Østre Landsret
Præsidenten

Justitsministeriet
Slotsholmsgade 10
1216 København K

1. oktober 2021

J.nr.: 21/22278-1

Sagsbehandler: Stine Dyppel

Sendt pr. mail til: jm@jm.dk, hlm@jm.dk og nat@jm.dk.

Justitsministeriet har ved brev af 28. september 2021 (sagsnr. 2020-187-0036) anmodet om eventuelle bemærkninger til høring over udkast til 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.).

I den anledning skal jeg meddele, at landsretten ikke ønsker at udtale sig om udkastet.

Med venlig hilsen

Carsten Kristian Vollmer

Ellen Busck Porsbo

Til Justitsministeriet.

Politiforbundet har ingen bemærkninger til høringen.

Politiforbundets jr.nr. 2021-01357.

Med venlig hilsen

Jan Hempel
Forbundssekretær

POLITI FORBUNDET
Indsigt · Udsyn · Fremsyn

Gammel Kongevej 60, 11. sal
DK-1850 Frederiksberg

Tlf. +45 3345 5965
E-mail mail@politiforbundet.dk

Københavns Byret

Justitsministeriet

Præsidenten
Domhuset, Nytorv 25
1450 København K.
Tlf. 99 68 70 15
CVR 21 65 95 09
adm.kbh@domstol.dk
J.nr. 21/22460

Den 5. oktober 2021

Ved en mail af 28. september 2021 har Justitsministeriet anmodet om eventuelle bemærkninger til høring over udkast til 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.).

Jeg skal i den anledning på vegne af byretspræsidenterne oplyse, at byretterne ikke ønsker at udtale sig om udkastet.

Der henvises til J.nr. 2020-187-0036.

Med venlig hilsen

Søren Axelsen

Vestre Landsret
Præsidenten

Justitsministeriet
Sikkerhedskontor II
Slotsholmsgade 10
1216 København K

4. oktober 2021

J.nr.: 21/22717-2

Sendt pr. mail til jm@jm.dk, hlm@jm.dk og nat@jm.dk

Sagsbehandler: Lars B Olesen

Justitsministeriet har ved brev af 27. september 2021 (sagsnr. 2020-187-0036) anmodet om eventuelle bemærkninger til høring over udkast til 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.).

I den anledning skal jeg meddele, at landsretten ikke ønsker at udtale sig om udkastet.

Med venlig hilsen

Helle Bertung

DATATILSYNET

Justitsministeriet
Slotsholmsgade 10
1216 København K

14. oktober 2021

J.nr. 2021-11-0720
Dok.nr. 397756
Sagsbehandler
Anna Carolina Jensen

Sendt til jm@jm.dk; hlm@jm.dk; nat@jm.dk

Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

CVR 11883729

Høring over udkast til 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.)

Ved e-mail af 27. september 2021 har Justitsministeriet anmodet om Datatilsynets eventuelle bemærkninger til ovennævnte lovforslag.

Datatilsynet skal i den anledning udtale følgende:

1. Generelle bemærkninger

1.1 Det fremgår af lovforslaget, at det har til formål at bringe de gældende logningsregler i overensstemmelse med EU-retten som fortolket af EU-Domstolen.

Datatilsynet har dog i den forbindelse noteret sig det af Justitsministeriet anførte om, at dele af lovforslaget desuagtet vurderes at være forbundet med en væsentlig procesrisiko, jf. afsnit 2 nedenfor.

Datatilsynet skal endvidere generelt bemærke, 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.

1.2 Datatilsynet 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 vil derfor i det følgende som tilsynsmyndighed efter databeskyttelsesforordningen alene forholde sig til sidstnævnte del af lovforslaget.

Datatilsynet skal i den forbindelse bemærke, 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

med overholdelsen af de gældende logningsregler. Det kan derfor overvejes at præcisere denne kompetencefordeling i lovforslaget.

2. Videregivelse af loggede oplysninger

Med lovforslaget lægges der op til at ændre de gældende regler i retsplejeloven om politiets og anklagemyndighedens adgang til de oplysninger, som teleudbyderne er forpligtet til at logge.

Det vil således fremover alene være muligt at få adgang til sådanne oplysninger med henblik på bekæmpelse af grov kriminalitet eller beskyttelse af den nationale sikkerhed. Samtidig indebærer lovforslaget dog, at oplysninger, som er logget med det formål at beskytte den nationale sikkerhed, også vil kunne videregives til brug for politiets og anklagemyndighedens bekæmpelse af grov kriminalitet.

Af lovforslagets almindelige bemærkninger (pkt. 3.7.4.1) fremgår det, at teleudbyderes udlevering af loggede personoplysninger til politiet – for at efterkomme et pålæg i medfør af de i lovforslaget foreslåede bestemmelser herom – af Justitsministeriet anses for at være i overensstemmelse med databeskyttelsesforordningens behandlingsbetingelser, jf. artikel 6, stk. 1, litra c, hvorefter personoplysninger kan videregives, når det er nødvendigt for at overholde en retlig forpligtelse. Justitsministeriet finder endvidere, at en sådan videregivelse vil være i overensstemmelse med de grundlæggende behandlingsprincipper i databeskyttelsesforordningens artikel 5, herunder principperne om lovlighed og formålsbegrænsning.

Det fremgår samtidig af lovforslagets almindelige bemærkninger (pkt. 10), at der vurderes at være en væsentlig procesrisiko forbundet med, at der i lovforslaget lægges op til, at politiet og anklagemyndigheden vil kunne få adgang til trafikdata, der er logget med henblik på at beskytte den nationale sikkerhed, til brug for politiets og anklagemyndighedens bekæmpelse af grov kriminalitet.

Datatilsynet bemærker, 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 skal på den baggrund opfordre 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.

Med venlig hilsen

Anna Carolina Jensen

19. oktober 2021

Til Justitsministeriet

fremsendt pr. mail til jm@jm.dk
med kopi til hlm@jm.dk og nat@jm.dk

Dansk Journalistforbund
medier & kommunikation

The Danish Union of Journalists

Gammel Strand 46
1202 København K
Danmark

+45 3342 8000
dj@journalistforbundet.dk
journalistforbundet.dk

Dansk Journalistforbunds høringssvar vedr. udkast til lov om ændring af reglerne om registrering og opbevaring af oplysninger om teletrafik (logning mv.)

Dansk Journalistforbund, DJ, skal hermed fremkomme med sit høringssvar vedr. udkast til 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) mv.).

Lovudkastet indeholder intet om den redaktionelle kildebeskyttelse:
Foruden de nedenstående generelle bemærkninger, vil vi fra DJ's side først og fremmest understrege en konkret og meget principiel problemstilling i forbindelse med logning: Mediernes muligheder for at kunne beskytte sine kilder jf. retsplejelovens bestemmelser.

Den logning, der foregår, bør under ingen omstændigheder kunne udgøre en risiko for mediernes muligheder for at kunne beskytte sine kilder.
Og logningsreglerne bør lige så lidt som telefonaflytning eller andre indgreb i meddelelseshemmeligheden kunne bringe denne kildebeskyttelse i fare.

Det foreliggende lovudkast indeholder ingen bestemmelser, der kan sikre denne kildebeskyttelse. Og i bemærkningerne til lovforslaget har man 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.

Generelt om logning:
Fra DJ's side anerkender vi, at det er et helt legitimt ønske fra regeringens og Folketingets side at ville styrke efterforskningen og retsforfølgningen af strafbare forhold. Det er dette ønske, der ligger bag den oprindelige lovgivning om registrering og opbevaring af oplysninger om teletrafik.

Fra DJ's side er vi 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.

Og i DJ er vi ikke overbeviste om, at den efterforskningsmæssige nytteværdi af logningen kan opveje de principielle problemer med overvågning og de praktiske risici ved opbevaring af de megastore datamængder.

Til de sidstnævnte praktiske risici hører ikke mindst risikoen for læk og udsivning af fortrolige oplysninger.

Fra DJ's side stiller vi os meget gerne til rådighed med hensyn til det ovennævnte om kildebeskyttelse.
Det gælder også, hvis dette høringssvar i øvrigt giver anledning til yderligere spørgsmål eller kommentarer.
Kontakten kan blandt andet ske på mail DJ@journalistforbundet.dk.

Venlig hilsen
pva. Dansk Journalistforbund

Hans Jørgen Dybro
politisk konsulent

Justitsministeriet

København, den 23. oktober 2021

Vedr. høring over udkast til 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.), Deres sagsnr. 2020-187-0036

Justitsministeriet har ved mail af 27. september 2021 anmodet om Dommerfuldmægtigforeningens eventuelle bemærkninger til udkast til 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.).

Foreningen skal i den anledning meddele, at foreningen ikke har bemærkninger til lovforslaget.

Dette høringssvar sendes alene elektronisk til: jm@jm.dk med kopi til hlm@jm.dk og nat@jm.dk.

På foreningens vegne,

René Bergfort
Høringsansvarlig
Dommerfuldmægtigforeningen

Justitsministeriet
Slotsholmsgade 10
1216 København K

13. oktober 2021

Høringssvaret er sendt elektronisk til jm@jm.dk, hlm@jm.dk og nat@jm.dk

DM's høringssvar vedr. forslag til revision af reglerne om registrering og opbevaring af oplysninger om teletrafik (logning) m.v. oktober 2021

DM takker for muligheden for at afgive bemærkninger, og vi finder det positivt, at Justitsministeriet nu har påbegyndt den lovrevision af logningsreglerne, der har været nødvendig siden 2016. Men vi finder den del af lovforslaget, der knytter sig til generel og udifferentieret logning af alle borgere for bekymrende.

Dele af Justitsministeriets foreslåede ordning vil reelt medføre opretholdelse af den nuværende tilstand, hvor kriminalitetsbekæmpelse kan legitimere en generel og udifferentieret logning af alle borgeres telefonsamtaler. Da flere EU-domme for længst har slået fast, at systematisk og ubegrænset indsamling af teledata er i strid med EU's regler, og en krænkelse af rette til fri kommunikation og privatliv, kan vi ikke tilslutte os denne del af lovforslaget.

Vi anerkender, at politiet skal have gode efterforskningsmuligheder i forbindelse med grov kriminalitet og terrortrusler, men vi mener det er uacceptabelt, at der opretholdes en tilstand, hvor der indsamles oplysninger om alle danskere, uanset om de nogensinde har været på kant med loven – hvem de taler i telefon med, hvor de befinder sig, når de taler og hvor længe de taler.

DM anbefaler på det kraftigste, at der findes en løsning med målrettet logning, hvor de grundlæggende frihedsrettigheder for alle danskere ikke indskrænkes, men hvor der alene foretages logning af konkrete personer, som politiet har en rimelig formodning om, er involveret i alvorlig kriminalitet eller terror.

Ønskes ovenstående uddybet er I velkomne til at kontakte undertegnede.

Venlig hilsen

Camilla Gregersen
Formand

DM
Peter Bangs Vej 30
2000 Frederiksberg

+45 38 15 66 00
dm.dk

Ved e-mail af 27. september 2021 har Justitsministeriet anmodet om Domstolsstyrelsens eventuelle bemærkninger til udkast til lovforslag om ændring af retsplejeloven og lov om elektroniske kommunikationsnet og -tjenester (Revision af logningsreglerne m.v.), Justitsministeriets j.nr. 2020-187-0036.

I den anledning kan Domstolsstyrelsen henvise til styrelsens høringssvar af 27. juli 2021 til præhøring over udkast til lovforslag om revision af logningsreglerne. Domstolsstyrelsen har ikke yderligere bemærkninger til udkastet til forslag til lov om ændring af retsplejeloven og lov om elektroniske kommunikationsnet og -tjenester (Revision af logningsreglerne m.v.).

Med venlig hilsen

Charlotte Edholm
Specialkonsulent og forretningsejer straffesagsområdet
Jura og Forretning
Tlf. direkte 2327 6255
ched@domstolsstyrelsen.dk

Domstolsstyrelsen
Center for Forretning og Udvikling
St. Kongensgade 1-3
1264 København K.
Tlf. (hovednr.): + 45 70 10 33 22
www.domstol.dk

PROSA
Forbundet af It-professionelle

Association of IT Professionals
Vester Farimagsgade 37A
1606 København V

Søren Frichs Vej 38K
8230 Åbyhøj

Overgade 54
5000 Odense

prosa.dk
+45 33 36 41 41

Justitsministeriet
jm@jm.dk, hlm@jm.dk og nat@jm.dk

København, 25. oktober 2021

Høringssvar til udkast til 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.)

PROSA takker for at blive inviteret til at deltage i høringen.

PROSA mener, at borgere som udgangspunkt skal have ret til et privatliv uden overvågning. GDPR lægger op til det samme: Man må ikke registere mere end man har brug for.

GDPR er vedtaget efter den første Logningsbekendtgørelse, og Snowdens afsløringer har vist at den massive registrering af borgere kan være farlig.

PROSA mener, at man skal lade værdierne fra GDPR gennemsyre Logningsbekendtgørelsen: Log kun det mest nødvendige, og i så kort tid som muligt, og gør det teknisk umuligt at få adgang til data uden retskendelse.

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

I PROSA har vi Trump-testen: Ville vi være trygge ved at give et redskab til Trump, Viktor Orban eller den polske regering, der har vist sig ret fjendtlige overfor abort og LGBT-personer? De er alle valgt ved frie demokratiske valg. Hvis vi ikke er trygge ved det, så bør vi heller ikke tillade at bruge redskabet i Danmark, for vi er kun eet folketingsvalg væk fra at det bedste demokrati bliver det værste demokrati.

I dens nuværende form består revisionen ikke Trump-testen: Der er al for meget overvågning af uskyldige.

Snowden bruger begrebet Turnkey Tyranny om et demokratisk land, der indfører teknologi, der kan bruges til at undertrykke befolkningen, hvis blot den falder i de forkertes hænder. Logningsbekendtgørelsen falder klart i den kategori.

Kriminelle vil udnytte alle de muligheder, der er i et frit samfund, men fjerner man friheden, så har man ikke længere et frit samfund. Vi har desuden aldrig set dokumentation for, at de drastiske indgreb i privatlivet har hjulpet. Det burde være nemt at dokumentere i dag.

Fagforeninger var ulovlige, da de opstod. Med den overvågning vi har i dag, så ville de have været kvalt i fødslen. PROSA mener, at i et frit samfund skal være frirum til, at samfundsændringer af samme størrelse kan opstå også i fremtiden.

Eller antag, at aborten stadig ikke var fri: Hvis man kunne tracke placeringen af alle mobiltelefoner, og alle opkald, så skal der ikke meget dataanalyse til at identificere de læger, som laver ulovlig aborter.

Hvis vi ønsker at udvikle vores demokrati også i fremtiden, så er vi nødt til at give plads til kontroversielle tanker, som udfordrer vores nuværende demokrati.

Privatlivsberøvelse som straf §786b

Når man har udstået sin straf skal man behandles som en uskyldig og naturligvis ikke overvåges, men vi kan godt se en rimelighed i at give en dommer mulighed for at kunne idømme frihedsberøvelse og privatlivsberøvelse i den kombination, som dommeren finder mest formålstjenesteligt. Men dette skal ikke ske per automatik.

Geografisk logning §786c+d

PROSA er som nævnt modstander af at logge folk, der ikke er under mistanke. Det gælder også baseret på geografi.

Men ønsker man at vedtage §786c+d, så bør det belyses, hvor stor en del af Danmark, der har 1.5 gange gennemsnittet. Vores fornemmelse siger, at dette i praksis vil betyde at alle større byer vil være dækket, idet landbrugsarealer vil trække gennemsnittet voldsomt ned. Lægger vi dertil alle sikringskritiske områder, så vil det formodentlig dække alle tættere befolkede områder.

Mobilmaster er desuden ikke designet til at logge kvadrater på 3x3 km^2. Og for at dække de 3x3 km^2 kan det derfor være nødvendigt at dække et langt større område.

Hvis dette i praksis betyder, at 100.000-vis af uskyldige vil blive logget, så mener vi ikke det er et proportionelt indgreb i privatlivet.

Vi kan have en vis sympati for, at man gerne vil logge ekstra områder med stor kriminalitet, men det bør i så fald være kunne ske efter behov og med en retskendelse, og sikring af at det er et proportionalt indgreb med logning af få uskyldige. Logning af mere end 2% af befolkningen vil vi finde uproportionalt.

Generel og udifferentieret logning i kriser §786e

Der lægges op til at lave generel og udifferentieret logning hvis Danmark står over for en alvorlig trussel.

Men det defineres ikke, hvad dette er.

PROSA mener derfor, at det ikke må være op til blot 2 ministere at blive enige om dette: Det skal være en folketingsbeslutning.

Udifferentieret logning af internet §786f

PROSA er stærke modstandere af den udifferentierede logning. At logge al internettraffik er formodentlig i strid med EU's menneskerrettigheder, idet det er et uproportionalt stort indgreb.

Som minimum bør denne logning begrænses til at omfatte de samme vilkår som den anden logning, men PROSA så helst den helt bortfaldt.

Anonyme taletidskort §786h

Da PROSA mener, at borgerne som udgangspunkt har ret til et privatliv, mener vi naturligvis også, at man skal have lov til at købe anonyme taletidskort.

Det kan f.eks. være hvis man ønsker at undslippe en eks-kæreste, som har adgang til registeret over ejeren af telefonnummeret. Her hjælper det ikke at have hemmelig adresse. Men det hjælper at bruge anonyme taletidskort.

Da der idag ikke er en infrastruktur til at foretage den obligatoriske registrering af disse kort, og da de udgør en mindre del af markedet, mener vi også at man børe undersøge, hvilke økonomiske konsekvenser det vil have. Hvis et taletidskort stiger fra 50 kr i dag til 500 kr, så vil det i praksis betyde en afskaffelse af taletidskort.

Hvis disse kort er særligt problematiske for politiet, så er vi åbne over for at gøre det nemmere at få retskendelse til at overvåge den type kort.

Men ved edition eller overvågning skal uskyldige informeres.

Demokratisk kontrol

Flere steder i revisionen lægges op til at Justitsministeren og Erhvervsministeren kan iværksætte og forlænge yderst indgribende logning.

En sådan beslutning bør være en folketingsbeslutning - både for at skabe demokratisk legitimitet og for at skabe den fornødne transperens om det.

Transparens

PROSA har uden held flere gange prøvet at få statistisk information om hvor meget logningsbekendtgørelsen bruges og hvor store straffe det medfører.

Det bør være et krav, at revisionen sikrer, at der opsamles statistisk materiale, så vi i fremtiden kan evaluere effekten af logningsbekendtgørelsen.

Det kunne f.eks. være:

- hvor mange sager, man har brugt bestemmelserne i,
- hvor mange fængselsår disse sager er blevet til
- hvor mange af disse sager, der ikke førte til dom
- hvor mange uskyldige, der er blevet logget

Forbundet af It-professionelle

Uskyldiges adgang til logdata

GDPR giver allerede i dag borgeren krav på at få en kopi af de data, der er registreret om borgeren - herunder de data, som opsamles som medfør af logningsbekendtgørelsen.

PROSA mener, at borgeren automatisk skal have en kopi, når en overvågning indstilles. Det kan f.eks. ske ved at en ikke-mistænkt logget borger modtager en SMS, hvor borgeren kan hente en kopi af de data, der er registeret. Dette skal senest ske en måned før data slettes.

Dette kan være med til at skabe transperens for borgeren, så borgeren ikke blot bliver gjort opmærksom på overvågningen, men også hans ret til at modtage de loggede data.

Venlig hilsen

Niels Bertelsen

Formand

Justitsministeriet
Att.: Sikkerhedskontor II
Slotsholmsgade 10
1216 København K
Sendt til jm@jm.dk, hlm@jm.dk og nat@jm.dk

Den 25. oktober 2021

Høring over forslag til lov om ændring af retsplejeloven og lov om elektronisk kommunikationsnet og -tjenester (revision af logningsreglerne)

Generelle bemærkninger

Dansk Erhverv og IT-Branchen takker for invitationen til høring over revisionen af logningsreglerne.

Dansk Erhverv og IT-Branchen støtter, at den juridisk uklare og omdiskuterede retstilstand på området skal bringes til ophør til fordel for klare regler, der hviler på et solidt juridisk grundlag. Justitsministeriet bør således med revisionen af logningsloven sikre, at der ikke fremover vil være tvivl om, hvorvidt lovgrundlaget for myndighedernes krav til teleselskaberne om at logge og udlevere trafikdata m.m., er i orden. Hvis myndighederne skal have adgang til data, skal retsgrundlaget være stærkt.

Nye logningsregler bør skabe klarhed og forudsigelighed på området, og 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 Dansk Erhverv og IT-Branchen ikke, at lovforslaget lever op til disse grundlæggende krav.

Justitsministeriet vurderer således selv, at der er en betydelig procesrisiko i forbindelse med 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.

Lovforslagets muligheder for at iværksætte 'målrettet logning' er endvidere så omfattende, at grænsen til generel logning udviskes. For borgere, der ofte befinder sig på fx befærdede steder, vil det være reglen nærmere end undtagelsen, at der logges teletrafikdata fra deres mobiltelefon.

Lovforslagets fortolkning af målrettet logning – og de deraf følgende nye krav om registrering og indberetning af kundedata (bl.a. CPR) – bliver i øvrigt teknisk og sikkerhedsmæssigt yderst vanskelige at efterleve. Der er ikke ét teleselskab, der i øjeblikket ved, hvordan de skal efterleve kravene.

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. En forhastet lovproces og urealistisk implementeringsfrist øger markant risikoen for, at vi står over for mange nye alvorlige sager om politiets anvendelse af teledata.

Det bemærkes derfor, at det grundlæggende er urealistisk at lade loven træde i kraft d. 1. januar 2022. Som minimum bør der indføres en betydeligt længere implementeringsfrist hvis forslaget, trods branchens advarsler, alligevel træder i kraft 1. januar 2022.

Det bliver desuden omkostningsfuldt for teleselskaberne at konstruere de nye systemer. Alene omstillingsomkostningerne er vurderet til 206 mio. kr. 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 206 mio. kr.

Grundlaget for at påføre så betydelige omstillingsomkostninger på selskaberne forekommer endvidere spinkelt i lyset af den nævnte procesrisiko. Dansk Erhverv og IT-Branchen har således en bekymring i forhold til, om lovforslaget ligger inden for EU rettens rammer. Såfremt det helt eller delvist underkendes som være uforenelige med EU-retten, vil teleselskabernes udgifter til nye it-systemer og procedurer være spildte.

Der bør derfor som et minimum foretages en ny byrdevurdering i lyset af det samlede forslag med henblik på en reel omkostningsdækning for selskaberne.

Specifikke bemærkninger
Teleindustrien har med førende tekniske og juridiske specialister fra medlemsvirksomheder foretaget en grundig gennemgang af forslaget. Dansk Erhverv og IT-Branchen støtter de specifikke kommentarer i Teleindustriens høringssvar.

Hovedpunkterne kan sammenfattes i følgende:

- Forslaget om registrering af unikt ID og indberetning af CPR/CVR/UniktID for alle kunder samt oplysning om forventet bruger til en fælles nummeroplysningsdatabase (118-databasen) er ikke proportionalt og bør udgå eller udskydes med henblik på en nærmere belysning

- Lovudkastet bør præciseres, så det fremgår at politiet skal oplyse de telefonnumre, der skal iværksættes målrettet personbestemt logning for.

- Regler om geografisk målrettet logning bør som hidtil forudsat kun omfatter mobiltjenester.

- Afsnittet i lovudkastet om en frafiltreringsmekanisme ønskes slettet.

- Det bør tydeliggøres i lovforslaget, hvilke udbydere, hvilke tjenester og hvilke datatyper, der er omfattet af de nye regler.

- Der efterlyses klare og enkle regler om udlevering af trafik- og lokaliseringsdata til politiet.

- Der bør sikres en reel omkostningsdækning for de teleselskaber, som bliver pålagt at foretage målrettet logning, som er et rent efterforskningsmæssigt værktøj.

- Der opfordres 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.

Økonomiske konsekvenser
JM anslår, at målrettet logning vil medføre et omfattende udvidet sagsbehandlingsarbejde, der medfører merudgifter for politiet, anklagemyndigheden og domstolene på potentielt over 200 mio. kr. årligt. Det vil betyde, at der skal ansættes ca. 200 nye medarbejdere til at håndtere målrettet logning (ved en pris for et årsværk på ca. en mio. kr. inkl. løn og overhead). Dertil kommer betydelige it-mæssige implementeringsomkostninger for dele af det offentlige til håndtering af målrettet logning

Dansk Erhverv og IT-Branchen bemærker, 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.

Det bemærkes endvidere, at der i processen ikke har været afsat tilstrækkelig tid til konsolidering af erhvervslivets omkostninger, der i lovforslaget er angivet til 206 mio. kr. Den foreslåede lov indeholder som tidligere påpeget mange elementer, der ikke indgik i vurdering af virksomhedernes administrative byrder. Omstillingsomkostningerne vil blive væsentligt højere end de angivne 206 mio. kr, hvorfor der om et minimum foretages en ny byrdevurdering i lyset af det samlede forslag med henblik på en kompensationsordning for selskaberne

Vi står naturligvis til rådighed, hvis der er spørgsmål til høringssvaret.

Med venlig hilsen

Poul Noer, fagchef for telepolitik, Dansk Erhverv

Mette Lundberg, direktør politik og kommunikation, IT-Branchen

Mediernes Hus
Kalkbrænderiløbskaj 4
2100 København Ø

+45 33 97 40 00
info@danskemedier.dk
www.danskemedier.dk

Danske Medier

Justitsministeriet
Sikkerhedskontor II
Slotsholmsgade 10
1216 København K

Sendt elektronisk til jm@jm.dk, hlm@jm.dk, nat@jm.dk

25. oktober 2021

Høringssvar vedr. revision af reglerne om registrering og opbevaring af oplysninger om teletrafik (logning m.v.)

Danske Medier har med tak modtaget Justitsministeriets høringsbrev af 27. september 2021 med opfordring til at fremkomme med bemærkninger til udkastet til forslag om ændring af retsplejeloven og lov om elektroniske kommunikationsnet og -tjenester.

