IT-Politisk Forening
Jesper Lund
jesper@itpol.dk

29. april 2021

Bemærkninger til Justitsministeriets lovskitse for revision af logningsreglerne

IT-Politisk Forening har følgende bemærkninger til Justitsministeriets lovskitse for revision af logningsreglerne af 23. marts 2021 (Dok. 1899781, Sagsnr. 2020-187-0036).

Logning for at beskytte den national sikkerhed

1. I C-511/18 og C-512/18, La Quadrature du Net m.fl. og C-520/18, Ordre des barreaux francophones et germanophone m.fl. (”LQDN-dommen”) fastslår EU-Domstolen, at EU-retten ikke er til hinder for en generel og udifferentieret lagringspligt for trafik- og lokaliseringsdata med henblik på beskyttelse af den nationale sikkerhed i de situationer, hvor den pågældende medlemsstat står over for en alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig (præmis 137).

   Et påbud om en sådan lagring må ikke have systematisk karakter. Påbuddet skal tidsmæssigt være begrænset til det strengt nødvendige (med mulighed for forlængelse), og det skal være underlagt strenge garantier, som beskytter de berørte personer mod risikoen for misbrug af deres personoplysninger (præmis 138). Det er væsentligt, at et påbud (afgørelse) om lagring kan gøres genstand for en effektiv prøvelse ved en domstol eller en uafhængig administrativ myndighed, der træffer bindende afgørelse med henblik på at kontrollere, om der foreligger en alvorlig trussel mod den nationale sikkerhed, samt om de retsgarantier, der skal være fastsat ved lov, er overholdt (præmis 139).

2. På baggrund af LQDN-dommen beskriver lovskitsen en ordning for generel og udifferentieret logning til national sikkerhed, hvor Justitsministeren kan fastsætte en logningspligt for teleudbydere for en periode op til et år. Lovskitsen beskriver en vurdering af om der foreligger en alvorlig trussel mod den nationale sikkerhed, som tager udgangspunkt i offentligt tilgængelige analyser fra Center for Terroranalyse (CTA). Ved domstolsprøvelsen er det alene Justitsministeriets vurdering og de offentligt tilgængelige oplysninger fra CTA, som kan gøres genstand for en prøvelse. Justitsministeriet vurderer, at de nuværende sektorspecifikke databeskyttelsesregler for teleudbydere yder en tilstrækkelig beskyttelse mod misbrug.

3. Det er IT-Politisk Forenings klare opfattelse, at et påbud om generel og udifferentieret logning skal være baseret på **konkrete efterretninger** (omstændigheder), som gør det muligt at antage, at der foreligger en alvorlig trussel mod den nationale sikkerhed. Trusselsvurderingerne fra CTA er først og fremmest generelle. CTA har således siden 2014 vurderet, at terrortruslen er alvorlig, hvilket er defineret som ”kapacitet, hensigt og planlægning” til terror. **Hvis en CTA terrortrusselvurdering på niveauet ”alvorlig” er tilstrækkelig til at igangsætte generel og udifferentieret logning, vil denne logning**

hurtigt få en systematisk karakter. Hvis den af Justitsministeriet skitserede ordning var blevet indført efter den første logningsdom i 2014, ville Danmark have haft generel og udifferentieret logning til beskyttelse af den nationale sikkerhed i hele perioden 2014-2021 (fordi CTA terrortrusselsvurderingen har været "alvorlig" siden 2014).

4. Når EU-Domstolen tillader generel og udifferentieret logning skyldes det, at **beskyttelse** af den nationale sikkerhed mod alvorlige trusler er et mere tungtvejende hensyn end bekæmpelse af (grov) kriminalitet.[1] Den tidsmæssige udstrækning af påbuddet om logning og opbevaringsperioden for de lagrede oplysninger[2] bør derfor tage hensyn til, at formålet primært har et fremadrettet fokus med **forebyggelse af konkrete trusler, hvilket bør tale for væsentligt kortere opbevaringsperioder end ved efterforskning af kriminalitet.**

   På den baggrund vil IT-Politisk Forening anbefale, at eventuelle påbud om logning af hensyn til den nationale sikkerhed **kun kan fastsættes for en kortere periode end et år, eksempelvis op til en måned.** Hvis den alvorlige trussel fortsat består, vil der være mulighed for at forlænge påbuddet, herunder med en ny domstolsprøvelse af, om den konkrete alvorlige trussel fortsat består.

5. Ifølge præmis 139 i LQDN-dommen skal en uafhængig domstol "kontrollere, om en af disse situationer foreligger, samt om de betingelser og garantier, der skal være fastsat, er overholdt". Det må nødvendigvis omfatte en reel kontrol af **grundlaget for afgørelsen** om at udstede et påbud om generel og udifferentieret logning.

6. Påbuddet om logning skal gøres genstand for prøvelse af en domstol eller en uafhængig administrativ myndighed. Det behøver ikke at være de almindelige danske domstole, men kunne være et særligt kontrolorgan på det efterretningsmæssige område. Det afgørende er at denne myndighed kan udøve kontrollen af påbud om logning i fuldstændig uafhængighed af regeringen, og at kontrollen får et reelt indhold (herunder en uafhængig vurdering af, om der foreligger en ekstraordinær situation, som berettiger dette meget vidtgående indgreb).

