IT-Politisk Forening

Web: www.itpol.dk
Email: bestyrelsen@itpol.dk

25. oktober 2021

Høringssvar vedr. udkast til lovforslag om ændring af retsplejeloven og lov om elektroniske kommunikationsnet og -tjenester (Revision af reglerne om logning), J.nr. 2020-187-0036

Hensigten med lovforslaget er at tilpasse de danske regler om logning og politiets adgang til oplysninger hos teleudbydere m.v. til EU-retten efter en række domme fra EU-Domstolen siden 2014. De nuværende danske retsregler i retsplejelovens § 786, stk. 4 og logningsbekendtgørelsen lever ikke op til EU-rettens krav. Siden januar 2021 har Justitsministeriet ikke anvendt reglerne i logningsbekendtgørelsen over for teleudbyderne, som imidlertid har fortsat logningen på formelt frivillig basis.

De nuværende danske logningsregler fastsætter en generel og udifferentieret logningspligt af alle trafikdata med henblik på kriminalitetsbekæmpelse, hvilket efter EU-retten overskrider grænsen for det strengt nødvendige i et demokratisk samfund.

Lovforslaget medfører ingen reelle ændringer på dette punkt. Den nuværende generelle og udifferentierede logning, som strider mod EU-retten, vil fortsætte. Formelt sker dette med henvisning til national sikkerhed, men logningsordningens reelle indhold er at sikre tilgængelighed af de samme oplysninger som i dag til kriminalitetsbekæmpelse. Dette kritiske element af lovforslaget er forbundet med en **væsentlig procesrisiko** efter Justitsministeriets egen vurdering. De juridiske problemer, som lovforslaget skaber, kan føre til en sagsophobning i straffesagskæden.

Lovforslaget bliver motiveret med at der indføres en målrettet logning, og præsentationen af den målrettede logning til bekæmpelse af grov kriminalitet er første hovedpunkt i lovforslaget (pkt. 3.1) før den generelle og udifferentierede logning med henblik på beskyttelse af den nationale sikkerhed (pkt. 3.2).

Realiteten er imidlertid, at den generelle og udifferentierede logning af alle trafikdata vil fortsætte i den overskuelige fremtid. Den målrettede logning, der skulle udgøre den nødvendige tilpasning til EU-retten, er alene ment som en ”reserve ordning” der kan iværksættes med kort varsel, hvis den generelle og udifferentierede logning ikke kan fortsætte, eksempelvis fordi Justitsministeriet taber en retssag (overgang til målrettet logning af denne grund nævnes direkte i bemærkningernes pkt. 3.6.3.1). Skulle det komme så vidt, vil der formelt ske en overgang til målrettet logning, men ordningen er kun målrettet af navn. Kriterierne for ”målretning” er så omfattende, at mere end

halvdelen af landets befolkning vil være omfattet. Den præsenterede målrettede logning til kriminalitetsbekæmpelse er i virkeligheden mere generel og udifferentieret end den er målrettet.

Forberedelserne til den målrettede logning, der efter planen formentlig aldrig skal bruges (men alene holdes i reserve, hvis den generelle og udifferentierede logning en dag må opgives), vil medføre betydelige udgifter for både staten og teleudbyderne. Der vil være en overhængende risiko for, at disse udgifter er spildte, hvis EU-Domstolen underkender den danske målrettede logning, fordi den er for omfattende.

Logning af IP-adresser tildelt kilden til en brugers adgang til internettet er efter EU-retten tilladt på generelt og udifferentieret basis, men alene hvis det sker med henblik på bekæmpelse af grov kriminalitet. Lovforslaget viderefører imidlertid blot den gældende logning af adgangen til internettet uden at begrænse anvendelsen til sager om grov kriminalitet. Der sker endda en udvidelse af internet-logningens omfang.

En række EU-domme siden 2014 har gjort det nødvendigt for Danmark at ændre retsplejelovens regler om indgreb i meddelelseshemmeligheden (kapitel 71) og især edition (kapitel 74) for så vidt angår politiets adgang til lagrede trafikdata og lokaliseringsdata (”teledata”) hos teleudbyderne. Udlevering af disse oplysninger til politiet udgør generelt et alvorligt indgreb i den grundlæggende ret til privatliv og databeskyttelse, og sådanne alvorlige indgreb skal efter EU-retten være betinget af, at der er tale om grov kriminalitet.

Lovforslaget indeholder et nyt kriminalitetskrav for edition af visse oplysninger, men fordi kriminalitetskravet generelt sænkes, vil politiet ud fra en samlet vurdering få en større adgang til de følsomme oplysninger om borgernes kommunikation med andre personer og deres færden i det fysiske rum. Lovforslagets ændringer af retsplejelovens kapitel 71 og 74 er ikke tilstrækkelige til at bringe dansk ret i overensstemmelse med EU-retten.

Endeligt vil lovforslaget indføre en generelt pligt til registrering og verificering af nummeroplysningsdata, inklusive for taletidskort, hvor dette vil være meget byrdefuldt. Selv om denne registreringspligt påhviler teleudbyderne, kan den få store konsekvenser for udsatte personer i samfundet. I værste fald kan de blive afskåret fra at kommunikere med andre mennesker via telefoni. Lovforslagets bemærkninger ignorerer fuldstændigt disse konsekvenser.

Efter IT-Politisk Forenings opfattelse vil en ”værktøjskasse” til politiet, som består af hastesikring (som § 786 a), en reelt målrettet logning af trafikdata (som § 786 d) og eventuelt en generel og udifferentieret logningspligt for tildelte IP-adresser (som § 786 f, men begrænset til efterforskning af grov kriminalitet), sikre en passende balance mellem hensynet til politiet efterforskningsmuligheder og det alvorlige indgreb i borgernes grundlæggende ret til privatliv, databeskyttelse og ytringsfrihed, jf. artikel 7, 8 og 11 i Charter om Grundlæggende Rettigheder, som er uløseligt forbundet med en logningspligt for teleudbydere.

Disse vurderinger og synspunkter uddybes i det følgende med nummererede afsnit (punkter).

Oversigt over IT-Politisk Forenings høringssvar

Udbydere omfattet lovforslaget

1. Den generelle og udifferentierede logningspligt (de forslåede § 786 e og § 786 f i retsplejeloven) gælder for udbydere af elektroniske kommunikationsnet eller -tjenester som defineret i telelovens § 2, nr. 4 og 7. IT-Politisk Forening antager, at der hermed menes de samme udbydere som er omfattet af § 1 i den nuværende logningsbekendtgørelse, uanset at ordene ”til slutbrugere” alene indgår i § 1 i logningsbekendtgørelsen men ikke i lovforslaget.

2. Pligten til målrettet logning (retsplejelovens §§ 786 b – 786 d) påhviler udbydere, der med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikke-accessorisk del af virksomheden. Det vil være udbydere af mobiltelefoni, fastnettelefoni og internetadgangstjenester (bredbånd), der har dette som deres hovedvirksomhed, jf. pkt. 3.1.3.1 i de almindelige bemærkninger. Denne indskrænkning af udbyderkredsen er begrundet med, at udbydere der skal foretage målrettet logning skal modtage og behandle oplysninger om bl.a. den personkreds, som er omfattet af målrettet logning.

3. Forskellen mellem de to udbyderbegreber vil i praksis være virksomheder der tilbyder midlertidig internetadgang til sine kunder i forbindelse med salg af varer eller tjenester på kommercielt basis, for eksempel WiFi hotspots på hoteller, kursuscentre, campingpladser restauranter, caféer m.v. Disse tjenester har siden 2007 været omfattet af logningsbekendtgørelsen, selvom om det nu annullerede logningsdirektiv kun omfattede offentlige elektroniske kommunikationsnet og -tjenester.

4. IT-Politisk Forening vil anbefale, at logningspligten kun skal gælde for udbydere af elektroniske kommunikationsnet eller -tjenester, der har dette som sin hovedydelse eller som en ikke-accessorisk del af virksomheden (svarende til §§ 786 b – 786 d), uanset om der er tale om generel og udifferentieret logning eller målrettet logning. For de øvrige udbydere (f.eks. et WiFi hotspot på en café) vil slutbrugerforholdet næsten altid have en midlertidig karakter, og det er usandsynligt at der vil blive registreret oplysninger som i praksis kan anvendes i en politimæssig efterforskning. Brugeridentiteten vil typisk være en MAC-adresse, ikke en direkte identificeret person.

5. Hvis internetlogningen i § 786 f udvides til at omfatte source portnumre, vil disse udbydere (hoteller, campingpladser, caféer, m.v.) blive pålagt ganske betydelige økonomiske byrder i forhold til de gældende logningsregler. Det er ikke proportionalt henset til de begrænsede anvendelsesmuligheder af de loggede oplysninger.

Afgrænsning af de logningspligtige oplysninger

6. I lovforslagets almindelige bemærkninger pkt. 3.1.3.4 angives på listeform (nr. 1-9) de trafikdata som er omfattet af logningspligten i retsplejelovens §§ 786 b – 786 d (målrettet logning) og § 786 e (generel og udifferentieret logning). Ifølge de indledende bemærkninger i pkt. 1 er der tale om de samme oplysninger, som i dag er registrerings- og opbevaringspligtige. Det må skulle forstås som oplysninger omfattet af § 4 og § 6 i logningsbekendtgørelsen. For internetadgang vil § 786 f fastsætte omfanget af logningspligten (som i dag er fastsat i § 5 i logningsbekendtgørelsen).

7. IT-Politisk Forening finder det positivt, at de logningspligtige trafikdata fastsættes direkte i lovteksten frem for at det gøres efterfølgende i bekendtgørelsesform (med undtagelse af logningspligten for slutbrugeres adgang til internettet, jf. § 786 f). Logning er et vidtgående indgreb i borgernes grundlæggende ret til bl.a. privatliv og databeskyttelse, og det er derfor vigtigt, at rækkevidden af dette indgreb er afgrænset tilstrækkeligt klart og præcist.

8. Idet det er hensigten, at logningspligten skal omfatte de samme trafikdata som i dag, jf. punkt 6 ovenfor, vil IT-Politisk Forening anbefale at det for listen af trafikdata i pkt. 3.1.3.4 (side 46) præciseres, at nr. 1-7 gælder for fastnet- og mobiltelefoni samt SMS-, EMS- og MMS-kommunikation, svarende til § 4 i den nuværende logningsbekendtgørelse. Det vil skabe konsistens med de efterfølgende bemærkninger i pkt. 3.1.3.4 (side 47) om at lokaliseringsdata, der udgør trafikdata i forbindelse med internetforbrug, fortsat ikke er registrerings- og opbevaringspligtige. På den måde undgås det, at lovforslaget skaber ny uklarhed i forhold til de gældende regler om hvad ”kommunikationens start og afslutning” i nr. 6 omfatter.[1]

9. Det bør også præciseres, at logningspligten kun omfatter oplysninger som genereres eller behandles i udbyderens net, svarende til hvad der fremgår af § 1 i den nuværende logningsbekendtgørelse, medmindre andet eksplicit er fastsat (jf. næste punkt om

1 Der har tidligere været en vis fortolkningstvivl om dette i forhold til § 4 i logningsbekendtgørelsen.

nummeroplysningsdata). I modsat fald kan der være fastsat en logningspligt for oplysninger, som udbyderen ikke har nogen mulighed for at registrere, fordi de ikke er tilgængelige i udbyderens system (end ikke kortvarigt). Denne præcisering vil bl.a. have betydning for pligten til at registrere den forbundne celle ved afsendelse og modtagelse af MMS-beskeder, hvis celler for MMS ikke teknisk kan udskilles fra den øvrige datatrafik.[2]

10. For telefoni-tjenester vil der med lovforslaget blive indført en registreringspligt for slutbrugerens identitet, uanset om udbyderen har et forretningsmæssigt behov for at behandle disse oplysninger, jf. den foreslåede § 786 h i retsplejeloven om registrering og verificering af nummeroplysningsdata. For øvrige tjenester (dvs. internetadgang) antager IT-Politisk Forening, at kun oplysninger som af forretningsmæssige årsager genereres eller behandles i udbyderens systemer er omfattet af logningspligten, ligesom det er tilfældet i dag.[3]

Generel og udifferentieret logning til beskyttelse af den nationale sikkerhed (§ 786 e)

11. Efter den foreslåede § 786 e i retsplejeloven kan Justitsministeren fastsætte regler om generel og udifferentieret logning af trafikdata, når der foreligger tilstrækkeligt konkrete omstændigheder, der giver anledning til at antage, at Danmark står over for en alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig. Den generelle og udifferentierede logningspligt kan fastsættes for en periode på højst 1 år ad gangen. Opbevaringsperioden for de lagrede oplysninger vil være 1 år fra registreringstidspunktet.

12. Det fremgår af de almindelige bemærkninger pkt. 3.2.3.1, at det vil indgå som et væsentligt moment ved vurderingen af om der foreligger en alvorlig trussel mod den nationale sikkerhed, om der er foretaget sigtelser, sket varetægtsfængsling eller rejst tiltale for forhold omfattet af straffelovens kapitel 12 og 13, ligesom domfældelser efter disse bestemmelser i straffeloven vil kunne tillægges betydelig vægt ved vurderingen. Et andet element, som kan indgå i vurderingen er ”Vurderingen af Terrortruslen mod Danmark” (VTD), som årligt udarbejdes af Center for Terroranalyse (CTA).