Danske Medier finder det positivt, at regeringen nu tager skridt til at revidere de danske logningsregler som følge af flere afgørelser fra EU-Domstolen, der har fastslået, at EU's logningsdirektiv, som de gældende danske regler bygger på, er ugyldigt, og at EU-retten ikke tillader national lovgivning, der foreskriver en generel og udifferentieret logning af samtlige trafik- og lokaliseringsdata.

Foreningen har ikke kommentarer til det overordnede spørgsmål om logning, men 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 i medfør af retsplejelovens regler om indgreb i meddelelseshemmeligheden.

Danske Medier har flere gange i forbindelse med de gentagne udskydelser af revisionen af logningsreglerne understreget vigtigheden af, at eventuelle indgreb i meddelelseshemmeligheden ikke må udgøre en risiko for mediernes muligheder for at beskytte deres kilder. Kildebeskyttelsen - og dermed i yderste konsekvens pressens funktion som offentlighedens kontrol- og informationsorgan - kan således kompromitteres, såfremt der kan ske kortlægning af, hvor en journalist har befundet sig, og hvem journalisten har været i kontakt med. Der henvises til Europarådets Rekommandation R (2000) 7 og princip nr. 6 i bilaget til rekommandationen.

Omfattende mulighed for registrering og opbevaring af trafikdata

Den foreslåede revision af logningsreglerne, der fortsat giver en ganske omfattende mulighed for at registrere og opbevare trafikdata, fjerner desværre ikke 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 § 172.

Foreningen har noteret, at der i udkastets § 786 d, stk. 4, gives mulighed for en hurtig efterprøvelse fra rettens side, såfremt der er tilfælde, hvor særlige principielle hensyn kan siges at gøre sig gældende, fx 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.

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.

Manglende beskyttelse af kildebeskyttelsen ved politiets adgang til loggede oplysninger

Udover den ovennævnte og i øvrigt indirekte henvisning til de principielle hensyn, der kan gøre sig gældende i forhold til logning af trafikdata fra kommunikationsapparater, der anvendes af advokater, læger og journalister, er det 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 om kildebeskyttelse i kapitel 71 om indgreb i meddelelseshemmeligheden, der skal inddrages ved spørgsmål om udlevering af oplysninger, der er registrerings- og opbevaringspligtige efter udkastets §§ 786 a- 786 e.

Foreningen skal i den anledning i øvrigt henlede opmærksomheden på, at retsplejelovens kapitel 73 og 74 allerede indeholder henvisninger til § 172 i bestemmelserne om ransagning, beslaglæggelse og edition, og at det derfor er helt naturligt, at kapitel 71 om indgreb i meddelelseshemmeligheden ligeledes udtrykkeligt afspejler dette afgørende hensyn.

Danske Medier står naturligvis til rådighed, såfremt ovenstående ønskes uddybet. Henvendelse herom kan rettes til undertegnede på telefon 3397 4000 eller mail cm@danskemedier.dk.

Venlig hilsen
Danske Medier

Christina Mary Moshøj
Seniorkonsulent, cand. jur.

Høring over udkast af 27/9 2021 til lovforslag om revision af logningsreglerne

Indhold

Justitia | Fruebjergvej 3 | 2100 København Ø | 23926100 | info@justitia-int.org

Indledning

I det følgende fremgår Justitias bemærkninger til udvalgte dele af Justitsministeriets udkast af 27. september 2021 til 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.) (herefter benævnt "lovudkastet").

Justitia har kun forholdt sig til de dele af lovudkastet, der udtrykkeligt behandles i høringssvaret. Manglende omtale af dele af lovudkastet og bestemmelserne heri kan således ikke i sig selv ses som udtryk for, at Justitia er enig i disse.

Overordnede bemærkninger til lovudkastet

De danske logningsregler har – som minimum – siden 2016 været i strid med EU-retten.[1] Her fastslog EU-Domstolen, at nationale regler som de danske, der foreskriver generel og udifferentieret logning, er ulovlige og bl.a. strider mod privatlivets fred.[2] I 2020 udtalte EU-Domstolen, at der undtagelsesvis og midlertidigt kan ske generel og udifferentieret logning, hvis et land står overfor en alvorlig trussel mod den nationale sikkerhed, der er reel og aktuel eller forudsigelig.[3] I øvrige tilfælde kan der ske målrettet logning til bekæmpelse af som minimum grov kriminalitet.[4] For en nærmere gennemgang af de nuværende logningsregler i lyset af EU-Domstolens praksis henvises til Justitias analyse "Ulovlig logning – tid til en lovrevision".[5]

Justitia finder det positivt, at Justitsministeriet nu er i gang med den nødvendige lovrevision af logningsreglerne. Lovudkastet giver dog på en række punkter 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.

Denne risiko er navnlig en konsekvens af de foreslåede rammer for vurderingen af, om der foreligger en trussel, der kan legitimere generel og udifferentieret logning, sammenholdt med den del af

[1] EU-Domstolens dom (Store Afdeling) af 8/4 2014 i de forenede sager C-293/12 og C-594/12 (Digital Rights-dommen), EU-Domstolens dom (Store Afdeling) af 21/12 2016 i de forenede sager C-203/15 og C-698/15 (Tele2-dommen) og EU-Domstolens Dom (Store Afdeling) af 6/10 2020 i de forenede sager C-511/18, C-512/18 og C-520/18 (La Quadrature-dommen)
[2] Tele2-dommen
[3] La Quadrature-dommen, præmis 134-139
[4] La Quadrature-dommen, præmis 146-147
[5] Tilgængelig her

Justitia | Fruebjergvej 3 | 2100 København Ø | 23926100 | info@justitia-int.org

forslaget, hvorefter der kan gives adgang til disse loggede data til brug for bekæmpelse af grov kriminalitet.

Dertil kommer, at særligt rammerne for den foreslåede målrettede geografiske logning forekommer så vide, at der de facto vil blive tale om generel logning. Med andre ord synes kriterierne for målrettet geografisk logning at medføre, at så store dele af landet underlægges logning, at logningen ikke længere kan anses målrettet.

Når Justitsministeriet endda derudover 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,[6] forekommer der reelt at være tale om en de facto udvidelse af den nuværende (ulovlige) logningsordning.

Justitia finder i øvrigt ikke, at lovudkastet indeholder fornødne prøvelses- og kontrolforanstaltninger.

Samlet set forekommer ovenstående svært problematisk i lyset af EU-Domstolens praksis. Ifølge Justitias vurdering vil vedtagelse af den foreslåede løsning 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"[7] og med samtidig henvisning til, at reglerne vil kunne anvendes i hele perioden frem til en eventuel dom ved EU-Domstolen.[8] Der lægges hermed op til (endnu) en lang årrække med logning, hvis lovlighed er tvivlsom.

Bemærkninger til forslagene vedrørende generel og udifferentieret logning

EU-retten er som udgangspunkt til hinder for generel og udifferentieret logning.[9] Dog kan der *undtagelsesvis* og *midlertidigt* ske en sådan form for logning, hvis et land står overfor en alvorlig trussel mod den nationale sikkerhed, der er reel og aktuel eller forudsigelig.[10]

I lovudkastet foreslås det at indføre en ny bestemmelse i retsplejeloven (§ 786e), hvorefter justitsministeren efter forhandling med erhvervsministeren kan fastsætte regler om generel og udifferentieret logning, 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.[11]

[6] I henhold til reglerne om indgreb i meddelelseshemmeligheden, jf. RPL § 781, stk. 1, nr. 3
[7] S. 106 i lovudkastet
[8] S. 86 i lovudkastet
[9] Digital Rights-dommen (C-293/12 og C-594/12), præmis 69-71, Tele2-dommen (C-203/15 og C-698/15), præmis 103-107 og La Quadrature-dommen, præmis 117-119 og 141
[10] La Quadrature-dommen, præmis 134-139
[11] Lovudkastets § 1, nr. 9, indsættelse af § 786 e

Justitia | Fruebjergvej 3 | 2100 København Ø | 23926100 | info@justitia-int.org

Vurdering af om der foreligger en trussel der kan legitimere generel og udifferentieret logning

EU-Domstolens praksis foreskriver, at der kun må logges generelt og udifferentieret i en begrænset periode,[12] hvorved tidsperioden desuden skal begrænses til det strengt nødvendige,[13] og at denne form for logning aldrig må blive hovedreglen[14] eller antage systematisk karakter.[15] Vurderingen skal være baseret på konkrete omstændigheder,[16] og der skal være tale om en reel og aktuel eller forudsigelig trussel.[17] Domstolens praksis må på den baggrund forstås sådan, at der er tale om et ekstraordinært tiltag reserveret til ekstraordinære situationer.

I lovudkastet forudsættes det, at vurderingen af, om der foreligger en tilstrækkelig trussel til at kunne iværksætte generel og udifferentieret logning, skal bero på antallet og karakteren af verserende og/eller afgjorte sager om straffelovens kap. 12 og 13, Center for Terroranalyses (CTA) årlige terrortrusselsvurdering (VTD) samt øvrige relevante analyseprodukter. CTA's terrortrusselsvurdering er ifølge Justitsministeriet tilstrækkelig dynamisk til, at vurderingen ikke vil få systematisk karakter.[18]

Justitia hæfter sig ved, at det i lovudkastet er formuleret således, at CTA's vurdering kan indgå som *et element (af flere)* i vurderingen.[19] Ifølge Justitias vurdering er det afgørende, at CTA's klassificering af, at terrortruslen er "alvorlig", ikke bør kunne stå alene som grundlag for at iværksætte generel og udifferentieret logning. CTA har vurderet trusselsniveauet "alvorligt" hvert år siden 2014.[20] Der er således tale om et generelt trusselsbillede, der har gjort sig gældende i som minimum 7 år, og som ikke kan antages at ændre sig foreløbigt.

Iværksættelse af generel og udifferentieret logning på baggrund af CTA's klassificering alene vil derfor ikke overholde kravet om, at generel og udifferentieret logning skal være et tidsbegrænset tiltag reserveret til ekstraordinære situationer. Tværtimod vil dette medføre, at generel og udifferentieret logning bliver hovedreglen, pålægges for en ikke-begrænset periode samt antager systematisk karakter. Dette er i direkte strid med EU-Domstolens praksis som gennemgået netop ovenfor.

Ifølge Justitia må vurderingen foretages på baggrund af konkrete, dokumenterbare omstændigheder, der gør trusselsantagelsen reel og aktuel eller forudsigelig. Dette kunne f.eks. være

[12] La Quadrature-dommen, præmis 137
[13] La Quadrature-dommen, præmis 138
[14] La Quadrature-dommen, præmis 111
[15] La Quadrature-dommen, præmis 138
[16] La Quadrature-dommen, præmis 137
[17] La Quadrature-dommen, præmis 137
[18] S. 55 ff. i lovudkastet
[19] S. 55-56 i lovudkastet
[20] Publikationer (pet.dk)

Justitia | Fruebjergvej 3 | 2100 København Ø | 23926100 | info@justitia-int.org

tilfældet, hvis PET på baggrund af efterretninger får en reel mistanke om, at et ekstremistisk netværk er i færd med at planlægge et konkretiseret og nært forestående terrorangreb i Danmark.

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 fremfor "bredere tendensanalyser og vurderinger af fænomener".[21]

For så vidt angår sager om straffelovens kap. 12 og 13 bemærker Justitia, at det er afgørende at have for øje, at truslen skal være "reel og aktuel eller forudsigelig". Der bør derfor udvises varsomhed i forhold til at lægge vægt på navnlig allerede afgjorte sager om straffelovens kap. 12 og 13, der som udgangspunkt må antages i højere grad at belyse bagudrettede forhold.

Kompetence til at iværksætte generel og udifferentieret logning

I henhold til den foreslåede § 786 e, stk. 1, er det justitsministeren, der bemyndiges til at vurdere, om der er grundlag for at iværksætte generel og udifferentieret logning samt til at fastsætte reglerne herom. Dog fastsættes reglerne efter forhandling med erhvervsministeren.

Justitia ønsker at bemærke, at generel og udifferentieret logning er særligt omfattende og dermed indgribende, og den juridiske vurdering af, om betingelserne for at pålægge en sådan logningsordning er opfyldt, kan risikere at blive politiseret.

Om end det er positivt, at det ikke er justitsministeren alene, der i lovudkastet 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.

En anden – og formentlig bedre – mulig løsning, kunne være at oprette en uafhængig særenhed, hvis medlemmer skal være med til at foretage vurderingen. Udpegelsen af enhedens medlemmer bør i så fald ske på et formelt set mere uafhængigt grundlag end udpegelsen af tilsynet med efterretningstjenesterne.[22] Således bør det ikke være justitsministeren – der også er ansvarlig for politiet/PETs virksomhed – som har kompetence til at vælge medlemmerne, idet der i så fald ville ske en unødig sammenblanding af interesser. Medlemmerne bør i stedet vælges af Folketinget, i lighed med Folketingets Ombudsmand.

I begge tilfælde kan der indføres regler om, hvorvidt der blandt de personer, der foretager vurderingen af truslen, kræves fuld enighed eller et bestemt antal stemmer for, at en ordning om generel og udifferentieret logning kan initieres. Disse regler bør sikre, at den endelige vurdering i

[21] Som beskrevet på s. 56 i lovudkastet
[22] PET-lovens § 16

alle tilfælde vil fremstå objektiv. Det vil således ikke være tilfredsstillende, hvis der f.eks. gives justitsministeren vetoret.

Desuden vil det være fordelagtigt at underlægge vurderingen af, om der foreligger en tilstrækkelig trussel, parlamentarisk kontrol.

I alle tilfælde er det afgørende, at dem der er involveret i vurderingen, skal have tilgang til alt materiale og alle oplysninger, der er af betydning for vurderingen. Der kan i den forbindelse drages inspiration fra Tilsynet med Efterretningstjenesterne, som i medfør af PET-lovens § 20 har adgang til alle oplysninger, der har betydning for tilsynets virksomhed.

For at yde tilstrækkelige retssikkerhedsmæssige garantier i forbindelse med vurderingen af, om betingelserne er opfyldt, bør en sådan ordning desuden kun kunne iværksættes efter rettens kendelse. Et krav om kendelse 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.

Tidsmæssig udstrækning af påbud om generel og udifferentieret logning

Ifølge EU-retten skal et påbud om generel og udifferentieret logning skal tidsmæssigt begrænses til det strengt nødvendige.[23] Desuden må varigheden af et påbud om logning ikke overstige et forudseeligt tidsrum.[24]

I henhold til den foreslåede § 786 e, stk. 2, kan regler om generel og udifferentieret logning fastsættes for en periode på op til 1 år ad gangen.

Efter Justitias opfattelse går en periode på 1 år, når denne periode anvendes som udgangspunktet, væsentligt ud over det strengt nødvendige.

Justitia har bemærket, at det fremgår af lovudkastets almindelige bemærkninger, at reglerne om generel og udifferentieret logning ophæves, hvis der opstår grundlag for at antage, at reglerne ikke længere kan opretholdes.[25] Rammerne omkring denne vurdering konkretiseres imidlertid ikke nærmere, herunder hvem der har ansvar for at foretage vurderingen og hvor ofte den foretages.

[23] La Quadrature-dommen, præmis 138
[24] La Quadrature-dommen, præmis 138
[25] Lovudkastets s. 59

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. Herved sikres det, at reglerne rent faktisk kun opretholdes, så længe der består et grundlag for opretholdelsen. Hver forlængelse á 14 dage bør afgøres ved kendelse.

Adgang til oplysninger der er logget generelt og udifferentieret

Af lovudkastet fremgår det, at Justitsministeriet vurderer, at EU-Domstolens praksis ikke er til hinder for, at medlemsstaterne kan give politi og anklagemyndighed adgang til trafik- og lokaliseringsdata, der er logget med henblik på at beskytte den nationale sikkerhed, i de tilfælde, hvor politi og anklagemyndighed bekæmper grov kriminalitet.[26]

I lovudkastet lægges der således op til, at reglerne om adgang til loggede oplysninger kan indrettes sådan, at der kan gives adgang til oplysninger til brug for et formål, der er mindre tungtvejende end det, oplysningerne oprindeligt blev logget af hensyn til.

Justitia er ikke enig i Justitsministeriets tolkning af dommen på dette punkt. Justitia er opmærksom på, at Justitsministeriet selv har angivet, at ministeriets læsning af præmis 166 i La Quadrature-dommen sker under "en væsentlig procesrisiko", [27] hvilket i sig selv forekommer bemærkelsesværdigt.

Ifølge Justitias vurdering vil den foreslåede løsning imidlertid ikke blot udgøre en væsentlig procesrisiko, men vil være i direkte strid med EU-Domstolens praksis. Vedtagelse af den foreslåede løsning vil således indebære en ikke uvæsentlig risiko for, at Danmark vil blive dømt ved en eventuel sag for EU-Domstolen.

Præmis 166 lyder således:

> *"Det skal desuden tilføjes, således som det navnlig fremgår af denne doms præmis 115 og 133, at adgangen til de trafikdata og lokaliseringsdata, som udbyderne lagrer som følge af en foranstaltning, der er vedtaget i henhold til artikel 15, stk. 1, i direktiv 2002/58, i princippet kun kan begrundes i det mål af almen interesse, med henblik på hvilket disse udbydere er blevet pålagt at foretage denne lagring. Det følger navnlig heraf, at der under ingen omstændigheder kan gives adgang til sådanne data med henblik på at retsforfølge og straffe en almindelig strafbar handling, når lagringen heraf er begrundet i formålet om bekæmpelse af grov kriminalitet eller a fortiori i formålet om beskyttelse af den nationale sikkerhed. I overensstemmelse med proportionalitetsprincippet, således som dette er blevet præciseret i denne doms*

[26] Pkt. 3.7.2 i lovudkastet
[27] S. 106 i lovudkastet

> *præmis 131, kan en adgang til data, der er lagret med henblik på bekæmpelse af grov kriminalitet, under forudsætning af, at de i den foregående præmis nævnte materielle og proceduremæssige betingelser, der gælder for at opnå en sådan adgang, overholdes, til gengæld begrundes i formålet om beskyttelse af den nationale sikkerhed."* (Justitias fremhævning)

Justitsministeriets tolkning bygger på, at der i præmissen ikke "eksplicit" tages stilling til, om hensynet til at efterforske og retsforfølge grov kriminalitet vil kunne begrunde, at politi og anklagemyndighed kan få adgang til lagrede trafik- og lokaliseringsdata, der er lagret med henblik på at beskytte den nationale sikkerhed.[28]

Desuden henviser Justitsministeriet til, at der i præmis 166 henvises til proportionalitetsprincippet i dommens præmis 131 samt at dommens præmis 131 henviser til præmis 55 i Ministerio Fiscal-dommen, og ministeriet anfører på den baggrund:[29]

> *"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 den nyligt afsagte H.K.-dom[30] gentager EU-Domstolen præmis 166 fra La Quadrature-dommen:

> *"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*

[28] S. 105 i lovudkastet
[29] S. 105-106 i lovudkastet
[30] Sag C-746/18

Justitia | Fruebjergvej 3 | 2100 København Ø | 23926100 | info@justitia-int.org

> *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)."* (Justitias fremhævning)

Justitsministeriet fremhæver dog også H.K.-dommens præmis 33:[31]

> *"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 og 146)."* (Justitsministeriets fremhævning i fed. Justitias fremhævning understreget)

Som det fremgår af ovenstående bygger ræsonnementet i lovudkastet dels på, at EU-Domstolen i præmis 166 i La Quadrature-Dommen henviser til præmis 131 i samme dom, som henviser tilbage til præmis 55 i Ministerio Fiscal-dommen.

Præmis 55 i Ministerio Fiscal-dommen omhandler spørgsmålet om, hvorvidt der kan gives adgang til en helt anden form for data, end den her omhandlede, nemlig data med henblik på at identificere indehavere af SIM-kort (brugeridentitetsoplysninger). Ministerio Fiscal-dommen omhandler udelukkende spørgsmålet om adgang til persondata, og ikke spørgsmålet om hvordan og hvorvidt disse logges (dvs. målrettet eller generelt og udifferentieret). I præmis 55 og de omkringliggende præmisser forklarer EU-Domstolen, at der lovligt kan gives adgang til oplysninger af hensyn til bekæmpelse af kriminalitet i almindelighed, hvis adgangen til den pågældende type oplysninger ikke udgør et alvorligt indgreb. Der kan med andre ord gives adgang til brugeridentitetsoplysninger vedrørende SIM-kort i videre omfang end til trafik- og lokaliseringsdata, fordi adgang til sådanne oplysninger ikke udgør et lige så alvorligt et indgreb.

Justitia har svært ved at følge Justitsministeriets ræsonnement om, at præmis 55 i Ministerio Fiscal-dommen understøtter ministeriets fortolkning af EU-Domstolens retspraksis vedrørende det her omhandlede spørgsmål.

Når EU-Domstolen i La Quadrature-dommens præmis 166 henviser til dommens præmis 131, er der for det første blot tale om en generel henvisning til proportionalitetsprincippet (jf. ordlyden i præmis

[31] S. 107-108 i lovudkastet

166, "*I overensstemmelse med proportionalitetsprincippet, således som dette er blevet præciseret i denne doms præmis 131*"). Justitia er ikke enig i, at en generel henvisning til proportionalitetsprincippet kan fortolkes således, at EU-Domstolen har haft til hensigt at svække selve ordlyden i præmis 166, der i sig selv fremstår klar. For så vidt angår præmis 55 i Ministerio Fiscal-dommen, der udgør en sekundær henvisning, indgår denne præmis i en helt anden sammenhæng både faktuelt og juridisk, som synes svær at sammenligne med det her omhandlede spørgsmål.

Det er desuden værd at bemærke, at henvisningen til præmis 131 end ikke sker i sammenhæng med spørgsmålet om, hvorvidt der kan gives adgang til data, der er logget til et mindre tungtvejende formål, end det formål, som den ønskede adgang er begrundet i. Tværtimod sker henvisningen til præmis 131 i forbindelse med spørgsmålet om, hvorvidt der kan gives adgang til data, der er logget til et *mere* tungtvejende formål end det formål, som den ønskede adgang er begrundet i (dvs. f.eks. adgang til data til brug for bekæmpelse af terrorisme, når dataene oprindeligt er blevet logget til bekæmpelse af menneskehandel, hvilket er tilladt). Endelig omfatter præmis 166s henvisning til præmis 131 ikke "den deri nævnte praksis", hvilket EU-Domstolen ellers har for vane eksplicit at nævne, når henvisningen til en anden præmis også omfatter den øvrige praksis, der nævnes i præmissen.[32] Henvisningen til præmis 131 kan således end ikke antages også at omfatte en henvisning til præmis 55 i Ministerio Fiscal-dommen.

Justitia mener ikke, at præmis 166 i La Quadrature-dommen, som bekræftes i H.K.-dommen, kan læses på anden måde, end at der ikke må gives adgang til data under hensyn til forfølgelsen af et mål, der er mindre tungtvejende end det mål, dataene oprindeligt blev logget til. Således må der ifølge Justitias vurdering ikke kunne gives adgang til data til brug for bekæmpelse af grov kriminalitet, hvis de pågældende data er opnået via en logningsordning, der er iværksat af hensyn til beskyttelse af den nationale sikkerhed. Dette følger direkte af ordlyden af præmis 166 (se Justitias fremhævning i den citerede præmis ovenfor).

Justitsministeriets ræsonnement bygger ligeledes på præmis 33 i H.K.-dommen. Justitia er opmærksom på, at der kan argumenteres for, at præmis 33 i H.K.-dommen kan læses sådan, at adgang til data til brug for bekæmpelse af grov kriminalitet ikke er udelukket, selvom dataene er logget via en generel og udifferentieret logningsordning. Det er dog ikke dét spørgsmål, som EU-Domstolen reelt behandler eller forholder sig til i præmis 33. Spørgsmålet der behandles, er afgrænsningen af *grov* kriminalitet overfor kriminalitet *i almindelighed*, herunder hvilke former for data, der kan gives adgang til, når formålet med adgangen alene er kriminalitet i almindelighed. Det er derfor også mere nærliggende at læse præmissen sådan, at den egentlige pointe er, at når det gælder trafik- og lokaliseringsdata, vil minimumskravet altid være bekæmpelse af *som minimum* grov kriminalitet/beskyttelse af den offentlige sikkerhed, hvorefter en målrettet logningsordning af trafik- og lokaliseringsdata aldrig kan retfærdiggøre bekæmpelse af kriminalitet i almindelighed. Dette underbygges af, at præmis 33 i H.K.-dommen henviser til præmis 140 og 146 i La Quadrature-

[32] Se f.eks. La Qaudrature-dommens præmis 165, 175, 176 og 188

dommen, som netop tilsvarende omhandler spørgsmålet om afgrænsningen mellem data, der kan begrunde bekæmpelse af kriminalitet i almindelighed overfor data, der kun kan begrunde bekæmpelse af som minimum grov kriminalitet.

Modsat fremgår det utvetydigt af præmis 31 i H.K.-dommen, at "*Hvad angår de formål, der kan begrunde de offentlige myndigheders adgang til de data, […], 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*". I præmissen henvises der desuden til præmis 166 i La Quadrature-dommen, hvor det som nævnt utvetydig fremgår, at "*adgangen til […] trafikdata og lokaliseringsdata, […] i princippet kun kan begrundes i det mål af almen interesse, med henblik på hvilket disse udbydere er blevet pålagt at foretage denne lagring*". At EU-Domstolen skriver "i princippet" må antages at være knyttet til betragtningen senere i præmis 166 om, at der dog – pga. proportionalitetsprincippet – godt kan gives adgang til data, når formålet med adgangen er *mere* tungtvejende end det formål, som dataene oprindeligt blev logget af hensyn til. Dette understøttes yderligere af, at H.K.-dommens præmis 31 ikke indeholder dette forbehold.

Adgang til data, der er logget med henblik på at beskytte den nationale sikkerhed, når formålet med adgangen er bekæmpelse af grov kriminalitet, vil i øvrigt forekomme som en omgåelse af kravet om, at der kun må ske målrettet logning til bekæmpelse af grov kriminalitet mv.

Når hensynet til bekæmpelse af grov kriminalitet ikke kan begrunde generel og udifferentieret logning, må det samme hensyn så meget desto mindre kunne begrunde selve adgangen til oplysninger, der er lagret på baggrund af generel og udifferentieret logning. En sådan adgang ville gøre kravet vedr. målrettet logning illusorisk og som minimum arbitrært. Således ville der i forlængelse heraf skabes usikkerhed og inkonsistens i retstilstanden, hvis omfanget af data, som politiet har tilgang til i en sag om f.eks. grov narkokriminalitet, afhang af den nationale terrortrussel.