7. Det er efter IT-Politisk Forenings opfattelse nødvendigt med særlige sikkerhedsforanstaltninger og retsgarantier for at beskytte de berørte personer (hele befolkningen) mod risikoen for misbrug. De omtalte sektorspecifikke databeskyttelsesregler i fodnote 7 i lovskitsen er baseret på e-databeskyttelsesdirektivet 2002/58/EF, og tager ikke i tilstrækkeligt grad højde for den potentielt store mængde oplysninger, som kan blive opbevaret i henhold til et påbud om logning af hensyn til den nationale sikkerhed. EU-Domstolen har i tidligere domme fremhævet nødvendigheden af særlige sikkerhedsforanstaltninger i forbindelse med krav om logning.[3]

---

1 LQDN-dommen præmis 136

2 Lovskitsen omtaler ikke direkte opbevaringsperioden i forbindelse med logning til national sikkerhed (IT-Politisk Forening antager at "op til et år" refererer til påbuddets tidsmæssige udstrækning). Ved et enkeltstående påbud om logning til national sikkerhed vil opbevaringsperioden i sagens natur svare til perioden for påbuddets virkning. Hvis et påbud senere forlænges, vil det være nødvendigt at fastsætte en slettefrist for oplysninger som allerede er lagret efter påbuddet. I modsat fald kan opbevaringsperioden komme til at overstige et år eller en anden fastsat øvre grænse for opbevaringsperioden.

3 Præmis 122 i Tele2-dommen (forenede sager C-203/15 og C-698/15) og præmis 66-68 i Digital Rights Ireland dommen (forenede sager C-293/12 og C-594/12). I de nævnte sager er der tale om udbydere, som i forvejen er underlagt krav om databeskyttelse, herunder behandlingssikkerhed, i e-databeskyttelsesdirektivet. Det må betyde, at kravene i e-databeskyttelsesdirektivet ikke er tilstrækkelige, når der i national lovgivning fastsættes krav om logning. EU-Domstolen stiller eksempelvis i Tele2-dommen krav om, at de loggede oplysninger skal opbevares inden for EU. Det krav følger ikke af e-databeskyttelsesdirektivet.

Adgang til oplysninger lagret med henblik på beskyttelse af den nationale sikkerhed

8. Ifølge Tele2-dommen (forenede sager C-203/15 og C-698/15) af 21. december 2016 er EU-retten til hinder for en generel og udifferentieret lagringspligt af samtlige trafik- og lokaliseringsdata vedrørende samtlige abonnenter med henblik på bekæmpelse kriminalitet. Dette gentages i LQDN-dommen med præmis 141-142. Når EU-Domstolen med LQDN-dommen i ekstraordinære situationer tillader generel og udifferentieret logning med henblik på at beskytte den nationale sikkerhed mod alvorlige trusler, må det være underforstået at logning til national sikkerhed skal holdes adskilt fra logning til kriminalitetsbekæmpelse. **I modsat fald vil den beskyttelse af grundlæggende rettigheder, som Tele2-dommen sikrer, blive undergravet. En formålsbegrænsning for en lagringspligt har kun en reel virkning, hvis myndighedernes adgang til de lagrede oplysninger er underlagt den samme formålsbegrænsning.**

9. EU-Domstolen kræver i præmis 138 af LQDN-dommen, at lagring af data til beskyttelse af national sikkerhed skal "være omfattet af begrænsninger og underlagt strenge garantier, der gør det muligt effektivt at beskytte de berørte personers personoplysninger mod risikoen for misbrug." Efter IT-Politisk Forenings opfattelse må risikoen for misbrug omfatte behandling af de lagrede oplysninger til andre formål end national sikkerhed, idet national sikkerhed er det eneste formål som kan begrunde en generel og udifferentieret lagringspligt.

10. I præmis 166 af LQDN-dommen udtaler EU-Domstolen specifikt, at adgangen til lagrede oplysninger kun kan begrundes i det mål almen interesse, som har givet anledning til lagringspligten, eller et mere tungtvejende hensyn. Denne formålsbegrænsning for adgangen i forhold til formålet med lagringen gentages i præmis 31 i dommen af 2. marts 2021 i sagen Prokuratuur C-746/18.

11. Lovskitsen omtaler præmis 166 i LQDN-dommen og præmis 31 i Prokuratuur-dommen som argumenter for ("på den ene side"), at der i sager om grov kriminalitet ikke kan gives adgang til oplysninger, som er pligtmæssigt lagret med henblik på beskyttelse af alvorlige trusler mod den national sikkerhed. Derefter anføres præmis 33 i Prokuratuur-dommen som argument for at der godt kan gives adgang ("på den anden side").

    Ud fra disse overvejelser vurderer Justitsministeriet, at LQDN-dommen ikke er til hinder for at politiet i sager om grov kriminalitet kan få adgang til oplysninger, som er lagret med henblik på at beskytte den nationale sikkerhed. Lovskitsen omtaler dog på side 66 en **væsentlig procesrisiko** ved denne fortolkning i lyset af præmis 166 i LQDN-dommen.

12. Efter IT-Politisk Forenings læsning af LQDN-dommen er præmis 166 formuleret som en streng formålsbegrænsning mellem lagring og den efterfølgende adgang. Der er en klar distinktion mellem national sikkerhed og bekæmpelse af grov kriminalitet, som er særlig vigtigt når kun førstnævnte formål giver mulighed for at fastsætte en generel og udifferentieret lagringspligt.

