



Revision af logningsreglerne

1. Executive summary

Siden ikrafttrædelsen af de såkaldte logningsregler i 2007, har det været omdiskuteret, om forpligtelsen til at lagre en række persondata går for vidt i forhold til bl.a. privatlivets fred. Logningsbekendtgørelsen omfatter bl.a. oplysninger om, hvem danske borgere ringer til, sms'er med, og hvilke mobilmaster deres mobiltelefon kobler sig på. Den 8. april 2014 afsagde EU-Domstolen en afgørelse, der erklærede EU's logningsdirektiv for uforeneligt med netop beskyttelsen af privatlivets fred og persondata i EU's Charter om Grundlæggende Rettigheder (Charteret). Justitsministeriet har i et notat om dommen konkluderet, at den danske logningsordning ikke er i strid med Charteret. Det må dog anses for tvivlsomt, om Justitsministeriets konklusion lægger tilstrækkelig vægt på det forhold, at de danske logningsregler, og den deraf følgende lagring af persondata, griber ind i alle danske borgeres privatliv uden krav om mistanke eller lignende. Netop dette forhold var af afgørende betydning i EU-Domstolens dom, samt i en række relevante afgørelser fra Den Europæiske Menneskerettighedsdomstol (EMD). På den baggrund konkluderes det, at der er stærke holdepunkter for at antage, at de danske logningsregler ikke er forenelige med Charteret og Den Europæiske Menneskerettighedskonvention (EMRK). Det anbefales derfor, at der foretages yderligere ændringer af bl.a. logningsbekendtgørelsen således, at der alene kan foretages logning af persondata vedrørende konkrete personer, som, politiet har en rimelig formodning om, er involveret i alvorlig kriminalitet, og at de loggede data derefter alene kan udleveres i henhold til reglerne i Retsplejeloven, der kræver mistanke og retskendelse.

2. De danske logningsregler

Terrorangrebene i USA den 11. september 2001 ændrede holdningen til logning af persondata. Med Folketingets vedtagelse af Terrorpakke I i 2002 indførte man derfor bl.a. Retsplejelovens¹ § 786, stk. 4, der må

¹ LBK nr 1139 af 24/09/2013



anses som en undtagelse til udgangspunktet i Telelovens² regler om hemmeligholdelse af elektronisk kommunikation mv.³ Bestemmelsen har følgende ordlyd: *”Det påhviler udbydere af telenet eller teletjenester at foretage registrering og opbevaring i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. Justitsministeren fastsætter efter forhandling med erhvervs- og vækstministeren nærmere regler om denne registrering og opbevaring.”*

I kølvandet på terrorangrebene i Madrid (2004) og London (2005) vedtog EU i 2006 det såkaldte logningsdirektiv⁴. I medfør af Retsplejelovens § 786, stk. 4, 2. pkt. blev logningsbekendtgørelsen udstedt, og den trådte i kraft den 15. september 2007 samtidig med Retsplejelovens § 786, hvormed logningsdirektivet blev implementeret i dansk ret⁵.

Det fremgår af logningsbekendtgørelsens § 4, at en udbyder⁶ blandt andet skal registrere oplysninger om mobiltelefoni samt meddelelseskommunikation, herunder A- og B-numre (det opkaldende og modtagende nummer) samt navn og adresse på abonnenten mv. Yderligere skal identiteten af kommunikationsudstyret samt den eller de celler, en mobiltelefon er forbundet til og telefonmasternes placering, registreres. Samtidig skal tidspunkterne for kommunikationens start og slutning registreres. Ifølge bekendtgørelsen § 4, stk. 1 nr. 6 skal der 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 art. 5, stk. 1 litra f, nr. 1⁷

² Lov om elektroniske kommunikationsnet og – tjenester (teleloven) nr. 169 af 3. marts 2011 Jf. lovbek. nr. 128 af 7. februar 2014.

³ Der kan henvises til Munk-Hansen. C, m.fl.: *Retssikkerhed i konkurrence med andre hensyn*, Jurist- og Økonomforbundets Forlag, kapitel 2 om Logning og retssikkerhed af Charlotte Bagger for en specifik gennemgang af reglerne i teleloven og udbudsbekendtgørelsen om hemmeligholdelse.

⁴ Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15. marts 2006 om lagring af data genereret i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF, EUT(2006) L105/54.

⁵ Munk-Hansen. C, m.fl.: *Retssikkerhed i konkurrence med andre hensyn*, Jurist- og Økonomforbundets Forlag, kapitel 2 om Logning og retssikkerhed af Charlotte Bagger, s. 53. Bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen).

⁶ Af elektroniske kommunikationsnet eller –tjenester til slutbrugere

⁷ Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15. marts 2006 om lagring af data genereret i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF, EUT(2006) L105/54



Det fulgte indtil for nylig af § 5, stk. 1 i logningsbekendtgørelsen, at en udbyder skulle registrere oplysninger om internet-sessions, herunder om afsender og modtagers IP-adresse, portnumre⁸, transportprotokol⁹ og tidspunktet for kommunikationens start og slutning mv¹⁰. Justitsministeriet tog dog for nylig skridt til at ophæve reglen i bekendtgørelsens § 5, stk. 1 samt stk. 4 og 5. Ændringerne trådte i kraft den 22. juni 2014¹¹, dog således, at de såkaldte identitetsoplysninger fortsætter. I medfør af § 5, stk. 2 (nu § 5, stk. 1) skal udbydere derfor fortsat registrere en række oplysninger om en brugers adgang til internettet. Det drejer sig bl.a. om brugernes identitet og eventuelt telefonnummer samt tidspunktet for kommunikationens start og slutning. Der skal desuden stadig registreres oplysninger om lokale netværks præcise geografiske eller fysiske placering, hvis der er tale om trådløs adgang til internet¹²

Logningsbekendtgørelsens § 6 indeholder bestemmelser om pligten til at registrere en række oplysninger om brug af udbyderens egne e-mail- og internettelefon-tjenester bl.a. om afsender og modtagers e-mailadresser. Adgangen til de oplysninger, der bliver registreret og opbevaret i medfør af logningsbekendtgørelsen, bliver reguleret i retsplejelovens kapitel 71 om indgreb i meddelelseshemmeligheden, der bl.a. kræver mistanke om en alvorlig forbrydelse og retskendelse, og kapitel 74 om edition¹³. For en nærmere gennemgang kan der henvises til Justitsministeriets detaljerede redegørelse om de danske logningsregler¹⁴.

3. Eksempler på anvendelse af loggede tele- og internetoplysninger

I Justitsministeriets redegørelse om diverse spørgsmål vedrørende logningsreglerne fra 2012 konkluderer politiet, at logningsreglerne generelt er *af meget væsentlig betydning for politiets efterforskning og opklaring*

⁸ Bruges ligesom IP-adressen til at identificere afsenderen/modtageren i en kommunikation på nettet.

⁹ Oplysninger om de "færdselsregler" (protokol), som styrer kommunikationen

¹⁰ For en nærmere forklaring af hvad sessionslogning er henvises der til Munk-Hansen, C, m.fl.: *Retssikkerhed i konkurrence med andre hensyn*, Jurist- og Økonomforbundets Forlag, kapitel 2 om Logning og retssikkerhed af Charlotte Bagger, s. 51 -52. Der kan i øvrigt henvises til Justitsministeriets notat om betydning af EU-domstolens dom af 8.april i de forenede sager c.293/12 og c-594/12 for de danske logningsregler, s. 22 for en nærmere begrundelse for at ophæve sessionslogningen. når en række kriterier var opfyldt

¹¹ BEK nr 660 af 19/06/2014 - Bekendtgørelse om ændring af bekendtgørelse om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen).