Samlet set må spørgsmålet således skulle afgøres i henhold til EU-Domstolens ganske tydelige formuleringer om spørgsmålet i både La Quadrature-dommens præmis 166 og H.K.-dommens præmis 31, hvorimod diverse præmis-henvisninger til Domstolens formuleringer om andre retlige spørgsmål ikke kan tages til indtægt for, at der åbnes op for en sådan omgåelse, der ville stride mod hele grundtanken i den begrænsning, som EU-Domstolen har fastslået.

Effektiv prøvelse af generel og udifferentieret logning

Ifølge EU-retten skal en afgørelse om, at der skal logges generelt og udifferentieret, kunne gøres til genstand for effektiv prøvelse med henblik på at kontrollere, om betingelserne for logning er opfyldt.[33]

Det fremgår af lovudkastet, at gyldigheden af regler om generel og udifferentieret logning vil kunne prøves i henhold til den almindelige adgang til domstolsprøvelse efter GRL § 63. Det fremgår i den

[33] La Quadrature-dommen, præmis 139

forbindelse af lovudkastet, at grundlaget for vurderingen af, at der kan indføres generel og udifferentieret logning, offentliggøres ved reglernes udstedelse.[34]

Det forudsættes imidlertid i lovudkastet, at de bagvedliggende klassificerede oplysninger, der ligger til grund for de analyseprodukter, der er anvendt i vurderingen, ikke udleveres til brug for en retssag. Det vil derimod være allerede offentliggjorte analyseprodukter og offentlige oplysninger om straffesager, der kan indgå i domstolenes vurdering.[35]

Justitia er enig i, at grundlaget for vurderingen af, at der kan indføres generel og udifferentieret logning, bør offentliggøres ved reglernes udstedelse. 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 evt. retssag, giver imidlertid 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. Umiddelbart forekommer denne løsning derfor ikke at opfylde kravene til effektiv prøvelse.

Justitia er samtidig opmærksom på, at saglige hensyn gør sig gældende i forbindelse med klassificeringen af det relevante materiale. 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., hvor der bl.a. beskikkes en særlig advokat, der får tilgang til det relevante materiale,[36] og hvor visse dele af domstolsbehandlingen foregår for lukkede døre.[37] Mht. beskikkelse af en særlig advokat kan der ligeledes med inspiration fra denne ordning antages et antal advokater, der står til rådighed til formålet, og som således også kan underlægges særlige sikkerhedsmæssige procedurer.[38]

Det bemærkes derudover, at domstolsprøvelsen giver anledning til at overveje spørgsmål vedrørende retlig interesse.

Som det fremgår ovenfor anbefaler Justitia i øvrigt, at et påbud om generel og udifferentieret logning i alle tilfælde vil kræve kendelse. Dette vil medføre øget retssikkerhed i ethvert tilfælde, hvor en sådan logning påtænkes.

[34] S. 60 i lovudkastet
[35] S. 84 i lovudkastet
[36] Udlændingelovens § 45e
[37] Udlændingelovens § 45g
[38] Udlændingelovens § 45j

Justitia | Fruebjergvej 3 | 2100 København Ø | 23926100 | info@justitia-int.org

I tillæg til domstolsprøvelse kan der med fordel gives Datatilsynet og Tilsynet med Efterretningstjenesterne eksplicit hjemmel til at foretage legalitetskontrol af beslutninger om generel og udifferentieret logning.

Bemærkninger til forslagene vedrørende målrettet logning

EU-retten tillader målrettet logning af trafik- og lokaliseringsdata i det omfang det sker til bekæmpelse af grov kriminalitet, alvorlige trusler mod den offentlige sikkerhed eller trusler mod den nationale sikkerhed (herefter benævnt "grov kriminalitet").[39] Der må derimod ikke ske logning af disse data til brug for bekæmpelse af kriminalitet i almindelighed.[40]

For så vidt angår den i lovudkastet foreslåede definition af "grov kriminalitet" henvises der til det særskilte afsnit herom nedenfor.

Geografisk målrettet logning (lovudkastets § 1, nr. 9, indsættelse af ny § 786c)

Den målrettede logningsordning skal begrænses til det strengt nødvendige for så vidt angår de berørte personer. Denne afgrænsning kan dels ske som en geografisk afgrænsning, idet en sådan målretning vil reducere antallet af berørte personer.[41]

EU-Domstolen har fastslået, at der kan ske afgrænsning ud fra et geografisk kriterium, når der i et eller flere områder er identificeret en forhøjet risiko for planlægning eller udførelse af grov kriminalitet. Domstolen nævner som eksempler: *"steder eller infrastrukturer, der regelmæssigt besøges af et meget stort antal personer, eller strategiske steder, såsom lufthavne, banegårde eller vejafgiftsområder"*. Vurderingen skal foretages på grundlag af objektive og ikke-diskriminerende forhold.[42]

I lovudkastet foreslås det, at der iværksættes logning i områder, hvor der er et højere antal anmeldelser eller domfældelser for grov kriminalitet. Logningspligten træder i kraft, når antallet af anmeldelser/domfældelser i et område udgør mindst 1,5 gange landsgennemsnittet. De geografiske områder der underlægges logning skal i henhold til lovudkastet udgøre 3x3 km.[43]

Desuden foreslås det i lovudkastet, at der iværksættes logning i områder, der er særligt sikringskritiske. Som eksempler nævnes kongehusets residenser, Christiansborg Slot, statsministerboligen Marienborg, ambassader, politiets ejendomme, kriminalforsorgens institutioner, bro-, tunnel- og færgeforbindelser, trafikknudepunkter og større indfaldsveje,

[39] La Quadrature-dommen, præmis 146-147
[40] La Quadrature-dommen, præmis 140
[41] La Quadrature-dommen, præmis 150
[42] La Quadrature-dommen, præmis 150
[43] Lovudkastets § 1, nr. 9 (indsættelse af ny § 786c, stk. 1, nr. 1 og 2)

Justitia | Fruebjergvej 3 | 2100 København Ø | 23926100 | info@justitia-int.org

grænseovergange, busterminaler, fjernbanestationer, stationer på bybaner, militære områder, kolonne 3-virksomheder og offentligt godkendte flyvepladser.[44]

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.[45]

Konkret begrundet målrettet logning (lovudkastets § 1, nr. 9, indsættelse af ny § 786d)

I lovudkastet foreslås det, at politiet gives mulighed for at meddele konkret begrundede pålæg om logning, når der "er grund til at antage", at kommunikationsapparater, personer eller geografiske områder har forbindelse til grov kriminalitet.[46] Pålæg sker ved retskendelse.[47] Tidsrummet for logningen fastsættes i kendelsen og skal være så kort som muligt, men må ikke overstige 6 måneder. Tidsrummet kan imidlertid forlænges, dog højst 6 måneder ad gangen.[48]

Kravet om, at der skal være "grund til at antage", at der eksisterer en forbindelse, indebærer i henhold til lovudkastet, at kravet er lavere end det, der gælder for at foretage telefonaflytning.[49] Der kan derfor i henhold til lovudkastet bl.a. meddeles pålæg, når politiet har grund til at antage, at der er en forbindelse til planlægning af grov kriminalitet.[50]

Som eksempler nævnes i lovudkastet bl.a. personer, der har været i kontakt med personer, der er eller har været genstand for et tvangsindgreb i retsplejelovens kapitel 70-75 på baggrund af grov kriminalitet og personer med nære relationer til personer, der har forbindelse til grov kriminalitet, som f.eks. ægtefæller eller samlevere.[51]

Justitia er for så vidt enig i, at det kan være legitimt at iværksætte logning overfor 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 en gang 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.

[44] Lovudkastets § 1, nr. 9 (indsættelse af ny § 786c, stk. 2)
[45] La Quadrature-dommen, præmis 111
[46] Lovudkastets § 1, nr. 9 (indsættelse af ny § 786d, stk. 1)
[47] Lovudkastets § 1, nr. 9 (indsættelse af ny § 786d, stk. 2)
[48] Lovudkastets § 1, nr. 9 (indsættelse af ny § 786d, stk. 2)
[49] Telefonaflytning i medfør af RPL § 781, stk. 1, nr. 1
[50] S. 42 i lovudkastet
[51] S. 42-43

Justitia | Fruebjergvej 3 | 2100 København Ø | 23926100 | info@justitia-int.org

Effektiv prøvelse af målrettet logning

Prøvelse af målrettet logning i medfør af lovudkastets §§ 786b-c

Det fremgår af lovudkastet, at gyldigheden af de regler om målrettet logning, der er baseret på klare og objektive kriterier, vil kunne prøves i henhold til den almindelige adgang til domstolsprøvelse efter GRL § 63. Det beskrives i lovudkastet, at kendetegnet ved disse logningsregler er, at det er objektivt konstaterbart, hvornår der logges.[52] Som en følge af, at det er objektivt konstaterbart, hvornår der logges, er der i henhold til lovudkastet heller ikke behov for at foretage underretning af de personer, der berøres af denne form for logning.[53]

Justitia forstår lovudkastet således, at ovenstående betragtninger gør sig gældende ved målrettet personbestemt logning i medfør af den foreslåede § 786b samt målrettet geografisk logning i medfør af den foreslåede § 786c.[54]

I det omfang det rent faktisk er objektivt konstaterbart ved en ren læsning af loven, herunder for den berørte, hvornår der logges, har Justitia ikke bemærkninger til, at prøvelse blot kan ske i henhold til den almindelige adgang til domstolsprøvelse uden videre regulering. Justitia hæfter sig dog ved, at det ikke er alle former for målrettet logning i medfør af ovennævnte bestemmelser, hvor dette er tilfældet.

Særligt hæfter Justitia sig ved, at det fremgår af lovudkastet, at oversigten over de områder, der i henhold til den foreslåede § 786c, stk. 1 (områder med et større antal anmeldelser om og domfældelser for grov kriminalitet) og stk. 2 (særligt sikringskritiske områder) underlægges målrettet geografisk logning, ikke vil blive offentliggjort.[55] For disse typer af målrettet logning gælder det således, at personer i de berørte områder ikke vil have kendskab til, at deres oplysninger logges, hvorved der i det konkrete tilfælde ikke består en reel mulighed for at få efterprøvet den målrettede geografiske logning.

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

[52] S. 81 i lovudkastet
[53] S. 82 i lovudkastet
[54] S. 81-82 i lovudkastet
[55] S. 48-49 i lovudkastet

Justitia | Fruebjergvej 3 | 2100 København Ø | 23926100 | info@justitia-int.org

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.[56] I den forbindelse er det væsentligt, at afgrænsningen af de særligt sikringskritiske områder,[57] nødvendiggør en skønsmæssig vurdering.[58]

Den samlede oplistning af, hvad der kan udgøre særligt sikringskritiske områder, forekommer at kunne omfatte særdeles store dele af landet. Som eksempler på mulige særligt sikringskritiske områder nævnes bl.a. en række motorveje, trafikerede ringveje, større indfaldsveje, stationer samt tunnel-, færge og broforbindelser.[59]

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. Ifølge Justitias opfattelse bør en sådan vurdering underlægges yderligere kontrol, såvel forudgående som efterfølgende.

Bemærkninger til den foreslåede definition af "grov kriminalitet"

Som nævnt ovenfor tillader EU-retten målrettet logning af trafik- og lokaliseringsdata i det omfang det sker til bekæmpelse af grov kriminalitet, alvorlige trusler mod den offentlige sikkerhed eller trusler mod den nationale sikkerhed ("grov kriminalitet mv.").[60] Der må derimod ikke ske logning af eller gives adgang til disse data til brug for bekæmpelse af kriminalitet i almindelighed.[61]

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 (RPL § 781, stk. 1, nr. 3).

Det nugældende kriminalitetskrav i RPL § 781, stk. 1, nr. 3 indebærer, at der som udgangspunkt skal være tale om en lovovertrædelse med en strafferamme på minimum 6 år, før der kan gøres indgreb i meddelelseshemmeligheden.

[56] S. 171 i lovudkastet
[57] I henhold til den foreslåede § 786, stk. 2
[58] Dette er også forudsat i lovudkastet, hvor det fremgår, at iværksættelse af sådan logning vil kræve, at der vurderes at være særlige beskyttelseshensyn, der kan begrunde, at området anses særligt sikringskritisk, jf. s. 168 i lovudkastet
[59] S. 169 i lovudkastet
[60] La Quadrature-dommen, præmis 146-147
[61] La Quadrature-dommen, præmis 140 og 166

Justitia | Fruebjergvej 3 | 2100 København Ø | 23926100 | info@justitia-int.org

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.[62]

Justitia er opmærksom på, at EU-retten ikke indeholder nærmere krav til definitionen af grov kriminalitet, herunder grænsedragningen over for kriminalitet i almindelighed. Justitia finder det imidlertid 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.[63] 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.

Med venlig hilsen

Jacob Mchangama
Direktør

JUSTITIA
Mobil/Cell +45 24 66 42 20
E-mail: jacob@justitia-int.org
http://www.justitia-int.org

Helene Qvist Petersen
Advokat

JUSTITIA
E-mail: helene@justitia-int.org
http://www.justitia-int.org

[62] Lovudkastets § 1, nr. 2 (indsættelse af ny § 781a) og § 1, nr. 9 (indsættelse af ny §§ 786b, 786c og 786d)
[63] Lovudkastets § 1, nr. 9 (indsættelse af ny § 786b, stk. 2 nr. 1 og stk. 3)

Til

Justitsministeriet

(Deres j.nr. 2020-1870036)

HORESTA takker for muligheden for at afgive høringssvar vedr. ovennævnte lovforslag.

Lovforslaget indeholder forslag om, at udbydere – med et kommercielt formål – på en række områder tilpligtes at foretage målrettet (personbestemt, geografisk mv.) logning af en række oplysninger. HORESTA noterer med tilfredshed, at hoteller, restaurant, cafeer mv., som tilbyder gæsterne internetadgang ikke er omfattet af disse foreslåede forpligtelser, idet disse ikke anses for at have et kommercielt formål med f.eks. at udbyde internetadgang, idet tilbuddet om internetadgang alene er en accessorisk ydelse knyttet til hovedydelsen.

Hoteller, Restauranter og andre turismevirksomheder anses således for så vidt angår de foreslåede regler om mere omfattende målrettet logning ikke for at være udbydere

Hoteller, restauranter og andre turismevirksomheder er dog fortsat, bortset fra altså i tilknytning til de nu foreslåede regler om målrettet logning, at anse for udbydere mere generelt, jf. logningsbekendtgørelsen, herunder i forhold til de oplysninger, som fortsat skal logges efter logningsbekendtgørelsens § 5, stk. 2.
I 2014 reviderede man logningsreglerne således, at udbydere af internetadgang, f.eks. et hotel, som giver sine gæster adgang til internettet, fra den foreslåede ikrafttrædelsesdato, den 22. juni 2014, ikke længere skulle logge og gemme oplysninger om, hvilke internetsider brugere/gæster har besøgt – den såkaldte sessionslogning.

Derimod fastholdt man reglerne i bekendtgørelsens nuværende § 5, stk. 2, hvorefter en udbyder fortsat skal registrere følgende oplysninger:

1) den tildelte brugeridentitet,
2) den brugeridentitet og det telefonnummer, som er tildelt kommunikationer, der indgår i et offentligt elektronisk kommunikationsnet,
3) navn og adresse på den abonnent eller registrerede bruger, til hvem en internetprotokol-adresse, en brugeridentitet eller et telefonnummer var tildelt på kommunikationstidspunktet og
4) tidspunktet for kommunikationens start og afslutning.

Det var positivt, at man afskaffede reglerne om sessionslogning, men det var - og er fortsat - uklart, hvorfor reglerne i § 5, stk. 2, som alene er formelle oplysninger om brugerne, blev fastholdt, når reglerne om i 5, stk. 1, blev ophævet. Det er således uklart, hvad de oplysninger, som gemmes efter § 5, stk. 2, kan og skal bruges til.

Med fastholdelsen af, at udbyderen fortsat skal gemme de oplysninger, som fremgår af bekendtgørelsens § 5, stk. 2, tog man ikke hele skridtet. Hoteller og andre udbyderen skal fortsat fastholde - og betale for – et teknisk set up, som kan registrere og gemme de oplysninger, der fremgår af § 5, stk. 2.

Det er – og har hele tiden været – HORESTA's opfattelse, at logningsreglerne således afstedkommer en betydelig belastning for vore medlemmer, som grundlæggende ikke står mål med i hvilket omfang myndighederne anvender logningsoplysningerne i deres arbejde.

Yderligere er der det aspekt, at logningsreglerne har været (er) "hullede som en si", derved at f.eks. offentlige biblioteker, skoler mv. 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, så udover, at der også her er et "hul", så er der også tale om konkurrenceforvridning, idet sommerhusudlejning og privat udlejning via f.eks. Airbnb ikke pålægges de samme forpligtelser og administrative byrder og udgifter, som traditionelle overnatningsvirksomheder gør.

HORESTA opfordrede i forbindelse med ophævelse af sessionslogningen til, at også bestemmelsen i bekendtgørelsens § 5, stk. 2, blev ophævet, denne opfordring skal hermed gentages. Alternativt skal det foreslås, at hoteller, restauranter og andre turismevirksomheder helt udeholdes fra logningsbekendtgørelsens udbyderbegreb.

Med venlig hilsen

Kaare Friis Petersen
Erhvervsjuridisk chef

HORESTA

Vodroffsvej 32 • DK-1900 Frederiksberg C • T +45 35 24 80 80 • D +45 35 24 80 04 • M +45 22 11 88 47 • www.horesta.dk

IT-Politisk Forening

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

25. oktober 2021

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Oversigt over IT-Politisk Forenings høringssvar

Udbydere omfattet lovforslaget

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

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

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

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

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

Afgrænsning af de logningspligtige oplysninger

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

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

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

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

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

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

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

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

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

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

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

---

2 Denne problemstilling er velkendt under de nuværende logningsregler.

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

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

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

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

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

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

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

4 LQDN-dommen præmis 136.

varetægtsfængslinger og tiltalerejsning har en bagudrettet karakter.

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

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

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

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

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

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

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

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

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

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

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

Domstolskontrol af påbud om logning til beskyttelse af den nationale sikkerhed

28. Efter præmis 139 i LQDN-dommen er det væsentligt, at et påbud (afgørelse) om lagring kan gøres til genstand for en effektiv prøvelse ved en domstol eller en uafhængig administrativ myndighed, der træffer bindende afgørelser med henblik på at kontrollere, om der foreligger en alvorlig trussel mod den nationale sikkerhed, samt om de retsgarantier, der skal være fastsat ved lov, er overholdt.

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

30. Kontrollen behøver ikke være henlagt til de almindelige danske domstole. Det kunne også være et særligt kontrolorgan, hvor medlemmerne eksempelvis er udpeget blandt erfarne dommere fra landsretterne med den nødvendige sikkerhedsgodkendelse for at kunne behandle fortrolige efterretninger. Det afgørende er, at denne myndighed kan udøve kontrollen af påbud om logning i fuldstændig uafhængighed af regeringen, og at kontrollen får et reelt indhold (herunder en uafhængig vurdering af, om der foreligger en ekstraordinær situation, som berettiger dette meget vidtgående indgreb).

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

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

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

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

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

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

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

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

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

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

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

39. Ifølge Tele2-dommen (forenede sager C-203/15 og C-698/15) af 21. december 2016 er EU-retten til hinder for en generel og udifferentieret lagringspligt af samtlige trafikdata og lokaliseringsdata vedrørende samtlige abonnenter med henblik på bekæmpelse af kriminalitet. Dette gentages i LQDN-dommen med præmis 141-142.

40. Når EU-Domstolen med LQDN-dommen i ekstraordinære situationer tillader generel og udifferentieret logning med henblik på at beskytte den nationale sikkerhed mod alvorlige trusler, må det være underforstået at logning til national sikkerhed skal holdes adskilt fra logning til kriminalitetsbekæmpelse. I modsat fald vil den beskyttelse af grundlæggende rettigheder, som Tele2-dommen sikrer, blive undergravet. **En formålsbegrænsning for en lagringspligt har kun en reel virkning, hvis myndighedernes adgang til de lagrede oplysninger er underlagt den samme formålsbegrænsning.**

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

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

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

44. Ud fra disse overvejelser vurderer Justitsministeriet, at LQDN-dommen ikke er til hinder for at politiet i sager om grov kriminalitet kan få adgang til oplysninger, som er lagret med henblik på at beskytte den nationale sikkerhed. Lovforslaget omtaler dog i pkt. 3.7.2 og pkt. 10 (forholdet til EU-retten) en **væsentlig procesrisiko** ved denne fortolkning i lyset af præmis 166 i LQDN-dommen.

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

46. Præmis 33 i Prokuratuur-dommen forholder sig alene til kriminalitetsbekæmpelse, og det

sker konkret i forhold til en sag, hvor det estiske politi fik adgang til lagrede trafikdata og lokaliseringsdata uden at der var tale om grov kriminalitet. Præmis 33 gentager EU-Domstolens retspraksis, om at der i forhold til bekæmpelse af ikke-grov kriminalitet slet ikke kan fastsættes en lagringspligt for trafikdata og lokaliseringsoplysninger, hverken målrettet eller generel og udifferentieret. Det må endvidere skulle læses i sammenhæng med præmis 29, hvor EU-Domstolen udtaler at "en sådan adgang kun kan gives, for så vidt som disse data er blevet lagret af disse udbydere på en måde, der er i overensstemmelse med den nævnte artikel 15, stk. 1" [i e-databeskyttelsesdirektivet]. I det estiske sag er både lagringen og den efterfølgende adgang i strid med EU-retten, fordi lagringspligten er generel og udifferentieret til kriminalitetsbekæmpelse, og den estiske lovgivning tillader adgang til lagrede trafikdata og lokaliseringsdata i sager om ikke-grov kriminalitet.

Risikoen for sagsophobning i straffesagskæden

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

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

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

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

Målrettet logning (§§ 786 b – 786 d)

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

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

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

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

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

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

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

57. For den personbestemte målrettede logning er det IT-Politisk Forenings klare opfattelse, at LQDN-dommens præmis 149 indebærer, at der på grundlag af objektive forhold skal foretages **en konkret vurdering af de personer, som udpeges til målrettet logning**. Kravene til grundlaget for denne vurdering skal naturligvis være lavere end kravene til mistankegrundlaget for at de loggede oplysninger efterfølgende kan udleveres til politiet. En målrettet logning mod en person bør eksempelvis kunne igangsættes på grundlag af efterretningsmæssige vurderinger uden at der nødvendigvis er en efterforskning rettet mod

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

personen.

58. Den målrettede logning skal have karakter af undtagelsen, jf. EU-Domstolens fortolkning af e-databeskyttelsesdirektivets artikel 15, stk. 1 i Tele2-dommens præmis 104. Lagring af trafikdata og lokaliseringsdata må således ikke blive hovedreglen. Det sætter en naturlig begrænsning på hvor mange personer, der kan være omfattet af en personbestemt målrettet logning, og hvor store geografiske områder der kan indgå i den målrettede logning ud fra geografiske kriterier.

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

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

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

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

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

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

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

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

Retsgarantier og transparens for målrettet logning

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

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

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

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

---

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

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

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

71. Efter IT-Politisk Forenings opfattelse forudsætter en reel udøvelse af adgangen til effektive retsmidler for en domstol, at **de berørte personer får underretning om den målrettede logning, når denne underretning ikke længere kan skade en igangværende efterforskning.** EU-Domstolen har fremhævet underretning af de berørte personer som en *de facto* nødvendighed i en række domme, eksempelvis præmis 220 i sagen A-1/15 om EU-Canada PNR-aftalen.[11] Det bør også gælde for den personbestemte målrettede logning i den foreslåede § 786 d i retsplejeloven, hvor der er forudgående domstolskontrol. Den beskikkede advokat vil ikke være i besiddelse af alle relevante oplysninger, således at adgangen til effektive retsmidler kan udøves fuldt ud for den berørte person.

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

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

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

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

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

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

kriminalitet.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Politiets adgang til oplysninger om slutbrugers internetadgang (edition)

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

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

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

92. Som EU-Domstolen anfører i præmis 155 i LQDN-dommen har internetbrugerne en forventning om, at deres identitet ikke afsløres, når de søger information på internettet. Den Europæiske Menneskerettighedsdomstol (EMD) henviser ligeledes til forventningen om "anonymitet" online som en vigtig faktor i præmis 117 i dommen af 24. april 2018 i sagen Benedik v. Slovenia, sagsnr. 62357/14, i overensstemmelse med tidligere EMD retspraksis.

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

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

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

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

14 Som nævnt tidligere afslører den tildelte IP-adresse ikke i sig selv noget om brugerens kommunikation på internettet. En sådan afsløring finder imidlertid sted, i hvert fald delvist, når politiet anmoder om oplysninger om en brugers identitet ud fra en IP-adresse, fordi denne anmodning altid vil have en direkte forbindelse til en konkret kommunikation på internettet (eksempelvis besøg på en bestemt hjemmeside eller ytringer på en social medie platform).

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

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

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

97. Den tildelte IP-adresse kan ikke i sig selv afsløre hvilke internetsteder, som abonnenten har frekventeret, eller hvilke personer der er kommunikeret med. Det samme gør sig i princippet gældende for registrering af portnumre. Efter IT-Politisk Forenings opfattelse er registrering af portnumre ved CG-NAT dog mere betænkelig, fordi hyppigheden af registreringer af portnumre i visse situationer kan tegne et præcist billede af abonnentens vaner og adfærdsmønstre for så vidt angår brugen af internettet og eventuelt ophold i hjemmet, når der er tale om registrering for faste internetforbindelser.[16]

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

Hastesikring (§ 786 a)

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

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

Politiets adgang til de lagrede oplysninger (overordnede bemærkninger)

107. Vedrørende spørgsmålet om politiets adgang til oplysninger lagret med henblik på beskyttelse af den nationale sikkerhed har IT-Politisk Forening anført sine bemærkninger under punkt 38-46 ovenfor. Bemærkningerne nedenfor i punkt 108-160 gælder således alene i forhold til adgang begrundet i kriminalitetsbekæmpelse.