    Præmis 33 i Prokuratuur-dommen forholder sig alene til kriminalitetsbekæmpelse, og det sker konkret i forhold til en sag, hvor det estiske politi fik adgang til lagrede trafik- og lokaliseringsdata uden at der var tale om grov kriminalitet. Præmis 33 gentager EU-Domstolens retspraksis, om at der i forhold til bekæmpelse af ikke-grov kriminalitet slet ikke kan fastsættes en lagringspligt for trafik- og lokaliseringsoplysninger, hverken målrettet eller generel og udifferentieret. Det må endvidere skulle læses i sammenhæng med

præmis 29, hvor EU-Domstolen udtaler at ”en sådan adgang kun kan gives, for så vidt som disse data er blevet lagret af disse udbydere på en måde, der er i overensstemmelse med den nævnte artikel 15, stk. 1” [i e-databeskyttelsesdirektivet]. I det estiske sag er både lagringen og den efterfølgende adgang i strid med EU-retten, fordi lagringspligten er generel og udifferentieret til kriminalitetsbekæmpelse, og den estiske lovgivning tillader adgang til lagrede trafik- og lokaliseringsdata i sager om ikke-grov kriminalitet.

Udvidelser af omfanget af logningspligten (datatyper)

13. Lovskitsen beskriver flere udvidelser af den nuværende logning for så vidt angår de datatyper som skal logges. Det gælder både for den generelle og udifferentierede logning til national sikkerhed og den målrettede logning til kriminalitetsbekæmpelse.

14. På side 32 omtales logning af lokaliseringsdata for ikke-aktive mobiltelefoner. Hertil skal IT-Politisk Forening bemærke, at en sådan kontinuerlig registrering af mastetilknytninger, uanset om en mobiltelefon aktivt benyttes eller ej, vil føre til en meget detaljeret registrering for de berørte personer. **Der vil reelt være tale om en fuldstændig kortlægning af deres bevægelsesmønstre, permanente og midlertidige opholdssteder, samt hvilke sociale miljøer de berørte personer frekventer.**[4] Hvis det sker i forbindelse med logning til beskyttelse af den nationale sikkerhed vil den berørte personkreds være hele befolkningen.

15. På side 33 omtales ”nyere kommunikationsformer” som en anden mulig udvidelse af omfanget af logningspligten. Det er uklart for IT-Politisk Forening, om dette refererer til teletjenester som VoLTE (Voice over LTE) og VoWiFi (Voice over WiFi), eller andre nyere kommunikationsformer (eventuelt kommunikationstjenester fra andre udbydere end teleselskaber). IT-Politisk Forening vil vende tilbage med bemærkninger, når Justitsministeriets overvejelser på dette punkt bliver beskrevet mere konkret.

16. På side 51 omtales registrering af MAC-adresser på de computere, telefoner og tablets som ”brugeren ejer og anvender”. Konteksten er registrering af oplysninger vedr. civil identitet, som er en datatype hvor LQDN-dommen tillader en generel og udifferentieret lagringspligt til bekæmpelse af alle kriminelle forhold.

    Det er uklart for IT-Politisk Forening hvordan denne registrering skal finde sted, idet MAC-adresser på computere m.v. ikke nødvendigvis er oplysninger som behandles i udbyderens net.[5] I tilfælde hvor udbyderen behandler brugerens MAC-adresse i sit net og har teknisk mulighed for at foretage en registrering, **kan der efter omstændighederne være tale om en registrering, som kan sidestilles med registrering af dynamiske IP-adresser for at spore kilden til en kommunikation på internettet.** Det falder uden for rammerne af logning af oplysningerne om civil identitet, idet en sådan pligtmæssig lagring alene kan finde sted hvis formålet er bekæmpelse af grov kriminalitet.

Generel logning af IP-adresser og adgang til de lagrede oplysninger

17. Lovskitsen beskriver en generel og udifferentieret logning af IP-adresser med en opbevaringsperiode på et år. Det svarer til § 5, stk. 1 i den nuværende

4 Følsomme personoplysninger som politiske og religiøse præferencer vil i mange tilfælde kunne udledes af en sådan kortlægning af bevægelsesmønstre via lagring af lokaliseringsdata for inaktive mobiltelefoner.

5 IT-Politisk Forening vil gerne uddybe disse tekniske detaljer over for Justitsministeriet.

logningsbekendtgørelse. Derudover beskrives en logning af de portnumre, som anvendes af brugeren ved adgang til internettet (”source port number”). IT-Politisk Forening antager, at denne registrering kun skal ske i de tilfælde (CG-NAT), hvor flere abonnenter kan bruge en IPv4-adresse på samme tid.[6]

18. LQDN-dommen tillader generel og udifferentieret registrering af tildelte IP-adresser til bekæmpelse af grov kriminalitet (præmis 155). Det forudsætter dog en streng overholdelse af de materielle og processuelle betingelser, som skal gælde for brugen af disse data. EU-Domstolen begrunder denne undtagelse fra hovedreglen om, at der ikke kan ske generel og udifferentieret logning af trafik- og lokaliseringsdata til kriminalitetsbekæmpelse med, at den tildelte IP-adresse er mindre følsom end andre former for trafikdata (præmis 152).

