JUSTITSMINISTERIET

Folketinget
Retsudvalget
1240 København K
DK Danmark

Dato: 18. november 2021
Kontor: Sikkerhedskontor II
Sagsbeh: NAT
Sagsnr.: 2020-187-0036
Dok.: 2174368

KOMMENTERET HØRINGSOVERSIGT

Forslag til lov om ændring af retsplejeloven og lov om elektroniske kommunikationsnet og -tjenester (Revision af reglerne om registrering og opbevaring af oplysninger om teletrafik (logning) m.v.) (L 93)

I. Hørte myndigheder og organisationer m.v.

Et udkast til lovforslag har i perioden fra den 27. september 2021 til den 25. oktober 2021 været sendt i høring hos følgende myndigheder og organisationer m.v.:

Advokatrådet, Andelsboligforeningernes Fællesrepræsentation, Amnesty International, Bitbureauet, Brancheforeningen Teleindustrien, Business Software Alliance Danmark, Campingrådet, CSC Danmark A/S, Danmarks Restauranter, Dansk Erhverv, Dansk Energi, Dansk IT, Dansk Journalistforbund, Dansk Magisterforening, Dansk Metal, Danske Advokater, Datatilsynet, Den Danske Dommerforening, DI, DI Digital, Dommerfuldmægtigforeningen, Domstolsstyrelsen, Forbrugerrådet TÆNK, Foreningen af Danske Internet Medier, Foreningen af Offentlige Anklagere, Hi3G Denmark ApS, HK-Landsklubben Danmarks Domstole, HK-Landsklubben for Politiet, HORESTA, Ingeniørforeningen IDA, Institut for Menneskerettigheder, IT-Branchen, IT-Politisk Forening, Justitia, KMD, Landsforeningen af Forsvarsadvokater, Lejernes LO, Politiets Efterretningstjeneste, Politiforbundet, PROSA, Retspolitisk Forening, Rigsadvokaten, Rigspolitiet, Rådet for Digital Sikkerhed, SAM-DATA (HK), samtlige byretter, SE/Stofa, Sø- og Handelsretten, TDC A/S, Telia A/S, Telenor A/S, Vestre Landsret og Østre Landsret.

Slotsholmsgade 10
1216 København K.

T +45 3392 3340
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Udkastet har desuden i perioden fra den 28. september 2021 til den 25. oktober 2021 været sendt i høring hos Danske Medier.

II. Høringssvarene

1. Indledning

Justitsministeriet har modtaget høringssvar fra:

Amnesty International, Brancheforeningen Teleindustrien, Citizen First, Dansk Journalistforbund, Dansk Magisterforening, Danske Advokater, Dansk Erhverv, Danske Medier, Datatilsynet, DI, Dommerfuldmægtigforeningen, Domstolsstyrelsen, Fiberby, Forbrugerrådet TÆNK, Forsikring og Pension, HORESTA, Ingeniørforeningen IDA, Institut for Menneskerettigheder, IT-Branchen, IT-Politisk Forening, Justitia, KLID, Københavns Byret på vegne af byretspræsidenterne, Politiforbundet, PROSA, Retspolitisk Forening, Rigsadvokaten, Rigspolitiet, Rådet for Digital Sikkerhed, Vestre Landsret og Østre Landsret,

Nedenfor er gengivet de væsentligste punkter i de modtagne høringssvar. Samtlige høringssvar er vedlagt.

Justitsministeriets kommentarer til høringssvarene er anført i *kursiv*.

Dommerfuldmægtigforeningen, Domstolsstyrelsen, Politiforbundet, Rigsadvokaten og **Rigspolitiet** har ingen bemærkninger til lovforslaget.

Københavns Byret har på vegne af landets byretspræsidenter meddelt, at byretterne ikke ønsker at udtale sig i anledning af udkastet.

Vestre Landsret og Østre Landsret ønsker ikke at udtale sig i anledning af udkastet.

2. Generelt

Amnesty International (Amnesty) byder initiativet til at gennemføre nye regler for logning af teledata velkommen. Amnesty har gentagne gange kritiseret den nuværende logningsordning for at være i strid med menneskerettighederne. En generel og uddifferentieret logning af hele befolkningen er

et omfattende og alvorligt indgreb i retten til respekt for privatliv, beskyttelse af personoplysninger samt ytrings- og informationsfriheden. Det går ud over, hvad der er strengt nødvendigt eller proportionalt til brug for kriminalitetsbekæmpelse eller beskyttelse af statens sikkerhed, og er dermed i strid med internationale menneskerettighedstandarder. Amnesty finder det yderst kritisabelt, at regeringen med det længe ventede lovforslag fremlægger en logningsmodel, der i stor grad vil give mulighed for at videreføre den nuværende ulovlige retstilstand.

Dansk Erhverv og **IT-Branchen** bemærker, at nye logningsregler bør skabe klarhed og forudsigelighed på området, og at tiltagene skal være proportionale, således at de konkrete indsamlinger og anvendelsen af disse stemmer overens med formålet med indsatsen. Ligeledes bør det være tilstrækkeligt godtgjort, at reglerne ligger inden for EU-rettens rammer. Imidlertid mener parterne ikke, at lovforslaget lever op til disse grundlæggende krav. Justitsministeriet vurderer således selv, at der er en betydelig procesrisiko forbundet med at give politiet og anklagemyndigheden adgang til trafikdata, der er registreret og opbevaret med henblik på at beskytte den nationale sikkerhed, til brug for politiets og anklagemyndighedens bekæmpelse af grov kriminalitet. Der vil således fortsat være usikkerhed om grundlaget for de tiltag, som myndighederne kræver af teleselskaberne. Parterne bemærker desuden, at en stor offentlig satsning på mobil- og internetovervågning vil have som en uønsket bivirkning, at der vækkes mistillid til danskernes mulighed for privat og uovervåget anvendelse af telekommunikationsmidler. Dansk Erhverv og IT-Branchen støtter i øvrigt de specifikke kommentarer i Teleindustriens høringssvar.

Dansk Journalistforbund (DJ) anerkender, at det er et helt legitimt ønske at ville styrke efterforskningen og retsforfølgningen af strafbare forhold. Fra DJ's side er man imidlertid generelt kritiske over for den meget massive overvågning, som logningen indebærer. DJ er generelt imod overvågning af store områder og store grupper af helt uskyldige borgere, som ikke er i nærheden af at begå kriminelle handlinger. DJ er desuden ikke overbevist om, at den efterforskningsmæssige nytteværdi af logningen kan opveje de principielle problemer med overvågning og de praktiske risici ved opbevaring af store datamængder. Til sidstnævnte risici hører ikke mindst risikoen for læk og udsivning af fortrolige oplysninger.

Dansk Magisterforening (DM) anfører, at dele af Justitsministeriets foreslåede ordning reelt vil medføre opretholdelse af den nuværende tilstand,

hvor kriminalitetsbekæmpelse kan legitimere en generel og udifferentieret logning af alle borgeres telefonsamtaler. Da flere EU-domme har slået fast, at systematisk og ubegrænset indsamling af teledata er i strid med EU's regler og udgør en krænkelse af retten til fri kommunikation og privatliv, kan DM ikke tilslutte sig denne del af lovforslaget. DM anerkender, at politiet skal have gode efterforskningsmuligheder i forbindelse med grov kriminalitet og terrortrusler, men DM mener, at det er uacceptabelt, at der opretholdes en tilstand, hvor der indsamles oplysninger om alle danskere. DM anbefaler på det kraftigste, at der findes en løsning med målrettet logning, hvor der alene foretages logning af konkrete personer, som politiet har en rimelig formodning om, er involveret i alvorlig kriminalitet eller terror.

Danske Advokater bemærker, at ændring af logningsreglerne er et nødvendigt tiltag for at bringe de danske regler i overensstemmelse med EU-retten. Danske Advokater anerkender ministeriets udfordring med at balancere hensynene til effektiv efterforskning af kriminalitet og varetagelse af national sikkerhed mod henholdsvis sikring af slutbrugernes grundlæggende rettigheder og udbydernes praktiske forpligtelser til at bistå politiet. Danske Advokater ser imidlertid med stor bekymring på de nye logningsregler, idet lovforslaget i den nuværende form indebærer en betydelig risiko for, at Danmark overtræder EU-retten i forhold til slutbrugernes grundlæggende rettigheder. Endvidere er det bekymrende, at lovforslaget i den nuværende form er særdeles byrdefuldt for teleselskaberne, som pålægges meget store omkostninger og administrativt arbejde med henblik på at implementere og gennemføre logning efter de nye logningsregler. Danske Advokater anfører, at hvis lovforslaget bliver vedtaget i sin nuværende form, risikerer man at få et uproportionalt "overvågningssamfund" – særligt i de større byer. Det skyldes, at forslaget indebærer, at undtagelsen om generel og udifferentieret logning gøres til hovedreglen.

Danske Medier finder det positivt, at regeringen nu tager skridt til at revidere de danske logningsregler som følge af flere afgørelser fra EU-Domstolen. Foreningen finder det vigtigt, at regler om logning sikrer en fornøden balance mellem beskyttelse af borgernes privatliv og personoplysninger og på den anden side statens sikkerhed og effektiv kriminalitetsbekæmpelse. Dette er navnlig afgørende, når det skal overvejes, hvorvidt myndighederne kan få adgang til de loggede trafikdata.

Datatilsynet bemærker, at de foreslåede logningsregler – selv om der lægges op til en indskrænkning i forhold til de gældende regler – fortsat må

forventes at indebære behandling af store mængder personoplysninger. Det er således Datatilsynets vurdering, at de foreslåede logningsregler kun bør indføres, hvis vægtige samfundsmæssige hensyn taler derfor. I sidste ende må dette bero på en politisk vurdering af, om de samfundsmæssige hensyn, som lovforslaget tilsigter at varetage, har en sådan karakter, at lovforslaget skal fremsættes i sin nuværende form.

DI vurderer, at lovforslaget er for omfattende, komplekst, omkostningsfuldt og med en for hastig ikrafttrædelse. Flere af disse forhold vil kunne forbedres, og DI vurderer, at en udsættelse af ikrafttrædelsen er vigtig, da der er tale om en omfattende omstilling. Behovet for at sikre politiet gode redskaber er helt forståeligt, men det er vigtigt, at der samtidig tages hensyn i forhold til erhvervslivet, og en sådan balance synes ikke at være helt opnået i nærværende forslag.

Fiberby anfører, at de generelt er enige med Teleindustrien og IT-Politisk Forening i deres kommentarer til lovudkastet, og de henviser til disse høringssvar for så vidt angår de mere generelle bemærkninger.

Forbrugerrådet TÆNK bemærker, at de støtter Rådet for Digital Sikkerheds høringssvar.

Forsikring og Pension bemærker, at Forsikring og Pension står uforstående over for, at Justitsministeriet har undladt at gøre Forsikring og Pension til høringspart. Forsikring og Pension har en reel interesse for området, og der er tale om dataadgang, som kan have stor indflydelse på deres medlemmers mulighed for at smidiggøre sagsgangen for selskaberne i forbindelse med potentielle sager om forsikrings- og pensionssvindel.

KLID henholder sig til høringssvaret indsendt af IT-Politisk Forening.

Justitia finder det positivt, at Justitsministeriet nu er i gang med den nødvendige lovrevision af logningsreglerne. Lovudkastet giver dog på en række punkter tænketanken anledning til bekymring. Justitia er opmærksom på, at logningsreglerne indebærer en vanskelig afbalancering mellem navnlig hensynene til effektiv kriminalitetsbekæmpelse, herunder terror, på den ene side og respekten for grundlæggende rettigheder på den anden side. Dele af lovudkastet indebærer imidlertid risiko for, at den nuværende (ulovlige) retstilstand de facto opretholdes, hvorved krænkelsen af privatlivets fred og retten til persondatabeskyttelse vil fortsætte.

Ingeniørforeningen IDA (IDA) anerkender, at politiet som led i kriminalitetsforebyggende indsatser og efterforskning skal have adgang til og mulighed for at anvende værktøjer, der er tidssvarende. IDA mener dog, at lovforslaget i sin helhed er alt for vidtrækkende i forhold til proportionalitetsprincippet. IDA kan derfor ikke bakke op om lovforslaget. IDA finder det desuden uacceptabelt, at Justitsministeriet ikke arbejder for at sikre danske borgeres grundlæggende rettigheder, men tværtimod holder fast i en tvivlsom praksis og efter eget udsagn løber en "væsentlig procesrisiko" i forhold til EU-Domstolens afgørelser.

Institut for Menneskerettigheder (IMR) bemærker, at bekæmpelse af terrorisme og alvorlig kriminalitet er af særdeles stor væsentlighed, og at det er nødvendigt, at politiet har de fornødne redskaber til at bekæmpe det, men at dette naturligvis skal ske inden for rammerne af Danmarks internationale forpligtelser. Lovudkastet skal efter instituttets opfattelse ændres på flere områder for at være i overensstemmelse med EU-retten.

IT-Politisk Forening anfører, at den nuværende generelle og udifferentierede logning, som strider mod EU-retten, vil fortsætte. Lovforslaget medfører ingen reelle ændringer på dette punkt. Formelt sker logningen 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. IT-Politisk Forening anfører desuden, at en "værktøjskasse" til politiet, som består af hastesikring (som den foreslåede § 786 a), en reelt målrettet logning af trafikdata (som den foreslåede § 786 d) og eventuelt en generel og udifferentieret logningspligt for tildelte IP-adresser (som den foreslåede § 786 f, men begrænset til efterforskning af grov kriminalitet) sikrer en passende balance mellem hensynet til politiets efterforskningsmuligheder og det alvorlige indgreb i borgernes grundlæggende ret til privatliv, databeskyttelse og ytringsfrihed, jf. artikel 7, 8 og 11 i EU's Charter om Grundlæggende Rettigheder (Chartret), som er uløseligt forbundet med en logningspligt for teleudbydere.

PROSA bemærker, at forbundet har forståelse for, at det kan være nødvendigt at overvåge mistænkte for at kunne fange kriminelle. Men dette bør kun ske i begrænset omfang, og det bør som udgangspunkt ske med retskendelse.

PROSA anfører endvidere, at der med forslaget er tale om for megen overvågning af uskyldige og om en teknologi, der kan bruges til at undertrykke befolkningen, hvis den falder i de forkerte hænder.

Retspolitisk Forening bemærker, at foreningen finder det uforsvarligt, at den udøvende magt lægger op til, at landets lovgivende magt skal løbe en betragtelig procesrisiko. Foreningen anfører, at den ikke kan anbefale vedtagelse af lovforslaget i dets nuværende form. Den foreslåede ordning ville placere Danmark i toppen internationalt set af overvågningsramte lande, uden at kriminalitetsstatistik eller terrortrusselsituationen kan siges at fordre det. Politiet og domstolene skal have pålidelige og dækkende oplysninger at arbejde med, så rette skyldige kan blive dømt og uskyldige gå fri. Men foreningen finder det uacceptabelt, at snart sagt alle og enhver skal mistænkeliggøres og overvåges. Det er en grundlæggende del af at leve i et frit land, at man kan bevæge sig frit omkring og ringe og SMS'e til, hvem man har lyst til, uden at staten skal vide besked.

Rådet for Digital Sikkerhed (RfDS) bemærker, at det er positivt, at regeringen lægger op til at bringe de danske logningsregler i overensstemmelse med EU-retten og begrænse den generelle og udifferentierede logning til situationer, hvor der er en reel og aktuel eller forudsigelig trussel mod den nationale sikkerhed. Logning skal imidlertid ses i lyset af, at politiet allerede foretager en betydelig opsamling af og/eller har adgang til data om borgerne, som f.eks. omfattet opsamling af nummerplader (ANPG), adgang til privates overvågningsoptagelser og adgang til DNA-oplysninger hos Nationalt Genomcenter. Fælles for disse tiltag er, at der opsamles store datamængder om danskere, som ikke er i politiets søgelys. Det er vigtigt, at der foretages afvejning af proportionaliteten hver gang, der skal ske indgreb i og begrænsning af borgernes fundamentale rettigheder. Der er ikke nogen tvivl om, at politiets muligheder for at efterforske kriminalitet er af stor betydning for borgernes tryghed og borgernes fundamentale rettigheder til sikkerhed og retfærdighed, men RfDS finder det beklageligt, at regeringen ikke tillægger borgernes ret til databeskyttelse nogen vægt og alene lægger op til at begrænse den generelle og udifferentierede logning, som har karakter af masseovervågning, fordi det følger af EU-domstolens afgørelser. RfDS bemærker, at når borgerne har en følelse af at være overvåget, kan dette resultere i en tilbageholdenhed i at udøve andre rettigheder som f.eks. retten til at ytre sig eller forsamle sig.

Justitsministeriet henviser til pkt. 2 i lovforslagets almindelige bemærkninger, hvoraf det bl.a. fremgår, at indhentelse af registrerede og opbevarede oplysninger om teletrafik er et centralt efterforskningsværktøj for politiet i forbindelse med efterforskningen af kriminalitet, ligesom det kan være afgørende for anklagemyndighedens muligheder for strafforfølgning ved domstolene. Det gælder bl.a. i en række sager om grov kriminalitet, herunder i sager om bandekriminalitet, drab, narkotikakriminalitet og terrorisme. Politiet anvender oplysninger fra udbydere af elektroniske kommunikationsnet eller -tjenester (udbydere), jf. telelovens § 2, nr. 1, på forskellige stadier af efterforskningen. I den indledende fase kan det navnlig være aktuelt at analysere oplysninger om relevante personers kommunikationsmønstre og færden. Det gør det muligt at målrette den efterfølgende efterforskningsmæssige indsats, herunder udelukke personer, der ikke har relevans for sagen, fra efterforskningen. Oplysninger registreret og opbevaret af udbyderne kan navnlig være med til at målrette politiets indsamling af andre beviser på et tidligt stadie af efterforskningen, f.eks. for hurtigt at finde og identificere en ellers ukendt gerningsmand. I tilfælde hvor den formodede gerningsmand er kendt af politiet, men forsvundet, kan trafikdata også bidrage til at opspore den mistænkte. En analyse af indhentede oplysninger fra udbyderne kan også resultere i nye spor i efterforskningen eller kaste lys over andre forhold, der gør det nødvendigt at indhente yderligere oplysninger fra udbyderne. Ved efterforskning i lukkede, kriminelle miljøer, f.eks. i sager vedrørende organiseret narkotika- eller bandekriminalitet, kan oplysninger registreret og opbevaret af udbyderne bidrage til, at mistænkte kan kædes sammen, og at kriminelle netværk optrevles. På tilsvarende vis anvendes oplysninger fra udbyderne til at afkræfte, om mistænkte har relationer til kriminelle netværk eller grupperinger.

Det fremgår i forlængelse heraf, at det er af afgørende betydning for regeringen at sikre, at politiet har de efterforskningsredskaber, der skal til for at kunne bekæmpe kriminalitet og sikre borgernes tryghed, og for at anklagemyndigheden kan strafforfølge tiltalte ved domstolene. Regeringen foreslår på den baggrund en revision af reglerne om registrering og opbevaring af teletrafik m.v., der i videst muligt omfang skal medvirke til at sikre, at trafikdata m.v. fortsat kan anvendes til effektiv kriminalitetsbekæmpelse. Den foreslåede revision vil alt andet lige medføre, at politiet ikke får adgang til den samme mængde data som i dag. Revisionen bidrager imidlertid til at sikre en så effektiv kriminalitetsbekæmpelse på baggrund af registrerede og opbevarede oplysninger som muligt inden for rammerne af EU-retten.

Justitsministeriet bemærker desuden, at der med lovforslaget lægges op til at ophæve den gældende retsplejelovs § 786, stk. 4, og logningsbekendtgørelsen, som er udstedt i medfør heraf. Den generelle og udifferentierede registrering og opbevaring af teletrafik, som i dag sker med hjemmel heri, vil således ikke kunne fortsætte.

I stedet lægges der bl.a. op til at indføre en todelt ordning for registrering og opbevaring af trafikdata. For det første foreslås en ordning, hvorefter Rigspolitiet meddeler udbydere pålæg om at foretage målrettet personbestemt og geografisk registrering og opbevaring af trafikdata, jf. de foreslåede §§ 786 b-786 d i retsplejeloven. For det andet foreslås en ordning med generel og udifferentieret registrering og opbevaring af trafikdata, hvorefter justitsministeren bemyndiges til efter forhandling med erhvervsministeren at kunne fastsætte regler, der pålægger udbydere at foretage generel og udifferentieret registrering og opbevaring 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 antages at være reel og aktuel eller forudsigelig (generel og udifferentieret registrering og opbevaring), jf. den foreslåede § 786 e i retsplejeloven. Registrerings- og opbevaringspligten efter den foreslåede § 786 e vil skulle udmøntes ved bekendtgørelse, og registreringspligten vil højst kunne fastsættes for en periode på 1 år ad gangen.

Udgangspunktet for den foreslåede todelte ordning for registrering og opbevaring af trafikdata er den målrettede registrering og opbevaring. Der vil alene kunne fastsættes midlertidige regler om generel og udifferentieret registrering og opbevaring af trafikdata, hvis det vurderes, at der foreligger en alvorlig trussel mod den nationale sikkerhed.

Retshåndhævende myndigheder vil fortsat skulle indhente en retskendelse for at opnå adgang til bl.a. de trafikdata, der registreres og opbevares efter de foreslåede §§ 786 a-786 e i retsplejeloven. Hertil kommer, at det efter lovforslaget fremadrettet alene vil være muligt for de retshåndhævende myndigheder at få adgang til trafikdata m.v., der registreres og opbevares efter de foreslåede §§ 786 a-786 e i retsplejeloven, hvis det sker med henblik på efterforskning eller retsforfølgning af grov kriminalitet. I dag er det muligt at opnå adgang til oplysninger, der registreres og opbevares i medfør af regler udstedt efter retsplejelovens § 786, stk. 4, med henblik efterforskning eller retsforfølgning af alle former for kriminalitet.

Justitsministeriet bemærker herudover, at der med lovforslaget lægges op til at videreføre de gældende krav til beskyttelse af bl.a. registrerings- og opbevaringspligtige oplysninger, jf. pkt. 3.1.1.3 i lovforslagets almindelige bemærkninger. Behandling af personoplysninger for politiet vil desuden være underlagt henholdsvis Datatilsynets og Tilsynet med Efterretningstjenesternes tilsyn.

For nærmere om den foreslåede ordning med målrettet registrering og opbevaring af trafikdata henvises til pkt. 3 i den kommenterede høringsoversigt.

For nærmere om den foreslåede ordning med generel og udifferentieret registrering og opbevaring af trafikdata henvises til pkt. 4 i den kommenterede høringsoversigt.

For nærmere om den i lovforslaget nævnte væsentlige procesrisiko henvises til pkt. 12 i den kommenterede høringsoversigt.

For nærmere om ikrafttræden og implementering af lovforslaget henvises til pkt. 15 i den kommenterede høringsoversigt.

For nærmere om de administrative omkostninger for erhvervet henvises til pkt. 16 i den kommenterede høringsoversigt.

Endelig skal Justitsministeriet beklage, at Forsikring og Pension ikke var på høringslisten i forbindelse med høringen over lovforslaget. Ministeriet har noteret sig, at Forsikring og Pension ønsker at være høringspart over lovforslag, der vedrører reglerne om registrering og opbevaring af trafikdata m.v. Justitsministeriet takker i øvrigt for høringssvaret fra Forsikring og Pension, som Justitsministeriet – ligesom de andre indkomne høringssvar – adresserer i nærværende kommenterede høringsoversigt.

3. Målrettet registrering og opbevaring af trafikdata

Brancheforeningen Teleindustrien (TI) opfordrer til, at der ikke indføres danske særregler om målrettet logning, men at det sikres, at de nye regler om målrettet logning ligger inden for EU-rettens rammer.

TI bemærker i relation til målrettet personbestemt logning, at lovudkastet kan læses sådan, at teleudbyderne skal iværksætte målrettet personbestemt

logning baseret på oplysningen om en persons identitet (f.eks. navn og adresse eller CPR). Men overblikket over sammenhængen mellem, hvilke personer der abonnerer på hvilke telefonnumre findes i 118-databasen, som kun politiet har adgang til. TI opfordrer til, at det præciseres i lovforslaget, at politiet skal oplyse de telefonnumre, der skal iværksættes målrettet personbestemt logning for, så der er fuldstændig klarhed om, hvordan logning skal iværksættes, og med henblik på at sikre, at der ikke efterfølgende opstår tvivl om omfanget af teleudbydernes praktiske bistand til politiet. TI opfordrer konkret til, at det nævnes i både selve lovteksten i de nye § 786 b og § 786 d og i bemærkningerne hertil, at teleudbydernes iværksættelse af målrettet personbestemt logning skal ske efter politiets pålæg om, hvilke telefonnumre der er omfattet af indgrebet.

Herudover anfører TI, at ordlyden af de foreslåede bestemmelser i § 786 b, stk. 4, nr. 2 og 3, ikke er hensigtsmæssig, da det ikke er personen, der genererer trafikdata, men derimod den elektroniske kommunikation. TI foreslår, at der i stedet skrives "… trafikdata fra telefonnumre eller kommunikationsapparater (imei), der benyttes af personer, der har været genstand for indgreb [i meddelelseshemmeligheden]".

Det bemærkes desuden, at det efter TI's opfattelse ikke er korrekt som anført i den foreslåede bestemmelse i § 786 b, stk. 4, nr. 4, at politiets adgang til trafikdata efter § 786, stk. 2, er et "indgreb". § 786, stk. 2, omfatter derimod den situation, hvor en person giver samtykke til politiets adgang til trafikdata. TI foreslår desuden, at det præciseres i lovudkastet på side 164, at et samtykke til målrettet personbestemt logning skal være et selvstændigt samtykke, da det skal være muligt at give samtykke til udlevering, uden at der samtidig gives samtykke til overvågning – og omvendt.

TI anfører for så vidt angår målrettet geografisk logning, at lovudkastet kan læses sådan, at teleudbyderne skal iværksætte målrettet geografisk logning både for mobiltelefoner, der benytter masterne i et område, og for fastnettelefoner med installationsadresser i området. Men målrettet geografisk logning for fastnettelefoner har ikke været en del af den forudgående tekniske afklaring, og modsat mobilområdet findes der ikke it-løsninger, der giver fastnet-operatørerne et samlet overblik over, hvilke fastnet- og ip-telefoner der findes i et geografisk område. TI opfordrer til, at regler om geografisk målrettet logning som hidtil forudsat kun omfatter mobiltjenester (oplysninger om, hvilke mobiltelefonnumre der benytter mobilmasterne, som dækker et fokusområde).

Såfremt Justitsministeriet overvejer at indføre regler om, at målrettet geografisk logning også skal omfatte fastnettelefoni og IP-telefoni, opfordrer TI til, at der forinden nedsættes en arbejdsgruppe med deltagelse af Rigspolitiet, Rigsadvokaten og telebranchen til nærmere analyse af politiets eventuelle behov og løsningsmodeller for adgang til geografisk loggede trafikdata om fastnet- og IP-telefoni med installationsadresser i et fokusområde.

TI gør i øvrigt opmærksom på, at det ikke har indgået i den erhvervsøkonomiske analyse (AMVAB), at geografisk målrettet logning også skulle omfatte fastnet- og IP-telefonitjenester. Da der som nævnt ikke eksisterer systemer, der kan håndtere geografisk målrettet logning af fastnetforbindelser, vil den i lovforslaget angivne og allerede særdeles væsentlige erhvervsøkonomiske byrdevurdering skulle opjusteres betragteligt.

TI gør desuden opmærksom på, at antallet af fastnet- og IP-telefonikunder kun udgør kun ca. 8 pct. af alle telefoniabonnementer i Danmark, og at antallet af fastnet- og IP-telefoniabonnementer faldt fra andet halvår 2019 til andet halvår 2020 med 26,8 pct. (Energistyrelsens Telestatistik for 2. halvår 2020). Set i lyset af det begrænsede antal fastnet- og IP-telefoniabonnementer begrunder Justitsministeriet selv på side 138 i lovudkastet, at indsamlingen af unikt ID for eksisterende fastnet- og IP-telefonikunder har begrænset efterforskningsmæssig værdi. I dette lys opfordrer TI til, at det nøje undersøges, hvilken efterforskningsmæssig værdi målrettet geografisk logning af fastnet- og IP-telefoner vil have set i forhold til de omstillingsomkostninger og administrative byrder en sådan forpligtelse vil have for teleudbyderne.

Dansk Erhverv og IT-Branchen anfører, at lovforslagets muligheder for at iværksætte målrettet logning er så omfattende, at grænsen til generel logning udviskes. For borgere, der ofte befinder sig på befærdede steder, vil det være reglen nærmere end undtagelsen, at der logges teletrafikdata fra deres mobiltelefon.

Danske Advokater anfører, at det er foreningens vurdering, at der, med de foreslåede regler, er en risiko for, at generel og udifferentieret logning kommer til at udgøre hovedreglen og ikke den begrænsede undtagelse. En sådan praksis vil være i strid med EU-retten. Det er bl.a. tilfældet, idet den målrettede logning er så bred, at der kan sås væsentlig tvivl om, hvorvidt målretningen i sig selv eller de enkelte målrettede logningstemaer tilsammen er så omfattende, at de reelt udgør generel og udifferentieret logning.

Fiberby anfører i relation til den foreslåede § 786 d, at Fiberby ikke kan identificere kommunikationsudstyr, som ikke er direkte tilkoblet deres netværk.

IDA er i princippet er indforstået med, at det kan være et væsentligt middel til en succesfuld efterforskning, at afgrænsede geografiske områder eller udvalgte kriminaliserede grupper logges i et begrænset tidsrum. IDA er dog kritisk over for den måde, hvorpå målrettet personbestemt og geografisk logning foreslås implementeret i nærværende lovforslag. Det skyldes dels, at de foreslåede løsninger teknisk ikke synes muligt uden store investeringer, dels at lovforslaget generel er udtryk for et skred i opfattelsen af, hvornår logning af trafikdata skal bruges som middel.

IDA bemærker desuden, at hvis geografisk målrettet logning skal foregå, kræver det, at Justitsministeriet sammen med telebranchen finder en bedre og langt mere specifikt målrettet løsning, eller at man kun gennemfører geografisk logning i særlige situationer for en kort, afgrænset tidsperiode. Alternativt bør geografisk målrettet logning droppes som en mulighed. IDA anfører i den forbindelse, at der også for så vidt angår geografisk målrettet logning sker et skred mod generel og udifferentieret logning i forhold til tidligere intentioner. Det er således oplyst til Information, at forslaget vil føre til logning af 15-20 pct. af Danmarks samlede areal, hvilket svarer til hele Sjælland eller ca. 3 mio. borgere.

Herudover bemærker IDA, at det af pkt. 3.1.3.3 i de almindelige bemærkninger til lovforslaget anføres, at enkeltpersoner, der vurderes at være nære kontakter til mistænkte, der har været aflyttet for grov kriminalitet, også kan logges. I forslaget er disse nære kontakter eksemplificeret ved "ægtefæller eller samlevere". Eftersom lovforslaget skriver "f.eks.", må det antages, at ægtefæller og samlevere ikke udgør en fuldstændig liste. IDA finder det nødvendigt, at det tydeligt fremgår af loven, hvem der defineres som "nærkontakt".

IMR bemærker, at ministeriet med lovudkastet lægger op til, at der skal fastsættes pligt til målrettet geografisk logning i områder på 3 km gange 3 km forudsat, at der er et øget kriminalitetsbillede i det pågældende område, og på en lang række særligt sikringskritiske områder bl.a. trafikknudepunkter og større indfaldsveje (lovudkastets forslag til en ny § 786 c i retsplejeloven). Der er efter instituttets opfattelse en risiko for, at den målrettede

geografiske logning kan gå hen og blive så omfattende, at den de facto må anses for at være generel og udifferentieret, idet der bl.a. er tale om nogle ganske lave krav til, at der i et forholdsvis stort område fastsættes pligt til at foretage logning, som omfatter alle elektroniske kommunikationsmidler og samtlige trafikdata fra alle abonnenter og registrerede brugere, der befinder sig i området. Lovudkastet tager imidlertid ikke højde for denne risiko, idet pligten til at logge i områder af 3 km gange 3 km ikke er underlagt nogen proportionalitetsvurdering, men alene foretages på baggrund af en årlig vurdering af det aktuelle kriminalitetsbillede (lovudkastets bemærkninger til lovforslagets § 1, nr. 9). Instituttet anbefaler, at Justitsministeriet i lovudkastet sikrer, at målrettet geografisk logning ikke får et omfang, som de facto må anses for generelt og udifferentieret.

IT-Politisk Forening bemærker, at teleselskaberne skal indrette deres systemer, således at der med kort varsel kan foretages en overgang fra generel og udifferentieret logning til målrettet logning.

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

Herudover anfører foreningen, at 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.

Det er IT-Politisk Forenings klare opfattelse, at La Quadrature du Net-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 personen. En målrettet logning, som omfatter over halvdelen af befolkningen, kan ikke med rimelighed siges at opfylde de krav, som EU-Domstolen opstiller. 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. de foreslåede § 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.

Foreningen bemærker desuden, at det i den forbindelse er 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. IT-Politisk Forening vil derfor anbefale, at de foreslåede §§ 786 b og 786 c udgår af lovforslaget, og at den målrettede logning alene baseres på den foreslåede § 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.

IT-Politisk Forening bemærker også, at 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. 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.

Endelig anfører foreningen, at 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.