¹² Tidligere logningsbekendtgørelsen § 5, stk. 3 (nu § 5, stk. 2.)

¹³ Se særligt reglerne i RPL § 781-782, der opstiller generelle betingelser for adgangen til oplysningerne.

¹⁴ Se Notat om betydning af EU-Domstolens dom af 8.april i de forenede sager c.293/12 og c-594/12 for de danske logningsregler, punkt. 3., s. 6 og frem. Tilgængelig her:

<http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2014/Notat%20om%20logningsdirektivet.pdf>



*af alvorlige forbrydelser”.*¹⁵ I samme redegørelse udtaler PET, at: ” *efterretningstjenesten anvender oplysninger om teletrafik i betydeligt omfang navnlig i forbindelse med længerevarende efterforskninger, indenfor terrorområdet, og oplysningerne om teletrafik har i flere tilfælde haft afgørende betydning for at kunne afdække terrorrelationer i både ind- og udland”.*¹⁶

Justitsministeriets redegørelse indeholder en række eksempler på, hvornår loggede tele- og internetoplysninger har været anvendt i forbindelse med forskellige former for kriminalitet. Dog har PET ikke ønsket at bidrage med konkrete eksempler grundet faren for at kompromittere tjenestens arbejdsmetoder.

I forhold til loggede teleoplysninger er bl.a. nævnt organiseret narkohandel, et skudattentat begået af tre medlemmer af en rockergruppe, drabssager, hvor man i forbindelse med logning af teleoplysninger har kunnet knytte gerningsmanden til gerningsstedet, hjemmerøverier, samt i den store Rockersag i forbindelse med både drab, våbenbesiddelse og vold, hvor politiet indhentede mere end 730.000 loggede historiske kaldsdata på i alt ca. 85 telefonnumre.¹⁷ Som eksempel på brug af loggede internetoplysninger nævnes endvidere databedrageri hos en dansk online betalingsformidler, hvor flere af deres kunder havde fået hacket og tømte deres konti. Her fik politiet via registreringen af IP-adresser fundet frem til én bestemt IP-adresse, der var brugt til at logge ind på alle de hakkede konti. På baggrund af de loggede oplysninger fandt politiet frem til gerningsmanden. Yderligere har politiet brugt loggede internetoplysninger til opklaring af røverier og netbank indbrud.

¹⁵ Retsudvalget 2012-13 REU alm. del Bilag 125 side 35

”Offentligt Redegørelse om diverse spørgsmål vedrørende logningsreglerne”. Tilgængelig her:
<http://www.ft.dk/samling/20121/alm-del/reu/bilag/125/1200765.pdf>

¹⁶ Ibid. side 36

¹⁷ Retsudvalget 2012-13, REU alm. del bilag 125 - Justitsministeriets redegørelse om diverse spørgsmål vedrørende logningsreglerne, pkt. 5.3.9. -



4. EMRK og Charteret

På trods af, at logningsdirektivet er erklæret for ugyldigt, konkluderer Justitsministeriet, at Charterets art. 7 og 8 finder anvendelse på de danske logningsregler, hvilket også lægges til grund i nærværende analyse¹⁸.

Ifølge Charterets art. 7 har: *”Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin kommunikation”*. I forhold til logning bliver bestemmelsen suppleret af Charterets art. 8, hvorefter:

”1. Enhver har ret til beskyttelse af personoplysninger, der vedrører den pågældende. 2. Disse oplysninger skal behandles rimeligt, til udtrykkeligt angivne formål og på grundlag af de berørte personers samtykke eller på et andet berettiget ved lov fastsat grundlag. Enhver har ret til adgang til indsamlede oplysninger, der vedrører den pågældende, og til berigtigelse heraf. 3. Overholdelsen af disse regler er underlagt en uafhængig myndigheds kontrol.”

Charterets art. 7 om respekt for privatlivet svarer indholdsmæssigt til EMRK art. 8, og Charterets art. 8 om personoplysninger er bl.a. baseret på EMRK art. 8.

EMRK er inkorporeret i dansk ret og dermed en del af gældende dansk lovgivning¹⁹. Det nærmere indhold af EMRK fastlægges af Den Europæiske Menneskerettighedsdomstols (EMD) autoritative fortolkning, og der findes her en omfangsrig praksis på området for art. 8, herunder i forhold til staters overvågning og indsamling af persondata. Denne praksis er dermed direkte relevant for vurderingen af, hvorvidt de danske logningsregler er forenelige med privatlivets fred.

EMRK art. 8 lyder som følger:

1. Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance. 2. Ingen offentlig myndighed kan gøre indgreb i udøvelsen af denne ret, undtagen for så vidt 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 sundheden eller sædeligheden eller for at beskytte andres ret og frihed.

¹⁸ 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, 2. juni 2014, justitsministeriet, EU-retskontoret, s. 19-21

¹⁹ Lov nr. 285 af 29. april 1992. Dentrådte i kraft 1. juli 1992



5. EU-domstolens dom om logningsdirektivets ugyldighed

Den 8. april 2014 afsagde EU-Domstolen dom i *Digital Rights and others v. Ireland*²⁰ (herefter "Digital Rights"), hvorefter logningsdirektivet (direktiv 2006/24/EF) af 15. marts 2006 blev erklæret ugyldigt.

EU-domstolen indleder med at fastslå, at direktivet indebærer et indgreb i art. 7 og 8 i Charteret af særlig alvorlig og vidtrækkende karakter, eftersom " *Den omstændighed, at lagringen af data og den efterfølgende anvendelse af dem finder sted, uden at abonnenten eller den registrerede bruger oplyses herom, er desuden, som generaladvokaten har anført i punkt 52 og 72 i forslaget til afgørelse, egnet til at skabe en følelse hos de berørte personer af, at deres privatliv er genstand for konstant overvågning.* " ²¹.

Herefter undersøger EU-Domstolen, om indgrebet alligevel kan begrundes.

Domstolen fremhæver, at den lagring, direktivet forskriver, ikke i sig selv krænker det væsentligste indhold i beskyttelsen efter Charterets art. 7 og 8, da der bl.a. ikke er hjemmel til at gøre sig bekendt med indholdet af kommunikationen.²² Oplysninger bliver desuden behandlet for at bekæmpe grov kriminalitet og international terrorisme. Logning af oplysninger forfølger således et legitimt formål ²³.

Det væsentligste element i EU-Domstolens analyse vedrører, hvorvidt Direktivet både er egnet til at nå det tilsigtede mål og ikke går videre, end hvad der er passende og nødvendigt for at nå dette mål, dvs. om proportionalitetsprincippet er overholdt.

EU-Domstolen fremhæver, at EU-lovgivers skønsbeføjelser i denne henseende er underlagt en streng efterprøvelse, hvilket bl.a. er begrundet med indgrebenes alvorlige og vidtrækkende karakter.²⁴

Ifølge EU-Domstolen er den lagring, der er hjemlet i direktivet, egnet til at gennemføre det mål, som forfølges. EU-Domstolen er imidlertid af den opfattelse, at bekæmpelse af grov kriminalitet ikke i sig selv kan begrunde, at logningen af oplysninger i medfør af direktivet anses som nødvendig²⁵.