19. Den tildelte IP-adresse kan ikke i sig selv afsløre hvilke internetsteder, som abonnenten har frekventeret, eller hvilke personer der er kommunikeret med. Det samme gør sig i princippet gældende for registrering af portnumre. Efter IT-Politisk Forenings opfattelse er registrering af portnumre ved CG-NAT dog mere betænkelig, fordi hyppigheden af registreringer af portnumre i visse situationer kan tegne et præcist billede af abonnentens vaner og adfærdsmønstre for så vidt angår brugen af internettet og eventuelt ophold i hjemmet, når der er tale om registrering for faste internetforbindelser.[7]

20. IT-Politisk Forening er bekendt med at visse internetudbydere, herunder de fire mobiloperatører, på frivillig basis udfører en registrering af portnumre. I en række tilfælde bliver registrerede oplysninger om portnumre imidlertid ikke brugt, fordi politiet ikke har et portnummer fra den anden ende af kommunikationen (eksempelvis den besøgte webserver eller den anvendte webmail-tjeneste).

    Af hensyn til proportionaliteten af den ret omfattende registrering (baseret på antal dataposter om den enkelte abonnent), og ikke mindst risikoen for at der kan blive registreret oplysninger om abonnentens adfærdsvaner i privatlivet (jf. punkt 19 ovenfor), vil IT-Politisk Forening opfordre til, at Justitsministeriet inden fremsættelse af lovforslaget undersøger i hvilket omfang politiet har været i stand til at udnytte registrerede portnumre hos de udbydere, som gør dette på frivillig basis.

21. Lovligheden af en generel og udifferentieret lagring af IP-adresser er som nævnt i punkt 18 ovenfor betinget af, at der er fastsat materielle og processuelle betingelser for brugen af disse oplysninger. Disse betingelser skal for det første begrænse adgangen til sager om grov kriminalitet, og derudover skal den uafhængige domstolskontrol sikre, at det i den konkrete sag er proportionalt at pålægge internetudbyderen at udlevere oplysninger om brugerens identitet.[8]

22. Som EU-Domstolen anfører i præmis 155 i LQDN-dommen har internetbrugerne en forventning om, at deres identitet ikke afsløres når de søger information på internettet. Den Europæiske Menneskerettighedsdomstol (EMD) henviser ligeledes til forventningen om ”anonymitet” online som en vigtig faktor i præmis 117 i dommen af 24. april 2018 i sagen

6 Carrier-Grade Network Address Translation (NAT) som i dag anvendes af en del internetudbydere på grund af manglen på IPv4-adresser.

7 Der er betydelige lighedspunkter med højfrekvent registrering af elforbrug via ”smarte” el-målere, som ligeledes kan afsløre en persons adfærdsmønstre i hjemmet.

8 De nuværende retsregler for udlevering af oplysninger om en internetbrugers identitet (retsplejelovens § 804) indeholder ikke denne proportionalitetsvurdering. Derudover er adgangen ikke begrænset til sager om grov kriminalitet.

Benedik v. Slovenia, sagnr. 62357/14, i overensstemmelse med tidligere EMD retspraksis.

Proportionalitetsvurderingen vedr. afsløring af en internetbrugers identitet bør derfor altid inddrage en vurdering af den kontekst (kommunikation på internettet), som er den konkrete årsag til at politiet ønsker internetbrugerens identitet oplyst.[9]

Målrettet logning

23. I Tele2-dommen og gentaget i LQDN-dommen fastslår EU-Domstolen, at EU-retten ikke er til hinder for en målrettet logningspligt af trafik- og lokaliseringsdata med henblik på bekæmpelse af grov kriminalitet. EU-Domstolen anfører, at denne målretning kan ske ud objektive kriterier om personkredsens forbindelse, i det mindste indirekte, til grov kriminalitet[10] samt geografiske områder, hvor der er en forhøjet risiko for at grov kriminalitet bliver planlagt eller begået.[11]

24. Lovskitsen beskriver på denne baggrund (side 30-34) en ordning for målrettet logning, hvor der er fire kategorier af personer med mulig direkte eller indirekte forbindelse til grov kriminalitet, samt en række geografiske områder hvor der er formodning om forhøjet kriminalitet, enten ud fra områdets karakter (for eksempel infrastruktursteder der besøges af et stort antal personer) eller baseret på statistikker om lovovertrædelser fra politiets sagsbehandlingssystemer.

25. Justitsministeriet anfører på side 30 i lovskitsen, at EU-Domstolen har fastsat en forholdsvis lav tærskel, jf. anvendelse af begrebet ”kan afsløre en forbindelse”, for kravet til grundlaget for, at der kan iværksættes en personbestemt målrettet logning.

26. IT-Politisk Forening er ikke nødvendigvis uenig i denne vurdering, men det er samtidigt vigtigt at være opmærksom på, at den målrettede logning skal have karakter af undtagelsen fra hovedreglen om, at der ikke sker lagring af trafik- og lokaliseringsdata. Det sætter en naturlig begrænsning på hvor mange personer, der kan være omfattet af en personbestemt målrettet logning, og hvor store geografiske områder der kan indgå i den målrettede logning ud fra geografiske kriterier.