Justitia bemærker, at særligt rammerne for den foreslåede målrettede geografiske logning forekommer så vide, at der de facto vil blive tale om generel logning. Justitia ønsker at understrege, at det er afgørende, at kriterierne for målrettet logning ikke får en sådan karakter, at logningen de facto bliver generel som hovedregel. Det bør i den forbindelse nøje overvejes, om kriterierne i den foreslåede § 786, stk. 1 og 2, samlet set reelt vil medføre, at så store dele af landet underlægges logning, at logningen ikke længere kan anses målrettet. Dette vil ifølge Justitias vurdering være i strid med EU-Domstolens praksis.

Justitia bemærker herudover i relation til den foreslåede § 786 d (om konkret begrundet målrettet logning), at der med lovforslagets krav om, at der skal være "grund til at antage", at der eksisterer en forbindelse til grov kriminalitet, fastsættes et lavere krav end det, der gælder for at foretage telefonaflytning. Justitia er enig i, at det kan være legitimt at iværksætte logning over for en person, der er i kontakt med miljøer, hvor der begås grov kriminalitet, men det bør sikres, at kriteriet om, hvornår der kan antages at være en forbindelse til grov kriminalitet, afgrænses tilstrækkeligt, herunder at der ikke gives adgang til, at enhver person, der har været i en hvilken som helst form for kontakt med en, der engang er blevet aflyttet, kan gøres til genstand for logning. De nærmere kriterier for vurderingen af, om der kan antages at bestå en forbindelse til grov kriminalitet – og hvad denne forbindelse skal bestå i – fremstår efter Justitias opfattelse ikke tilstrækkeligt klare i lovudkastet.

PROSA bemærker, at når man har udstået sin straf, skal man behandles som en uskyldig og naturligvis ikke overvåges. PROSA anfører, at forbundet kan se en rimelighed i at give en dommer mulighed for at kunne idømme frihedsberøvelse og privatlivsberøvelse i den kombination, som dommeren finder mest formålstjenstligt. Men dette skal ikke ske per automatik.

PROSA anfører endvidere, at forbundet er modstander af at logge folk, der ikke er under mistanke, og at det også gælder, når det sker baseret på geografi. Ønsker man alligevel at vedtage de foreslåede §§ 786 c og d, bør det ifølge forbundet belyses, hvor stor en del af Danmark, der har 1,5 gange gennemsnittet. PROSA anfører endvidere, at hvis den målrettede geografiske logning i praksis betyder, at hundredetusindvis af uskyldige vil blive logget, vil det ikke være et proportionelt indgreb i privatlivet. Forbundet bemærker, at forbundet finder logning af mere end 2 pct. af befolkningen uproportionalt.

Retspolitisk Forening advarer mod som foreslået at indføre et system, der skal sikre målrettet overvågning af dømte kriminelle i op til et årti efter deres endte afsoning. Dette vil være et direkte angreb på alle konstruktive resocialiseringsbestræbelser, der desværre kun flugter alt for godt med Justitsministeriets nylige forslag om begrænsning af livstidsdømtes adgang til at kommunikere med personer uden for anbringelsesstedet.

Foreningen anfører også, at forslaget om oprettelse af geografiske zoner på 3 km gange 3 km i de delområder af landet, hvor antallet af beboere dømt for grov kriminalitet er 1,5 gange større end landsgennemsnittet gennem de seneste 3 år, vil bidrage til den stempling af bestemte boligområder som ghettoer, der efterhånden møder stigende kritik.

RfDS bemærker, at den målrettede personbestemte logning må betragtes som reel ekstra straf for en lovovertrædelse, og det strider grundlæggende mod princippet om, at man er uskyldig, indtil andet er bevist, at introducere logning efter udstået straf. Videre finder RfDS det betænkeligt, at teleselskaberne – herunder helt små teleudbydere – skal have adgang til oplysninger om straffede, herunder med mulighed for på baggrund af opbevaringslængden at inducere sig frem til den straframme, som har været gældende for de straffede. Det kan også være problematisk, hvis grupper af straffede går sammen og etablerer sig som teleudbyder for at få adgang til disse data om straffede – eller forsøger at infiltrere teleselskaberne.

I forhold til den målrettede geografiske logning bemærker RfDS, at denne form for logning – som under gældende ret – vil opsamle betydelige mængder af logning om personer, som aldrig vil komme i politiets søgelys. Givet de kriterier for iværksættelsen af logningen, som forslaget lægger op til, bør det belyses, om der de facto foretages en logning, der reelt er noget mindre end under den eksisterende generelle udifferentierede logning (hvor meget

af Danmark falder under den geografiske logning omtalt i § 786 c) og ligeledes, om der kan være en diskriminerende bias bygget ind i denne logning, hvor svage borgere med lave indkomster generelt vil blive overvåget mere end gennemsnittet. Logning inden for området udvidet til 3 gange 3 km er meget vidtgående. Lovforslaget lægger også op til en geografisk betydeligt bredere logning end opsummeret på side 33-34 i "Skitse for revision af logningsreglerne m.v.", som Justitsministeriet udsendte i offentlig høring den 23. marts 2021.

Herudover bemærker RfDS, at det er problematisk, at der lægges op til, at teleselskaberne skal tilknytte CPR-numre til alle telefonoplysninger. La Quadrature du Net-dommen lægger op til, at der kan registreres oplysninger om borgernes identitet, men teleselskaberne har som led i deres forretning ikke på forhånd tilknyttet CPR-numre på alle telefonnumre/kundeforhold, og det er generelt positivt, at teleselskaberne dataminimerer deres indsamling af personoplysninger.

Justitsministeriet bemærker indledningsvist, at der i medfør af EU-Domstolens praksis, der er beskrevet nærmere under pkt. 2, 3.1.2 og 3.2.2 i lovforslagets almindelige bemærkninger, som udgangspunkt alene vil kunne iværksættes målrettet registrering og opbevaring af trafikdata. Kun i tilfælde, hvor der foreligger en alvorlig trussel mod den nationale sikkerhed, der er reel og aktuel eller forudsigelig, vil der kunne iværksættes generel og udifferentieret registrering og opbevaring af trafikdata. Det foreslås på den baggrund med lovforslaget, at der indføres en ordning med målrettet personbestemt og geografisk registrering og opbevaring, jf. pkt. 3.1.3.1 og 3.1.3.2 i lovforslagets almindelige bemærkninger. Det bemærkes i den forbindelse, at EU-Domstolen i sin dom af 6. oktober 2020 (La Quadrature du Net-dommen) har peget på, at en ordning med målrettet registrering og opbevaring netop vil kunne tage udgangspunkt i kategorier af berørte personer eller et geografisk kriterium, jf. præmis 168.

For så vidt angår den foreslåede målrettede personbestemte registrering og opbevaring af trafikdata bemærker Justitsministeriet, at der med den foreslåede ordning lægges op til, at Rigspolitiet meddeler udbydere pålæg om at foretage målrettet personbestemt registrering og opbevaring af trafikdata på baggrund af objektive forhold, som gør det muligt at fokusere målrettet på de personer, hvis trafikdata kan afsløre en forbindelse, i det mindste indirekte, til grov kriminalitet, bidrage til bekæmpelse af grov kriminalitet,

eller forhindre en alvorlig fare for den offentlige sikkerhed eller en risiko for den nationale sikkerhed.

Som det fremgår af pkt. 3.1.3.1 i lovforslagets almindelige bemærkninger, er det på baggrund af La Quadrature du Net-dommens præmis 148 Justitsministeriets vurdering, at personer kan være omfattet af en pligt for udbydere til at foretage målrettet personbestemt registrering, når visse objektive forhold tilsiger, at trafikdata om de pågældende – direkte eller indirekte – kan medvirke til at afdække en forbindelse til grov kriminalitet.

På denne baggrund lægges der i lovforslaget op til, at der efter forslaget til § 786 b i retsplejeloven vil skulle foretages målrettet personbestemt registrering og opbevaring af trafikdata vedrørende personer, der er dømt for grov kriminalitet og for kommunikationsapparater og personer, der har været genstand for visse indgreb i meddelelseshemmeligheden.

Justitsministeriet bemærker, at det i lovforslaget er præciseret, at iværksættelse af målrettet personbestemt registrering og opbevaring af trafikdata efter den foreslåede § 786 b i retsplejeloven vil skulle ske på baggrund af pålæg fra Rigspolitiet, der indeholder de relevante telefonnumre eller kommunikationsapparater tilhørende de personer, der skal iværksættes registrering og opbevaring for. Det er ligeledes præciseret, at tilsvarende gælder for så vidt angår iværksættelse af målrettet personbestemt registrering og opbevaring af trafikdata efter den foreslåede § 786 d i retsplejeloven.

For så vidt angår IDA's bemærkning om, at det bør fremgå tydeligere af lovforslaget, hvem der skal forstås som »nære relationer« til personer, der har forbindelse til grov kriminalitet, jf. lovforslagets pkt. 3.1.3.3 om den foreslåede § 786 d i retsplejeloven, skal Justitsministeriet bemærke, at personkredsen må vurderes konkret i forhold til, om der foreligger grund til at antage en forbindelse til grov kriminalitet. Efter omstændighederne vil også fjernere relationer end ægtefæller og samlevere kunne være omfattet, hvis disse konkret har tæt kontakt til den pågældende person.

For så vidt angår TI's bemærkning vedrørende brug af begrebet »indgreb« i § 786 b, stk. 4, nr. 4 (§ 786 b, stk. 3, nr. 4, i det fremsatte lovforslag), er formuleringen af den foreslåede § 786 b, stk. 3, nr. 4, ændret, så det nu fremgår, at der kan foretages målrettet personbestemt registrering og opbevaring af trafikdata vedrørende kommunikationsapparater, der har været genstand for pålæg i medfør af retsplejelovens § 786, stk. 2.

Vedrørende TI's forslag om, at det præciseres i lovforslaget, at et samtykke til målrettet personbestemt registrering og opbevaring efter den foreslåede § 786 b, stk. 3, nr. 4, skal være et selvstændigt samtykke, skal Justitsministeriet bemærke, at det allerede af bemærkningerne til bestemmelsen i lovforslaget fremgår, at der i forbindelse med indhentelse af samtykke til teleoplysning også vil kunne indhentes samtykke til den efterfølgende tidsbegrænsede registrering og opbevaring af trafikdata. Det vil i den forbindelse være et krav, at samtykket er klart og utvetydigt og kommer fra den person, registrerings- og opbevaringspligten vedrører. Det fremgår desuden, at samtykket til enhver tid vil kunne trækkes tilbage.

Justitsministeriet bemærker desuden for så vidt angår den foreslåede ordning med målrettet geografisk registrering og opbevaring af trafikdata, jf. den foreslåede § 786 c i retsplejeloven, at det er et krav for anvendelse af ordningen, at der er tale om områder, der har en forbindelse til grov kriminalitet. Der skal enten være tale om områder på 3 km gange 3 km, hvor der er 1,5 gange flere anmeldelser af eller beboere dømt for grov kriminalitet end landsgennemsnittet, eller særligt sikringskritiske områder. Med begrebet landsgennemsnittet sigtes til, at henholdsvis antallet af anmeldelser af og beboere dømt for grov kriminalitet i det pågældende område skal sammenholdes med gennemsnittet af henholdsvis antallet af anmeldelser af og beboere dømt for grov kriminalitet på landsplan i områder af en tilsvarende arealmæssig størrelse. Dette er præciseret i de specielle bemærkninger til bestemmelsen.

Der lægges med lovforslaget op til at fastsætte klare og objektive kriterier for, hvornår der vil kunne iværksættes registrering og opbevaring af trafikdata efter det foreslåede § 786 c, stk. 1, i retsplejeloven. Der er desuden i de specielle bemærkninger til det foreslåede § 786 c, stk. 2, oplistet en række eksempler på områder, hvor der vil kunne foretages registrering og opbevaring af trafikdata efter bestemmelsen.

Kriterierne er fastsat i dialog med bl.a. Rigspolitiet og har til formål at sikre, at målrettet geografisk registrering og opbevaring af trafikdata sker på grundlag af objektive og ikke-diskriminerende forhold, der tilsiger, at der i et område er forhøjet risiko for, at der planlægges eller begås grov kriminalitet, eller at der er tale om et område, hvor særlige beskyttelseshensyn gør sig gældende. Den foreslåede størrelse på områder á 3 km gange 3 km er fastsat ud fra en vurdering af, at det ved områder af denne størrelse

vurderes muligt at etablere en ordning, som kan implementeres i samspil mellem myndighederne og udbyderne. Samtidig er det vurderingen, at den praktiske implementering af målrettet registrering og opbevaring af trafikdata vedrørende områder af denne størrelse vil være i overensstemmelse med EU-rettens krav om alene at foretage registrering og opbevaring i det omfang, det er strengt nødvendigt.

Den målrettede registrering og opbevaring af trafikdata er indsnævret væsentligt i forhold til den generelle og udifferentierede registrering og opbevaring af trafikdata, der finder sted i dag. Hvor man med den generelle og udifferentierede registrering og opbevaring i dag kan registrere og opbevare trafikdata vedrørende alle brugere over hele landet, skal der ved den målrettede registrering og opbevaring udvælges nærmere bestemte områder og personer, som har en forbindelse til grov kriminalitet.

I forhold til den målrettede geografiske registrering og opbevaring af trafikdata skønner Rigspolitiet på det foreløbige grundlag, at udbyderne som følge af den målrettede geografiske registrering og opbevaring af trafikdata vil blive pålagt at logge områder svarende til ca. 15-20 pct. af Danmarks samlede landareal. Der tages forbehold for, at der kan være usikkerhed forbundet med Rigspolitiets skøn. Præcist hvor stor en procentandel, som der i sidste ende vil blive registreret og opbevaret trafikdata vedrørende af udbyderne, vil bl.a. afhænge af, hvordan udbydernes master er placeret i de relevante områder. Som det også fremgår af pkt. 3.1.3.4 i lovforslagets almindelige bemærkninger, skal udbyderne iværksætte den målrettede geografiske registrering og opbevaring, så den alene omfatter det område, der er strengt nødvendigt.

I områder, hvor der kan foretages målrettet geografisk registrering og opbevaring af trafikdata, vil der blive registreret og opbevaret trafikdata vedrørende de personer, der befinder sig i området, mens de befinder sig i området – uanset om personerne konkret har en forbindelse til grov kriminalitet. Registreringen og opbevaringen af trafikdata relaterer sig imidlertid til området, som har en forbindelse til grov kriminalitet, og ikke til personerne, der befinder sig i området. Registreringen og opbevaringen af trafikdata vil derfor naturligvis heller ikke fortsætte, når en person bevæger sig ud af området og ind i et område, der ikke har en forbindelse til grov kriminalitet.

Uanset at den foreslåede ordning med målrettet geografisk registrering og opbevaring af trafikdata potentielt vil medføre, at der registreres og opbevares trafikdata i områder, hvor der løbende befinder sig mange personer, vil der efter Justitsministeriets opfattelse ikke blive tale om generel og udifferentieret registrering og opbevaring af trafikdata i perioder, hvor der ikke er grundlag for det. Der vil efter Justitsministeriets opfattelse heller ikke blive tale om, at registreringen og opbevaringen af trafikdata risikerer at blive hovedreglen frem for undtagelsen. Den målrettede geografiske registrering og opbevaring af trafikdata vil efter Justitsministeriets opfattelse netop være målrettet, idet den kun kan iværksættes i områder, hvor der er konstateret en forbindelse til grov kriminalitet – enten i form af et højere antal anmeldelser af eller beboere dømt for grov kriminalitet, eller områder med særlige sikringsbehov.

Det bemærkes, at der herudover lægges op til, at der kan meddeles udbydere konkret begrundede pålæg om at foretage målrettet registrering og opbevaring af trafikdata vedrørende kommunikationsapparater, personer eller bestemte områder, som politiet har grund til at antage har forbindelse til lovovertrædelser, som efter loven kan straffes med fængsel i 3 år eller derover, forsætlige overtrædelser af straffelovens kapitel 12 eller 13, overtrædelser af straffelovens § 124, stk. 2, § 125, § 127, stk. 1, § 235, § 266 eller § 281, overtrædelser af udlændingelovens § 59, stk. 8, nr. 1-5, krænkelser eller overtrædelser som er omfattet af § 781, stk. 2 eller 3, eller en lovovertrædelse omfattet af straffelovens § 81 a. For nærmere herom henvises til pkt. 3.1.3.3 i lovforslagets almindelige bemærkninger.

For så vidt angår det af Justitia anførte om, at det er en betingelse for at kunne anvende den foreslåede § 786 d i retsplejeloven, at der er grund til at antage, at kommunikationsapparater, personer eller bestemte områder har en forbindelse til grov kriminalitet, skal Justitsministeriet bemærke, at det lavere krav i denne bestemmelse i forhold til kravet for at kunne foretage indgreb i meddelelseshemmeligheden, jf. retsplejelovens § 781, stk. 1, nr. 1, skal ses på baggrund af, at registrering og opbevaring af trafikdata typisk vil være relevant på et tidspunkt af efterforskningsstadiet, hvor politiet ikke har en konkretiseret mistanke. Det skal videre bemærkes, at den foreslåede § 786 d i retsplejeloven som udgangspunkt er undergivet forudgående domstolskontrol, jf. det foreslåede stk. 2 i bestemmelsen. Retten vil bl.a. skulle vurdere, om indgrebet er proportionalt, jf. henvisningen til retsplejelovens § 782, stk. 1, i det foreslåede § 786 d, stk. 3. Endelig skal det bemærkes, at for at politiet kan få adgang til de oplysninger, der registreres og opbevares

i medfør af den foreslåede § 786 d, skal dette ske efter en retskendelse i medfør af reglerne om edition eller reglerne om indgreb i meddelelseshemmeligheden, jf. de foreslåede §§ 781 a og 804 a i retsplejeloven. For nærmere om anvendelsesområdet for den foreslåede § 786 d kan Justitsministeriet henvise til bemærkningerne til bestemmelsen i lovforslaget, hvor der er givet eksempler på, hvilken personkreds pålæg om registrering og opbevaring efter bestemmelsen bl.a. kan tænkes anvendt over for.

Justitsministeriet bemærker desuden, at der med lovforslaget lægges op til, at justitsministeren i en overgangsperiode – dvs. i perioden fra lovens ikrafttræden og indtil det tidspunkt, hvor den nødvendige it-systemunderstøttelse er etableret og klar til at blive sat i drift – vil kunne fastætte regler om fravigelse af lovens bestemmelser i de foreslåede §§ 786 b-786 d, herunder at reglerne helt eller delvist ikke skal anvendes, jf. § 3, stk. 4, i det fremsatte lovforslag (§ 3, stk. 2, i høringsversionen). Der vil f.eks. kunne fastsættes regler om, hvilke tjenester og datatyper den målrettede registrering og opbevaring i en overgangsperiode skal omfatte. Der vil også eksempelvis kunne fastsættes regler om, at kun dele af den målrettede registrering og opbevaring i en overgangsperiode skal sættes i kraft. Der lægges i den forbindelse ikke op til at bemyndige justitsministeren til at fastsætte andre betingelser for iværksættelse af den målrettede registrering og opbevaring af trafikdata end dem, som fremgår af de foreslåede §§ 786 b-786 d i retsplejeloven. Det forudsættes, at udviklingsarbejdet i relation til den nødvendige it-systemunderstøttelse generelt sker i dialog mellem de relevante myndigheder og telebranchen, således at det sikres, at den kommende it-systemunderstøttelse i Rigspolitiet er kompatibel med den it-systemunderstøttelse, ordningen forudsætter for så vidt angår udbyderne. Der henvises til det, der anføres under pkt. 15 i den kommenterede høringsoversigt og i pkt. 3.1.3.4 i lovforslagets almindelige bemærkninger.

Med hjemmel i lovforslagets § 3, stk. 4, vil der f.eks. – hvis drøftelserne mellem de relevante myndigheder og telebranchen måtte føre til det resultat – kunne fastsættes regler om, at den foreslåede ordning med målrettet geografisk registrering og opbevaring i en overgangsperiode ikke vil skulle omfatte fastnettelefoni, herunder IP-telefoni.

Det bemærkes også, at lovforslaget er justeret, så det fremgår af lovforslagets § 3, stk. 2, at justitsministeren fastsætter tidspunktet for ikrafttræden af lovens § 2, stk. 2. Det vil betyde, at udbyderne først på et tidspunkt nærmere fastsat af justitsministeren skal være klar til at understøtte og administrere

registrering af unikt ID for slutbrugere og eventuelle oplysninger om bruger. Lovforslagets § 2, nr. 2, relaterer sig bl.a. til den foreslåede ordning med målrettet registrering og opbevaring af trafikdata. Det forudsættes derfor, at lovforslagets § 2, nr. 2, sættes i kraft på det tidspunkt, der passer i forhold til de relevante regler om målrettet registrering og opbevaring af trafikdata i overgangsperioden. Forslaget skal således ses i sammenhæng med lovforslagets § 3, stk. 4, hvor det foreslås, at justitsministeren i en overgangsperiode kan fastsætte regler om fravigelse af de foreslåede §§ 786 b-786 d i retsplejeloven, herunder at reglerne helt eller delvist ikke skal anvendes. Der henvises til de specielle bemærkninger hertil.

Herudover bemærker Justitsministeriet, at udgangspunktet for udarbejdelsen af lovforslaget har været lovskitsen af 23. marts 2021. Justitsministeriet har i forbindelse med arbejdet med lovforslaget konkretiseret de mere overordnede overvejelser, der fremgår af lovskitsen, bl.a. på side 33-34. Efter ministeriets opfattelse afviger den foreslåede ordning med målrettet geografisk registrering og opbevaring af trafikdata ikke fra det, der mere overordnet anføres i lovskitsen på side 33-34. I lovskitsen anføres bl.a., at det efter Justitsministeriets opfattelse vil kunne pålægges udbyderne at etablere målrettet geografisk registrering og opbevaring af trafikdata ud fra myndighedernes vurdering af – på grundlag af objektive og ikke-diskriminerende forhold – en forhøjet risiko for, at der planlægges eller begås kriminalitet i et givent område. I forlængelse heraf anføres det bl.a., at det vil være muligt at pålægge etablering af målrettet registrering og opbevaring på steder, der er kendetegnet ved et højt antal tilfælde af grov kriminalitet m.v., f.eks. hvis politiet har konstateret, at der i et givent område – f.eks. en bydel – statistisk set oftere begås grov kriminalitet end andre steder. Det anføres også, at det vil være muligt at pålægge etablering af målrettet registrering og opbevaring på steder, hvor der i særlig grad kan begås grov kriminalitet m.v., såsom steder eller infrastrukturer, der regelmæssigt besøges af et meget stort antal personer, og at der i et område også kan vurderes at være en forhøjet risiko for grov kriminalitet m.v. i forbindelse med konkrete begivenheder – f.eks. sportsarrangementer, konferencer eller statsbesøg. Endelig anføres det, at det vil være muligt, at pålægge etablering af målrettet registrering og opbevaring på strategiske steder, såsom lufthavne, banegårde eller vejafgiftsområder.

Justitsministeriet bemærker endvidere, at der med lovforslaget lægges op til at videreføre de gældende krav til beskyttelse af bl.a. registrerings- og op-

bevaringspligtige oplysninger, jf. pkt. 3.1.1.3 i lovforslagets almindelige bemærkninger. Behandling af personoplysninger for politiet vil desuden være underlagt henholdsvis Datatilsynets og Tilsynet med Efterretningstjenesternes tilsyn. Hertil kommer, at der med den foreslåede § 786 g i retsplejeloven lægges op til, at der skal kunne fastsættes regler om opbevaring af oplysninger registreret og opbevaret i medfør af de foreslåede §§ 786 a-786 f eller pålæg eller regler udstedt i medfør heraf. Det forudsættes bl.a., at der med hjemmel i bestemmelsen fastsættes regler om, at sådanne oplysninger skal opbevares på servere i EU.

Det er Justitsministeriets vurdering, at lovforslaget, herunder den foreslåede ordning med målrettet registrering og opbevaring af trafikdata, ligger inden for rammerne af EU-retten. Der henvises til pkt. 10 i lovforslagets almindelige bemærkninger.

For nærmere om implementering af den foreslåede ordning med målrettet geografisk registrering og opbevaring af trafikdata henvises til pkt. 15 i den kommenterede høringsoversigt.

For nærmere om de administrative omkostninger for erhvervslivet ved ordningen henvises til pkt. 16 i den kommenterede høringsoversigt.

For nærmere om den foreslåede ordning med målrettet registrering og opbevaring af trafikdata henvises til pkt. 3.1 i lovforslagets almindelige bemærkninger.

4. Generel og udifferentieret registrering og opbevaring af trafikdata

Amnesty bemærker, at Justitsministeriet i lovforslaget henviser til, at der vil indgå en række elementer til at vurdere, om der er en alvorlig trussel mod den nationale sikkerhed. Vurderingen skal basere sig på en gennemgang af verserende og afsluttet sager under straffelovens kapitel 12 og 13, den årlige rapport fra Center for Terroranalyse (CTA) samt øvrige analyseprodukter fra nationale efterretningstjenester. I lovforslaget fremstår CTA-vurderingen samt gennemgang af relevante verserende sager som de bærende elementer. Amnesty bemærker i den forbindelse, at EU-rettens definition af en alvorlig trussel mod den nationale sikkerhed skal forstås som, at det er ekstraordinært opstået faktiske trusler mod staten, der udløser, at der midlertidigt kan foretages den generelle logning. For at være i overensstemmelse

med EU-retten anbefaler Amnesty, at der kun benyttes efterretningsinstrumenter, som er designet til at give løbende trusselsbilleder og kan oplyse om akut opstående situationer, der gør en trusselsvurdering reel og eller aktuel/forudsigelig frem for instrumenter, som giver årlige analyser af længerevarende trusselstilstande.

Herudover bemærker Amnesty, at når dét, der giver adgangen til den generelle og udifferentieret logning, kun er ekstraordinært opstået sikkerhedssituationer af midlertidig karakter, virker det påfaldende, at man vil tage udgangspunkt i, at der kan indføres generelt påbud om at logge med et års varighed ad gangen med mulighed for mindre. Efter Amnestys opfattelse virker det tidsmæssige forslag, som er konstrueret på denne måde, ikke til at leve op til en præmis om en begrænsning til strengt nødvendige ekstraordinært opstået trusler mod den nationale sikkerhed. Amnesty anbefaler, at man skal operere med langt kortere tidsrum, hvor udgangspunktet bør være, at der tages udgangspunkt i uger i stedet for år, og at man opererer med en mulighed for forlængelser i stedet for en mulighed for forkortelse. Dette vil være i overensstemmelse med, at en trusselsvurdering skal bygge på konkret opstående situationer, der gør en trusselsvurdering reel og eller aktuel/forudsigelig, og ikke analyser af længerevarende trusselstilstande.

Danske Advokater anfører, at det er foreningens vurdering, at der med de foreslåede regler er en risiko for, at generel og udifferentieret logning kommer til at udgøre hovedreglen og ikke den begrænsede undtagelse. En sådan praksis vil være i strid med EU-retten. Det er bl.a. tilfældet, idet La Quadrature du Net-dommens undtagelse for generel og udifferentieret logning anvendes ud over sine rammer og medfører en fortsættelse af den status quo, der netop er underkendt af EU-domstolen i de afsagte domme.

Danske Advokater bemærker desuden, at der i lovforslaget er fastlagt en periode på op til 1 år ad gangen, idet den konkrete varighed skal vurderes fra gang til gang og kan reduceres, hvis truslen aftager. Perioden kan endvidere forlænges i op til 1 år ad gangen. Hvorvidt varigheden kan holdes til "det strengt nødvendige", må i høj grad afhænge af ministeriets administration heraf. Løbende 1-årige forlængelser vil dog ikke være forenelig med EU-rettens forbud mod generel og udifferentieret logning.

Foreningen bemærker endvidere, at det foreslås, at oplysninger, der er registreret og opbevaret som følge af en pligt til generel og udifferentieret regi-

strering og opbevaring, vil skulle opbevares i 1 år fra registreringstidspunktet, også efter overgangen til målrettet registrering og opbevaring. Oplysninger registreret og opbevaret som følge af en pligt til generel og udifferentieret registrering og opbevaring, der er indhentet af politiet og anklagemyndigheden, inden opbevaringsperioden for de pågældende oplysninger er udløbet, vil også efter udløbet af opbevaringsperioden kunne anvendes i efterforskningen og som bevis i straffesager. Sådan formålsforskydning synes efter Danske Advokaters opfattelse at være uforenelig med EU-retten, såvel som persondataretten, eks. GDPR art 5.

IDA bemærker, at der i forslaget til § 786 e i retsplejeloven lægges op til, at justitsministeren efter forhandling med erhvervsministeren kan pålægge udbydere at foretage en generel og udifferentieret registrering og opbevaring, 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". Registreringspligten kan fastsættes for højst 1 år ad gangen. IDA mener ikke, at dette er i tråd med EU-retten, hvor der tales om, at tidsperioden skal begrænses til det strengt nødvendige, og at generel og udifferentieret logning aldrig må blive hovedreglen eller antage systematisk karakter, ligesom vurderingen skal være baseret på konkrete omstændigheder, og der skal være tale om en reel og aktuel eller forudsigelig trussel. CTA's VTD har siden 2014 angivet terrortruslen i Danmark som "alvorlig", og om end den tidligere har været lavere, er det tvivlsomt, at den skulle falde inden for de næste år. Der er derfor ikke tale om "en begrænset periode, når der foreligger tilstrækkelige konkrete omstændigheder". Der er snarere tale om en ny normaltilstand, som vi ikke foreløbigt kan se en ende på. Det skal tages med i afvejningen af proportionalitetsprincippet. Hertil kommer, at politiet i de sidste år har fået en række andre værktøjer til hjælp, herunder ansigtsgenkendelse i lufthavne, ANPG (nummerpladegenkendelse), opsætning af TV-overvågningskameraer og adgang til private TV-overvågningsoptagelser samt adgang til DNA-oplysninger hos Nationalt Genomcenter – tiltag, som også indsamler store mængder data om tilfældige danskere, der aldrig har været eller kommer i politiets søgelys. Logning af teletrafik er altså ikke længere den eneste mulighed for at fremme efterforskning hos politiet. Også dette bør tages med i afvejningen af proportionalitetsprincippet.

Herudover finder IDA det problematisk, at det er justitsministeren i forhandling med erhvervsministeren, der kan forlænge påbud om generel og udifferentieret logning med et år ad gangen. I så alvorlige ændringer af borgernes

grundlæggende rettigheder bør det som det mindste krav være en afgørelse, der foretages i Folketinget efter en grundig demokratisk diskussion. Alternativt kan der iværksættes generel og udifferentieret logning i korte, afgrænsede tidsperioder som f.eks. 14 dage. Ved perioder af dette tidsrum vil et administrativt tilsyn udpeget af Folketinget kunne stå for godkendelsen.

IDA kan derfor ikke støtte et forslag, der gør det muligt at fortsætte med generel og udifferentieret logning.

Herudover bemærker IDA, at konkrete begivenheder kunne være anledning til tidsafgrænset logning. Begivenhedsbestemt logning kunne ske under et klimatopmøde, et statsbesøg eller en stor sportsbegivenhed. Ved sådanne begivenheder kunne generel og udifferentieret logning være acceptabel i et minimalt geografisk område og i en skarpt afgrænset periode som f.eks. 14 dage op til begivenheden og under selve begivenheden. Medmindre der sker en hændelse op til eller under disse begivenheder, som giver anledning til at anvende logningsdata i efterforskningsarbejde, kan data herefter slettes omgående. IDA anbefaler Justitsministeriet at sætte en begivenhedsbestemt logning i stedet for den de facto permanente og udifferentierede logning.

IMR bemærker, at der i lovudkastet lægges op til, at det skal være muligt at pålægge teleudbyderne/teleindustrien at foretage generel og udifferentieret logning af alle kommunikationsmidler for alle borgere i op til 1 år ad gangen, hvis en række nærmere omstændigheder er overholdt. Der gælder et klart udgangspunkt efter EU-retten om, at generel og udifferentieret logning er forbudt. EU-Domstolen tillader imidlertid ganske undtagelsesvist generel og udifferentieret logning, hvis konkrete omstændigheder viser en alvorlig, reel og aktuel eller forudsigelig trussel mod den nationale sikkerhed, og dette sker for en periode, som tidsmæssigt er begrænset til det strengt nødvendige. Det er endvidere en betingelse, at logningen ikke har en systematisk karakter. Instituttet vurderer, at ministeriets forslag næppe stemmer overens med EU-Domstolens nuværende praksis. Der er således efter instituttets opfattelse en risiko for, at EU-Domstolen vil nå frem til, at betingelserne for at iværksætte generel og udifferentieret logning ikke er opfyldt, og at logningen antager en systematisk karakter i strid med EU-retten. Instituttet anbefaler, at Justitsministeriet sikrer, at adgangen til generel og udifferentieret logning til beskyttelse af national sikkerhed begrænses til ekstraordinære undtagelsessituationer.

IT-Politisk Forening bemærker, at lovforslaget motiveres 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 vil fortsættes i den overskuelige fremtid.

Foreningen anfører desuden, at det på baggrund af præmis 137-139 i La Quadrature du Net-dommen er foreningens klare opfattelse, at eventuelle påbud om logning af hensyn til den nationale sikkerhed kun kan fastsættes for en væsentlig kortere periode end 1 år, eksempelvis op til 1 måned. Derudover skal vurderingen være baseret på konkrete efterretninger om en fremtidig alvorlig trussel mod den nationale sikkerhed.