²⁰EU-Domstolens dom (Store Afdeling) 8. april 2014 (*) I de forenede sager C-293/12 og C-594/12. Tilgængelig her: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=462425>, besøgt 25.06.2014

²¹ Ibid.

²² Præmis 38-40.

²³ Præmis 40-42

²⁴ Præmis 48



Det fremgår af præmis 51, at: ” *Hvad angår spørgsmålet, om den datalagring, som er foreskrevet i direktiv 2006/24, er nødvendig, skal det fastslås, at bekæmpelse af grov kriminalitet, og navnlig organiseret kriminalitet og terrorisme, ganske vist er af afgørende betydning for at sikre den offentlige sikkerhed, og at effektiviteten heraf i vidt omfang kan være afhængig af anvendelse af moderne efterforskningsteknikker. Et sådant mål af almen interesse kan imidlertid, hvor grundlæggende det end er, ikke i sig selv begrunde, at en foranstaltning med henblik på datalagring som den, der er indført med direktiv 2006/24, anses for nødvendig af hensyn til bekæmpelsen af grov kriminalitet.*”

EU-Domstolen anfører, at beskyttelsen af personoplysninger har særlig betydning for privatlivets fred. Derfor skal undtagelser fra eller begrænsninger i beskyttelsen af disse oplysninger indskrænkes til det strengt nødvendige. Beskyttelsen af personoplysning efter Charterets art. 8 har desuden ifølge domstolen særlig betydning for retten til respekt for privatlivet efter Charterets art. 7.²⁶

Herudover fremgår følgende af præmis 54:

”*Den pågældende EU-lovgivning skal således fastsætte klare og præcise regler, som regulerer rækkevidden og anvendelsen af den omhandlede foranstaltning og opstille 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.*”

Helt centralt står dommens præmis 56: -

”*Hvad angår spørgsmålet, om det indgreb, som direktiv 2006/24 indebærer, er begrænset til det strengt nødvendige, bemærkes, at dette direktiv i henhold til dets art. 3, sammenholdt med dets art. 5, stk. 1, foreskriver lagring af alle trafikdata vedrørende fastnettelefoni, mobiltelefoni, internetadgang samt e-mail og telefoni via internettet. Det omfatter således alle elektroniske kommunikationsmidler, hvis anvendelse er meget udbredt og af stadigt stigende betydning i den enkeltes dagligdag. Desuden omfatter dette direktiv i henhold til dets art. 3 alle abonnenter og registrerede brugere. Det indebærer dermed et indgreb i de*

²⁵ Præmis 51-53

²⁶ Præmis 52-53



grundlæggende rettigheder for praktisk talt hele den europæiske befolkning.”²⁷. præmis 57-59 har følgende ordlyd:

*”I denne henseende skal det for det første fastslås, at direktiv 2006/24 generelt 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. [...] præmis 58: Direktiv 2006/24 omfatter således dels 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. Direktivet finder dermed anvendelse selv på personer, for hvis vedkommende der ikke findes noget som helst indicium for, at deres adfærd kan have – selv en indirekte eller fjern – forbindelse til grov kriminalitet.**[...]*

Præmis 59: ”Dels kræver det nævnte direktiv, skønt det har til formål at bidrage til bekæmpelsen af grov kriminalitet, 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 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.”

EU-domstolen påpeger endvidere i sin analyse, at direktivet ikke fastsætter tilstrækkelige garantier, der gør det muligt at sikre effektiv beskyttelse af lagrede data mod risikoen for misbrug og mod enhver ulovlig adgang til og anvendelse af disse oplysninger²⁸ Det må umiddelbart antages, at dansk ret isoleret set opfylder kravene om tilstrækkelige garantier, herunder kravet om retskendelse, værn mod misbrug af opbevarede oplysninger, kontrol fra uafhængig myndighed, samt varighed af lagringsperioden, hvorfor denne del af afgørelsen derfor ikke gennemgås yderligere²⁹. Disse efterfølgende retssikkerhedsgarantier er dog ikke automatisk tilstrækkelige til at kvalificere logningsreglerne som proportionelle, såfremt det indledende indgreb i sig selv er så intensivt, at det må betegnes som uproportionelt, jf. nærmere nedenfor.

Ordlyden i domstolens afsluttende præmis 65 er imidlertid afgørende:

²⁷ Justitsministeriets 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 regler, punkt 2, side. 3.

²⁸ Præmis 60-64

²⁹ Der kan henvises til gennemgangen af de danske regler herom i Justitsministeriets 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, 2, juni 2014, s. 6



*”Det fremgår af det ovenstående, at direktiv 2006/24 ikke fastsætter klare og præcise regler, der regulerer rækkevidden af **indgrebet** i de grundlæggende rettigheder, som er fastslået i chartrets art. 7 og 8. Det må derfor fastslås, at dette direktiv 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.”*

EU-Domstolen erklærede henset til samtlige bemærkninger i dommen, og dermed uden udtrykkeligt at klargøre, hvor meget vægt de enkelte kriterier om lagring, adgang og varighed skulle tillægges, at EU-lovgiver ved vedtagelsen af direktivet havde overskredet de grænser, som overholdelsen af proportionalitetsprincippet kræver henset til Charterets art. 7, 8 og 52, stk. 1.³⁰ Dermed blev direktivet erklæret ugyldigt i sin helhed.

6. Justitsministeriet analyse af dommens betydning for dansk ret

I Justitsministeriets notat³¹ foretages en vurdering af dommens betydning for de danske logningsregler. Det anføres indledningsvist, at man ønsker at vurdere, hvorvidt de danske logningsregler er i overensstemmelse med Charterets bestemmelser om retten til respekt for privatliv og familieliv, jf. art. 7 samt bestemmelser om retten til beskyttelse af personoplysninger, jf. art. 8. Dette sker på baggrund af EU-Domstolens dom af 8. april 2014.

Justitsministeriet anfører, som nævnt, at Charteret samt praksis fra EMD finder anvendelse i forhold til de danske logningsregler.³²

Justitsministeriet konkluderer, at registrering og opbevaring i henhold til logningsbekendtgørelsen udgør et indgreb i retten til privatliv og i retten til beskyttelse af personoplysninger, jf. Charterets art. 7-8. Det vurderes videre, at registrering og opbevaring i henhold til bekendtgørelsen - med henblik på efterforskning og retsforfølgelse - forfølger et sagligt formål samt, at registrering og opbevaring er egnet til at opnå dette formål.

³⁰ Præmis 69 – Samtlige bemærkninger/præmisser i EU-dommen er desuden ikke nævnt i dette referat. Kun de væsentligste præmisser er medtaget.

³¹ Justitsministeriets 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 regler, punkt 4, side. 19-30.

³² *ibid.* S. 22



Ifølge Justitsministeriet har erfaringerne med sessionslogning vist, at de oplysninger, der bliver sessionslogget, kun i meget begrænset omfang er brugbare i praksis i forbindelse med efterforskning og retsforfølgning af strafbare forhold³³. Derfor konkluderer ministeriet, at disse regler ikke er egnede til at opnå formålet om at skabe mulighed for at anvende oplysningerne som led i efterforskning og retsforfølgelse. Justitsministeriet ophævede derfor reglerne om sessionslogning, og disse ændringer trådte i kraft den 22. juni 2014.³⁴

Det bemærkes, at Justitsministeriet ikke anfører, at sessionslogning er i strid med Charteret eller EMRK art. 8 samt, at justitsministeren i et åbent samråd³⁵ åbnede for muligheden for at genindføre sessionslogning, såfremt de tekniske muligheder for anvendelse af ordningen forbedres.³⁶

Justitsministeriet analyserer herefter, om indgrebet i de danske logningsregler er afgrænset til det strengt nødvendige på baggrund af samme treledede begrundelse, som er anvendt af Domstolen: Registrering af oplysninger (i) adgang til de registrerede oplysninger (ii) varighed af opbevaring (iii).