27. I forhold til målrettet logning ud fra geografiske kriterier er det vigtigt at være opmærksom på, at mobiltelefoner fra en bestemt lokation (eksempelvis en rockerborg) kan forbinde til en række mobilmaster som ikke nødvendigvis er den nærmeste, og at foreningsmængden af disse master, afhængig af de konkrete geografiske og radiomæssige forhold, kan dække et område med ganske mange personer.[12]

28. Den mulige personkreds med de fire kategorier på side 31 synes at være relativt omfattende, og særligt kategorien ”personer der tidligere har været i kontakt med personer der har været aflyttet” kan omfatte et stort antal personer afhængig af hvordan ”kontakt” defineres (er et enkelt opkald eller SMS tilstrækkeligt, eller kræves der en mere kvalificeret kontakt?). Det

9 Som nævnt tidligere afslører den tildelte IP-adresse ikke i sig selv noget om brugerens kommunikation på internettet. En sådan afsløring finder imidlertid sted, i hvert fald delvist, når politiet anmoder om oplysninger om en brugers identitet ud fra en IP-adresse, fordi denne anmodning altid vil have en direkte forbindelse til en konkret kommunikation på internettet. Det vil være mere indgribende end adgang til oplysninger om en brugers civile identitet uden denne kontekst, selv om der i begge tilfælde er tale om udlevering af abonnementsoplysninger.

10 LQDN-dommen præmis 148.

11 LQDN-dommen præmis 150.

12 Dette forhold vil i høj grad gøre sig gældende for en geografisk logning ved eksempelvis Nørreport Station.

fremgår heller ikke af side 31 hvor længe personer kan befinde sig i de forskellige kategorier.

29. Det er ligeledes uklart for IT-Politisk Forening, om personer i de fire kategorier automatisk udsættes for målrettet logning i en vis periode, eller om de fire kategorier er ment som udgangspunktet for en konkret vurdering af personerne. **Efter IT-Politisk Forenings opfattelse indebærer præmis 149, at der skal foretages en vis konkret vurdering af de personer, som udvælges til målrettet logning.** Kravene til grundlaget for denne vurdering skal naturligvis være lavere end kravene til mistankegrundlaget for at de loggede oplysninger efterfølgende kan udleveres til politiet. En målrettet logning mod en person skal eksempelvis kunne igangsættes på grundlag af efterretningsmæssige vurderinger uden at der nødvendigvis er en efterforskning rettet mod personen.

Retsgarantier for målrettet logning

30. Det er væsentligt at personer som udsættes for målrettet logning har adgang til effektive retsmidler for en domstol, jf. artikel 47 i Charter om Grundlæggende Rettigheder. Det må også gælde for den situation, hvor de målrettet loggede oplysninger ikke bliver udleveret til politiet.[13] Kravet om målrettet logning udgør i sig selv et indgreb i den grundlæggende ret til privatliv og databeskyttelse, jf. Charterets artikel 7 og 8.

31. Efter IT-Politisk Forenings opfattelse forudsætter en reel udøvelse af adgangen til effektive retsmidler for en domstol, at **de berørte personer får underretning om den målrettede logning, når denne underretning ikke længere kan skade en igangværende efterforskning.** EU-Domstolen har fremhævet underretning af de berørte personer som en *de facto* nødvendighed i en række domme, eksempelvis præmis 220 i sagen A-1/15 om EU-Canada PNR-aftalen.[14]

32. For målrettet logning baseret på geografiske kriterier vil IT-Politisk Forening anbefale, at politiet offentliggør de relevante områder på et kort. Afhængig af omstændighederne for den konkrete geografiske målrettede logning kan denne underretning (til offentligheden) udskydes, hvis offentliggørelse kan forstyrre en igangværende efterforskning.

Begrænsning af retten til indsigt hos teleselskaber

33. På side 39 i lovskitsen anføres det:

> *"Forpligtelsen til at holde ovennævnte oplysninger fortrolige vil også kunne omfatte en forpligtelse til at sikre, at den enkelte bruger ikke, f.eks. gennem anmodninger om indsigt i egne oplysninger efter de databeskyttelsesretlige regler – eller på anden vis – kan tilegne sig oplysninger om, hvordan den geografiske og personbestemte målrettede logning på et givet tidspunkt er tilrettelagt."*

13 Justitsministeriets lovskitse omtaler domstolsprøvelse i forbindelse med målrettet logning på side 39, men den skitserede ordning vil alene give mulighed for domstolsprøvelse af proportionalitetskravet, hvis politiet søger at få adgang til de lagrede oplysninger.

14 Fra præmis 220 i A-1/15 der omhandler en analog situation med målrettet lagring af PNR-oplysninger for visse flypassagerer: *"En sådan underretning er nemlig de facto nødvendig for at gøre det muligt for flypassagererne at udøve deres ret til at anmode om indsigt i PNR-oplysninger, der vedrører dem, og til i givet fald at anmode om berigtigelse af disse samt til i overensstemmelse med chartrets artikel 47, stk. 1, at have adgang til effektive retsmidler for en domstol (jf. analogt dom af 21.12.2016, Tele2 Sverige og Watson m.fl., C-203/15 og C-698/15, EU:C:2016:970, præmis 121 og den deri nævnte retspraksis)."*

34. IT-Politisk Forening forstår dette som en overvejelse hos Justitsministeriet om at fastsætte lovbestemte begrænsninger af de registreredes rettigheder, således at en abonnent ikke kan få indsigt i egne oplysninger, jf. GDPR artikel 15, hos en teleudbyder.

