovgivningen reguleret af de generelle bestemmelser i persondataloven, i det omfang disse ikke er fortrængt af særregler i f.eks. telelovgivningen, jf. herved persondatalovens § 2, stk. 1.

Det fremgår af persondatalovens § 55, at Datatilsynet fører tilsyn med enhver behandling, der omfattes af loven. Tilsynet med de bestemmelser i persondataloven, som finder anvendelse på teleudbydernes behandling af personoplysninger, fordi de ikke er fortrængt af særregler i telelovgivningen, ligger derfor hos Datatilsynet. Datatilsynet udøver sine funktioner i fuld uafhængighed, jf. lovens § 56.

Af persondatalovens §§ 41 og 42 fremgår bl.a., at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Det fremgår endvidere, at en dataansvarlig, når denne overlader en behandling af oplysninger til en databehandler, skal sikre sig, at databehandleren kan træffe de nævnte tekniske og organisatoriske sikkerhedsforanstaltninger, og påse, at dette sker. Det er i forarbejderne til persondataloven forudsat, at foranstaltningerne under hensyn til det aktuelle tekniske niveau og de omkostninger, som er forbundet med deres iværksættelse, vil tilvejebringe et tilstrækkeligt sikkerhedsniveau i forhold til de risici, som behandlingen indebærer, og arten af de oplysninger, som skal beskyttes, jf. herved også databeskyttelsesdirektivets artikel 17, stk. 1, 2. afsnit.

I persondataloven er der desuden fastsat nærmere regler om overførsel af oplysninger til tredjelande.

Det fremgår af persondatalovens § 27, stk. 1, at oplysninger kun må overføres til et tredjeland, hvis dette land sikrer et tilstrækkeligt sikkerhedsniveau. Ved tredjeland forstås en stat, som ikke indgår i EU, og som ikke har gennemført aftaler, der er indgået med EU, og som indeholder regler svarende til databeskyttelsesdirektivet, jf. persondatalovens § 3, nr. 9.

Vurderingen af, om beskyttelsesniveauet i et tredjeland er tilstrækkeligt, skal efter persondatalovens § 27, stk. 2, ske på grundlag af samtlige de forhold, der har indflydelse på en overførsel, herunder navnlig oplysningernes art, behandlingens formål og varighed, oprindelseslandet og det endelige bestemmelsesland, samt de retsregler, herunder regler for god forretningsskik og sikkerhedsforanstaltninger, som gælder i tredjelandet.

Kommissionen kan med bindende virkning for medlemsstaterne træffe beslutning om, at et bestemt tredjeland sikrer et tilstrækkeligt beskyttelsesniveau, jf. artikel 25, stk. 6, i databeskyttelsesdirektivet.

I de tilfælde, hvor et tredjeland ikke kan siges at sikre et tilstrækkeligt beskyttelsesniveau, kan der ske overførsel af oplysninger til det pågældende tredjeland, hvis betingelserne i § 27, stk. 3, er opfyldt, herunder hvis den registrerede har givet udtrykkeligt samtykke hertil, jf. stk. 3, nr. 1, eller hvis overførslen er nødvendig eller følger af lov eller bestemmelser fastsat i henhold til lov for at beskytte en vigtig samfundsmæssig interesse eller

for, at et retskrav kan fastlægges, gøres gældende eller forsvares, jf. stk. 3, nr. 4. Det bemærkes i den forbindelse, at det følger af persondatalovens § 50, stk. 2, at ved overførsel af oplysninger, som nævnt i bestemmelsens stk. 1 – det vil bl.a. sige ved overførsel af følsomme personoplysninger – til tredjelande i medfør af bl.a. § 27, stk. 3, nr. 2-4, skal der indhentes en tilladelse fra Datatilsynet.

Uden for de i stk. 3 nævnte tilfælde kan Datatilsynet give tilladelse til, at der overføres oplysninger til tredjelande, som ikke opfylder stk. 1, hvis den dataansvarlige yder tilstrækkelige garantier for beskyttelse af de registreredes rettigheder, jf. persondatalovens § 27, stk. 4.

Efter persondatalovens § 27, stk. 5, kan overførsel til tredjelande ske uden tilladelse fra Datatilsynet, på grundlag af kontrakter, der er i overensstemmelse med standardkontraktbestemmelser godkendt af Kommissionen.