Justitsministeriet indleder punkt (i) med at fremhæve, at den registrering og opbevaring, der foretages i medfør af logningsbekendtgørelsen, svarer til den registrering, der skulle foretages med udgangspunkt i logningsdirektivet. Dernæst fastslås, at der foretages registrering og opbevaring, der går videre end de forpligtelser, der fulgte af logningsdirektivet. Overimplementeringen består bl.a. i, at der foretages registrering og opbevaring af oplysninger om både den første og sidste mast, som en mobiltelefon er forbundet til som led i en kommunikation, jf. logningsbekendtgørelsen § 4, stk. 1, nr. 6, hvorfor de danske regler på dette område er signifikant mere indgribende, end hvad der fulgte af direktivet. Dernæst anføres det, at:

”For så vidt angår vurderingen i forhold til Charterets art. 7 og 8 bemærkes, at registrering og opbevaring af oplysninger foretaget i henhold til logningsbekendtgørelsen - på samme generelle vis som registrering og opbevaring foretaget i henhold til logningsdirektivet – omfatter alle personer og alle elektroniske

³³ Justitsministeriets 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 regler, punkt 4, side. 22.

³⁴ Bekendtgørelse 2014-06-19 nr. 660 om ændring af bekendtgørelse om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen) § 2. Der henvises til punkt. 6, hvor der er en gennemgang af justitsministeriets begrundelse for at ophæve sessionslogning

³⁵ Tilgængelig her: <http://www.ft.dk/webtv/video/20131/reu/td.1130634.aspx?from=02-06-2014&to=08-08-2014&selectedMeetingType=Udvalg&committee=REU&as=1#pv>, sidst besøgt 8. august 2014

³⁶ 2. juni 2014: Åbent samråd med justitsministeren om hvad den danske regering agter at foretage sig som reaktion på dommen. (domstolens dom i de forenede sager C-293/12 og C-594/12 Digital Rights Ireland og Seitlinger m.fl.) m.v).



kommunikationsmidler og samtlige trafikdata uden nogen form for differentiering, begrænsning eller undtagelse under hensyn til målet om at bekæmpe kriminalitet³⁷

Herefter foretages der dog ikke yderligere vurdering af den indledende logning af oplysninger, der ellers udgør selve indgrebet i Charter-rettighederne og EMRK og dermed det mest essentielle og centrale element af logningsreglerne³⁸

Justitsministeriet anfører herefter, at der baseret på dommens præmis 54, foreligger et krav om, at lovgivningen fastsætter klare og præcise regler, der gør det muligt at beskytte personoplysningerne mod misbrug.

Herefter gennemgår Justitsministeriet relevante momenter fra EMDs afgørelse i Weber og Saravia mod Tyskland (54934/00). Ministeriet lægger vægt på præmisserne 93-95, der vedrører en nærmere diskussion af forholdet mellem EMRK art. 8 og hemmelig overvågning. Med forbehold for forskellen mellem hemmelig overvågning og logning i medfør af bekendtgørelsen kan Weber-afgørelsen ifølge ministeriet tjene som grundlag for vurderingen af de krav, der må stilles til national lovgivning.

Dernæst gennemgås de relevante danske regler, og på den baggrund vurderer ministeriet, at dansk ret indeholder klare betingelser for adgangen til oplysninger, der er registreret og opbevaret i henhold til logningsbekendtgørelsen, samt tilstrækkelige garantier mod misbrug.

Justitsministeriet overvejer i sin konklusion vægten af analysens enkelte dele, og det anerkendes, at der består en vis tvivl om, hvilken vægt de enkelte dele skal tillægges. Justitsministeriet konkluderer dog samlet set, men med særlig vægt på dansk rets klare og præcise regler for adgangen til og opbevaring af oplysningerne, at de danske logningsregler er i overensstemmelse med Charterets art. 7 og 8.³⁹

³⁷ Justitsministeriets 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 regler, punkt 4, side. 23.

³⁸ Se afsnit 5. ovenfor, hvor disse præmisser i dommen gennemgås.

³⁹ Det skal bemærkes at kun de væsentligste dele af Justitsministeriets analyse er medtaget her. Se Justitsministeriets 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 regler punkt. 4 s. 19-30



7. Analyse af Justitsministeriets afsnit om dommens betydning for de danske regler

Justitsministeriet foretager i notatet en vurdering af tre facetter af den danske logningsbekendtgørelse: Registrering af oplysninger (i) adgang til de registrerede oplysninger (ii) varighed af opbevaring (iii). Der må dog stilles spørgsmålstegn ved, hvorvidt Justitsministeriet reelt foretager så intensiv prøvelse af det indledende indgreb i form af den automatiske og omfattende lagring af persondata uden krav om mistanke m.v., som påkrævet, når henses til EU-Domstolens præmisser om, at (i) selve indgrebet er ”omfattende og særligt alvorligt”, (ii) indgreb i Charterets art. 7 og 8 skal afgrænses til ”det strengt nødvendige” og, (iii) der skal foretages en ”streng kontrol” af sådanne indgreb. Justitsministeriets vurdering synes således dels at indeholde en relativt overfladisk vurdering af selve indgrebet og dels at bygge på en antagelse om, at de efterfølgende retssikkerhedsgarantier, der skal modvirke selve indgrebets betænkelige karakter, er afgørende for vurderingen af, hvorvidt indgrebet kan karakteriseres som strengt nødvendigt og proportionalt i Charteret og EMRKs forstand.

Endvidere synes notatet indirekte at bygge på en antagelse om, at den nationale skønsmargin er bredere, end hvad EU-dommen og relevant retspraksis fra EMD tilsiger, jf. *Digital Rights* krav om ”streng prøvelse”.⁴⁰ En sådan analyse og konklusion havde været mere nærliggende, såfremt EU-domstolen havde lagt vægt på de samme momenter som Generaladvokatens forslag, der fandt, at logningsdirektivet krænkede Charteret grundet bl.a. manglende klarhed i lovgivningen⁴¹, mens EU-Domstolen lægger større vægt på kravet om proportionalitet.⁴²

Justitsministeriets notat indeholder ikke en selvstændig vurdering eller diskussion af nødvendighedskravet i forhold til den indledende logning af data, der ellers udgør et af de absolutte hovedspørgsmål ved vurderingen

⁴⁰ Se praksis fra EMD nedenfor, og se præmis 48 i EU-Domstolens dom (”digital rights”) om logningsdirektivets ugyldighed, hvoraf det følger EU-lovgiver er underlagt en streng efterprøvelse.

⁴¹ Præmis 106-132 - FORSLAG TIL AFGØRELSE FRA GENERALADVOKAT P. CRUZ VILLALÓN fremsat den 12. december 2013 (1). Sag C-293/12 Digital Rights Ireland Ltd mod The Minister for Communications, Marine and Natural Resources The Minister for Justice, Equality and Law Reform The Commissioner of the Garda Síochána Ireland og The Attorney General.

⁴² Fra præmis 50 og frem EU-Domstolens dom (Store Afdeling) 8. april 2014 (*) i de forenede sager C-293/12 og C-594/12. Tilgængelig her:

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=462425>, besøgt 25.06.2014



af, om indgrebet er strengt nødvendigt. Uden selve lagringen ville de retssikkerhedsgarantier, Justitsministeriet lægger afgørende vægt på, slet ikke være nødvendige.