13. Den seneste (marts 2021) vurdering fra CTA er at terrortrusselsniveauet er ”alvorlig”, hvilket er næsthøjeste niveau på en fem-punkt skala fra ”minimal” til ”meget alvorlig”. CTA har vurderet truslen mod Danmark til at være ”alvorlig” siden 2014. Det anføres i den forbindelse i bemærkningerne, at terrortruslen mod Danmark ikke altid har været ”alvorlig” i CTA’s vurderinger, hvilket nærmest synes at antyde, at terrortruslen skulle have været lavere i midten af 00’erne, hvor der var store terrorbombeangreb i Madrid og London.

---

2 Denne problemstilling er velkendt under de nuværende logningsregler.

3 Udbydere af internetadgangstjenester (bredbånd) vil normalt registrere navn og adresse for abonnenten af hensyn til den løbende fakturering. Derudover leveres internetadgangstjenester typisk til et nettermineringspunkt på en kendt adresse. En café der kortvarigt tilbyder internetadgang til sine kunder vil derimod ikke behandle oplysninger om slutbrugerens navn og adresse, idet der rent teknisk alene er behov for at identificere slutbrugeren med eksempelvis en MAC-adresse i et WiFi hotspot for at overføre trafikken til internettet fra udbyderens net (WiFi hotspot).

14. 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 trafikdata 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).

15. 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 (LQDN-dommens præmis 138). Det er væsentligt, at et påbud (afgørelse) om lagring kan gøres til genstand for en effektiv prøvelse ved en domstol eller en uafhængig administrativ myndighed, der træffer bindende afgørelser, 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).

16. 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.[4] Generel og udifferentieret logning med henblik på bekæmpelse af grov kriminalitet er ikke tilladt efter EU-retten. Den tidsmæssige udstrækning af påbuddet om logning og opbevaringsperioden for de lagrede oplysninger bør derfor tage hensyn til, at **formålet primært har et fremadrettet fokus med forebyggelse af konkrete alvorlige trusler mod den nationale sikkerhed**, hvilket bør tale for væsentligt kortere opbevaringsperioder end ved efterforskning af kriminalitet.

17. På baggrund af præmis 137-139 i LQDN-dommen er det således IT-Politisk Forenings klare opfattelse, at eventuelle påbud om logning af hensyn til den nationale sikkerhed **kun kan fastsættes for en væsentligt kortere periode end et år, eksempelvis op til en måned.** Derudover skal vurderingen være baseret på konkrete efterretninger om en fremtidig alvorlig trussel mod den nationale sikkerhed.

18. Det er ligeledes et krav fra EU-Domstolen side, at den generelle og udifferentierede logning med henblik på beskyttelse af den nationale sikkerhed **ikke må have systematisk karakter.** Formuleringen i præmis 138 ”Selv om det ikke kan udelukkes, at et påbud [..] kan forlænges som følge af, at en sådan trussel fortsat består [..]” må indebære, at forlængelse af påbuddet skal være undtagelsen.

19. Hvis Justitsministeren vil basere vurderingen på momenter som sigtelser, varetægtsfængslinger og tiltalerejsning efter straffelovens kapitel 12 og 13 eller CTA’s vurdering af terrortrusselsniveauet i VTD’en, virker det overvejende sandsynligt, at der ret hurtigt bliver tale om en generel og udifferentieret logning af systematisk karakter. Det er også tvivlsomt om disse momenter kan udgøre ”tilstrækkeligt konkrete omstændigheder” i forhold til en **fremtidig trussel** mod den nationale sikkerhed. Specielt sigtelser,

4 LQDN-dommen præmis 136.

varetægtsfængslinger og tiltalerejsning har en bagudrettet karakter.

20. Ifølge lovforslagets bemærkninger har CTA vurderet terrortruslen til at være alvorlig siden 2014. I realiteten har PET og CTA vurderet terrortruslen mod Danmark til at være alvorlig i noget mere end 7 år. Af VTD'en fra januar 2012 fremgår det eksempelvis, at "CTA vurderer, at der **fortsat er en alvorlig terrortrussel** mod Danmark fra netværk, grupper og enkeltpersoner, der bekender sig til en militant islamistisk ideologi."[5] I forordet til PET's årsberetning for 2006-2007 står der ligefrem følgende: "Som det fremgår af PET's løbende vurderinger af terrortruslen, står Danmark for tiden over for **det alvorligste trusselsbillede i mange år, og terrorangreb kan finde sted uden varsel**."[6] (vores fremhævning).

21. Den i pkt. 3.2.3 beskrevne ordning fremstår i realiteten som en generel og udifferentieret lagringspligt af alle trafikdata uden en reel tidsbegrænsning baseret på generelle vurderinger af terrortrusselsniveauet. Efter lovforslaget vil trafikdata lagret med henblik på beskyttelse af den nationale sikkerhed også kunne anvendes til kriminalitetsbekæmpelse, hvilket kommenteres særskilt nedenfor i punkt 38-46 i dette høringssvar.

22. Den primære funktion af logningsordningen vil således ikke være national sikkerhed, men at sikre tilgængelighed af historiske trafikdata med henblik på kriminalitetsbekæmpelse, svarende til det primære formål med de nuværende logningsregler.

23. Hvis der ikke længere er en alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig, skal der ifølge lovforslaget iværksættes en overgang fra generel og udifferentieret logning til målrettet logning med henblik på bekæmpelse af grov kriminalitet.

24. I denne situation vil der være lagret trafikdata for hele befolkningen (på generel og udifferentieret basis), som ikke længere er nødvendige for formålet om beskyttelse af den nationale sikkerhed. Efter databeskyttelsesrettens grundlæggende princip om opbevaringsbegrænsning skal personoplysninger slettes, når de ikke længere er nødvendige for de formål, hvortil de pågældende personoplysninger behandles.

25. De lagrede trafikdata skal ifølge lovforslaget imidlertid fortsat opbevares indtil 1 år fra registreringstidspunktet med henblik på efterforskning og retsforfølgelse af grov kriminalitet, jf. pkt. 3.2.3.2 (side 60). Det nye formål (bekæmpelse af grov kriminalitet) kan imidlertid ikke begrunde en generel og udifferentieret lagringspligt for alle trafikdata eller opretholdelse af en sådan lagringspligt.

26. Den generelle og udifferentierede lagringspligt med henblik på beskyttelse af den nationale sikkerhed kan umuligt siges at være tidsmæssigt begrænset til det strengt nødvendige (som

5 National Trusselsvurdering, PET/CTA januar 2012 https://pet.dk/Efterretningsafdelingen/CTA/~/media/VTD%20NTV/NTVjanuar201231012012pdf.ashx

6 Politiets Efterretningstjeneste Årsberetning 2006-2007 https://www.pet.dk/~/media/Aarsberetninger/PET_%C3%A5rsberetning_2006_2007.ashx

præmis 138 eksplicit kræver), når lagringen på denne måde kan opretholdes længere end hvad der er nødvendigt for formålet.

27. Der synes heller ikke i den foreslåede § 786 e i retsplejeloven at være fastsat begrænsninger for lagringen af data og strenge garantier, der gør det muligt effektivt at beskytte de berørte personers personoplysninger mod risikoen for misbrug, som det er forudsat i præmis 138 af LQDN-dommen. Fordi generel og udifferentieret logning udgør et særligt alvorligt indgreb i grundlæggende rettigheder, må henvisningen til begrænsninger og garantier i præmis 138 skulle forstås som **yderligere retsgarantier** udover det som gælder for den øvrige logning. Der er ingen sådanne yderligere retsgarantier for logning til beskyttelse af den nationale sikkerhed i lovforslaget.

Domstolskontrol af påbud om logning til beskyttelse af den nationale sikkerhed

28. Efter præmis 139 i LQDN-dommen er det væsentligt, at et påbud (afgørelse) om lagring kan gøres til genstand for en effektiv prøvelse ved en domstol eller en uafhængig administrativ myndighed, der træffer bindende afgørelser 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.

29. IT-Politisk Forening anerkender, at et påbud (afgørelse) om forebyggende lagring af hensyn til beskyttelse af den nationale sikkerhed kan være truffet på grundlag af fortrolige efterretninger. En effektiv prøvelse af afgørelsen, som præmis 139 kræver, må imidlertid forudsætte, at domstolen eller den uafhængige administrative myndighed også har mulighed for at vurdere sådanne fortrolige oplysninger.

30. Kontrollen behøver ikke være henlagt til de almindelige danske domstole. Det kunne også være et særligt kontrolorgan, hvor medlemmerne eksempelvis er udpeget blandt erfarne dommere fra landsretterne med den nødvendige sikkerhedsgodkendelse for at kunne behandle fortrolige efterretninger. 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).

31. På trods af det ret eksplicitte krav i præmis 139 indeholder lovforslaget ingen særlige regler for så vidt angår prøvelse af betingelserne for den generelle og udifferentierede logning. Efter Justitsministeriets opfattelse er den almindelige adgang til domstolsprøvelse, jf. grundlovens § 63, tilstrækkelig.

32. Justitsministeriet anfører i pkt. 3.6.3.1, at anlæggelse af civile søgsmål forudsætter retlig interesse. Hvis IT-Politisk Forening, Foreningen imod Ulovlig Logning eller en anden civilsamfundsorganisation skulle ønske at anfægte Justitsministerens bekendtgørelse[7] om

7 IT-Politisk Forening antager at påbud om generel og udifferentieret logning efter retsplejelovens § 786 e, stk. 1 vil blive udmøntet som bekendtgørelser med en gyldighed på op til et år, jf. § 786 e, stk 2.

generel og udifferentieret logning, kan de altså antageligt imødese en langvarig proces ved domstolene, hvor Justitsministeriet først vil prøve at få sagen afvist med henvisning til manglende retlig interesse.

33. Det fremgår endvidere af bemærkningerne i pkt. 3.6.3.1, at domstolene i det civile søgsmål kun får mulighed for at vurdere uklassificerede dokumenter som VTD'en fra CTA. Eventuelle klassificerede oplysninger, som har indgået i beslutningen om generel og udifferentieret logning, vil ikke blive forelagt domstolene.

34. Den domstolskontrol, som Justitsministeriet beskriver i pkt. 3.6.3.1, kan ikke med nogen rimelighed opfylde EU-Domstolens eksplicitte krav i præmis 139 om en effektiv prøvelse af, om der foreligger en alvorlig trussel mod den nationale sikkerhed som er reel og aktuel eller forudsigelig.

35. Der er mindst to årsager til dette. For det **første** vil domstolen ikke have adgang til alle relevante oplysninger, herunder eventuelle klassificerede efterretninger. For det **andet** vil tidsfaktoren for anlæggelse af civile søgsmål betyde, at der går lang tid fra påbuddet om generel og udifferentieret logning til domstolens efterprøvelse af, om betingelserne er opfyldt. I mange tilfælde vil der først skulle sikres et økonomisk grundlag for overhovedet at kunne føre sagen. Realistisk set vil processen med et sådant civilt søgsmål tage mere end et år, og domstolens afgørelse vil således vedrøre en bekendtgørelse, som ikke længere er gældende, men måske erstattet af en ny bekendtgørelse om generel og udifferentieret logning, potentielt på et andet beslutningsgrundlag.

36. Justitsministeriets forslag vedr. domstolskontrol vil i praksis medføre, at der aldrig kommer en domstolskontrol af de konkrete beslutninger om at iværksætte generel og udifferentieret logning under hensyntagen til en alvorlig trussel mod den nationale sikkerhed, som er reel og aktuel eller forudsigelig.

37. For civilsamfundsorganisationer vil det i øvrigt give mere mening at indsamle økonomiske midler til at anlægge et civilt søgsmål mod Justitsministeriet med påstand om, at **retsplejelovens § 786 e som sådan skal ophæves** eller subsidiært ikke skal anvendes af Justitsministeriet, fordi denne anvendelse vil stride mod EU-retten, eksempelvis på grund af den manglende mulighed for effektiv domstolsprøvelse af grundlaget for et påbud om generel og udifferentieret logning.

Adgang til oplysninger lagret efter § 786 e (national sikkerhed)

38. Efter lovforslaget vil trafikdata fra den generelle og udifferentierede logning til beskyttelse af den nationale sikkerhed også kunne anvendes til politiets efterforskning og retsforfølgelse i sager om grov kriminalitet. De foreslåede § 780 a og § 804 a i retsplejeloven om adgang til lagrede oplysninger henviser samlet til §§ 786 a – 786 e, uden at skelne mellem om oplysningerne er lagret med henblik på bekæmpelse af grov kriminalitet (§§ 786 a – 786 d), hvor kun målrettet logning eller hastesikring tillades, eller national sikkerhed (§ 786 e).

39. 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 trafikdata og lokaliseringsdata vedrørende samtlige abonnenter med henblik på bekæmpelse af kriminalitet. Dette gentages i LQDN-dommen med præmis 141-142.

40. 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.**

41. 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.

42. I præmis 166 af LQDN-dommen udtaler EU-Domstolen specifikt, at adgangen til lagrede oplysninger kun kan begrundes i det mål af 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 ("Prokuratuur-dommen").

43. Lovforslaget 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 den national sikkerhed. Derefter anføres præmis 33 i Prokuratuur-dommen som argument for at der godt kan gives adgang ("på den anden side").