Det bemærkes, at bestemmelsen i persondatalovens § 27 om overførsel af personoplysninger til tredjelande både gælder ved videregivelse af personoplysninger til en anden dataansvarlig, ved overladelse af personoplysninger til en databehandler samt ved intern brug, f.eks. inden for en koncern.

4. Dommens betydning for de danske logningsregler

4.1. På baggrund af EU-Domstolens dom af 8. april 2014 er der rejst spørgsmål om, hvorvidt de danske logningsregler kan opretholdes, altså om de gældende danske logningsregler er i overensstemmelse med Charterets bestemmelser om retten til respekt for privatliv og familieliv (artikel 7) og om retten til beskyttelse af personoplysninger (artikel 8).

4.2. Justitsministeriet skal indledningsvis bemærke, at det er ministeriets vurdering, at Charteret finder anvendelse i forhold til de danske logningsregler.

Efter Charterets artikel 51 finder det anvendelse i forhold til medlemsstaterne, "når de gennemfører EU-retten". Det fremgår af de såkaldte forklaringer til Charterets artikel 51, der i overensstemmelse med Traktaten om Den Europæiske Unions artikel 6, stk. 1, og Charterets artikel 52, stk. 7, skal tages i betragtning i forbindelse med fortolkningen af dette, at Charteret også finder anvendelse, når medlemsstaterne handler inden for EU-retten. Samtidig følger det af e-data-beskyttelsesdirektivets artikel 15, stk. 1, 2. pkt., at medlemsstaterne af hensyn til bl.a. forebyggelse, efterforsk-

ning, afsløring og retsforfølgning i straffesager kan vedtage retsforskrifter om lagring af data i en begrænset periode[1]. En medlemsstat, der, som sket ved de danske logningsregler, fastsætter regler om logning af teledata, handler således efter Justitsministeriets opfattelse inden for rammerne af EU-retten.

På den baggrund er det Justitsministeriets opfattelse, at de danske logningsregler – selv om Danmark, nu hvor logningsdirektivet er erklæret ugyldigt, strengt taget ikke gennemfører dette – som følge af e-databeskyttelsesdirektivets artikel 15 falder inden for EU-rettens anvendelsesområde, jf. Charterets artikel 51, stk. 1, således som denne bestemmelse er fortolket i EU-Domstolens dom i sag C-617/10, Hans Åkerberg Fransson[2].

4.3. Det skal derfor vurderes, om den gældende danske lovgivning på området er i overensstemmelse med Charterets bestemmelser om retten til respekt for privatliv og familieliv (artikel 7) og ret til beskyttelse af personoplysninger (artikel 8).

De rettigheder, der sikres ved Charterets artikel 7 om respekt for privatliv og familieliv, svarer indholdsmæssigt til de rettigheder, der er sikret ved Den Europæiske Menneskerettighedskonventions (herefter EMRK) artikel 8. Ligeledes er Charterets artikel 8 om beskyttelse af personoplysninger baseret på bl.a. EMRK artikel 8.

EMRK artikel 8 har følgende ordlyd:

> "Stk. 1. Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance.
> Stk. 2. Ingen offentlig myndighed må gøre indgreb i udøvelsen af denne ret, medmindre det sker i overensstemmelse med loven og er nødvendigt i et demokratisk samfund af hensyn til den nationale sikkerhed, den offentlige tryghed eller landets økonomiske velfærd, for at forebygge uro eller forbrydelse, for at beskytte sundhe-

[1] Det bemærkes, at det fremgår af direktivets artikel 1, stk. 3, at direktivet under ingen omstændigheder gælder for bl.a. "statens aktiviteter på det strafferetlige område." Efter Justitsministeriets opfattelse er denne undtagelse vedrørende det strafferetlige område begrænset til tilfælde, hvor staten opbevarer og behandler data som led i strafferetlige aktiviteter. I modsætning hertil retter de danske logningsregler sig mod teleudbydere.