Det er ligeledes ifølge foreningen et krav fra EU-Domstolen, at den generelle og udifferentierede logning med henblik på beskyttelse af den nationale sikkerhed ikke må have systematisk karakter. Hvis justitsministeren vil basere vurderingen på 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. Særligt sigtelser, varetægtsfængslinger og tiltalerejsning har en bagudrettet karakter.

Foreningen anfører endvidere, at den i pkt. 3.2.3 beskrevne ordning i realiteten fremstår som en generel og udifferentieret lagringspligt af alle trafikdata uden en reel tidsbegrænsning baseret på generelle vurderinger af terrortrusselsniveauet. 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.

Herudover anfører IT-Politisk Forening, at 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. I denne situation vil der være lagret

trafikdata for hele befolkningen, som ikke længere er nødvendig 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. 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. 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. Den generelle og udifferentierede lagringspligt kan umuligt siges at være tidsmæssigt begrænset til det strengt nødvendige, når lagringen på denne måde kan opretholdes længere, end hvad der er nødvendigt for formålet.

Endelig anfører foreningen, at der ikke i den foreslåede § 786 e i retsplejeloven synes 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 i La Quadrature du Net-dommen. Fordi generel og udifferentieret logning udgør et særligt alvorligt indgreb i grundlæggende rettigheder, må henvisningen til de begrænsninger og garantier i præmis 138 skulle forstås som yderligere retsgarantier ud over det, som gælder for den øvrige logning.

Justitia anfører, at det er afgørende, at CTA's vurdering af, at terrortruslen er "alvorlig", ikke bør kunne stå alene som grundlag for at iværksætte generel og udifferentieret logning. CTA har vurderer trusselsniveauet "alvorligt" hvert år siden 2014. Iværksættelse af generel og udifferentieret logning på baggrund af CTA's vurdering alene vil derfor ikke overholde kravet om, at generel og udifferentieret logning skal være et tidsbegrænset tiltag reserveret til ekstraordinære situationer. Ifølge Justitia må vurderingen foretages på baggrund af konkrete, dokumenterbare omstændigheder, der gør trusselsantagelsen reel og aktuel eller forudsigelig. Justitia er enig i, at underliggende analyser fra CTA samt øvrige relevante analyseprodukter – afhængig af deres karakter – kan indgå som delelementer i vurderingen. Det er i den forbindelse afgørende, at der skal være tale om analyser baseret på konkrete omstændigheder frem for "bredere tendensanalyse og vurdering af fænomener". Der bør udvises varsomhed i forhold til at lægges vægt på navnlig allerede afgjorte sager om straffelovens kapitel 12 og 13, der som udgangspunkt må antages i højere grad at belyse bagudrettede forhold.

Justitia bemærker desuden, at det efter forslaget til § 786 e, stk. 1, i retsplejeloven er justitsministeren, der efter forhandling med erhvervsministeren kan fastsætte regler om generel og udifferentieret logning. Om end det er positivt, at det ikke er justitsministeren alene, der foreslås at have kompetence til at pålægge generel og udifferentieret logning, finder Justitia det anbefalelsesværdigt, at vurderingen underlægges yderligere kontrol og objektivitet. Der kunne f.eks. stilles krav om, at vurderingen foretages i samarbejde med Tilsynet med Efterretningstjenesterne, eller der kan oprettes en særenhed. Desuden vil det være fordelagtigt at underlægge vurderingen af, om der foreligger en tilstrækkelig trussel, parlamentarisk kontrol. I alle tilfælde er det ifølge Justitia afgørende, at dem, der er involveret i vurderingen, har adgang til alt materiale og alle oplysninger, der er af betydning for vurderingen. Der kan i den forbindelse drages inspiration fra Tilsynet med Efterretningstjenesterne.

Justitia bemærker endvidere, at for at yde tilstrækkelige retssikkerhedsmæssige garantier i forbindelse med vurderingen af, om der foreligger en alvorlig trussel mod den nationale sikkerhed, bør en sådan ordning kun kunne iværksættes efter rettens kendelse. Et krav om retskendelse vil naturligvis være mere tids- og ressourcekrævende, men henset til, at der kun i helt ekstraordinære tilfælde bør kunne pålægges generel og udifferentieret logning, vil behovet for at skaffe en kendelse opstå så sjældent, at de retssikkerhedsmæssige garantier, der er forbundet med kravet, opvejer disse ulemper. Retten bør i den henseende have tilgang til alt det materiale og alle de oplysninger, der ligger til grund for vurderingen af behovet for at pålægge generel og udifferentieret logning. For at bevare fortroligheden kan rettens behandling af spørgsmålet foregå for lukkede døre. Der kan i øvrigt iværksættes yderligere sikkerhedsprocedurer for at undgå risikoen for læk af klassificerede oplysninger.

Herudover anfører Justitia, at forslaget til § 786 e, stk. 2, i retsplejeloven, hvorefter regler om generel og udifferentieret logning kan fastsættes for en periode på op til 1 år ad gangen, går væsentligt ud over det strengt nødvendige. Justitia har bemærket, at det fremgår af udkastets almindelige bemærkninger, at reglerne om generel og udifferentieret logning ophæves, hvis der opstår grundlag for at antage, at reglerne ikke længere kan opretholdes. Rammerne for denne vurdering konkretiseres imidlertid ikke nærmere. På grund af den indgribende karakter, som generel og udifferentieret logning har, bør reglerne ifølge Justitias opfattelse indebære en pligt til løbende at

tage stilling til, om det konkrete trusselsbillede fortsat er tilstrækkeligt aktuelt til at tillade ordningens opretholdelse. Justitia foreslår på den baggrund, at udgangspunktet fastsættes til 14 dage med mulighed for forlængelse, hvis omstændighederne fortsat gør sig gældende ved periodens udløb. Hver forlængelse á 14 dage bør afgøres ved kendelse.

PROSA anfører, at det ikke i forslaget defineres, hvad en alvorlig trussel mod Danmark er.

RfDS bemærker, at der bør være snævrere rammer for den generelle og udifferentierede lognings tidsmæssige udstrækning. Generel og uddifferentieret logning bør således kun ske "i en begrænset periode, når der foreligger tilstrækkeligt konkrete omstændigheder… for en alvorlig trussel mod den nationale sikkerhed… som må anses for at være reel og aktuel eller forudsigelig", jf. La Quadrature du Net-dommen. Hovedreglen er ifølge RfDS, at der ikke må kunne foretages generel udifferentieret logning, men at der, når der kan dokumenteres en reel, aktuel og forudsigelig trussel, kan skrues op for logningen for at imødegå truslen og skrues ned igen, når den aktuelle trussel er afværget. Dermed må overvågningen heller ikke få karakter af at være systematisk og skal være begrænset i tid.

Justitsministeriet bemærker, at det fremgår af bl.a. pkt. 3.2.2 i lovforslagets almindelige bemærkninger, at det følger af bl.a. La Quadrature du Net-dommen, at der kan fastsættes nationale regler, der foreskriver generel og udifferentieret lagring af trafik- og lokaliseringsdata vedrørende alle brugere i en begrænset periode, når der foreligger tilstrækkeligt konkrete omstændigheder, der gør det muligt at antage, at en medlemsstat står over for en alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig. Det fremgår også, at dette gælder i situationer, hvor staten har en interesse i at beskytte statens væsentlige funktioner og grundlæggende samfundsinteresser, og omfatter forebyggelse og bekæmpelse af aktiviteter, der alvorligt kan destabilisere et lands grundlæggende forfatningsmæssige, politiske, økonomiske eller sociale strukturer og navnlig direkte true samfundet, befolkningen eller staten som sådan, såsom bl.a. terrorvirksomhed.

Med lovforslaget lægges der op til, at justitsministeren bemyndiges til efter forhandling med erhvervsministeren at fastsætte regler om, at det påhviler udbydere at foretage generel og udifferentieret registrering og opbevaring 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. Der vil således alene kunne fastsættes regler om generel og udifferentieret registrering og opbevaring af trafikdata, hvis der foreligger en sådan alvorlig trussel mod den nationale sikkerhed.

Som det fremgår af pkt. 3.2.3.2 i lovforslagets almindelige bemærkninger, har Justitsministeriet overvejet, hvordan det kan sikres, at den generelle og udifferentierede registrering og opbevaring af trafikdata tidsmæssigt begrænses til det strengt nødvendige, således at registreringen og opbevaringen ikke får en systematisk karakter. Det er Justitsministeriets vurdering, at en tidsmæssig udstrækning for generel og udifferentieret registrering og opbevaring af trafikdata på op til 1 år fra udstedelsen af en bekendtgørelse herom vil være proportional i de tilfælde, hvor det vurderes, at Danmark står over for en alvorlig trussel mod den nationale sikkerhed. Det foreslås på den baggrund, at udbyderes registreringspligt højst vil kunne fastsættes for en periode på 1 år ad gangen. Den tidsmæssige udstrækning skal begrænses til det strengt nødvendige, og udstrækningen skal derfor fastsættes til mindre end 1 år, såfremt det skønnes tilstrækkeligt. Det forudsættes også, at fastsatte regler ophæves, hvis det er den samlede vurdering, at de ikke længere kan opretholdes. Det forudsættes endvidere, at udbyderne med kort varsel kan understøtte en overgang fra generel og udifferentieret registrering og opbevaring til målrettet personbestemt og geografisk registrering og opbevaring.

Det foreslås, at oplysninger, der registreres i medfør af regler udstedt efter det foreslåede § 786 e, stk. 1, i retsplejeloven skal opbevares i 1 år fra registreringstidspunktet.

Det forudsættes i forlængelse heraf, at der med hjemmel i den foreslåede bemyndigelsesbestemmelse i retsplejelovens § 786 e fastsættes regler om, at oplysninger, der er registreret og opbevaret som følge af en pligt til generel og udifferentieret registrering og opbevaring af trafikdata, vil skulle opbevares i 1 år fra registreringstidspunktet, også efter overgangen til målrettet registrering og opbevaring. Det skal ses i lyset af, at oplysninger, der er registreret og opbevaret som følge af en gældende pligt til generel og udifferentieret registrering og opbevaring, vil være registreret på lovligt grundlag, og at sådanne oplysninger derfor vil kunne opbevares i 1 år efter selve registreringen. Det bemærkes, at det vil være et krav for, at politiet og anklagemyndigheden kan få adgang til sådanne oplysninger, at det sker med

henblik på bekæmpelse af grov kriminalitet eller beskyttelse af den nationale sikkerhed. Oplysninger registreret og opbevaret som følge af en pligt til generel og udifferentieret registrering og opbevaring, der er indhentet af politiet og anklagemyndigheden inden opbevaringsperioden for de pågældende oplysninger er udløbet, vil også efter udløbet af opbevaringsperioden kunne anvendes i efterforskningen og som bevis i straffesager.

For så vidt angår bemærkningerne fra IT-Politisk Forening og Danske Advokater vedrørende bl.a. behandlingsprincipperne i databeskyttelsesforordningen artikel 5, henvises der til den kommenterede høringsoversigts pkt. 17 om forholdet til databeskyttelseslovgivningen og pkt. 3.7.4.1 i lovforslagets almindelige bemærkninger.

Af pkt. 3.2.3.1 i lovforslagets almindelige bemærkninger fremgår det bl.a., at det er Justitsministeriets opfattelse, at vurderingen af, om der foreligger en alvorlig trussel mod den nationale sikkerhed, der er reel og aktuel eller forudsigelig, skal foretages med inddragelse af flere forskellige elementer.

Der bør således indgå en række forskellige vurderinger, analyser m.v. i vurderingen af, om der foreligger en alvorlig trussel mod den nationale sikkerhed, der er reel og aktuel eller forudsigelig. Det kan bl.a. være oplysninger om antallet og karakteren af verserende eller afgjorte straffesager om overtrædelse af straffelovens kapitel 12 og 13. Det vil således kunne indgå som et væsentligt moment ved vurderingen, om der er foretaget sigtelser, sket varetægtsfængsling eller rejst tiltale for forhold omfattet af straffelovens kapitel 12 og 13, ligesom domfældelser, hvorved der er dømt for overtrædelse af de bestemmelser, der hører under straffelovens kapitel 12 eller 13, vil kunne tillægges betydelig vægt ved vurderingen.

Endvidere vil en række uklassificerede analyseprodukter udgivet af bl.a. Politiets Efterretningstjeneste, Forsvarets Efterretningstjeneste eller Center for Cybersikkerhed kunne indgå i vurderingen af, om der foreligger en alvorlig trussel mod den nationale sikkerhed, der er reel og aktuel eller forudsigelig. Det vil f.eks. kunne være Center for Cybersikkerheds årlige trusselsvurdering af cybertruslen mod Danmark, men også andre relevante trusselsvurderinger vil kunne indgå.

Et yderligere element, som vil kunne indgå i vurderingen af, om der foreligger en trussel mod den nationale sikkerhed, der er reel og aktuel eller for-

udsigelig, er »Vurderingen af Terrortruslen mod Danmark« (VTD), som årligt udarbejdes af Center for Terroranalyse (CTA). VTD'en er CTA's samlede vurdering af terrortruslen mod Danmark og danske interesser i udlandet.

VTD'en indeholder en samlet vurdering af terrortruslen mod Danmark fra bl.a. militant islamisme, højreekstremisme og venstreekstremisme. Inden for hver af disse kategorier vurderes terrortruslen mod Danmark. Som led heri vurderes det bl.a., om det er sandsynligt, at en eller flere aktører har kapacitet til og/eller intention om at begå et terrorangreb, og om planlægning af et terrorangreb i det kommende år er sandsynlig.

Vurderingen af, om der foreligger en alvorlig trussel mod den nationale sikkerhed, som er reel og aktuel eller forudsigelig, vil skulle foretages regelmæssigt, så det sikres, at både nationale og internationale forhold af betydning for Danmarks nationale sikkerhed inddrages. Inddragelsen af flere af hinanden uafhængige analyseprodukter vil kunne styrke det vurderingsmæssige grundlag af det samlede trusselsbillede.

Det er samlet set Justitsministeriets vurdering, at der på baggrund af en gennemgang af aktuelle straffesager omhandlende overtrædelser af bestemmelserne i straffelovens kapitel 12 og 13, herunder både verserende sager og sager, hvori der er sket domfældelse, samt på baggrund af VTD'en og øvrige analyseprodukter kan foretages en velunderbygget vurdering af truslen mod Danmarks nationale sikkerhed med henblik på at konstatere, om der er tilstrækkelige solide grunde til at antage, at Danmark står over for en alvorlig trussel mod den nationale sikkerhed, som er reel og aktuel eller forudsigelig, hvor f.eks. aktiviteter alvorligt kan destabilisere Danmarks grundlæggende forfatningsmæssige, politiske, økonomiske eller sociale strukturer og navnlig direkte true samfundet, befolkningen eller staten som sådan, såsom bl.a. terrorvirksomhed.

Justitsministeriet bemærker, at der med lovforslaget lægges op til at videreføre de gældende krav til beskyttelse af bl.a. registrerings- og opbevaringspligtige oplysninger, jf. pkt. 3.1.1.3 i lovforslagets almindelige bemærkninger. Behandling af personoplysninger for politiet vil desuden være underlagt henholdsvis Datatilsynets og Tilsynet med Efterretningstjenesternes tilsyn. Hertil kommer, at der med den foreslåede § 786 g i retsplejeloven lægges op til, at der skal kunne fastsættes regler om opbevaring af oplysninger

registreret og opbevaret i medfør af de foreslåede §§ 786 a-786 f i retsplejeloven eller pålæg eller regler udstedt i medfør heraf. Det forudsættes bl.a., at der fastsættes regler om, at sådanne oplysninger skal opbevares på servere i EU.

Gyldigheden af regler udstedt i medfør af den foreslåede bemyndigelse i § 786 e i retsplejeloven kan prøves, jf. grundlovens § 63. Det forudsættes, at grundlaget for vurderingen af, at der foreligger en alvorlig trussel mod Danmarks nationale sikkerhed, der nødvendiggør fastsættelse af regler om generel og udifferentieret registrering og opbevaring af trafikdata, offentliggøres ved udstedelsen af reglerne. For nærmere om prøvelse af den foreslåede ordning med generel og udifferentieret registrering og opbevaring af trafikdata, herunder vurderingen af, om der foreligger en alvorlig trussel mod den nationale sikkerhed, som er reel og aktuel eller forudsigelig, henvises til pkt. 11 i den kommenterede høringsoversigt.

Det er Justitsministeriets vurdering, at lovforslaget, herunder den foreslåede ordning med generel og udifferentieret registrering og opbevaring af trafikdata i situationer, hvor der foreligger en alvorlig trussel mod den nationale sikkerhed, ligger inden for rammerne af EU-retten. Der henvises i den forbindelse til pkt. 10 i lovforslagets almindelige bemærkninger.

For nærmere om den foreslåede ordning med generel og udifferentieret registrering og opbevaring af trafikdata henvises til pkt. 3.2 i lovforslagets almindelige bemærkninger.

5. Generel og udifferentieret registrering og opbevaring af oplysninger om en slutbrugers adgang til internettet

Fiberby foreslår – for at sikre teknologineutralitet – at følgende skal oplyses i forbindelse med udlevering af IP-oplysninger:

- Dato og tid (DS/ISO 8601 format)
- IP-version (IPv4 eller IPv6)
- IP-protokol (TCP/UDP/ICMP/…)
- Afsender IP
- Afsender port
- Modtager IP
- Modtager port

Efter Fiberbys opfattelse bør disse logningsdata efterbehandles, så det bl.a. sikres, at overflødige modtageradresser slettes i de tilfælde, hvor samme port-nummer ikke er anvendt af flere slutbrugere. Det vil kunne sikre, at der opbevares så få oplysninger som muligt. Fiberby anbefaler, at oplysninger om modtager-IP og port bør oplyses i forbindelse med udlevering for at sikre ønsket om teknologineutralitet.

IT-Politisk Forening anfører, at det efter foreningens opfattelse er hævet over enhver tvivl, at præmis 152-156 i La Quadrature du Net-dommen omhandler registrering af source IP-adresser (kilden til en forbindelse) og ikke sessionslogning. Foreningen anfører videre, at logning af IP-adresser tildelt kilden til en brugers adgang til internettet efter EU-retten er tilladt på generel og udifferentieret basis, men alene hvis det sker med henblik på bekæmpelse af grov kriminalitet. Lovforslaget viderefører blot den gældende logning af adgangen til internettet uden at begrænse anvendelsen til sager om grov kriminalitet. Der sker endda en udvidelse af internetlogningens omfang. Det bør derfor præciseres i den foreslåede § 786 f i retsplejeloven eller bemærkningerne hertil, 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 retforfølgelse af grov kriminalitet.

IT-Politisk Forening bemærker desuden, at det som en konsekvens af La Quadrature du Net-dommen vil være nødvendigt at indsætte en ny bestemmelse i retsplejelovens kapitel 74 om politiets adgang til oplysninger om en slutbrugers adgang til internettet. Den foreslåede § 804 a i retsplejeloven kan i princippet være udgangspunkt for en sådan bestemmelse. Ud over 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.

Foreningen anfører videre, at der – ud over hvad der gælder efter gældende ret – efter den foreslåede § 786 f, stk. 3, i retsplejeloven vil blive fastsat regler om registrering af yderligere oplysninger for at sikre en entydig identifikation af en bruger af internettet. Af bemærkningerne i pkt. 3.3 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 vedrørende 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). Den tildelte IP-adresse kan ikke i sig selv afsløre, hvilke internetsteder 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. Brug af portnumre sammen med en IP-adresse for at identificere en bruger bag CG-NAT vil være meget afhængig af, at timestamps er 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 forskel, kan internetudbyderen identificere den forkerte bruger med deraf følgende risiko for, at en uskyldig person bliver genstand for politiets efterforskning. Hvis internetlogning i den foreslåede § 786 f i retsplejeloven 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.

På den baggrund anbefaler IT-Politisk Forening, 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.

PROSA er stærke modstandere af den udifferentierede logning, idet logning af al internettrafik formodentlig er i strid med EU's menneskerettigheder, idet det er et uproportionalt stort indgreb. Som minimum bør denne logning begrænses til at omfatte de samme vilkår som den anden logning.

Justitsministeriet bemærker, at La Quadrature du Net-dommens præmis 152-156 efter Justitsministeriets opfattelse alene vedrører registrering og opbevaring af IP-adresser i form af såkaldt sessionslogning, jf. også pkt.

3.3.3 i lovforslagets almindelige bemærkninger. Det skal ses i lyset af, at en sporing som nævnt i dommens præmis 153 (en sporing af en internetbrugers søgemønstre og dermed af den pågældendes onlineaktiviteter, der gør det muligt at skabe en detaljeret profil af denne internetbruger) efter Justitsministeriets opfattelse vil kræve registrering og opbevaring af sessioner, dvs. såkaldt sessionslogning, som blev afskaffet i Danmark ved ikrafttræden af bekendtgørelse nr. 660 af 19. juni 2014 om ændring af bekendtgørelse om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen). Ved sessionslogning forstås den situation, hvor en slutbruger sender eller modtager data på internettet, og en udbyder registrerer og opbevarer oplysninger om internetsessionens initierende og afsluttende pakke, herunder oplysninger om afsendende og modtagende IP-adresse, afsendende og modtagende portnummer samt transportprotokol, hver gang en slutbruger tilgår f.eks. en server eller kommunikerer direkte over internettet med en anden slutbruger. Sessionslogning medfører således indsamling af detaljerede informationer om selve kommunikationen (hvilke hjemmesider, der besøges m.v.).

Sessionslogning adskiller sig fra registrering og opbevaring af oplysninger om, hvilken slutbruger der på et givet tidspunkt har benyttet en given IP-adresse, eventuelt med et såkaldt portnummer. Registrering og opbevaring af sådanne oplysninger vil således ikke kunne medføre en sådan sporing. Det er Justitsministeriets opfattelse, at sådanne oplysninger i stedet skal henføres til det, der i La Quadrature du Net-dommens præmis 157-159 anføres om civile identitetsoplysninger. Herved er lagt vægt på, at disse oplysninger alene vedrører identiteten på brugerne af elektroniske kommunikationsmidler, og at disse data ikke i sig selv gør det muligt at få kendskab til datoen og tidspunktet for samt varigheden og modtagerne af den kommunikation, der er foretaget, og heller ikke de steder, hvorfra denne kommunikation har fundet sted, eller oplysning om, hvor ofte denne kommunikation har været foretaget med visse personer i en bestemt periode. Det indebærer, at oplysningerne bortset fra de pågældendes kontaktoplysninger, såsom deres adresser, ikke tilvejebringer nogen form for oplysninger om den foretagne kommunikation og dermed om disse personers privatliv.

Justitsministeriet vurderer på baggrund af det anførte, at det inden for rammerne af EU-retten er muligt at foretage generel og udifferentieret registrering og opbevaring af oplysninger om, hvilken slutbruger der på et givet

tidspunkt har benyttet en given IP-adresse, eventuelt med et såkaldt portnummer – og at give myndighederne adgang til at indhente sådanne oplysninger, jf. pkt. 3.7 i lovforslagets almindelige bemærkninger – med henblik på bekæmpelse af al kriminalitet. Det skal som nævnt ses i lyset af, at disse oplysninger ikke kan tilvejebringe oplysninger om selve kommunikationen mellem personer eller personers internetaktivitet og dermed heller ikke om disse personers privatliv. Hertil kommer, at behovet for entydigt og effektivt at kunne fastlægge identiteten på en slutbruger af en given IP-adresse fortsat vil have en central betydning for politiets efterforskning. Registrering og opbevaring af oplysninger om f.eks. IP-adresser, der alene opfylder beskrivelsen i EU-Domstolens præmis 157, vil derfor efter Justitsministeriets opfattelse fortsat kunne opbevares og anvendes til brug for efterforskning af al kriminalitet.

Det er på den baggrund også Justitsministeriets vurdering, at de nugældende danske regler i logningsbekendtgørelsens § 5, stk. 1, der foreskriver, at udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal foretage generel og udifferentieret registrering af oplysninger om en brugers adgang til internettet (herunder IP-adresser) uden noget krav om, at det skal ske med henblik på bekæmpelse af grov kriminalitet, er i overensstemmelse med La Quadrature du Net-dommen. Det skyldes, at de danske regler ikke omfatter registrering og opbevaring af sessioner, men alene registrering og opbevaring af identitetsoplysninger på slutbrugerens adgang til internettet. Det er endvidere Justitsministeriets vurdering, at det vil være i overensstemmelse med EU-Domstolens praksis, at udlevering af registrerede og opbevarede identitetsoplysninger om slutbrugerens adgang til internettet fortsat sker efter f.eks. de gældende regler om edition, hvor der ikke stilles krav om, at oplysningerne skal udleveres med henblik på bekæmpelse af grov kriminalitet, jf. pkt. 3.7 i lovforslagets almindelige bemærkninger.

Det bemærkes, at såfremt der indføres regler om f.eks. registrering og opbevaring af sessioner, der giver mulighed for en sporing som beskrevet i præmis 153, vil disse regler kun være i overensstemmelse med La Quadrature du Net-dommen, hvis de opfylder de krav, der opstilles for en sådan lagring i præmis 152-156. Efter Justitsministeriets opfattelse kan disse præmisser bl.a. kun efterleves derved, at adgang til sådanne oplysninger betinges af, at udleveringen sker med henblik på bekæmpelse af grov kriminalitet.

Justitsministeriet bemærker endvidere, at lovforslaget lægger op til en præcisering af de nugældende regler om adgang til oplysninger om en slutbrugers adgang til internettet (herunder IP-adresser), således at det er klart, hvad der skal registreres og opbevares, og hvad der kan gives adgang til. Dette er efter Justitsministeriets opfattelse nødvendigt bl.a. på baggrund af den teknologiske udvikling. Justitsministeriet bemærker, at præciseringen sikrer, at der ligesom efter den gældende logningsbekendtgørelses § 5, stk. 1, også fremadrettet kan ske identifikation af slutbrugerens adgang til internettet. Der henvises til pkt. 3.3.3 i lovforslagets almindelige bemærkninger.

I forhold til Fiberbys bemærkninger om teknologineutralitet i forbindelse med udbydernes udlevering af IP-oplysninger bemærker Justitsministeriet, at Justitsministeriet forventer, at en præcisering af de konkrete oplysninger, udbyderne skal udlevere, vil fremgå af de regler, som efter forslaget vil kunne udstedes i medfør af det foreslåede § 786 f, stk. 3, i retsplejeloven. Der henvises desuden til de specielle bemærkninger til den foreslåede § 786 f.

Justitsministeriet bemærker endelig i forlængelse af Fiberbys bemærkninger, at der med lovforslaget alene lægges op til, at registrere og opbevare samt give adgang til udlevering af den afsendende IP-adresse. Der lægges således ikke op til at omfatte den modtagende IP-adresse. Forslaget svarer på dette punkt til gældende ret.

6. Den foreslåede definition af "grov kriminalitet"

Danske Advokater anbefaler, at det præciseres, hvad der forstås ved "grov kriminalitet". Hvor der er tale om logning af konkrete straffede personer, bør tærsklen for logning relateres til den konkrete straf, idet der ved nogle overtrædelser af gode grunde er vide rammer for strafudmålingen.

IDA bemærker – med henvisning til pkt. 3.1.3.1 i lovforslagets almindelige bemærkninger – at IDA finder det særdeles problematisk at sænke strafferammen til 3 år, idet logning er et alvorligt indgreb i den enkeltes ret til privatliv. Dette er udtryk for et skred, der udfordrer proportionalitetsprincippet.

IT-Politisk Forening anfører, at lovforslaget indeholder et nyt kriminalitetskrav for edition af visse oplysninger, men fordi kriminalitetskravet generelt sænkes, vil politiet ud fra en samlet vurdering få større adgang til de

følsomme oplysninger om borgernes kommunikation med andre personer og deres færden i det fysiske rum. 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, at "ordningen derfor, alt andet lige, [vil] være mindre indgribende, end det er tilfældet i dag." Det er ifølge foreningen 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. 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, men 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. Det er 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. 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.

Justitia bemærker, at når Justitsministeriet foreslår en definition af "grov kriminalitet", der indebærer en væsentlig lempelse sammenholdt med det kriminalitetskrav, der hidtil har været gældende for adgangen til loggede data, forekommer der reelt at være tale om en de facto udvidelse af den nuværende (ulovlige) logningsordning. De hidtidige logningsregler har ikke indeholdt et kriminalitetskrav for så vidt angår selve registreringen af oplysninger, idet alle oplysningerne netop er blevet logget generelt og udifferentieret. Dog har selve adgangen til oplysningerne været reguleret af bl.a. reglerne om indgreb i meddelelseshemmeligheden, der indeholder et kriminalitetskrav (retsplejelovens § 781, stk. 1, nr. 3). I lovudkastet lægges der op

til en væsentlig lempelse af kriminalitetskravet, både for så vidt angår adgangen til oplysningerne og selve registreringen heraf, idet det foreslås, at der som udgangspunkt skal være tale om en lovovertrædelse med en strafferamme på minimum 3 år. Dertil kommer en række særligt angivne lovovertrædelser. Justitia finder det bemærkelsesværdigt, at der foreslås en så markant lempelse af kriminalitetskravet. Uanset fraværet af en EU-retlig definition af "grov kriminalitet", må der i reglerne tages udgangspunkt i en almensproglig forståelse af, hvad der adskiller denne form for kriminalitet fra kriminalitet i almindelighed, dvs. alvorsgraden af selve den kriminaliserede handling. Det i lovudkastet foreslåede strafferammekrav vil bl.a. indebære, at simpel vold (straffelovens § 244) vil blive anset som "grov kriminalitet". I praksis vil dette indebære, at en person, der er dømt for simpel vold, automatisk vil blive underlagt logning i 3 år efter at have afsonet sin dom. Som eksempler på simpel vold kan nævnes lussinger, kast med genstande, benspænd eller spytklat i ansigtet. Justitia har svært ved at se rimelighed eller proportionalitet i den i lovudkastet foreslåede definition af "grov kriminalitet". Justitia anbefaler, at definitionen baserer sig på en højere strafferamme end 3 års fængsel, f.eks. 6 år.

RfDS bemærker, at strafferammen for at iværksætte den geografiske logning bør være seks år. Ved sammenligning med "Skitse for revision af logningsreglerne m.v.", som Justitsministeriet sendte i offentlig høring den 23. marts 2021, ser der ud til, at der er sket en ændring i opfattelsen af, hvad der er grov kriminalitet. Af skitsen (navnlig p. 58) fremgik det, at der ved grov kriminalitet var tale om forhold, der kunne give seks års fængsel. Med lovforslaget lægges der op til, at grov kriminalitet og deraf følgende logning skal ske ved en straframme på tre års fængsel, som f.eks. omfatter simpel vold i form af lussinger og spytklat i ansigtet. Henset til mængden af personer, som logges uden nogensinde at komme i politiets søgelys under den geografiske logning, foreslår RfDS ud fra en proportionalitetsafvejning, at strafferammen for at iværksætte den geografiske logning bør være seks år. Generelt er det RfDS opfattelse, at der bør være en bred demokratisk debat om opfattelsen af, hvad grov kriminalitet er.

I forhold til Danske Advokaters ønske om en præcisering af, hvad der skal forstås ved »grov kriminalitet«, skal Justitsministeriet bemærke, at kravet i lovforslaget er defineret sådan, at lovovertrædelser, der kan straffes med fængselsstraf i 3 år eller derover, kan danne grundlag for en registrerings- og opbevaringspligt for så vidt angår trafikdata samt for adgang til de re-

gistrerings- og opbevaringspligtige trafikdata. Herudover vil en registrerings- og opbevaringspligt for så vidt angår trafikdata samt adgang til de registrerings- og opbevaringspligtige trafikdata kunne komme på tale ved en række nærmere angivne lovovertrædelser, der kan være vanskelige at efterforske, hvis ikke der er adgang til indgreb i meddelelseshemmeligheden, eller hvor indgreb i meddelelseshemmeligheden er et relevant eller hensigtsmæssigt efterforskningsmiddel. Der henvises til pkt. 3.7.1.2.2 i lovforslagets almindelige bemærkninger for en nærmere beskrivelse af disse bestemmelser. Denne måde at beskrive et kriminalitetskrav på adskiller sig ikke fra, hvad der i øvrigt gælder i retsplejelovens regler om tvangsindgreb. Justitsministeriet mener på det grundlag, at lovforslaget tilstrækkelig præcist beskriver, hvad der skal forstås ved »grov kriminalitet«. For så vidt angår Danske Advokaters ønske om at relatere tærsklen for registrering og opbevaring efter den foreslåede § 786 b, stk. 1, i retsplejeloven til den konkrete straf, der er blevet idømt, skal Justitsministeriet derfor bemærke, at dette af samme grunde ikke findes hensigtsmæssigt.

Justitsministeriet skal vedrørende grænsen for, hvilke lovovertrædelser der kan kvalificeres som »grov kriminalitet«, bemærke, at der må tilkomme medlemsstaterne et vist skøn i den henseende, når EU-Domstolen i sin dom af 6. oktober 2020 (La Quadrature du Net m.fl.) ikke præciserer, hvordan dette skal forstås. Strafferammernes maksimum udtrykker efter Justitsministeriets opfattelse, hvor grov en forbrydelse i almindelighed må anses for at være, uanset at strafferammen kan være bred og derfor også rumme forhold, der isoleret set kun medfører en straf i bunden af strafferammen. Der henvises til pkt. 3.7.3.1 i lovforslagets almindelige bemærkninger, hvor der er givet eksempler på forbrydelser, der efter ministeriets vurdering hhv. vil og ikke vil være grov kriminalitet.