44. 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. Lovforslaget omtaler dog i pkt. 3.7.2 og pkt. 10 (forholdet til EU-retten) en **væsentlig procesrisiko** ved denne fortolkning i lyset af præmis 166 i LQDN-dommen.

45. 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 vigtig når kun førstnævnte formål giver mulighed for at fastsætte en generel og udifferentieret lagringspligt.

46. 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 trafikdata 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 trafikdata 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 trafikdata og lokaliseringsdata i sager om ikke-grov kriminalitet.

Risikoen for sagsophobning i straffesagskæden

47. Hvis Justitsministeriets fortolkning af præmis 166 i LQDN-dommen skal forelægges præjudicielt for EU-Domstolen i forbindelse med en straffesag, kan konsekvensen ifølge lovforslagets bemærkninger være en sagsophobning i straffesagskæden, ligesom det i en periode vil kunne hindre effektiv strafforfølgning af en lang række kriminalitetstyper.

48. Det er IT-Politisk Forenings vurdering, at en præjudiciel forelæggelse for EU-Domstolen om fortolkning af præmis 166 vil ske relativt hurtigt. Når politiet og anklagemyndigheden anmoder om adgang til trafikdata lagret efter retsplejelovens § 786 e i en sag om grov kriminalitet, må det forventes, at den beskikkede advokat for at varetage sin klients interesser vil gøre indsigelse mod dette med henvisning til, at oplysningerne af politiet søges udleveret til et formål, som er uforeneligt med det formål som begrunder den generelle og udifferentierede lagringspligt (national sikkerhed).

49. Når dommeren i lovens bemærkninger direkte kan se, at der efter Justitsministeriets opfattelse er tvivl om fortolkning af EU-retten (præmis 166 i LQDN-dommen) og at Justitsministeriet har anlagt en fortolkning med **væsentlig procesrisiko**, er det forventeligt at dommeren vil forelægge spørgsmålet for EU-Domstolen. Det kan enten ske ved byretten eller ved landsretten efter den beskikkede advokats forventede kære af byrettens afgørelse om at give politiet adgang til oplysningerne.

50. Det skal i den forbindelse bemærkes, at EU-Domstolen inden for de senere år har fået forelagt en række sager, hvor der i straffesagen ved de nationale domstole var opstået tvivl om, hvorvidt de nationale lovbestemmelser om enten selve lagringen eller betingelserne for politiet adgang er forenelige med artikel 15, stk. 1 i e-databeskyttelsesdirektivet 2002/58/EF, som fortolket af EU-Domstolens hastigt voksende retspraksis på dette område.

Målrettet logning (§§ 786 b – 786 d)

51. Lovforslaget indfører med de foreslåede §§ 786 b – 786 d i retsplejeloven en målrettet logningsordning med henblik på bekæmpelse af grov kriminalitet ud fra personbestemte og geografiske kriterier. Den målrettede logning omfatter de samme trafikdata som den

generelle logning, og opbevaringsperioden er 1 år. Det gælder for alle varianter af den målrettede logning.

52. Den målrettede logning vil først blive igangsat, når der ikke længere foretages generel og udifferentieret logning efter § 786 e. Der vil altså aldrig være overlap mellem målrettet og generel logning. Teleselskaberne skal indrette deres systemer, således at der med kort varsel kan foretages en overgang fra generel og udifferentieret logning til målrettet logning.

53. Den målrettede logning er ganske omfattende. Justitsministeriet har oplyst til Dagbladet Information, at den målrettede logning vil omfatte 15-20 procent af Danmarks areal og mere end halvdelen af landets befolkning.[8] Det skyldes, at de geografiske kriterier koncentrerer logningen i større byer, blandt andet som følge af, at den lange liste med sikringskritiske områder i § 786 c, stk. 2 inkluderer alle større indfaldsveje, busterminaler og togstationer (herunder bybaner som S-tog, metro og letbane).

54. Målrettet logning ud fra geografiske kriterier vil omfatte et større område end det område som egentlig er genstand for den målrettede logning. For hvert geografisk område omfattet af målrettet logning skal teleselskaberne udpege de fornødne master, således at det angivne området dækkes fuldstændigt, jf. de almindelige bemærkninger pkt. 3.1.3.4. Afhængig af de konkrete geografiske og radiomæssige forhold vil disse master tilsammen dække et (langt) større område.

55. I Tele2-dommen og gentaget i LQDN-dommen fastslår EU-Domstolen, at EU-retten ikke er til hinder for en målrettet logningspligt af trafikdata og lokaliseringsdata med henblik på bekæmpelse af grov kriminalitet. Den målrettede logning skal imidlertid være begrænset til det strengt nødvendige for så vidt angår kategorierne af data, der skal lagres, de omhandlede kommunikationsmidler, de berørte personer og den fastsatte varighed af lagringen (jf. LQDN-dommens præmis 147 og Tele2-dommens præmis 108).

56. For at sikre, at indgrebet (den specifikke målrettede logning af et område eller en personkreds) er i overensstemmelse med proportionalitetsprincippet, må varigheden af indgrebet ikke overstige hvad der er strengt nødvendigt i forhold til de omstændigheder, som begrunder indgrebet, dog med forbehold af muligheden for at forlænge foranstaltningen (LQDN-dommens præmis 151).

57. For den personbestemte målrettede logning er det IT-Politisk Forenings klare opfattelse, at LQDN-dommens præmis 149 indebærer, at der på grundlag af objektive forhold skal foretages **en konkret vurdering af de personer, som udpeges 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 bør eksempelvis kunne igangsættes på grundlag af efterretningsmæssige vurderinger uden at der nødvendigvis er en efterforskning rettet mod

8 Justitsministeriet kalder logning af areal på størrelse med Sjælland 'målrettet', Information 11. oktober 2021 https://www.information.dk/indland/2021/10/justitsministeriet-kalder-logning-areal-paa-stoerrelse-sjaelland-maalrettet

personen.

58. Den målrettede logning skal have karakter af undtagelsen, jf. EU-Domstolens fortolkning af e-databeskyttelsesdirektivets artikel 15, stk. 1 i Tele2-dommens præmis 104. Lagring af trafikdata og lokaliseringsdata må således ikke blive hovedreglen. 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.

59. En målrettet logning som omfatter over halvdelen af befolkningen kan ikke med nogen rimelighed siges at opfylde de krav, som EU-Domstolen opstiller, jf. punkt 55-60 ovenfor. Kun den målrettede logning efter den foreslåede § 786 d i retsplejeloven er baseret på konkrete vurderinger af personer eller geografiske områder. Den øvrige målrettede logning, dvs. § 786 b og § 786 c, er baseret på mere eller mindre automatiske kriterier, hvor der ikke er gjort noget reelt forsøg på at begrænse logningen til det strengt nødvendige.

60. Det er i den forbindelse problematisk, at der ikke sker nogen som helst differentiering af de omfattede trafikdata eller opbevaringsperioden (altid 12 måneder) ud fra de konkrete omstændigheder, som begrunder den specifikke målrettede logning. Ud fra en samlet vurdering af §§ 786 b – 786 d er logningsordningen langt tættere på at være generel og udifferentieret end målrettet.

61. IT-Politisk Forening vil derfor anbefale, at § 786 b og § 786 c udgår af lovforslaget, og at den målrettede logning alene baseres på § 786 d, hvor der forudsættes en konkret vurdering. Det vil kunne sikre, at den målrettede logning begrænses til det strengt nødvendige efter EU-Domstolens retspraksis.

62. Den fulde ”målrettede” logningsordning med §§ 786 b – 786 d kræver desuden ganske omfattende og komplekse IT-udviklingsprojekter hos både teleselskaberne og Rigspolitiet. Kompleksiteten understreges af, at foranalysen hos Rigspolitiet tidligst vil foreligge i 2023. Inden disse komplekse IT-systemer er udviklet og implementeret, vil der være en betydelig risiko for, at EU-Domstolen har underkendt den danske målrettede logningsordning, eller en tilsvarende ordning i et andet EU-land, fordi den er for omfattende til at kunne være begrænset til det strengt nødvendige. Skulle EU-Domstolen afsige en sådan dom, vil de betydelige udgifter hos teleselskaberne og Rigspolitiet i sagens natur være spildte.

63. Den personbestemte målrettede logning i § 786 b er problematisk og stigmatiserende. Den omfatter alle tidligere straffede personer for grov kriminalitet (i 3-10 år), samt alle personer eller kommunikationsapparater, som har været genstand for et indgreb i meddelelseshemmeligheden (i 1 år efter indgrebet). Uanset at tidligere straffede personer generelt har større sandsynlighed for at begå ny kriminalitet, kan det umuligt være i overensstemmelse med proportionalitetsprincippet, at alle personer i denne gruppe udsættes for målrettet logning uden en konkret vurdering.

64. Den målrettede logning i § 786 b vil desuden kræve, at oplysninger om tidligere straffede

personer overføres til alle landets teleselskaber med CPR-nummer, så teleselskaberne kan implementere den målrettede logning. Det skaber betydelige risici for misbrug af de pågældende oplysninger. Risikoen for databrud, hvor store dele af strafferegisteret bliver lækket på internettet (eller falder i hænderne på cyberkriminelle, der hacker sig ind i et teleselskabs systemer), bliver også betydeligt større, når en række teleselskaber skal opbevare og behandle disse oplysninger.

65. Den geografisk målrettede logning i § 786 c, stk. 1 omfatter områder på 3 km x 3 km, hvor antallet af anmeldelser af grov kriminalitet (nr. 1) og antallet af beboere dømt for grov kriminalitet (nr. 2) er mindst 1,5 gange landsgennemsnittet opgjort som gennemsnittet over de seneste tre år. Ud fra formuleringen i lovteksten med "antallet" er det uklart hvordan der vil blive taget højde for befolkningstætheden i de enkelte områder på 3 km x 3 km. Hvis der med "landsgennemsnittet" menes gennemsnittet i et referenceområde med det samme antal beboere eller lignende, vil IT-Politisk Forening anbefale, at det bliver præciseret i lovteksten eller i hvert fald bemærkningerne.

Retsgarantier og transparens for målrettet logning

66. For den målrettede logning i § 786 d skal politiet indhente en retskendelse, og der skal beskikkes en advokat som ved indgreb i meddelelseshemmeligheden (§§ 784 og 785 i retsplejeloven). Der vil ikke efter lovforslaget blive givet efterfølgende underretning til de berørte personer omfattet af indgrebet i § 786 d.

67. For den øvrige målrettede logning (§ 786 b og 786 c) skal politiet ikke indhente en retskendelse, og der bliver ikke beskikket en advokat for at varetage interesserne for de personer, der omfattes af indgrebet. Listen med geografiske områder i § 786 c vil desuden bliver hemmeligholdt for offentligheden. Justitsministeriet begrunder dette med, at offentliggørelse vil kunne medføre en betydelig forhøjelse af risikoen for omgåelse.

68. Når den målrettede logning ud fra geografiske kriterier forventeligt vil omfatte mere end halvdelen af befolkningen, jf. punkt 53 ovenfor, er dette argument mod offentliggørelse ikke videre logisk. For befolkningen som helhed vil den manglende offentliggørelse bidrage yderligere til at skabe en følelse af at være under konstant overvågning, svarende til hvad der af EU-Domstolen blev problematiseret for den generelle og udifferentierede logning i den første dom fra 2014, der annullerede logningsdirektivet.[9]

69. En anden konsekvens af den manglende transparens vedr. den geografiske målrettede logning er, at det bliver vanskeligt for Folketinget eller civilsamfundsorganisationer at monitorere, om logningen er begrænset til det strengt nødvendige.[10]

---

9 Præmis 37 i de forenede sager C-293/12 og C-594/12 ("Digital Rights Ireland dommen").

10 Dette argument er dog mindre relevant hvis den målrettede logning omfatter mere end halvdelen af befolkningen, som det skitseres i lovforslaget. I den situation bør det på forhånd stå klart, at den målrettede logning ikke er begrænset til den strengt nødvendige, og at der reelt er tale om en generel og udifferentieret logning til kriminalitetsbekæmpelse.

70. 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. Den målrettede logning udgør i sig selv et indgreb i den grundlæggende ret til privatliv og databeskyttelse for de berørte personer, jf. Charterets artikel 7 og 8.

71. 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.[11] Det bør også gælde for den personbestemte målrettede logning i den foreslåede § 786 d i retsplejeloven, hvor der er forudgående domstolskontrol. Den beskikkede advokat vil ikke være i besiddelse af alle relevante oplysninger, således at adgangen til effektive retsmidler kan udøves fuldt ud for den berørte person.

72. 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.

Generel og udifferentieret logning af en slutbrugers adgang til internettet (§ 786 f)

73. LQDN-dommen tillader generel og udifferentieret logning af IP-adresser, der er tildelt kilden til en forbindelse (”source IP-adresser”), til bekæmpelse af grov kriminalitet (præmis 152-156). Det forudsætter dog en streng overholdelse af de materielle og processuelle betingelser, som skal gælde for brugen af disse data (se punkt 89-93 i dette høringssvar), og at lagringsperiode ikke overstiger hvad der er strengt nødvendigt for formålet.

74. EU-Domstolen begrunder denne undtagelse fra hovedreglen om, at der ikke kan ske generel og udifferentieret logning af trafikdata og lokaliseringsdata til kriminalitetsbekæmpelse med, at den tildelte IP-adresse er mindre følsom end andre former for trafikdata (LQDN-dommens præmis 152).