Både EU-Domstolens præmisser, samt dele af den EMD retspraksis, der henvises til i "*Digital Rights*" afgørelsen, rejser dog væsentlig tvivl om denne fremgangsmåde og den udtalte præmis om, at efterfølgende retssikkerhedsgarantier vil være tilstrækkelige til at "redde" et intensivt indgreb.

Af EU-Domstolens præmisser skal igen særligt fremhæves præmis 56-59 og ordvalget i præmis 58, hvor det følgende fremgår: "[...] **uden at de personer, hvis data lagres, dog – end ikke indirekte – befinder sig i en situation, der vil kunne give anledning til strafferetlig forfølgning. Direktivet finder dermed anvendelse selv på personer, for hvis vedkommende der ikke findes noget som helst indicium for, at deres adfærd kan have – selv en indirekte eller fjern – forbindelse til grov kriminalitet.**[...]"

Præmis 58 synes således at være et signal fra EU-Domstolen om, at det i sig selv er betænkeligt automatisk at lagre persondata om alle borgeres elektroniske kommunikation uden, at der foreligger en mistanke vedrørende alvorlig kriminalitet, hvilket underbygges af, at præmissen kan læses som en detaljeret forskrift for, hvordan logningsregler kan afgrænses, så de overholder proportionalitetsprincippet. Som Martin Husovec har udtalt om præmis 58: "*This Paragraph seems to be an indispensable precondition [...]it seems very unlikely that the court would make an exact suggestion of this kind, if it would not perceive this condition as a crucial one.*"⁴³

Et andet væsentligt punkt, der fremhæves i dommen er omfanget af den indledende logning. Det er særligt i præmis 56, hvor det fremgår, at datadirektivet "[...]foreskriver **lagring af alle trafikdata vedrørende fastnettelefoni, mobiltelefoni, internetadgang samt e-mail og telefoni via internettet. Det omfatter således alle elektroniske kommunikationsmidler, hvis anvendelse er meget udbredt og af stadigt stigende betydning i den enkeltes dagligdag. Desuden omfatter dette direktiv i henhold til dets art. 3 alle abonnenter og registrerede brugere. Det indebærer dermed et indgreb i de grundlæggende rettigheder for praktisk talt hele den europæiske befolkning.**"

⁴³ Martin Husovec ekspert i internet law, advokat, samt IMPRS_CI Doctoral Research fellow at Max Planck institute. I en artikel til Stanford law school "First European constitutional court suspends data retention after the decision of the court of justice of EU". Tilgængelig her: <http://cyberlaw.stanford.edu/blog/2014/04/first-european-constitutional-court-suspends-data-retention-after-decision-court>, sidst besøgt 10. august 2014.



Denne trussel mod privatlivets fred og borgernes følelse af konstant overvågning blev også fremhævet af den tyske forfatningsdomstol, der allerede i 2010 erklærede den tyske implementering af logningsdirektivet for forfatningsstridig:

"Even though the storage does not extend to the contents of the communications, these data may be used to draw content-related conclusions that extend into the users' private sphere. In combination, the recipients, dates, time and place of telephone conversations, if they are observed over a long period of time, permit detailed information to be obtained on social or political affiliations and on personal preferences, inclinations and weaknesses. Depending on the use of the telecommunication, such storage can make it possible to create meaningful personality profiles of virtually all citizens and track their movements. It also increases the risk of citizens to be exposed to further investigations without themselves having given occasion for this. In addition, the possibilities of abuse that are associated with such a collection of data aggravate its burdensome effect. In particular since the storage and use of data are not noticed, the storage of telecommunications traffic data without occasion is capable of creating a diffusely threatening feeling of being watched which can impair a free exercise of fundamental rights in many areas".⁴⁴

I modsætning til EU-Domstolen fremhæver Justitsministeriet alene én dom fra EMD, nemlig Weber & Saravia, der omhandler hemmelig overvågning. Det er dog ikke klart, at Weber & Saravia er den mest direkte relevante dom, selvom den indeholder relevante overordnede principper. Dommen omhandlede en ordning, der gav adgang til "strategisk aflytning" af trådløs telekommunikation, når en række kriterier var opfyldt. Der var derfor ikke, som i tilfældet med logning, tale om automatisk lagring af så godt som alle personers tele- og internetdata bagudrettet i tid. Endvidere lagde EMD i præmis 106 vægt på, at de tyske myndigheder i Weber & Saravia havde en "fairly wide margin of appreciation", hvilket ikke var tilfældet i *Digital Rights*, jf. kravet om "streng nødvendighed" og EU-Domstolens "strenge prøvelse". Der er dog en række andre domme fra EMD, der synes mere direkte relevante, eftersom de netop omhandler lagring af persondata, om end i form af DNA, fingeraftryk og celleprøver. Særligt dommene i *S and Marper v. UK* og *M.K. v. France* bør fremhæves.⁴⁵

⁴⁴ 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 –dom af 2. marts 2010 (engelsk oversættelse) tilgængelig her:

<http://www.bverfg.de/pressemitteilung/bvg10-011en.html>, sidst besøgt 9. august 2014.

⁴⁵ Se afsnit 6. umiddelbart ovenfor.



I *S and Marper v. UK* klagede to personer, der var blevet sigtet for kriminalitet og siden løsladt, over, at det engelske politi beholdt deres DNA, fingeraftryk og celleprøver i en database, uanset at de ikke var blevet tiltalt eller dømt for forbrydelserne.⁴⁶

EMD gjorde indledningsvist klart, at den blotte lagring af data, der relaterer sig til privatlivets fred, udgør et indgreb i EMRK art. 8 uanset den efterfølgende brug deraf, samt at en samlet vurdering af et sådant indgrebs forenelighed med art. 8 afhænger af *”the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained.”*⁴⁷ Endvidere lagde EMD vægt på, at en begrundet frygt for, hvordan indsamlet persondata vil kunne anvendes i fremtiden henset til den teknologiske udvikling, var et relevant moment i bedømmelsen af indgrebet.⁴⁸

I dommens præmis 103 fremhæves, at behovet for retssikkerhedsgarantier vejer særlig tungt, når det drejer sig om persondata, der processes automatisk og ikke mindst, når de anvendes i politimæssigt øjemed. I den forbindelse skal den relevante lovgivning særligt sikre, at *”such data are relevant and not excessive in relation to the purposes for which they are stored”*. EMD anerkendte, at hensynet til privatlivsbeskyttelse kan vige til fordel for bekæmpelsen af kriminalitet, særligt organiseret kriminalitet og terrorisme, og at ny teknologi er vigtige redskaber i den henseende, men gjorde klart, at der skal foretages en *”streng prøvelse”* af både lagring og efterfølgende anvendelse, når det sker uden samtykke.⁴⁹

I forhold til det konkrete indgreb fandt EMD ikke, at indsamlingen af klagernes persondata var proportionel, hvorfor indgrebet var i strid med EMRK art. 8. Det er i forhold til logningsreglerne særligt relevant at fremhæve følgende præmis fra dommen:

”In this respect, the Court is struck by the blanket and indiscriminate nature of the power of retention in England and Wales. The material may be retained irrespective of the nature or gravity of the offence with which the individual was originally suspected or of the age of the suspected offender; fingerprints and samples may be taken – and retained – from a person of any age, arrested in connection with a recordable offence, which includes minor or non-imprisonable offences. [...] in particular, there is no provision for independent

⁴⁶ *S. and Marper mod Storbritannien* dom af 4. december 2008

⁴⁷ *Ibid.* para 67

⁴⁸ *Ibid.* para 70-71

⁴⁹ *Ibid.* para 104-105.



review of the justification for the retention according to defined criteria, including such factors as the seriousness of the offence, previous arrests, the strength of the suspicion against the person and any other special circumstances.”⁵⁰

Præmissen om ”blanket retention” og ”indiscriminate nature” af de indsamlede personoplysninger uden hensyn til krav om mistanke eller lignende ligger meget tæt op af EU-Domstolens præmisser om samme i Digital Rights afgørelsen.