I forhold til det af RfDS anførte om indholdet af lovskitsen skal Justitsministeriet bemærke, at det i lovskitsen for så vidt angår indgreb i meddelelseshemmeligheden blev konkluderet, at et strafferammekrav på 6 års fængsel eller derover med sikkerhed måtte antages at opfylde betingelsen om, at indgrebet alene anvendtes i relation til efterforskningen af grov kriminalitet (lovskitsen, pkt. 7.3.2, s. 70). Det blev for så vidt angår indgreb i meddelelseshemmeligheden videre konkluderet, at ministeriet ikke fandt, at nogen af de lovovertrædelser, der kunne begrunde indgreb i meddelelseshemmeligheden efter kriminalitetskravet i § 781, på forhånd kunne kvalificeres således, at de ikke vedrørte grov kriminalitet, men at dette dog skulle undersøges nærmere (lovskitsen, pkt. 7.3.2, s. 70). Det fremgår videre af lovskitsen, at

Justitsministeriet i den forbindelse fandt, at det burde undersøges, om der – i lyset af at lagringen af data ville ske mere målrettet – var rum for at stille et lempeligere kriminalitetskrav end det nuværende på 6 år (lovskitsen, hhv. pkt. 7.3.1 og 7.3.2, hhv. s. 69 og 71).

I forhold til det af Justitia anførte om lempelse af kriminalitetskravet for teleoplysning og udvidet teleoplysning med den foreslåede § 781 a i retsplejeloven skal Justitsministeriet bemærke, at denne lempelse kun gælder for teleoplysning og udvidet teleoplysning af de oplysninger, der registreres og opbevares i medfør af de foreslåede §§ 786 a-786 e i retsplejeloven eller efter pålæg eller regler udstedt i medfør heraf. Kriminalitetskravet for eksempelvis aflytning, jf. retsplejelovens § 780, stk. 1, nr. 1, vil som udgangspunkt stadig være, at der er tale om efterforskning af en lovovertrædelse, som efter loven kan straffes med fængsel i 6 år eller derover, jf. retsplejeloven § 781, stk. 1, nr. 3.

Justitsministeriet bemærker videre, at det er hensigtsmæssigt, at der gælder samme kriminalitetskrav for politiets adgang til oplysninger, der er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven eller efter pålæg eller regler udstedt i medfør heraf, uanset hvordan politiet søger adgang til disse. Justitsministeriet er af den opfattelse, at et kriminalitetskrav på 3 år er rimeligt at stille som krav for, at politiet kan få adgang til oplysninger, der er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven eller efter pålæg eller regler udstedt i medfør heraf, uanset på hvilken måde der anmodes om adgang til dem.

Endelig skal Justitsministeriet om kriminalitetskravet på 3 år bemærke, at et tilsvarende krav gælder i artikel 2, stk. 2, i rådets rammeafgørelse nr. 2002/584/RIA af 13. juni 2002 om den europæiske arrestordre og om procedurerne for overgivelse mellem medlemsstaterne. Efter denne bestemmelse kan en række nærmere angivne kategorier af lovovertrædelser medføre fuldbyrdelse på grundlag af en europæisk arrestordre uden kontrol af dobbelt strafbarhed, hvis lovovertrædelserne kan straffes med frihedsstraf af en maksimal varighed på mindst 3 år.

Vedrørende høringssvaret fra IT-Politisk Forening, hvor det bemærkes, at den foreslåede registrering og opbevaring reelt vil omfatte de samme personer og oplysninger som i dag, og at politiet samtidig får lettere adgang til »lagrede (historiske) teleoplysninger«, skal Justitsministeriet for det første

bemærke, at den generelle og udifferentierede registrering og opbevaring af teletrafik, der efter retsplejelovens § 786, stk. 4, og regler udstedt i medfør heraf finder sted i dag, bliver ophævet, og at der med den foreslåede ordning vil blive pligt til at foretage registrering og opbevaring af oplysninger på de nærmere angivne betingelser, der følger af de foreslåede §§ 786 a-786 f i retsplejeloven. For det andet skal Justitsministeriet bemærke, at politiets adgang til historiske oplysninger om, hvilken sendemast en mobiltelefon har været sat i forbindelse med, med den foreslåede ordning bliver indskrænket, således at der i det omfang, oplysningen er registrerings- og opbevaringspligtig efter de foreslåede §§ 786 a-786 e i retsplejeloven eller pålæg eller regler udstedt i medfør heraf, skal være tale om efterforskning af en lovovertrædelse, der kan straffes med fængsel i 3 år eller derover.

Vedrørende IT-Politisk Forenings bemærkninger i forhold til listen af lovovertrædelser, der kan begrunde fravigelse af kriminalitetskravet, skal Justitsministeriet bemærke, at denne i det væsentlige svarer til, hvad der allerede i dag følger af retsplejelovens § 781, stk. 1, nr. 3, og § 781, stk. 2 og 3. For en dels vedkommende er der tale om forbrydelser, der også må kvalificeres som grove, uanset strafferammen, f.eks. overtrædelser af straffelovens kapitel 12 og 13, der vedrører hhv. landsforræderi og andre forbrydelser mod statens selvstændighed og sikkerhed samt forbrydelser mod statsforfatningen og de øverste statsmyndigheder, terrorisme m.v. Andre af de særskilte nævnte forbrydelser vil ofte være vanskelige at opklare, hvis ikke der var adgang til at registrere, opbevare og indhente eksempelvis oplysninger om, hvilke kommunikationsapparater der har været forbundet med hinanden.

7. Hastesikring

RfDS bemærker, at det i forbindelse med at politi og anklagemyndighed kan hastesikre loggede oplysninger, for trafik- og lokaliseringsdata er et krav for adgang, at det sker med henblik på bekæmpelse af grov kriminalitet. Det bør præciseres, hvad der forstås ved hastesikring.

TI anfører, at teleudbyderne jævnligt oplever, at politiets begæring om hastesikring af lokaliseringsdata efter de gældende regler ikke følges op af en efterfølgende begæring om udlevering af de hastesikrede data (efter kendelse). TI finder det betænkeligt, at der således ikke er sikkerhed for, at den effektive prøvelse af indgreb i form af hastesikring, som EU-Domstolens foreskriver i La Quadrature du Net-dommens præmis 163, finder sted. TI

foreslår, at der fastsættes regler om, at politiets pålæg om hastesikring altid efterfølgende automatisk skal forelægges for retten til godkendelse.

TI finder desuden, at det er betænkeligt, at der efter den foreslåede ændring til retsplejelovens § 786 a ikke længere er nogen tidsgrænse for, hvor længe data maksimalt kan kræves hastesikret uden kendelse. Da der er tale om en beslutning hos politiet, som efter lovudkastet ikke prøves ved domstolene, er det tvivlsomt, om der i en hastig hverdag faktisk vil ske den grundige vurdering af, om kravene til (fortsat) hastesikring er til stede, når en hastesikring forlænges. Der kan meget hurtigt blive tale om, at data gemmes i meget lange perioder. Som bestemmelsen er formuleret, vil data kunne opbevares længere end ét år. TI opfordrer til, at den foreslåede ændring af retsplejelovens § 786 a, stk. 2 bør angive en maksimal periode i hvilken data kan hastesikres – f.eks. på ét år, svarende til reglerne om logning.

Justitsministeriet skal vedrørende det af RfDS anførte om forståelsen af »hastesikring« bemærke, at hastesikring efter gældende ret indebærer, at politiet kan udstede pålæg til udbydere af telenet eller tjenester om sikring af elektroniske data med henblik på, at oplysningerne er til stede og – hvis betingelserne herfor er opfyldt – på et senere tidspunkt kan udleveres til politiet til brug for efterforskningen, jf. pkt. 3.5.1 i lovforslagets almindelige bemærkninger. Dette ændrer lovforslaget ikke på. Derimod indebærer lovforslaget, at et pålæg om hastesikring fremover vil kunne forlænges inden for rammen på 90 dage, der fremgår af retsplejelovens § 786 a, stk. 2, 3. pkt., at det vil kunne opretholdes ud over de 90 dage, samt at politiet fremover kun kan få adgang til oplysninger, der er hastesikret, hvis der er tale om efterforskning af grov kriminalitet, jf. hhv. de foreslåede §§ 781 a og 804 a i retsplejeloven.

Justitsministeriet skal i forhold til det af TI anførte om automatisk, efterfølgende domstolskontrol bemærke, at en udbyder, der pålægges hastesikring i medfør af retsplejelovens § 786 a, vil kunne kræve spørgsmålet om sikringens lovlighed prøvet af domstolene, jf. retsplejelovens § 746. Justitsministeriet skal endvidere om TI's bemærkninger vedrørende hastesikringsperiodens varighed bemærke, at ministeriet ikke ønsker på forhånd at begrænse perioden til et bestemt antal dage. Det bemærkes dog, at det ligesom i dag efter forslaget vil gælde, at hastesikringen skal være så kort som mulig, jf. retsplejelovens § 786 a, stk. 1, 3. pkt. Hastesikringen kan derfor ikke uden grund forlænges i lange perioder.

Justitsministeriet skal endvidere generelt bemærke, at lovforslaget i forhold til høringsversionen er tilpasset, så det nu klart fremgår, at pålæg om hastesikring kun må meddeles, hvis efterforskningen angår en lovovertrædelse, som efter loven kan straffes med fængsel i 3 år eller derover, en forsætlig overtrædelse af straffelovens kapitel 12 eller 13, en overtrædelse af straffelovens § 124, stk. 2, § 125, § 127, stk. 1, § 235, § 266 eller § 281, en overtrædelse af udlændingelovens § 59, stk. 8, nr. 1-5, en krænkelse eller overtrædelse, som er omfattet af retsplejelovens § 781, stk. 2 eller 3, eller en lovovertrædelse omfattet af straffelovens § 81 a. Det vil betyde, at pålæg om hastesikring for alle typer elektronisk data alene vil kunne benyttes af hensyn til bekæmpelse af grov kriminalitet eller beskyttelse af den nationale sikkerhed.

8. Registrering og verificering af nummeroplysningsdata

Fiberby anfører, at det ikke er klart, om der lægges op til, at udbyderne skal registrere ét CPR-nummer eller samtlige CPR-numre, der er en del af en given husstand. Det er heller ikke klart, hvad der skal ske med produkter solgt til erhvervsdrivende, men som må benyttes privat, såsom arbejdsgiverbetalt "fri telefon" og arbejdsgiverbetalt internet. I realiteten vil den personbestemte målrettede overvågning blive til den husstandsbestemte målrettede overvågning. Fiberby ser derfor ikke CPR som en egnet nøgle til den personbestemte målrettede overvågning, når det gælder faste forbindelser. Fiberby opfordrer til, at der i forbindelse med kommunikationsnet og -tjenester med et fast leveringspunkt benyttes verificerede enhedsadresser som unik identifikation af leveringspunktet, og at krav om registrering og verificering af CPR bortfalder.

IDA finder det it-sikkerhedsmæssigt kritisk og uforholdsmæssigt ressourcekrævende, at der lægges op til at stille krav om, at der skal implementeres et system med registrering og verificering af nummeroplysningsdata for udbydere af taletidskort. Herudover anfører IDA bl.a., at forslaget vil kræve en særlig indsats i forhold til særligt sårbare grupper, og at forslaget vil medføre, at en række ikke nærmere definerede udbydere kommer til at have en lang række personfølsomme data liggende, f.eks. kopier af billedlegitimation. Endvidere anfører IDA, at der ikke vil være garanti for, at det vil kunne forhindre eller mindske fortsat organiseret kriminalitet. IDA kan derfor ikke bakke op om denne del af forslaget.

IT-Politisk Forening bemærker, at lovforslaget indfører en generel pligt til registrering og verificering af nummeroplysningsdata, inklusive for taletidskort, hvor dette vil være meget byrdefuldt. Selvom 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.

Foreningen anfører, at 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. 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 bl.a. 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. 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. 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. IT-Politisk Forening finder det principielt forkert, at borgerne skal registreres hos staten som betingelse for at få "lov" til at kommunikere med hinanden via telefoni.

Foreningen har endvidere for så vidt angår udbyderes registrering og verificering af brugere af taletidskort bemærket, at registreringen og verificeringen kan 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. 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 den foreslåede § 786 h i retsplejeloven og de almindelige bemærkninger pkt. 3.4.2. Efterregistrering af taletidskort vil være en meget kompliceret opgave og givetvis forbundet med ganske betydelige udgifter. 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. 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. 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 apps. De potentielle fordele for politiet ved en køberregistrering af taletidskort i 2021 er således væsentligt mindre end tidligere.

IT-Politisk Forening anfører videre, at for de personer, som bliver berørt af krav om registrering for så vidt angår taletidskort, 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. 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 dokumentation for deres identitet, som køberregistreringen kræver. En del taletidskort sælges via kiosker, og hvis disse salgssteder fremover skal opbevare kopier af ID-dokumenter eller andre registreringer baseret på fremvisning af ID-dokumenter, vil der blive skabt nye risici for identitetstyveri. Online-registrering med NemID er ikke en mulighed for alle, eksempelvis personer, som kun opholder sig midlertidigt i Danmark. Det er heller ikke alle fastboende borgere, som har NemID. IT-Politisk Forening opfordrer Justitsministeriet til at foretage en grundig analyse af konsekvenserne, herunder de menneskeretlige aspekter, inden en eventuel bekendtgørelse om registrering af taletidskort sendes i høring.

PROSA bemærker, at borgerne som udgangspunkt har ret til et privatliv, og at man derfor også skal have lov til at købe anonyme taletidskort. Forbundet anfører endvidere, at da der i dag ikke er en infrastruktur til at foretage den obligatoriske registrering af disse kort, og da de udgør en mindre del af markedet, bør det undersøges, hvilke økonomiske konsekvenser forslaget vil have. PROSA anfører desuden, at hvis anonyme taletidskort er særligt problematiske for politiet, så er forbundet åbne over for at gøre det nemmere at få retskendelse til at overvåge den type kort.

TI bemærker, at forslaget om registrering af unikt ID og indberetning af CPR/CVR/Unikt ID for alle kunder samt oplysning om forventet bruger til en fælles nummeroplysningsdatabase (118-databasen) ikke er proportionalt henset til kriminelles lette muligheder for ikke at blive registreret og den deraf følgende begrænsede efterforskningsmæssige værdi, sammenholdt med den estimerede omkostningsbyrde for telebranchen, som udgør over halvdelen af den samlede omkostningsmæssige byrde forbundet med lovudkastet. Gennemførelsen af forslaget vil kræve betydelige ændringer i processer og it-systemer hos teleudbyderne og vil koste telebranchen langt over 100 mio. kr. i tilpasning af it-systemer og et større tocifret millionbeløb i løbende årlige administrative driftsomkostninger. Forslaget tegner sig således for over halvdelen af lovforslagets samlede økonomiske byrde for telebranchen – og synes allerede af den grund ikke at være berettiget og proportionalt.

Herudover anfører TI, at forslaget ikke er nødvendigt for at sikre Danmarks efterlevelse af EU-dommene om målrettet logning. Forslaget ses heller ikke

at være nødvendigt i forhold til indførelsen af de nye regler om målrettet logning, idet politiet allerede i dag via politiets eksisterende adgang til 118-databasen kan identificere, hvilke telefonnumre der er registreret i navngivne fokuspersoners navn, og på den baggrund iværksætte målrettet personbestemt logning for sådanne telefonnumre. Det bemærkes, at denne adgang i flere årtier har været tilstrækkelig til, at politiet har kunnet identificere konkrete mistænkte med henblik på at foretage indgreb i meddelelseshemmeligheden og udlevering af teleoplysninger.

TI anfører desuden, at forslaget bygger på den misforståelse, at der kan ske en "entydig identifikation af brugeren af et givet kommunikationsmiddel". Forslaget vil imidlertid ikke sikre politiet konkret og reel viden om, hvilke telefonnumre og kommunikationsmidler kriminelle og andre fokus-personer benytter, idet kriminelle let vil kunne få brugeradgang til telefonabonnementer uden registrering, uanset gennemførelse af forslaget. Det er således ikke usædvanligt, at en privatkunde tegner abonnement på to abonnementer til eget brug, og kriminelle kan derfor let undgå registrering ved at få en anden person til at oprette abonnement i eget navn (stråmand) og overlade abonnementet til fokuspersonen, eller en mobiltelefon kan lånes af en ven eller et familiemedlem. Henset til omgåelsesmuligheden og den deraf følgende begrænsede efterforskningsmæssige værdi sat over for den estimerede omkostningsbyrde for telebranchen forekommer forslaget således ikke at være proportionalt.

TI opfordrer derfor til, at denne del udgår af lovudkastet eller udskydes med henblik på at nedsætte en arbejdsgruppe til nærmere analyse af politiets behov for adgang til verificerede nummeroplysningsdata og alternative løsningsmodeller, som er mindre byrdefulde for branchen.

Herudover anfører TI, at såfremt Justitsministeriet fortsat finder, at der er behov for at stille krav ud over CPR-registrering i kundesystemer og datavask inden levering til 118-databasen, opfordrer TI til, at lovforslag om sådanne regler udskydes med henblik på at nedsætte en arbejdsgruppe til nærmere analyse af politiets behov for adgang til kundedata om de danske telekunder og alternative løsningsmodeller.

TI anfører endvidere, at forsyningspligtudbyderen (TDC/Nuuday) ønsker at fremhæve, at selskabet stærkt frabeder sig at skulle registrere CPR-numre i den landsdækkende nummeroplysningsdatabase (118-databasen), dels hen-

set til persondataretlige betænkeligheder, dels henset til at der vil skulle påregnes store ekstraomkostninger, hvis det skal sikres, at 118-databasen fremover udelukkende supporteres fra EU.

TI bemærker også, at spørgsmålet om opbevaring af nummeroplysningsdata i EU eller tredjelande er kort omtalt i lovudkastet, men det fremgår ikke, om Justitsministeriets vurdering vedrører de gældende regler om nummeroplysningsdata eller de foreslåede nye regler om at registrere indberettede CPR-numre m.v. i 118-databasen – ligesom Justitsministeriets vurdering af spørgsmålet om opbevaring i EU kun forholder sig til Tele2-dommen om logning af trafikdata, men ikke forholder sig til Schrems II-dommen og spørgsmålet om opbevaring af kundedata/CPR m.v. i tredjelande, herunder it-supportadgang fra tredjelande. TI anmoder om, at bemærkningerne tydeliggøres og præciseres på disse punkter, så det står klart, hvilke nye krav der vil blive stillet til forsyningspligtudbyderen mht. it-løsning for 118-databasen, hvis teleudbyderne skal indberette CPR-numre hertil.

TI bemærker desuden, at lovudkastets forslag til ændring af telelovens § 31, stk. 2, hvorefter "Unikt ID" foreslås at indgå i definitionen af "nummeroplysningsdata", vil få den afledte konsekvens, at teleudbyderne vil blive forpligtede til at afgive CPR/CVR/unikt ID "til alle, der ønsker det", jf. telelovens § 31, stk. 1, medmindre kunden er registreret med hemmeligt eller udeladt nummer. Et krav om sådant videresalg af telekundernes CPR/CVR/ID er næppe tilsigtet. TI er opmærksom på lovbemærkningerne, pkt. 3.8., hvoraf det fremgår, at der med lovændringen ikke tilsigtes en generel videregivelse til nummeroplysningsdata-baser af unikke ID, herunder CPR-numre. TI bemærker hertil, at ordlyden af selve bestemmelsen i telelovens § 31, stk. 1, og den foreslåede ændring til telelovens § 31, stk. 2, fører til den modsatte forståelse, og at en model, hvor lovregler fraviges i en underliggende bekendtgørelse, ikke synes hensigtsmæssig.

Endvidere bemærker TI, at lovudkastets forslag til ændring af telelovens § 31, stk. 2, også vil få den afledte konsekvens, at teleudbyderne vil blive forpligtede til at afgive oplysning om eventuel registreret bruger til "til alle, der ønsker det", jf. telelovens § 31, stk. 1, medmindre kunden er registreret med hemmeligt eller udeladt nummer. TI bemærker hertil, at registrering af bruger indebærer stor persondataretlig kompleksitet i forhold til netop spørgsmålet om videregivelse af data om brugerens navn og adresse til brug for nummeroplysningstjenester inkl. 118-databasen, herunder om oplysning om brugeren, kunden eller begge skal videregives "til alle der ønsker det", jf.

telelovens § 31, stk. 1. Spørgsmålet om videregivelse af nummeroplysningsdata for abonnementer, hvor der ud over kundens navn og adresse også er registreret brugerens navn og adresse, er ikke reguleret i den gældende bekendtgørelse om nummeroplysningsdatabaser og kan ikke umiddelbart reguleres uden afklaring af spørgsmålet om brugerens stillingtagen til spørgsmålet om registrering og videregivelse af data om brugerens navn og adresse. Det er på denne baggrund TI's opfattelse, at registrering af eventuel bruger i nummeroplysningsdatabaser kræver forudgående accept fra brugeren, og at der derfor ikke giver mening at stille krav i lovudkastet om, at teleudbydere skal indrette proces for dialog med kunden om forventet bruger og registrere forventet bruger samt indberette oplysningen til 118-databasen. Det er TI's opfattelse, at brugerregistrering som hidtil kun kan tilbydes som en service fra de selskaber, der ønsker at tilbyde brugere en sådan registrering.

Endelig bemærker TI for så vidt angår taletidskort, at krav om registrering af nye taletidskort vil medføre en ekstrem forretningsmæssig omvæltning og negativ økonomisk påvirkning for en række udbydere. Kravet nødvendiggør, at operatørerne udvikler nye systemer til brug for kundernes selvbetjening og angivelse af de krævede personlige oplysninger samt automatisk kundeverifikationsopslag i CPR-registeret. Disse systemer er ikke udviklet i dag, og kræver en grundlæggende omstilling af virksomhedernes forretningsgange.

Retspolitisk Forening bemærker, at muligheden for at oprette uregistrerede taletidskort med lovforslaget foreslås helt afskaffet med den begrundelse, at mange kriminalle benytter sig af denne mulighed for at undgå at blive aflyttet og overvåget. Men mange almindelige mennesker vil blive ramt, typisk folk som ikke har råd til at betale et almindelige abonnement.

Justitsministeriet anerkender, at forslaget om, at der skal stilles krav om, at udbyderne, herunder også udbydere af taletidskort, skal registrere og verificere unikt ID, ikke i sig selv vil kunne garantere, at oplysninger om slutbrugeren og brugeren er korrekte. Det fremgår således bl.a. også af lovforslaget, at det f.eks. ikke kan udelukkes, at en slutbruger forsætligt afgiver oplysninger til udbyderen, der kan verificeres, men ikke er korrekte. Det kan f.eks. være tilfældet, hvis personen har begået identitetstyveri og på den baggrund misbruger en anden persons personlige oplysninger i forbindelse med afgivelse af oplysning om nummeroplysningsdata. Der henvises til pkt. 3.4.2 i lovforslagets almindelige bemærkninger.

Det er imidlertid Justitsministeriets opfattelse, at forslaget om at registrere og verificere unikt ID vil sikre, at der i videst muligt omfang kan ske en entydig identifikation af slutbrugeren/brugeren af et givet kommunikationsmiddel, og at verifikationen vil medføre, at identifikationen i videst muligt omfang er korrekt. Dette anses som afgørende for den foreslåede ordning om målrettet personbestemt registrering og opbevaring af trafikdata, at der i videst muligt omfang kan ske en entydig identifikation af slutbrugeren/brugeren af et givet kommunikationsmiddel, og at denne identifikation verificeres, så den i videst muligt omfang er korrekt. Dels for i videst mulig omfang at undgå, at der sker uforvarende registrering og opbevaring af forkerte personers trafikdata, dels for så vidt muligt at sikre, at der af hensyn til bekæmpelse af grov kriminalitet også kan findes frem til de personer og alle de telefonnumre, de er registreret til, der efter lovforslaget kan iværksættes registrering og opbevaring vedrørende.

I relation til TI's bemærkning om, at forsyningspligtsudbyderen frabeder sig at skulle registrere personnumre i den landsdækkende nummeroplysningsdatabase (118-databasen), dels henset til persondataretlige betænkeligheder, dels henset til at der vil skulle påregnes store ekstraomkostninger, hvis det skal sikres, at 118-databasen fremover udelukkende supporteres fra EU, bemærkes det, at det af de specielle bemærkninger til den foreslåede § 786 g i retsplejeloven fremgår, at nummeroplysningsdata som defineret i § 31, stk. 2, i teleloven, og som udbydere bl.a. skal indsamle og registrere til brug for nummeroplysningsdatabasen, jf. bekendtgørelse nr. 435 af 9. maj 2011 om nummeroplysningsdatabaser, ikke vil være omfattet af bestemmelsen. Med lovforslaget lægges der således ikke op til at stille særskilt krav til, at nummeroplysningsdata opbevares på servere i EU.

Det følger af databeskyttelsesforordningen, at overførsel af personoplysninger til et tredjeland skal ske inden for rammerne af forordningens kapitel V (artikel 44-50). Efter forordningens artikel 46, stk. 2, kan overførsel bl.a. ske, hvis der stilles fornødne garantier m.v., gennem standardbestemmelser om databeskyttelse (dvs. kontraktskabeloner, som udfyldes og underskrives af dataeksportøren og dataimportøren) vedtaget af Europa-Kommissionen.

Lovforslagets § 2, nr. 2, hvorefter udbyderne fremadrettet også vil skulle registrere unikt ID og eventuelle oplysninger om bruger som nummeroplysningsdata, ændrer ikke ved den vurdering, der skal foretages efter reglerne

i databeskyttelsesforordningen, når personoplysninger ønskes opbevaret uden for EU.

Justitsministeriet bemærker til IT-Politisk Forenings bemærkninger om, at registrering og verificering af taletidskort vil være ganske kompliceret, at det i lovforslaget forudsættes, at der fastsættes regler om, at uregistrerede taletidskort skal være omfattet af de samme krav om registrering og verificering af nummeroplysningsdata som andre abonnenter i nummeroplysningsbekendtgørelsen. Dette for at sikre, at også sådanne udbydere skal leve op til kravene i bekendtgørelsen med henblik på, at det ikke længere vil være muligt at købe uregistrerede taletidskort. Det er Justitsministeriets opfattelse, at dette kan medvirke til at begrænse den væsentlige omgåelsesrisiko, som brugen af uregistrerede taletidskort udgør, og som allerede i dag udnyttes af organiserede kriminelle m.v. Justitsministeriet bemærker i den forbindelse, at registreringen af uregistrerede taletidskort ikke i sig selv vil kunne forhindre kriminelle i at kommunikere anonymt på anden vis.

Der forudsættes ikke med lovforslaget fastsat krav til, hvordan verificering af unikt ID skal foretages, hvorfor udbyderne inden for lovforslagets rammer vil kunne finde den model for understøttelse af verificering, der passer bedst med deres forretningsmodel. Der henvises til pkt. 3.4.2 i lovforslagets almindelige bemærkninger. Justitsministeriet bemærker i denne forbindelse, at der efter det oplyste er andre lande i EU, hvor det ikke er muligt at købe uregistrerede taletidskort.

Til TI's bemærkninger om, at lovforslagets § 2, nr. 2, om, at telelovens § 31, stk. 2, bl.a. fremover også skal omfatte unikt ID, vil medføre, at udbyderne vil blive forpligtet til at afgive unikt ID til alle datakøbere, bemærker Justitsministeriet, at det fremgår af pkt. 3.8 i lovforslagets almindelige bemærkninger, at regler om videregivelse af oplysninger om unikt ID forudsættes udmøntet i bekendtgørelsen om nummeroplysningsdatabaser således, at oplysninger herom kun vil kunne videregives til forsyningspligtudbyderens landsdækkende nummeroplysningstjeneste (118-databasen). Med lovændringen tilsigtes der således ikke en generel videregivelse til nummeroplysningsdatabaser af unikke ID, herunder personnumre.

For nærmere om de administrative omkostninger for erhvervet henvises til pkt. 16 i den kommenterede høringsoversigt.

9. De foreslåede udbyderbegreber

Danske Advokater anbefaler, at udbyderbegrebet for al logning (målrettet såvel som generel) begrænses yderligere til kun at gælde for de udbydere, der udbyder til slutbrugere (eller anden tilsvarende begrænsning, som sikrer mod dublering af forpligtelserne), at det yderligere kvalificeres til at angå udbydere af en særlig størrelse (eks. baseret på antal abonnenter), og at der endvidere gives mulighed for outsourcing af logningsforpligtelsen, herunder det døgnbetjente kontaktpunkt.

Foreningen anbefaler også, at det overvejes, hvordan og i hvilket omfang udbyderne får kendskab og adgang til baggrunden for den målrettede logning ud fra et persondataretligt og informationssikkerhedsmæssigt perspektiv.

Endelig anbefaler Danske Advokater, at processen for sikkerhedsgodkendelse af de relevante medarbejdere effektiviseres, og at processens transparens øges i det omfang, at det sikkerhedsmæssigt tillades.

Fiberby bemærker, at det er uklart, hvilke udbydere der er omfattet af hvilke forpligtelser. Lovudkastet er generelt formuleret med stort fokus på telefoni. Generelt bruges begrebet "udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden" på tværs af lovudkastet. Fiberby antager sig, fordi Fiberby driver et kommunikationsnetværk og udbyder en kommunikationstjeneste som hovedydelse, for omfattet af begrebet.

Fiberby forstår forslaget sådan, at registrering og opbevaring fremover vil kunne iværksættes for de data, der er registrerings- og opbevaringspligtige i dag. Fiberby antager, at det er meningen at de foreslåede §§ 786 b-d i retsplejeloven også skal omfatte internetudbydere og adgang til internettet. Den foreslåede § 786 f gør dog at, udbyderne skal opsamle trafikdata uanset de foreslåede §§ 786 b-e, og dermed mener Fiberby ikke, at det giver mening at pålægge en udbyder som Fiberby forpligtelserne i de foreslåede §§ 786 b-786 e. Fiberby mener, at intentionen er, at de foreslåede §§ 786 b-d kommer til at genindføre sessionslogningen eventuelt på et senere tidspunkt, for i første omgang at kunne harmonere med begrænsningen til data, der er registrerings- og opbevaringspligtige i dag. Fiberby mener ikke, at teksten om sessionslogning i pkt. 3.3.3 udelukker, at sessionslogning kan indføres, men

at det blot vurderes, at dette vil kræve en begrænsning mht. udlevering. En genindførsel af sessionslogning vil være forbundet med store omkostninger til udvikling, hardware og lagring af loggede oplysninger. Fiberby henviser til IT-Politisk Forenings høringssvar for argumentationen mod sessionslogning ift. EU-domstolens praksis. Fiberby anbefaler, at internetudbydere med fast leveringspunkt fritages for §§ 786 b-e, samt at sessionslogning ikke genindføres.

HORESTA anfører, at hoteller, restauranter og andre turismevirksomheder fortsat – bortset fra i tilknytning til de foreslåede regler om målrettet logning – er at anse for udbydere mere generelt. Det gælder f.eks. i forhold til oplysningerne i logningsbekendtgørelsens § 5, stk. 2, som der lægges op til fortsat skal logges. HORESTA finder det positivt, at man afskaffede reglerne om sessionslogning, men det er fortsat uklart, hvorfor reglerne i logningsbekendtgørelsens § 5, stk. 2, som alene er formelle oplysninger om brugerne, blev fastholdt, når reglerne om sessionslogning blev ophævet. Ifølge HORESTA er det således uklart, hvad de oplysninger, som gemmes efter logningsbekendtgørelsens § 5, skt. 2, kan og skal bruges til. Hoteller og andre udbydere vil med forslaget om at videreføre denne forpligtelse fortsat skulle fastholde og betale for et teknisk setup, som kan registrere og gemme de oplysninger, der fremgår af logningsbekendtgørelsens § 5, stk. 2. HORESTA anfører videre, at det er HORESTAs opfattelse, at logningsreglerne afstedkommer en væsentlig belastning for deres medlemmer, som grundlæggende ikke står mål med, i hvilket omfang myndighederne anvender logningsoplysningerne i deres arbejde.

Hertil bemærker HORESTA, at f.eks. offentlige biblioteker, skoler m.v. aldrig har været underlagt logningsreglerne. Heller ikke private udbydere af overnatninger i form af f.eks. sommerhusudlejning og udlejning via f.eks. bureauer som Airbnb er omfattede af logningsforpligtelsen. Udover at der dermed også her er et "hul", så er der også tale om konkurrenceforvridning, idet sommerhusudlejning og privat udlejning via f.eks. Airbnb ikke pålægges samme forpligtelser og administrative byrder og udgifter som traditionelle overnatningsvirksomheder gør.

HORESTA anbefaler, at den forpligtelse, der i dag følger af logningsbekendtgørelsens § 5, stk. 2, ikke videreføres. Alternativt foreslås det, at hoteller, restauranter og andre turismevirksomheder helt udeholdes fra udbyderbegreberne.

IT-Politisk Forening anbefaler, 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 de foreslåede §§ 786 b-786 d i retsplejeloven), uanset om der er tale om generel og udifferentieret 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.

TI anmoder om, at det tydeliggøres i lovforslaget, hvilke udbydere der er omfattet af de nye regler. TI anfører, at det af lovforslaget fremgår, at "hvis de omfattede oplysninger kan registreres af flere udbydere, skal oplysningerne registreres og opbevares af mindst én af udbyderne." Det følger desuden af teleloven § 10, at logningsforpligtelsen m.v. påhviler "udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere". TI bemærker hertil, at telelovens § 10 mangler i lovudkastets gennemgang af de gældende regler.