75. I den nuværende logningsbekendtgørelses § 5, stk. 1 er der fastsat krav om registrering af oplysninger vedr. en brugers adgang til internettet. Registreringspligten omfatter den tildelte IP-adresse, den tildelte brugeridentitet, navn og adresse på brugeren (hvis de behandles af udbyderen), samt start- og sluttidspunktet for tildelingen. Oplysningerne kan udleveres til politiet efter retsplejelovens § 804 (edition), hvor der ikke er nogen begrænsning til grov

11 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).”

kriminalitet.

76. Med LQDN-dommen har EU-domstolen fastslået, at det inden for EU-rettens rammer er muligt at pålægge internetudbydere at registrere og opbevare oplysninger om tildelt IP-adresser, svarende til § 5, stk. 1 i logningsbekendtgørelsen, men politiets adgang til disse oplysninger skal begrænses til sager om grov kriminalitet. Det vil kræve ændringer af retsplejelovens editionsregler for så vidt angår udlevering af oplysninger om en brugers adgang til internettet, således at politiets adgang begrænses til sager om grov kriminalitet (se punkt 89-93 nedenfor).

77. Justitsministeriet har imidlertid en anden fortolkning af LQDN-dommen. Justitsministeriet bemærker først, at begrebet 'IP-adresser' ikke er entydigt defineret af EU-Domstolen. Derefter vurderer Justitsministeriet, at præmis 152-156 omhandler en logningspligt for internetsessioner, hvor destinationen for trafikken registres.[12] Det begrundes med præmis 153 i LQDN-dommen, hvor det nævnes, at IP-adresser kan "anvendes til bl.a. at foretage en udtømmende sporing af en internetbrugers søgemønstre og dermed af den pågældendes onlineaktiviteter" (benævnt "clickstream" i den engelske oversættelse af dommen).

78. Registrering af source IP-adresser, svarende til § 5, stk. 1 i logningsbekendtgørelsen, vil efter Justitsministeriets opfattelse falde ind under præmis 157-159 i LQDN-dommen, som omhandler civil identitet. Eftersom denne type registrering ikke udgør et alvorligt indgreb i grundlæggende rettigheder, skal den ikke være formålsbegrænset til grov kriminalitet. Der behøver heller ikke at være en begrænsning for lagringsperioden.

79. På den baggrund mener Justitsministeriet, at de nuværende regler om internetlogning kan videreføres uden ændringer, både for så vidt angår den generelle og udifferentierede lagringspligt og politiets muligheder for at få adgang til de lagrede oplysninger.

80. Efter IT-Politisk Forenings opfattelse er det hævet over enhver tvivl, at præmis 152-156 omhandler registrering af source IP-adresser (kilden til en forbindelse), og ikke sessionslogning. Det ses tydeligst i besvarelsen af de præjudicielle spørgsmål sidst i dommen, hvor det fremgår, at EU-retten **ikke er til hinder for** lovgivningsmæssige foranstaltninger

> "*der med henblik på beskyttelse af den nationale sikkerhed, bekæmpelse af **grov kriminalitet** og forebyggelse af alvorlige trusler mod den offentlige sikkerhed foreskriver generel og udifferentieret lagring af de IP-adresser, **der er tildelt kilden til en forbindelse**, i en periode, der er tidsmæssigt begrænset til det strengt nødvendige.*" (vores fremhævning)

81. I Præmis 152 skelnes der klart mellem IP-adressen for kilden til en kommunikation (source IP) og modtageren af kommunikationen (destination IP). **Det er kun IP-adresserne for**

12 Det vil svare til den sessionslogning, som var en del af logningsbekendtgørelsen indtil ændringen ved bekendtgørelse nr. 660 af 19. juni 2014.

kilden til en kommunikation, som er mindre følsomme end øvrige trafikdata, fordi de ikke som sådan afslører nogle oplysninger om de tredjemænd, der har været i kontakt med den person, som har foretaget kommunikationen.

82. I forhold til præmis 153 vil registrering af IP-adressen for kilden til en forbindelse udgøre et alvorligt indgreb i grundlæggende rettigheder, fordi den sammenholdt med IP-adresser i eksterne logfiler giver mulighed for at foretage en sporing af brugerens onlineaktiviteter. At der i sporingen indgår oplysninger fra eksterne logfiler, og ikke blot de oplysninger som internetudbyderen har registreret, fremgår også af præmis 154. I det tilfælde hvor en lovovertrædelse er begået online kan lagring af IP-adressen "udgøre det eneste efterforskningsmiddel, der kan gøre det muligt at identificere den person, som denne adresse var tildelt på det tidspunkt, hvor den pågældende overtrædelse blev begået." **Det er kun source IP-adresser som bliver tildelt en bruger.**

83. EU-Domstolen anerkender i præmis 155-156, at selv lagring af IP-adressen for kilden til en kommunikation udgør et indgreb i grundlæggende rettigheder af alvorlig karakter, idet brugerne af internettet har en forventning om at deres identitet ikke afsløres, når de tilgår information online.

84. Men fordi en lagring af IP-adressen for kilden til en kommunikation kan være det eneste efterforskningsmiddel, der gør det muligt at identificere gerningspersonen til en lovovertrædelse online (jf. præmis 154), finder EU-Domstolen ud fra en samlet proportionalitetsafvejning, at en **generel og udifferentieret lagring af IP-adressen der er tildelt kilden til en forbindelse** er inden for EU-rettens rammer (præmis 155), men kun hvis det er bekæmpelse af grov kriminalitet som begrunder indgrebet (præmis 156).

85. EU-Domstolen berører i øvrigt indirekte sessionslogning i en anden del af LQDN-dommen. I præmis 174 om den automatiske analyse af trafikdata og lokaliseringsdata i Frankrig (for alle personer) omtales dette indgreb som særligt alvorligt, og denne konstatering gælder "så meget desto mere når de data, der er genstand for den automatiserede analyse [..] **kan afsløre arten af de oplysninger, der er blevet tilgået online.**" (vores fremhævning).

86. Indgreb der omtales i præmis 174, herunder altså generel og udifferentieret sessionslogning, kan kun opfylde kravet om proportionalitet i de situationer, hvor en medlemsstat står over for en alvorlig trussel mod den nationale sikkerhed, som er reel og aktuel eller forudsigelig (jf. præmis 177). Indgrebet i præmis 152-156 forudsætter derimod alene at formålet er bekæmpelse af grov kriminalitet.

87. På grundlag af punkt 80-86 ovenfor må det være hævet over enhver tvivl, at LQDN-dommens præmis 152-156 ikke vedrører sessionslogning som antaget af Justitsministeriet, men derimod registrering af IP-adresser m.v. for kilden til en forbindelse, svarende til § 5, stk. 1 i den nuværende logningsbekendtgørelse.

88. Det bør derfor præciseres i den foreslåede § 786 f i retsplejeloven eller de tilhørende bemærkninger, at den generelle og udifferentierede registrering og opbevaring af

oplysninger om en slutbrugers adgang til internettet alene omfatter IP-adresser m.v. som er tildelt kilden til en forbindelse, **og at oplysningerne kun kan anvendes ved efterforskning og retsforfølgelse af grov kriminalitet.**

Politiets adgang til oplysninger om slutbrugers internetadgang (edition)

89. Som en konsekvens af LQDN-dommens præmis 152-156 vil det være nødvendigt at indsætte en ny bestemmelse i retsplejelovens kapitel 74 om politiets adgang til oplysninger om en slutbrugers adgang til internettet. I dag bruges retsplejelovens § 804 til dette formål, men denne bestemmelse er ikke begrænset til sager om grov kriminalitet. Der er heller ikke "strenge betingelser og garantier for så vidt angår brugen af disse data", som krævet af LQDN-dommens præmis 156.

90. Den foreslåede § 804 a i retsplejeloven (for andre trafikdata end IP-adresser) kan i princippet være udgangspunktet for en sådan ny editionsbestemmelse for politiets adgang til oplysninger om en slutbrugers adgang til internettet.[13]

91. Udover et kriminalitetskrav, der begrænser adgangen til sager om grov kriminalitet (som i den foreslåede § 804 a i retsplejeloven), skal lovgrundlaget, der regulerer politiets adgang, også sikre en proportionalitetsvurdering i den konkrete sag mellem hensynet til politiets efterforskning af onlinekriminalitet og beskyttelsen af internetbrugerens grundlæggende rettigheder.

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

93. Proportionalitetsvurderingen vedr. afsløring af en internetbrugers identitet (edition af oplysninger om en bruger af internettet) bør derfor altid inddrage en grundig vurdering af den kontekst (den konkrete kommunikation på internettet), som er årsagen til at politiet ønsker internetbrugerens identitet oplyst.[14]

Logning af source porte m.v. ved delte IP adresser (CG-NAT)

94. Udover de nuværende regler i logningsbekendtgørelsen § 5, stk. 1 om registrering af tildelt

13 Altså identifikation af en bruger på grundlag af en IP-adresse og eventuel øvrige information, som politiet har fået kendskab til i forbindelse med en efterforskning, eksempelvis fra logfiler for en server brugt til ulovlige aktiviteter (der opfylder kravene til grov kriminalitet).

14 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 (eksempelvis besøg på en bestemt hjemmeside eller ytringer på en social medie platform).

IP-adresse og brugeridentitet (samt navn og adresse, hvis disse oplysninger behandles), vil der efter den foreslåede § 786 f, stk. 3 i retsplejeloven blive fastsat regler om registrering af yderligere oplysninger for at sikre en entydig identifikation af en bruger af internettet.

95. På grund af den globale mangel på IPv4-adresser vil en række internetforbindelser være baseret på Carrier-Grade Network Address Translation (CG-NAT) teknologien, hvor flere abonnenter tilgår internettet med den samme offentlige IP-adresse (som kilden til deres kommunikation, altså source IP-adresse).[15]

96. Af bemærkningerne i pkt. 3.3 (side 68) fremgår det, at Justitsministeren vil fastsætte regler om registrering af portnumre (”source port number”). Portnummeret vil sammen med IP-adressen og et præcist timestamp kunne udgøre en unik identifikation af brugeren. Bemærkningerne omtaler også ”andre identificerende oplysninger”, som en udbyder tildeler slutbrugeren vedr. adgang til internettet. Det er uklart for IT-Politisk Forening hvad der menes med ”andre identificerende oplysninger”, hvis det har specifik reference til situationen med deling af IP-adresser (CG-NAT).

97. 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.[16]

98. 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).

99. I en nylig redegørelse[17] om efterforskning af en sag om seksuel afpresning via digitale medier skriver Rigspolitiet eksempelvis:

”Dertil kommer, at en given IP-adresse kan have mange samtidige brugere, og

15 Dette må ikke forveksles med situationen hvor eksempelvis flere personer i en husstand deler en internetforbindelse via NAT i den router som er tilsluttet nettermineringspunktet. Ved CG-NAT vil internetudbyderen muligvis kunne registrere yderligere oplysninger (f.eks. source portnumre), som gør det muligt at skelne mellem de abonnenter, der anvender samme IP-adresse, fordi delingen af IP-adressen mellem flere abonnenter (slutbrugere) administreres i internetudbyderens udstyr. Hvis der er tale om deling af en internetforbindelse i en husstand, har internetudbyderen ingen teknisk mulighed for ar skelne mellem de enkelte brugere.

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

17 Rigspolitiet: Notat om efterforskningen af en sag om omfattende seksuel afpresning via digitale medier (Operation sextortion), REU Alm.del - Bilag 399

identificering af en eksakt mistænkt kræver derfor et portnummer. ***Da de fleste sociale platforme ikke logger de portnumre, som er brugt fra IP-adressen****, kan det vise sig, at oplysninger om IP-adressen ikke kan anvendes til at identificere den relevante bruger bag en IP-adresse. Dette skyldes, at der ofte er flere tusinde brugere, der samtidig kan anvende samme IP-adresse.*" (vores fremhævning)

100. Brug af portnumre sammen med en IP-adresse for at identificere en bruger bag CG-NAT vil være meget afhængig af, at timestamps er perfekt synkroniseret mellem internetudbyderen og den eksterne server, hvor der i logfilerne gemmes både IP-adresse og portnummer for de besøgende på websiden. Hvis der er blot et par sekunders mismatch, kan internetudbyderen meget vel identificere den forkerte bruger, med deraf følgende risiko for at en uskyldig person bliver genstand for politiets efterforskning.[18]

101. Logning af portnumre vil kræve en omfattende registrering hos internetudbyderne. Antallet af dataposter vil være det samme som sessionslogning, dog med mindre datamængder fordi destination IP-adresse og portnummer ikke skal registreres. Websider består i dag generelt af mange forskellige elementer fra forskellige webservere, som hentes i separate datakanaler for at optimere overførslen. Det øger antallet af sessioner ganske kraftigt. På en computer vil læsning af en artikel på www.jp.dk generere omkring 200 sessioner.[19] Hver gang der klikkes på et nyt artikel-link, genereres der omkring 200 nye sessioner.