[2] I denne sag havde de svenske myndigheder fastsat regler om sanktioner i tilknytning til et direktiv, uden at direktivet forpligtede hertil. EU-Domstolen fandt, at strafforfølgningen af Åkerberg Fransson efter de pågældende bestemmelser udgjorde en gennemførelse af EU-retten i den forstand, hvori udtrykket er anvendt i Charterets artikel 51, stk. 1, selv om den svenske lovgivning ikke var vedtaget for at gennemføre direktivet i national ret, da anvendelsen af de svenske regler havde til formål at sanktionere en tilsidesættelse af direktivets bestemmelser og dermed havde til formål at gennemføre medlemsstaternes traktatmæssige forpligtelse til effektivt at sanktionere adfærd, der skader Unionens finansielle interesser.

den eller sædeligheden eller for at beskytte andres rettigheder og friheder."

Det følger af Charterets artikel 52, stk. 3, at i det omfang Charteret indeholder rettigheder svarende til dem, der er sikret ved EMRK, har de samme betydning og omfang som i konventionen. I det omfang rettighederne i Charteret således svarer til rettighederne i EMRK, skal rettighederne i Charteret derfor fortolkes i overensstemmelse med Den Europæiske Menneskerettighedsdomstols (herefter Menneskerettighedsdomstolen) retspraksis vedrørende de relevante bestemmelser i EMRK.

4.4. I det følgende foretages en analyse af betydningen af EU-Domstolens dom af 8. april 2014 for dansk ret med udgangspunkt i dommen og artikel 7 og 8 i Charteret og med inddragelse af Menneskerettighedsdomstolens praksis vedrørende EMRK, hvor det er relevant.

4.4.1. Indledningsvis bemærkes, at registreringen og opbevaringen af oplysninger foretaget i henhold til logningsbekendtgørelsen tager udgangspunkt i den forpligtelse til at foretage registrering og opbevaring af oplysninger, der fulgte af logningsdirektivet. Der er grundlæggende tale om registrering og opbevaring af den samme type af oplysninger, dvs. oplysninger, der skaber mulighed for i et vist omfang at få indblik i kommunikationen foretaget af de personer, hvis oplysninger registreres og opbevares, uden at der dog skabes mulighed for at få indblik i indholdet af denne kommunikation.

Formålet med registreringen og opbevaringen af oplysninger efter logningsbekendtgørelsen er desuden det samme som formålet med registrering og opbevaring ifølge logningsdirektivet, dvs. at skabe mulighed for at anvende oplysningerne som led i efterforskning og retsforfølgning af strafbare forhold.

Med udgangspunkt i EU-Domstolens afgørelse vedrørende logningsdirektivet er det derfor Justitsministeriets vurdering, at registreringen og opbevaringen af oplysninger foretaget i henhold til logningsbekendtgørelsen udgør et indgreb i retten til privatliv, jf. Charterets artikel 7, og retten til beskyttelse af personoplysninger, jf. Charterets artikel 8.

Det er desuden Justitsministeriets vurdering, at registreringen og opbevaringen af oplysninger i henhold til logningsbekendtgørelsen med henblik på, at oplysningerne kan indgå som led i efterforskning og retsforfølgning

af strafbare forhold, forfølger et sagligt formål, og at registreringen og opbevaringen af oplysninger er egnet til at opnå dette formål.

Særligt for så vidt angår oplysninger registreret som led i sessionslogning, jf. logningsbekendtgørelsens § 5, stk. 1, har erfaringerne dog vist, at oplysningerne kun i meget begrænset omfang er brugbare i praksis i forbindelse med efterforskning og retsforfølgning af strafbare forhold. Det skyldes bl.a., at reglerne er udformet på en måde, der gør det muligt for internetudbyderne at nøjes med at logge hver 500. datapakke, der indgår i en slutbrugers kommunikation på internettet. Endvidere kan internetudbyderne foretage registreringen af internetkommunikationen på kanten til andre net i deres netværk. Der henvises nærmere herom til pkt. 5.5.1.1 i Justitsministeriets redegørelse af 21. december 2012 til Folketingets Retsudvalg om diverse spørgsmål vedrørende logningsreglerne. Det er efter Justitsministeriets opfattelse tvivlsomt, om reglerne om sessionslogning på nuværende tidspunkt og i deres nuværende udformning kan anses for "egnede" til at opnå deres formål (skabe mulighed for anvendelse af oplysningerne som led i efterforskning og retsforfølgning af strafbare forhold). Justitsministeriet vil derfor tage skridt til at ophæve reglerne herom i bekendtgørelsens § 5, stk. 1. Der kan i forlængelse heraf henvises til, at justitsministeren i folketingsåret 2014-15 vil fremsætte et lovforslag om revision af logningsreglerne.