Det anførte i lovudkastet og i den gældende telelovs § 10 skaber ifølge TI usikkerhed om, hvem der er forpligtet til at sikre, at logning af trafikdata er en mulighed, jf. de foreslåede §§ 786 b-786 e i retsplejeloven. "Udbydere af tjenester til slutbrugere" er de teleudbydere, som sælger abonnementer til slutkunder, herunder gensælgere, og der findes mere end 100 sådanne udbydere i Danmark. Disse mange tjenesteudbydere besidder oftest ikke trafik- og lokaliseringsdata. TI anbefaler derfor, at tilføjelsen "… til slutbrugere" slettes i telelovens § 10.

TI foreslår endvidere, at det præciseres i lovforslaget, at pligtsubjektet er den udbyder af elektroniske kommunikationsnet eller -tjenester, der producerer den tjeneste, som genererer de logningspligtige oplysninger (den tjenesteproducerende udbyder) – dvs. normalt netværksoperatøren. Det skal stå klart, at det primært er netværksoperatørerne og de udbydere, der driver centralerne, herunder de fire store danske mobilnet-værkoperatører Telia, Telenor, TDC Net og Hi3G, der er pligtsubjekt ift. logning og hastesikring af trafik- og lokaliseringsdata, men at det er udbydere af tjenester til slutbrugere, der besidder kundedata.

TI anfører desuden, at begrebet "den dataansvarlige", som det fremgår af lovudkastet, bør rettes til "den tjenesteproducerende udbyder".

Herudover foreslår TI, at man forenkler beskrivelsen af pligtsubjektet i lovforslaget.

Justitsministeriet bemærker, at der i høringsversionen af lovudkastet var lagt op til at anvende to forskellige udbyderbegreber. For så vidt angår de foreslåede §§ 786 e-786 h i retsplejeloven var der lagt op til, at forpligtelsen skulle gælde udbydere af elektroniske kommunikationsnet eller -tjenester. For så vidt angår den foreslåede ordning med målrettet registrering og opbevaring, jf. de foreslåede §§ 786 b-786 d i retsplejeloven, var der lagt op til en indskrænkelse af udbyderbegrebet, så forpligtelsen alene skulle gælde erhvervsmæssige udbydere, dvs. udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden.

Som det fremgår af pkt. 3.1.3.1 i lovforslagets almindelige bemærkninger, skyldtes forslaget om indskrænkelsen i udbyderbegrebet for så vidt angår den foreslåede målrettede registrering og opbevaring, at en anvendelse af det vide udbyderbegreb, der gjaldt for de foreslåede §§ 786 e-786 h i retsplejeloven, ville føre til, at samtlige udbydere af elektroniske kommunikationsnet eller -tjenester, herunder f.eks. også restauranter, caféer, campingpladser og hoteller, der eksempelvis tilbyder adgang til et trådløst internet-hot spot, ville skulle have oplysninger om, hvilke personer og områder der vil skulle registreres og opbevares oplysninger for i medfør af de foreslåede §§ 786 b-786 d i retsplejeloven.

Dette skal imidlertid ses i lyset af, at der i høringsversionen af lovforslaget var lagt op til at forpligte de relevante udbydere direkte i de foreslåede §§ 786 b og 786 c i retsplejeloven i lovteksten. Selvom det var beskrevet i bemærkningerne, at pligten for udbyderne først vil indtræde, når udbyderne har modtaget tilstrækkelige oplysninger fra myndighederne til at iværksætte målrettet registrering og opbevaring af trafikdata, vurderes det mest hensigtsmæssigt, at lovforslaget ændres, så det også direkte af lovteksten i de foreslåede §§ 786 b og 786 c i retsplejeloven fremgår, at Rigspolitiet skal meddele udbyderne pålæg om målrettet registrering og opbevaring af trafikdata, førend forpligtelsen indtræder for udbyderne. Det vil medføre øget klarhed over, hvilke udbydere der er omfattet af forpligtelsen til målrettet registrering og opbevaring af trafikdata, idet det alene vil være de udbydere, som Rigspolitiet retter pålæg om målrettet registrering og opbevaring af

trafikdata direkte til. På den måde vil Rigspolitiet desuden kunne rette pålæggene mod et begrænset antal udbydere og på den måde indsnævre antallet af udbydere, der får oplysninger om, hvilke personer og områder der vil skulle registreres og opbevares oplysninger for efter pålæg udstedt i medfør af de foreslåede §§ 786 b- 786 d i retsplejeloven.

På den baggrund vurderes det ikke længere nødvendigt at operere med forskellige udbyderbegreber i lovforslaget. Der lægges derfor op til, at lovforslaget justeres, så der fremadrettet anvendes begrebet "udbydere", som skal forstås i overensstemmelse med samme udtryk i telelovens § 2, nr. 1, hvilket vil fremgå klart af lovforslagets bemærkninger. Det vil også betyde, at der generelt arbejdes med samme udbyderbegreb som det, der kendes fra den gældende logningsbekendtgørelse, og som i øvrigt svarer til det, der bruges i telelovgivningen.

Der lægges ikke med dette lovforslag op til at ændre på de udbyderbegreber, der ellers anvendes i telelovgivningen.

Der lægges heller ikke med dette lovforslag op til at ændre reglerne for sikkerhedsgodkendelse.

Justitsministeriet bemærker desuden, at begrebet "den dataansvarlige udbyder" i lovforslaget er ændret til "den tjenesteproducerende udbyder".

Justitsministeriet bemærker endelig, at telelovens § 10 pålægger "udbydere af kommunikationsnet eller -tjenester til slutbrugere" en pligt til bl.a. at indrette det tekniske udstyr og de tekniske systemer, som udbyderen anvender, så politiet kan få adgang til registrerings- og opbevaringspligtige oplysninger efter lovforslaget. Ved udbydere til slutbrugere forstås parter, som på kommercielt grundlag stiller net eller tjenester til rådighed for flere slutbrugere. Det omfatter derfor ikke udbydere, der alene udbyder adgang til kommunikationsnet på engrosmarkedet, f.eks. ejere af fibernet, som andre selskaber udbyder til slutbrugere. Det fremgår af forarbejderne til bestemmelsen, at det ikke er nødvendigt at pålægge alle led i værdikæden en sådan forpligtelse for at opnå formålet med indgreb i meddelelseshemmeligheden.

Udbyderbegrebet i den gældende § 786, stk. 4, i retsplejeloven, er ikke afgrænset til "udbydere til slutbrugere" som i telelovens § 10. Da lovforslagets udbyderbegreb er en videreførelse af det gældende begreb i retsplejeloven, er det Justitsministeriets opfattelse, at det ikke er nødvendigt eller

hensigtsmæssigt at ændre udbyderbegrebet i telelovens § 10. Justitsministeriet lægger herved vægt på, at det efter bemærkningerne til bestemmelsen ikke er nødvendigt at pålægge alle udbydere i værdikæden en sådan forpligtelse for at opnå formålet med indgreb i meddelelseshemmeligheden.

10. Afgrænsningen af registrerings- og opbevaringspligtige oplysninger

IT-Politisk Forening finder det positivt, at de logningspligtige trafikdata fastsættes direkte i loven frem for, at det gøres efterfølgende i bekendtgørelsesform (med undtagelse af logningspligten for slutbrugeres adgang til internettet, jf. den foreslåede § 786 f i retsplejeloven). 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.

Foreningen foreslår – idet det er hensigten, at logningspligten skal omfatte de samme trafikdata som i dag – at det for listen af trafikdata i pkt. 3.1.3.4 anføres, at nr. 1-7 gælder for fastnet- og mobiltelefoni samt SMS-, EMS- og MMS-kommunikation svarende til den gældende § 4 i logningsbekendtgørelsen.

IT-Politisk Forening anfører endvidere, at det bør 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. 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. Denne præcisering vil have betydning for pligten til at registrere den forbundne celle ved afsendelse af MMS-beskeder, hvis celler for MMS ikke teknisk kan udskilles fra den øvrige datatrafik.

Foreningen bemærker desuden, at der for telefonitjenester med lovforslaget vil blive indført en registreringspligt for slutbrugerens identitet, uanset om udbyderens har et forretningsmæssigt behov for at behandle disse oplysninger, jf. den foreslåede § 786 h i retsplejeloven. For øvrige tjenester (dvs. internetadgang) antager foreningen, at kun oplysninger, som af forretningsmæssige årsager genereres eller behandles i udbyderens systemer, er omfattet af logningspligten, ligesom det er tilfældet i dag.

TI bemærker, at det ikke er beskrevet i lovudkastet, hvilke teletjenester der er omfattet af logningsforpligtelsen i de enkelte bestemmelser. Rækkevidden af teleudbydernes forpligtelse er således ikke klart beskrevet i reglerne. Af lovforslagsbemærkningerne fremgår det dog, at logningsforpligtelserne vil omfatte de samme typer af trafikdata, som er omfattet af de gældende regler i logningsbekendtgørelsen.

TI anmoder om, at det tydeliggøres, hvilke tjenester der er omfattet af de nye regler.

TI bemærker desuden, at det ikke er anført i lovteksten, hvilke typer af trafikdata, der er omfattet af logningsforpligtelsen. Det fremgår således blot i de foreslåede §§ 786 b-786 e i retsplejeloven, at det påhviler udbyderne at foretage registrering og opbevaring af "trafikdata". Rækkevidden af teleudbydernes forpligtelse er således ikke klart beskrevet i lovforslaget.

TI anmoder om, at afgrænsningen af, hvilke typer af trafikdata der skal logges, i lighed med indholdet af reglerne i den gældende logningsbekendtgørelse oplistes direkte i reglerne og ikke kun beskrives i lovforslagets bemærkninger.

TI bemærker endvidere, at "navn og adresse på abonnenten eller den registrerede bruger", som er nævnt i opremsningen i §§ 4 og 5 i den gældende logningsbekendtgørelse, ikke bør nævnes i opremsningen af trafikdata, dels fordi sådanne kundedata/nummer-oplysningsdata ikke er trafikdata, dels fordi politiets adgang til disse data ikke er afgrænset til sager om efterforskning af grov kriminalitet. Nummeroplysningsdata findes således i 118-databasen, som politiet har umiddelbar adgang til uden kendelse.

Særligt for så vidt angår oplysninger om "identiteten på det benyttede kommunikationsudstyr", herunder IMEI-oplysninger, anbefaler TI, at det overvejes at fastsætte en selvstændig regel om logning af trafikdata, som viser sammenhængen mellem IMEI og IMSI og telefonnummer, men uden at vise sammenhængen med terminalens kommunikation eller lokalisering ("IMEI-oplysning"), og at der i denne regel tages stilling til, om log-ning af IMEI-oplysning kan foretages generelt, og hvor lang en opbevaringsperiode, der skal gælde. TI deltager gerne i en eventuel arbejdsgruppe til afklaring af de tekniske forhold vedrørende IMEI-oplysning.

For så vidt angår lokaliseringsdata for internetadgang/datakommunikation (MMS) noterer TI sig, at lovudkastet er afgrænset, så lokaliseringsdata/masteoplysninger ved internetadgang fra mobiltelefoner (datakommunikation) ikke er omfattet af krav om logning. Lokaliseringsdata/masteoplysninger ved internetadgang fra mobiltelefoner registreres kun i teleudbydernes analysesystemer til brug for fejlretning. Idet disse data efter forslaget ikke skal logges, giver det teleudbyderne mulighed for at vælge en teknisk løsning, som er delvist baseret på den eksisterende logning af trafikdata, som er baseret på data fra takseringssystemerne. TI anser det for at være en fejl, at reglerne i den gældende logningsbekendtgørelse ikke afgrænser kravet om logning af Celle-ID til kun af omfatte telefoni og SMS, idet dette var det eneste teknisk mulige ved udstedelsen af logningsbekendtgørelsen i 2007. TI anmoder om, at det præciseres i bemærkningerne til lovforslaget, at MMS-kommunikation også er datakommunikation (brug af internettet), og at der derfor ikke stilles krav om logning af lokaliseringsdata ifm. MMS-kommunikation.

TI bemærker også, at der i lovudkastets opremsning af datatyper, der skal logges, nævnes som nr. 6 "den eller de celler en mobiltelefon er forbundet til ved kommunikationens start og afslutning", som er samme tekst, som findes i § 5, nr. 6, i den gældende logningsbekendtgørelse. TI anmoder om, at teksten ikke videreføres i de nye logningsregler, idet teksten ikke er teknologineutral. For de nyere mobilteknologier, som er kommet til siden 2006, herunder VoLTE (4G taletelefoni, som er båret som da-tatrafik), registreres sidste celle ved taletelefoni kun i nogle tilfælde; og ved brug af WIFI-calling fra mobiltelefoner (opkald via en vilkårlig WiFi-forbindelse) registreres celle slette ikke. Det er således kun muligt at logge data, som i forvejen genereres og logges i mobilnetværkene, og der er derfor behov for, at krav om logning fastsættes enkelt og teknologineutralt. For at give udbyderne mulighed for at vælge fortsat at basere logning på CDR-data, anmoder TI konkret om, at teksten om registrering af lokaliseringsdata ifm. mobiltelefoni og SMS formuleres enkelt og teknologineutralt på følgende måde: "Registreret celle ved mobiltelefoni- og sms-kommunikation (lokaliseringsdata)".

TI bemærker, at det ikke giver mening at inddrage e-mailadresser i afgrænsningen af trafikdata, som telefoniudbyderne skal logge, jf. pkt. 8 og 9 i opremsningen over logningspligtige trafikdata i lovudkastet. Kravet om logning af mailadresse efter § 6 i den gældende logningsbekendtgørelse retter sig kun mod udbydere af internetadgangstjenester, jf. referencen i § 6 til

logningsbekendtgørelsens § 5 om logning af kilde-IP-adresser. Kravet om logning af mailadresse efter § 6 i den gældende logningsbekendtgørelse retter sig i øvrigt kun mod internetudbydernes egne e-mailtjenester. TI kan oplyse, at politiet kun ganske sjældent anmoder om levering af ydelsen "mailhistorik". Loggede data om e-mailadresser udleveres således kun ganske sjældent (hos TDC kun 3 gange inden for det sidste år). TI foreslår, at det overvejes at lade kravet om logning af e-mailadresser udgå af lovforslaget. Hvis krav om logning af e-mailadresser fastholdes, bør kravet – ligesom i de gældende regler i logningsbekendtgørelsen – fastsættes i tilknytning til reglen om logningskrav, som gælder for udbydere af internetadgangstjenester, dvs. i forlængelse af den foreslåede nye § 786 f i retsplejeloven om logning af kilde-IP-adresser, som også retter sig mod udbydere af internetadgangstjenester.

Justitsministeriet henviser til pkt. 3.1.3.4 i lovforslagets almindelige bemærkninger, hvoraf det bl.a. fremgår, at de foreslåede nye regler for registrering og opbevaring vil skulle omfatte de data, der er registrerings- og opbevaringspligtige i dag. Det vil sige de data, der efter retsplejelovens § 786, stk. 4, og regler udstedt i medfør heraf registreres og opbevares som »teletrafik« (trafikdata). Formålet med denne formulering har været at sikre, at der ikke sker en udvidelse af de omfattede registrerings- og opbevaringspligtige oplysninger i forhold til, hvad der efter retsplejelovens § 786, stk. 4, og regler udstedt i medfør heraf registreres og opbevares som teletrafik i dag. Justitsministeriet lægger derfor for så vidt angår de omfattede datatyper op til at anvende samme formuleringer, som fremgår af logningsbekendtgørelsen i dag.

Justitsministeriet bemærker, at lovforslaget er justeret, så det kommer til at fremgå klart, hvilke teletjenester de forskellige opremsninger af omfattede datatyper, der beskrives i lovforslagets almindelige og specielle bemærkninger vedrørende de foreslåede ordninger med målrettet samt generel og udifferentieret registrering og opbevaring af trafikdata, relaterer sig til.

Justitsministeriet bemærker desuden, at lovforslaget er justeret, så det nu klart fremgår klart af bemærkningerne til lovforslaget, at udbyderne alene vil være forpligtet til at foretage registrering og opbevaring af trafikdata, der genereres eller behandles i udbyderens net. Det betyder, at oplysninger om trafikdata, der f.eks. af tekniske grunde ikke generes eller behandles i udbyderens net, ikke skal registreres og opbevares. Det afgørende for, om trafikdata skal registreres og opbevares vil alene være, om en oplysning rent

faktisk genereres eller behandles i udbydernes systemer, også selv om det kun sker meget kortvarigt. Der henvises til pkt. 3.1.3.4 i lovforslagets almindelige bemærkninger.

Det er Justitsministeriets vurdering, at det er tilstrækkeligt, hvis uddybningen af, hvad der forstås ved de overordnede begreber vedrørende datatyper, der nævnes i de foreslåede bestemmelser i loven, fremgår klart af bemærkningerne til loven.

Justitsministeriet bemærker herudover, at der med lovforslaget lægges op til, at justitsministeren i en overgangsperiode – dvs. i perioden fra lovens ikrafttræden og indtil det tidspunkt, hvor den nødvendige it-systemunderstøttelse er etableret og klar til at blive sat i drift – vil kunne fastætte regler om fravigelse af lovens bestemmelser i de foreslåede §§ 786 b-786 d i retsplejeloven, herunder at reglerne helt eller delvist ikke skal anvendes, jf. lovforslagets § 3, stk. 4. Der vil f.eks. kunne fastsættes regler om, hvilke tjenester og datatyper den målrettede registrering og opbevaring i en overgangsperiode skal omfatte. Der vil også eksempelvis kunne fastsættes regler om, at kun dele af den målrettede registrering og opbevaring i en overgangsperiode skal sættes i kraft. Der lægges i den forbindelse ikke op til at bemyndige justitsministeren til at fastsætte andre betingelser for iværksættelse af den målrettede registrering og opbevaring af trafikdata end dem, som fremgår af de foreslåede §§ 786 b-786 d i retsplejeloven. Det forudsættes, at udviklingsarbejdet i relation til den nødvendige it-systemunderstøttelse generelt sker i dialog mellem de relevante myndigheder og telebranchen, således at det sikres, at den kommende it-systemunderstøttelse i Rigspolitiet er kompatibel med den it-systemunderstøttelse, ordningen forudsætter for så vidt angår udbyderne. Der henvises til det, der anføres under pkt. 15 i den kommenterede høringsoversigt og i pkt. 3.1.3.4 i lovforslagets almindelige bemærkninger.

Med hjemmel i lovforslagets § 3, stk. 4, vil der f.eks. – hvis drøftelserne mellem de relevante myndigheder og telebranchen måtte føre til det resultat – kunne fastsættes regler om, at der ikke stilles krav om registrering og opbevaring af lokaliseringsdata i forbindelse med MMS-kommunikation.

Det bemærkes også, at lovforslaget er justeret, så det nu fremgår af lovforslagets § 3, stk. 2, at justitsministeren fastsætter tidspunktet for ikrafttræden af lovens § 2, stk. 2. Det vil betyde, at udbyderne først på et tidspunkt

nærmere fastsat af justitsministeren skal være klar til at understøtte og administrere registrering af unikt ID og eventuelle oplysninger om bruger for slutbrugere. Lovforslagets § 2, nr. 2, relaterer sig bl.a. til den foreslåede ordning med målrettet registrering og opbevaring af trafikdata. Det forudsættes derfor, at lovforslagets § 2, nr. 2, sættes i kraft på det tidspunkt, der passer i forhold til de relevante regler om målrettet registrering og opbevaring af trafikdata i overgangsperioden. Forslaget skal således ses i sammenhæng med lovforslagets § 3, stk. 4, hvor det foreslås, at justitsministeren i en overgangsperiode kan fastsætte regler om fravigelse af de foreslåede §§ 786 b-786 d i retsplejeloven, herunder at reglerne helt eller delvist ikke skal anvendes. Der henvises til de specielle bemærkninger hertil.

11. Prøvelse, retssikkerhed, demokratisk kontrol og transparens

Amnesty bemærker, at beslutningen om at iværksætte generel og udifferentieret logning efter lovforslaget kan prøves ved en domstol, men efterretningsmateriale af fortrolig karakter vil være undtaget, såsom klassificerede oplysninger og analyser fra efterretningstjenesterne. Amnesty har svært ved at se, hvordan en domstol vil være i stand til at foretage en reel efterprøvelse af, om betingelserne for et påbud om logning er opfyldt, hvis domstolen samtidig er afskåret for at se det klassificeret materiale, der i sagens natur vil være de bærende elementer for den trusselsvurdering, der ligger til grund for at iværksætte logningen. Da en afgørelse om at iværksætte logningen skal gøres til genstand for en effektiv prøvelse ved domstol eller en uafhængig administrativ enhed med henblik på at kontrollere, om der faktisk foreligger en alvorlig trussel mod staten, vil denne ordning vil ikke leve op til EU-retten. Amnesty anbefaler, at man genovervejer, hvordan man kan sikre en effektiv domstolsprøvelse og i den forbindelse benytter sig af nogle af de særlige procedurer, der allerede er etableret i retssystemet til at håndtere sager af fortrolig karakter.

Citizen First anbefaler, at der i lovforslaget indbygges en eksplicit understøttelse af frivilligt selvinkriminerende sikkerhedsstrukturer, som ikke kan overvåges, dvs. en godkendelsesmodel til at undgå logning. En sådan model vil f.eks. kunne indebære, at borgeren har et chipkort tilknyttet MitID, som kan genere en ny ikke-linkbar kvalificeret digital signatur inkl. de nødvendige mekanismer til at bevise, at sessionen er afledt af en godkendt struktur. Herefter vil vedkommende kunne stilles til ansvar og/eller overvåges i forhold til det formål, som sessionen vedrører. Herved vil det sikres, at a) en borger kan gå sikkert på nettet og gennemføre digitale transaktioner sikkert,

hvorved både borgeren selv og alle involverede serviceleverandører sikres helt eller delvist mod cyberangreb, hvilket ikke er muligt i dag og ulovligt med det aktuelle forslag, b) det virker kriminalitetsforebyggende, fordi en stigende andel af samfundsprovesser vil forebygge kriminalitet, og ansvar vil være nemmere at etablere, og c) kriminelle vil få sværere ved at gemme sig, fordi det bliver mere acceptabelt at fokusere på restgruppen.

Danske Advokater bemærker, at med forslaget kan justitsministeren efter forhandling med erhvervsministeren iværksætte generel og udifferentieret logning, hvis det vurderes, at der foreligger en alvorlig trussel mod den nationale sikkerhed. Dette kan ske uden om Folketinget, og en sådan beslutning vil ikke være underlagt domstolskontrol. Danske Advokater mener, at det retssikkerhedsmæssigt er betænkeligt, og vil advare imod, at man vedtager lovforslaget i sin nuværende form. Beslutningen om at overgå til/fastholde generel og udifferentieret logning er ikke underlagt automatisk domstolskontrol. Beslutningen kan ifølge lovforslaget efterfølgende prøves ved domstolen efter Grundlovens § 63, idet de klassificerede oplysninger, der indgår i vurderingen af, om der er tale om en alvorlig trussel mod den nationale sikkerhed, dog ikke kan indgå. Det fremgår i den forbindelse af lovforslaget, at der derfor vil være en risiko for, at retten vurderer, at de oplysninger, der er fremlagt under sagens behandling, ikke er tilstrækkelige til at vurdere, om f.eks. betingelserne for at foretage generel og udifferentieret registrering og opbevaring af trafikdata er opfyldt. Denne manglende transparens og manglende retslige eller parlamentarisk prøvelse udgør en risiko for – eller i hvert fald manglende indsigt i – om der sker indførelse af generel og udifferentieret logning på et unødvendigt/retsstridigt grundlag. Lovforslagets bemærkning om, at såfremt retten under en sag måtte komme frem til, at betingelserne for en generel og udifferentieret registrering og opbevaring af trafikdata ikke er opfyldt, vil dette ikke være til hinder for, at den med lovforslaget foreslåede ordning for målrettet registrering og opbevaring af trafikdata iværksættes i muligt omfang, giver Danske Advokater anledning til bekymring for, at udgangspunktet bliver generel og udifferentieret logning, medmindre domstolen ved en sag anlagt af private med begrænset indsigt i grundlaget for vurderingen af "alvorlig trussel mod den nationale sikkerhed" skulle komme frem til det modsatte. I så henseende kan målrettet logning iværksættes. Danske Advokater anbefaler, at der indføres krav om i) mandat fra Folketinget, og ii) domstolsprøvelse ved iværksættelse, eller iii) tilsyn fra en uafhængig administrativ myndighed.

Fiberby foreslår, at der offentliggøres en årlig rapport med statistiske værdier omkring lovens anvendelse. Denne rapport bør indeholde følgende data omkring logningsmekanismen:

- Antal personer omfattet af personbestemt målrettet logning (§ 786 b).
- Antal 3 gange 3 km områder omfattet af geografisk målrettet logning (§ 786 c).
- Antal anvendelser af målrettet logning (§ 786 d).
- Antal dage i seneste kalenderår med generel og udifferentieret logning (§ 786 e).

Derudover bør rapporten indeholde følgende statistik omkring retssager:

- Antal domsfældelser opgjort per straffelovsparagraf, samt hvilken § 786 a-f logningen var udført efter.
- Antal editionskendelser opgjort per straffelovsparagraf.

Uden en sådan rapportering vil det ifølge Fiberby være umuligt at debattere lovgivningens anvendelighed, proportionalitet og effektivitet. Endelig bør den nye lovgivning også tilføjes en revisionsbestemmelse, gerne med et loft over, hvor mange gange den kan udskydes.

IDA anbefaler, at det skrives ind i lovforslaget, at der skal etableres skærpet tilsyn, f.eks. et tilsyn i tråd med Tilsynet med Efterretningstjenesterne udpeget af Folketinget. Dette gælder både perioder med målrettet logning og eventuelle perioder med generel og udifferentieret logning.

IT-Politisk Forening anfører i relation til domstolskontrol af påbud om logning til beskyttelse af den nationale sikkerhed, at det efter præmis 139 i La Qudrature du Net-dommen er væsentligt, at et påbud (afgørelse) om lagring kan gøres til genstand for effektiv prøvelse ved en domstol eller en uafhængig administrativ myndighed. Foreningen anerkender, at et påbud om forebyggende lagring af hensyn til beskyttelse af den nationale sikkerhed kan være truffet på grundlag af fortrolige efterretninger. En effektiv prøvelse af afgørelsen må imidlertid forudsætte, at domstolen eller den uafhængige administrative myndighed også har mulighed for at vurdere sådanne fortrolige oplysninger. 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.

Foreningen bemærker desuden, at Justitsministeriet i pkt. 3.6.3.1 anfører, 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 om generel og udifferentieret logning, kan de således antageligt imødese en langvarig proces ved domstolene, hvor Justitsministeriet først vil prøve at få sagen afvist med henvisning til manglende retlig interesse.

Herudover bemærker foreningen, at den domstolskontrol, som beskrives i pkt. 3.6.3.1, ikke kan opfylde EU-Domstolens krav. Dette skyldes for det første, at domstolen ikke vil 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. Realistisk set vil processen med et 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.

Justitsministeriets forslag vedrørende domstolskontrol vil ifølge IT-Politisk Forening 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.

For så vidt angår målrettet logning anfører IT-Politisk Forening, at lovforslaget mangler transparens. Både i relation til manglende underretning og manglende offentliggørelse af listen over geografiske områder, der vil være omfattet af den målrettede geografiske logning. 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. En anden konsekvens af den manglende transparens er, at det bliver vanskeligt for Folketinget eller civilsamfundsorganisationer at monitorere, om logningen er begrænset til det strengt nødvendige.

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. Det bør også gælde for den personbestemte målrettede logning i den foreslåede § 786 d i retsplejeloven. 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.

Justitia anfører, at lovudkastet ikke indeholder fornødne prøvelses- og kontrolforanstaltninger. For så vidt angår prøvelse af den generelle og udifferentierede logning anfører Justitia, at ifølge EU-retten skal en afgørelse om, at der logges generelt og udifferentieret, kunne gøres til genstand for effektiv prøvelse med henblik på at kontrollere, om betingelserne for logning er opfyldt. Forudsætningen i lovudkastet om, at de bagvedliggende klassificerede oplysninger, der ligger til grund for de analyseprodukter, der er anvendt i vurderingen, ikke udleveres til brug for en eventuel retssag, giver anledning til at overveje, om domstolsprøvelsen i så fald kan siges at være effektiv. Det forekommer ikke muligt for en domstol at foretage en egentlig vurdering af, om betingelserne for generel og udifferentieret logning er opfyldt, hvis det samlede faktuelle grundlag for beslutningen ikke kan indgå i rettens vurdering.

Justitia anbefaler, at det nøje genovervejes, hvordan der bedst muligt findes en balance mellem hensynet til effektiv prøvelse på den ene side og bevarelsen af fortrolighed på den anden side. Der kan i den forbindelse drages inspiration fra den proces, der anvendes i medfør af udlændingelovens kapitel 7b ved domstolsbehandling af visse beslutninger om administrativ udvisning m.v.

Justitia bemærker derudover, at domstolsprøvelsen giver anledning til at overveje spørgsmål vedrørende retlig interesse.

Endvidere anfører Justitia, at der – i tillæg til domstolsprøvelse – med fordel kan gives Datatilsynet og Tilsynet med Efterretningstjenesterne eksplicit hjemmel til at foretage legalitetskontrol af beslutninger om generel og udifferentieret logning.

For så vidt angår prøvelse af den målrettede logning anfører Justitia, at det ikke for alle former for målrettet logning i medfør af de foreslåede §§ 786 b og c i retsplejeloven er objektivt konstaterbart ved ren læsning af loven, herunder for den berørte, hvornår der logges. Justitia er opmærksom på, at legitime hensyn kan berettige, at de nærmere detaljer for, hvilke personer og områder der logges, ikke offentliggøres, så længe logningen pågår. Dog bør der ifølge Justitias opfattelse ske offentliggørelse/underretning af al målrettet logning, når disse hensyn ikke længere gør sig gældende – typisk ved ophøret af den pågældende logning. Dette vil etablere en reel adgang til prøvelse af den pågældende logning. I visse tilfælde vil omstændighederne bevirke, at der i en længere periode ikke kan ske offentliggørelse af/underretning om målrettet logning. For i videst muligt omfang at bevare retssikkerheden i disse tilfælde foreslås det at give Datatilsynet og Tilsynet med Efterretningstjenesterne eksplicit hjemmel til at foretage legalitetskontrol med den målrettede logning, der iværksættes. I henhold til lovudkastet er det desuden myndighederne, der på egen hånd skal udarbejde årlige oversigter over, hvilke geografiske områder, der skal underlægges logning i henhold til den foreslåede § 786, stk. 1 og 2. I den forbindelse er det væsentligt, at afgrænsningen af de særligt sikringskritiske områder, nødvendiggør en skønsmæssig vurdering. Den samlede oplistning af, hvad der kan udgøre særligt sikringskritiske områder, forekommer at kunne omfatte særdeles store dele af landet. Det forekommer ifølge Justitias opfattelse retssikkerhedsmæssigt betænkeligt, at myndighederne egenhændigt kan foretage vurderingen af, hvilke områder der skal omfattes af de årlige oversigter for geografisk målrettet logning, uden der samtidig gives nogen mulighed for prøvelse af disse vurderinger.

PROSA anfører, at der flere steder i revisionen lægges op til, at justitsministeren og erhvervsministeren kan iværksætte og forlænge indgribende logning. En sådan beslutning bør være en folketingsbeslutning – både for at skabe demokratisk legitimitet og for at skabe den fornødne transparens.

Forbundet bemærker desuden, at det bør være et krav, at revisionen sikrer, at der opsamles statistisk materiale, så man i fremtiden kan evaluere effekten af logningen, herunder hvor mange sager, man bruger bestemmelserne i, hvor mange af disse sager, der ikke førte til dom, hvor mange uskyldige, der blev logget m.v.

RfDS anfører, at der helt overordnet er behov for et overblik over den samlede overvågning af borgerne. Borgerne bør således bibringes et samlet

overblik over den statslige masseovervågning, der finder sted i det danske samfund, og på den baggrund bør der tages en værdipolitisk offentlig debat af det rimelige heri.

Herudover anfører RfDS også, at det i forhold til det konkrete lovforslag er bekymrende, at teleselskaberne har og fortsat får rollen som statens forlængede arm ud fra et generelt retssikkerhedsmæssigt perspektiv.

RfDS bemærker endvidere, at vurderingen af, om et forhold er omfattet af national sikkerhed, efterfølgende bør prøves ved domstolene således, at beslutninger om iværksættelsen af generel udifferentieret logning ikke ligger hos justitsministeren (sammen med erhvervsministeren) alene. For det første kunne det være hensigtsmæssigt med en bredere demokratisk kontrol – f.eks. en ekspertgruppe nedsat af Folketinget eller Tilsynet med Efterretningstjenesterne. For det andet bør iværksættelsen af den generelle udifferentierede logning automatisk efterfølgende prøves ved en dommer. Domstolene bør have adgang til alle relevante oplysninger. Ligeledes bør det i øvrigt prøves ved domstolen, om der kan iværksættes personbestemt og geografisk målrettet logning.

Desuden bemærker RfDS, at der bør udarbejdes en offentlig konsekvensanalyse fsva. logningsreglerne, så en proportionalitetsafvejning kan foretages. Rådet mener, der er behov for en bredere kortlægning og værdipolitisk debat om politiets efterhånden omfattende masseovervågning af borgernes data.