102. Nogle internetudbydere udfører allerede denne registrering på frivillig basis. Andre internetudbydere kan imidlertid være i den situation, at deres nuværende udstyr slet ikke er i stand til at foretage en registrering og opbevaring af tildelte portnumre. Det er usandsynligt at hoteller, restauranter, caféer og campingpladser, der tilbyder deres kunder adgang til internettet via WiFi hotspots, vil have udstyr som kan lave logning af portnumre.

103. Som anført ovenfor (jf. punkt 98-99) vil den yderligere registrering af portnumre hos internetudbyderne ofte ikke kunne bruges af politiet. Samtidig er der tale om registrering af omfattende datamængder, som kan medføre store økonomiske og praktiske byrder hos nogle udbydere (jf. punkt 101-102), og som ikke mindst indebærer en risiko for at der kan blive registreret oplysninger om abonnentens adfærdsvaner i privatlivet (jf. punkt 97).

104. På den baggrund vil IT-Politisk Forening anbefale, at der ikke fastsættes krav om logning af portnumre. Alternativt bør der fastsættes passende undtagelser for mindre udbydere som hoteller, restauranter og caféer samt almindelige internetudbydere, hvis deres nuværende tekniske udstyr ikke tillader logning af portnumre.

---

18 Risikoen for dette afhænger af hvor hurtigt internetudbyderen "genbruger" et portnummer fra en tidligere session til en anden slutbruger.

19 Undersøgelse udført af IT-Politisk Forening i 2016. Det afgørende er ikke det præcise tal, men at almindelige internetaktiviteter som læsning af nyheder hos et online nyhedsmedie (der viser målrettede reklamer) genererer et meget stort antal sessioner.

Hastesikring (§ 786 a)

105. IT-Politisk Forening har ingen bemærkninger til de foreslåede ændringer af retsplejelovens § 786 a, idet politiets adgang til hastesikring af trafikdata og lokaliseringsdata begrænses til efterforskning af grov kriminalitet i overensstemmelse med LQDN-dommen.

106. Efter IT-Politisk Forenings opfattelse vil en "værktøjskasse" til politiet, som består af hastesikring (som § 786 a), en reelt målrettet logning af trafikdata (som § 786 d) og eventuelt en generel og udifferentieret logningspligt for tildelte IP-adresser (som § 786 f, men begrænset til efterforskning af grov kriminalitet), sikre en passende balance mellem hensynet til politiet efterforskningsmuligheder og det alvorlige indgreb i borgernes grundlæggende ret til privatliv, databeskyttelse og ytringsfrihed, jf. artikel 7, 8 og 11 i Charter om Grundlæggende Rettigheder, som er uløseligt forbundet med en logningspligt for udbydere af elektroniske kommunikationsnet og -tjenester.

Politiets adgang til de lagrede oplysninger (overordnede bemærkninger)

107. 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 38-46 ovenfor. Bemærkningerne nedenfor i punkt 108-160 gælder således alene i forhold til adgang begrundet i kriminalitetsbekæmpelse.

108. Politiets adgang til lagrede oplysninger indebærer et indgreb i de rettigheder, som er sikret af e-databeskyttelsesdirektivets 2002/58/EF, navnlig artikel 5, 6 og 9 i dette direktiv.[20] Adgangen til lagrede oplysninger skal derfor 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.[21]

109. I en række domme siden 2014 har EU-Domstolen udviklet en ganske detaljeret retspraksis, som nationale retsregler for politiets adgang til trafikdata og lokaliseringsdata skal opfylde. Der har i Danmark været mindre fokus på disse aspekter af EU-dommene end spørgsmålet om den generelle og udifferentierede lagringspligt i forbindelse med de årlige lovforslag om (udskydelse af) revision af logningsreglerne.

110. Hvis der er tale om alvorlige indgreb i rettigheder sikret af e-databeskyttelsesdirektivet, har EU-Domstolen fastslået, at det på området for kriminalitetsbekæmpelse kun er bekæmpelse

20 EU-Domstolen har blandt andet fastslået dette i præmis 76-80 af Tele2-dommen, præmis 35-38 i C-207/16 Ministerio Fiscal og præmis 96-97 i LQDN-dommen.

21 Det er i LQDN-dommens præmis 167 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 fastsat ved lov). 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.")

af grov kriminalitet som kan begrunde sådanne indgreb, jf. eksempelvis præmis 55-57 i C-207/16 Ministerio Fiscal. Det er derfor vigtigt at fastlægge hvilke indgreb der er alvorlige.

111. I præmis 35 af C-746/18 Prokuratuur fastslår EU-Domstolen, at "offentlige myndigheders adgang til en samling af trafikdata eller lokaliseringsdata, der kan tilvejebringe oplysninger om den kommunikation, som en bruger har foretaget ved hjælp af et elektronisk kommunikationsmiddel, eller om placeringen af det terminaludstyr, som den pågældende gør brug af, og som kan gøre det muligt at drage præcise slutninger vedrørende de berørte personers privatliv" **udgør et alvorlig indgreb**, og at det derfor kun er bekæmpelse af grov kriminalitet som kan begrunde dette indgreb.

112. Politiets adgang til trafikdata og lokaliseringsdata, der kan afsløre hvem brugeren kommunikerer med (oplysninger om brugerens kommunikation) eller hvor brugeren opholder sig, vil altid udgøre et alvorlig indgreb. Det gælder uanset varigheden af den periode, for hvilken der er anmodet om adgang til de nævnte data, jf. præmis 39-40 i Prokuratuur-dommen.

113. De pågældende trafikdata og lokaliseringsdata gør det muligt at drage præcise slutninger vedrørende privatlivet for de personer, hvis data er blevet lagret, 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] Det understreger den følsomme karakter af disse data, og at adgang til oplysningerne udgør et alvorlig indgreb.

114. Ikke-alvorlige indgreb i rettigheder sikret af e-databeskyttelsesdirektivet er først og fremmest adgang til oplysninger om slutbrugerens civile identitet, hvis dette ikke kræver behandling af følsomme trafikdata og lokaliseringsdata. I Ministerio Fiscal dommen har EU-Domstolen fastslået, at adgang til identitetsoplysninger for brugerne af de SIM-kort, som inden for en kort periode (12 dage) havde været anvendt i en bestemt stjålet telefon (identificeret ud fra dens IMEI-nummer), ikke udgør et alvorlig indgreb. Det afgørende i denne situation er, at der ikke kan skabes en forbindelse til brugerens kommunikation eller placeringen af terminaludstyret.

115. Politiets adgang til trafikdata og lokaliseringsdata skal ske efter forudgående domstolskontrol undtagen i behørigt begrundede hastende tilfælde. Den nationale lovgivning skal fastsætte materielle og processuelle betingelser for denne adgang. Hvis der er tale om et alvorligt indgreb (altså de fleste sager om adgang til trafikdata og lokaliseringsdata), er det ikke tilstrækkeligt at begrænse adgangen til sager om grov kriminalitet, jf. præmis 118 i Tele2-dommen. Der skal være 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. Det kan indebære begrænsninger for kategorier af data og varigheden af den periode, for hvilken der anmodes om adgang.

22 Jf. eksempelvis præmis 36 i Prokuratuur-dommen.

116. De danske retsbestemmelser i retsplejelovens kapitel 71 og 74 (der regulerer politiet adgang til lagrede trafikdata og lokaliseringsdata) er fra henholdsvis 1980'erne og 1990'erne, og de er ikke blevet opdateret i lyset af den ændrede retspraksis fra EU-Domstolen. Det har især betydning for editionsreglerne i kapitel 74, fordi dette indgreb i den gældende retsplejelov ikke har nogen begrænsning til sager om grov kriminalitet.

117. Det er særdeles uhensigtsmæssigt, hvis de danske retsbestemmelser om politiets adgang til trafikdata og lokaliseringsdata ikke er i overensstemmelse med EU-retten. Det skaber retlig usikkerhed for alle parter i straffesagskæden. Retsanvendende myndigheder har imidlertid en forpligtelse til at undlade at anvende nationale retsregler i det omfang, de ikke er i overensstemmelse med EU-retten.

118. Selv om retsplejelovens § 804 i dag giver mulighed for at udlevere lokaliseringsdata i alle sager om efterforskning af lovovertrædelser undergivet offentlig påtale, har retsanvendende myndigheder (herunder anklagemyndigheden) en pligt til at sikre, at det alene sker i sager om grov kriminalitet, således at dansk ret ikke anvendes i strid med EU-retten. Så vidt IT-Politisk Forening er orienteret, har de retsanvendende myndigheder ikke generelt sikret dette siden 2014, hvor EU-Domstolen første gang fastslog, at politiets adgang til lokaliseringsdata kun kan gives i sager om grov kriminalitet.[23]

119. Det er derfor positivt, at Justitsministeriet nu, omend med betydelig forsinkelse, foreslår ændringer af retsplejeloven med henblik på at bringe de danske retsregler i overensstemmelse med EU-retten. Som det anføres nedenfor i høringssvaret er de foreslåede ændringer (kriminalitetskravet i § 804 a) imidlertid ikke tilstrækkelige.

Adgang til teleoplysninger (retsplejelovens kapitel 71)

120. I dansk ret har meddelelseshemmeligheden altid omfattet såvel kommunikationens indhold som de tilhørende teleoplysninger.[24] For at politiet kan få adgang til lagrede (historiske) teleoplysninger skal betingelserne for indgreb i meddelelseshemmeligheden i kapitel 71 være opfyldt.[25] Det gælder uanset om de pågældende teleoplysninger er lagret af kommercielle årsager, typisk fakturering af abonnenten, eller for at opfylde en lagringspligt (logningsbekendtgørelsen).

121. Betingelserne for adgang omfatter i retsplejelovens § 781 mistankekravet, indikationskravet samt kriminalitetskravet, som begrænser indgrebet til efterforskning af bestemte

23 Af fodnote 3 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" fremgår det, at Justitsministeriet er opmærksom på den manglende overensstemmelse mellem retsplejelovens editionsregler og EU-retten i forhold til politiets adgang til visse loggede oplysninger.

24 Oplysninger om hvem der kommunikerer med hvem.

25 Teleoplysninger omfatter efter dansk retspraksis ikke lokaliseringsdata for kommunikation via mobiltelefoni, som er omfattet af EU-rettens beskyttelse af meddelelseshemmeligheden (fortrolighed af kommunikation) i e-databeskyttelsesdirektivet 2002/58/EF.

lovovertrædelser, som kan siges at udgøre grov kriminalitet. Derudover skal der foretages en proportionalitetsvurdering i forhold til den person, som indgrebet rettes mod, jf. § 782, stk. 1. Der skal endvidere beskikkes en advokat for denne person (§§ 784-785), og indgreb skal ske efter retskendelse (§ 783). Efter indgrebets afslutning skal der ske underretning, med visse undtagelser (§ 788).

122. De danske bestemmelser om teleoplysning[26] bør generelt opfylde kravene i EU-Domstolens retspraksis for politiets adgang til trafikdata og lokaliseringsdata, dog med en enkelt mulig undtagelse. 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."

123. Formuleringen "bestemte grunde til at antage, at der på den pågældende måde gives meddelelser eller foretages forsendelser til eller fra en mistænkt" i retsplejeloven § 781, stk. 1, nr. 1 må indebære, at politiet kan få adgang til teleoplysninger vedrørende en person, som alene modtager meddelelser fra en mistænkt. Det synes ikke at være foreneligt med Tele2-dommens præmis 119.[27]

124. Den foreslåede § 781 a i retsplejeloven indfører et lavere kriminalitetskrav (med en strafferamme på 3 år) for teleoplysning og udvidet teleoplysning, hvis indgrebet består i pålæg om udlevering af oplysninger, der er registrerings- og opbevaringspligtige efter §§ 786 a – 786 e. For IT-Politisk Forenings generelle bemærkninger om det lavere kriminalitetskrav henvises til punkt 166-177 nedenfor.

125. Det nuværende kriminalitetskrav i § 781 er fortsat gældende, hvis pålægget består i udlevering af teleoplysninger, som ikke er registrerings- og opbevaringspligtige. Det kan eksempelvis være oplysninger om udgående opkald, hvis de fortsat lagres af teleselskabet efter et år, hvor opbevaringsperioden for registreringspligten efter §§ 786 b – 786 e er udløbet. I denne situation vil politiet dog uden videre kunne hastesikre de pågældende oplysninger via retsplejelovens § 786 a, hvorefter der vil kunne gives adgang (teleoplysning) via det lempeligere kriminalitetskrav i § 781 a.

Adgang til registreringspligtige oplysninger efter editionsreglerne (§ 804 a)

126. Med den foreslåede § 804 a i retsplejeloven indsættes et kriminalitetskrav (svarende til det i § 781 a) for pålæg om edition af oplysninger, der er registrerings- og opbevaringspligtige i medfør af hastesikring (§ 786 a), målrettet logning (§§ 786 b – 786 d) samt generel og udifferentieret logning (§ 786 e). Derudover sikrer den foreslåede § 806, stk. 10, at der skal beskikkes en advokat for den berørte person (eller de berørte personer), og at der efter

26 Udvidet teleoplysning kommenteres særskilt nedenfor i punkt 154-160.

27 Hvis en journalist har kontakt med en ukendt whistleblower, som er genstand for en efterforskning, vil det være meget problematisk, hvis politiet kan foretage teleoplysning mod journalisten (fordi journalisten er modtager af meddelelser fra en mistænkt) med henblik på at afdække hvem den ukendte whistleblower er.

indgrebets afslutning skal ske underretning af de berørte personer.