Det er i den forbindelse særligt væsentligt at hæfte sig ved, at EMD i præmis 125 eksplicit konkluderede, at selve indsamlingen og lagringen af persondata udgjorde et så intensivt og uproportionalt indgreb, at det ikke var nødvendigt at vurdere indholdet af de retssikkerhedsgarantier, som skulle modvirke en for bred og vilkårlig adgang til og misbrug af de relevante data:

” In conclusion, the Court finds that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants’ right to respect for private life and cannot be regarded as necessary in a democratic society. This conclusion obviates the need for the Court to consider the applicants’ criticism regarding the adequacy of certain particular safeguards, such as too broad an access to the personal data concerned and insufficient protection against the misuse or abuse of such data”

Denne præmis synes mest nærliggende at skulle fortolkes således, at masseindsamling af persondata uden afgrænsning i sig selv er uproportionelt, uanset efterfølgende retssikkerhedsgarantier, hvilket igen synes at understøtte en sådan udlægning af afgørelsen i *Digital Rights*.⁵¹

I den nylige dom M.K. v France fra 2013 blev klager sigtet for tyveri, og i den forbindelse blev hans fingeraftryk og foto registreret i en database og opretholdt efter politiet frafaldt sigtelsen.⁵² EMD gentog de centrale præmisser fra S. and Marper fremhævet ovenfor, ligesom EMD lagde vægt på, at

⁵⁰ Ibid. para 119

⁵¹ Ibid. para 125



*the purpose of the database, notwithstanding the legitimate aim pursued, necessarily involves adding and retaining as many names as possible,*⁵³

samt, at database og de regler der galdt for den

*“would in practice be tantamount to justifying the storage of information on the whole population of France, which would most definitely be excessive and irrelevant.”*⁵⁴

EMD fremhævede også, at

*“the risk of stigmatisation, stemming from the fact that persons in the applicant’s position, who have not been convicted of any offence and are entitled to the presumption of innocence, are treated in the same way as convicted persons. While, from this angle, the retention of private data cannot be equated with the voicing of suspicions, the conditions of retention of the data must not give the impression that the persons concerned are not being treated as innocent.”*⁵⁵

Både det forhold, at EMD udtaler, at en database der omfatter en hel befolkning, samt at uskyldige omfattes på samme måde som personer, der er dømt eller tiltalt, er særdeles relevante for de danske logningsregler, eftersom samme forhold gør sig gældende her.

Det er i den forbindelse væsentligt at fremhæve, at de danske logningsregler er langt mere omfattende end de britiske og franske ordninger, der blev underkendt i *S and Marper* og *M.K. v France*, eftersom de danske logningsregler omfatter alle personer, der anvender den relevante teknologi uden nogen form for personmæssig afgrænsning, mens de franske og britiske regler alene omfattede personer, der var blevet sigtet for visse former for kriminalitet.

S and Marper v. UK, *M.K. v. France* samt *Digital Rights* afgørelsen synes således alle at lægge afgørende vægt på selve indgrebets omfattende karakter i form af både intensitet og personkreds, hvorfor det må formodes, at masseindsamling af persondata uden skelen til konkret mistanke eller lignende i sig selv er svært foreneligt med både Charterets Art. 7 og 8, samt EMRK art. 8. Det skal i den forbindelse fremhæves, at begge afgørelser er nyere end *Weber & Saravia*, ligesom *S & Marper* er en Storkammerdom afsagt af 17 dommere, mens *Weber*

⁵² *M.K. v France* dom af 18 april 2013

⁵³ *Ibid.* para 36

⁵⁴ *Ibid.* para 37

⁵⁵ *Ibid.* para 33



& *Saravia* er en admissibilitetsafgørelse. På denne baggrund må præjudikatsværdien af *S & Marper* og *M.K. v. France* antages at være betydeligt vægtigere end *Weber & Saravia*.

Det er i den forbindelse særdeles påfaldende, at Justitsministeriets notat ikke indeholder nogen diskussion af *S and Marper v. UK* eller *M.K. v. France*. Afgørelserne fremhæves da også som centrale i den rapport om Digital Rights afgørelsen, som to europæiske eksperter udfærdigede for to af Europaparlamentets parlamentariske grupper den 30. juni 2014:

"While all cases include essential general principles in the context of data storage, *S. and Marper v. UK* and *M.K. v. France*, are of specific importance since the facts and circumstances of these cases are similar to the DRD situation and concern also the mass collection and storage of data for L[aw] E[enforcement] purposes".⁵⁶

Anvendes principperne fra *M.K. v. France* og *Marper and S v. UK* på de danske logningsregler, synes det, uanset en vis tvivl, mere nærliggende at konkludere, at reglerne i deres nuværende udformning ikke opfylder kravene til proportionalitet, eftersom de (i) omfatter sensitive persondata, der tillader myndighederne at danne sig et præcist og indgående blik i borgernes geografiske færden, hvordan, hvor længe og hvem de kommunikerer med, (ii) omfatter alle borgere uanset relation til alvorlig kriminalitet eller ej (iii) omfatter registrering af store dele af borgernes kommunikation, herunder al telekommunikation, uanset hvem borgerne kommunikerer med. Disse forhold synes således ikke at være fornødent afgrænset hverken i forhold til personkreds, mistankegrundlag, indhold eller senere brug.

Selvom det må erkendes, at logningsreglerne har spillet en væsentlig rolle i efterforskningen af alvorlig kriminalitet, og formodningsvist også i forhold til terror, kan hensynet til bekæmpelse af alvorlig kriminalitet ikke i sig selv medføre, at et så intensivt indgreb som masseindsamling af persondata anses for "strengt nødvendigt". Det er eksempelvis klart, at indsamling og lagring af DNA og fingeraftryk, som i de ovennævnte EMD sager, også ville være væsentlige hjælpemidler for politiet i alvorlige straffesager, der både ville kunne medvirke til at fælde skyldige og fjerne mistanken fra uskyldige, men at hensynet til privatlivets fred ikke kan retfærdiggøre omfattende lagring af sådan data.

⁵⁶ "Comprehensive Study on the Court of Justice of the EU's ruling on the Data Retention Directive" af 30 juni 2014 tilgængelig her: http://www.en.uni.lu/fdef/actualites/comprehensive_study_on_the_court_of_justice_of_the_eu_s_ruling_on_the_data_retention_directive, sidst besøgt 10. August 2014.



Som det fremgår nedenfor af anbefalingerne, vil det dog også være muligt at bibeholde logningsinstrumentet i en mere afgrænset, målrettet og proportionel version, der tager større hensyn til indgrebets intensive karakter samtidig med, at det giver myndighederne adgang til at anvende de teknologiske muligheder, som logning medfører.