35. **Hertil skal IT-Politisk Forening bemærke, at der efter EU-retten ikke kan indføres en fuldstændig begrænsning af retten til indsigt.** Efter EU-Domstolens retspraksis vil en lovgivning, der ikke fastsætter nogen mulighed for den registrerede for at få adgang til adgang til personoplysninger, som vedrører den pågældende, udgøre et indgreb i det væsentlige indhold af den grundlæggende ret til effektiv domstolsbeskyttelse, således som denne er sikret af Charteret artikel 47.[15]

36. Det udelukker ikke, at retten til indsigt kan begrænses midlertidigt af hensyn til forebyggelse, efterforskning, afsløring eller retsforfølgning af strafbare handlinger, jf. GDPR artikel 23, stk. 1, litra d (når en sådan begrænsning respekterer det væsentligste indhold af de grundlæggende rettigheder og frihedsrettigheder og er en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund).

Politiets adgang til lagrede oplysninger hos teleselskaber (kriminalitetsbekæmpelse)

37. Vedrørende spørgsmålet om politiets adgang til oplysninger lagret med henblik på beskyttelse af den nationale sikkerhed har IT-Politisk Forening anført sine bemærkninger under punkt 8-12 ovenfor. Bemærkningerne nedenfor i punkt 38-45 gælder således alene i forhold til adgang begrundet i kriminalitetsbekæmpelse.

38. Indledningsvist skal IT-Politisk Forening bemærke, at det er positivt at Justitsministeriet med lovskitsen (side 69) lægger op til, at der fremover kun kan gives adgang til lagrede trafik- og lokaliseringsdata i sager om grov kriminalitet. Det er ikke tilfældet i dag, hvor politiet kan få adgang til visse trafik- og lokaliseringsdata efter editionsreglerne i retsplejelovens § 804.

39. Spørgsmålet om hvorvidt teleselskaber må videregive trafik- og lokaliseringsdata til politiet er reguleret af e-databeskyttelsesdirektivet, jf. bl.a. præmis 58 i LQDN-dommen.[16] Politiets adgang til lagrede oplysninger skal ske i henhold til en lovgivningsmæssig foranstaltning, der opfylder kravene i artikel 15, stk. 1 i e-databeskyttelsesdirektivet. Det gælder uanset om oplysninger er lagret i henhold til en logningspligt eller af kommercielle årsager, jf. præmis 167 i LQDN-dommen.[17]

40. IT-Politisk Forening vil desuden henvise til, at præmis 115-121 i Tele2-dommen fastsætter en række konkrete krav til lovbestemmelser om udlevering af lagrede trafik- og lokaliseringsdata til politiet. IT-Politisk Forening har i et høringssvar[18] af 18. april 2017

15 Præmis 95 i C-362/14 Schrems.

16 Præmis 58 i LQDN-dommen, sidste sætning: ”*Det samme gør sig gældende for de bestemmelser, der regulerer de nationale myndigheders adgang til og brug af disse data.*” Sagerne C-207/16 Ministerio Fiscal og C-746/18 Prokuratuur omhandler desuden alene spørgsmålet om adgang til lagrede oplysninger, og retsgrundlaget for disse domme er primært e-databeskyttelsesdirektivet.

17 Det er en forudsætning for politiets adgang, at oplysningerne er lagret på en måde, som er i overensstemmelse med artikel 5, 6, 9 (kommercielle årsager) eller artikel 15, stk. 1 (lagringspligt). Herved må skulle forstås, at lagringen skal være lovlig for at oplysningerne lovligt kan udleveres til politiet. Denne fortolkning bekræftes af præmis 29 i Prokuratuur-dommen (”*..at en sådan adgang kun kan gives, for så vidt som disse data er blevet lagret af disse udbydere på en måde, der er i overensstemmelse med den nævnte artikel 15, stk. 1.*”)

18 Høringssvar vedr. L 191 om ændring af revisionsforpligtelse i folketingsåret 2016-17, tilgængelig online her.

givet en indledende vurdering af disse krav (fra Tele2-dommen) i forhold til de nuværende retsregler om adgang til lagrede oplysninger i retsplejelovens kapitel 71 og 74.

41. For trafik- og lokaliseringsdata kan der kun gives adgang for politiet i sager om grov kriminalitet, og adgangen skal ske efter forudgående domstolskontrol undtagen i behørigt begrundede hastende tilfælde. Lovgivningen skal fastsætte materielle og processuelle betingelser, som i hvert enkelt tilfælde sikrer, at adgangen begrænses til hvad der er strengt nødvendigt for den konkrete efterforskning, jf. præmis 38 i Prokuratuur-dommen.

42. Ifølge præmis 119 i Tele2-dommen **kan der som udgangspunkt kun gives adgang til data vedrørende personer, der er mistænkt for at planlægge, ville begå eller have begået en alvorlig lovovertrædelse eller på en eller anden måde være involveret i en sådan lovovertrædelse.** I særlige situationer som terrorsager kan der også gives adgang til andre personers data, hvis der foreligger objektive forhold som gør det mulige at antage, at disse data kan bidrage til bekæmpelsen af en sådan virksomhed. EU-Domstolen gentager dette krav (kun adgang for oplysninger vedr. mistænke personer) i præmis 50 af Prokuratuur-dommen.

43. Retsplejeloven opfylder ikke dette krav på flere punkter. Det gælder dels personkredsen i retsplejelovens § 781, stk. 1, nr. 1,[19] dels muligheden for udvidet teleoplysning i retsplejelovens § 780, stk. 1, nr. 4 (og "mastesug" generelt, uanset om det er efter § 780).