127. I de specielle bemærkninger til § 804 a anføres det, at bestemmelsen primært vil omfatte historiske masteoplysninger, hvor adgang i dag gives via retsplejelovens § 804 (uden noget kriminalitetskrav, beskikkelse af en advokat eller efterfølgende underretning af de berørte personer).

128. Hensigten med § 804 a er at bringe editionsreglerne i overensstemmelse med EU-Domstolens retspraksis. Efter IT-Politisk Forenings opfattelse kræver dette imidlertid større ændringer end den foreslåede § 804 a.

129. Den simpleste ændring af retsplejeloven for at sikre overensstemmelse med EU-retten må være at udvide begrebet teleoplysning til at omfatte lokaliseringsdata i tilknytning til den elektroniske kommunikation. Det ville bringe påbud om udlevering af lokaliseringsdata ind under kapitel 71, inklusive den fulde beskyttelse med indikationskravet i § 781, stk. 1, nr. 2 og proportionalitetsvurderingen i § 782, stk. 1 Der vil være behov for en mindre tilpasning af mistankekravet i § 781, stk. 1. nr. 1, men det er også nødvendigt for teleoplysning for at sikre, at der kun kan gives adgang til data vedr. en mistænkt person.

130. Selv om der indføres et kriminalitetskrav i § 804 a, er de grundlæggende betingelser for edition i kapitel 74 stadig gældende. Der skal efter retsplejelovens § 804 være grund til at antage, at oplysningerne kan tjene som bevis i en efterforskning, hvilket synes at være et forholdsvist mildt relevanskriterium sammenlignet med de tilsvarende krav i kapitel 71, specielt indikationskravet. Bemærkningerne til § 804 er relativt sparsomme for så vidt angår fortolkningen af kriterierne for pålæggelse af edition.[28]

131. Der er i retsplejelovens § 804 ikke noget krav om, at oplysningerne skal vedrøre en person, som er mistænkt i den pågældende efterforskning. Der vil fortsat kunne udleveres masteoplysninger om andre personer med indirekte forbindelse til efterforskningen, eller oplysninger om et stort antal personer der har befundet sig i et bestemt område (”udvidet masteoplysning”, som kommenteres i punkt 154-160 nedenfor).

132. Der er heller ikke i § 804 (eller § 804 a) et krav om at politiets adgang skal begrænses til det strengt nødvendige i den konkrete efterforskning, jf. punkt 115 i dette høringssvar (og den citerede retspraksis fra EU-Domstolen). For indgreb der falder ind under retsplejelovens kapitel 71 bør proportionalitetsvurderingen i § 782, stk. 1 kunne sikre dette, fordi denne vurdering eksplicit skal laves i forhold til den berørte person.[29]

133. Proportionalitetsvurderingen i § 805, stk. 1 er baseret på ”det tab eller den ulempe, som

28 Jf. Folketingstidende 1998-99, tillæg A, s. 875-876 (specielle bemærkninger til retsplejelovens §§ 804-805).

29 I eksempelvis U 2016.351 Ø fandt landsretten, at historiske teleoplysninger i en periode for 1,5 måned forud for gerningstidspunktet var uforholdsmæssigt, hvorfor perioden blev begrænset til 14 dage før gerningstidspunktet, se Lene Wacher Lentz, *Retsplejelovens regulering af politiets adgang til teledata*, Tidsskrift for Kriminalret. 2017, 10, s. 1240-1252

indgrebet kan antages at medføre”, hvilket må skulle forstås som forhold hos den udbyder af elektroniske kommunikationsnet og -tjenester, som indgrebet formelt rettes mod, og ikke som udgangspunkt den krænkelse og ulempe, som indgrebet medfører for de berørte personer (som i § 782, stk. 1). Bemærkningerne til § 805 er dog relativt sparsomme i forhold til hvordan proportionalitetsvurderingen skal foretages.

134. Af lovforslagets almindelige bemærkninger pkt. 3.7.4.1 fremgår det ganske vist, at domstolene ligesom i dag vil skulle foretage en afvejning af hensynet til at få udleveret oplysninger til brug for efterforskning af grov kriminalitet over for brugernes krav på hemmeligholdelse, sådan som dette er sikret i e-databeskyttelsesdirektivet og i EU’s charter om grundlæggende rettigheder, jf. Østre Landsrets kendelse af 7. maj 2018 i sag nr. B-2451-17 og B-2458-17.

135. Det er korrekt, at Østre Landsret i den konkrete kendelse om civilretlig edition af oplysninger vedr. brugeren af en IP-adresse afviste adgangen til edition ud fra en samlet afvejning, hvor kravene om hemmeligholdelse i telelovens § 7, stk. 1 og i § 23, stk. 1 i den daværende udbudsbekendtgørelse[30] blev indfortolket i retsplejelovens udelukkelses- eller fritagelsesgrunde for vidnepligt i §§ 169 – 172. Det havde imidlertid også betydning for landsrettens afvejning i den pågældende sag, at IP-adresse oplysningerne alene var lagret af teleselskaberne efter krav i logningsbekendtgørelsen med henblik på udlevering til politiet, hvorefter udlevering til en privat aktør ikke ville være proportionalt.

136. IT-Politisk Forening er ikke bekendt med editionssager efter § 804, hvor kravene om hemmeligholdelse i telelovens § 7, stk. 1 m.v. er blevet brugt til at begrænse politiets adgang til edition. En række oplysninger opbevares af teleselskaberne netop med henblik på udlevering til politiet, jf. ikke mindst logningsreglerne som har dette formål. IT-Politisk Forening er derimod bekendt med, at politiet via editionsreglerne får udleveret oplysninger om alle brugere i et bestemt område (udvidet masteoplysning) eller samtlige brugere af en delt IP-adresse (ved CG-NAT). Det er i begge tilfælde meget vidtgående indgreb i rettigheder sikret af Charter om Grundlæggende Rettigheder.

137. En proportionalitetsvurdering via retsplejelovens § 805, stk. 1 vil formentlig forudsætte, at teleudbyderen konkret gør indsigelser, som det skete i den omtalte sag fra Østre Landsret. Det vil typisk ikke ske på grund af udbydernes afståelseserklæringer til Rigspolitiet. Den beskikkede advokat (edition via § 804 a) skal varetage interesserne for de berørte personer, og advokaten kan næppe uden videre påberåbe sig teleudbyderens interesser og forpligtelser til fortrolighed.

138. Proportionalitetskravet fremstår under alle omstændigheder langt klarere med formuleringen i retsplejelovens § 782, stk. 1 i kapitel 71, hvor indgrebet ikke må foretages, såfremt det efter indgrebets formål, sagens betydning og den krænkelse og ulempe, som indgrebet må antages at forvolde den eller de personer, som det rammer, ville være et uforholdsmæssigt indgreb.

30 Daværende gennemførelse af artikel 6 i e-databeskyttelsesdirektivet 2002/58/EF.

139. IT-Politisk Forening skal derfor anbefale, at der i retsplejelovens § 806, stk. 10 indsættes en henvisning til § 782, stk. 1, så der foretages en udtrykkelig proportionalitetsvurdering direkte i forhold til den berørte person, i stedet for en indirekte vurdering via udbyderens interesser og krav om fortrolighed (som § 805, stk. 1 muligvis kan sikre). Derudover bør det præciseres, at der som udgangspunkt kun kan udleveres data vedr. en person, som er mistænkt i efterforskningen.

140. Editionsreglerne i retsplejelovens kapitel 74 bruges på en lang række meget forskellige indgreb. Edition af trafikdata og lokaliseringsdata hos teleselskaber (masteoplysninger, IP-adresser, m.v.) har generelt større lighedspunkter med indgreb i meddelelseshemmeligheden efter kapitel 71 end det typiske editionsindgreb (på andre områder). Alene af den grund ville det være mest logisk, at samle alle indgreb, hvor teleselskaber pålægges at udlevere personoplysninger beskyttet af e-databeskyttelsesdirektivet, i retsplejelovens kapitel 71.

141. På den måde ville dansk ret få en konsistent beskyttelse af metadata for elektronisk kommunikation, i stedet for den nuværende lovregulering hvor nogle metadata (teleoplysninger) falder ind under kapitel 71, mens andre metadata (lokaliseringsdata og IP-adresser) omfattes af de mere lempelige editionsregler i kapitel 74. EU-retten giver imidlertid begge typer metadata (teleoplysninger, lokaliseringsdata og IP-adresser) samme beskyttelse i e-databeskyttelsesdirektivet.[31]

Adgang til ikke-registreringspligtige trafikdata og lokaliseringsdata efter editionsreglerne

142. Politiets adgang til ikke registreringspligtige trafikdata og lokaliseringsdata vil efter lovforslaget fortsat skulle ske efter den almindelige editionsregel i § 804. Det betyder, at disse oplysninger vil kunne udleveres til politiet i efterforskning af alle lovovertrædelser undergivet offentlig påtale.

143. Ikke-registreringspligtige trafikdata og lokaliseringsdata vil jf. de almindelige bemærkninger pkt. 3.1.3.4 omfatte lokaliseringsdata, der udgør trafikdata i forbindelse med internetforbrug, og lokaliseringsdata fra ikke-aktive mobiltelefoner. For en bruger der har en smartphone vil der i praksis være tale om særdeles detaljerede oplysninger om telefonens mastetilknytninger i løbet af dagen, fordi telefonen hele tiden har internettrafik fra apps i baggrunden for at hente statusopdateringer til notifikationer m.v.

144. Mobiludbyderne opbevarer ifølge lovforslagets bemærkninger disse oplysninger i cirka 14 dage på frivillig basis. Efter bemærkningerne i pkt. 3.1.3.4 påhviler det udbyderne, at holde oplysningerne adskilt fra trafikdata og lokaliseringsdata, som er registrerings- og opbevaringspligtige efter retsplejelovens §§ 786 a – 786 e, givetvis fordi der efter lovslaget vil gælde forskellige regler for udlevering til politiet.

145. Denne skelnen mellem forskellige typer trafikdata og lokaliseringsdata er begrundet i, at

31 Definition af teleoplysninger er fra ændringen af retsplejeloven i 1985 (med videreførelse af tidligere definition), hvor mobiltelefoni og dermed masteoplysninger havde en relativt begrænset udbredelse.

LQDN-dommen efter Justitsministeriets opfattelse alene regulerer data, der gøres registrerings- og opbevaringspligtige i medfør af regler, der udformes på baggrund af artikel 15, stk. 1, i direktiv nr. 2002/58. Kun for disse data er det ifølge Justitsministeriets opfattelse nødvendigt at begrænse adgangen til sager om grov kriminalitet, og den foreslåede § 804 a gælder derfor kun for pålæg om edition af registrerings- og opbevaringspligtige oplysninger.

146. Hertil skal IT-Politisk Forening bemærke, at ifølge præmis 167 i LQDN-dommen kan medlemstaterne i deres nationale lovgivning fastsætte regler om adgang til trafikdata og lokaliseringsdata med henblik på bekæmpelse af **grov kriminalitet**, når disse data af udbyderen er lagret på en måde, der er i overensstemmelse med artikel 5, 6 og 9 eller artikel 15, stk. 1, i direktiv 2002/58. Lagring i overensstemmelse med artikel 15, stk. 1 vil være en national lovgivning om registrerings- og opbevaringspligt. Artikel 5, 6 og 9 omfatter samtlige undtagelser fra e-databeskyttelsesdirektivets krav om, at trafikdata og lokaliseringsdata skal slettes umiddelbart efter kommunikationens afslutning. Lagring af kommercielle årsager hos teleudbyderen må derfor kun ske i henhold til de angivne undtagelser i artikel 5, 6, og 9.[32]

147. Betingelsen om grov kriminalitet i LQDN-dommens præmis 167 gælder altså uanset om data er lagret på grundlag af en registrerings- og opbevaringspligt (efter artikel 15, stk. 1) eller af kommercielle årsager (artikel 5, 6 og 9).

148. Af EU-Domstolens øvrige domme om e-databeskyttelsesdirektivet fremgår det endvidere, at politiets adgang til lagrede trafikdata og lokaliseringsdata udgør et indgreb i rettigheder sikret af dette direktiv, **uanset årsagen til lagringen.** Dette indgreb skal ske i henhold til en lovgivningsmæssig foranstaltning som opfylder kravene i direktivets artikel 15, stk. 1. Hvis der er tale om et alvorlig indgreb, skal materielle og processuelle betingelser sikre, at indgrebet er begrænset til sager om grov kriminalitet, jf. punkt 110-115 ovenfor i høringssvaret.

149. Politiets adgang til de lokaliseringsdata, som mobiludbyderne lagrer i 14 dage på frivillig basis i overensstemmelse med artikel 6 eller 9 i e-databeskyttelsesdirektivet, **vil med sikkerhed udgøre et alvorligt indgreb i rettigheder sikret af direktivet**, som fortolket i lyset af artikel 7 og 8 i Charter om Grundlæggende Rettigheder. Der er som nævnt ovenfor tale om meget detaljerede lokaliseringsdata, der kan afsløre de berørte personers vaner i dagligdagen, midlertidige eller varige opholdssteder, daglige eller andre rejser, hvilke aktiviteter der udøves, og de sociale miljøer, de frekventerer.