På den anførte baggrund forholder det nedenfor angivne sig ikke til reglerne om sessionslogning efter bekendtgørelsens § 5, stk. 1.

4.4.2. Som anført i pkt. 2 ovenfor er det i forhold til logningsdirektivet EU-Domstolens opfattelse, at indgrebet i de grundlæggende rettigheder beskyttet i Charterets artikel 7 og 8 ikke er tilstrækkeligt afgrænset med henblik på at sikre, at det pågældende indgreb rent faktisk er begrænset til det strengt nødvendige.

Med udgangspunkt i EU-Domstolens treleddede begrundelse for, at Domstolen ikke fandt indgrebet tilstrækkeligt afgrænset, jf. gennemgangen af dommen i pkt. 2 ovenfor, analyseres i det følgende betydningen af dommen i forhold til de gældende danske regler om registreringen af oplysninger (I), adgangen til de registrerede oplysninger (II) og varigheden af opbevaringen af de registrerede oplysninger (III).

I. For så vidt angår *registreringen og opbevaringen* af oplysninger bemærkes, at den registrering og opbevaring, der skal foretages i henhold til log-

ningsbekendtgørelsen, som udgangspunkt svarer til den registrering og opbevaring, der skulle foretages med udgangspunkt i logningsdirektivet. Hertil kommer, at der som anført i pkt. 3 ovenfor på enkelte punkter (mobiltelefoni og sessionslogning og trådløs adgang til internettet) foretages registrering og opbevaring af oplysninger, der går videre end de forpligtelser, der fulgte af logningsdirektivet.

For så vidt angår vurderingen i forhold til Charterets artikel 7 og 8 bemærkes, at registreringen og opbevaringen af oplysninger foretaget i henhold til logningsbekendtgørelsen – på samme generelle vis som registreringen og opbevaringen foretaget i henhold til logningsdirektivet – omfatter alle personer og alle elektroniske kommunikationsmidler og samtlige trafikdata uden nogen form for differentiering, begrænsning eller undtagelse under hensyn til målet om at bekæmpe kriminalitet.

II. I relation til spørgsmålet om *adgangen* til de oplysninger, der er registreret og opbevaret i henhold til logningsbekendtgørelsen, bemærkes, at logningsdirektivet i vidt omfang overlader det til medlemsstaterne at udfylde de materielle og proceduremæssige betingelser for denne adgang, ligesom direktivet også i vidt omfang overlader det til medlemsstaterne at fastsætte de nærmere krav til opbevaringen af oplysningerne.

Som anført i EU-Domstolens dom, præmis 54, må det kræves, at lovgivningen fastsætter klare og præcise regler, således at de personer, hvis oplysninger registreres og opbevares, råder over tilstrækkelige garantier, der gør det muligt effektivt at beskytte deres personlige oplysninger mod risikoen for misbrug og mod ulovlig adgang til og anvendelse af disse oplysninger.

Menneskerettighedsdomstolen har i sin afgørelse af 29. juni 2006 i sagen *Weber og Saravia mod Tyskland (54934/00)*, særligt præmis 93-95, taget stilling til forholdet mellem EMRK artikel 8 og hemmelig overvågning af kommunikation med henblik på kriminalitetsbekæmpelse. I den forbindelse bemærkede Menneskerettighedsdomstolen, at det ikke kan kræves af national lovgivning, at den enkelte skal være i stand til at forudse, hvornår vedkommendes kommunikation bliver overvåget. Derimod må det kræves, at national lovgivning er tilstrækkeligt klar for så vidt angår betingelserne for, at hemmelig overvågning af kommunikation kan iværksættes med henblik på at sikre den enkelte mod vilkårlige indgreb i retten til privatliv. Menneskerettighedsdomstolen opsummerede herefter sin retspraksis således:

> "In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed."