44. **Efter Tele2-dommen præmis 121 skal der ske underretning de berørte personer (hvis oplysninger politiet har fået adgang til), så snart underretningen ikke kan skade politiets efterforskning.** Denne underretning er ifølge EU-Domstolen *de facto* nødvendig for at de berørte personer kan udøve den adgang til retsmidler, som udtrykkeligt er fastsat i artikel 15, stk. 2, i e-databeskyttelsesdirektivet.

45. De nuværende bestemmelser i retsplejeloven om adgang til lagrede trafik- og lokaliseringsdata opfylder ikke kravene om underretning af abonnenten i alle tilfælde. Det gælder enhver adgang som sker i henhold til editionsreglerne (§ 804). Når adgangen sker i henhold til kapitel 71 (teleoplysninger), skal der ifølge § 788 som udgangspunkt gives underretning ved indgrebets afslutning. Mulighederne for at udelade underretning i § 788, stk. 4 synes dog at være mere omfattende end hvad præmis 121 i Tele2-dommen tillader.[20]

Definitionen af "grov kriminalitet" i forbindelse med adgang til lagrede oplysninger

46. Af lovskitsen fremgår det flere steder, at Justitsministeriet vil overveje, om der kan fastsættes et lempeligere kriminalitetskrav for de tilfælde, hvor adgangen til lagrede oplysninger kun kan ske ved efterforskning af grov kriminalitet. Dette begrundes blandt andet i, at logningen fremover bliver mere målrettet.[21]

19 Formuleringen "bestemte grunde til at antage, at der på den pågældende måde gives meddelelser eller foretages forsendelser til eller fra en mistænkt" i § 781, stk. 1, nr. 1 må indebære, at politiet kan få adgang til teleoplysninger vedrørende en person, som alene **modtager meddelelser fra en mistænkt**.

20 Udover udsættelse af underretningen indtil det ikke længere kan skade en igangværende efterforskning, giver retsplejelovens § 788, stk. 4 mulighed for helt at udelade underretningen, hvis hensynet til beskyttelse af fortrolige oplysninger om politiets efterforskningsmetoder eller omstændighederne i øvrigt taler imod underretning.

21 Hvis der er generel og udifferentieret logning til national sikkerhed med mulighed for at politiet kan få adgang i sager om grov kriminalitet (som lovskitsen lægger op til), vil logningen reelt ikke blive "mere målrettet". De oplysninger, som formelt logges målrettet ud fra personkreds og geografiske kriterier, vil i praksis være en delmængde af de oplysninger som i forvejen er logget med henblik på beskyttelse af den nationale sikkerhed (med samme muligheder for adgang i lovskitsen).

47. IT-Politisk Forening undrer sig over disse overvejelser. Både målrettet logning og adgang til lagrede trafik- og lokaliseringsdata udgør et alvorligt indgreb i retten til privatliv og databeskyttelse, idet der er tale om oplysninger som vil kunne gøre det muligt at drage meget præcise slutninger vedrørende privatlivet for de berørte personer, såsom vaner i dagligdagen, midlertidige eller varige opholdssteder, daglige eller andre rejser, hvilke aktiviteter der udøves, disse personers sociale relationer og de sociale miljøer, de frekventerer.[22]

48. Det alvorlige indgreb, som politiets adgang til disse følsomme oplysninger udgør, bliver ikke mindre af, at der eventuelt er færre personer, som får alle deres trafik- og lokaliseringsdata lagret (hvis logningspligten bliver mere målrettet), og færre situationer hvor politiet får adgang til lagrede lokaliseringsoplysninger (hvis dette kun kan ske i sager om grov kriminalitet).

49. IT-Politisk Forening mener tværtimod, at der er grund til at foretage en kritisk vurdering af den nuværende afgræsning af grov kriminalitet i forhold til adgangen til lagrede teleoplysninger (retsplejelovens § 781). Hovedreglen om en strafferamme på 6 år er suppleret af en katalogliste med række forbrydelser med lavere strafferamme. For nogle af disse er en klassificering som "grov kriminalitet" givetvis passende, men der findes også kriminalitetstyper, hvor det primære fællestræk synes at være, at der ofte er flere gerningspersoner som kommunikerer med hinanden.

50. På side 12 i "Notat af 2. juni 2014 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" anføres dette af Justitsministeriet:

> "*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 forhold at flere gerningspersoner kommunikerer med hinanden, og at adgang til lagrede trafik- og lokaliseringsdata derfor kan være et relevant efterforskningsmiddel for politiet, er ikke et element som bør indgå i en afgrænsning af hvad der er grov kriminalitet.

Registrering af taletidskort

51. Ifølge lovskitsen (side 55) vil Justitsministeriet fremsætte et lovforslag om, at der ved salg af taletidskort fremadrettet skal ske registrering af oplysninger om køberens identitet. Det fremgår ikke hvilke oplysninger der skal registreres, og i hvilket omfang de eventuelt skal dokumenteres eller verificeres af teleudbyderen eller salgsstedet for salg af taletidskort.

52. En arbejdsgruppe under Justitsministeriet har arbejdet med overvejelser om dette siden 2006 uden at tidligere justitsministre har fundet anledning til at indføre en sådan

22 Jf. Tele2-dommen præmis 99.

registrering af køberne af taletidskort. Ved Justitsministeriets møderække med civilsamfundsorganisationer i oktober-november 2016 om revision af logningsreglerne blev det bekræftet, at der ikke (i 2016) var planer om registrering af taletidskort. Ikke mindst i lyset af den teknologiske udvikling og de nuværende mere "grænseoverskridende" markedsforhold på telemarkedet (jf. punkterne nedenfor) undrer det derfor IT-Politisk Forening, at forslaget om registrering af taletidskort pludseligt kommer i 2021.