108. Politiets adgang til lagrede oplysninger indebærer et indgreb i de rettigheder, som er sikret af e-databeskyttelsesdirektivets 2002/58/EF, navnlig artikel 5, 6 og 9 i dette direktiv.[20] Adgangen til lagrede oplysninger skal derfor ske i henhold til en lovgivningsmæssig foranstaltning, der opfylder kravene i artikel 15, stk. 1 i e-databeskyttelsesdirektivet. Det gælder uanset om oplysninger er lagret i henhold til en logningspligt eller af kommercielle årsager, jf. præmis 167 i LQDN-dommen.[21]

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

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

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

21 Det er i LQDN-dommens præmis 167 en forudsætning for politiets adgang, at oplysningerne er lagret på en måde, som er i overensstemmelse med artikel 5, 6, 9 (kommercielle årsager) eller artikel 15, stk. 1 (lagringspligt fastsat ved lov). Herved må skulle forstås, at lagringen skal være lovlig for at oplysningerne lovligt kan udleveres til politiet. Denne fortolkning bekræftes af præmis 29 i Prokuratuur-dommen ("..at en sådan adgang kun kan gives, for så vidt som disse data er blevet lagret af disse udbydere på en måde, der er i overensstemmelse med den nævnte artikel 15, stk. 1.")

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

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

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

113. De pågældende trafikdata og lokaliseringsdata gør det muligt at drage præcise slutninger vedrørende privatlivet for de personer, hvis data er blevet lagret, såsom vaner i dagligdagen, midlertidige eller varige opholdssteder, daglige eller andre rejser, hvilke aktiviteter der udøves, disse personers sociale relationer og de sociale miljøer, de frekventerer.[22] Det understreger den følsomme karakter af disse data, og at adgang til oplysningerne udgør et alvorlig indgreb.

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

115. Politiets adgang til trafikdata og lokaliseringsdata skal ske efter forudgående domstolskontrol undtagen i behørigt begrundede hastende tilfælde. Den nationale lovgivning skal fastsætte materielle og processuelle betingelser for denne adgang. Hvis der er tale om et alvorligt indgreb (altså de fleste sager om adgang til trafikdata og lokaliseringsdata), er det ikke tilstrækkeligt at begrænse adgangen til sager om grov kriminalitet, jf. præmis 118 i Tele2-dommen. Der skal være materielle og processuelle betingelser, som i hvert enkelt tilfælde sikrer, at adgangen begrænses til hvad der er strengt nødvendigt for den konkrete efterforskning, jf. præmis 38 i Prokuratuur-dommen. Det kan indebære begrænsninger for kategorier af data og varigheden af den periode, for hvilken der anmodes om adgang.

22 Jf. eksempelvis præmis 36 i Prokuratuur-dommen.

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

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

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

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

Adgang til teleoplysninger (retsplejelovens kapitel 71)

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

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

23 Af fodnote 3 i "Notat af 2. juni 2014 om betydningen af EU-Domstolens dom af 8. april 2014 i de forenede sager C-293/12 og C-594/12 (om logningsdirektivet) for de danske logningsregler" fremgår det, at Justitsministeriet er opmærksom på den manglende overensstemmelse mellem retsplejelovens editionsregler og EU-retten i forhold til politiets adgang til visse loggede oplysninger.

24 Oplysninger om hvem der kommunikerer med hvem.

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

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

122. De danske bestemmelser om teleoplysning[26] bør generelt opfylde kravene i EU-Domstolens retspraksis for politiets adgang til trafikdata og lokaliseringsdata, dog med en enkelt mulig undtagelse. Ifølge præmis 119 i Tele2-dommen kan der som udgangspunkt "kun gives adgang til data vedrørende personer, der er mistænkt for at planlægge, ville begå eller have begået en alvorlig lovovertrædelse eller på en eller anden måde være involveret i en sådan lovovertrædelse."

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

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

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

Adgang til registreringspligtige oplysninger efter editionsreglerne (§ 804 a)

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

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

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

indgrebets afslutning skal ske underretning af de berørte personer.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Adgang til ikke-registreringspligtige trafikdata og lokaliseringsdata efter editionsreglerne

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

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

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

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

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

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

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

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

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

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

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

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

indgreb.

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

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

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

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

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

154. Ifølge præmis 119 i Tele2-dommen kan der som udgangspunkt kun gives adgang til data vedrørende personer, der er mistænkt for at planlægge, ville begå eller have begået en alvorlig lovovertrædelse eller på en eller anden måde være involveret i en sådan lovovertrædelse. I særlige situationer, såsom de situationer, hvor vitale interesser for den nationale sikkerhed, forsvaret eller den offentlige sikkerhed er truet af terrorvirksomhed, kan der også gives adgang til andre personers data, hvis der foreligger objektive forhold som gør det mulige at antage, at disse data kan bidrage til bekæmpelsen af en sådan virksomhed.

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

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

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

33 Jf. U.2017.1934Ø.

”udvidet masteoplysning”.[34]

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

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

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

Underretning af den registrerede, når oplysninger udleveres til politiet

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

175. På side 12 i "Notat af 2. juni 2014 om betydningen af EU-Domstolens dom af 8. april 2014 i de forenede sager C-293/12 og C-594/12 (om logningsdirektivet) for de danske logningsregler" anføres dette af Justitsministeriet:

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

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

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

Statistikker for politiets adgang til trafikdata og lokaliseringsdata

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

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

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

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

Immuniteter og privilegier (forholdet til tavshedspligt)

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

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

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

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

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

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

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

Registrering og verificering af nummeroplysningsdata (118-databasen)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Registrering af taletidskort

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

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

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

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

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

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

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

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

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

Konsekvenser for borgerne af registrering af taletidskort

205. For de personer, som bliver berørt af krav om registrering, vil ulemperne imidlertid være de samme som tidligere. Personer som har behov for anonym kommunikation, eksempelvis en whistleblower hos en efterretningstjeneste som vil kontakte en journalist om ulovlig masseovervågning af befolkningen, kan ikke længere bare købe en "burner phone" (en billig GSM-telefon og taletidskort, som smides væk efter et enkelt opkald) for at beskytte sig mod riskoen for de repressalier, som en sådan afsløre vil kunne medføre.[40]

206. Krav om køberregistrering af taletidskort kan medføre, at nogle personer (eksempelvis særligt udsatte grupper som hjemløse) vil blive afskåret fra at gøre brug af mobiltelefoni, fordi de ikke kan levere den dokumention for deres identitet, som køberregistreringen kræver. En del taletidskort sælges via kiosker, og hvis disse salgssteder fremover skal

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

opbevare kopier af ID-dokumenter eller andre registreringer baseret på fremvisning af ID-dokumenter, vil der blive skabt nye risici for identitetstyveri. Online-registrering med NemID er ikke en mulighed for alle, eksempelvis personer som kun opholder sig midlertidigt i Danmark. Det er heller ikke alle fastboende borgere som har NemID.

207. I et notat af 29. april 2021 med bemærkninger til lovskitsen for revision af logningsreglerne af 23. marts 2021 opfordrede IT-Politisk Forening til, at Justitsministeriet udarbejdede en grundig konsekvensanalyse af disse aspekter, herunder en menneskeretlig vurdering af risikoen for at visse udsatte persongrupper kan blive helt afskåret fra at kommunikere med andre mennesker via mobiltelefoni, inden et lovforslag med registrering af taletidskort blev fremsat.

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

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

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

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

Justitsministeriet
Sikkerhedskontor II

Dato 25. oktober, 2021

Høringssvar vedrørende:

Høring over udkast til 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 (log-
ning) m.v.) dateret 27. september, 2021.

På vegne af Citizen First (under etablering som en non-profit NGO med fokus på digital repræsentation af borgerne) har Priway følgende kommentarer:

1. Udgangspunktet er dårlige infrastruktur standarder i telesektoren (f.eks. 5G, NemID/MitID og EMV betalinger), som hverken sikrer borgerne eller systemerne ligesom cyberkriminelle har lette vilkår til at tracke ofre, målrette angreb og lave f.eks. identitetstyveri.

Det har ført til en situation, hvor den kommercielle infrastruktur a priori udfører invasiv overvågning som så udnyttes både kommercielt, kriminelt og af staten medmindre andre strukturer eksplicit sikrer mod dette.

Hvorvidt staten OGSÅ pålægger overvågning og hvorledes offentlige myndigheder tilgår sådanne sensitive person- og systemdata ændrer i princippet ikke på den grundlæggende problemstilling - man lovgiver om en forværring af en allerede dårlig sikkerhedsstruktur.

Hele lovforslaget forfalder derfor reelt til en ”pest eller kolera” diskussion af proportionaliteten mellem mere overvågning og den kriminalitets-bekæmpende hensigt.

Vi er sikre på at andre vil bruge kræfter på at diskutere om de konkrete aspekter og vælger ikke at tage yderligere stilling hertil, idet vi betragter den diskussion som ufrugtbar.

2. Vi konstaterer dog at lovforslaget reelt forsøger at gøre sikkerhed umuligt ved at PÅLÆGGE teleinfrastrukturen at strippe og blokere alle sikkerhedsmekanismer på vegne af borgeren og organisationer med henblik på at tilsikre en invasiv overvågning.

Det betyder at ingen borgere kan gå sikkert på nettet inkl. f.eks. Forsvarets personale, Rigspolitiet, politikere, forsvarsadvokater, journalister, forskere.

Her overser man en væsentlig pointe – hvor man aldrig vil kunne overtale kriminelle til selv at inkriminere sig, så har den almindelige borgere og legale personer en stærk egeninteresse i bedre sikkerhed, som man reelt blokerer og dermed forværrer.

Vores forslag er derfor at man i loven indbygger eksplicit understøttelse af FRIVILLIGT SELV-INKRIMINERENDE SIKKERHEDSSTRUKTURER SOM IKKE KAN OVERVÅGES, dvs. en godkendelsesmodel til at undgå logning, fordi de hensyn overfor en dommer som varetages af logningsbekendtgørelsen er tilgodeset på anden vis.

Hvad indebærer det? F.eks. at en militærperson kan gå på nettet og bevise overfor infrastrukturen at sessionen er legitim og sikkerhedsmæssigt valideret i forhold til formålet uden at hverken device eller borgeren kan identificeres i nettet.

Konkret kan det f.eks. ske ved 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.

I tilknytning hertil at vedkommende kan stilles til ansvar og/eller overvåges i forhold til det formål, som sessionen vedrører.

På den måde kan en borger f.eks. bidrage til en reelt anonym sundhedsforskning i en sammenhæng og stå til ansvar og med en dommerhandling overvåges på de sociale net, hvis de konkrete betingelser er til stede.

Hvordan det konkret verificeres og specifikke krav hertil kan overlades til en certificerings/godkendelsesproces, mens selve loven kan være teknologi-neutral med fokus på de reelle behov.

På den måde opnås 3 kritiske forhold på samme tid:

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 samfundsprocesser vil forebygge kriminalitet og ansvar vil være nemmere at etablere.

c) Det betyder at de kriminelle får stadigt sværere ved at gemme sig, fordi det bliver nemmere og mere acceptabelt at fokusere på restgruppen. Hvis lovlydige borgere kan beskytte sig mod overvågning fjerner man et af hovedargumenterne mod logning som sådan.

Med henvisning til GDPR er teknologiens aktuelle stade sådan at sådanne strukturer snart bliver almindelige og dermed lovpligtige indenfor EU. Det bliver en hovedopgave for Citizen First at stille sådanne strukturer til rådighed for alle borgere på non-profit basis som en del af opgraderingen af cybersecurity.

På vegne af Citizen First

Stephan Engberg
Priway ApS

Ingeniørforeningen, IDA
Kalvebod Brygge 31-33
DK-1780 København V
Tlf. +45 33 18 48 48

ida.dk

Justitsministeriet
Sikkerhedskontor II
Slotsholmsgade 10
1216 København K
jm@jm.dk

hlm@jm.dk / nat@jm.dk.

Høring over udkast til lovforslag 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.)

25. oktober 2021

Høringssvar fra Ingeniørforeningen, IDA
IDA takker for muligheden for at svare på høring over udkast til lovforslag 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.)

Lovforslaget indeholder bemærkelsesværdigt mange elementer med forskelligt niveau af præcision. IDA svarer på nogle af disse elementer. At der er delelementer, vi ikke berører i høringssvaret, er ikke nødvendigvis ensbetydende med, at vi er positivt indstillet.

Generelle bemærkninger

IDA værdsætter, at logningsbekendtgørelsen endelig forsøges revideret.

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, der hører under EU-rettens generelle principper og grundlæggende rettigheder, som er sikret i EU's charter om grundlæggende rettigheder, nærmere bestemt:
Artikel 7, hvoraf det følger, at enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin kommunikation. Samme rettigheder er sikret i Den Europæiske Menneskerettighedskonventions artikel 8.
Artikel 8, hvoraf enhver har ret til beskyttelse af personoplysninger, der vedrører den pågældende.

Artikel 11, der sikrer individets ret til ytringsfrihed, hvilket også omfatter retten til meningsfrihed og frihed til at modtage eller meddele oplysninger eller tanker uden indblanding fra offentlig myndighed og uden hensyn til landegrænser. Samme rettigheder er sikret i Den Europæiske Menneskerettighedskonventions artikel 10.

IDA kan derfor ikke bakke op om lovforslaget.

IDA bemærker desuden, på baggrund af udmeldinger fra Justitsministeriet[1], at forslaget til ændringer i den nuværende praksis ikke sker af hensyn til borgernes rettigheder, men fordi "vi skal" og at det er Justitsministeriets tydelige ønske at fortsætte den generelle og udifferentierede logning af alle borgere i videst muligt omfang.

IDA finder det uacceptabelt, at Justitsministeriet ikke arbejder for at sikre danske borgeres grundlæggende rettigheder, men tværtimod holder fast i en tvivlsom praksis og, efter eget udsagn jf. kapitel 10 i høringsmaterialet, løber en "væsentlig procesrisiko" i forhold til EU-Domstolens afgørelser.

Specifikke kommentarer til lovforslaget.
Opsamling på kommentarer til lovforslaget. Kommentarerne uddybes i det følgende.

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

IDA finder det særdeles problematisk at sænke strafframmen til tre år, idet logning som skrevet er et alvorligt indgreb i den enkeltes ret til privatliv.

Det er IDAs holdning, at hvis geografisk målrettet logning skal foregå, så 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 og for en kort, afgrænset tidsperiode. Alternativt bør geografisk målrettet logning droppes som en mulighed.

IDA finder det nødvendigt, at det tydeligt fremgår af loven, hvem der defineres som "nærkontakt".

[1] https://www.justitsministeriet.dk/pressemeddelelse/justitsministeren-vil-med-nyt-lovforslag-om-logning-sikre-saa-effektiv-kriminalitetsbekaempelse-som-muligt/

IDA finder det it-sikkerhedsmæssigt kritisk og uforholdsmæssigt ressourcekrævende at skulle implementere et system som det foreslåede for taletidskort. Tilmed er der, iflg. høringsmaterialet, ingen garanti for, at det vil kunne forhindre eller mindske fortsat organiseret kriminalitet. IDA kan derfor ikke bakke op om forslaget, som det er beskrevet i høringsmaterialet.

IDA finder forslaget problematisk og et eksempel på, hvordan man på mange punkter er på vej fra en proportionelt afvejet lovgivning med respekt for borgernes grundlæggende rettigheder.

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 ikrafttrædelsen til et sikkert og gennemtestet system er på plads og at man i den mellemliggende periode stopper alle kritiserede former for logning.

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

IDA anbefaler Justitsministeriet at sætte en begivenhedsbestemt logning i stedet for den de facto permanente generelle og udifferentierede logning.

Lovforslaget indeholder to hovedpunkter. Et forslag til fortsat generel og udifferentieret logning og et forslag til målrettet registrering og opbevaring af teledata, i lovforslaget kaldet trafikdata:

IDAs holdning til fortsat generel og udifferentieret registrering og opbevaring af trafikdata

I forslagets § 786 e lægges op til, at justitsministeren efter forhandling med erhvervsministeren kan pålægge udbydere at foretage en 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."* 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*, at det *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,* jf. præmis 111, 137 og 138 i Quadrature du Net-dommen. Center for Terroranalyses Vurdering af terrortruslen i Danmark har siden 2014 været "alvorlig", og om end den tidligere har været lavere, er det tvivlsomt, at den skulle falde indenfor de næste år. Der er derfor ikke tale om "*en begrænset periode*, når der foreligger tilstrækkeligt konkrete omstændigheder" (Quadrature du Net, præmis 137). Der er snarere tale om, at dette er en ny normal tilstand, som vi ikke foreløbig kan se en ende på. Dette skal tages med i afvejningen af proportionalitetsprincippet. Vi kan ikke demokratisk holde til, at vi som borgere i en længere årrække lever uden, at de grundlæggende rettigheder som respekten for privatliv, beskyttelse af personoplysninger og retten til ytringsfrihed bliver holdt i hævd.

Dertil 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. I de seneste år er der tilmed sket en udvidelse af mulighederne for at bruge disse værktøjer. 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.

IDA finder det også problematisk, at det er justitsministeren i forhandling med erhvervsministeren, der kan forlænge et påbud om generel og udifferentieret logning med et år ad gangen. For det første er et år for lang tid til at kunne defineres som en "konkret omstændighed". 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 af for og imod. Alternativt kan der iværksættes generel udifferentieret logning i korte, afgrænsede tidsperioder som 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.

<u>IDAs holdning til målrettet registrering og opbevaring af trafikdata</u>

IDA er i princippet 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 overfor den måde, hvorpå målrettet person- 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 generelt er udtryk for et skred i opfattelsen af, hvornår logning af trafikdata skal bruges som middel.

Strafferammen bør ikke sænkes til tre år
I lovforslaget, jf. afsnit 3.1.3.1, lægges der op til, at strafferammen skal sænkes fra de i dag gældende seks år til tre år. Grundlaget for at bruge logning af trafikdata er bekæmpelse af grov kriminalitet. Grov kriminalitet har hidtil været i forståelsen minimum seks års strafferamme, men nu sænkes straframmen til tre år, hvilket udvider personkredsen, der kan falde indenfor målrettet logning betragteligt og dermed igen udvander argumentet for at gå på kompromis med borgernes grundlæggende rettigheder. IDA mener, at forslaget er udtryk for et skred, der udfordrer proportionalitetsprincippet.

IDA finder det særdeles problematisk at sænke straframmen til tre år, idet logning som sagt er et alvorligt indgreb i den enkeltes ret til privatliv. Dette foreslåede skred udfordrer proportionalitetsprincippet.

Forslag om logning i celler af 3 x 3 km er ikke teknisk overbevisende
I lovforslaget, jf. afsnit 3.1.3.2 lægges der op til, at den geografiske logning skal ske i celler af 3 x 3 km. IDA finder flere elementer i forslaget problematiske: Rigspolitiet har til Information (11.10.2021) oplyst, at disse celler af 3 x 3 km vil svare til 15-20 pct. af Danmarks samlede areal, hvilket svarer til hele Sjælland eller til ca. 3 mio. borgere. Rent teknisk er udfordringen, at man ikke kan logge indenfor et afgrænset område på 3 x 3 km, men at man for at dække 3 x 3 km, vil være nødt til at gøre brug af master, der samlet set vil række langt ud over dette område og dermed registrerer data på langt flere borgere end tiltænkt. En anden konsekvens af forslaget er, at en by som København med Christiansborg, Amalienborg, PET og FE hovedkvarterer, samt andre kritiske nøglepunkter som f.eks. Nørreport Station, vil komme under permanent og udifferentieret logning. Dette kan ikke forsvares og er på ingen måder i overensstemmelse med de eksempler Justitsministeriet selv beskrev i skitse for revision af logningsreglerne fra 29. april 2021. Her angav ministeriet angivet eksempler som

1. Bydele, hvor politiet har konstateret, at der statistisk set oftere begås grov kriminalitet end andre steder,
2. Områder, hvor der ligger "rockerborge" eller hashklubber mv.
3. Områder, hvor der aktuelt verserer bandekonflikt.

IDA mener, at der også her sker et skred mod generel og udifferentieret logning i forhold til de tidligere intentioner. Samtidig må en geografisk logning ikke ende med at blive en de facto permanent logning.

Det er IDAs holdning, at hvis geografisk målrettet logning skal foregå, så 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 og for en kort, afgrænset tidsperiode. Alternativt bør geografisk målrettet logning droppes som en mulighed.

Uklart, hvornår man er nærkontakt til mistænkte for grov kriminalitet
Det fremgår af lovforslaget, jf. afsnit 3.1.3.3., 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".

Registrering af taletidskort kan medføre ny kilde til misbrug
Der lægges i lovforslaget, jf. afsnit 3.4.2, op til, at der ved salg af uregistrerede taletidskort skal registreres og verificeres de samme nummeroplysningsdata for uregistrerede taletidskort som for andre abonnenter. Det vil kræve enten udlevering af CPR-nummer eller billedlegitimation, som f.eks. pas eller for udlændinge, et nationalt civilt identitetskort. Udbyderen skal hermed kontrollere om ID og den pågældende kunde er identiske. Det foreslås, at udbyderen også vil kunne kombinere billed-ID med et opslag i CPR. Kravet er herefter, at udbyderen f.eks. opbevarer en kopi af kundens billedlegitimation i deres system og at Energistyrelsen kan føre tilsyn med om udbyderne har dokumentation for at have foretaget verificering.
Konsekvensen af forslaget er dels, at der ikke længere vil kunne sælges uregistrerede taletidskort, hvilket vil være en hæmsko for f.eks. udlændinge, der opholder sig i Danmark i en længere periode i forbindelse med forskning eller erhvervsrejser, ligesom det vil kræve en særlig indsats i forhold til særligt sårbare grupper som hjemløse, der er afhængige af mobiltelefoner. Men forslaget, som det er fremlagt, vil også kunne medføre, at en række ikke nærmere definerede udbydere kommer til at have en lang række personfølsomme data liggende, f.eks. kopier af billedlegitimation som pas og som tilmed vil kunne få adgang til CPR-registret. Enten vil dette føre til et meget afgrænset antal udbydere og dermed gøre en helt almindelig service verden over til en yderst besværlig affære i Danmark, eller også vil det medføre nye højst sårbare systemer spredt udover kiosker og supermarkedet, som i sig selv vil kunne være mål for kriminelle handlinger. Samtidig er det i teksten til lovforslaget, s. 72, angivet, at "den foreslåede verificering

ikke kan udelukke alle tilfælde, hvor en slutbruger forsætligt afgiver oplysninger til udbyderen…der kan verificeres, men ikke er korrekte……f.eks. ved identitetstyveri."

IDA finder det it-sikkerhedsmæssigt kritisk og uforholdsmæssigt ressourcekrævende at skulle implementere et system som det foreslåede. Tilmed er der, iflg. høringsmaterialet, ingen garanti for, at det vil kunne forhindre eller mindske fortsat organiseret kriminalitet. IDA kan derfor ikke bakke op om forslaget, som det er beskrevet i høringsmaterialet.

Udlevering af yderligere oplysninger uden kendelse er uacceptabelt
Det foreslås, at der efter §804 indsættes en skærpet udgave af telelovens §13 med pligt til udlevering af yderligere oplysninger om slutbrugers adgang til det 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, ikke mindst set i lyset af, at det er tiltænkt en straframme på 3 år og ikke 6 år, som normalt er definitionen på grov kriminalitet. Denne del af forslaget er endnu et eksempel på det skred væk fra proportionalitetsprincippet og mangel på respekt for borgernes grundlæggende rettigheder, som lovforslaget i sin helhed er et udtryk for.

IDA finder forslaget problematisk og et eksempel på, hvordan man på mange punkter er på vej fra en proportionelt afvejet lovgivning med respekt for borgernes grundlæggende rettigheder.

En overgangsperiode med erkendt risiko for fejl er ikke acceptabelt
Ifølge lovforslaget, jf. §3, skal en revideret logningsbekendtgørelse træde i kraft allerede 1. januar 2022. En it-understøttelse til den del af lovforslaget, der vedrører målrettet person- og geografisk logning vil ikke være udviklet på dette tidspunkt, og der vil derfor være tale om en (relativt lang) overgangsperiode, hvor en sådan logning ville 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 nyt it-system, fordi det skal basere sig på ældre it-systemer 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 ikrafttrædelsen til et sikkert og gennemtestet system er på plads, og at man i den mellemliggende periode stopper alle former for logning.

Krav til et kommende system af registrering og opbevaring af trafikdata, logning.

IDA kan ikke støtte lovforslaget, som det ligger af en række ovenfor nævnte årsager. Hvis det lykkedes at finde et acceptabelt system, der kan fungere som værktøj for politiet, så foreslår IDA, at to yderligere elementer tages med:

Skærpet tilsyn med sletning af data

Da registrering og opbevaring af trafikdata udfordrer grundlæggende rettigheder i EU's charter for grundlæggende rettigheder som Artikel 7 om respekt for privatliv og familieliv, sit hjem og sin kommunikation, Artikel 8, om beskyttelse af personoplysninger og Artikel 11, der sikrer individets ret til ytringsfrihed, skal det sikres, at logningsdata slettes igen. Både hos udbyderne og hos politiet.

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 målrettet og evt. perioder med generel og udifferentieret logning.

IDA anbefaler begivenhedsbestemt logning

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 acceptabelt i et minimalt geografisk område og i en skarpt afgrænset periode som f.eks. 14 dage op til begivenheden og under selve begivenheden. Med mindre, 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 generelle og udifferentierede logning.

Opsamling

IDA anerkender forsøget med at etablere en målrettet person- og geografisk bestemt logning, men den foreslåede ordning er på ingen måde er tilnærmelsesvis

tilstrækkelig målrettet og der er både store tekniske, juridiske og økonomiske udfordringer.

IDA kan ikke acceptere, at den generelle og udifferentierede logning af alle danske borgere kan fortsætte, sådan som lovforslaget de facto lægger op til. Derfor bør hele afsnit 3.2 slettes og erstattes med situationsbestemt mulighed for logning.