Det bemærkes, at der i forbindelse med registrering og opbevaring af oplysninger i henhold til logningsbekendtgørelsen ikke er tale om egentlig hemmelig overvågning (logningen medfører således ikke i sig selv, at politi mv. automatisk får adgang til de opbevarede data), ligesom der heller ikke er tale om overvågning af indholdet af kommunikationen mv. (logningen indebærer således ikke nogen adgang til indholdet af de opbevarede data). Med forbehold herfor må Menneskerettighedsdomstolens afgørelse dog efter Justitsministeriets opfattelse antages at kunne tjene som grundlag for vurderingen af de krav, der må stilles til national lovgivning for så vidt angår adgangen til og opbevaringen af oplysninger, der er registreret og opbevaret i henhold til logningsbekendtgørelsen.

Som beskrevet i pkt. 3.2.4 ovenfor er adgangen til de oplysninger, der er registreret og opbevaret i henhold til logningsbekendtgørelsen med henblik på at kunne anvendes som led i efterforskning og retsforfølgning af strafbare forhold, reguleret i retsplejelovens kapitel 71 om indgreb i meddelelseshemmeligheden og kapitel 74 om edition.

For så vidt angår de materielle betingelser for adgangen til registrerede og opbevarede oplysninger i form af indgreb i meddelelseshemmeligheden, skal der særligt henvises til retsplejelovens § 781, der opstiller krav til mistankegrundlaget (mistankekravet), behovet for at foretage indgrebet (indikationskravet) samt til grovheden af den kriminalitet, som mistanken angår (kriminalitetskravet).

For så vidt angår kriminalitetskravet bemærkes, at der som betingelse for indgreb i meddelelseshemmeligheden generelt kræves, at der er tale om kriminalitet af en vis grovhed (strafferamme på mindst 6 års fængsel eller forsætlig overtrædelse af straffelovens kapitel 12 om forbrydelser mod statens selvstændighed og sikkerhed eller straffelovens kapitel 13 om forbrydelser mod statsforfatningen og de øverste statsmyndigheder, terrorisme mv.).

Overtrædelse af en række andre specifikke bestemmelser i straffeloven og særlovgivningen, herunder udlændingeloven kan dog også begrunde indgreb i meddelelseshemmeligheden, jf. retsplejelovens § 781, stk. 1, nr. 3, stk. 2 og stk. 3.

Som det fremgår af pkt. 3.2.4 ovenfor, er det ved indsættelsen af de særlige bestemmelser i retsplejelovens § 781, stk. 1, nr. 3, generelt forudsat, at der bør sættes snævre grænser for politiets adgang til at foretage indgreb i meddelelseshemmeligheden, at der i forbindelse med overvejelser om at udvide adgangen hertil foretages en overordnet afvejning af på den ene side hensynet til en effektiv kriminalitetsbekæmpelse og på den anden side hensynet til borgernes privatliv, og at der imidlertid kan vise sig at være særlige kriminalitetsformer, hvor sædvanlige efterforskningsmetoder ikke er tilstrækkelige.

I forbindelse med indsættelse af hver enkelt af de særligt oplistede bestemmelser i retsplejelovens § 781, stk. 1, nr. 3, er der således foretaget en konkret vurdering af behovet for at udvide adgangen til at foretage indgreb i meddelelseshemmeligheden. Behovet begrundes med, at udviklingen af nye kriminalitetsformer i det moderne samfund gør det nødvendigt at tage andre end de sædvanlige efterforskningsmetoder i brug, og at der løbende bør tages stilling til dette behov. Det gælder f.eks., hvor kommunikationsdata er det afgørende bevismiddel eller det helt relevante efterforskningsmiddel, hvor overtrædelsen begås af en flerhed af personer, har karakter af et komplot eller som led i organiseret international kriminalitet, eller hvor overtrædelsen sker ad ren elektronisk vej.

Det bemærkes i forlængelse heraf, at mistankekravet i retsplejelovens § 781, stk. 1, nr. 1, og indikationskravet i stk. 1, nr. 2, samt proportionalitetskravet i § 782 ligeledes finder anvendelse for så vidt angår de særligt oplistede bestemmelser. Der henvises i øvrigt til den nærmere beskrivelse af de materielle betingelser i pkt. 3.2.4 ovenfor.

Ved indhentelse af historiske teleoplysninger skal de materielle betingelser for både editionspålæg, jf. retsplejelovens § 804, og indgreb i meddelelseshemmeligheden, jf. retsplejelovens § 781, være opfyldt.