53. Da registrering af taletidskort blev overvejet for 15 år siden, var taleopkald og SMS-beskeder via almindelige GSM-telefoner den primære (eller eneste) mulighed for mobil kommunikation mellem personer. Siden 2006 har den teknologiske udvikling flyttet en del af tale- og beskedkommunikationen fra mobiltelefoni til apps på smartphones, hvor teleselskaberne alene ser mobildatatrafik uden at vide hvad denne datatrafik indeholder (hvem der kommunikerer med hvem). Der er sågar et marked for særligt sikre "crypto" telefoner, som kommunikerer indbyrdes via mobildatatrafik, og hvor enhederne kommer med egne SIM-kort, antageligt fra et land hvor der ikke er krav om individuel registrering abonnenter for SIM-kort.[23]

54. Markedsforholdene på telemarkedet har ændret sig betydeligt siden 2006, og muligheden for "free roaming" i EU betyder, at der på danske mobilnet vil befinde sig et væsentligt større antal udenlandske SIM-kort end for 10-15 år siden.

55. Den fremtidige teknologiske udvikling vil formentlig byde på et stort antal IoT-enheder (Internet of Things), som gør brug af mobilnettet til datatrafik (især 5G). Disse enheder vil ofte ikke kunne henføres til en bestemt person, men de vil have mobildatatrafik som i praksis ikke vil kunne skelnes fra smartphones der gør brug af kommunikations apps.

56. Disse forhold vedrørende den teknologiske og markedsmæssige udvikling på mobilmarkedet må føre til den konklusion, at de potentielle fordele for politiet ved en køberregistrering af taletidskort i 2021 er væsentligt mindre end tidligere.

57. For de personer, som bliver berørt af krav om registrering, vil ulemperne imidlertid være de samme som tidligere. Personer som har behov for anonym kommunikation, eksempelvis en whistleblower hos en efterretningstjeneste som vil kontakte en journalist om ulovlig masseovervågning af befolkningen, kan ikke længere bare købe en "burner phone" (en billig GSM-telefon og taletidskort, som smides væk efter et enkelt opkald) for at beskytte sig mod riskoen fra de repressalier, som en sådan afsløre vil kunne medføre.[24]

58. Krav om køberregistrering af taletidskort kan medføre, at nogle personer (eksempelvis særligt udsatte grupper som hjemløse) vil blive afskåret fra at gøre brug af mobiltelefoni, fordi de ikke kan levere den dokumention for deres identitet, som køberregistreringen kræver. En del taletidskort sælges via kiosker, og hvis disse salgssteder fremover skal opbevare kopier af ID-dokumenter eller andre registreringer baseret på fremvisning af ID-dokumenter, **vil der blive skabt nye risici for identitetstyveri.** Online-registrering med NemID er ikke en mulighed for alle, eksempelvis personer som kun opholder sig midlertidigt i Danmark. Det er heller ikke alle fastboende borgere som har NemID.

59. For at opsummere er der betydelige praktiske udfordringer ved en ordning med køberregistrering af taletidskort. **IT-Politisk Forening vil som minimum opfordre til, at**

23 Et eksempel er tjenesten EncroChat, som dog ikke længere eksisterer på dette specialiserede marked.
24 Dette er alene et hypotetisk eksempel. Enhver lighed med virkeligheden er aldeles utilsigtet.

Justitsministeriet foretager en grundig konsekvensanalyse af disse aspekter, herunder en menneskeretlig vurdering af risikoen for at visse udsatte persongrupper kan blive helt afskåret fra at kommunikere med andre mennesker via mobiltelefoni, inden et lovforslag om registrering af taletidskort fremsættes.

60. Sidst men ikke mindst finder IT-Politisk Forening det principielt forkert, at borgerne skal registreres hos staten som betingelse for at de får "lov" til at kommunikere med hinanden, uanset at denne registrering i visse tilfælde måske kun vil indebære beskedne administrative byrder for borgerne.

Indsamling i realtid af trafik- og lokaliseringsdata

61. Ifølge præmis 183-189 i LQDN-dommen indebærer indsamlingen af data i realtid, der gør det muligt at lokalisere et terminaludstyr, et større indgreb end adgang til tilsvarende historiske (lagrede) lokaliseringsdata. Kravene for adgang til data i realtid skal derfor være strengere, fordi der er tale om et større indgreb. Efter IT-Politisk Forenings umiddelbare vurdering kan denne del af LQDN-dommen have konsekvenser for retsplejelovens bestemmelser om teleobservation (§ 791 a, stk. 5, nr. 1), hvor de materielle betingelser for indgrebet ikke synes at afspejle EU-Domstolens vurdering af indgrebets omfang.

62. I lovskitsen omtales denne del af LQDN-dommen alene i fodnote 2 som "en særlig fransk regel vedrørende mulighederne for at få kunne adgang til trafik- og lokaliseringsdata i realtid". Der er imidlertid tale om en generel fortolkning af e-databeskyttelsesdirektivet i lyset af Charteret for så vidt angår myndigheders adgang til trafik- og lokaliseringsdata i realtid.

63. Af tidsmæssige årsager vil IT-Politisk Forening følge op på spørgsmålet om adgang til trafik- og lokaliseringsdata **i realtid** på et senere tidspunkt.