150. Lovforslaget bør derfor ændres, således at § 804 a omfatter enhver adgang til trafikdata og lokaliseringsdata som udgør et alvorligt indgreb efter EU-retten. Som nævnt i punkt 114 ovenfor er det primært adgang til oplysninger om civil identitet, der ikke udgør et alvorlig

32 Med nuværende gennemførelse af direktivet i dansk ret vil det være §§ 10-11 i BEK nr. 1882 af 04/12/2020 om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester og nummeruafhængige interpersonelle kommunikationstjenester.

indgreb.

Adgang til oplysninger om en bruger af en IP-adresse (edition)

151. Efter lovforslaget vil politiets adgang til oplysninger om en bruger af en IP-adresse fortsat ske efter den almindelige editionsregel i retsplejelovens § 804, selv om der er tale om behandling af trafikdata, som er registrerings- og opbevaringspligtige efter § 786 f.

152. Som anført ovenfor i punkt 73-88 i høringssvaret kan en generel og udifferentieret lagringspligt for tildelte IP-adresser kun ske med henblik på bekæmpelse af grov kriminalitet, og der skal være "strenge betingelser og garantier for så vidt angår brugen af disse data", jf. LQDN-dommens præmis 156.

153. Det vil som minimum forudsætte, at politiets adgang til oplysninger om en bruger af en IP-adresse sker via den foreslåede § 804 a i retsplejeloven med de ændringer, som er beskrevet i punkt 89-93 ovenfor i høringssvaret.

Adgang til oplysninger om mange personer (udvidet teleoplysning/masteoplysning)

154. 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, såsom de situationer, hvor vitale interesser for den nationale sikkerhed, forsvaret eller den offentlige sikkerhed er truet af terrorvirksomhed, 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.

155. EU-Domstolen gentager i præmis 50 af Prokuratuur-dommen kravet om, at der som udgangspunkt kun kan gives adgang til data vedr. mistænkte personer.

156. I retsplejelovens kapitel 71 giver bestemmelserne om udvidet teleoplysning i § 780, stk. 1, nr. 4 politiet adgang til at indhente oplysninger om hvilke telefoner inden for et nærmere angivet område der sættes i forbindelse med andre telefoner. Indhentningen (udvidet teleoplysning) vil både omfatte oplysninger om personer, der har været i området og kommunikeret med andre, samt hvem de har kommunikeret med via telefonsamtaler, SMS eller MMS.

157. Politiet kan også bruge editionsreglerne i retsplejeloven til at få adgang til oplysninger om alle personer, der har været i et bestemt område i et bestemt tidsrum[33] (hvis der er registreret lokaliseringsdata for dem, enten på baggrund af en logningspligt, mobiludbydernes frivillige lagring i 14 dage eller politiets hastesikring af sidstnævnte lokaliseringsdata i henhold til retsplejelovens § 786 a). Dette indgreb kaldes i et notat fra Teleindustrien

33 Jf. U.2017.1934Ø.

”udvidet masteoplysning”.[34]

158. I begge tilfælde sker der udlevering af oplysninger om ikke-mistænkte personer i betydelig omfang (alle personer i et bestemt område). Udvidet teleoplysning og udvidet masteoplysning er ikke begrænset til situationer hvor vitale interesser for den nationale sikkerhed, forsvaret eller den offentlige sikkerhed er truet af terrorvirksomhed, jf. kravene i præmis 119 i Tele2-dommen.

159. Når udvidet masteoplysning sker efter editionsreglerne, er indgrebet til rådighed for politiet i alle sager uden noget kriminalitetskrav eller andre materielle betingelser. Efter lovforslaget vil der være et kriminalitetskrav (i § 804 a), hvis udvidet masteoplysning sker mod lokaliseringsdata, der er hastesikret efter retsplejelovens § 786 a. Hvis indgrebet sker inden for 14 dage, kan politiet efter lovforslaget fortsat bruge § 804 uden kriminalitetskrav og uden beskikkelse af en forsvarer til at varetage interesserne for de mange berørte personer.

160. Det grundlæggende problem ved udvidet masteoplysning er dog ikke kriminalitetskravet, men at politiet efter præmis 119 i Tele2-dommen kun må få adgang til data vedr. mistænkte personer. Det samme problem gælder for udvidet teleoplysning.

Underretning af den registrerede, når oplysninger udleveres til politiet

161. Efter Tele2-dommen præmis 121 skal der ske underretning de berørte personer (hvis oplysninger politiet har fået adgang til), så snart underretningen ikke længere 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.

162. Efter gældende ret sker der kun underretning af den berørte person ved teleoplysning, hvor retsplejelovens § 788 indgår i betingelserne for indgrebet. Med lovforslaget vil der også ske underretning ved edition i det omfang at det sker efter den foreslåede § 804 a (registrerings- og opbevaringspligtige oplysninger).

163. Der vil efter lovforslaget fortsat ikke ske underretning af de(n) berørte person(er) ved udvidet teleoplysning og udlevering af oplysninger via den almindelige editionsbestemmelse i § 804. Der sker heller ikke underretning efter den foreslåede § 804 b.

164. Den manglende underretning i disse tilfælde er ikke i overensstemmelse med EU-retten, som generelt kræver underretning af de berørte personer, når virksomheder udleverer personoplysninger om dem til politiet,[35] idet en sådan underretning er en forudsætning for

34 Notat om logning og udlevering af teledata til politiet – juridiske emner (Teleindustriens forslag og ønsker til ændring og præcisering af gældende regler), Februar 2020 https://www.teleindu.dk/wp-content/uploads/2020/04/NOTAT-TI-notat-til-JM-og-RP-om-logning-og-udlevering-feb-2020.pdf

35 Med mulighed for udsættelse af underretningen indtil det ikke længere kan forstyrre den igangværende efterforskning.

udøvelsen af retten til effektive retsmidler i henhold til Charterets artikel 47.[36]

165. Mulighederne for at undlade underretning i retsplejelovens § 788, stk. 4 er desuden mere omfattende end hvad præmis 121 i Tele2-dommen (og EU-retten generelt) synes at tillade. Udover udsættelse af underretningen indtil det ikke længere kan skade en igangværende efterforskning, giver § 788, stk. 4 mulighed for helt at undlade underretningen, hvis hensynet til beskyttelse af fortrolige oplysninger om politiets efterforskningsmetoder eller omstændighederne i øvrigt taler imod underretning. IT-Politisk Forening er ikke bekendt med information om hvor ofte politiet (eller PET) gør brug af muligheden for helt at undlade underretning, da der ikke findes offentligt tilgængelige statistikker herfor.

Ændring af kriminalitetskravet for grov kriminalitet (adgang til lagrede oplysninger)

166. Efter EU-retten skal alvorlige indgreb i den grundlæggede ret til privatliv og databeskyttelse i forbindelse med kriminalitetsbekæmpelse være betinget af, at der er tale om grov kriminalitet. EU-retten har dog ingen fast definition af hvad der er ”grov kriminalitet”.

167. I retsplejeloven er en række indgreb betinget af, at der er tale om kriminalitet af en vis grovhed (kriminalitetskrav). For indgreb i meddelelseshemmeligheden, herunder teleoplysning, er udgangspunktet en strafferamme på fængsel i 6 år eller derover, samt en række af lovovertrædelser med strafferamme under 6 år, som af forskellige grunde er tilføjet. Der er samme kriminalitetskrav for telefonaflytning og teleoplysning.

168. Ved den seneste store revision af retsplejelovens regler om indgreb i meddelelseshemmeligheden i 1985 blev det primære kriminalitetskrav ændret fra en strafferamme på 8 år til 6 år. Begrundelsen for dette var, at Folketinget tidligere havde sænket strafferammen for en række forbrydelser. Det er IT-Politisk Forenings opfattelse, at strafferammerne generelt er blevet forhøjet siden 1985 med en række lovforslag om strafskærpelse, uden at det har givet anledning til at ændre kriminalitetskravet for indgreb i meddelelseshemmeligheden. Konsekvensen er at efterforskning af flere og flere lovovertrædelser giver mulighed for indgreb i meddelelseshemmeligheden, herunder teleoplysning.

169. Med lovforslaget ændres kriminalitetskravet til en strafferamme på fængsel i 3 år eller derover, og lovovertrædelser, der kan medføre strafskærpelse efter straffelovens § 81 a, bliver tillige omfattet af kriminalitetskravet uanset den oprindelige strafferamme. I retsplejelovens kapitel 71 vil det principielt kun gælde for teleoplysninger, som er omfattet en registrerings- og opbevaringspligt efter §§ 786 a – 786 e, men eventuelle oplysninger som ikke er undergivet en sådan pligt, vil uden videre kunne hastesikres, hvorefter de er omfattet af § 786 a. I praksis er det kriminalitetskravet for historisk teleoplysning (og udvidet teleoplysning) som sådan, der sænkes ganske betydeligt.

36 Jf. eksempelvis analysen af EU-retten i punkt i 320 i generaladvokatens forslag til afgørelse i C-311/18 Facebook Ireland og Schrems.

170. Det nye kriminalitetskrav vil også gælde i den foreslåede § 804 a i retsplejelovens kapitel 74 om edition. Her er der i dag ikke noget kriminalitetskrav, hvilket som anført tidligere i dette høringsvar er i strid med EU-retten, fordi editionsreglerne bruges til udlevering af oplysninger som udgør et alvorligt indgreb i grundlæggende rettigheder, eksempelvis udlevering af masteoplysninger (lokaliseringsdata).

171. Ændringen af kriminalitetskravet synes at være begrundet med, at logningen fremover bliver mere målrettet. I de almindelige bemærkninger pkt. 3.7.3.1 anføres det direkte, at "ordningen derfor, alt andet lige, [vil] være mindre indgribende, end det er tilfælde i dag." Det er en bemærkelsesværdig konklusion, når logningen reelt vil omfatte de samme personer og oplysninger som i dag, og politiet samtidig får lettere adgang til lagrede (historiske) teleoplysninger.

172. For edition af visse masteoplysninger (de logningspligtige) indføres der ganske vist et kriminalitetskrav, som indskrænker politiets adgang i forhold til gældende dansk ret. Denne ændring bringer imidlertid alene dansk ret i overensstemmelse med EU-retten. Idet alle retsanvendende myndigheder (herunder anklagemyndigheden) har en pligt til ikke at anvende danske retsbestemmelser i det omfang de strider mod EU-retten, bør denne indskrænkning af adgangen til masteoplysninger allerede være afspejlet i den aktuelle retspraksis.

173. En række EU-retsakter opererer med 3 år som grænsen for grov kriminalitet. På den baggrund har IT-Politisk Forening ingen grund til at betvivle, at en strafferamme på 3 år vil være i overensstemmelse med EU-retten. Det ændrer dog ikke ved, at det bør give anledning til betydelige retspolitiske overvejelser, at kriminalitetskravet sænkes i den danske retsplejelov for teleoplysning, ikke mindst i lyset af de hensyn, som har ført til fastsættelse af det nuværende kriminalitetskrav.

174. Derimod er det efter IT-Politisk Forenings opfattelse tvivlsomt, om den ganske omfattende liste af yderligere lovovertrædelser med en strafferamme på under 3 år (herunder enkelte lovovertrædelser uden for straffeloven) kan indgå i et kriminalitetskrav, som skal begrænse anvendelsen af alvorlige indgreb i meddelelseshemmeligheden til grov kriminalitet.

175. 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."*

176. Det forhold at flere gerningspersoner kommunikerer med hinanden, og at adgang til lagrede trafikdata 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.

177. Formålet med kriminalitetskravet er at begrænse anvendelsen af det alvorlige indgreb, som politiets adgang til følsomme trafikdata og lokaliseringsdata udgør, til alvorlige lovovertrædelser. Det skal sikre, at der er proportionalitet mellem på den ene side alvoren af den lovovertrædelse som efterforskes og på den anden side den krænkelse og ulempe for de berørte personer, som indgrebet uløseligt medfører. Hvis kriminalitetskravet omfatter næsten alle lovovertrædelser, hvor politiet erfaringsmæssigt ønsker at bruge trafikdata og lokaliseringsdata i efterforskningen, bliver denne begrænsning af anvendelsen af det alvorlige indgreb illusorisk. En begrænsning af politiets beføjelser begrundet i proportionalitet skal have en reel effekt.

Statistikker for politiets adgang til trafikdata og lokaliseringsdata

178. IT-Politisk Forening vil anbefale, at der i lovforslaget indføres et krav om at anklagemyndigheden skal udarbejde og offentliggøre årlige statistikker vedrørende politiets adgang til lagrede trafikdata og lokaliseringsdata.

179. Statistikken bør omfatte tal for antal sager, hvor politiet har fået adgang til trafikdata, opdelt på teleoplysninger, lokaliseringsdata og IP-adresser. Der bør laves en særskilt statistik for antal sager, hvor politiet anmoder om oplysninger om mange personer (udvidet teleoplysning og udvidet masteoplysning efter editionsreglerne) samt det gennemsnitligt antal berørte personer i disse sager.

180. Sådanne statistiske oplysninger vil være væsentlige for Folketinget og civilsamfundsorganisationer i forhold til at vurdere omfanget af statens indgreb i retten til privatliv og databeskyttelse. Fra 2013 til 2017 var der eksempelvis en stigning i antallet af indgreb med udvidet teleoplysning på hele 350% ifølge statistiske oplysninger fra anklagemyndigheden.