Som det fremgår af pkt. 3.6.3.1 i lovforslagets almindelige bemærkninger, foreslås der ikke indført særlige regler om domstolsprøvelse for så vidt angår den generelle og udifferentierede registrering og opbevaring. Kontrollen med denne registrering og opbevaring vil skulle ske efter den almindelige adgang til domstolsprøvelse, jf. grundlovens § 63.

Den almindelige domstolsprøvelse af øvrighedsmyndighedens grænser vil navnlig være relevant i forbindelse med en prøvelse af, om ordningen med generel og udifferentieret registrering og opbevaring med henblik på beskyttelse mod en alvorlig trussel mod den nationale sikkerhed er i overensstemmelse med bl.a. EU-retten. Prøvelsen vil normalt finde sted som et civilt søgsmål anlagt mod den relevante myndighed. Det vil afhænge af de almindelige civilprocessuelle regler, om et søgsmål kan anlægges, herunder navnlig reglerne om partshabilitet og retlig interesse. Det bemærkes i den

forbindelse, at lovforslaget er justeret, så det nu fremgår klart under pkt. 3.6.3.1 i lovforslagets almindelige bemærkninger, at det forudsættes, at enhver, der har været berørt af en iværksat generel og udifferentieret registrering og opbevaring af trafikdata, vil have den fornødne retlige interesse i at indbringe grundlaget herfor for retten i form af et civilt søgsmål. Dette skal ses i lyset af, at generel og udifferentieret registrering og opbevaring af trafikdata vil berøre alle personer, der befinder sig i Danmark. Det skal endvidere ses i lyset af, at EU-Domstolen i La Quadrature du Net-dommens præmis 139 anfører, at det er væsentligt, at en afgørelse, hvorved udbyderne pålægges at foretage generel og udifferentieret registrering og opbevaring af trafikdata, kan gøres til genstand for en effektiv prøvelse med henblik på at kontrollere, om der foreligger den fornødne alvorlige trussel mod den nationale sikkerhed, samt om de betingelser og garantier, der skal være fastsat, er overholdt.

Det bemærkes endvidere, at det forudsættes, at de bagvedliggende klassificerede oplysninger, der ligger til grund for vurderingen af, om der foreligger en alvorlig trussel mod den nationale sikkerhed, ikke vil kunne kræves udleveret til brug for en retssag, jf. bl.a. retsplejelovens § 169, stk. 2, 3. pkt. Det vil på den baggrund navnlig være selve vurderingen af, om der foreligger en alvorlig trussel mod den nationale sikkerhed, og de offentliggjorte produkter, der ligger til grund herfor, herunder den offentliggjorte VTD, andre relevante offentliggjorte analyseprodukter og eventuelle relevante oplysninger om offentlige straffesager om straffelovens kapitel 12 og 13, og ikke de bagvedliggende klassificerede oplysninger og analyser, der vil kunne indgå i vurderingen af, om betingelserne for at foretage generel og udifferentieret registrering og opbevaring af trafikdata er opfyldt.

Det vil i sidste ende være retten, som afgør, hvilken bevismæssig vægt fremlagte oplysninger skal tillægges i den enkelte sag, jf. princippet om den fri bevisbedømmelse. Retten vil på grundlag af det, der er passeret under forhandlingerne, og bevisførelsen afgøre, hvilke faktiske omstændigheder der skal lægges til grund for sagens pådømmelse, jf. retsplejelovens § 344. Såfremt retten under en sag måtte komme frem til, at betingelserne for en generel og udifferentieret registrering og opbevaring af trafikdata ikke er opfyldt, vil der efter forslaget i stedet skulle iværksættes målrettet registrering og opbevaring af trafikdata.

Det fremgår desuden af pkt. 3.6.3. i lovforslagets almindelige bemærkninger, at der ikke foreslås indført særlige regler om domstolsprøvelse for så

vidt angår den målrettede registrering og opbevaring af trafikdata på baggrund af objektive og klare kriterier fastsat i loven. Kontrollen med denne registrering og opbevaring vil således også skulle ske efter den almindelige adgang til domstolsprøvelse, jf. grundlovens § 63.

Kendetegnende for den generelle og udifferentierede registrering og opbevaring, der er omtalt i pkt. 3.2 og 3.3, og de dele af den målrettede registrering og opbevaring, som ikke iværksættes på baggrund af konkret begrundede pålæg, der er beskrevet i pkt. 3.1, er, at der ikke på samme måde som for de konkret begrundede pålæg skal foretages en vurdering af registreringen og opbevaringen af trafikdata i forhold til en konkret person eller et konkret område. I stedet vil den målrettede registrering og opbevaring skulle iværksættes ud fra klare og objektive kriterier, som er fastsat direkte i loven.

Det bemærkes, at der ikke vil blive offentliggjort en oversigt over de områder, der vil blive registreret og opbevaret oplysninger vedrørende som følge af de foreslåede pligter til målrettet geografisk registrering og opbevaring af trafikdata. Der henvises i den forbindelse til det under pkt. 3.1.3.4 i lovforslagets almindelige bemærkninger anførte om, at offentliggørelse af sådanne oplysninger bl.a. vil kunne skade myndighedernes muligheder for at efterforske og retsforfølge kriminalitet. Der henvises i øvrigt til det under pkt. 3.1.3.4 i lovforslagets almindelige bemærkninger anførte om forholdene omkring udbydernes udvælgelse af master til at dække et givet område. Der lægges dog med lovforslaget op til, at der fastsættes så klare og objektive kriterier for udvælgelsen af de områder, der kan iværksættes målrettet geografisk registrering og opbevaring af trafikdata vedrørende, i selve loven, at det ud fra disse kriterier vil være muligt at udlede, i hvilke områder der f.eks. vil være lav eller høj sandsynlighed for, at der vil blive registreret og opbevaret oplysninger på baggrund af den foreslåede ordning med målrettet registrering og opbevaring af trafikdata.

Det vil være tydeligt, hvornår der sker en generel og udifferentieret registrering og opbevaring på baggrund af en alvorlig trussel mod den nationale sikkerhed, idet dette vil fastsættes ved bekendtgørelse. Det vil efter forslaget endvidere gælde, at udbydernes pligt til at registrere oplysninger generelt og udifferentieret fastsat i medfør af den foreslåede § 786 e, stk. 1, i retsplejeloven højst vil kunne fastsættes for en periode på 1 år ad gangen.

Det vil desuden være tydeligt, hvornår der sker en generel og udifferentieret registrering og opbevaring af oplysninger om en slutbrugers adgang til internettet (herunder IP-adresser). Denne pligt vil således efter forslaget gælde helt generelt.

Herudover vil det være tydeligt, at der vil ske målrettet registrering og opbevaring af trafikdata vedrørende personer, som er dømt for grov kriminalitet, eller som har været genstand for et af de omfattede indgreb i meddelelseshemmeligheden, idet der foreslås fastsat objektivt konstaterbare og klare kriterier for iværksættelse af registrering og opbevaring af trafikdata for så vidt angår disse dele af den målrettede personbestemte ordning.

Det bemærkes i den forbindelse, at der ved behandlingen af en anmodning om aflytning eller teleoplysning vil være en indgrebsadvokat til stede, jf. retsplejelovens § 784. Der vil desuden som udgangspunkt skulle gives underretning om indgrebet til indehaveren af den pågældende telefon, jf. retsplejelovens § 788.

Det vil endvidere være tydeligt, at der vil ske målrettet geografisk registrering og opbevaring af trafikdata fra de dele af udbydernes net, der er nødvendigt for at dække nærmere bestemte områder på 3 km gange 3 km, hvor antallet af anmeldelser om og beboere dømt for grov kriminalitet udgør mindst 1,5 gange landsgennemsnittet opgjort som gennemsnit de sidste 3 år.

For så vidt angår de særligt sikringskritiske områder er der oplistet en lang række eksempler i de specielle bemærkninger til det foreslåede § 786 c, stk. 2, i retsplejeloven, jf. lovforslagets § 1, nr. 10.

Det er Justitsministeriets vurdering, at en prøvelse af, om den foreslåede ordning er i overensstemmelse med bl.a. EU-retten, mest hensigtsmæssigt sker inden for de almindelige rammer for domstolenes kontrol med øvrighedsmyndighedens grænser, hvilket normalt vil være et civilt søgsmål anlagt mod den relevante myndighed – i dette tilfælde Justitsministeriet.

Justitsministeriet bemærker herudover, at det ud fra samme betragtninger er Justitsministeriets opfattelse, at der for ordningerne med generel og udifferentieret registrering og opbevaring samt for de nævnte dele af ordningerne med målrettet registrering og opbevaring ikke vil være behov for at foretage underretning af de pågældende. Der henvises i den forbindelse til

det ovenfor anførte om, at det – på baggrund af de objektive og klare kriterier, der foreslås fastsat i loven for disse ordninger – vil være almindeligt kendt, at der i de omfattede tilfælde vil kunne foretages registrering og opbevaring.

Det bemærkes herudover, at det er Justitsministeriets vurdering, at der som i dag generelt bør ske domstolskontrol i forbindelse med, at politiet ønsker adgang til de registrerede og opbevarede oplysninger. Adgangen hertil vil efter forslaget – som i dag – skulle ske efter retsplejelovens regler om indgreb i meddelelseshemmeligheden eller om edition afhængigt af, hvilke oplysninger der er tale om. Dog med den forskel, at det for så vidt angår oplysninger, der er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven, vil være en betingelse for at få adgang til sådanne oplysninger, at det sker med henblik på bekæmpelse af grov kriminalitet, herunder beskyttelse af den nationale sikkerhed.

Endvidere bemærker Justitsministeriet, at der ikke med lovforslaget lægges op til at sætte generelle krav til sikkerhedsmekanismer på internettet m.v. Lovforslaget har således til formål at revidere de gældende regler om registrering og opbevaring af teletrafik m.v.

Endelig anerkender Justitsministeriet, at der med lovforslaget er tale om en nyskabelse i forhold til den gældende retstilstand, og at der kan vise sig behov for at revidere reglerne i takt med, at der indsamles erfaringer med den foreslåede ordning og administrationen heraf. De nye regler og virkningen heraf vil naturligvis løbende skulle evalueres i takt med, at de – og den nødvendige systemunderstøttelse – gradvist indfases.

12. Adgang til registrerede og opbevarede oplysninger

Amnesty anfører, at der efter Amnestys opfattelse ikke er grundlag for ud fra EU-Domstolens praksis at konkludere, at der må gives adgang til logningsdata under forfølgelsen af et formål, der er mindre tungtvejende end det formål, som gav adgang til at logge dataet. Amnesty finder det i den forbindelse bemærkelsesværdigt, at Justitsministeriet selv skriver, at der er en "væsentlig proces risiko" for, at disse regler i lovforslaget vil blive underkendt af EU-Domstolen. Amnesty anbefaler, at myndighederne kun har adgang til logningsdata genereret efter et påbud om generel og udifferentieret logning, hvis det er med henblik på at beskytte den nationale sikkerhed,

og at adgang ikke gives til andre mindre tungtvejende formål, såsom kriminalitetsbekæmpelse.

Danske Advokater mener ikke, at der er kongruens mellem det, der kan udløse en pligt til at foretage generel og udifferentieret logning, og det der kan ske udlevering af de pågældende oplysninger for.

Forsikring og Pension anfører, at forsikrings- og pensionsbranchen for at afdække potentielle sager om forsikrings- og pensionssvindel under særlige omstændigheder kan have behov for at undersøge tele- og masteoplysninger fra de skadelidtes mobiltelefoner, jf. bekendtgørelse om undersøgelser foretaget af forsikringsselskaber § 8. Forsikring og Pension er derfor ærgerlige over, at der i lovforslaget ikke åbnes op for en adgang til en hurtigere og mere smidig proces, hvor teledata og masteoplysninger med kundens udtrykkelige samtykke kan udveksles mellem tele- og forsikrings-/pensionsselskaberne.

IDA bemærker, at det foreslås, at der indsættes en skærpet udgave af telelovens § 13 med pligt til udlevering af yderligere oplysninger om en slutbrugers adgang til elektroniske kommunikationsnet eller -tjenester uden kendelse, herunder oplysninger om hvilke mobilabonnementer og kommunikationsenheder en slutbruger er registreret med. Hvis oplysningerne er relevante og afgørende for opklaringen af en sag, så kan det være helt reelt og rimeligt at få udleveret sådanne oplysninger, men det må være op til en dommer at afgøre dette. Denne del af forslaget er ifølge IDA endnu et eksempel på det skred væk fra proportionalitetsprincippet og mangel på respekt for borgernes grundlæggende rettigheder, som lovforslaget i sin helhed er udtryk for.

IMR bemærker, at Justitsministeriet i lovudkastet lægger op til, at politiet – under en væsentlig procesrisiko – skal kunne få adgang til oplysninger, som er indsamlet som følge af generel og udifferentieret logning, i sager om efterforskning m.v. af grov kriminalitet. Dette vil medføre, at politiet kan bruge loggede oplysninger i sager, der ikke i sig selv kunne begrunde generel og udifferentieret logning, da en sådan logning kræver en alvorlig trussel mod den nationale sikkerhed. Instituttet finder det problematisk, at skiftende regeringer siden 2016 har udskudt revisionen af logningsreglerne til trods for, at de er i strid med EU-retten, bl.a. med den begrundelse at ville sikre, at revisionen omfatter beskyttelsen af grundlæggende rettigheder i overensstemmelse med EU-retten, for efterfølgende at foreslå en ordning, der går

imod disse domme og dermed efter instituttets opfattelse med overvejende sandsynlighed er i strid med EU's Charter om Grundlæggende Rettigheder. Instituttet anbefaler, at politiets adgang til oplysninger, som er indsamlet som følge af generel og udifferentieret logning, begrænses til sager vedrørende beskyttelse af national sikkerhed.

IT-Politisk Forening anfører for så vidt angår adgang til oplysninger registreret og opbevaret i medfør af regler fastsat efter den foreslåede § 786 e i retsplejeloven, at når EU-Domstolen med La Quadrature du Net-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.

Efter IT-Politisk Forenings læsning af 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. Foreningen formoder, at en præjudiciel forelæggelse for EU-Domstolen om fortolkning af præmis 166 vil ske relativt hurtigt.

For så vidt angår adgang til andre registrerede og opbevarede oplysninger, anfører IT-Politisk Forening, at der er positivt, at Justitsministeriet nu foreslår ændringer af retsplejeloven med henblik på at bringe de danske retsregler i overensstemmelse med EU-retten. De foreslåede ændringer i den foreslåede § 804 a i retsplejeloven er imidlertid ikke tilstrækkelige. IT-Politisk Forening anbefaler, 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 vedrørende en person, som er mistænkt i efterforskningen. 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.

For så vidt angår adgang til oplysninger, der ikke er registrerings- og opbevaringspligtige, efter editionsreglerne anfører IT-Politisk Forening, at La Quadrature du Net-dommens kriminalitetskrav gælder, 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). Lovforslaget bør derfor ændres, således at den foreslåede § 804 a i retsplejeloven omfatter enhver adgang til trafikdata og lokaliseringsdata, som udgør et alvorligt indgreb efter EU-retten. Det er primært adgang til oplysninger om civil identitet, der ikke udgør et alvorligt indgreb.

For så vidt angår adgang til oplysninger om en bruger af en IP-adresse anfører foreningen, at politiets adgang til sådanne oplysninger bør ske via den foreslåede § 804 a i retsplejeloven med de ændringer, som foreningen foreslår ovenfor.

For så vidt angår adgang til udvidet teleoplysning/masteoplysning anfører IT-Politisk Forening, at udvidet teleoplysning og udvidet masteoplysning ikke er 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. 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. 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 vedrørende mistænkte personer. Det samme problem gælder for udvidet teleoplysning.

For så vidt angår underretning af den registrerede, når oplysninger udleveres til politiet, anfører IT-Politisk Forening, at der efter forslaget fortsat ikke vil ske underretning af de(n) berørte person(er) ved udvidet teleoplysning og udlevering af oplysninger via den almindelige editionsbestemmelse i § 804 i retsplejeloven. Det er efter foreningens opfattelse i strid med EU-retten,

som generelt kræver underretning af de berørte personer, når virksomheder udleverer personoplysninger om dem til politiet, idet en sådan underretning er en forudsætning for udøvelsen af retten til effektive retsmidler i Chartrets artikel 47. 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. Ud over 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 efterforsknings metoder 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.

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

Justitia mener, at vedtagelse af lovforslaget vil indebære en ikke uvæsentlig risiko for, at Danmark vil blive dømt ved en eventuel sag for EU-Domstolen. Justitia finder det ligeledes bemærkelsesværdigt, at Justitsministeriet agter at vedtage regler under en erkendt "væsentlig procesrisiko" og med samtidig henvisning til, at reglerne vil kunne anvendes i hele perioden frem til en eventuel dom ved EU-Domstolen.

Justitia anfører, at der i lovudkastet lægges op til, at reglerne om adgang til loggede oplysninger indrettes sådan, at der kan gives adgang til oplysninger til brug for et formål, der er mindre tungtvejende end det, oplysningerne oprindeligt blev logget til. Justitia er ikke enig i Justitsministeriets tolkning af dommen på dette punkt. Ifølge Justitia vil den foreslåede løsning ikke blot udgøre en væsentlig procesrisiko, men være i direkte strid med EU-Domstolens praksis.

RfDS bemærker, at det er problematisk, at Justitsministeriet fremlægger et forslag, hvor de selv medgiver, at der er en væsentlig procesrisiko ved forslaget. Derfor bør det afklares nærmere, om og i givet fald under hvilke omstændigheder logning, der er opsamlet til beskyttelse af nationens sikkerhed, kan anvendes til opklaring af grov kriminalitet.

TI efterlyser klare og enkle regler om udlevering af trafik- og lokaliseringsdata til politiet og foreslår, at Strafferetsplejeudvalget generelt inddrages i overvejelserne om revision af reglerne om politiets adgang til data.

TI opfordrer til, at der i retsplejelovens kapitel 71 fastsættes regler, der definerer følgende nye tvangsindgreb og fastsætter de nærmere betingelser for politiets adgang til at benytte indgrebet – uanset om de pågældende typer af teledata er omfattet af logningsreglerne eller ej.

Desuden finder TI det besynderligt, at der i lovudkastets forslag til ny § 781 a i retsplejeloven lægges op til, at der skal gælde et anderledes og lempeligere kriminalitetskrav for adgang til teleoplysning og udvidet teleoplysning, hvis der er tale om loggede trafikdata, end hvis der ikke er tale om loggede trafikdata. En sådan sondring vil gøre reglerne om udlevering af trafikdata mere komplekse end i dag.

TI finder det positivt, at der med lovudkastets forslag til ny § 804 a i retsplejeloven fastsættes rammer for udlevering af 'masteoplysning' og 'udvidet masteoplysning', dvs. udlevering af lokaliseringsdata, som teleudbyderne registrerer til brug for fejlretning. TI finder det dog ærgerligt, at der lægges op til, at den foreslåede nye § 804 a kun gælder for udlevering af lokaliseringsdata, der er logget eller hastesikret efter de foreslåede nye regler i §§ 786 a-786 e i retsplejeloven. Det er TI's opfattelse, at der bør defineres tvangsindgreb for enhver form for udlevering af trafik- og lokaliseringsdata til politiet – uanset om de pågældende typer af trafik- og lokaliseringsdata er omfattet af logningsreglerne eller ej.

Det er således TI's opfattelse, at trafik- og lokaliseringsdata ikke bør kunne udleveres til politiet alene efter de almindelige regler om edition i retsplejelovens § 804. Særligt for så vidt angår lokaliseringsdata bemærker TI, at lokaliseringsdata kan belyse en persons geografiske færden og derfor efter TI's opfattelse er fortrolige data omfattet af principperne om privatlivsbeskyttelse. Dette gælder enhver form for lokaliseringsdata, uanset om der er tale om lokaliseringsdata omfattet af logningsreglerne eller ej. Persondataretligt giver det ikke mening, at samme data skal have to forskellige beskyttelser, blot fordi EU-Domstolen kun har udtalt sig om, at loggede data kun må bruge til bekæmpelse af grov kriminalitet. Historiske lokaliseringsdata bør derfor efter TI's opfattelse nyde beskyttelse på mindst samme niveau som lokaliseringsdata, der opsamles til brug for teleobservation.

Det er i øvrigt TI's opfattelse, at La Quadrature du Net-dommens præmis 152-156 ikke vedrører sessionslogning. TI finder det overraskende, at lovudkastet lægger op til, at loggede kilde-IP-adresser ikke skal være omfattet af den nye udleveringsregel i ny § 804 a (med særlige kriminalitetskrav), men ifølge lovudkastet skal kunne udleveres efter de almindelige regler om edition i retsplejelovens § 804 (dvs. uden særlige kriminalitetskrav). Særligt i forbindelse med lovovertrædelser, som ikke er grov kriminalitet, finder TI, at det bør afklares, om det er proportionalt, at politiet får adgang til lagrede oplysninger om kunder bag en IP-adresse. TI finder det desuden generelt uafklaret – også i forhold til sager om grov kriminalitet – om det er proportionalt, at der i sager om udlevering af brugeridentiteten bag en mobil dynamisk IP-adresse, hvor det ikke er muligt for politiet at fremskaffe både IP-adresse og portnummer, sker udlevering af oplysninger om tusindvis af brugeridentiteter på ikke-mistænkte og helt tilfældige kunder. Set i dette lys opfordrer TI til, at Justitsministeriet genovervejer fortolkningen af La Quadrature du Net-dommens præmis 152-159 med henblik på at afklare, om den foreslåede nye § 804 a, som sætter rammerne for udlevering af loggede data, også bør omfatte kilde-IP-adresser logget efter den foreslåede nye § 786 f i retsplejeloven.

TI anmoder herudover om, at teksten på side 47 i høringsversionen om kategorisering af IMEI-nummer suppleres med en beskrivelse af de konkrete tilfælde, hvor IMSI- og IMEI-numre kan udleveres til politiet uden kendelse efter den foreslåede § 804 b, stk. 1, i retsplejeloven nemlig de situationer, hvor oplysning om IMSI- og IMEI-nummer findes registreret som kundedata i tjenesteudbydernes kundeordresystemer (kundedatabaser og salgssystemer).

TI beder desuden om, at teksten på side 47 præciseres, så det tydeliggøres, at udlevering af trafikdata, herunder oplysning om IMEI- og IMSI-nummer, der genereres ifm. trafik, altid sker efter kendelse, uanset om der er tale om loggede trafikdata eller trafikdata, som ikke er omfattet af krav om logning. Med udgangspunkt i Ministerio Fiscal-dommen er det TI's umiddelbare opfattelse, at udlevering af "IMEI-oplysning" kan udleveres efter den almindelige regel om edition i retsplejelovens § 804, uanset at der er tale om loggede trafikdata. Hvis denne opfattelse lægges til grund, vil det kunne præciseres i lovforslagsbemærkninger til de foreslåede nye §§ 804 a og 804 b i retsplejeloven, at disse regler ikke finder anvendelse for "IMEI-oplysning".

Herudover bemærker TI, at det efter TI's opfattelse ikke er muligt at forstå indholdet af den foreslåede § 804 b i retsplejeloven. Hvis det er hensigten at give politiet adgang uden kendelse til oplysning om sammenhængen mellem IMEI og telefonnummer, som er baseret på trafikdata opsamlet i mobilnettene (såkaldt 'IMEI-oplysning'), opfordrer TI til, at dette præciseres i både lovtekst og bemærkninger.

TI anmoder om, at det anføres direkte i lovteksten i den foreslåede § 804 b i retsplejeloven, at bestemmelsen ikke omhandler trafikdata. Den gældende § 13 i teleloven, som den foreslåede § 804 b skal afløse, omhandler heller ikke trafikdata, men teleudbyderne har ofte oplevet, at politiet anmoder om udlevering af trafikdata med henvisning til telelovens § 13, hvilket teleudbyderne bruger mange ressourcer på at måtte afvise.

TI anmoder desuden om, at det – i lighed med bemærkningerne til telelovens § 13 – præciseres i lovforslagsbemærkningerne til den foreslåede nye § 804 b i retsplejeloven, at bestemmelsen alene omhandler statiske oplysninger om adresser eller numre, som udbyderen har tildelt slutbrugeren. Bestemmelsen i telelovens § 13 omhandler således alene oplysning om adresser og numre, som findes registreret som kundedata i tjenesteudbydernes kundeordresystemer (kundedatabaser og salgssystemer). TI opfordrer til, at bemærkningerne til den gældende telelovens § 13 blot gentages som bemærkninger til den foreslåede § 804 b i retsplejeloven for derved at tydeliggøre, at der ikke lægges op til ændring af gældende ret (bortset fra ændringen om, at bestemmelsen fremover kun kan bruges af politiet i sager, der er undergivet offentlig påtale).

Justitsministeriet henviser til pkt. 3.7.2 i lovforslagets almindelige bemærkninger, hvoraf det bl.a. fremgår, at det efter Justitsministeriets opfattelse må lægges til grund, at der efter EU-Domstolens opfattelse i princippet kun må gives adgang til registrerings- og opbevaringspligtig trafikdata med henblik på at efterforske og retsforfølge en strafbar overtrædelse, hvis den strafbare overtrædelse vedrører det hensyn, der er baggrunden for, at teleudbyderne m.v. er pålagt at registrere og opbevare de pågældende data, idet der dog kan gives adgang til registrerede og opbevarede trafikdata med henblik på at beskytte den nationale sikkerhed, selv om registrerings- og opbevaringsforpligtelsen er pålagt med henblik på at bekæmpe grov kriminalitet.

Som det fremgår af La Quadrature du Net-dommens præmis 166, finder EU-Domstolen, at hensynet til at efterforske og retsforfølge almindelig kriminalitet ikke kan begrunde, at politiet og anklagemyndigheden kan få adgang til registrerings- og opbevaringspligtige trafikdata. EU-Domstolen tager derimod ikke eksplicit stilling til, om hensynet til at efterforske og retsforfølge grov kriminalitet kan begrunde, at politiet og anklagemyndigheden kan få adgang til trafikdata, der er lagret med henblik på at beskytte den nationale sikkerhed.

Domstolen henviser dog i præmis 166 til dommens præmis 131, som lyder:

> *»131. Det fremgår nærmere bestemt af Domstolens praksis, at medlemsstaternes mulighed for at begrunde en begrænsning af de rettigheder og forpligtelser, der navnlig er fastsat i artikel 5, 6 og 9 i direktiv 2002/58, skal vurderes ved at bedømme alvoren af det indgreb, som en sådan begrænsning indebærer, og ved at kontrollere, at betydningen af det mål af almen interesse, der forfølges med denne begrænsning, står i forhold til denne alvor (jf. i denne retning dom af 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, præmis 55 og den deri nævnte retspraksis).«*

Når EU-Domstolen henviser til præmis 55 i Ministerio Fiscal-dommen og det her opstillede proportionalitetskrav, må dette efter Justitsministeriets opfattelse fortolkes således, at Domstolen herved – fortsat – har den opfattelse, at det indgreb i de grundlæggende rettigheder, som teleudbyderes pligt til at registrere og opbevare trafikdata og offentlige myndigheders adgang hertil udgør, kan begrundes i hensynet til forebyggelse, efterforskning og retsforfølgning af straffelovsovertrædelser, der har til formål at bekæmpe kriminalitet, der på samme måde kan kvalificeres som »grov«, jf. Ministerio Fiscal-dommens præmis 56.

Justitsministeriet vurderer således – under en væsentlig procesrisiko, som kan aktualiseres ved de nye reglers ikrafttræden, i lyset af præmis 166 i La Quadrature du Net-dommen – at dommen ikke er til hinder for, at medlemsstaterne kan give politiet og anklagemyndigheden adgang til trafikdata, der er registreret og opbevaret med henblik på at beskytte den nationale sikkerhed, til brug for politiets og anklagemyndighedens bekæmpelse af grov kriminalitet. I tilknytning hertil skal det dog bemærkes, at det må antages, at den grove kriminalitet skal være af en sådan alvorlig karakter, at det vil være i overensstemmelse med det EU-retlige proportionalitetskrav at give politiet og anklagemyndigheden adgang til sådanne registrerede og opbevarede trafikdata.

EU-Domstolens dom af 2. marts 2021 i H.K.-sagen, som omtales nærmere i pkt. 2.3 i lovforslagets almindelige bemærkninger, har ikke endeligt afgjort spørgsmålet om adgang til trafikdata, der er registreret og opbevaret med henblik på at beskytte den nationale sikkerhed, til brug for politiets og anklagemyndighedens bekæmpelse af grov kriminalitet. På den ene side indeholder dommens præmis 31 en gengivelse af dele af den førnævnte præmis 166 i La Quadrature du Net-dommen, idet der udtales følgende:

> *»31. Hvad angår de formål, der kan begrunde de offentlige myndigheders adgang til de data, som udbydere af elektroniske kommunikationstjenester lagrer som følge af en foranstaltning, der er i overensstemmelse med disse bestemmelser, fremgår det af Domstolens praksis, at en sådan adgang kun kan begrundes i det mål af almen interesse, med henblik på hvilket disse tjenesteudbydere er blevet pålagt at foretage denne lagring (jf. i denne retning dom af 6.10.2020, La Quadrature du Net m.fl., C-511/18, C-512/18 og C-520/18,EU:C:2020:791, præmis 166).«*

På den anden side konstaterer EU-Domstolen følgende i præmis 33 i H.K.-sagen:

> *»33. Hvad angår det formål om forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager, der forfølges med den i hovedsagen omhandlede lovgivning, er det i overensstemmelse med proportionalitetsprincippet kun bekæmpelsen af grov kriminalitet og forebyggelsen af alvorlige trusler mod den offentlige sikkerhed, der kan begrunde alvorlige indgreb i de grundlæggende rettigheder, der er sikret ved chartrets artikel 7 og 8, såsom de indgreb, som lagring af trafikdata og lokaliseringsdata indebærer, uanset om der er tale om generel og udifferentieret lagring eller målrettet lagring. Det er således kun de indgreb i de nævnte grundlæggende rettigheder, der ikke er alvorlige, som kan begrundes i det formål, der forfølges med den i hovedsagen omhandlede lovgivning, om at foretage forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager i almindelighed (jf. i denne retning dom af 6.10.2020, La Quadrature du Net m.fl., C-511/18, C-512/18 og C-520/18, EU:C:2020:791, præmis 140 og146).«*

Herudover skal Justitsministeriet bemærke, at EU-Domstolen ikke forholder sig generelt til, hvad der kan kvalificeres som henholdsvis »almindelig kriminalitet«, »grov kriminalitet« og »beskyttelsen af den nationale sikkerhed«. Det fremgår imidlertid af præmis 166 i La Quadrature du Net-dom-

men, at adgangen til registrerede registrerings- og opbevarede opbevaringspligtige data »i princippet kun kan begrundes i det mål af almen interesse med henblik på hvilket disse udbydere er blevet pålagt at foretage denne lagring«. Justitsministeriet forstår dette således, at der skal foretages en vurdering af kriminalitetens grovhed i forhold til, hvad der har begrundet registreringen og opbevaringen af oplysningerne.

Desuden bemærkes det, at den franske Conseil d'État, som er den øverste administrative domstol i Frankrig, i opfølgning af EU-Domstolens dom i La Quadrature du Net-sagen, som Conseil d'État havde forelagt præjudicielt for EU-Domstolen, i sin afgørelse af 21. april 2021 har fastslået, at den eksisterende trussel mod den nationale sikkerhed i Frankrig kan begrunde en pligt for teleudbyderne til generel og udfifferentieret at registrere og opbevare trafik- og lokaliseringsdata på nuværende tidspunkt, og at de franske efterforskningsmyndigheder kan få adgang hertil med henblik på bekæmpelse af alvorlig kriminalitet.

Conseil d'État er således nået til samme konklusion vedrørende spørgsmålet om adgang til trafikdata, der er registreret og opbevaret som følge af en pligt hertil med henblik på at beskytte den nationale sikkerhed, til brug for politiets og anklagemyndighedens bekæmpelse af grov kriminalitet, som er udgangspunktet for lovforslaget på dette punkt.

Justitsministeriet bemærker desuden, at det i medfør af artikel 15, stk. 1, i direktiv 2002/58, er muligt for medlemsstaterne, under iagttagelse af de i direktivet fastsatte betingelser, at vedtage »retsforskrifter med henblik på at indskrænke rækkevidden af de rettigheder og forpligtelser, der omhandles i [direktivets] artikel 5, artikel 6, artikel 8, stk. 1, 2, 3 og 4, og artikel 9«. Dette omfatter bl.a. retsforskrifter, der pålægger udbyderne af elektroniske kommunikationstjenester at lagre trafik- og lokaliseringsdata.

Som det fremgår af pkt. 2 i lovforslagets almindelige bemærkninger, har EU-Domstolen afsagt flere domme, der angår fortolkningen af e-databeskyttelsesdirektivets (direktiv 2002/58) artikel 15, stk. 1, sammenholdt med artikel 7 (om respekt for privatlivet), artikel 8 (om beskyttelse af personoplysninger) og artikel 11 (om ytrings- og informationsfrihed) i EU's Charter om Grundlæggende Rettigheder (Chartret). Det gælder bl.a. La Quadrature du Net-dommen.