Formodningen om, at automatisk logning af persondata, som i de danske regler er i strid med Charteret og EMRK, støttes da også af Søren Sandfeld Jakobsen, professor i it-ret ved Aalborg Universitet, der i et interview med Politiken har udtalt følgende *"Selv om vi har regler i retsplejeloven om, at politiet skal indhente en dommer kendelse, er det min vurdering, at Justitsministeriets tolkning af EU-dommen er for snæver. Som jeg læser dommen, rammer den proportionaliteten i vid forstand, og dermed i forhold til selve indsamlingen af data. Derfor mener jeg stadig væk, at de danske logningsregler vil være i strid med chartret"*⁵⁷

I den ovennævnte detaljerede rapport om konsekvenserne af Digital Rights-afgørelsen, som to eksperter har udarbejdet for Europaparlamentet, konkluderes det, at

*"To conclude, the analysis has demonstrated the far-reaching impact of the DRD Judgement. Essential is that the blanket retention data of unsuspecting persons for the later use for L[aw] E[enforcement] is not in line with Article 7 and 8 CFR since it is not possible to establish a link between the data retained and a threat to public security. For any other possible future data retention measure, the EU as well as the Member States are obliged to demonstrate the necessity of the measures in every single case."*⁵⁸

En anden ekspert indenfor EU-retten, professor Steven Peers, deler denne opfattelse: *"First of all, any new Directive would have to be in some sense targeted upon communication which has a particular link with serious crime and terrorism. Very simply, mass surveillance is an unjustifiable infringement of Charter rights."*⁵⁹

Omvendt har en svensk ekspert udpeget af det svenske Justitsministerium konkluderet, at de svenske logningsregler er i overensstemmelse med Charteret.⁶⁰ Denne rapport synes dog i høj grad at hvile på samme

⁵⁷ Artikel i Politiken 2, juni 2014 "Teleindustrien overvejer retssag mod regeringen efter overvågning". Tilgængelig her: <http://politiken.dk/oekonomi/virksomheder/ECE2306591/teleindustrien-overvejer-retssag-mod-regeringen-efter-overvaagning/> , Sidst besøgt: 18. juni 2014.

⁵⁸"Comprehensive Study on the Court of Justice of the EU's ruling on the Data Retention Directive" af 30 juni 2014 tilgængelig her: http://www.uni.lu/fdef/actualites/comprehensive_study_on_the_court_of_justice_of_the_eu_s_ruling_on_the_data_retention_directive, sidst besøgt 10. August 2014. side. 95

Artikel: "the data retention judgement cjeu" Tilgængelig her: <http://eulawanalysis.blogspot.dk/2014/04/the-data-retention-judgment-cjeu.html> - Siden er sidst besøgt 17.07.2014



synspunkter som Justitsministeriets notat, hvorfor den ikke lægger tilstrækkelig vægt på intensiteten af det indledende indgreb i form af logning men fremhæver betydningen af efterfølgende retssikkerhedsgarantier.

8. Nationale domme fra andre lande:

Den 27. juni 2014 erklærede den østrigske forfatningsdomstol de østrigske logningsregler for ugyldige. Det var den første afgørelse om logningsregler i nationalt regi, efter EU-Domstolen erklærede direktivet for ugyldigt i april.⁶¹

Ifølge den østrigske forfatningsdomstol var de østrigske logningsregler i strid med EMRK art 8 om retten til respekt for privatlivet. Reglerne var ifølge domstolen ikke proportionale, da de udgjorde et alvorligt indgreb i fundamentale rettigheder, især fordi de medførte overvågning af for mange mennesker uden en mistanke⁶².

Den 3. juli 2014 annullerede også den slovenske forfatningsdomstol deres nationale logningsregler af lignende årsager⁶³. Den slovenske domstol fandt de nationale logningsregler for at være uproportionale, bl.a. fordi der skete massiv og ikke-selektiv logning, der udgjorde et indgreb over for en stor del af befolkningen, uden en tilstrækkelig begrundelse var givet herfor. Der var desuden ikke givet tilstrækkelig begrundelse for den valgte logningsperiode på 8 måneder, ligesom brugen af loggede data ikke var begrænset til alvorlig kriminalitet⁶⁴.

Den 8. juli 2014 blev de rumænske logningsregler også erklæret ugyldige af den rumænske forfatningsdomstol. Begrundelsen for reglernes ugyldighed vil først blive offentliggjort i august 2014⁶⁵. Disse domme synes også at styrke formodningen af, at masselogning af persondata uden afgrænsning i forhold til personkreds, mistankegrundlag eller lignende er uforeneligt med Charterets og EMRK.

⁶⁰ Datalagring, EU-rätten och svensk rätt” Ds 2014:23, Utgiven: 13 juni 2014, Typ: Departementsserien (Ds)
Avsändare: Justitiedepartementet. Tilgængelig her: <http://www.regeringen.se/content/1/c6/24/23/60/0561d122.pdf>, sidst besøgt 31. august 2014

⁶¹ Østrigsk pressemeddelelse om de østrigske logningsreglers ugyldighed 27 juni 2014, tilgængelig her: <http://radiobruelleslibera.wordpress.com/2014/06/27/data-retention-down-in-austria/>, sidst besøgt: 10 august 2014.

⁶² Artikel: “[Austrian Constitutional Court rules data retention unconstitutional](http://www.digitalrights.ie/austrian-constitutional-court-rules-data-retention-unconstitutional/)”, tilgængelig her: <http://www.digitalrights.ie/austrian-constitutional-court-rules-data-retention-unconstitutional/>,

⁶³ Afgørelsen er til rådighed her, dog kun på slovensk: https://www.ip-rs.si/fileadmin/user_upload/Pdf/sodbe/US_RS_ZEKom-1_3julij2014.tif, sidst besøgt 19-07-2014.

⁶⁴ Kort referat af dommen til rådighed her: <http://radiobruelleslibera.wordpress.com/2014/06/27/data-retention-down-in-austria/>, sidst besøgt 19.07.2014

⁶⁵ Officiel pressemeddelelse fra den rumænske forfatningsdomstol: Tilgængelig her <http://www.ccr.ro/noutati/COMUNICAT-DE-PRES-99>