181. Rigsadvokaten udarbejder og offentliggør allerede en statistik for indgreb i meddelelseshemmeligheden. Denne statistik er siden 2019 desværre blevet langt mindre detaljeret end tidligere.[37] Derudover omfatter statistikken kun indgreb efter retsplejelovens kapitel 71, hvilket betyder at politiets adgang til lokaliseringsdata (masteoplysninger) og IP-adresser efter editionsreglerne ikke er omfattet af statistikken.

Immuniteter og privilegier (forholdet til tavshedspligt)

182. I de almindelige bemærkninger pkt. 3.10 overvejer Justitsministeriet, om der i retsplejeloven skal indsættes en særlig beskyttelse for personer undergivet nationale regler

37 De mere detaljerede statistiske oplysninger om eksempelvis teleoplysning og udvidet teleoplysning fordelt på kriminalitetstyper (som var i statistikken før 2019) kan stadig ses i besvarelser af REU spørgsmål, så IT-Politisk Forening formoder, at den statistiske optælling stadig finder sted.

om tavshedspligt (eksempelvis læger, advokater, præster og journalister) i forhold til registrering og opbevaring af trafikdata og lokaliseringsdata samt politiets muligheder for at få adgang til sådanne lagrede oplysninger.

183. I EU-Domstolens dom vedr. logningsdirektivet i 2014 blev det problematiseret, at dette direktiv ikke fastsatte nogle begrænsninger for personer undergivet nationale regler om tavshedspligt.[38] Det samme gjorde sig gældende for de nationale logningsregler i Tele2-dommen. I LQDN-dommen nævnes det endvidere i præmis 118, at logning kan have en afskrækkende virkning på whistleblowere, hvilket i sagens natur vil være særdeles uheldigt.

184. Justitsministeriet finder imidlertid ikke, at der er behov for en særlig beskyttelse af personer undergivet tavshedspligt. Det begrundes med, at det vil være vanskeligt at undtage disse personer fra logningen, og at teleoplysning efter gældende ret ikke kan siges at anfægte det særlige fortrolighedsforhold, som vidneudelukkelsesreglerne i retsplejelovens § 170 skal beskytte. I pkt. 3.10 er dette begrundet med, at teleoplysning ikke giver adgang til indholdet af kommunikationen, med henvisning til side 107 i betænkning 1023/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter.

185. Hertil vil IT-Politisk Forening anføre, at vurderingen af forholdet mellem metadata og indholdet af kommunikationen har ændret sig ganske væsentligt siden 1984. I dag er det den almindelige opfattelse, at lagring og adgang til metadata (som trafikdata og lokaliseringsdata) kan udgøre et lige så alvorligt indgreb som adgang til indholdet af kommunikationen, hvilket anerkendes af EU-Domstolen med præmis 99 i Tele2-dommen.[39]

186. Analyser af lagrede lokaliseringsdata kunne eksempelvis bruges til at afsløre en ukendt whistleblower, som har haft fysiske møder med en journalist, ved at samkøre lokationsprofiler for journalisten med tilsvarende profiler for de personer, som kunne være den "eftersøgte" whistleblower. Teleoplysning mod journalisten kan potentielt også bruges til dette formål. Retsplejeloven indeholder ingen særlig beskyttelse mod adgang til trafikdata og lokaliseringsdata i sådanne situationer. Hvis politiet anmoder om adgang til trafikdata og lokaliseringsdata der ikke er registrerings- og opbevaringspligtige, sker det (med lovforslaget) efter retsplejelovens § 804, hvor der ikke bliver beskikket en advokat, og hvor teleselskaberne typisk har afgivet afståelseserklæringer i forhold til eventuelle indsigelser.

Registrering og verificering af nummeroplysningsdata (118-databasen)

187. Efter den foreslåede ændring af telelovens § 31, stk. 2 skal nummeroplysningsdata for 8-cifrede abonnementsnumre (118-databasen) udvides med et unikt ID for abonnenten, som udgangspunkt CPR-nummer eller CVR-nummer (erhvervskunder). For personer uden CPR-

38 Digital Rights Ireland dommen (forenede sager C-293/12 og C-594/12), præmis 58.

39 Tidligere NSA General Counsel Stewart Baker har efter Snowden afsløringerne udtalt: "metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content." https://www.justsecurity.org/10318/video-clip-director-nsa-cia-we-kill-people-based-metadata/

nummer skal der i stedet registreres fødselsdato, statsborgerskab ved fødslen og køn, samt pasnummer eller tilsvarende for et civilt identitetskort.

188. Teleselskaberne skal desuden verificere abonnentens identitetsoplysninger inden de overføres til 118-databasen. Der stilles ikke krav om hvordan verificeringen skal foretages, men specielt for personer uden CPR-nummer vil det givetvis give anledning til betydelige byrder, fordi mange mobilabonnementer i dag sælges online, hvor forevisning af eksempelvis et pas ikke er en mulighed. Det gælder ikke mindst for taletidskort, se punkt 197-211 nedenfor.

189. Der vil endvidere være krav om efterregistrering af unikt ID for eksisterende mobilabonnementer, men ikke for eksisterede fastnetabonnementer, da denne opgave ville påføre to virksomheder en udgift på 125 mill. kr. ifølge AMVAB-målingen i pkt. 6.

190. Formålet med det unikke ID, og verificering af nummeroplysningsdata, er at der i videst muligt omfang kan ske en entydig identifikation af brugeren af et givet kommunikationsmiddel. De omfattende registersamkøringer, som skal udpege områder med forhøjet risiko for kriminalitet ud fra oplysninger om tidligere dømte personer m.v. (den foreslåede § 786 c, stk. 1 i retsplejeloven), vil givetvis også blive nemmere, hvis Rigspolitiet har direkte adgang til CPR-nummer for samtlige abonnenter.

191. Der er i lovforslaget ingen vurdering af mulige risici ved at registrere CPR-nummer eller et andet unikt ID i 118-databasen. Relevante risici omfatter blandt andet den altid aktuelle risici for databrud, hvor konsekvenserne vil blive langt større, når der er registreret CPR-nummer i 118-databasen. En anden væsentlig risiko er ”function creep”, hvor den registrerede sammenhæng mellem CPR-nummer og telefonnummer bruges af andre myndigheder end politiet, eller bruges af politiet til andre formål end tiltænkt med lovforslaget. Et eksempel på sidstnævnte ”function creep” kunne være integration af 118-databasen i POL-INTEL.

192. Mange mobilabonnementer bruges formentlig af en anden person end den registrerede abonnent i 118-databasen. En verificering af nummeroplysningsdata vil ikke i væsentligt grad ændre på dette. Hvis abonnenten er en virksomhed eller en forening, skal der registreres et CVR-nummer i 118-databasen, og til de automatiserede analyser vil det i praksis være ukendt hvem der er den egentlige bruger af abonnementet. Der er ganske vist mulighed for at registrere brugeren med et nyt felt i 118-databasen, hvis det er en anden person end abonnenten, men det gælder kun hvis oplysningen er kendt på registreringstidspunktet. I mange tilfælde vil denne oplysning ikke være kendt, eller den bliver hurtigt forældet, fordi en virksomhed overdrager mobilabonnementet til en anden person, eksempelvis en ny medarbejder.

193. Politiet er allerede i dag klar over, at deres målpersoner kan bruge andre telefonnumre end dem, som måtte være registreret i 118-databasen. En verificering af nummeroplysningsdata vil ikke i nævneværdig grad ændre på dette. Tilpas organiserede kriminelle vil oprette

skuffeselskaber eller foreninger og registrere abonnementer med CVR-nummer. Det sker sikkert allerede i dag, og politiet tager utvivlsomt højde for dette i deres efterforskning.

194. Med de mange omgåelsesmuligheder, og de ganske betydelige risici ved registrering af CPR-nummer i 118-databasen, er ulemperne efter IT-Politisk Forenings opfattelse langt større end de mulige fordele.

195. Sidst, men bestemt ikke mindst, finder IT-Politisk Forening det principielt forkert, at borgerne skal registreres hos staten som betingelse for at få "lov" til at kommunikere med hinanden via telefoni. Det fremgår imidlertid af de specielle bemærkninger til § 786 h, at der vil blive fastsat regler om, at udbyderne fremadrettet ikke må give slutbrugeren adgang til elektroniske kommunikationsnet eller -tjenester, før verificeringen er foretaget. Det er en nærmest absurd indskrænkning af borgernes frihedsrettigheder.

196. Det vil formentlig også være temmelig virkningsløst i forhold til de personer, hvis kommunikation politiet gerne vil overvåge, fordi der i dag findes et stort antal kommunikationstjenester udover telefoni (primært etableret i udlandet), hvor det ikke er muligt for staten at gennemtvinge en tilsvarende registrering og verificering af brugerne.

Registrering af taletidskort

197. Med hjemmel i den foreslåede § 786 h i retsplejeloven vil Justitsministeren endvidere udstede regler om registrering og verificering af brugere af taletidskort.

198. De nærmere detaljer for denne registrering er ikke fastlagt på nuværende tidspunkt, men vil antageligt fremgå af et kommende bekendtgørelsesudkast, når dette sendes i høring. For taletidskort kan registreringen og verificeringen blive ganske kompliceret, fordi mobiltelefoni med taletidskort typisk ikke sælges direkte fra teleudbyderne, men via kiosker, supermarkeder og andre mellemled (herunder automater i lufthavne), som generelt næppe vil have forudsætninger for at udføre den krævede registrering og verificering af slutbrugeren.

199. Det er endvidere uklart ud fra bemærkningerne i lovforslaget, om der skal ske efterregistrering af de eksisterende taletidskort. På dette punkt er der modstridende oplysninger i de specielle bemærkninger til § 786 h (side 190) og de almindelige bemærkninger pkt. 3.4.2 (side 73). Efterregistrering af taletidskort vil være en meget kompliceret opgave og givetvis forbundet med ganske betydelige udgifter. For taletidskort omtaler AMVAB-målingen kun den løbende administrative byrde ved registrering af nye taletidskort på 69 mill. kr. om året. **På den baggrund formoder IT-Politisk Forening, at der ikke skal ske efterregistrering af taletidskort (men det er som nævnt uklart i lovbemærkningerne).**

200. En arbejdsgruppe under Justitsministeriet har arbejdet med overvejelser om registrering af taletidskort siden 2006 uden at tidligere justitsministre har fundet anledning til at indføre en sådan 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.

201. 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 det særligt sikrede terminaludstyr (telefonen) kommer med egne SIM-kort, antageligt fra et land hvor der ikke er krav om individuel registrering af abonnenter for SIM-kort.

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

203. 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.

204. 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.

Konsekvenser for borgerne af registrering af taletidskort

205. 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 for de repressalier, som en sådan afsløre vil kunne medføre.[40]

206. 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

40 Dette er alene et hypotetisk eksempel. Enhver lighed med virkeligheden er aldeles utilsigtet.

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.

207. I et notat af 29. april 2021 med bemærkninger til lovskitsen for revision af logningsreglerne af 23. marts 2021 opfordrede IT-Politisk Forening til, at Justitsministeriet udarbejdede 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 med registrering af taletidskort blev fremsat.

208. Lovforslaget har imidlertid alene en analyse af de økonomiske byrder for udbydere af taletidskort, som er ganske betydelige (se næste punkt), samt en særdeles kortfattet kommentar i pkt. 7 (administrative konsekvenser for borgerne) om, at borgerne kan blive nødsaget til at verificere sig i nogle tilfælde ved fysisk fremvisning af tilstrækkelig identifikation eller ved online eller telefonisk angivelse af de relevante oplysninger. Der er ingen vurdering af hvor mange borgerne, der ikke vil være i stand til at opfylde dokumentationskravene, eller hvilke konsekvenser det vil have.

209. De økonomiske byrder for udbyderne af taletidskort er i øvrigt ganske betydelige. Ifølge AMVAB-målingen vil der være årlige udgifter på 69 mill. kr. ved salg af nye taletidskort. Antagelserne bag denne beregning fremgår ikke. Ifølge telestatistikken fra Energistyrelsen er der ultimo 2020 to udbydere af taletidskort som tilsammen har omkring 150.000 aktive taletidskort.

210. Hvis der eksempelvis hvert år sælges 100.000 nye taletidskort, vil der være en udgift på omkring 700 kr. for etablering af et ”abonnement” (for taletidskort), som i mange tilfælde vil være ganske kortvarigt, eksempelvis en turist fra et ikke-EU land der besøger Danmark. Disse udgifter kan markedet næppe bære, og den sandsynlige konsekvens er at udbyderne af taletidskort vil forlade det danske marked. De fleste udbydere af mobiltelefoni kræver, at abonnenten har et CPR-nummer, og de nye krav om registrering og verificering af slutbrugeren vil utvivlsomt forstærke den tendens, fordi verificering bliver meget besværlig for personer uden et dansk CPR-nummer. I værste fald kan konsekvensen blive, at personer uden et CPR-nummer mere eller mindre afskæres fra at bruge mobiltelefoni i Danmark (udover roaming med SIM-kort fra andre lande, hvis det er en mulighed).

211. IT-Politisk Forening skal derfor gentage opfordringen til Justitsministeriet om at foretage en grundig analyse af konsekvenserne, herunder de menneskeretlige aspekter, inden en eventuel bekendtgørelse om registrering af taletidskort sendes i høring.