De proceduremæssige betingelser for adgang til sådanne oplysninger fremgår af retsplejelovens § 783 (krav om retskendelse), § 784 (advokatbeskikkelse for den, som indgrebet vedrører) og § 788 (efterfølgende underretning af den, som indgrebet vedrører).

Også ved indhentelse af andre oplysninger (alene) efter reglerne om edition, jf. retsplejelovens § 804, jf. pkt. 3.2.4.1 ovenfor, gælder der proceduremæssige betingelser, jf. retsplejelovens § 806, herunder krav om retskendelse.

Dansk ret indeholder således klare betingelser for adgangen til oplysninger, der er registreret og opbevaret i henhold til logningsbekendtgørelsen[3].

Ud over adgang i form af indgreb i meddelelseshemmeligheden og pålæg om edition efter bestemmelserne i retsplejeloven findes der som nævnt ovenfor i pkt. 3.2.5 på visse områder hjemmel til, at myndigheder kan kræve at få indblik i oplysninger, der er registreret og opbevaret i henhold til logningsbekendtgørelsen. Således vil både Datatilsynet og Erhvervsstyrelsen kunne kræve at få adgang til oplysninger registreret og opbevaret i henhold til logningsbekendtgørelsen, hvis det måtte være relevant for de pågældende myndigheders tilsynsvirksomhed. Dette vil kun i helt særlige tilfælde være relevant for Datatilsynet, og efter det af Erhvervs- og Vækstministeriet oplyste usandsynligt i forhold til Erhvervsstyrelsen. Endvidere har Skatteministeriet oplyst, at de oplysninger, der i praksis indhentes, er oplysninger, der registreres i henhold til udbudsbekendtgørelsen, og at det er usandsynligt, at SKAT skulle få behov for at indhente oplysninger registreret i henhold til logningsbekendtgørelsen. Efter det oplyste har Skatteministeriet ikke taget stilling til, om sådanne oplysninger i givet fald ville kunne indhentes med hjemmel i skattekontrollovens § 8 D.

For så vidt angår opbevaringen af oplysninger, der er registreret i henhold til logningsbekendtgørelsen, bemærkes, at persondataloven som anført i pkt. 3.4 ovenfor gælder for oplysninger, som registreres og opbevares efter logningsbekendtgørelsen, og at Datatilsynet fører tilsyn med enhver behandling, der omfattes af loven.

Hertil kommer, at der i udbudsbekendtgørelsen er fastsat særlige bestemmelser for teleudbydere, herunder bekendtgørelsens § 23 om sletning eller anonymisering af trafikdata, der også finder anvendelse på trafikdata, der er registreret og opbevaret i henhold til logningsbekendtgørelsen. Det indebærer som nævnt i pkt. 3.3 ovenfor, at oplysninger, som teleudbyderne registrerer og opbevarer alene med det formål at opfylde forpligtelsen i

[3] Justitsministeriet vil i forbindelse med den kommende revision af logningsreglerne nærmere overveje forholdet mellem Danmarks internationale forpligtelser med hensyn til retten til respekt for privatlivet og de krav, der efter retsplejelovens editionsregler gælder i forhold til politiets adgang til visse loggede oplysninger.

henhold til logningsbekendtgørelsen, ikke vil kunne opbevares i mere end 1 år.

Der er således i dansk ret etableret en række garantier vedrørende adgangen til og opbevaringen af oplysninger, der er registreret og opbevaret i henhold til logningsbekendtgørelsen. For så vidt angår adgangen til oplysningerne adskiller de danske regler sig væsentligt fra logningsdirektivet, der i vidt omfang overlod reguleringen af disse spørgsmål til medlemsstaterne.

III. Om *opbevaringsperioden* for oplysninger, der registreres og opbevares i henhold til logningsbekendtgørelsen, bemærkes, at det efter retsplejelovens § 786, stk. 4, påhviler teleudbydere at foretage registrering og opbevaring i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. I overensstemmelse hermed fremgår det af logningsbekendtgørelsens § 9, at de registrerede oplysninger skal opbevares i 1 år.