Med venlig hilsen

Grit Munk	Helena Juul
Chefkonsulent, IDA	Chefkonsulent, IDA

INSTITUT FOR
MENNESKE
RETTIGHEDER

Justitsministeriet
Slotsholmsgade 10
1216 København K
E-mail: jm@jm.dk, hlm@jm.dk og nat@jm.dk

WILDERS PLADS 8K
1403 KØBENHAVN K
TELEFON 3269 8888
MOBIL 91325719
MIKL@HUMANRIGHTS.DK
MENNESKERET.DK

DOK. NR. 21/02860-2

25. OKTOBER 2021

HØRINGSSVAR OVER REVISION AF REGLERNE OM REGISTRERING OG OPBEVARING AF OPLYSNINGER OM TELETRAFIK (LOGNING) M.V.

Justitsministeriet har ved e-mail af 27. september 2021 anmodet om Institut for Menneskerettigheders eventuelle bemærkninger til udkast til forslag til lov om ændring af retsplejeloven og lov om elektroniske kommunikationsnet og -tjenester (Revision af reglerne om registrering og opbevaring af teletrafik (logning) m.v.).

Instituttet indleder med at sammenfatte sine væsentligste bemærkninger:

SAMMENFATNING

Med lovudkastet foreslår Justitsministeriet nye bestemmelser i retsplejeloven, som bl.a. skal regulere registrering og opbevaring af oplysninger om elektronisk kommunikation (logning) samt den senere adgang til sådanne oplysninger til brug for efterforskning og retsforfølgning.

I nærværende høringssvar begrænser instituttet sine bemærkninger om lovudkastet til følgende tre elementer:

1. Adgang til at fastsætte pligt til generel og udifferentieret logning til beskyttelse af national sikkerhed,
2. den efterfølgende adgang til oplysninger, som er logget til dette formål, og
3. målrettet geografisk logning.

Instituttet ønsker at bemærke, 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 således efter instituttets opfattelse ændres på flere områder for at være i overensstemmelse med EU-retten.

Tidsbegrænset generel og udifferentieret logning

I lovudkastet lægges der 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.

- Institut for Menneskerettigheder anbefaler, at Justitsministeriet sikrer, at adgangen til generel og udifferentieret logning til beskyttelse af national sikkerhed begrænses til ekstraordinære undtagelsessituationer.

Politiets adgang til loggede oplysninger

I lovudkastet lægger Justitsministeriet – under en væsentlig procesrisiko – op til, at politiet skal kunne få adgang til oplysninger, som er indsamlet som følge af generel og udifferentieret logning, i sager om efterforskning mv. 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.

- Institut for Menneskerettigheder anbefaler, at politiets adgang til oplysninger, som er indsamlet som følge af generel og udifferentieret logning, begrænses til sager vedrørende beskyttelse af national sikkerhed.

Målrettet geografisk logning

Ministeriet lægger med lovudkastet 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 § 1, nr. 9).

- Institut for Menneskerettigheder anbefaler, at Justitsministeriet i lovudkastet sikrer, at målrettet geografisk logning ikke får et omfang, som de facto må anses for generelt og udifferentieret.

INDLEDENDE OM LOGNING

Logning betyder, at det registreres, hver gang en borger ringer til nogen, sender en sms eller på anden måde gør brug af elektronisk kommunikation. Dermed gemmes data om, hvem man taler med eller sender beskeder til, hvor man er, samt hvornår og hvor længe man taler sammen.

Sådanne data gør det muligt at tegne et meget præcist billede af en borger på baggrund af for eksempel borgerens vaner i dagligdagen, midlertidige eller varige opholdssteder, rejser, aktiviteter og sociale

relationer. Oplysninger giver desuden indblik i, hvilke sociale miljøer borgeren færdes i. På baggrund af de indsamlede data kan der laves profiler af borgerne, som er lige så følsomme som selve indholdet af de opkald, beskeder og meddelelser, som logges.[1]

Myndighedernes adgang til at kræve, at teleudbydere/teleindustrien logger befolkningens teledata indebærer indgreb i borgerens ret til beskyttelse af privatliv, databeskyttelse og alt efter intensitet, beskyttelsen af ytrings- og informationsfrihed.

Generel og udifferentieret logning indebærer meget vidtrækkende indgreb i retten til respekt for privatliv og beskyttelse af personoplysninger, som følger af artikel 7 og 8 i EU's Charter om Grundlæggende Rettigheder.[2]

Med generel og udifferentieret menes en pligt til logning, som omfatter alle elektroniske kommunikationsmidler og samtlige trafikdata fra alle abonnenter og registrerede brugere, uden nogen begrænsning i den tidsmæssige periode for opbevaringen af oplysningerne og det geografiske område.[3]

EU-Domstolen har i lyset af dette fastslået, at myndighederne som det helt klare udgangspunkt ikke kan kræve "generel og udifferentieret logning" af befolkningen, da dette er i strid med EU-retten, herunder EU's Charter om Grundlæggende Rettigheder.[4]

Målrettet logning af bestemte personer eller grupper med henblik på kriminalitetsbekæmpelse er derimod efter omstændighederne muligt, hvis fornødne retsgarantier sikres.

Generelt kan man ud af EU-Domstolens praksis opdele logning i tre kategorier. Den mest alvorlige kategori vedrører logning for at bekæmpe kriminalitet af hensyn til den nationale sikkerhed. Der er tale om meget alvorlig kriminalitet, som derfor efter EU-Domstolens praksis i ekstraordinære undtagelsessituationer giver mulighed for at iværksætte generel og udifferentieret logning. Den næstmest alvorlige kategori handler om logning for at bekæmpe grov kriminalitet. Hensynet til at bekæmpe grov kriminalitet giver mulighed for at

---

[1] De forenede sager C-203/15 og C-698/15 (Tele2), præmis 99.
[2] De forenede sager C-203/15 og C-698/15 (Tele2), præmis 100.
[3] De forenede sager C-203/15 og C-698/15 (Tele2), præmis 105, og Eksponeret – Grænser for privatliv i en digital tid, Birgitte Kofod Olsen og Rikke Frank Jørgensen, Gads Forlag, 2018, side 65 og 69.
[4] De forenede sager C-203/15 og C-698/15 (Tele2), præmis 103.

fastsætte målrettet logning af alle typer af oplysninger. Endelig er der en sidste kategori, som handler om logning for at bekæmpe almindelig kriminalitet. Her må logning alene anvendes i forhold til en række begrænsede typer af oplysninger.

Det følger også af EU-Domstolens praksis, at oplysninger, som er logget til et bestemt formål, i princippet ikke senere må anvendes til et andet formål. Det vil sige, at hvis teleselskaberne har logget oplysninger af hensyn til den nationale sikkerhed, så må politiet ikke senere få adgang til oplysninger i en sag om grov kriminalitet. Eller hvis der er iværksat målrettet logning over for en person på grund af en mistanke om grov kriminalitet (f.eks. mistanke om organiseret bandekriminalitet), så må politiet ikke få adgang til oplysningerne i en sag, hvor de mistænker samme person for at have begået almindelig kriminalitet (f.eks. simpelt tyveri).

EU-Domstolen tillader dog, at oplysninger, som er logget for at bekæmpe grov kriminalitet, godt må anvendes i en sag, som handler om national sikkerhed (f.eks. terrorisme), fordi adgangen til oplysninger angår et formål, som er mere alvorligt end det formål, som oplysningerne blev indsamlet til.[5]

I Danmark har teleudbydere mv. siden 2007 været forpligtet til at foretage generel og udifferentieret logning, selvom dette har været i strid med EU-retten. Skiftende regeringer har desuden ad flere omgange udskudt den nødvendige revision af de danske regler, herunder med henblik på at sikre overholdelsen af EU-retten. Instituttet har kritiseret disse udskydelser gentagne gange.[6]

ADGANGEN TIL AT FORETAGE TIDSBEGRÆNSET GENEREL OG UDIFFERENTIERET LOGNING

I lovudkastet lægges der 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.

---

[5] De forenede sager C-511/18, C-512/18 og C-520/18 (La Quadrature du Net), præmis 166.

[6] Se instituttets høringssvar af 26. februar 2021 om udskydelsen af revisionsreglerne med henvisning til tidligere høringssvar: https://menneskeret.dk/sites/menneskeret.dk/files/media/document/H%C3%B8ringssvar%20vedr.%20udkast%20til%20lov%20om%20%C3%A6ndring%20af%20revisionsbestemmelse%20%28logning%29.pdf

Som nævnt er det klare udgangspunkt, 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.[7]

Adgangen til undtagelsesvis logning skyldes, at en trussel mod den nationale sikkerhed er så alvorlig, at det kan retfærdiggøre alvorlige indgreb i individets grundlæggende rettigheder. Sådanne alvorlige indgreb kan derimod ikke retfærdiggøres, hvis formålet er at bekæmpe grov kriminalitet mv.[8]

I lovudkastet lægges der op til, at der ved vurderingen af, om der foreligger en alvorlig trussel mod den nationale sikkerhed, der er reel og aktuel eller forudsigelig, skal inddrages oplysninger om antallet og karakteren af verserende eller afgjorte straffesager om overtrædelser af straffelovens kapitel 12 og 13. Det er således Justitsministeriets vurdering, at det er et væsentligt moment ved vurderingen af trusselsbilledet, 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 og 13, vil kunne tillægges betydelig vægt ved vurderingen (lovudkastets almindelige bemærkninger, punkt 3.2.3.1).

Der er efter instituttets opfattelse flere grunde til, at verserende og afgjorte straffesager ikke kan tillægges betydelig vægt ved vurderingen af, hvornår man i medfør af EU-Domstolens praksis kan iværksætte generel og udifferentieret logning.

Afgjorte straffesager kan ikke uden videre sige noget om, hvorvidt der er en reel og aktuel eller forudsigelig trussel, som er alvorlig, idet straffesager har et bagudrettet sigte, hvor en gerningsperson straffes for kriminalitet, som denne allerede har begået eller har haft til hensigt at begå.

Derudover indeholder straffelovens kapitel 12 og 13 delikter af en så forskelligartet karakter, at der er væsentlig forskel på, hvilken

---

[7] De forenede sager C-511/18, C-512/18 og C-520/18 (La Quadrature du Net), præmis 137 og 138.
[8] De forenede sager C-511/18, C-512/18 og C-520/18 (La Quadrature du Net), præmis 136

betydning en sigtelse, varetægtsfængsling og domfældelse vil kunne tillægges ved vurderingen af, om der er en alvorlig trussel mod den nationale sikkerhed. Der må således skulle foretages en konkret vurdering af alvoren af det begåede forhold.

Et andet element i vurderingen er de årlige analyser fra Center for Terroranalyses, "Vurderingen af Terrortruslen mod Danmark". Derudover kan der også indgå andre uklassificerede analyseprodukter udgivet af Politiets Efterretningstjeneste, Forsvarets Efterretningstjeneste eller Center for Cybersikkerhed i vurderingen (lovudkastets almindelige bemærkninger, punkt 3.2.3.1).

Sådanne analyseprodukter kan efter instituttets opfattelse indgå – men dog med en mindre vægt – i den samlede vurdering af, om der foreligger en alvorlig trussel mod den nationale sikkerhed, som er reel og aktuel eller forudsigelig. Der må dog være tale om, at sådanne mere generelle analyseprodukter kan tjene til at støtte konkrete og reelle forhold, herunder efterretninger om konkrete personer, og at de derfor ikke kan stå alene.

Det skyldes, at analyseprodukter såsom Center for Terroranalyses vurdering af terrortruslen mod Danmark har en mere generel karakter, og foretager en overordnet vurdering af terrortruslen mod Danmark, som gør sig gældende for et år ad gangen. Center for Terroranalyse har f.eks. vurderet, at terrortruslen mod Danmark som minimum de sidste syv år har været "alvorlig". Instituttet forstår imidlertid lovudkastet sådan, at en vurdering af terrortruslen mod Danmark som "alvorlig" er et tilstrækkeligt højt niveau – i kombination med øvrige elementer – til, at der vil kunne indføres generel og udifferentieret logning.

Generel og udifferentieret logning må samtidig ikke antage en systematisk karakter. Hvis pligten til at logge generelt og udifferentieret knyttes op på mere generelle analyseprodukter, så den tidsmæssige periode fastsættes i overensstemmelse med, hvor ofte sådanne produkter udarbejdes, og hvis pligten til logning f.eks. også fastholdes i fraværet af øvrige, konkrete elementer, så er der efter instituttets opfattelse en væsentlig risiko for, at en sådan pligt må anses for at antage en systematisk karakter i strid med EU-Domstolens nuværende retspraksis.

Det følger videre, at der kan pålægges teleudbyderne at logge generel og udifferentieret i op til 1 år fra udstedelsen af en bekendtgørelse, men dog, at den tidsmæssige periode skal begrænses til det strengt nødvendige, og at fastsatte regler ophæves, hvis der opstår grundlag

for at antage, at de ikke længere kan opretholdes (lovudkastets almindelige bemærkninger, punkt 3.2.3.2).

Instituttets har svært ved at se, at ministeriet vil kunne pege på sådanne omstændigheder, som kan godtgøre, at en pligt til at logge generelt og udifferentieret i 1 år vil være berettiget, når ministeriet skal begrænse den tidsmæssige periode til det strengt nødvendige. Det skyldes, at ministeriet, efter instituttets opfattelse, skal kunne godtgøre længden af den tidsmæssige periode på tidspunktet, hvor pligten fastsættes.

Det er samlet set instituttets opfattelse, at den vurdering, som Justitsministeriet beskriver i lovudkastet, hvor det skal være muligt at fastsætte generel og udifferentieret logning i op til 1 år ad gangen, næppe stemmer overens med EU-Domstolens nuværende praksis, der som nævnt alene tillader generel og udifferentieret logning til beskyttelse af national sikkerhed i ekstraordinære undtagelsessituationer, og forudsat, at perioden er begrænset til det strengt nødvendige.

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.

- Institut for Menneskerettigheder anbefaler, at Justitsministeriet sikrer, at adgangen til generel og udifferentieret logning til beskyttelse af national sikkerhed begrænses til ekstraordinære undtagelsessituationer.

POLITIETS ADGANG TIL LOGGEDE OPLYSNINGER

I lovudkastet lægger Justitsministeriet op til, at politiet skal kunne få adgang til oplysninger, som er indsamlet som følge af generel og udifferentieret logning, i sager om efterforskning mv. 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.

Justitsministeriet begrunder denne opfattelse med, at EU-Domstolen i La Quadrature du Net-dommen af 6. oktober 2020[9] ikke eksplicit tager stilling til, om hensynet til at efterforske og retsforfølge grov

[9] De forenede sager C-511/18, C-512/18 og C-520/18 (La Quadrature du Net).

kriminalitet kan begrunde, at politiet og anklagemyndigheden kan få adgang til trafikdata, der er lagret med henblik på at beskytte den nationale sikkerhed (lovudkastets bemærkninger, punkt 3.7.2).

Instituttet mener ikke, at det kan tillægges væsentlig betydning, at EU-Domstolen ikke eksplicit forholder sig til, om hensynet til at efterforske og retsforfølge grov kriminalitet kan begrunde en adgang til trafikdata, der er lagret med henblik på at beskytte den nationale sikkerhed, idet EU-Domstolen efter instituttets opfattelse i dommen fastslår, at myndighedernes adgang til loggede oplysninger kun kan begrundes ud fra de hensyn, som har ført til, at teleudbydere mv. i første omgang er blevet pålagt at foretage logningen.[10]

EU-Domstolen giver således i dommens præmis 166 en nærmere anvisning af, hvordan proportionalitetsprincippet skal anvendes i forhold til adgangen til loggede oplysninger, og henviser samtidig til dommens præmis 131, hvor EU-Domstolen beskriver det generelle proportionalitetsprincip, hvorefter formålet med at gøre indgreb skal stå mål med indgrebets alvorlighed. EU-Domstolen henviser derudover til præmis 55 i Ministerio Fiscal-dommen (C-207/16), hvor EU-Domstolen ligeledes redegør for det generelle proportionalitetsprincip.

Justitsministeriet anvender i lovudkastet denne henvisning til at inddrage præmis 56 i Ministerio Fiscal-dommen (som der ikke henvises til i La Quadrature du Net-dommen) for at nå frem til, at indgrebet i grundlæggende rettigheder ved pligten til at registrere og opbevare trafikdata og adgangen til disse oplysninger, kan begrundes i hensynet til forebyggelse, efterforskning og retsforfølgelse af straffelovsovertrædelser, hvis der er tale om grov kriminalitet (lovudkastets almindelige bemærkninger, punkt 3.7.2).

Instituttet har en anden fortolkning af EU-Domstolens retspraksis og er af den opfattelse, at når EU-Domstolen henviser til præmis 55 i Ministerio Fiscal-dommen og den deri indeholdte retspraksis, må det forstås sådan, at EU-Domstolen alene har ønsket at inddrage den specifikke præmis fra dommen, som EU-Domstolen henviser til, og den praksis, som heri er nævnt, men ikke øvrige præmisser fra samme dom.

Derudover handler Ministerio Fiscal-dommen om SIM-kort oplysninger og sondringen mellem grov og almindelig kriminalitet, som er noget andet end den fortolkning, som ministeriet anvender dommen til støtte

[10] De forenede sager C-511/18, C-512/18 og C-520/18 (La Quadrature du Net), præmis 166, samt sag C-746/18 (H.K.), præmis 31.

for, nemlig adgang til oplysninger til brug for efterforskning i sager om grov kriminalitet, som er logget af hensyn til statens sikkerhed.

EU-Domstolen henviser i øvrigt i præmis 55 i Ministerio Fiscal-dommen til præmis 115 i Tele2-dommen (de forenede sager C-203/15 og C-698/15), hvor det generelle proportionalitetsprincip ligeledes beskrives. Tele2-dommen handler om muligheden for at fastsætte en pligt til generel og udifferentieret logning.

Instituttet forstår præmis 131 i La Quadrature du Net-dommen sådan, at EU-Domstolen endnu engang ønsker at forklare, at der på dette område gælder et proportionalitetsprincip, og at domstolen underbygger dette ved at henvise til øvrig praksis, hvor domstolen har forklaret om et tilsvarende proportionalitetsprincip. Instituttet bemærker i øvrigt, at det EU-retlige proportionalitetsprincip er skabt af EU-Domstolen selv, og at det i det lys er naturligt, at EU-Domstolen beskriver princippet i de sager, hvor det er relevant.

Justitsministeriet lægger efter instituttets opfattelse for så vidt angår politiets og anklagemyndighedens efterfølgende adgang til oplysninger, som er indsamlet som følge af generel og udifferentieret logning, i det store hele op til videreførelsen af den ordning, som EU-Domstolen i 2016[11] fandt i strid med EU-retten, herunder de grundlæggende rettigheder til privatliv, databeskyttelse samt ytrings- og informationsfrihed, blot med en lidt anderledes begrundelse end hidtil.

Justitsministeriet anfører da også, at der er en "væsentlig procesrisiko" forbundet med regeringens udlægning af dommen (lovudkastets almindelige bemærkninger, punkt 3.7.2).

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.

- Institut for Menneskerettigheder anbefaler, at politiets adgang til oplysninger, som er indsamlet som følge af generel og

[11] De forenede sager C-203/15 og C-698/15 (Tele2)

udifferentieret logning, begrænses til sager vedrørende beskyttelse af national sikkerhed.

MÅLRETTET GEOGRAFISK LOGNING

Ministeriet lægger med lovudkastet 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).

Instituttet forstår lovudkastet således, at ministeriet lægger op til en todelt logningsordning, hvor der vil blive fastsat pligt til målrettet logning (individuel og geografisk) i alle perioder, hvor der ikke er mulighed for at fastsætte en pligt til generel og udifferentieret logning.[12]

Der er to muligheder for at fastsætte målrettet, geografisk logning i et område af 3 km gange 3 km. Det kan for det første ske, hvis antallet af anmeldelser om lovovertrædelser begået i området, som efter loven kan straffes med fængsel i 3 år eller derudover, samt en række nærmere opregnede overtrædelser af straffeloven, udlændinge og retsplejeloven, udgør mindst 1,5 gange landsgennemsnittet opgjort som gennemsnit over de seneste 3 år.

Derudover kan det for det andet ske, hvis antallet af beboere dømt for lovovertrædelser som efter loven kan straffes med fængsel i 3 år eller derudover, samt en række nærmere opregnede overtrædelser af straffeloven, udlændinge og retsplejeloven, udgør mindst 1,5 gange landsgennemsnittet opgjort som gennemsnit over de seneste 3 år.

Det fremgår derudover af lovudkastet, at det påhviler teleudbyderne at udpege de fornødne master, så det angivne område på 3 km gange 3 km dækkes fuldstændigt, hvilket bl.a. vil indebære, at det typisk vil være nødvendigt at medtage master uden for området på 3 km gange 3 km. Det betyder, at områder, der geografisk er placeret i nærheden af det omfattede område, vil kunne blive omfattet af pligten til logning, da det ikke er muligt at frasortere data inden for de enkelte cellers

---

[12] Pressemeddelelse af 27. september 2021, »Justitsministeren vil med nyt lovforslag om logning sikre så effektiv kriminalitetsbekæmpelse som muligt«, tilgængelig her, https://www.justitsministeriet.dk/pressemeddelelse/justitsministeren-vil-med-nyt-lovforslag-om-logning-sikre-saa-effektiv-kriminalitetsbekaempelse-som-muligt/

rækkevidde, som stammer fra telefoner, der reelt har befundet sig uden for de udpegede områder (lovudkastets bemærkninger til § 1, nr. 9).

Det indebærer 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.

Der er efter instituttet opfattelse 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. Derudover vil der desuden i praksis blive logget oplysninger fra telefoner, som befinder sig uden for de omfattede områder, og hvor der således ikke er et forhøjet kriminalitetsbillede.

Ydermere skal den målrettede geografisk logning også ses i sammenhæng med, at der med lovudkastet lægges op til, at der i en række områder, som er defineret som særligt sikringskritiske, altid vil blive foretaget logning, såsom trafikknudepunkter og større indfaldsveje m.v.

Rigspolitiet vurderer på et foreløbigt grundlag, at teleselskaberne som følge af den målrettede geografiske logning vil blive pålagt at logge områder svarende til cirka 15-20 procent af Danmarks samlede landareal.[13]

EU-Domstolen har ikke tidligere forholdt sig til en ordning med målrettet geografisk logning, som der med lovudkastet lægges op til. På baggrund af EU-Domstolens nuværende praksis må en ordning, hvor der sker logning af hensyn til bekæmpelse af grov kriminalitet, dog ikke de facto udgøre generel og udifferentieret logning.

Der må efter instituttets opfattelse være et tidspunkt, hvor en såkaldt målrettet ordning, som opdeler pligten til at logge i mindre enheder (f.eks. af områder af 3 km gange 3 km og særligt sikringskritiske områder), alligevel bliver anset for generel og udifferentieret som følge af logningens samlede udstrækning. Det er imidlertid efter instituttets opfattelse – og i mangel af praksis fra EU-Domstolen – uklart, hvornår dette tidspunkt indtræder.

---

[13] Information, »Justitsministeriet kalder logning af areal på størrelse med Sjælland "målrettet"«, 11. oktober 2021, tilgængelig her, https://www.information.dk/indland/2021/10/justitsministeriet-kalder-logning-areal-paa-stoerrelse-sjaelland-maalrettet

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 § 1, nr. 9).

Tilsvarende skal der for så vidt angår de særligt sikringskritiske områder alene foretages en vurdering af, om der vurderes at være særlige beskyttelseshensyn, der kan begrunde, at området anses for at være særligt sikringskritisk (lovudkastets bemærkninger til § 1, nr. 9).

- Institut for Menneskerettigheder anbefaler, at Justitsministeriet i lovudkastet sikrer, at målrettet geografisk logning ikke får et omfang, som de facto må anses for generelt og udifferentieret.

Med venlig hilsen

Louise Holck
DIREKTØR

Rådet for Digital Sikkerhed

25.10.2021

Rådet for Digital Sikkerheds høringssvar til udkast til forslag til lov om ændring af retsplejeloven og lov om elektroniske kommunikationsnet og -tjenester

Logningsreglerne skal evalueres og bringes i overensstemmelse med EU-retten og dermed tilvejebringe et klart og lovligt grundlag for logningen. Behov for logning til gavn for den nationale sikkerhed og bekæmpelse af alvorlig kriminalitet skal afvejes proportionelt med borgernes rettigheder i Charteret.

Rådet for digital Sikkerhed har forståelse for, at politiet som led i kriminalitetsforebyggende indsatser og efterforskning skal have adgang til og mulighed for at anvende værktøjer, der er tidssvarende. Rådet for Digital Sikkerhed mener helt overordnet, at lovforslaget i sin helhed er alt for vidtrækkende i forhold til proportionalitetsprincippet og retten til privatlivets fred, som er sikret i EU's charter om grundlæggende rettigheder.

Den generelle udifferentierede logning bør kun iværksættes i afgrænsede perioder, hvor der foreligger en reel og aktuel eller forudsigelig trussel mod Danmark. Godkendelsen heraf bør underlægges bredere demokratisk kontrol og domstolsprøvelse. Ligeledes er det vigtigt, at definitionen af grov kriminalitet ikke udvandes, og at overvågningen i form af geografisk målrettet logning reduceres.

Domstolene skal have mulighed for at få forelagt al relevant dokumentation for deres afgørelse af om logning kan iværksættes. Beslutninger om iværksættelsen af generel udifferentieret logning skal efterfølgende prøves ved domstolene. Lovudkastet giver derfor på en række punkter anledning til bekymring og i det følgende gives et overblik over de principper, RfDS mener, bør ligge til grund ved revision af logningsreglerne.

Rådet for Digital Sikkerhed (RfDS) takker for muligheden for at afgive bemærkninger til udkast til 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.)

Baggrund og formål

Justitsministeriet lægger med lovforslaget op til at revidere de gældende regler for registrering og opbevaring af oplysninger om teletrafik (logning) mv. – bl.a. på baggrund af EU-Domstolens dom af 6. oktober 2020.

I den pressemeddelelse[1] der er udsendt af Justitsministeriet gives der udtryk for, at regeringen ikke vil "ændre logningsreglerne af lyst, men fordi vi skal" og at "Regeringen så helst, at vi kunne fortsætte med at logge, som vi gør i dag", dvs. generel og udifferentieret logning.