9. Alternativ ordning

På baggrund af overstående foreslås det at indføre en alternativ ordning baseret på en 2-ledet proces. I tilfælde, hvor politiet eller PET har en "rimelig formodning" om, at en person er involveret i kriminalitet omfattet af retsplejelovens § 781, stk. 3 (strafferamme på 6 år m.v.), kan det pålægges teleudbydere m.v. at logge data omfattet af logningsbekendtgørelsen i en periode på eks. 6 eller 12 måneder. Kravene for udlevering og politiets adgang til de loggede oplysninger vil imidlertid ikke ændre sig. Politiet skal dermed stadig opfylde kravene i Retsplejelovens kapitel 71 om indgreb i meddelelshemmeligheden og kapitel 74 om edition, herunder om forbrydelsens alvorlighed, mistanke, krav om retskendelse mv, før politiet kan få adgang til de loggede data.⁶⁶ I det omfang politiet ikke indhenter de loggede data på baggrund af en retskendelse mv. indenfor 6-12 måneder, slettes data, med mindre politiet anmoder om forlængelse af perioden med yderligere 6-12 måneder, hvilket selvsagt vil kræve, at den rimelige formodning stadig består på tidspunktet for fornyelse. Den rimelige formodning må ikke alene bygge på personers deltagelse i politiske aktiviteter, medlemskab af lovlige foreninger eller partier eller deltagelse i den offentlige debat, ligesom religiøs overbevisning, etnicitet eller herkomst heller ikke kan danne baggrund for en rimelig formodning. Det bør også overvejes at give Datatilsynet og Tilsynet med Efterretningstjenesterne eksplicit hjemmel til at foretage legalitetskontrol med den logning, der foretages, på baggrund af "rimelig formodning", ligesom Justitsministeriet årligt bør udfærdige en rapport, der indeholder detaljeret statistik vedrørende anvendelsen af logningsreglerne. Endeligt bør den, der har været genstand for logning, som hovedregel underrettes, såfremt politiet ved udløbet af 6-12 måneders perioden (eller evt. forlængelse deraf) ikke har fået udleveret disse data på baggrund af reglerne i retsplejeloven. En sådan ordning vil også kræve nogle ændringer i udbudsbekendtgørelsen og teleloven, der omfatter visse af de samme data som logningsbekendtgørelsen, jf. e-datadirektivet (2002/58) art. 6, stk. 2 (som implementeret i udbudsbekendtgørelsen (nr. 715/2011) § 23, og som politiet jf. reglerne i retsplejeloven kan få adgang til). Dog skal det understreges, at EMDs praksis tillader lagring af persondata til brug for teleselskabers bogførings- og debiteringshensyn, hvorfor der vil være videre adgang til at bibeholde denne ordning end den, der følger af logningsbekendtgørelsen, og som alene er oprettet og anvendes med henblik på politi- og efterforskningsmæssig virksomhed.⁶⁷

⁶⁶ Det skal bemærkes, at visse oplysninger som registres i henhold til logningsbekendtgørelsen kan indhentes alene efter reglerne om edition.

⁶⁷ P.G. & J.H. v UK dom af 25. september 2001 para. 42



En ordning som foreslået ovenfor vil drastisk formindske omfanget af logning af persondata således, at de ikke omfatter almindelige borgere, men alene personer, der på baggrund af en rimelig formodning om involvering i alvorlige strafbare forhold, er kommet i politiets søgelys. Ordningen vil særligt være relevant i forhold til personer, som er blevet radikaliseret og færdes i ekstremistiske miljøer, men hvor der (endnu) ikke foreligger en konkret mistanke om eksempelvis terrorplaner eller lignende. Også personer, der er medlemmer af eller færdes i rockerbander eller grupper, der er kendt for at begå organiseret kriminalitet, men ikke er omfattet af en konkret mistanke, ville kunne omfattes af ordningen. Hvis der opstår en mistanke mod de pågældende personer, og de øvrige betingelser i Retsplejelovens Kapitel 71 er opfyldt, vil politi og efterretningstjeneste dermed kunne få bagudrettet adgang til data, der er logget om de pågældende personer. Omvendt må det anerkendes, at politiet vil miste et væsentligt værktøj i mere almindelige straffesager, herunder drabssager, hvor der ikke har været nogen formodning om, at en mistænkt ville begå alvorlig kriminalitet, da den pågældendes persondata ikke vil være logget og dermed ikke tilgængelig for politiet. Det må forventes, at en sådan ordning ville reducere omfanget af personer, hvis data logges fra millioner til hundreder eller tusinder, og de loggede data fra milliarder til tusinder eller titusinder, hvilket selvagt også vil reducere risikoen for misbrug. Selvom betingelserne for logning indsnævres kraftigt, vil de eksisterende retssikkerhedsmæssige garantier dog stadig gælde, hvorfor det alene er alvorlig kriminalitet, der er relevant for logning, ligesom udlevering af data vil kræve mistanke og retskendelse udstedt af uafhængige domstole. Med en sådan ordning vil de danske logningsregler langt bedre afspejle de afgrænsningskrav, der lægges vægt på af både EU-Domstolen og EMD som led i den samlede proportionalitetsvurdering.

Mere overordnet vil en sådan ny og mere afgrænset ordning også markere, at Danmark tager de retssikkerhedsmæssige udfordringer som den teknologiske udvikling skaber alvorligt og, at der sættes hegnsplade for, i hvilket omfang man vil tillade, at ny teknologi giver myndigheder adgang til at gribe ind i borgernes grundlæggende ret til respekt for privatliv. En sådan markering er nødvendig, eftersom der forud for afgørelsen i *Digital Rights* har været seriøse forslag fra ministerielle ekspertgrupper om at udvide snarere end at begrænse logningsreglerne og anden digital overvågning, i form af krav om bl.a. valideret brugeradgang til offentlige hotspots.⁶⁸ Et nyt udkast til lovforslag fra Beskæftigelsesministeriet lægger op til at give

⁶⁸ Politiken 23. juni 2011



Arbejdstilsynet adgang til oplysninger fra indkomstregisteret med henblik på at bekæmpe social dumping.⁶⁹ SKAT har ved flere lejligheder anmodet teleselskaber om teledata med henvisning til Skattekontrollovens § 8D, der ikke kræver mistanke eller retskendelse, ligesom de data, der er omfattet af logningsreglerne ville være et attraktivt redskab for kommuner i indsatsen mod socialt bedrageri, ved eks. at få informationer om mastedata, der vil kunne sandsynliggøre, at en person reelt opholder sig på en anden adresse end den, vedkommende har oplyst i folkeregisteret. Det må også forventes, at regler, der tillader automatisk lagring af data, vil give myndigheder et konstant stigende informationsniveau om borgernes privatsfære i takt med, at de redskaber, vi anvender, efterlader sig digitale spor. Uden grænser for automatisk indsamling af sådanne spor vil vi potentielt kunne ende i en situation, hvor offentlige myndigheder vil kunne lagre og få adgang til størstedelen af de aktiviteter, et menneske foretager sig.

10. Konklusion

Den 8. april 2014 afsagde EU Domstolen en afgørelse, der erklærede EU's logningsdirektiv for uforeneligt med netop beskyttelsen af privatlivets fred og persondata i Charteret. Justitsministeriet har i et notat om dommen konkluderet, at den danske logningsordning ikke er i strid med Charteret. Det må dog anses for tvivlsomt, om, Justitsministeriets konklusion lægger tilstrækkelig vægt på det forhold, at de danske logningsregler, og den deraf følgende lagring af persondata, griber ind i alle danske borgeres privatliv uden krav om mistanke eller lignende. Netop dette forhold, hvilket var af afgørende betydning i EU-domstolens dom, samt i en række relevante afgørelser fra EMD. På den baggrund konkluderes det, at der er stærke holdepunkter for at antage, at de danske logningsregler ikke er forenelige med Charteret og EMRK. Det anbefales derfor, at der foretages yderligere ændringer af bl.a. logningsbekendtgørelsen således, at der alene kan foretages logning af persondata vedrørende konkrete personer, som, politiet har en rimelig formodning om, er involveret i alvorlig kriminalitet, og at de loggede data derefter alene kan udleveres i henhold til reglerne i Retsplejeloven.

⁶⁹ Forslag til lov om ændring af lov om arbejdsmiljø og lov om ansvaret for og styringen af den aktive beskæftigelsesindsats af 12. august 2014. Tilgængelig her: <http://prodstoragehoeringspo.blob.core.windows.net/d42f5590-3795-4895-b618-c750f774a579/Udkast%20til%20lovforslag%20om%20C3%A6ndring%20af%20AML,%20ekstern%20h%C3%B8ring,%2012.%20aug.%202014.pdf>, sidst besøgt 24. august 2014.



Skrevet af
Jacob Mchangama
d. 4. september 2014