Der henvises til pkt. 3.2.3 ovenfor for en beskrivelse af motiverne bag fastlæggelsen af opbevaringsperioden til 1 år. Som det fremgår heraf, er det udtrykkeligt anført i forarbejderne til lov nr. 378 af 6. juni 2002 (pkt. 3.1.3.1 i de almindelige bemærkninger til lovforslaget), at fastsættelsen af en opbevaringsperiode på 1 år ikke går videre, end hensynet til forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager tilsiger.

Også på dette punkt adskiller dansk ret sig fra logningsdirektivet, idet det i direktivet var overladt til medlemsstaterne selv at fastlægge en opbevaringsperiode på mellem 6 måneder og 2 år. EU-Domstolen fremhævede i den forbindelse bl.a., at det ikke var præciseret i direktivet, at fastsættelsen af lagringsperioden skal være baseret på objektive kriterier for at sikre en begrænsning til det strengt nødvendige, jf. præmis 64.

Det bemærkes desuden, at der som også anført ovenfor gælder en forpligtelse for teleudbyderne i medfør af udbudsbekendtgørelsens § 23 til at slette eller anonymisere oplysninger, der udelukkende er registreret og opbevaret i henhold til logningsbekendtgørelsen, ved udløbet af den 1-årige opbevaringsperiode.

For så vidt angår, hvor længe de registrerede oplysninger skal opbevares, har Danmark således på dette punkt fastsat en klar afgrænsning i lovgivningen baseret på hensynet til efterforskning og kriminalitetsbekæmpelse.

4.5. Det bemærkes endelig, at EU-Domstolen anfører i præmis 66-68, at logningsdirektivet ikke fastsætter tilstrækkelige garantier i forhold til effektiv beskyttelse af lagrede data mod risikoen for misbrug og mod enhver ulovlig adgang til og anvendelse af disse data, således som foreskrevet i Charterets artikel 8. Navnlig sikrer direktivet efter Domstolens opfattelse ikke en irreversibel destruktion af dataene ved udløbet af lagringsperioden. Direktivet fastsætter endvidere ikke krav om, at lagrede data skal opbevares på EU's område, hvilket kan underminere den uafhængige myndighedskontrol, der skal foretages efter Charterets artikel 8, stk. 3.

4.5.1. Som det fremgår ovenfor under pkt. 3.3, er der på teleområdet i sikkerhedsbekendtgørelsen fastsat sikkerhedskrav til teleudbyderne.

Formålet med sikkerhedsbekendtgørelsen er at sikre en effektiv beskyttelse af data mod risiko for misbrug samt ulovlig adgang til og benyttelse af data. Dette omfatter også data, der er blevet logget efter logningsbekendtgørelsen.

Efter reglerne i sikkerhedsbekendtgørelsen er der bl.a. krav om, at tjenesteudbyderne skal udarbejde en sikkerhedspolitik, der som minimum sikrer, at det kun er en begrænset kreds af personer, som får adgang til persondata til lovlige formål, og at der bl.a. ikke kan ske en ubeføjet eller ulovlig lagring, behandling, adgang eller videregivelse af persondata. Endvidere er der – som nærmere redegjort for under pkt. 3.3 – efter udbudsbekendtgørelsens § 23 krav om, at teleudbydere ikke kan opbevare logningsdata ud over logningsperioden på 1 år, idet teleudbyderne efter den nævnte bestemmelse er forpligtet til at slette eller anonymisere dataene.

Hertil kommer, at udbyderne skal overholde persondatalovens regler om fornødne tekniske og organisatoriske sikkerhedsforanstaltninger.

Disse sikkerhedskrav og -foranstaltninger er som nævnt ovenfor en gennemførelse af henholdsvis e-data-beskyttelsesdirektivet og databeskyttelsesdirektivet. Dommens præmis 67 må efter Justitsministeriets opfattelse forstås sådan, at der navnlig sigtes til krav om irreversibel destruktion af data. Dette er som nævnt ovenfor opfyldt ved udbudsbekendtgørelsens § 23, hvorefter teleudbyderne ikke kan opbevare oplysninger, der (alene) er logget efter logningsreglerne, ud over logningsperioden på 1 år, hvorefter dataene skal slettes eller anonymiseres.