Logningen skal ses i lyset af, at politiet allerede foretager betydelig opsamling af og/eller har adgang til data om borgerne som f.eks. omfatter opsamling af nummerplader (ANPG), adgang til privates TV-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 – herunder retten til beskyttelse af personoplysninger. 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 overhovedet 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

[1] https://www.justitsministeriet.dk/pressemeddelelse/justitsministeren-vil-med-nyt-lovforslag-om-logning-sikre-saa-effektiv-kriminalitetsbekaempelse-som-muligt/

af EU domstolens afgørelser. RfDS skal bemærke, 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.

Rådet for Digital Sikkerheds bemærkninger til lovforslaget

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 og forudsigelig trussel" mod den nationale sikkerhed.

Logning til kriminalitetsbekæmpelse skal foregå proportionalt: Logning kan spille en væsentlig rolle i forhold til den nationale sikkerhed, opklaring og kriminalitetsbekæmpelse. Disse formål med logningen skal balanceres og vurderes i forhold til begrænsninger i retten til privatliv, retten til databeskyttelse og mulighed for at ytre sig, som EU's Charter giver borgerne. Indgrebet i de nævnte rettigheder mhp. at forfølge de omtalte formål skal derfor opfylde tre betingelser:

1. *Indgrebet skal have en klar og præcis lovhjemmel,*
2. *Indgrebet skal forfølge et eller flere legitime formål, og*
3. *Indgrebet skal være proportionalt.*

Helt overordnet er der behov for et overblik over den samlede overvågning af borgerne: Borgerne bør 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.

I forhold til det konkrete forslag er det bekymrende, at teleselskaberne har og fortsat får rollen som statens forlængede arm ud fra et generelt retssikkerhedsmæssigt perspektiv.

Der bør være snævre rammer for den generelle og udifferentierede lognings tidsmæssige udstrækning. Generel og uddifferentieret logning bør 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" (Quadrature du Net, præmis 137). Hovedreglen er altså, 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 skruens 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.

Vurderingen af om et forhold er omfattet af national sikkerhed bør efterfølgende 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, således at borgerne sikres retssikkerhedsgaranti. 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, jf. nedenfor.

Det er problematisk, at Justitsministeriet fremlægger et forslag, hvor de selv medgiver, at der er en væsentlig procesrisiko ved forslaget, jf. pp. 106-107. 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.

Med forslaget introduceres en personbestemt og geografisk målrettet logning relateret til grov kriminalitet. Der lægges op til, at logningen kan anvendes af politiet ved kriminalitet, som har en straframme på mindst tre års fængsel. Lagringstiden for den personbestemte målrettede logning foreslås at blive henholdsvis 3, 5 og 10 år efter udstået straf. Det 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.

Den geografisk målrettede logning vil - som under de gældende regler - 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 (anmeldelser større end 1,5 gange landsgennemsnittet og beboere dømt for lovovertrædelser større end 1,5 gange landsgennemsnittet og tillige 3x3 kilometer rundt om den mængde sikringskritiske områder, som nævnes i forslaget pp. 168-170) 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 § 786c) 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 indenfor området udvidet til 3*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 mv.", som Justitsministeriet udsendte i offentlig høring den 23. marts 2021.

Straframmen for at iværksætte den geografiske logning bør være seks år. Ved sammenligning med "Skitse for revision af logningsreglerne mv.", som Justitsministeriet udsendte 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 straframmen 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.

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

Problematisk med krav om at tilknytte CPR til telefonoplysninger: Det er problematisk, at der lægges op til, at teleselskaberne skal tilknytte CPR-numre til alle telefonoplysninger. 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.

Økonomisk byrde for teleselskaberne bør reduceres: 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.

Der bør udarbejdes en offentlig konsekvensanalyse udarbejdes fsva. logningsreglerne, så en proportionalitetsafvejning kan foretages på et godt og solidt fagligt grundlag.

Rådet mener, der er behov for en bredere kortlægning og værdipolitisk debat om politiets efterhånden omfattende masseovervågning af borgernes data

Rådet står naturligvis til rådighed for en uddybelse af ovenstående synspunkter.

På bestyrelsens vegne

Henning Mortensen

Formand, Rådet for Digital Sikkerhed

København, den 25. oktober 2021

AMNESTY INTERNATIONALS BEMÆRKNINGER TIL HØRING OVER UDKAST TIL 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.)

Justitsministeriet har ved e-mail af 27. september 2021 anmodet om Amnestys eventuelle bemærkninger til ovennævnte lovforslag.

Amnesty International har følgende generelle bemærkninger til lovforslaget:

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.

Ligeledes mener Amnesty at det siden 2016 er blevet gjort klart for Justitsministeriet, at den danske logningsordning er i strid med EU-retten[1]. EU-Domstolen har i en række sager taget stilling til, hvilke rammer afbalanceringen af grundlæggende rettigheder overfor beskyttelsen af national sikkerhed giver for logningsordninger. Ifølge EU-retten er en generel og uddifferentieret logning som udgangspunkt ulovlig, hvorimod målrettet logning kan tillades under visse omstændigheder. I ekstraordinære situationer, hvor et land står overfor en konkret trussel mod national sikkerhed, kan der helt undtagelsesvist ske en generel og uddifferentieret logning af befolkningen. I disse undtagelsessituationer skal logningen begrænses til et strengt nødvendigt tidsrum og må ikke få systematisk karakter. Denne retsopfattelse er senest blevet bekræftet i La Quadrature-dommen[2] fra 2020, som også lovforslaget løbende henviser til.

Amnesty finder det yderst kritisabelt, at regeringen med det længe ventede lovforslag fremlægger en logningsmodel der vil i stor grad giver mulighed for at videreføre den nuværende ulovlige retstilstand. Amnestys bemærkninger vil begrænse sig til lovforslagets dele der vedrører adgangen til at foretage generel og udifferentieret logning med henblik på beskyttelse af den nationale sikkerhed,

[1] Se således forenede sager C-203/15 og C-698/15

[2] Se således forenede sager C-511/18, C-512/18 og C-520/18 og pressemeddelelsen

domstolsprøvelsen heraf og adgangen til den data der er blevet logget med henvisning dertil.

Amnesty International har følgende specifikke bemærkninger til lovforslaget:

I lovforslaget lægges der op til, at det vil være muligt at pålægge teleudbydere at foretage generel og uddifferentieret logning for alle borgere for op til et år ad gangen, hvis der er en trussel mod den nationale sikkerhed.

Som nævnt ovenfor, er en generel og udifferentieret logning (af trafik- og lokaliseringsdata) et så alvorligt indgreb i de grundlæggende rettigheder, at dette indgreb kun må udgøre undtagelsen og ikke reglen efter EU-retten. Anvendelsen af denne form for logning skal derfor begrænses til de situationer, hvor en stat står overfor en reel, aktuel eller forudsigelig alvorlig trussel mod den nationale sikkerhed.[3] EU-domstolen har understreget, at denne form for logning kun må tages midlertidigt i brug og ikke må få en systematisk karakter. Samtidig skal der være mulighed for, at det kan prøves ved en domstol eller en uafhængig administrativ enhed, om staten rent faktisk står overfor en alvorlig trussel mod den nationale sikkerhed. [4]

<u>En alvorlig trussel mod den nationale sikkerhed</u>
I regeringens lovforslag henviser Justitsministeriet 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 kan også indgå i vurderingen. I lovforslaget fremstår CTA vurderingen samt gennemgang af relevante verserende sager som de bærende elementer.[5] 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 fremfor instrumenter som giver årlige analyser af længerevarende trusselstilstande.

<u>Domstolsprøvelse</u>
Efter lovforslaget, kan beslutningen om at iværksætte logning prøves ved en domstol, men efterretningsmateriale af fortrolig karakter vil være undtaget, så

[3] Se hertil Forenede sager C-511/18, C-512/18 og C-520/18, præmis 137
[4] Se hertil Forenede sager C-511/18, C-512/18 og C-520/18, præmis 138-139
[5] Se hertil lovforslagets side 59-60

som klassificeret oplysninger og analyser fra efterretningstjenesterne.[6] 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.[7]

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.

Tidsmæssige udstrækning af påbud om generel og udifferentieret logning

Justitsministeriet vurderer, at det vil være proportionalt hvis et påbud om generel og udifferentieret logning højst fastlægges for et år ad gangen med mulighed for mindre end et år, hvis det skønnes nødvendigt.[8]

EU-Domstolen har præciseret, at "henset til alvoren af det indgreb i de grundlæggende rettigheder som følger af en generelle og udifferentieret logning skal den tidsmæssige udstrækning der kan gives adgang til at logge i begrænses til det strengt nødvendige", og må "ikke overstige et forudsigeligt tidsrum". Det understreges, at denne lagring ikke må have "en systematisk karakter". [9]

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 et 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

[6] Se hertil lovforslagets side 84

[7] Se hertil lovforslagets side 139

[8] Se hertil lovforslagets side 59

[9] Se hertil Forenede sager C-511/18, C-512/18 og C-520/18, præmis 137-138

bygge på konkret opstående situationer der gør en trusselsvurdering reel og eller aktuel/forudsigelig, og ikke analyser af længerevarende trusselstilstande.

Adgangen til logget data

I lovforslaget lægges der op til, at politi og anklagemyndigheden til brug for bekæmpelse af grov kriminalitet, kan få adgang til lagret data der er blevet logget med henblik på at beskytte den nationale sikkerhed. Justitsministeriet vurderer, at dette vil være i overensstemmelse med EU-retten som fortolket af EU-Domstolen i La Quadrature-dommen.[10]

I La Quadrature-dommen operer EU-Domstolen med en klar distinktion mellem national sikkerhed og bekæmpelse af grov kriminalitet. Det står klart, at det kun er hensynet til national sikkerhed der giver mulighed for at fastsætte en generel og udifferentieret logning[11]. Efter Amnesty opfattelse er der ikke 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. Tværtimod vil den formålsbegrænsning der ligger i, at der kun kan pålægges en general og udifferentieret logning med henblik på at beskytte den nationale sikkerhed kun reel have virkning hvis at den også efterfølgende gælder for myndighedernes adgang til det loggede data.

Amnesty finder det i den forbindelse stærkt bemærkelsesværdigt, at Justitsministeriet selv i samme forbindelse skriver at der er en "væsentlig proces risiko" for at disse regler i lovforslaget vil blive underkendt af EU-Domstolen.[12] Dvs. at den fortolkning ligger til grund for loven er samtidig en, hvor Justitsministeriet egen analyse er, at dette med stor sandsynlighed vil blive underkendt af EU-Domstolen, hvis de skulle vurdere de danske regler.

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 så som kriminalitetsbekæmpelse.

Amnesty International, 25. oktober 2021.

[10] Se hertil lovforslagets side 106

[11] Se forenede sager C-511/18, C-512/18 og C-520/18 præmis 166 samt sag C-746/18 præmis 31

[12] Se hertil lovforslagets side 106

Justitsministeriet

Sendt til:
jm@jm.dk, hlm@jm.dk og nat@jm.dk

Forsikring & Pension

Høringssvar til forslag til lov om ændring af retsplejeloven og lov om elektroniske kommunikationsnet og -tjenester

25.10.2021

Forsikring & Pension
Philip Heymans Allé 1
2900 Hellerup
Tlf.: 41 91 91 91
fp@forsikringogpension.dk
www.forsikringogpension.dk

Hassan Mobeen Anwar
Konsulent
Dir. 41919139
hma@forsikringogpension.dk

Vores ref. HMA
Sagsnr. GES-2020-00028
DokID 432792

Indledning

Forsikring og Pension udeladt som høringspart

Indledningsvis kan det påpeges, at Forsikring og Pension står uforstående over for, at Justitsministeriet har undladt at gøre Forsikring og Pension til høringspart for så vidt angår "Ændring af retsplejeloven og teleloven (Revision af reglerne om registrering og opbevaring af oplysninger om teletrafik (logning) m.v.) (Nov. II)."

Forsikring og Pension har en reel interesse for området, og der er tale om data-adgang, som kan have stor indflydelse på vores medlemmers mulighed for at smidiggøre sagsgangen for selskaberne, herunder deres kunder.

Forsikrings- og pensionsbranchens adgang til tele- og masteoplysninger

Hvorfor ønskes der en lettere adgang til tele- og masteoplysninger?

Forsikrings- og pensionsbranchen er hvert år udsat for mange forsøg på svindel, som jf. vores egen undersøgelse i 2020 kostede branchen (og dens kunder) mere end 800 mio.kr. For at afdække potentielle sager om forsikrings- og pensionssvindel kan selskaberne under særlige omstændigheder have behov for at undersøge tele- og masteoplysninger fra de skadelidtes mobiltelefoner.

Selskaberne kan under disse særlige omstændigheder ved hjælp af f.eks. masteoplysninger sandsynliggøre en adfærd, og herved af- eller bekræfte en lokalitet eller på baggrund af opkaldshistorik validere en forklaring, som enten rigtig eller urigtig.

Der er for selskaberne på nuværende tidspunkt begrænsede muligheder for at foretage disse særlige undersøgelser, som desuden foretages på baggrund af nøje overvejelser og en grundig vurdering, hvor der altid foreligger en velbegrundet og dokumenteret mistanke om svindel, jf. bekendtgørelse om undersøgelser foretaget af forsikringsselskaber § 8. I den forbindelse er det som en del af reglerne

præciseret, at selskaberne skal vælge de mindst indgribende metoder for at afdække potentiel svindel, og at den valgte metode skal stå i rimeligt forhold til karakteren af den undersøgte sag, jf. § 3.

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. Det bør i den forbindelse påpeges, at der er tale om oplysninger, som forsikrings- og pensionsselskaberne i dag kun kan få adgang til, ved at indhente dem via kunden/den skadelidte. Dette vurderes at vanskeliggøre sagsgangen mere end nødvendigt og gør også at potentiel svindel opdages senere i processen eller helt bliver overset som følge af den mere tidskrævende proces.

Ved at regulere adgangen til udveksling af tele- og masteoplysninger i lovgivningen vil man for det første få oplistet nogle overordnede rammer for, hvordan disse oplysninger må videregives og under, hvilke omstændigheder oplysningerne kan videregives med kundens samtykke. For det andet vil en regulering medføre en smidigere sagsgang for selskaberne og deres kunder/skadelidte.

Det er på baggrund af ovenstående vores håb, at I vil tage vores bemærkninger til overvejelse og hjælpe med at gøre adgangen til udveksling af data mellem teleindustrien og forsikrings- og pensionsbranchen lettere.

Med venlig hilsen

Hassan Mobeen Anwar

Til Justitsministeriet,

Justitsministeriet har ved brev af 27. september 2021 (sagsnr. 2020-187-0036) anmodet om eventuelle bemærkninger til høring over udkast til 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.) i høring.

Udkastet giver ikke Rigspolitiet anledning til bemærkninger.

Med venlig hilsen

Hülya Celik
Specialkonsulent

POLITI

Rigspolitiet
Koncernledelsessekretariatet
Polititorvet 14
1780 København V

Mobil 51 33 06 64
E-mail hce001@politi.dk

Web www.politi.dk
Facebook facebook.com/politi
Twitter twitter.com/rigspolitiet

Til Justitsministeriet

25. oktober 2021

BILAG til TI's høringssvar
Høring over udkast til ændring af retsplejeloven og teleloven (revision af reglerne om logning) – Telebranchens yderligere konkrete bemærkninger

I forlængelse af TI's overordnede bemærkninger i TI's høringssvar, har TI nedenstående yderligere konkrete bemærkninger til lovudkastet.

Indhold BILAG

A. Taletidskort

Med lovudkastets forslag til ny RPL § 786h (lovudkast § 1, pkt. 9) samt forslag til ændring af TL § 31, stk. 2 (lovudkast § 2, nr. 2) samt bemærkningerne til de foreslåede to bestemmelser, foreslås samlet set regler om, at telebranchen forpligtes til at gøre følgende:
(a) registrere CPR- og CVR-nummer på danske kunder i udbydernes kundedatabaser,
(b) indberette de registrerede CPR- og CVR-numre til 118-databasen,
(c) registrere Unikt ID for kunder uden CPR/CVR (udlændinge) i form af fire felter: fødselsdato, køn, statsborgerskab og pasnummer samt indberetning heraf til 118, og
(d) indrette proces for dialog med kunder om forventet bruger og registrere forventet bruger samt indberetning heraf til 118-databasen.

Nedenfor vil TI ud fra bemærkningerne til § 786h fremføre specifikke bemærkninger vedrørende taletidskort.

Ikrafttræden og implementeringsperiode
Til § 786 h, skriver JM på side 190 (TI's understregning):

> *"Det forudsættes desuden, at der skal registreres og verificeres de samme nummeroplysningsdata for uregistrerede taletidskort som for andre abonnenter omfattet af bekendtgørelse nr. 435 af 9. maj 2011 om nummeroplysningsdatabaser. Ordningen vil medføre, at det fra tidspunktet for lovens ikrafttræden ikke længere vil være muligt at købe nye uregistrerede taletidskort.*

Det foreslås også, at der fastsættes overgangsbestemmelser, således at udbyderne kan nå at tilvejebringe den nødvendige systemunderstøttelse for verificering af kunder på tidspunktet for forpligtelsens indtrædelse.
Endeligt foreslås det, at udbyderne også skal indsamle og registrere unikt ID for alle eksisterende mobilabonnementer. Derfor forudsættes det, at der fastsættes regler vedrørende en overgangsordning, således at udbyderne inden en nærmere bestemt periode skal have foretaget den fornødne registrering af eksisterende mobilabonnementskunder. Der foreslås, at dette krav om indsamling og registrering af eksisterende kunder ikke gælder for andre kundegrupper som f.eks. taletidskort, fastnet- og IP-telefoni, hvor kravet alene vil være fremadrettet."

Efterregistrering af taletidskort
TI kvitterer positivt for, at det ikke bliver et krav at efterregistrere eksisterende kunder på taletidskort, men at kravet alene vil være fremadrettet. Det er nemlig ikke muligt at komme i direkte kontakt med kunder som anvender et allerede aktiveret taletidskort i f.eks. en varmepumpe.

Ny-registrering af taletidskort
Oprettelsen af kunder på taletidskort fungerer ikke som for andre mobilabonnementer. Taletidskort er ikke-aktiverede SIM-kort, som er distribueret ud til fysiske udsalgssteder (byggecentre, tankstationer, dagligvarebutikker, kiosker etc.). Kunden skal desuden selv aktivere taletidskortet gennem online indtastning af kode eller lignende i det takseringssystem, udbyderen anvender til løbende at kontrollere taletidskortets saldo.

Der distribueres i Danmark flere hundredetusinde taletidskort om året på det fysiske marked. Distributionen sker endvidere fra anslået flere tusinde fysiske salgssteder som f.eks. butikker, tankstationer, kiosker m.m. De flere hundredetusinde kunder, der i kortere eller længere tid årligt anvender et taletidskort, fordeler sig hovedsageligt på ældre, unge og børn, europæere med arbejde i Danmark samt migranter og turister. Det er hele dette marked, der potentielt rammes med den foreslåede regulering, og et krav om ny-registrering vil for en række eksisterende udbydere af taletidskort medføre en ekstrem forretningsmæssig omvæltning og negativ økonomisk påvirkning.

Ny-registrering kræver ny systemudvikling
Hvis det fremadrettet skal være muligt for kunderne at registrere sig, kræver det, at operatørerne udvikler nye systemer, som kunderne via selvbetjening kan logge ind i, for at angive de krævede personlige oplysninger. For at taletidskort skal kunne sælges i fremtiden, kræves det videre, at systemerne automatisk kan lave et opslag i CPR-registeret for at verificere kunden.

Denne funktion er ikke udviklet i dag, og den kræver en grundlæggende omstilling af de eksisterende virksomheders forretningsgange. Dette kan umuligt nå at blive udviklet og implementeret til den 1. januar 2022.

TI indstiller derfor, at et eventuelt krav om registrering af nye taletidskort tidligst træder i kraft 1. januar 2023.

TI skal i øvrigt bemærke, at danske udbydere af taletidskort har et tæt samarbejde med politiet og f.eks. altid kan oplyse, hvor et taletidskortkort er købt. Med udgangspunkt i erfaringer fra andre lande, er det TI's opfattelse, at tvungen CPR-registrering næppe får kriminelle borgere til i højere grad at lade sig registrere. Tværtimod vil det påtænkte krav snarere øge efterspørgslen på krypterede applikationer, som f.eks. Signal eller WhatsApp, eller eksempelvis taletidskort fra andre lande. Begge dele vil utvivlsomt vanskeliggøre politiets arbejde.

Verifikation af oplysninger for danske statsborgere og udlændinge
Til § 786h, skriver JM på side 188-198 (TI's understregning):

> *"Endeligt foreslås det, at der skal registreres og verificeres de samme nummeroplysningsdata for uregistrerede taletidskort som for andre abonnenter. Det vil indebære, at der fra lovens ikrafttræden ikke længere vil kunne købes anonyme taletidskort.*
> *Der stilles ikke krav til, hvordan verificeringen skal foretages. Verificering vil eksempelvis kunne ske gennem en ny systemunderstøttet adgang til opslag i Det Centrale Personregister, hvorved det oplyste CPR-nummer kontrolleres i CPR-systemet for at verificere, at det af slutbrugeren oplyste er korrekt. Hvis slutbrugeren ikke har et CPR-nummer kan verificeringen af de af slutbrugeren oplyste oplysninger i stedet ske ved, at slutbrugeren fremviser billedlegitimation i form af et pas eller nationalt civilt identitetskort. Udbyderen kan herved kontrollere, at passet eller det nationale identitetskort, hvor fødselsdato og hhv. pasnummer eller personnummer vil fremgå, sammen med foto af slutbrugeren, stemmer overens med den person, som slutbrugeren til udbyderen oplyser at være. For personer med et CPR-nummer vil udbyderne af elektroniske kommunikationsnet og –tjenester også kunne kombinere et opslag i CPR med forevisning af billede-ID. Det afgørende er, at der foretages en verificering af slutbrugerens unikke ID.*
> *…*
> *Endvidere forudsættes det, at der fastsættes regler om, at udbyderne fremadrettet ikke må give slutbrugeren adgang til elektroniske kommunikationsnet eller -tjenester, før verificeringen er foretaget."*

Verifikation af oplysninger for danske statsborgere
Med lovforslaget pålægges operatørerne at verificere nye brugere af taletidskort, inden tjenesten kan tages i brug. Det betyder, operatørerne skal være i stand til at foretage en online registrering og verificering af slutbrugere, der aktiverer deres taletidskort.

Dette krav og de omfattende omstillinger og systemudviklinger, det medfører, er således forbundet med betydelige omkostninger og udviklingstid for selskaberne, da systemerne skal kunne fungere automatisk, så kunden kan verificeres i realtid, da kunden således ikke må opnå adgang til tjenesten, før verificeringen er foretaget. I praksis vil det betyde, at kunden skal kunne tilgå en aktiveringsside via terminalen som taletidskortet er sat i for at aktivere kortet - altså opnå adgang til denne selvbetjeningsside før verificeringen er foretaget. Verificeringen bør kunne være mulig med oplysninger fra NemID/MitID.

TI indstiller, at det bør være muligt at kunne tilgå en selvbetjeningsside hos udbyderen inden verificeringen er foretaget, samt at det også gøres muligt for kunden at fremsende den krævede dokumentation for identiteten via SMS/MMS/mail direkte til udbyderen. Endelig bør det også forud for verificering være muligt for kunden at ringe til udbyders kundeservice for at kunne modtage vejledning herom.

Verifikation af oplysninger for udenlandske statsborgere
I lovbemærkningerne står det beskrevet, at verifikation af udenlandske statsborgere, kan foretages ved kontrol af billedlegitimation. Da taletidskort skal aktiveres online og virke med det samme, kan operatørerne dog ikke se, hvordan sådan en løsning skal kunne fungere i praksis. Der foretages fysisk salg af taletidskort, men ikke en fysisk aktivering. Taletidskort kan således sidestilles med eksempelvis salg af café/oplevelsesgavekort.

Skulle verifikationen ske manuelt ved, at sælgeren af et taletidskort gennemfører en særlig proces med kopiering og lagring eksempelvis et pas, onsite-hjælp til kunden med aktivering af kort m.m. ville dette kræve opkvalificering af salgspersonale hos de førnævnte tusindvis af butikker, tankstationer, kiosker m.m. Alene denne opgave er i praksis ikke mulig at gennemføre. TI er i øvrigt ikke bekendt ikke med online-registre, hvor udbyderne via en API kan kontrollere internationale pasnumre eller identitetskort. TI ser således ikke en løsning med verifikation af udenlandske statsborgere som gangbar, medmindre det kan foregå digitalt via selvbetjening, hvor den udenlandske bruger selv kan uploade den krævede dokumentation.

TI frygter derfor, at salget af taletidskort til udlændinge med dette lovforslag reelt bliver afskaffet, og at det fremadrettet ikke længere vil være muligt som udlænding at lande i lufthavnen, købe et taletidskort og ringe hjem.

B. Opbevaringsformat (læsbarhed) og dansk realtid - ny § 786 g

Følgende fremgår på side 186 i lovudkastet (og tilsvarende på side 24) (TI's fremhævning):

> *Efter gældende ret findes der regler omkring opbevaring af trafikdata. Dette er eksempelvis tilfældet med retsplejelovens § 786, stk. 4, og de regler, der er udstedt i medfør heraf. Det fremgår af bemærkningerne til § 2, nr. 2 og 3, i lovforslag nr. L 35 som fremsat, jf. Folketingstidende 2001-02 (2. samling), tillæg A, side 879, at retsplejelovens § 786, stk. 4, indebærer en pligt for udbydere af telenet og teletjenester til at registrere "de oplysninger om tele- og internetkommunikation, der er relevante for politiets efterforskning og retsforfølgning af strafbare forhold". Det fremgår endvidere, at der vil kunne opstilles regler om opbevaringsformat (læsbarhed), foranstaltninger til beskyttelse mod uautoriseret adgang til og manipulation af loggen samt opbevaring af kontooplysninger. Endvidere fremgår det, at det bør tilstræbes, at reglerne sikrer, at korrekt dansk realtid registreres.*

TI bemærker, at der er tale om lovforslagsbemærkninger fra 2002, som ikke hidtil har været udmøntet.