Det er Justitsministeriets opfattelse, at bl.a. La Quadrature du Net-dommen udover for så vidt angår hastesikring (dommens præmis 160 ff.) – alene regulerer data, der gøres registrerings- og opbevaringspligtige i medfør af regler, der udformes i henhold til artikel 15, stk. 1, i direktiv nr. 2002/58. Der er med de foreslåede regler i §§ 786 a-786 f tale om sådanne regler. For oplysninger registreret og opbevaret i medfør af de foreslåede §§ 786 a-786 e eller efter pålæg eller regler udstedt i medfør heraf lægges der derfor også i lovforslaget op til, at der skal gælde et kriminalitetskrav i forbindelse med udlevering heraf. Det vil således alene være muligt at få adgang til oplysninger registreret og opbevaret i medfør af disse bestemmelser m.v., hvis det sker med henblik på bekæmpelse af grov kriminalitet.

For så vidt angår den foreslåede § 786 f i retsplejeloven bemærkes det, at det er Justitsministeriets opfattelse, at oplysninger om, hvilken slutbruger der på et givet tidspunkt har benyttet en given IP-adresse, eventuelt med et såkaldt portnummer og andre identificerende oplysninger, som udbyderen har tildelt slutbrugeren ved adgang til internettet, som efter forslaget skal registreres og opbevares efter den foreslåede § 786 f i retsplejeloven, ikke kan tilvejebringe oplysninger om selve kommunikationen mellem personer eller personers internetaktivitet og dermed heller ikke om disse personers privatliv. Det vurderes derfor, at det inden for rammerne af EU-retten er muligt at foretage generel og udifferentieret registrering og opbevaring af sådanne oplysninger med henblik på bekæmpelse af al kriminalitet. Da oplysningerne således efter Justitsministeriets opfattelse kan registreres og opbevares med henblik på bekæmpelse af al kriminalitet, vil myndighederne også efter Justitsministeriets opfattelse kunne få adgang til disse data med henblik på at bekæmpe al kriminalitet, jf. La Quadrature du Net-dommens præmis 166. For nærmere om registrering og opbevaring af en slutbrugerens adgang til internettet henvises til pkt. 5 i den kommenterede høringsoversigt.

Efter Justitsministeriets opfattelse gælder det desuden, at oplysninger, der ikke gøres registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven eller pålæg eller regler udstedt i medfør heraf, vil kunne udleveres efter de almindelige editionsregler, jf. retsplejelovens § 804, dvs. uden et krav om, at oplysningerne udleveres med henblik på efterforskning eller retsforfølgning af grov kriminalitet.

Endelig bemærker Justitsministeriet, at lovforslaget er koncentreret omkring en revision af de gældende regler for registrering og opbevaring af

teletrafik m.v. Der er derfor ikke med dette lovforslag lagt op til at foretage ændringer specifikt i relation til forsikrings- og pensionsselskabers mulighed for at foretage særlige undersøgelser i forbindelse med f.eks. forsikringssvindel.

Angående det i høringssvaret fra IT-Politisk Forening anførte om proportionalitetsprincippet skal Justitsministeriet bemærke, at der allerede efter gældende ret er mulighed for at foretage en afvejning i forhold til den, der har krav på beskyttelse af sine personoplysninger, jf. navnlig retsplejelovens § 804, stk. 4, og henvisningen til reglerne om vidnefritagelse- og vidneudelukkelse, jf. lovens §§ 169-172, herunder henvisningen til § 170, stk. 3. Retten kan således bestemme, at edition ikke skal pålægges om forhold, med hensyn til hvilke den, som pålægget retter sig mod, i medfør af lovgivningen har tavshedspligt, og hvis hemmeligholdelse har væsentlig betydning. Dette omfatter den tavshedspligt, som gælder efter lov om elektroniske kommunikationsnet og -tjenester. For nærmere herom kan henvises til pkt. 3.7.4.4.3 i lovforslagets almindelige bemærkninger. Endelig skal det bemærkes, at der med lovforslaget foreslås indført mulighed for advokatbeskikkelse for den, som oplysninger, der begæres udleveret efter den foreslåede § 804 a, angår, jf. lovforslagets § 1, nr. 12 (det foreslåede nye stk. 10 i § 806). Advokaten vil i forbindelse med begæringen kunne gøre gældende, at udlevering af oplysninger skal nægtes med henvisning til § 804, stk. 4, jf. § 170, stk. 3.

Justitsministeriets skal vedrørende det af IT-Politisk Forening anførte om, at der som udgangspunkt kun bør kunne udleveres oplysninger om mistænkte personer, bemærke, at der med lovforslaget kun ændres på kriminalitetskravet for udlevering af oplysninger, der er registrerings- og opbevaringspligtige efter §§ 786 a-786 e i retsplejeloven eller efter pålæg eller regler udstedt i medfør heraf. Betingelserne for i øvrigt at meddele pålæg om edition eller for at foretage indgreb i meddelelseshemmeligheden i form af teleoplysning og udvidet teleoplysning ændres ikke. Dette indebærer for så vidt angår indgreb i meddelelseshemmeligheden bl.a., at indgrebet skal være af afgørende betydning for efterforskningen (§ 781, stk. 1, nr. 2), og for så vidt angår edition bl.a. at de oplysninger, der pålægges udleveret, kan tjene som bevis (§ 804, stk. 1, 1. pkt.). Det centrale efter disse bestemmelser vil fortsat være oplysningernes betydning for efterforskningen af en lovovertrædelse, ikke om oplysningerne indeholder oplysninger om en mistænkt. Eksempelvis kan det tænkes, at oplysningerne skal bruges til at finde

ud af, hvem der har opholdt sig på et gerningssted på et konkret tidspunkt, uden at man på dette stadie af efterforskningen har en konkret mistænkt.

Angående det af IT-Politisk Forening og TI anførte om at samle reglerne i kapitlet om indgreb i meddelelseshemmeligheden, skal Justitsministeriet bemærke, at retsplejelovens regler sondrer mellem, om der sker indgreb i en forsendelse m.v. eller ej, jf. herved retsplejelovens § 801, stk. 3, 1. pkt., der undtager udlevering af breve, telegrammer og lignende under forsendelse samt oplysninger om forbindelse mellem telefoner m.v. fra reglerne om edition. Sådanne indgreb skal ske efter reglerne om indgreb i meddelelseshemmeligheden, jf. retsplejelovens kapitel 71. Justitsministeriet har ikke i forbindelse med revisionen af reglerne om registrering og opbevaring af teletrafik m.v. fundet det hensigtsmæssigt at foretage en mere generel ændring af retsplejelovens systematik på dette punkt.

Med lovforslaget vil der for oplysninger, der er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven eller efter pålæg eller regler udstedt i medfør heraf, gælde samme kriminalitetskrav, hvad enten oplysningerne udleveres efter reglerne om edition eller reglerne om indgreb i meddelelseshemmeligheden.

Justitsministeriet skal vedrørende det af IT-Politisk Forening og TI anførte om kravene til udvidet teleoplysning og til at få udleveret historiske masteoplysninger for et bestemt område samt underretning af de berørte bemærke, at i det omfang, der anmodes om oplysninger, der er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven eller efter pålæg eller regler udstedt i medfør heraf, kan sådanne oplysninger udleveres, såfremt der er tale om efterforskning af grov kriminalitet, jf. de foreslåede bestemmelser i hhv. § 781 a og § 804 a. Efter det foreslåede nye stk. 10 i § 806 vil der skulle ske underretning af de berørte efter reglerne i § 788. I det omfang, der ikke er pligt til at registrere og opbevare oplysningerne efter de foreslåede §§ 786 a-786 e i retsplejeloven eller efter pålæg eller regler udstedt i medfør heraf, kan disse forlanges udleveret efter de gældende regler om hhv. teleoplysning og edition. Justitsministeriet forstår EU-Domstolens praksis således, at kravet om efterforskning af grov kriminalitet m.v. kun skal gælde for så vidt angår oplysninger, der registreres og opbevares efter de foreslåede §§ 786 a-786 e eller efter pålæg eller regler udstedt i medfør heraf, jf. også ovenfor. For nærmere herom henvises til pkt. 3.7.2-3.7.4 i lovforslagets almindelige bemærkninger.

Justitsministeriet skal videre bemærke, at det af La Quadrature du Net-dommens præmis 167 fremgår, at det står medlemsstaterne frit for i deres lovgivning at fastsætte, at der under overholdelse af samme materielle og proceduremæssige betingelser kan gives adgang til trafik- og lokaliseringsdata med henblik på bekæmpelsen af grov kriminalitet eller beskyttelsen af den nationale sikkerhed, når de nævnte data af en udbyder lagres på en måde, der er i overensstemmelse med artikel 5, 6 og 9 eller artikel 15, stk. 1, i direktiv 2002/58. Efter Justitsministeriets opfattelse indebærer denne udtalelse også en mulighed for, at der gives adgang til trafikdata vedrørende personer, der kan afsløre en forbindelse, i det mindste indirekte, til grov kriminalitet, bidrage til bekæmpelsen af grov kriminalitet på den ene eller den anden måde eller forhindre en alvorlig fare for den offentlige sikkerhed eller endog en risiko for den nationale sikkerhed, jf. dommens præmis 148.

Endelig skal Justitsministeriet bemærke, at udlevering af oplysninger ved teleoplysning, udvidet teleoplysning eller edition af historiske masteoplysninger ligesom i dag vil være undergivet det almindelige proportionalitetsprincip, der gælder ved foretagelse af straffeprocessuelle tvangsindgreb, jf. hhv. retsplejelovens § 782, stk. 1, og § 805. Udvidet teleoplysning kan desuden kun foretages, når mistanken vedrører en forbrydelse, som har medført, eller som kan medføre fare for menneskers liv eller velfærd eller for betydelige samfundsværdier, jf. retsplejelovens § 781, stk. 5, 1. pkt.

Justitsministeriet skal vedrørende det af TI anførte om, at der for teleoplysning vedrørende oplysninger, der ikke er registrerings- og opbevaringspligtige i medfør af retsplejelovens §§ 786 a-786 e eller efter pålæg eller regler udstedt i medfør heraf, vil gælde et strengere kriminalitetskrav end for oplysninger, der er registrerings- og opbevaringspligtige i medfør af disse bestemmelser m.v., bemærke, at dette skyldes, at Justitsministeriet i det væsentlige har begrænset revisionen af reglerne om registrering og opbevaring af teletrafik m.v. til at angå de ændringer, der følger af EU-Domstolens praksis, herunder at fastsætte et særligt kriminalitetskrav for, at politiet kan få adgang til oplysninger, der er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven eller efter pålæg eller regler udstedt i medfør heraf. Justitsministeriet læser EU-Domstolens praksis sådan, at der stilles krav om efterforskning af grov kriminalitet, for så vidt politiet skal have adgang til oplysninger, der er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e eller efter pålæg eller regler udstedt i medfør heraf. For nærmere herom henvises til pkt. 3.7.2-3.7.4 i

lovforslagets almindelige bemærkninger. Det er ikke formålet med lovforslaget at ændre på reglerne om teleoplysning og edition i almindelighed.

Vedrørende det af TI anførte om at inddrage Strafferetsplejeudvalget skal Justitsministeriet bemærke, at der i øjeblikket arbejdes på at nedsætte Strafferetsplejeudvalget med henblik på at modernisere og fremtidssikre retsplejelovens regler om tvangsindgreb, så politiet har et effektivt retligt grundlag til at foretage f.eks. ransagning af nye kommunikationsformer, jf. herved udspillet Tryghed og sikkerhed i det offentlige rum – 16 initiativer for tryghed og sikkerhed af 10. oktober 2019, s. 8. I hvilket omfang udvalgets arbejde vil medføre forslag til ændringer af den foreslåede revision af reglerne om registrering og opbevaring af trafikdata m.v., kan Justitsministeriet ikke udtale sig om på nuværende tidspunkt.

Angående det i høringssvaret fra IDA og TI anførte om, at § 804 b i høringsversionen af lovforslaget er en udvidelse af telelovens § 13, da det fremgår mere eller mindre direkte af bemærkningerne til § 804 b, at bestemmelsen omfatter udlevering af trafikdata, skal Justitsministeriet bemærke, at § 804 b ikke tilsigter en udvidelse af telelovens § 13. Det er ikke formålet med § 804 b, at den skal omfatte trafikdata, herunder trafikdata i form af IMEI- og IMSI-numre, der generes i forbindelse med trafik. Justitsministeriet bemærker, at lovforslaget siden høringsversionen er ændret, så det klart fremgår af bemærkningerne, at den foreslåede § 804 b ikke omfatter udlevering af trafikdata, herunder trafikdata i form af IMEI- og IMSI-numre, der alene er indhentet som trafikdata opsamlet i mobilnettet.

13. Frafiltrering af registrerings- og opbevaringspligtige data

TI anmoder om, at det præciseres i lovforslaget, at teleudbydernes logningspligt og pligt til hastesikring af trafik- og lokaliseringsdata først indtræder på det tidspunkt, hvor teleudbyderen normalt ville slette lokaliseringsdata.

TI anmoder i forlængelse heraf om, at Justitsministeriet sletter afsnittet om en frafiltreringsmekanisme. Afsnittet knytter sig til, at Justitsministeriet i lovudkastet lægger op til en logningsmodel, hvor (1) teleudbyderne kun skal logge en meget begrænset del af den samlede mængde lokaliseringsdata, der registreres i teleudbydernes net til brug for fejlretningsanalyse, samtidig med, at der (2) ikke stilles forslag om at ændre politiets adgang til lokaliseringsdata fra fejlretningssystemerne efter de almindelige regler om edition (dvs. ingen særlige kriminalitetskrav), hvis blot politiet hverken anmoder

om hastesikring eller logning af disse lokaliseringsdata. TI vurderer, at gennemførelsen af forslaget om frafiltrering vil kræve et meget kompliceret teknisk set-up.

Det er TI's vurdering, at den foreslåede frafiltreringsmekanisme vil kunne give anledning til omfattende it-problemer, herunder risiko for nedbrud i søgesystemer, samt risiko for forsinkelser og fejl-meddelelser ved søgning. Større kompleksitet øger desuden risikoen for fejl både i implementeringen af systemet, men også i den operationelle drift af systemet – og sådanne fejl kan medføre, at der logges for meget eller for lidt.

Telebranchen anfører i øvrigt, at branchen ikke anser sig for forpligtet til at indrette systemer, der understøtter særlige frafiltreringsmekanismer ved udlevering af data fra teleudbydernes fejlretningssystemer, som ikke er omfattet af reglerne om logning og hastesikring, og som ikke er omfattet af veldefinerede indgreb i retsplejeloven, herunder ikke omfattet af reglerne om indgreb i meddelelseshemmeligheden, og som politiet blot anmoder om at få udlevereret efter de almindelige regler om edition.

I forhold til spørgsmålet om udlevering af lokaliseringsdata fra teleudbydernes fejlretningssystemer opfordrer TI i øvrigt til, at Justitsministeriet nærmere afklarer, hvorvidt det er i overensstemmelse med EU-Charterets krav om beskyttelse af privatlivets fred m.v., at disse fortrolige lokaliseringsdata om telekundernes færden kan udleveres til politiet alene efter reglerne om edition (dvs. uden særlige kriminalitetskrav) henset til EU-Domstolens betragtninger om privatlivsbeskyttelse m.v. i de mange domme om adgang til trafik- og lokaliseringsdata omfattet af logningspligt.

Justitsministeriet bemærker, at det af pkt. 3.1.3.4 i lovforslagets almindelige bemærkninger fremgår, at det med den foreslåede model vil påhvile udbyderne at kunne adskille oplysninger, der er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven eller efter pålæg eller regler udstedt i medfør heraf, fra oplysninger, der ikke er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven eller efter pålæg eller regler udstedt i medfør heraf. Det bemærkes desuden, at muligheden for at adskille oplysninger, der er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven eller efter pålæg eller regler udstedt i medfør heraf, fra oplysninger, der ikke er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i rets-

plejeloven eller efter pålæg eller regler udstedt i medfør heraf, efter det oplyste vil kræve et kompliceret teknisk set-up hos udbyderne. I perioden frem til et sådant set-up er på plads vil adskillelse af oplysninger alene kunne ske manuelt og på baggrund af eksisterende systemer. På den baggrund må det forventes, at der i væsentligt færre tilfælde vil blive indhentet oplysninger efter retsplejelovens § 804 i denne periode. Myndighederne vil gå i dialog med udbyderne om, hvordan der i videst muligt omfang kan ske adskillelse samt udlevering efter retsplejelovens § 804 i denne periode, og hvordan udleveringen kan ske mest hensigtsmæssigt.

Kravet om, at udbyderne skal kunne adskille oplysninger, der er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven eller efter pålæg eller regler udstedt i medfør heraf, fra oplysninger, der ikke er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven eller efter pålæg eller regler udstedt i medfør heraf, skal ses i lyset af, at udbyderne for en begrænset periode råder over visse lokaliseringsdata, der ikke i dag er og heller ikke efter lovforslaget gøres registrerings- og opbevaringspligtige, i egne systemer til brug for fejlretning m.v. Det gælder dels lokaliseringsdata i forbindelse med internetforbrug, dels lokaliseringsdata fra tændte telefoner, der ikke anvendes aktivt. Politiet vil i dag kunne hastesikre og få adgang til disse data efter retsplejelovens regler herom. Fordi der med lovforslaget lægges op til, at denne type data fremover heller ikke skal være registrerings- og opbevaringspligtige, vil politiet fortsat kunne få adgang til sådanne data efter de gældende regler om edition i det omfang, udbyderne er i besiddelse heraf. Det samme gælder trafikdata, der ikke gøres registrerings- og opbevaringspligtig efter den foreslåede ordning med målrettet registrering og opbevaring. Dvs. trafikdata, der ikke vedrører kommunikationsapparater, personer eller områder omfattet af ordningen med målrettet registrering og opbevaring af trafikdata. Det bemærkes i den forbindelse, at udbyderne har oplyst, at de som udgangspunkt sletter oplysninger, der ikke er registrerings- og opbevaringspligtige, efter ca. 14 dage.

Lovforslaget indebærer, at der efter de gældende regler om edition kan opnås adgang til oplysninger, der ikke er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven eller efter pålæg eller regler udstedt i medfør heraf, mens oplysninger, der er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven eller efter pålæg eller regler udstedt i medfør heraf, vil skulle tilgås efter de foreslåede regler i §§ 781 a og 804 a i retsplejeloven, hvorefter der kun vil

kunne opnås adgang til oplysningerne, hvis anmodningen sker med henblik på at bekæmpe grov kriminalitet.

Det er derfor afgørende, at udbyderne ved politiets anmodning om udlevering af oplysninger har mulighed for at adskille oplysninger, der ikke er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven eller efter pålæg eller regler udstedt i medfør heraf, for hvilke der ikke vil gælde et kriminalitetskrav, fra oplysninger, der er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven eller efter pålæg eller regler udstedt i medfør heraf, for hvilke der vil gælde et kriminalitetskrav.

Forudsættes det ikke i lovforslaget, at udbyderne skal kunne adskille de nævnte oplysninger fra hinanden, er det Justitsministeriets opfattelse, at der vil værre større risiko for, at der sker fejl i forbindelse med udlevering af oplysninger, og at der dermed f.eks. vil kunne opstå situationer, hvor der udleveres oplysninger, der er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven eller efter pålæg eller regler udstedt i medfør heraf, uden at kriminalitetskravet er opfyldt. Forudsætningen om, at udbyderne skal kunne adskille oplysningerne, er således indføjet med henblik på at begrænse risikoen for fejl.

Justitsministeriet bemærker desuden, at der i lovforslaget lægges op til, at registrerings- og opbevaringsforpligtelsen efter den foreslåede § 786 f i retsplejeloven (generel og udifferentieret registrering og opbevaring af oplysninger om en slutbrugers adgang til internettet) fastsættes direkte i bestemmelsen.

Der lægges desuden op til, at registrerings- og opbevaringsforpligtelsen efter den foreslåede § 786 e i retsplejeloven (generel og udifferentieret registrering og opbevaring af trafikdata) vil indtræde ved ikrafttræden af de regler, justitsministeren efter forhandling med erhvervsministeren fastsætter med hjemmel i den foreslåede bestemmelse.

Lovforslaget er endvidere tilpasset siden høringsversionen, så det nu klart fremgår, at udbydernes forpligtelse til at foretage målrettet registrering og opbevaring på baggrund af de foreslåede §§ 786 b-786 d i retsplejeloven indtræder, når udbyderne modtager pålæg herom fra Rigspolitiet. Der henvises til det under pkt. 10 anførte i den kommenterede høringsoversigt.

Efter Justitsministeriets opfattelse er det mest hensigtsmæssigt, hvis det klart fremgår af de foreslåede bestemmelser og regler udstedt i medfør heraf, hvornår forpligtelsen til registrering og opbevaring indtræder. En løsning, hvorefter man i lovforslaget præciserer, at udbydernes forpligtelse til registrering og opbevaring først indtræder på det tidspunkt, hvor udbyderne normalt ville slette de oplysninger, der ikke er registrerings- og opbevaringspligtige, vil bl.a. medføre, at registrerings- og opbevaringspligten ikke nødvendigvis vil indtræde på samme tidspunkt for alle udbydere, idet udbyderne efter det oplyste ikke har samme praksis for sletning af oplysninger, der ikke er registrerings- og opbevaringspligtige. Hertil kommer, at der ikke med en sådan løsning vil være sikkerhed for, at de oplysninger, det ønskes at gøre registrerings- og opbevaringspligtige, vil forefindes på det tidspunkt, hvor registrerings- og opbevaringspligten indtræder.

For nærmere om Justitsministeriets overvejelser om adgang til oplysninger, der ikke er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven eller efter pålæg eller regler udstedt i medfør heraf, henvises til pkt. 12 i den kommenterede høringsoversigt.

14. Forholdet til den redaktionelle kildebeskyttelse og tavshedspligt

Danske Medier bemærker, at foreningen flere gange i forbindelse med de gentagne udskydelser af revisionen af logningsreglerne har understreget vigtigheden af, at eventuelle indgreb i meddelelseshemmeligheden ikke må udgøre en risiko for mediernes muligheder for at beskytte deres kilder.

Danske Medier anfører desuden, at den foreslåede revision af logningsreglerne, der fortsat giver en ganske omfattende mulighed for at registrere og opbevare trafikdata, desværre ikke fjerner foreningens grundlæggende bekymring for, at en såvel generel og udifferentieret som en målrettet logning vil kunne kompromittere mediernes ret til at beskytte deres kilder i overensstemmelse med retsplejelovens regler om kildebeskyttelse og vidnefritagelse i retsplejelovens § 172.

Foreningen har noteret, at der i udkastets forslag til § 786 d, stk. 4, i retsplejeloven gives mulighed for en hurtig efterprøvelse fra rettens side, såfremt der er tilfælde, hvor særlige principielle hensyn kan siges at gøre sig gældende, f.eks. hvor der opstår spørgsmål om registrering og opbevaring af trafikdata fra kommunikationsapparater, der anvendes af advokater, læger eller journalister. Foreningen tilslutter sig dette forslag, men mener ikke at

henvisningen til retsplejelovens § 783, stk. 2, 3. og 5.-7. pkt., om underretning af den beskikkede advokat og det forholdsvis vage udtryk "særlige forhold" i sig selv er tilstrækkelig til at sikre, at indgreb i meddelelseshemmeligheden ikke underminerer kildebeskyttelse. Beskikkelsen af en såkaldt "indgrebsadvokat" vil først og fremmest have fokus på den mistænktes interesser, og en eventuel varetagelse af andres interesser, herunder mediets/journalistens særskilte interesse i at beskytte sine kilder, vil alt andet lige være sekundær.

Danske Medier anfører i forlængelse heraf, at dette rummer en klar risiko for, at hensynet til kildebeskyttelsen reelt tildeles en ringere beskyttelse end den, som lovgiver har tilsigtet ved reglernes udformning. En effektiv domstolsprøvelse fordrer derfor som minimum, at hensynet til kildebeskyttelsen særskilt fremhæves i bemærkningerne, som ét af de hensyn, som den beskikkede advokat skal holde sig for øje.

Herudover mener Danske Medier, at det er bekymrende, at lovforslaget ikke tager højde for reglerne om kildebeskyttelse. Dette gælder ikke mindst i relation til de bestemmelser, der regulerer politiets adgang til de loggede oplysninger. Danske Medier skal derfor opfordre til, at der indsættes en udtrykkelig henvisning til retsplejelovens § 172 i retsplejelovens kapitel 71, der skal inddrages ved spørgsmål om udlevering af oplysninger, der er registrerings- og opbevaringspligtige efter udkastets forslag til §§ 786 b-786 e i retsplejeloven. Foreningen skal i den anledning i øvrigt henlede opmærksomheden på, at retsplejelovens kapitel 73 og 74 allerede indeholder henvisninger til retsplejelovens § 172.

DJ bemærker, at den logning, der foregår, ikke bør kunne udgøre en risiko for mediernes muligheder for at kunne beskytte sine kilder, og at logningsreglerne lige så lidt som telefonaflytning eller andre indgreb i meddelelseshemmeligheden bør kunne bringe denne kildebeskyttelse i fare. DJ anfører desuden, at det foreliggende lovudkast ikke indeholder bestemmelser, der kan sikre denne kildebeskyttelse, og at man i bemærkninger til lovforslaget har undladt at gøre sig overvejelser om denne problemstilling.

DJ opfordrer derfor til, at den redaktionelle kildebeskyttelse sikres i forbindelse med revisionen af logningsreglerne. Det kan eksempelvis ske ved, at der indsættes en direkte henvisning til retsplejelovens § 172 om kildebeskyttelse i de relevante paragraffer om logning. Andre steder i retsplejeloven er

der allerede henvisninger til § 172 (bestemmelserne om ransagning, beslaglæggelse og edition), og DJ finder det helt naturligt og meget nødvendigt, at dette hensyn bliver afspejlet.

IT-Politisk Forening anfører, at det i Digital Rights-dommen blev problematiseret, at logningsdirektivet ikke fastsatte nogle begrænsninger for personer undergivet nationale regler om tavshedspligt. Det samme gjorde sig gældende for de nationale logningsregler i Tele2-dommen. I La Quadrature du Net-dommen nævnes det endvidere i præmis 118, at logning kan have en afskrækkende virkning på whistleblowere, hvilket i sagens natur vil være særdeles uheldigt. 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.

Hertil bemærker IT-Politisk Forening, 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.

Justitsministeriet bemærker, at der ikke ved registrering og opbevaring af teletrafik efter gældende ret sondres mellem, hvilke persongrupper kommunikationen foregår, herunder om kommunikationen foregår mellem en journalist og dennes kilde. Efter gældende ret kan det således forekomme, at der registreres og opbevares oplysninger, der vedrører kommunikationen mellem en journalist og dennes kilde. Der lægges ikke med lovforslaget op til at ændre gældende ret på dette område. Adgangen til registrerede og opbevarede oplysninger vedrørende journalisters kommunikation med deres kilder vil dog være undergivet begrænsninger.

Justitsministeriet skal i den forbindelse bemærke, at teleoplysning og udvidet teleoplysning kun giver adgang til oplysninger om, hvilke kommunikationsapparater, der har været sat i forbindelse med hinanden. Der gives ikke adgang til indholdet af kommunikationen.

Justitsministeriet bemærker videre, at der ikke med den foreslåede revision af reglerne om registrering og opbevaring af teletrafik m.v. er lagt op til ændringer af den personkreds, der efter gældende ret er undtaget fra indgreb i meddelelseshemmeligheden. Adgangen til teleoplysning og udvidet teleoplysning er således heller ikke efter gældende ret begrænset af retsplejelovens § 172 om vidnefritagelse for redaktører og redaktionelle medarbejdere ved et skrift, der er omfattet af § 1, nr. 1, i mediansvarsloven om f.eks., hvem der er kilde til en oplysning, jf. retsplejelovens § 786, stk. 2. Der henvises til bemærkningerne til lovforslagets § 1, nr. 2 (den foreslåede § 781 a), hvor det bl.a. fremgår, at bestemmelsen kun medfører et ændret kriminalitetskrav for teleoplysning- og udvidet teleoplysning. De øvrige betingelser for at foretage indgrebet, herunder personkredsen i retsplejelovens § 782, stk. 2, foreslås ikke ændret.

Justitsministeriet bemærker desuden, at de gældende regler om edition begrænses af retsplejelovens § 172, jf. retsplejelovens § 804, stk. 4. Dette vil også være tilfældet for den foreslåede § 804 a vedrørende edition af oplysninger, der er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven eller efter pålæg eller regler udstedt i medfør heraf. Der henvises til bemærkningerne til den foreslåede § 804 a i retsplejeloven, hvor det bl.a. fremgår, at bestemmelsen alene medfører et ændret kriminalitetskrav. De øvrige betingelser for at foretage edition, herunder at pålæg om edition ikke kan meddeles, såfremt der derved vil fremkomme oplysninger om forhold, som den pågældende ville være fritaget fra at afgive forklaring om som vidne, jf. lovens § 172, foreslås ikke ændret.

Endelig skal det vedrørende edition bemærkes, at det med lovforslagets § 1, nr. 12, foreslås at indsætte et nyt stk. 10 i retsplejelovens § 806, der indfører beskikkelse af indgrebsadvokat for den, som et pålæg om edition af registrerings- og opbevaringspligtig oplysninger efter den foreslåede § 804 a angår. Advokaten vil i den forbindelse kunne udtale sig om, hvorvidt begæringen om edition skal afvises, fordi oplysningerne er omfattet af vidnefritagelsesreglen i § 172.

15. Ikrafttræden og implementering

Dansk Erhverv og **IT-Branchen** bemærker, at lovforslagets fortolkning af målrettet logning – og de deraf følgende nye krav om registrering og indberetning af kundedata (bl.a. CPR) – bliver teknisk og sikkerhedsmæssigt yderst vanskelig at efterleve. De tekniske udfordringer betyder samtidig, at

der må regnes med en betydelig risiko for, at der vil opstå alvorlige fejl og uklarheder i forbindelse med logningen og udleveringen af data.

Dansk Erhverv og IT-Branchen anfører desuden, at en forhastet lovproces og urealistisk implementeringsfrist markant øger risikoen for nye alvorlige sager om politiets anvendelse af teledata. Det bemærkes, at det grundlæggende er urealistisk at lade loven træde i kraft den 1. januar 2022. Som minimum bør der indføres en betydeligt længere implementeringsfrist, hvis forslaget alligevel træder i kraft 1. januar 2022.

Danske Advokater anfører, at der er lagt op til at introducere en logningsordning, der tilsyneladende har været på vej i mere end 10 år, jf. de løbende historiske revisioner, som fremlægges som lovforslag i november og påtænkes (haste) behandlet til ikrafttrædelse 1. januar, men som først kan iværksættes i praksis minimum 1 år efter ikrafttrædelsen. Etablering af målrettet logning indebærer væsentlige praktiske udfordringer, behandling af personoplysninger, sikkerhedsmæssige risici og i øvrigt under en ramme, der berører borgernes grundlæggende rettigheder. I det lys virker det påfaldende, at nye regler skal hastes igennem, for kun at blive erstattet af en praktisk overgangsordning af en længere varighed, hvor hverken myndigheder eller udbydere er klar til at overholde reglerne.

DI bemærker, at det fremgår af lovforslagets § 3, stk. 1, at loven træder i kraft 1. januar 2022. Det vurderes at være meget hurtigt for en sådan kompleks lovgivning som denne, som indebærer en betydelig omstilling for en branche. Da denne hurtige ikrafttrædelse samtidig kræver en overgangsordning, skaber det en unødig omstilling, der kan undgås ved en senere ikrafttrædelse. Ydermere anfører Justitsministeriet selv, at der en betydelig procesrisiko ved forslaget. Dvs. vi kan risikere at gå for langt i forhold til EU-retten og dermed igen være nødt til at lave om på reglerne. Denne stop and go-tilgang er uhensigtsmæssig, da erhvervslivet har betydelige omstillingsomkostninger, hver gang reglerne ændres. Det anbefales samlet, at udskyde ikrafttrædelsesfristen for at undgå overgangsordningen samt for at få en afklaring af EU-retten.

DI anfører, at elementerne om geografisk målretning i lovforslaget vil være teknisk vanskelige at gennemføre for nogle kommunikationstjenester under visse omstændigheder, særligt de kommunikationstjenester, der er netværksuafhængige, og hvor kendskab til den geografiske placering derfor afhænger af brugerens enhed og lokationsindstillinger.

IDA bemærker, at det fremgår af lovforslaget, at it-understøttelsen af den del af lovforslaget, der vedrører målrettet personbestemt og geografisk logning, ikke vil være udviklet 1. januar 2022, og at der derfor vil være tale om en (relativt lang) overgangsperiode, hvor en sådan logning vil skulle foregå manuelt. Derudover fremgår det også, at et nyt it-system vil skulle basere sig på ældre, eksisterende it-systemer. Det fremgår af lovforslaget, at der både i forbindelse med det nye it-system og i perioden med manuel håndtering, vil være risiko for fejl, hvor personer, der burde logges, ikke bliver det, og omvendt, at personer, der ikke skal logges, bliver det. IDA kan ikke støtte, at der i en overgangsperiode vil være fejl, som medfører indgreb i retten til privatliv og beskyttelse af personoplysninger. IDA anbefaler derfor, at man udskyder ikrafttræden til et sikkert og gennemteste system er på plads, og at man i den mellemliggende periode stopper alle former for logning.