4.5.2. Særligt i forhold til EU-Domstolens bemærkning om, at logningsdirektivet ikke sikrer, at lagrede data skal opbevares på EU's område, bemærkes, at der i persondatalovens § 27 er fastsat nærmere regler for overførsel af oplysninger til lande uden for EU. Denne bestemmelse gælder også for oplysninger, der er blevet logget efter logningsbekendtgørelsen.

Persondatalovens regler indebærer således, at oplysninger kun må overføres til et tredjeland, hvis dette land sikrer et tilstrækkeligt sikkerhedsniveau, hvis betingelserne i lovens § 27, stk. 3, er opfyldt, hvis Datatilsynet i medfør af § 27, stk. 4, har givet tilladelse til overførslen, eller hvis overførslen sker på grundlag af kontrakter, der er i overensstemmelse med standardkontraktbestemmelser godkendt af Kommissionen.

Som nævnt ovenfor gælder bestemmelsen i persondatalovens § 27 om overførsel til tredjelande også ved overladelse af personoplysninger til en databehandler samt ved intern brug, f.eks. inden for en koncern.

5. Konklusion

Som det nærmere fremgår under pkt. 2 ovenfor, foretog EU-Domstolen en *samlet* vurdering af, om det indgreb i EU-borgernes rettigheder efter Charterets artikel 7 og 8, som logningsdirektivet indebar, var begrænset til det strengt nødvendige. Domstolen fandt – med henvisning til samtlige i dommen angivne betragtninger – at EU-lovgiver ved ikke at have fastsat klare og præcise regler for medlemsstaterne havde overskredet de grænser, som overholdelsen af proportionalitetsprincippet kræver, henset til Charterets artikel 7, 8 og 52, stk. 1, jf. dommens præmis 65 og 69.

Henset til, at dommen er baseret på en samlet vurdering, kan det give anledning til tvivl, hvilken vægt de enkelte led i begrundelsen skal tillægges, og dermed også hvilken betydning dommen i givet fald kan tillægges i forhold til de danske logningsregler.

I og med, at der er tale om en samlet vurdering, kan det forhold, at registreringen og opbevaringen af oplysninger foretaget i henhold til de danske logningsregler – på samme generelle vis som registreringen og opbevaringen foretaget i henhold til logningsdirektivet – omfatter alle personer og alle elektroniske kommunikationsmidler og samtlige trafikdata uden nogen form for differentiering, begrænsning eller undtagelse under hensyn til målet om at bekæmpe grov kriminalitet, efter Justitsministeriets opfattelse ik-

ke i sig selv føre til, at de danske regler må anses for at være i strid med Charteret.

Som det fremgår ovenfor, fastsætter den danske lovgivning klare og præcise regler, der indeholder en række væsentlige garantier med henblik på effektivt at beskytte logningsdata mod risikoen for misbrug og mod ulovlig adgang til og anvendelse af disse data.

Modsat logningsdirektivet indeholder dansk lovgivning en række materielle og proceduremæssige betingelser for adgangen til de registrerede oplysninger. Særligt skal det fremhæves, at adgangen til oplysningerne – som beskrevet ovenfor – sker under iagttagelse af retsplejelovens regler om indgreb i meddelelseshemmeligheden og/eller edition, hvilket medfører, at en række materielle og proceduremæssige krav skal være opfyldt, for at politiet kan få adgang til oplysningerne. Derudover fastsætter de danske logningsregler – modsat direktivet – pligten for teleudbyderne til at opbevare oplysningerne til 1 år. Endelig følger det af udbudsbekendtgørelsen, at oplysninger, der udelukkende er registreret og opbevaret under henvisning til logningsbekendtgørelsen, herefter irreversibelt skal slettes eller anonymiseres.

Samlet set finder Justitsministeriet af de ovenfor anførte grunde, at der ikke er grundlag for at antage, at de gældende danske regler om registrering og opbevaring af oplysninger i henhold til retsplejeloven og logningsbekendtgørelsen og om adgangen til disse oplysninger skulle være i strid med Charterets bestemmelser om retten til respekt for privatliv og familieliv (artikel 7) og ret til beskyttelse af personoplysninger (artikel 8)[4].

[4] Det bemærkes, at som anført ovenfor under pkt. 4.4.1 vil Justitsministeriet tage skridt til at ophæve reglerne om sessionslogning.