Mht. spørgsmålet om registrering af trafik- og lokaliseringsdata i dansk realtid, bemærker TI, at hvis en slutbruger benytter et dansk mobilabonnement til telefoni eller sms i udlandet (roaming), så vil tidsangivelsen i de registrerede trafikdata altid følge lokaltid i udlandet, da det er den udenlandske operatør CDR (Call detail record), der modtages og registreres i den danske teleudbyders systemer. Registrering af loggede data om telefoni og sms foretaget i udlandet i dansk realtid vil derfor indebære en ændring i rådata. TI må stærkt fraråde enhver form for ændring i rådata, jf. nærmere herom nedenfor om opbevaringsformat.

Mht. spørgsmålet om opbevaringsformat henviser TI til TI's notat den 3. maj 2021 til Justitsministeriet og Rigspolitiet i forbindelse med drøftelsen om lovskitsen til nye logningsregler, hvor TI på det kraftigste fraråder, at der stilles krav om konvertering af loggede trafik- og lokaliseringsdata (rådata) til et fælles format. I notatet anfører TI herom følgende, som TI fortsat ønsker at fremhæve:

TI bemærker helt overordnet, at det ved overvejelser om fælles format er nødvendigt at sondre mellem følgende:
1. Opbevaringsformat for trafik- og lokaliseringsdata, som registreres i netværksudbydernes trafiksystemer og centraler (herefter 'rådata').
2. Udleveringsformat (rækker, kolonner, overskrifter osv.) for trafik- og lokaliseringsdata, som nævnt i pkt. 1.
3. Koordinatsystem, som anvendes ved netværksudbydernes registrering af mastepositioner i de basisstation-tabeller, som løbende sendes til Rigspolitiet.
4. Format for kundedata, som registreres i tjenesteudbydernes administrative systemer.

Mht. (1) opbevaringsformat bemærkes helt overordnet, at det af de grunde, som oplistes nedenfor, kraftigt må frarådes at stille krav om, at teleudbyderne konverterer de rå trafik- og lokaliseringsdata (rådata), som opsamles fra netværksudbydernes trafiksystemer og centraler, til et andet format. Et fælles (2) udleveringsformat (rækker, kolonner, overskrifter osv.) er derimod en mulighed, jf. nærmere herom nedenfor.

Telebranchen har på den baggrund følgende bemærkninger til lovskitsens forslag om at stille krav om fælles format:
- ➔ Teleudbyderne ser ikke udfordringer i anvendelsen af WGS84 som fælles koordinatsystem.
- ➔ Teleudbyderne kan tilbyde at benytte et fælles udleveringsformat for trafik- og lokaliserings-data (rådata) for så vidt angår rækker, kolonner, overskrifter osv. – evt. med indlejret information om, hvordan de enkelte kolonner skal tolkes.
- ➔ Teleudbyderne fraråder på det kraftigste krav om konvertering af trafik- og lokaliserings-data (rådata), som kommer fra netværkssystemer, til et fælles opbevaringsformat.
- ➔ Det vil forøge risiko for fejlkilder, hvis konvertering af rådata til et fælles opbevaringsformat skal ske hos fire mobilnetværksudbydere i stedet for i ét samlet system til konvertering hos Rigspolitiet.

- ➔ Telebranchen anbefaler, at politiet som hidtil selv står for den konvertering af teleselskabernes rådata, som politiet har behov for, hvilket samtidig er eneste mulighed for sporbarhed tilbage til de oprindelige rådata, som bør være essentielt i straffesager. Rådata er vigtige, da konvertering af data billedligt talt svarer til at bede telebranchen om at tage fingeraftryk af alle kunder og derefter modificere dem inden udlevering til politiet.
- ➔ Krav om konvertering af rådata til et fælles opbevaringsformat vil påføre en væsentlig ekstra administrativ byrde på teleselskaberne.
- ➔ Kravet om sikring af dataintegritet … er modstridende med forslag om krav om konvertering af rådata til fælles opbevaringsformat. Krav om sikring af dataintegritet kræver, at det er rådata, der logges.
- ➔ Kundedata fra tjenesteselskabernes administrative systemer i form af navn, adresse, telefonnummer (nummeroplysningsdata) findes allerede i 118-databasen i et fastlagt format, jf. bekendtgørelse om nummeroplysningsdatabaser.
- ➔ Telebranchen kan under ingen omstændigheder acceptere eventuelle krav om samkøring af trafik- og lokaliseringsdata med kundedata. Trafik- og lokaliseringsdata findes kun hos netværksudbyderne (fire mobilnetudbydere), mens kundedata om abonnentens navn og adresse kun findes hos tjenesteudbyderne, som anvender mobilnetudbydernes netværk.

C. Slutbrugeres indsigtsret i trafikdata, som er logget efter regler om målrettet logning

Målrettet logning overfor grundlæggende databeskyttelsesrettigheder
TI bemærker, at telebranchen i dag behandler langt flere anmodninger om registreredes rettigheder end mange andre brancher, og at dette - forud for implementeringen af de foreslåede nye regler om målrettet logning - medfører en nødvendig stillingtagen til de nedenfor anførte udfordringer relateret til den gældende databeskyttelsesret.

TI er bekymret for sammenstødet mellem de foreslåede nye logningsregler og de grundlæggende rettigheder i databeskyttelsesretten, herunder særligt GDPR art. 15, som vedrører den registreredes ret til indsigt. TI har i den forbindelse en række betragtninger, som TI ønsker at henlede opmærksomheden på.

Retten til indsigt og den foreslåede geografiske og personbestemte målrettede logning
Retten til indsigt er én af grundpillerne i databeskyttelsesretten. Den skal bl.a. sikre, at den registrerede til enhver tid kan gøre sig bekendt med samt verificere om en dataansvarlig lovligt behandler oplysninger om den registrerede, samt hvilke konkrete oplysninger den dataansvarlige behandler.

Databeskyttelsesloven § 22, stk. 2, indeholder begrænsninger af den registreredes rettigheder i særlige tilfælde, herunder begrænsning af retten til indsigt. TI skal gøre opmærksom på, at anvendelse af undtagelsen skaber visse praktiske udfordringer i relation til den foreslåede geografiske og personbestemte målrettede logning. TI er

dog enig i, at en korrekt anvendelse af undtagelsen er en nødvendighed for at tilgodese samfundet interesser.

TI bemærker, at det ved målrettet logning ikke er utænkeligt, at der kan opstå situationer, hvor det er uhensigtsmæssigt - ud fra et efterforskningsperspektiv eller af hensyn til statens sikkerhed - at den registrerede får indsigt i, hvilke oplysninger der behandles.

TI finder det ikke rimeligt, at vurderingen af hvilke registrerede som skal begrænses i deres indsigtsret, samt hvilke konkrete oplysninger, som skal undtages, pålægges teleudbyderne.

TI har således en bekymring i forhold til, hvordan undtagelsen skal håndteres i praksis, samt hvem der skal bære ansvaret for, at undtagelsen anvendes korrekt. Et eksempel kunne være at person A er genstand for personbestemt målrettet logning retter henvendelse til sin teleudbyder og beder om indsigt i, hvilke oplysninger der behandles om person A. I en sådan situation synes det uklart, hvem der skal bære ansvaret for vurderingen af, om person A skal begrænses i sine databeskyttelsesretlige rettigheder, og hvem der skal afgøre, hvornår begrænsningen ophører, herunder hvad teleudbyderen skal svare for ikke at kompromittere, at vedkommende er underlagt målrettet logning.

Som anført ovenfor har TI forståelse for, at der i visse konkrete tilfælde kan og med rette skal ske en begrænsning af den registreredes rettigheder. Det er TI's holdning, at undtagelsen i databeskyttelseslovens § 22, stk. 2, skal fortolkes restriktivt, og således alene kan anvendes i konkrete tilfælde hvor de konkrete oplysninger bevirker, at den registreredes rettigheder reelt set kan kollidere med f.eks. statens sikkerhed eller have en negativ indvirkning på en konkret efterforskning. Det er dog også TI's holdning, at teleudbyderen ikke har det fornødne kendskab - eller i øvrigt intentioner om sådant kendskab – til at kunne konkludere, om de loggede oplysninger skal undtages fra f.eks. indsigtsretten for en given registreret, som af den ene eller anden årsag er underlagt målrettet logning. Det er derfor TI's vurdering, at lovforslaget bør anvise en løsning der gør det muligt for TI's medlemmer nemt og omkostningsfrit at konkludere i relation til, hvem undtagelsen skal anvendes og i hvilken udstrækning. Det er følgelig også Rigspolitiet, der bærer ansvaret for den foretagne vurdering. Alternativt, er det TI's vurdering, at Justitsministeriet skal uddybe og vejlede omkring hvordan teleudbyderen skal håndtere undtagelsen i databeskyttelseslovens § 22, stk. 2, i lyset af de foreslåede regler om målrettet logning.

Retten til indsigt og de nuværende regler om generel logning
De gældende logningsregler - hvor alle elektroniske kommunikationsoplysninger opbevares udifferentieret i 1 år - giver ikke anledning til bekymring i forbindelse med anmodning om indsigt fra den registrerede, da telebranchen kan imødekomme anmodningen uden at skulle bekymre sig om at kompromittere statens sikkerhed eller andre af statens interesser.

TI's medlemmer kan derfor ubekymret bekræfte den registrerede i at oplysninger om denne behandles, samt udlevere en kopi af oplysningerne uden at den registrerede derigennem vil få indsigt i, at den pågældende f.eks. er under efterforskning, og dermed uden at efterforskningen kompromitteres.

TI er velvidende om, at retten til indsigt ikke er en ubetinget ret, og at der derfor kan være konkrete omstændigheder, som begrunder en begrænsning i rettigheden. Det er dog ikke TI's erfaring, at der er udfordringer med at forene de nuværende generelle logningsregler med de konkrete undtagelser i databeskyttelsesretten.

D. Øvrige bemærkninger til lovudkastet

Internetkommunikation

Følgende fremgår på side 24 i lovudkastet (og tilsvarende på side 186) (TI's fremhævning):

> *"Efter gældende ret findes der regler omkring opbevaring af trafikdata. Dette er eksempelvis tilfældet med retsplejelovens § 786, stk. 4, og de regler, der er udstedt i medfør heraf. Det fremgår af bemærkningerne til § 2, nr. 2 og 3, i lovforslag nr. L 35 som fremsat, jf. Folketingstidende 2001-02 (2. samling), tillæg A, side 879, at retsplejelovens § 786, stk. 4, indebærer en pligt for udbydere af telenet og teletjenester til at registrere "de oplysninger om tele- og internetkommunikation, der er relevante for politiets efterforskning og retsforfølgning af strafbare forhold". …"*

TI bemærker, at lovforslaget fra 2002, der citeres fra, for så vidt angår omtalte "internetkommunikation" alene vedrører sporing af kilde-IP-adresser, hvilket fremgår tydeligt af lovforslaget fra 2002. Hvis citatet medtages i det kommende lovforslag til ændring af reglerne om logning, opfordrer TI til, at det præciseres, at der efter gældende ret ikke stilles krav om logning af internetkommunikation ud over krav om logning af kilde-IP-adresser.

Iværksættelse af logning – straks (bødestraf)

Følgende fremgår på side 44-45 i lovudkastet (TI's fremhævning):

> *"Det følger af telelovens § 10, stk. 4, at det påhviler udbyderen at sikre, at politiets anmodninger om fremskaffelse af oplysninger om teletrafik samt historisk teleoplysning og historisk udvidet teleoplysning behandles straks og på en sådan måde, at hensigten med indgrebet ikke forspildes. Overtrædelse af telelovens § 10, stk. 4, kan efter de gældende regler straffes med bøde, jf. telelovens § 81, stk. 1, nr. 1. På tilsvarende vis foreslås det, at der vil kunne pålægges bødestraf, hvis udbydere […] uden lovlig grund afviser at efterkomme et pålæg om iværksættelse af målrettet registrering og opbevaring, eller hvis iværksættelsen af pålægget ikke sker straks."*

TI bemærker at sammenligningen mellem den gældende regel i Telelovens § 10, stk. 4 om straks-iværksættelse af indgreb i meddelelseshemmeligheden ikke forekommer at være relevant, idet iværksættelse af logning ikke på samme måde som et indgreb i meddelelseshemmeligheden kan medføre, at hensigten med indgrebet forspildes. Iværksættelsen af logning synes således kun at haste, hvis pålægget sker tæt på det tidspunkt, hvor trafik- og lokaliseringsdata ellers ville blive slettet i udbyderens systemer (fx 14 dage for lokaliseringsdata).

TI foreslår, at sammenligningen udgår af lovforslaget. TI foreslår endvidere, at den sidste sætning udgår, så afsnittet alene omtaler muligheden for at pålægge bødestraf, hvis en udbyder uden lovlig grund afviser at efterkomme et pålæg om iværksættelse af logning.

Prøvelse af pålæg om logning
Følgende fremgår på side 45 i lovudkastet (TI's fremhævning):

> *"Der er ikke adgang til, at en udbyder […] foretager en retlig efterprøvelse af, om betingelserne [for iværksættelse af logning] konkret er opfyldt. Ansvaret for, at betingelserne for at påbegynde registrering og opbevaring er opfyldt, ligger således alene hos de myndigheder, der er kompetente til at pålægge registrering og opbevaring."*

TI anmoder om, at det uddybes i lovforslaget, hvad der er formålet med at afskære teleudbydernes adgang til retlig efterprøvelse af, om betingelserne for målrettet registrering/opbevaring er opfyldt.

Eventuelle fejl i pålæg om logning
Følgende fremgår på side 45 i lovudkastet (TI's fremhævning):

> *"… Såfremt et pålæg konkret måtte give anledning hertil, f.eks. pga. dets omfang, er der imidlertid ikke noget til hinder for, at udbyderen søger pålæggets udstrækning bekræftet hos politiet. Politiets bekræftelse heraf vil i den forbindelse være tilstrækkelig dokumentation for, at udbyderen har sikret den fornødne dokumentation af grundlaget for den iværksatte registrering og opbevaring".*

TI anmoder om, at det uddybes i lovforslaget, hvad konsekvensen er, hvis det viser sig, at der er fejl politiets pålæg, og politiet derfor ikke kan bekræfte pålæggets udstrækning.

Adgang til trafikdata om kommunikation, som ikke er logningspligtig
Følgende fremgår på side 47 i lovudkastet (TI's fremhævning):

> *"… Der lægges med lovforslaget op til, at disse yderligere lokaliseringsdata fremover fortsat ikke skal være registrerings- og opbevaringspligtige. Politiet vil derfor fortsat kunne få adgang til sådanne data efter de gældende*

> *regler om edition i det omfang, udbyderne af elektroniske kommunikationsnet eller -tjenester 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. Det bemærkes i den forbindelse, at udbyderne af elektroniske kommunikationsnet eller -tjenester har oplyst, at de som udgangspunkt sletter oplysninger, der ikke er registrerings- og opbevaringspligtige, efter ca. 14 dage. Forslaget 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, …"*

TI gør opmærksom på, at trafikdata om slutbrugerens kommunikation (telefoni-, sms- og datakommunikation) kun kan udleveres til politiet efter kendelse om indgreb i meddelelseshemmeligheden (teleoplysning).

Følgende fremgår på side 99 i lovudkastet (TI's fremhævning):

> *"Forskelligt fra almindelige masteoplysninger er oplysninger om, hvilke sendemaster en telefon eller kommunikationsapparat har signaleret til (allerede registreret lokaliseringsdata) uden at have været aktiv på den pågældende mast. Sådanne oplysninger er ikke omfattet af registreringspligten efter gældende ret. Trafikdata i forbindelse med internetforbrug er heller ikke registreringspligtigt efter den gældende § 786, stk. 4, og regler fastsat i medfør heraf. Hvis teleselskaberne er i besiddelse af sådanne oplysninger, kan de kræves udleveret efter reglerne om edition."*

TI bemærker, at politiets adgang til trafikdata om slutbrugerens datakommunikation (internetforbrug) efter TI's opfattelse kræver kendelse om indgreb i meddelelseshemmeligheden (teleoplysning).

Celleudvælgelse

Lovforslaget anfører på side 52 (og på side 167) (TI's fremhævning):

> *"Det forudsættes i den forbindelse, at udbyderne iværksætter registreringen og opbevaringen af trafikdata, så registreringen alene omfatter det område, der er strengt nødvendigt. Det påhviler i den forbindelse udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikke-accessorisk del af virksomheden, at udpege de fornødne master, således at det angivne område dækkes fuldstændigt."*

TI opfordrer til, at udtrykket strengt nødvendigt udelades i denne sammenhæng med henvisning til de teoretiske beregninger og usikkerheder, som udvælgelsen af master

til en fuldstændig dækning af felter på 3x3 km beror sig på, og som kan gå videre end, hvad der evt. kan anses som "strengt nødvendigt".

Begrebet Mastespring

Lovforslaget anfører på side 52 (og igen på side 167) (TI's fremhævning):

> *", ved udpegningen af de fornødne master tager højde for bygningsmassen og andre forhold, der typisk vil kunne forårsage såkaldte mastespring. Det vil bl.a. indebære, at det typisk vil være nødvendigt at medtage master uden for området på 3 km gange 3 km, da telefoner vil være mere tilbøjelige til at springe på master, der er placeret længere væk, såfremt disse er mindre belastede af trafikdata end de master, der befinder sig tættest ved telefonen. Er dette tilfældet, vil de oplysninger, der registreres og opbevares, være omfattet af den målrettede geografiske registrering og opbevaring."*

TI opfordrer til en præcisering af afsnittet, herunder at udtrykket "mastespring" udgå, da brugen af udtrykket er vildledende, idet anvendelse af master udenfor de geografisk afgrænsede områder kan forekomme uafhængigt af belastningen af masterne. TI foreslår derfor følgende tekst i stedet:

> … ved udpegningen af master tager højde for, at det vil være nødvendigt at medtage master uden for det angivne område på 3x3 km, i tilfælde hvor disse master kan give dækning i det angivne område. Samtidig vil master inden for det angivne område ofte også dække områder uden for de angivne områder. Er dette tilfældet, vil de oplysninger, der registreres og opbevares, være omfattet af den målrettede geografiske registrering og opbevaring.

Overgang fra generel logning til målrettet logning med kort varsel

Følgende fremgår på side 59 i lovudkastet (TI's fremhævning):

> *"… Det forudsættes også, at udbyderne af elektroniske kommunikationsnet eller -tjenester med kort varsel kan understøtte en overgang fra generel og udifferentieret registrering og opbevaring til målrettet personbestemt og geografisk registrering og opbevaring."*

TI bemærker, at en overgang med kort varsel fra generel logning til målrettet logning for et stort antal fokusnumre og fokusområder vil forudsætte, at politiet tilbyder en automatiseret løsning for oplysning om numre og områder (fx API).

I overgangsperioden indtil politiet er klar med en automatiseret løsning, og hvor iværksættelse målrettet logning derfor vil skulle ske på baggrund af manuelle lister fra politiet, vil det tage længere tid for teleudbyderne at iværksætte logningen.

Beskrivelse af lokaliseringsdata, som skal udleveres efter ny § 804 a
Følgende fremgår på side 159 i lovudkastet (TI's fremhævning):

> *"Den foreslåede § 804 a i retsplejeloven vil i praksis omfatte historiske masteoplysninger, det vil sige oplysninger om, hvilke sendemaster og maste-celler en telefon eller kommunikationsapparat har været registreret på. Oplysninger efter den foreslåede bestemmelse vil også omfatte oplysninger om, hvilke kommunikationsapparater der på et givent tidspunkt har befundet sig i et bestemt område. Bestemmelsen vil dog også omfatte andre oplysninger, som udbyderne af elektroniske kommunikationsnet og –tjenester er forpligtet til at registrerer efter §§ 786 a-786 e eller efter pålæg eller regler udstedt i medfør af disse bestemmelser."*

TI bemærker, at de foreslåede nye regler om logning efter §§ 786 a-786 e omfatter trafikdata om kommunikation (sms og telefoni) samt lokaliseringsdata ifm. sådan kommunikation.

Lokaliseringsdata kan udleveres som beskrevet i den citerede tekst efter den foreslåede nye § 804 a, mens udlevering af trafikdata om kommunikation kræver kendelse om indgreb i meddelelseshemmeligheden. Der resterer derfor efter TI's opfattelse ikke "andre oplysninger" som nævnt i den citerede tekst. TI foreslår, at teksten enten slettes eller uddybes.

TI foreslår i øvrigt, at teksten i 2. punktum i den citerede tekst præciseres til følgende ordlyd, som bruges af flere retter:

> Oplysning om, hvilke kommunikationsapparater der på et givent tidspunkt har været registreret på masteceller, som dækker et givet område.

TI opfordrer til at benytte begrebet "Udvidet masteoplysning" om sidstnævnte ydelse.

Overgangsordning for data logget før lovens ikrafttræden

Følgende fremgår af § 3, stk. 3 (side 7 i lovudkastet) (TI's fremhævning):

> *Stk. 3. For oplysninger, der på tidspunktet for lovens ikrafttræden er registreret og opbevaret efter retsplejelovens § 786, stk. 4, jf. lovbekendtgørelse nr. 1445 af 29. september 2020, finder kapitel 71 og 74 om indgreb i meddelelseshemmeligheden og edition som affattet ved denne lovs § 1, nr. 9, anvendelse.*

TI bemærker, at den omtalte § 1, nr. 9 omhandler logning (ikke udlevering).

TELE INDUSTRIEN
teleselskabernes branchesamarbejde

Til Justitsministeriet

Sendt pr. mail til jm@jm.dk, hlm@jm.dk, nat@jm.dk

c.c. Energistyrelsen tele@ens.dk

25. oktober 2021

Høring over udkast til ændring af retsplejeloven og teleloven (revision af reglerne om logning) – Teleindustriens bemærkninger

Ved brev af 27. september 2021 har Justitsministeriet sendt ovennævnte lovudkast i høring (sagsnr. 2020-187-0036). Teleindustrien (TI) takker for høringen og nedenfor findes TI's bemærkninger til lovudkastet.

TI har nedenstående overordnede bemærkninger til lovudkastet:

Indhold

Resumé

- **0.** 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 mv.

- **1.** 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) er ikke 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. Forslaget er ikke nødvendigt for at sikre Danmarks efterlevelse af EU-dommene om målrettet logning. **TI opfordrer 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 byrdefuld for branchen.

- **2.** Lovudkastet kan læses sådan, at teleudbyderne skal iværksætte **målrettet personbestemt logning** baseret på oplysningen om en persons identitet (fx 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.

- **3.** 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 fastnetoperatørerne 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.**

- **4.** TI anmoder om, at Justitsministeriet **sletter** afsnittet på side 47 i lovudkastet om en **frafiltreringsmekanisme**.

- **5.** TI anmoder om, at det tydeliggøres i lovforslaget, **hvilke udbydere, hvilke tjenester og hvilke datatyper**, der er omfattet af de nye regler.

- **6.** TI efterlyser **klare og enkle regler om udlevering af trafik- og lokaliseringsdata** til politiet. Men lovudkastet lægger op til nye komplekse udleveringsregler. TI foreslår, at **Strafferetsplejeudvalget inddrages** i overvejelserne om revision af reglerne om politiets adgang til teledata.

- **6.E.** Det **er ikke muligt at forstå indholdet af den foreslåede nye § 804 b**. 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, så der ikke hersker tvivl i den politiske proces om, hvad forslaget går ud på.

- **7.** TI anmoder om, at sikres en **reel omkostningsdækning** for de teleselskaber, som bliver pålagt at foretage målrettet logning, som er et rent efterforskningsmæssigt værktøj. TI opfordrer desuden 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.

Nedenfor findes uddybning til ovenfor nævnte punkter og i bilag 1 findes endvidere yderligere konkrete bemærkninger til øvrige dele af lovudkastet.

0. Implementeringsfrister og overgangsordning
TI gør opmærksom på, at teleudbyderne har behov for følgende implementeringsfrister – regnet fra det tidspunkt, hvor de foreslåede nye regler er endeligt vedtaget og endelige krav er udmøntet i bekendtgørelser:

A. It-løsninger til understøttelse af nye regler om målrettet logning: 15 måneder.
B. Ændringer i it-systemer og administrative processer til understøttelse af krav om registrering af unikt ID og bruger: 1½-2 år (for de største teleudbydere).
C. Ændring af 118-databasen med henblik på at kunne modtage indberetning af CPR/CVR/Unikt ID (EU-baseret database): 3-5 år (for forsyningspligtudbyderen).

Det bemærkes, at det anførte på side 53 i lovudkastet, jf. lovudkastets § 3, stk. 2 om at der kan udstedes en bekendtgørelse om en manual 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 skal stadig kunne håndtere personbestemt- og geografisk logning, hvilket kræver samme udvikling som punkt A.

TI bemærker, at i overgangsperioden indtil tekniske løsninger for målrettet logning er på plads, vil politiet som hidtil kunne anmode om hastesikring af lokaliseringsdata fra teleudbydernes fejlretningssystemerne; ligesom teleudbyderne uanset reglerne om logning, opbevarer trafikdata om kommunikation til brug for fakturering, som politiet kan indhente efter kendelse om teleoplysning efter de gældende regler om indgreb i meddelelseshemmeligheden.

1. Registrering af Unikt ID og indberetning heraf til 118-databasen (CPR mv.)
Med lovudkastets forslag til ny RPL § 786h (lovudkast § 1, pkt. 9) samt forslag til ændring af TL § 31, stk. 2 (lovudkast § 2, nr. 2) samt bemærkningerne til de foreslåede to bestemmelser, foreslås samlet set regler om, at telebranchen forpligtes til at gøre følgende:

(a) registrere CPR- og CVR-nummer på danske kunder i udbydernes kundedatabaser,
(b) indberette de registrerede CPR- og CVR-numre til 118-databasen,
(c) registrere Unikt ID for kunder uden CPR/CVR (udlændinge) i form af fire felter: fødselsdato, køn, statsborgerskab og pasnummer samt indberetning heraf til 118, og
(d) indrette proces for at dialog med kunder om forventet bruger og registrere forventet bruger samt indberetning heraf til 118-databasen.

Gennemførelsen af forslaget vil kræve betydelige ændringer i processer og it-systemer hos teleudbyderne, og vil koste telebranchen langt over 100 mio. kr. [1] 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.