TI gør opmærksom på, at teleudbyderne har behov for rimelige implementeringsfrister – regnet fra det tidspunkt, hvor de foreslåede nye regler er endeligt vedtaget og endelige krav er udmøntet i bekendtgørelser m.v. TI bemærker i den forbindelse, at it-løsninger til understøttelse af nye regler om målrettet logning vil kunne være klar 15 måneder efter reglernes ikrafttræden. Ændringer i it-systemer og administrative processer til understøttelse af krav om registrering af unikt ID og bruger vil kunne være klar efter 1½-2 år (for de største teleudbydere). Og ændring af 118-databasen med henblik på at kunne modtage indberetning af CPR/CVR/Unikt ID (EU-baseret database) vil kunne være klar 3-5 år efter reglernes ikrafttræden (for forsyningspligtudbyderen). TI bemærker desuden, at en manuel løsning til iværksættelse af målrettet logning også forudsætter implementeringstid hos teleudbyderne. En manuel løsning vil kun være manuel ift. at iværksætte logning og nedtage logning for et givet nummer. De underliggende systemer vil stadig skulle kunne håndtere personbestemt og geografisk logning, hvilket først vil kunne ske efter 15 måneder.

TI anfører desuden for så vidt angår forslaget om registrering og verificering af unikt ID m.v., at forsyningspligtudbyderen (TDC/Nuuday) har oplyst TI om, at de gældende forsyningspligtregler og vilkår for TDC's varetagelse af forsyningspligt på en udtømmende nummerfortegnelse (118-databasen), som indtil videre løber til og med 2022, ikke omfatter krav om, at 118-databasen skal kunne modtage og registrere hverken oplysning om CPR/CVR/ID eller oplysning om bruger. Der ses i øvrigt ikke, at der kan

skabes hjemmel til en ændring af kravene til forsyningspligtudbyderen inden for den nuværende forsyningspligtperiode.

Justitsministeriet bemærker, at lovforslaget siden høringsversionen er justeret, så det nu fremgår af pkt. 3.1.3.4 i lovforslagets almindelige bemærkninger, at den foreslåede ordning med målrettet personbestemt registrering og opbevaring af trafikdata og den foreslåede ordning med målrettet geografisk registrering og opbevaring af trafikdata for så vidt angår det foreslåede § 786 c, stk. 1, nr. 2 i retsplejeloven (områder med en et højere antal beboere dømt for grov kriminalitet), vil kræve udvikling af it-systemunderstøttelse hos bl.a. Rigspolitiet med henblik på en automatiseret proces.

Der vil være behov for at foretage en grundig foranalyse forud for selve systemudviklingen til understøttelse af den foreslåede målrettede registrering og opbevaring, idet der vil være tale om et komplekst it-projekt. It-systemudviklingen vil bl.a. skulle bygge oven på it-systemer fra flere forskellige myndigheder (herunder politiet og kriminalforsorg) og telebranchen. Foranalysen ventes tidligst at foreligge i 2023. Herefter vil Rigspolitiet kunne levere et skøn over, hvornår it-systemunderstøttelsen vil kunne ventes etableret og sat i drift.

Den målrettede registrering og opbevaring af trafikdata vil desuden kræve udvikling af it-systemunderstøttelse hos udbyderne med henblik på en automatiseret proces.

Det forudsættes, at udviklingsarbejdet generelt sker under dialog med telebranchen, således at det sikres, at den kommende it-systemunderstøttelse i Rigspolitiet er kompatibel med den it-systemunderstøttelse, ordningen forudsætter for så vidt angår udbyderne.

Da den nødvendige it-systemunderstøttelse ikke vil kunne være færdigudviklet på tidspunktet for lovens ikrafttrædelse, foreslås det, jf. lovforslagets § 3, stk. 4, at justitsministeren i en overgangsperiode – dvs. i perioden fra lovens ikrafttræden og indtil det tidspunkt, hvor den nødvendige it-systemunderstøttelse er etableret og klar til at blive sat i drift – vil kunne fastætte regler om fravigelse af lovens bestemmelser i de foreslåede §§ 786 b-786 d i retsplejeloven, herunder at reglerne helt eller delvist ikke skal anvendes. Der vil f.eks. kunne fastsættes regler om, hvilke tjenester og datatyper den målrettede registrering og opbevaring i en overgangsperiode skal omfatte.

Der vil også eksempelvis kunne fastsættes regler om, at kun dele af den målrettede registrering og opbevaring i en overgangsperiode skal sættes i kraft. Der lægges i den forbindelse ikke op til at bemyndige justitsministeren til at fastsætte andre betingelser for iværksættelse af den målrettede registrering og opbevaring af trafikdata end dem, som fremgår af de foreslåede §§ 786 b-786 d i retsplejeloven.

Hertil bemærkes, at der lægges op til, at loven skal træde i kraft 1. januar 2022, jf. lovforslagets § 3, stk. 1. Forud for 1. januar 2022 vil der i overensstemmelse med den foreslåede § 786 e i retsplejeloven blive foretaget en vurdering af, hvorvidt der i 2022 vil foreligge en alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig, jf. pkt. 3.2.3.1 i lovforslagets almindelige bemærkninger. På det foreliggende grundlag, herunder oplysninger om aktuelle straffesager omhandlende overtrædelser af bestemmelserne i straffelovens kapitel 12 og 13, herunder både verserende sager og sager, hvori der er sket domfældelse, den gældende »Vurderingen af Terrortruslen mod Danmark« (VTD) fra Center for Terroranalyse og øvrige analyseprodukter, er det Justitsministeriets forventning, at der i 2022 vil foreligge en alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig. Det er således Justitsministeriets forventning, at der i 2022 med hjemmel i den foreslåede § 786 e i retsplejeloven vil kunne fastsættes regler, der pålægger udbyderne at foretage generel og udifferentieret registrering og opbevaring af trafikdata.

De relevante myndigheder vil – under dialog med telebranchen – i umiddelbar forlængelse af lovens ikrafttræden skulle udarbejde bekendtgørelser, der fastsætter de nærmere rammer for målrettet registrering og opbevaring af trafikdata efter de foreslåede §§ 786 b-786 d i retsplejeloven, herunder regler om understøttelse af målrettet registrering og opbevaring af trafikdata i overgangsperioden fra lovens ikrafttræden, indtil den nødvendige it-systemunderstøttelse af målrettet registrering og opbevaring af trafikdata er på plads. Bekendtgørelserne vil skulle udstedes og træde i kraft hurtigst muligt efter lovens ikrafttræden. Med bekendtgørelserne vil der kunne tages højde for den systemunderstøttelse, der er til rådighed på tidspunktet for udstedelse af bekendtgørelsen.

Det bemærkes i den forbindelse, at det i lovforslaget forudsættes, at udbyderne med kort varsel kan understøtte en overgang fra generel og udifferentieret registrering og opbevaring til målrettet registrering og opbevaring i medfør af relevante udstedte bekendtgørelser.

Det bemærkes også, at lovforslaget siden høringsversionen er justeret, så det fremgår af lovforslagets § 3, stk. 2, at justitsministeren fastsætter tidspunktet for ikrafttræden af lovens § 2, stk. 2. Det vil betyde, at udbyderne først på et tidspunkt nærmere fastsat af justitsministeren skal være klar til at understøtte og administrere registrering af unikt ID og eventuelle oplysninger om bruger for slutbrugere. Lovforslagets § 2, nr. 2, relaterer sig bl.a. til den foreslåede ordning med målrettet registrering og opbevaring af trafikdata. Det forudsættes derfor, at lovforslagets § 2, nr. 2, sættes i kraft på det tidspunkt, der passer i forhold til de relevante regler om målrettet registrering og opbevaring af trafikdata i overgangsperioden. Forslaget skal således ses i sammenhæng med lovforslagets § 3, stk. 4, hvor det foreslås, at justitsministeren i en overgangsperiode kan fastsætte regler om fravigelse af de foreslåede §§ 786 b-786 d i retsplejeloven, herunder at reglerne helt eller delvist ikke skal anvendes. Der henvises til de specielle bemærkninger hertil.

I relation til risikoen for fejl bemærker Justitsministeriet, at indhentelse af oplysninger om trafikdata, som hører til kategorien teledata, er et centralt efterforskningsværktøj for politiet i forbindelse med efterforskningen af kriminalitet, ligesom det kan være afgørende for anklagemyndighedens muligheder for strafforfølgning ved domstolene. Det gælder i en række sager om grov kriminalitet, herunder bl.a. i sager om bandekriminalitet, drab, narkotikakriminalitet og terrorisme.

Det er fortsat vigtigt, at der – for så vidt angår teledata og andre tekniske beviser helt generelt – er opmærksomhed på, at de underlægges systematiske kvalitetskontroller, og at der gennem hele straffesagskæden er opmærksomhed på mulige fejlkilder og usikkerheder ved det pågældende bevis.

Som det fremgår af justitsministerens besvarelse af 10. november 2021 af spørgsmål nr. 35 (Alm. del) fra Folketingets Retsudvalg, er der truffet en række foranstaltninger, ligesom en række initiativer stadig er under implementering, med henblik på at sikre, at der hersker tillid til behandlingen af tekniske beviser, herunder teledata. Endvidere bemærkes det, at det fremgår

af Rigsadvokatmeddelelsen, afsnittet om anvendelse af teledata i straffesager, af 25. august 2020, at teledata altid vil indgå som ét blandt flere beviser i en sag, og betydningen af et bevis i form af teledata vil altid bero på en konkret vurdering af dels det enkelte bevis, dels sagens samlede omstændigheder i øvrigt. Det vil i sidste ende være retten, som afgør, hvilken bevismæssig vægt et bevis i form af teledata skal tillægges i den enkelte sag, jf. princippet om den fri bevisbedømmelse.

Justitsministeriet bemærker desuden, at der selvfølgelig i forbindelse med forberedelserne af et nyt udbud af forsyningspligttjenester vil skulle tages højde for de forpligtelser, som den foreslåede ordning for registrering og opbevaring af trafikdata m.v. medfører for forsyningspligtsudbyderen.

16. Administrative omkostninger for erhvervet

Dansk Erhverv og **IT-Branchen** bemærker, at det bliver omkostningsfuldt for teleselskaberne at konstruere de nye systemer. Den foreslåede lov indeholder dog mange elementer, der ikke indgår i vurderingen af virksomhedernes administrative byrder, og omstillingsomkostningerne må forventes at blive væsentligt højere end de anslåede 206 mio. kr.

Grundlaget for at påføre så betydelige omstillingsomkostninger på selskaberne forekommer ifølge Dansk Erhverv og IT-Branchen endvidere spinkelt i lyset af den nævnte procesrisiko. Dansk Erhverv og IT-Branchen er således bekymrede ift., om lovforslaget ligger inden for EU-rettens rammer. Måtte lovforslaget helt eller delvist underkendes som værende uforenelig med EU-retten, vil teleselskabernes udgifter til nye it-systemer og procedurer være spildte.

Dansk Erhverv og IT-Branchen mener, at der som minimum bør foretages en ny byrdevurdering i lyset af det samlede forslag med henblik på en reel omkostningsdækning for selskaberne.

DI bemærker, at der lægges op til omstillingsomkostninger for 206 mio. kr. samt omkostninger til årlig drift på 107 mio. kr. Der er tale om nationale regler og for så vidt en for telebranchen uvedkommende opgave, der ikke naturligt ligger i forlængelse af at drive televirksomhed. Da der hermed er tale om en betydelig byrde for en enkelt branche baseret på nationale regler og et for branchen uvedkommende hensyn, bør det overvejes, om der skal

være en kompensationsmulighed i reglerne. En måde at nedbringe omkostningerne er ved at gøre det nemmere for teleselskaberne at efterkomme kravene i reguleringen. I forhold til et ønske om fælles format kan det oplyses, at det er et omkostningsfuldt krav at stille. Teleselskaberne bruger typisk forskellige systemer og et eventuelt krav om ensretning kan både skabe risiko for data-tab eller -forvanskning ved omformatering men også øgede omkostninger. Teleselskaberne kan alene pålægges at udlevere rådata, eventuelt på en ensrettet måde.

IT-Politisk Forening anfører, at forberedelserne til den målrettede logning 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.

RfDS bemærker, at Justitsministeriet lægger op til, at teleselskaberne skal opbevare (og formodentlig videregive) de data, der omfattes af den kommende lovgivning, i et fælles opbevaringsformat. Desuden ser det ud til, at en række af de systemer, som skal understøtte ovenstående forslag, faktisk ikke findes endnu og derfor skal udvikles særligt til opfyldelse af denne lovgivning. Det er teleselskaberne, som skal forestå omkostningerne ved at etablere de foreslåede foranstaltninger. Disse omkostningerne vil blive overvæltet på borgerne, og at det dermed bliver dyrere at være telekunde. Den økonomiske byrde for teleselskaberne bør derfor reduceres.

TI bemærker, at spørgsmålet om økonomisk godtgørelse for teleudbydernes udgifter forbundet med iværksættelse af personbestemt eller geografisk målrettet logning af trafikdata eller hastesikring af trafik- og lokaliseringsdata, som politiet rekvirerer i medfør af de foreslåede nye §§ 786 a-786 d i retsplejeloven, ikke er omtalt i lovudkastet. TI anmoder om, at spørgsmålet om betaling afspejles i lovforslaget ved indsættelse af regler svarende til reglerne i retsplejelovens § 786, stk. 8 (betaling for teleudbydernes praktiske bistand ved indgreb i meddelelseshemmeligheden) og retsplejelovens § 804, stk. 5 (edition).

TI finder det centralt, at man ifm. de politiske drøftelser af lovforslaget også drøfter spørgsmålet om dækning af omkostninger, der følger med de ændrede logningsforpligtelser. Hvis man politisk vurderer, at det er i national interesse at sikre målrettet logning, så skal der også sikres en reel omkostningsdækning for de selskaber, som bliver pålagt at foretage logningen. TI

bemærker, at de foreslåede nye regler om målrettet logning især vil stille store krav til processorkraft til opsamling, filtrering og udlevering af loggede og hastesikrede data. Sådanne it-systemer vil være rene efterforskningsmæssige værktøjer, som teleselskaberne på ingen måde har egeninteresse i at udvikle. Dertil kommer etableringsomkostninger til systemunderstøttelse af registrering af unikt ID og bruger samt indberetning heraf til 118-databasen m.v., som alene hos de største udbydere udgør et trecifret millionbeløb. Vedtages lovforslaget i dets nuværende form, vil der således reelt være tale om, at staten bestiller en endog meget stor it-udviklingsopgave hos en række private aktører, der på ingen måde har behov for disse it-redskaber. TI anmoder om, at alle omkostninger til udvikling og drift af sådanne it-løsninger dækkes af staten.

Justitsministeriet bemærker, at der er foretaget en aktivitetsbaseret måling af virksomhedernes administrative byrder (AMVAB-måling) af lovforslaget. Lovforslaget forventes at medføre omstillingsomkostninger på 206 mio. kr. og løbende administrative byrder på ca. 107 mio. kr. årligt for telebranchen.

Det bemærkes, at den foretagne AMVAB-måling viste, at lovforslaget i sin daværende form forventeligt ville medføre omstillingsomkostninger på ca. 331 mio. kr., hvoraf 125 mio. kr. kunne henføres til to virksomheders efterregistrering af unikt ID på eksisterende fastnettelefoniabonnenter, herunder IP-telefoniabonnenter.

For ikke at pålægge telebranchen unødigt byrdefuld regulering, lægges der med lovforslaget op til, at der ikke skal stilles krav til efterregistrering af unikt ID på eksisterende fastnettelefoniabonnenter, herunder IP-telefoniabonnenter. Det vil reducere omstillingsomkostningerne fra branchen til de nævnte 206 mio. kr. Det bemærkes i den forbindelse, at et krav om efterregistrering af unikt ID på eksisterende fastnettelefoniabonnenter, herunder IP-telefoniabonnenter, vurderes at ville have begrænset efterforskningsmæssig værdi sat over for den estimerede omstillingsomkostning for branchen. Det bemærkes desuden, at der fortsat lægges op til, at der vil være krav om efterregistrering af unikt ID på øvrige abonnenter.

Omstillingsomkostningerne består herefter navnlig i ca. 63,5 mio. kr. til tilpasning af udbydernes systemer, så de kan indberette unikt ID på abonnenterne til den såkaldte 118-datase, samt 53 mio. kr. til varetagelsen af målrettet registrering og opbevaring af trafikdata.

De løbende administrative byrder vedrører særligt udgifter til målrettet registrering og opbevaring af trafikdata, byrder i forhold til registrering af brugere af taletidskort samt løbende drift og vedligehold af de tilpassede it-systemer. Navnlig registrering og verificering af unikt ID ved salg af taletidskort udgør en stor omkostning med ca. 69 mio. kr. årligt. Derimod vurderes der ikke at være væsentlige løbende administrative byrder ved registrering af unikt ID ved ny-oprettelse af abonnenter på mobil- eller fastnettelefoni.

Det følger af telelovens § 10, at udbydere af kommunikationsnet eller -tjenester til slutbrugere er forpligtede til at indrette det tekniske udstyr og de tekniske systemer, som udbyderen anvender, så politiet kan få adgang til registrerings- og opbevaringspligtige oplysninger. Denne pligt vil også gælde i relation til lovforslaget om revision af reglerne om registrering og opbevaring af teletrafik (logning) m.v.

Herudover bemærker Justitsministeriet, at følgende fremgår af lovskitsen af 23. marts 2021:

> *"Det vil kunne fastsættes nærmere regler om økonomisk godtgørelse for udgifter forbundet med et konkret pålæg om personbestemt eller geografisk målrettet logning. De nærmere regler vil kunne omfatte regler om betingelserne for at yde godtgørelse for udgifter forbundet med et konkret pålæg mv., om standardtakster for godtgørelsen og eventuelt om betingelser for at yde godtgørelse ud over standardtaksterne. I det omfang sådanne regler fastsættes, forudsættes det, at der ikke ydes godtgørelse ud over standardtaksterne, medmindre der ekstraordinært måtte være tale om, at et konkret pålæg mv. medfører uforholdsmæssige udgifter for en udbyder."*

Der lægges ikke med lovforslaget op til at fastsætte nærmere regler om økonomisk godtgørelse for udgifter forbundet med et konkret pålæg om personbestemt eller geografisk målrettet logning. Der lægges heller ikke op til at fastsætte nærmere regler om godtgørelse for udgifter forbundet med udlevering af oplysninger til politiet. Justitsministeriet skal hertil bemærke, at størstedelen af udgifterne i forbindelse med udlevering af oplysninger i dag afregnes med teleselskaberne via en såkaldt flatrate-aftale, hvor telebranchen kompenseres ud fra på forhånd fastlagte rammer. Hertil kompenseres telebranchen for særskilte udgifter forbundet med hastesikring af oplysninger uden for flatrate-aftalerne ud fra faste timegebyrer. Der lægges op til, at udgifter for telebranchen relateret til udlevering af oplysninger til politiet

fremadrettet håndteres på lignende vis, idet der kan være behov for visse tilpasninger.

Justitsministeriet bemærker endvidere, at formuleringen i de specielle bemærkninger til den foreslåede § 786 g i retsplejeloven hvor det anføres, at der vil kunne fastsættes regler om opbevaringsformat (læsbarhed), foranstaltninger til beskyttelse mod uautoriseret adgang til og manipulation af loggen samt opbevaring af kontooplysninger, svarer til den formulering, der i dag fremgår af forarbejderne til retsplejelovens § 786, stk. 4, jf. bemærkningerne til § 2, nr. 2 og 3, i lovforslag nr. L 35 som fremsat, jf. Folketingstidende 2001-02 (2. samling), tillæg A, side 879. Der er således alene tale om videreførelse af en mulighed, som også foreligger i dag. Det er ikke i lovforslaget forudsat, at bemyndigelsen udnyttes til at fastsætte sådanne regler i forbindelse med lovens ikrafttræden.

Som det fremgår af pkt. 3, 4 og 12 i den kommenterede høringsoversigt og pkt. 10 i lovforslagets almindelige bemærkninger, er det Justitsministeriets vurdering, af lovforslaget ligger inden for rammerne af EU-retten.

17. Forholdet til gældende databeskyttelsesretlige regler

Datatilsynet anfører, at tilsynet har forstået lovforslaget således, at det er Justitsministeriets vurdering, at de foreslåede regler om teleudbyderes registrering og opbevaring af oplysninger om trafikdata (logning) er omfattet af e-databeskyttelsesdirektivets anvendelsesområde, hvorimod de foreslåede regler om teleudbyderes videregivelse af loggede oplysninger – i det omfang der er tale om personoplysninger – er omfattet af databeskyttelsesforordningens anvendelsesområde.

Datatilsynet bemærker i den forbindelse, at det tidligere i nogle tilfælde har givet anledning til tvivl, om det er Erhvervsstyrelsen eller Datatilsynet, som på baggrund af henholdsvis e-databeskyttelsesdirektivet eller databeskyttelsesforordningen har kompetence til at føre tilsyn. Det kan derfor overvejes at præcisere denne kompetencefordeling i lovforslaget.

Herudover bemærker Datatilsynet, at princippet om formålsbegrænsning i databeskyttelsesforordningens artikel 5, stk. 1, litra b, indebærer, at personoplysninger skal indsamles til udtrykkeligt angivne og legitime formål og ikke må viderebehandles på en måde, der er uforenelig med disse formål. Bestemmelsen suppleres af databeskyttelsesforordningens artikel 6, stk. 4,

som nærmere fastsætter, hvornår der kan ske behandling af personoplysninger til et andet formål end det, personoplysningerne oprindeligt er indsamlet til. Behandling til et andet formål kan bl.a. ske, når behandlingen er baseret på EU-retten eller medlemsstaternes nationale ret, som udgør en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund af hensyn til de mål, der fremgår af databeskyttelsesforordningens artikel 23, stk. 1.

Datatilsynet opfordrer på den baggrund til, at det så vidt muligt i lovforslaget uddybes, hvorfor teleudbyderes videregivelse af loggede personoplysninger til politiet vurderes at være i overensstemmelse med princippet om formålsbegrænsning i databeskyttelsesforordningens artikel 5, stk. 1, litra b, i de tilfælde, hvor oplysningerne er logget med henblik på at beskytte den nationale sikkerhed, men videregives til brug for bekæmpelse af grov kriminalitet.

PROSA bemærker, at GDPR giver borgeren krav på at få en kopi af de data, der er registreret om borgeren, herunder de data, som indsamles i medfør af logningsbekendtgørelsen. PROSA anfører, at borgeren automatisk bør få en kopi, når en overvågning indstilles. F.eks. ved, at borgeren modtager en SMS, hvorigennem borgeren kan hente en kopi af de data, der er registreret om vedkommende.

TI anfører, at spørgsmålet om slutbrugernes indsigtsret i trafikdata, som er logget efter reglerne om målrettet logning, ikke er omtalt i lovudkastet. TI opfordrer til, at det konkretiseres i bemærkninger til lovforslaget, hvordan databeskyttelseslovens regler om begrænsninger i den registreredes indsigtsret finder anvendelse på loggede trafikdata.

Justitsministeriet bemærker, at lovforslaget ikke vedrører det mere generelle spørgsmål om kompetencefordeling mellem Erhvervsstyrelsen og Datatilsynet i relation til spørgsmål omfattet af henholdsvis e-databeskyttelsesdirektivet og databeskyttelsesforordningen. Lovforslaget har til formål at revidere de gældende regler om registrering og opbevaring af teletrafik (logning) m.v. Hertil kommer, at der lægges op til, at lovforslaget skal træde i kraft 1. januar 2022, så de gældende regler revideres hurtigst muligt. Der er på den baggrund ikke med dette lovforslag lagt op til at ændre ved eller præcisere det nævnte mere generelle spørgsmål om kompetencefordeling mellem Erhvervsstyrelsen og Datatilsynet.

Desuden bemærker Justitsministeriet, at lovforslaget siden høringsversionen er justeret, så der i retsplejelovens § 786 i indsættes en bestemmelse om tavshedspligt. Det fremgår således nu af pkt. 3.1.3.4 i lovforslagets almindelige bemærkninger, at det foreslås, at udbyderne pålægges en tavshedspligt for oplysninger om, hvor eller over for hvem der foretages målrettet registrering og opbevaring af trafikdata på baggrund af pålæg i medfør af de foreslåede § 786, stk. 3, og §§ 786 c og 786 d i retsplejeloven, som supplerer og præciserer tavshedspligten i telelovens § 7. Den foreslåede særlige tavshedspligt indebærer, at sådanne oplysninger skal hemmeligholdes af udbyderne, og at de alene må anvendes med henblik på videregivelse til politiet med henblik på beskyttelse af national sikkerhed og bekæmpelse af grov kriminalitet. Den foreslåede særlige tavshedspligt er ikke til hinder for lovbestemt adgang for f.eks. tilsynsmyndigheder i forbindelse med tilsyn.

Herudover foreslås det med den foreslåede § 786 i, stk. 2, i retsplejeloven, at tavshedspligten også skal finde anvendelse over for de personer, som oplysningerne vedrører, uanset en eventuel retlig forpligtelse til at videregive oplysningerne til den pågældende i henhold til databeskyttelseslovgivningen.

Derudover foreslås det med den foreslåede § 786 i, stk. 3, at udbydere skal orientere politiet om brud på persondatasikkerheden, jf. databeskyttelsesforordningens artikel 4, pkt. 12, der ville udløse en underretningspligt af de registrerede efter databeskyttelsesforordningens artikel 34.

For nærmere om den foreslåede tavshedspligt henvises til pkt. 3.1.3.4 i lovforslagets almindelige bemærkninger.

Justitsministeriet bemærker herudover, at det ikke er hensigten med forslaget at etablere en ordning, hvor borgeren automatisk får en kopi af de data, der er registreret om borgeren, når registrering og opbevaring indstilles.

I lyset af Datatilsynets høringssvar er lovforslagets pkt. 3.7.4.1 også blevet uddybet, så det nu bl.a. fremgår, at videregivelse af oplysninger, der er registreret og opbevaret af hensyn til beskyttelsen af national sikkerhed, fra udbyderne til politiet til brug for politiets bekæmpelse af grov kriminalitet, ikke vurderes at være uforenelig med de formål, hvortil oplysningerne oprindeligt er indsamlet jf. databeskyttelsesforordningens artikel 5, stk. 1, litra b. Justitsministeriet lægger i den forbindelse vægt på, at der er tale om nært beslægtede formål, og at politiets adgang til oplysninger, der er registreret

og opbevaret af hensyn til beskyttelsen af national sikkerhed, til brug for politiets bekæmpelse af grov kriminalitet, som det fremgår under pkt. 3.7.2 og 3.7.3 i lovforslagets almindelige bemærkninger, vurderes at være forenelig med EU-retten. Der vurderes dog som anført i lovforslaget at være en væsentlig procesrisiko forbundet med denne form for adgang.

Efter Justitsministeriets vurdering vil det således være i overensstemmelse med de grundlæggende behandlingsprincipper i forordningens artikel 5, herunder principperne om lovlighed og formålsbegrænsning, at udbyderne videregiver oplysninger, der er registreret og opbevaret af hensyn til beskyttelsen af national sikkerhed, til politiet med henblik på bekæmpelse af grov kriminalitet.

III. Lovforslaget

I forhold til det udkast til lovforslag, der blev sendt i høring den 27. september 2021, indeholder det fremsatte lovforslag følgende mere indholdsmæssige ændringer:

- I forslaget til retsplejelovens § 786 b, stk. 3, nr. 4, er »indgreb« ændret til »pålæg«.
- Det er tydeliggjort, at lovforslagets § 2, nr. 2, hvorefter omfanget af de oplysninger, der forstås ved nummeroplysningsdata efter telelovens § 31, stk. 2, udvides, ikke gælder for så vidt angår allerede eksisterende taletidskort- og fastnettelefoniabonnenter, jf. § 3, stk. 3, i det fremsatte lovforslag. Der vil således ikke skulle ske efterregistrering af unikt ID og eventuelle oplysninger om bruger for allerede eksisterende taletidskort- og fastnettelefoniabonnenter, herunder IP-telefoniabonnenter.
- Det er tydeliggjort, at der skal kunne fastsættes regler om, at kravene til registrering og verificering af nummeroplysningsdata også skal gælde for uregistrerede taletidskort. Det vil indebære, at der fra ikrafttræden af sådanne regler ikke længere vil kunne købes såkaldte "anonyme" taletidskort.
- Det er tydeliggjort, at udbyderne alene er forpligtet til at foretage registrering og opbevaring af data, der genereres eller behandles i udbyderens net. Det betyder, at oplysninger om trafikdata, der f.eks. af tekniske grunde ikke generes eller behandles i udbyderens net, ikke skal registreres og opbevares.

- Lovforslaget er justeret, så det for så vidt angår de foreslåede ordninger med målrettet og generel og udifferentieret registrering af trafikdata fremgår klart, hvilke teletjenester de forskellige opremsninger af omfattede datatyper, der beskrives i lovforslagets almindelige og specielle bemærkninger, relaterer sig til.
- Lovforslaget er justeret, så der alene arbejdes med ét udbyderbegreb, nemlig "udbydere", der skal forstås i overensstemmelse med det tilsvarende begreb i telelovgivningen.
- Det er i lovforslagets bemærkninger tydeliggjort, at det forudsættes, at udbydere, som pålægges at foretage målrettet personbestemt registrering og opbevaring af trafikdata efter de foreslåede §§ 786 b og 786 d i retsplejeloven, i forbindelse med meddelelse af pålæg herom får oplysninger om, hvilke telefonnumre eller kommunikationsapparater der skal iværksættes registrering og opbevaring af trafikdata vedrørende.
- I lovforslagets bemærkninger er begrebet "den dataansvarlige udbyder" ændret til "den tjenesteproducerende udbyder".
- Det er i lovforslagets bemærkninger tydeliggjort, at den foreslåede § 804 b i retsplejeloven, hvorved telelovens § 13 indholdsmæssigt foreslås videreført i retsplejeloven, ikke omfatter udlevering af trafikdata.
- Lovforslaget er justeret, så det klart fremgår, at hastesikring alene kan ske med henblik på bekæmpelse af grov kriminalitet, jf. bl.a. lovforslagets § 1, nr. 6, og de specielle bemærkninger hertil.
- For så vidt angår de foreslåede §§ 786 b og 786 c i retsplejeloven er forholdet til forvaltningsloven tydeliggjort. Det har ført til redaktionelle ændringer i lovtekst samt tilføjelser i almindelige og specielle bemærkninger.
- Der er indsat et nyt forslag til en ny § 786 i i retsplejeloven, hvorefter udbydere, der er pålagt at foretage registrering og opbevaring af trafikdata efter de foreslåede § 786 b, stk. 3, eller §§ 786 c eller 786 d under ansvar efter straffelovens §§ 152-152 e, er forpligtet til at hemmeligholde oplysninger, der modtages og behandles i forbindelse med et sådant pålæg. Tavshedspligten gælder også i forhold til den person, som oplysningerne vedrører, uanset en eventuel retlig forpligtelse til at videregive oplysningerne til den pågældende i henhold til databeskyttelseslovgivningen. Udbydere, der er pålagt at foretage registrering og opbevaring af trafikdata efter § 786 b, stk. 3, eller §§ 786 c eller 786 d, vil efter forslaget også være forpligtet til at orien-

tere politiet om brud på persondatasikkerheden, jf. databeskyttelsesforordningens artikel 4, nr. 12, der kunne udløse en underretningspligt af de pågældende personer efter databeskyttelsesforordningens artikel 34.

- Det er tydeliggjort, at det på det foreliggende grundlag er vurderingen, at der i 2022 vil foreligge en alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig, og at det således er Justitsministeriets forventning, at der i 2022 med hjemmel i den foreslåede § 786 e i retsplejeloven vil kunne fastsættes regler, der pålægger udbyderne at foretage generel og udifferentieret registrering og opbevaring af trafikdata. Det er samtidig tydeliggjort, at de relevante myndigheder – under dialog med telebranchen – i umiddelbar forlængelse af lovens ikrafttræden vil skulle udarbejde bekendtgørelser, der fastsætter de nærmere rammer for målrettet registrering og opbevaring af trafikdata efter de foreslåede §§ 786 b-786 d i retsplejeloven, herunder regler om understøttelse af målrettet registrering og opbevaring af trafikdata i overgangsperioden fra lovens ikrafttræden, indtil den nødvendige it-systemunderstøttelse af målrettet registrering og opbevaring af trafikdata er på plads. Bekendtgørelserne vil skulle udstedes hurtigst muligt efter lovens ikrafttræden. Med bekendtgørelserne vil der kunne tages højde for den systemunderstøttelse, der er til rådighed på tidspunktet for udstedelse af bekendtgørelsen. Det forudsættes, at udbyderne med kort varsel kan understøtte en overgang fra generel og udifferentieret registrering og opbevaring til målrettet registrering og opbevaring i medfør af relevante udstedte bekendtgørelser.
- Der er indsat et nyt § 786 e, stk. 3, i retsplejeloven, hvoraf det fremgår, at oplysninger registreret og opbevaret i medfør af den foreslåede § 786 e, stk. 1 – ligesom de øvrige registrerings- og opbevaringspligtige oplysninger – skal opbevares i 1 år.
- Lovforslagets § 3, stk. 4, er affattet, så det nu tydeligt fremgår, at justitsministeren efter forhandling med erhvervsministeren i en overgangsperiode kan fastsætte nærmere regler om fravigelse af retsplejelovens §§ 786 b-786 d som affattet ved denne lovs § 1, nr. 10, herunder at reglerne helt eller delvist ikke skal anvendes.

Herudover har Justitsministeriet foretaget en række ændringer og præciseringer af lovteknisk og redaktionel karakter.