Forslaget og baggrunden herfor er kun overfladisk beskrevet i lovudkastet – og forslaget har hverken indgået i Justitsministeriets lovskitse fremlagt i april 2021 eller i de seneste års omfattende drøftelser med branchen om tekniske løsninger til brug for målrettet logning. Forslaget er således ikke gennemarbejdet og indholdet og konsekvenserne af forslaget fremstår meget uklart[2].

Forslaget ses ikke at følge af EU-dommene om målrettet logning, idet meningen med EU-dommene aldrig har været, at der skal indføres mere registrering af data, herunder kundedata og indberetning heraf til en central database (118). Reglerne om logning/dataretention går ud på, at teleudbyderne skal bevare data, som ellers ville være blevet slettet. Det er dermed ikke hensigten, at teleudbyderne skal generere yderligere data, herunder kundedata, af hensyn til efterforskning og overvågning. Telebranchen driver således kommunikationsvirksomhed ikke overvågningsvirksomhed.

Forslaget ses heller ikke at være nødvendigt i forhold til indførelsen af de nye regler om målrettet logning, idet politiet, jf. nærmere herom nedenfor pkt. 2, 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

---

[1] Bemærk formodet slåfejl på side 138 i lovudkastet, hvor "omstillingsomkostninger" til tilpasning af teleudbydernes it-systemer til brug for registrering af Unikt ID og bruger samt indberetning heraf til 118-databasen er angivet til at være 63 mio. kr. – men TI skønner, at beløbet er væsentligt højere. Det bemærkes hertil, at lovudkastets samlede omstillingsomkostninger for telebranchen er angivet til at være 206 mio. kr., hvilket ikke modsvarer summen af de angivne beløb for de to dele af lovforslaget: (A) målrettet logning af trafik- og lokaliseringsdata, som korrekt er angivet til 53 mio. kr., hhv. (B) Registrering af Unikt ID og bruger samt indberetning heraf til 118, som er angivet til 63 mio. kr.

[2] Den del af forslaget, som vedrører registrering af Unikt ID for udlændinge og registrering af forventet bruger i teleudbydernes kundedatabaser, blev under stort tidspres og uden detaljeret beskrivelse introduceret for telebranchen til hastedrøftelse primo maj 2021, mens forslaget om selve indberetningen af oplysninger om CPR/CVR/ID og bruger til 118-databasen uden nærmere beskrivelse først blev introduceret for telebranchen ifm. den erhvervsøkonomiske analyse af lovudkastet (AMVAB-målingen), som blev gennemført i juli 2021. Ved begge lejligheder har branchen skriftlig ved breve af 6. maj og 6. juli 2021 kraftigt modsat sig forslagene. Teleindustriens breve til Justitsministeriet af 6. maj og 6. juli 2021 findes på TI's hjemmeside: https://www.teleindu.dk/brancheholdninger/logning-og-teledata/

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.

Forslaget bygger på den misforståelse, at der kan ske en "entydig identifikation af brugeren af et givet kommunikationsmiddel" (jf. afsnit 3.4.2. i lovforslagsbemærkninger – side 70 i lovudkastet). Forslaget vil imidlertid ikke sikre politiet konkret og reel viden om, hvilke telefonnumre og kommunikationsmidler kriminelle og andre fokuspersoner 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[3]. Henset til omgåelsesmuligheden og den deraf følgende begrænsede efterforskningsmæssige værdi sat overfor den estimerede omkostningsbyrde for telebranchen, forekommer forslaget således ikke at være proportionalt.

TI bemærker, at hvis Rigspolitiet har behov for, at nummeroplysningsdata i 118-databasen om telekundernes navn og adresse sammenholdes med CPR- og CVR-numre, vil Rigspolitiet selv – uden telebranchens mellemkomst via eksisterende standardfunktion i Det Centrale Personregister – kunne etablere en it-løsning som overbygning til Rigspolitiets adgang til 118-databasen, som på baggrund af verificerede nummeroplysningsdata i 118-databasen henter de registreredes CPR- og CVR-numre i Det Centrale Personregister (CPR) og Det Centrale Virksomhedsregister (virk.dk). En sådan samlet indhentelse af CPR- og CVR-numre må forventes at være langt billigere for det danske samfund og kræve langt mindre it-udvikling, end hvis ca. 100 udbydere af nummerbaserede mobil- og telefonitjenester skal indberette CPR/CVR-numre hver for sig med risiko for fejl.

Dertil kommer, at et CPR-nummer er en fortrolig personoplysning, og at behandling af denne oplysning bør minimeres mest muligt. Lovudkastets forslag om overførsel af CPR-numre for alle danske telekunder til 118-databasen skaber således en unødig behandling af danskernes CPR-numre. CPR-numrene behøver kun at blive registreret hos hvert teleselskab for sig.

Registrering af eventuel bruger og videregivelse af denne oplysning til 118-databasen som en del af nummeroplysningsdata vil – ud over at være en stor administrativ byrde for teleudbydere, der skal indsamle disse data – desuden indebære stor persondataretlig kompleksitet, dels mht. spørgsmålet om indhentelse af brugerens accept til

[3] I tilfælde, hvor pålæg om målrettet personbestemt logning er baseret på rene objektive kriterier, jf. den foreslåede nye § 786 b (personer, der tidligere har været straffet for grov kriminalitet hhv. personer, der tidligere har været genstand for indgreb i meddelelseshemmeligheden (og som er blevet orienteret herom efter RPL § 788)), kan oplysning om, hvilke telefonnumre fokuspersonen benytter, formentlig lettest afklares ved, at politiet spørger fokuspersonen.

registrering i 118-databasen, dels ift. oplysning af både kunden og brugeren om, at registrering af bruger i tilknytning til en kunde indebærer en registrering af, hvem der har en (familie)relation til hinanden (brugere hos privatkunder), hhv. hvem der er ansat hvor (brugere hos erhvervskunder). Det er desuden ikke reguleret i den gældende bekendtgørelse om nummeroplysningsdatabaser, om det er oplysning om brugeren, kunden, eller begge, der skal videregives "til alle der ønsker det", jf. TL § 31, stk. 1, og denne problemstilling bør derfor også adresseres i lovforslaget, hvis forslaget fastholdes.

TI anerkender, jf. nærmere herom nedenfor pkt. 1.A, at der – af hensyn til den generelle datakvalitet i 118-databasen – kan være behov for at indføre krav om, at (a) teleudbydere i deres egne kundedatabaser registrerer kundernes CPR/CVR-nummer og herefter verificerer kundens nummeroplysningsdata (navn og adresse), inden nummeroplysningsdata indberettes til 118-databasen. De fleste udbydere i Danmark benytter allerede sådanne forretningsgange, og et sådant forslag vil derfor ikke medføre store omkostninger for disse udbydere.

TI må derimod på baggrund af de overfor gennemgåede punkter meget klart henstille til at skrinlægge de foreslåede regler om
(b) indberetning af CPR- og CVR-nummer til 118-databasen,
(c) registrering af Unikt ID for udlændinge og indberetning heraf til 118, samt
(d) proces for dialog med kunder om forventet bruger samt registrering af forventet bruger og indberetning heraf til 118-databasen.

TI anmoder på denne baggrund om, at forslag til ny RPL § 786 h (lovudkast § 1, pkt. 9) samt forslag til ændring af TL § 31, stk. 2 (lovudkast § 2, nr. 2) udgår af lovforslaget.

1.A. Alternativ model til øget datakvalitet i 118 (verificering af kundens navn og adresse)
Som nævnt ovenfor anerkender telebranchen, at datakvaliteten i 118-databasen kan forbedres, idet der – pga. bl.a. slåfejl i oprettelsesprocessen hos nogle teleudbydere – findes eksempler på, at oplysninger om navn og adresse, som teleudbydere indberetter til 118-databasen, ikke svarer 100% til navn- og adressedata registreret i Det Centrale Personregister (CPR) hhv. Det Centrale Virksomhedsregister (virk.dk).

TI kan derfor efter omstændighederne for at styrke datakvaliteten i 118-databasen anerkende behovet for, at CPR-registrering gøres til en forudsætning for at oprette abonnement på mobil- og telefonitjenester i Danmark, og at CPR-registreringen herefter kan danne grundlag for krav om verificering af nummeroplysningsdata om navn og adresse inden indberetning heraf til 118-databasen.

En eventuel regel om registrering af CPR/CVR-nummer til brug for validering af nummeroplysningsdata bør efter TI's opfattelse i givet fald placeres i Telelovens afsnit II, kapitel 3 i afsnittet om behandling af persondata – fx som ny TL § 13 a med følgende ordlyd:

”§ X. Udbydere af elektroniske kommunikationstjenester, der videretildeler telefonnumre til slutbrugere (nummerbaserede kommunikationstjenester), skal registrere slutbrugerens CPR- eller CVR-nummer i udbyderens kundedatabase og på baggrund heraf verificere kundens nummeroplysningsdata, jf. § 31, stk. 2, inden tjenesten leveres til slutbrugeren.
Stk. 2. Udbydere som nævnt i stk. 1 skal for slutbrugere uden CPR- eller CVR-nummer kræve anden form for Unikt ID – fx forevisning af billedlegitimation – og på baggrund heraf verificere kundens nummeroplysningsdata, jf. § 31, stk. 2, inden tjenesten leveres til slutbrugeren.
Stk. 3. Udbydere som nævnt i stk. 1 og 2 skal indberette verificerede nummeroplysningsdata, som nævnt i stk. 1 og 2, til forsyningspligtudbyders udtømmende nummerfortegnelse, jf. § 14, stk. 2, nr. 4, hurtigst muligt og senest dagen efter leveringen af abonnementet til slutbrugeren.
Stk. 4. Udbydere som nævnt i stk. 1, skal på baggrund af de registrerede CPR- og CVR-numre løbende ajourføre verificeringen af kundens nummeroplysningsdata ved løbende opslag i CPR-registeret og CVR-registeret, så længe tjenesten leveres til kunden. Hvis den løbende ajourføring medfører ændringer i kundens nummeroplysningsdata, skal ændringerne indberettes til forsyningspligtudbyders udtømmende nummerfortegnelse, jf. § 14, stk. 2, nr. 4, hurtigst muligt og senest [dagen efter ajourføringen].
Stk. 5. Klima-, energi- og forsyningsministeren kan efter forhandling med justitsministeren fastsætte nærmere regler om registrering og verificering som nævnt i stk. 1 og 2.
Stk. 6. Nummerbaserede kommunikationstjenester leveret via mobile elektroniske kommunikationsnet net før 1. januar 2023, skal senest den 1. januar 2023 opfylde krav om registrering, verificering og indberetning som nævnt i stk. 1-4.
Stk. 4. Nummerbaserede kommunikationstjenester leveret via faste elektroniske kommunikationsnet før den 1. januar 2023 er undtaget fra krav om registrering, verificering og indberetning som nævnt i stk. 1-4, medmindre registrering af slutbrugerens CPR- eller CVR-nummer allerede findes i udbyderens kundedatabase”.

En sådan regel vil kunne bidrage til at sikre den datakvalitet i 118-databasen, som Rigspolitiet efterspørger.

1.B. Implementeringstid, hvis forslaget om CPR-indberetning til 118-databasen fastholdes

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 af nummeroplysningsdata om navn, adresse og telefonnummer, 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 finder, at et grundigt analysearbejde af politiets behov og alternative løsningsforslag er helt essentielt henset til det foreliggende forslags

store omkostningsmæssige byrde for telebranchen. Det er i denne forbindelse vigtigt at undgå, at det aktuelle lovforslag om revision af reglerne om logning af teletrafik, kommer til at indeholde eksplicitte regler om registrering af kundedata og indberetning heraf til 118-databasen, som ikke kan rumme mulige alternative løsningsforslag.

Fastholdes forslaget i sin helhed, har teleudbyderne brug for en implementeringsfrist til gennemførelse af de nødvendige ændringer i it-systemer og administrative processer. De store teleudbydere, og forsyningspligtudbyderen (TDC/Nuuday) oplyser, at lovudkastets forslag kræver en implementeringsfrist på mindst 1½-2 år for teleudbyderne hhv. 3-5 år for forsyningspligtudbyderen regnet fra det tidspunkt, hvor de endelige regler om registrering af Unikt ID og bruger samt indberetning til 118 er kendte, dvs. fra udstedelsen af ny bekendtgørelse om nummeroplysningsdatabaser og fastsættelse af nye vilkår for forsyningspligten.

Forsyningspligtudbyderen (TDC/Nuuday) har desuden 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.

Forsyningspligtudbyderen (TDC/Nuuday) har desuden oplyst TI om, at selskabet ønsker at fremhæve, at selskabet stærkt frabeder sig at skulle registrere CPR-numre i den landsdækkende nummeroplysningsdatabase (118-databasen), dels henset ovenfor nævnte persondataretlige betænkeligheder, dels henset til at der vil skulle påregnes store ekstraomkostninger, hvis det skal sikres, at 118-databasen fremover udelukkende supporteres fra EU.

Det bemærkes, at spørgsmålet om opbevaring af nummeroplysningsdata i EU eller tredjelande er kort omtalt i lovudkastet (jf. afsnit 3.8.2. i de alm. bemærkninger – side 130, nederst i lovudkastet[4]), men det fremgår ikke, om Justitsministeriets vurdering vedrører de gældende regler om nummeroplysningsdata eller de foreslåede nye regler om, at registrere indberettede CPR-numre mv 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 mv. i tredjelande, herunder it-supportadgang fra tredjelande. TI anmoder om, at lovforslagsbemærkningerne tydeliggøres og præciseres på disse punkter, så det står klart, hvilke nye krav, der vil blive

[4] Lovudkastet afsnit 3.8.2. i de alm. bemærkninger – side 130, nederst:
"*Det bemærkes, at nummeroplysningsdata, som defineret i § 31, stk. 2, i teleloven, og som udbydere af elektroniske kommunikationsnet eller -tjenester bl.a. skal indsamle og registrere til brug for nummeroplysningsdatabasen, jf. bekendtgørelse nr. 435 af 9. maj 2011 om nummeroplysningsdatabaser, efter Justitsministeriets opfattelse ikke kan anses som omfattet af Tele2-dommens præmis 122. Det er derfor ikke nødvendigt at indføre en bestemmelse om at nummeroplysningsdata opbevares på servere inden for EU, og den foreslåede bestemmelse tager ikke sigte herpå*."

stillet til forsyningspligtudbyderen mht. it-løsning for 118-databasen, hvis teleudbyderne skal indberette CPR-numre hertil.

1.C. Særligt om lovudkastets forslag til ændring af TL § 31 (definition af nummeroplysningsdata)

Som beskrevet under pkt. 1, anmoder TI om, at forslaget til ændring af TL § 31, stk. 2 (lovudkast § 2, nr. 2) udgår af lovforslaget. I forlængelse af TI's argumenter ovenfor pkt. 1 bemærker TI følgende vedrørende forslaget til ændring af § 31:

CPR/CVR/unikt ID
Det bemærkes, 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. reglen i teleloven § 31, stk. 1, medmindre kunden er registreret med hemmeligt eller udeladt nummer (HUA-markering), jf. § 31, stk. 4. Et krav om sådant videresalg af telekundernes CPR/CVR/ID er næppe tilsigtet.

TI er opmærksom på lovbemærkningerne i lovudkastet, hvor det følgende fremgår under punkt 3.8: *"Det bemærkes samtidig, at regler om videregivelse af oplysninger om det unikke ID forudsættes udmøntet i bekendtgørelsen om nummeroplysnings-databaser 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 CPR-numre*."

TI bemærker hertil, at ordlyden af selve bestemmelsen i TL § 31, stk. 1 og den foreslåede ændring til TL § 31, stk. 2 fører til den modsatte forståelse (nemlig at unikt ID indgår i nummeroplysningsdata, der skal videregives), og at en model, hvor lovregler fraviges i en underliggende bekendtgørelse, ikke synes hensigtsmæssig.

Telelovens § 31 implementerer artikel 112 i teledirektivet (2018/1972/EU) (og artikel 12 i eDatadirektivet), som kun vedrører nummeroplysningsdata i traditionel forstand (kundens navn, adresse og telefonnummer). Formålet med reguleringen, jf. artikel 112 i teledirektivet, er, at udbydere af nummeroplysningstjenester sikres adgang til nummeroplysningsdata i form af navn, adresse og telefonnummer. Indførelse af eventuelle regler om CPR-registrering med henblik på verificering af nummeroplysningsdata mv. bør derfor ikke indgå i Telelovens § 31, men kan mere hensigtsmæssigt ske via en selvstændig bestemmelse i Teleloven, jf. TI's forslag overfor i pkt. 1.B.

Registreret bruger
I forhold til forslaget om at lade "eventuel bruger" indgå i definitionen af "nummeroplysningsdata", jf. lovudkastets forslag til ændring af Telelovens § 31, stk. 2, vil også dette få den afledte konsekvens, at teleudbyderne vil blive forpligtede til at afgive op-

lysning om eventuel registreret bruger til "til alle, der ønsker det", jf. reglen i teleloven § 31, stk. 1 (medmindre kunden er registreret med hemmeligt eller udeladt nummer (HUA-markering), jf. § 31, stk. 4).

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. TL § 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 (d) 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.

1.D. Særligt om Taletidskort

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.

TI's betænkeligheder ved de foreslåede reglers betydning for udbuddet af taletidskort er uddybet i bilag 1 til dette høringssvar.

2. Målrettet person logning – politiet skal oplyse telefonnumre

Lovudkastets forslag til ny § 786 b og ny § 786 d om målrettet personbestemt logning samt bemærkningerne til de to bestemmelser lægger efter deres ordlyd op til, at bestemmelser og kendelser om målrettet personbestemt logning skal være rettet mod bestemte personer, og de nye regler og bemærkningerne hertil kan læses sådan, at teleudbyderne skal kunne iværksætte målrettet personbestemt logning alene baseret på oplysningen om en persons identitet.

Fx fremgår følgende på side 50 i lovudkastet (hvor fremhævelse):

"Myndighederne vil desuden skulle videreformidle oplysninger om, hvilke personer der skal foretages målrettet personbestemt registrering og opbevaring af trafikdata for efter de foreslåede regler i § 786 b i retsplejeloven til udbydere … med henblik på iværksættelse af målrettet registrering og opbevaring af trafikdata for de omfattede personer. Oplysningerne skal være tilstrækkelige til, at udbydere … kan iværksætte målrettet personbestemt registrering og opbevaring af trafikdata for de pågældende personer.

Myndighederne vil også skulle videreformidle retskendelser med konkret begrundede pålæg om målrettet registrering og opbevaring af trafikdata for konkrete personer indhentet efter den foreslåede § 786 d i retsplejeloven til udbydere …."

Endvidere fremgår følgende på side 159 i lovudkastet:

"Registrerings- og opbevaringspligten vil efter forslaget skulle gælde fra det tidspunkt, hvor udbydere … har modtaget tilstrækkelige oplysninger om de omfattede personer fra myndighederne til at iværksætte registrering og opbevaring målrettet de pågældende personer. "

Det er derimod ingen steder nævnt, hverken i forslag til ny § 786 b og ny § 786 d eller i bemærkningerne hertil, at teleudbydernes iværksættelse af målrettet personbestemt logning skal ske på baggrund af oplysning fra politiet om hvilke telefonnumre, der er omfattet af indgrebet.

TI gør opmærksom på, at det er af allerstørste vigtighed både praktisk og administrativt, at teleudbyderne ikke pålægges at iværksætte målrettet logning på baggrund af oplysning om fokuspersonens navn eller CPR-nummer. TI forudsætter således, at politiet selv, herunder ved opslag via 118-databasen (som indeholder oplysninger om telefonnummer, navn og adresse) og OCH, (som indeholder oplysning om telefonnummer og aktuel udbyder), finder frem til, hvilke telefonnumre der er registreret i tilknytning til fokuspersonen. Dertil kommer, at målrettet personbestemt logning ikke nødvendigvis knytter sig til fokuspersonens egne telefonnumre, men til andre kunders telefonnumre – fx andre registrerede kunder på fokuspersonens folkeregisteradresse (fx fokuspersonens ægtefælle) – som har overladt et abonnement til fokuspersonen, hvilket er en efterforskningsmæssig opgave at afdække. Det er derfor altid politiet – og ikke teleudbyderen – der må påtage sig ansvaret for at udpege hvilke telefonnumre mv., der skal iværksættes målrettet personbestemt logning for.

Fastholdes forslaget til § 786 b med ordlyden i lovudkastet, vil teleudbyderne blive pålagt en handlepligt, der ikke kan opfyldes af teleudbyderne uden politiets bistand. Overtrædelse af denne handlepligt er bødebelagt, jf. lovudkastets forslag til ny § 786 i. Lovudkastet kan således læses sådan, at teleudbyderne pålægges bøder, hvis teleudbyderne ikke selvstændigt udfører den efterforskningsmæssige opgave, der ligger i at afklare, hvilke numre og apparater en fokusperson anvender. Det vil selvsagt være en ganske uholdbar retstilstand, at telebranchen skal udføre efterforskningsarbejde

under bøderisiko – tilmed uden adgang til de værktøjer og adgange, som politiet har til rådighed til netop denne efterforskning, herunder politiets adgang til 118-databasen. Også derfor bør det fremgå af lovens ordlyd, at det er politiets ansvar at afklare, hvilke numre og apparater, som skal logges og at telebranchen opsætter målrettet logning efter anmodning fra politiet.

I forbindelse med TI's drøftelser med Justitsministeriet og Rigspolitiet i april 2021 ifm. lovskitsen var det en klar forståelse, at målrettet personbestemt logning kun skal iværksættes efter politiets oplysning om hvilke telefonnumre, der knyttes til fokuspersonen. Og også i Q&A til spørgeguide til den erhvervsøkonomiske analyse (AMVAB), som Erhvervsstyrelsen v. Deloitte rundsendte til teleudbyderne den 7. juli 2021 blev det anført, at udbyderne vil få en liste med numre:

> *"Spørgsmål 2: Under bemærkningerne til spørgsmål B1 om personbestemtlogning er det uklart om anmodningen om logning vil baseres på telefonnumre – kan det bekræftes, at processen vil være, at politiet angiver det telefonnummer der skal logges?*
> *Svar: Det kan bekræftes, at politiet til de 4 netværksudbydere vil levere oplysninger om, hvilke telefonnumre der skal være omfattet af målrettet personbestemt logning."*

TI anmoder om, at ovenstående eller tilsvarende fremgangsmåde præciseres i lovforslagets bemærkninger, 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.

Det bemærkes, at en proces, hvor telefonnummer skal oplyses ifm. iværksættelsen af et indgreb er helt normal praksis i sager om udlevering af teledata, jf. bl.a. ordlyden af RPL § 783:

> *"§ 783. Indgreb i meddelelseshemmeligheden sker efter rettens kendelse. I kendelsen anføres de telefonnumre, lokaliteter, adressater eller forsendelser, som indgrebet angår, jf. dog stk. 2. …*
> *Stk. 2. Angår efterforskningen en overtrædelse af straffelovens kapitel 12 eller 13 eller …, kan der i rettens kendelse i medfør af § 780, stk. 1, nr. 1 eller 3, ud over bestemte telefonnumre anføres den person, som indgrebet angår (den mistænkte). I så fald skal politiet snarest muligt efter udløbet af det tidsrum, inden for hvilket indgrebet kan foretages, underrette retten om de telefonnumre, som indgrebet har været rettet imod, og som ikke er anført i kendelsen."*

Det bemærkes desuden, at teleudbyderne ikke har adgang til den udtømmende nummerfortegnelse med samtlige numre i den samlede danske nummerplan, som er tildelt til slutkunder, inkl. hemmelige numre (118-databasen) – dvs. hverken tjenesteudbyderne, der sælger abonnementer til slutkunder, eller politigrupperne hos netværksoperatørerne, som yder praktisk bistand til politiet i det daglige, har adgang til 118-

databasen. 118-databasen er alene et værktøj, som stilles til rådighed for politiet (og andre myndigheder), jf. reglerne herom i telelovens § 14, stk. 2, nr. 4 og § 31, stk. 6.

TI henviser i øvrigt til pkt. 5 og pkt. 10 i TI's notat om svar på Justitsministeriets spørgsmål på 2. møde om revision af logningsreglerne (tekniske forhold og procedurer), fremsendt til Justitsministeriet den 27. april 2021[5], hvor TI detaljeret beskriver det proceduremæssige behov for, at pålæg om målrettet personbestemt logning indeholder oplysning om de konkrete telefonnumre, der skal logges.

TI forudsætter på denne baggrund, at teleudbyderne efter de nye regler om målrettet personbestemt logning kun pålægges at iværksætte logning på baggrund af en skriftlig anmodning eller rekvisition fra politiet med angivelse af det eller de konkrete telefonnumre, der skal være omfattet af målrettet personbestemt logning. TI forudsætter desuden, at politiets skriftlige anmodning enten indeholder henvisning til den relevante regel i den foreslåede nye § 786 b, eller indeholder henvisning til retskendelse efter den foreslåede nye § 786 d.

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 – fx ved tilføjelse af følgende stykke til de to bestemmelser:

> Stk. x. Iværksættelse af personbestemt målrettet registrering og opbevaring af trafikdata som nævnt i stk. 4 sker efter politiets pålæg herom til udbydere som nævnt i stk. 4. I pålægget anføres de telefonnumre eller kommunikationsapparater (imei), som indgrebet angår, samt hvilken bestemmelse i stk. 4 pålægget vedrører.

Se også pkt. 5 nedenfor med TI's yderligere konkrete forslag til tilføjelser i lovteksten.

Det bemærkes, at ordlyden af de foreslåede bestemmelser i § 786 b, stk. 4, nr. 2 og 3 ikke er hensigtsmæssig, da det sprogligt ikke giver mening af tale om "… trafikdata *fra personer*, der … har været genstand for indgreb [i meddelelseshemmeligheden]" hhv. "… trafikdata *fra personer*, der er indehavere af et kommunikationsapparat, der … har været genstand for indgreb …". Det er således ikke personen, der genererer trafikdata, men derimod den elektroniske kommunikation. TI foreslår, at der i stedet skrives "… trafikdata fra telefonnumre[6] 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

[5] Notatet findes på TI's hjemmeside: https://www.teleindu.dk/brancheholdninger/logning-og-teledata/

[6] Alternativt "nummerbaserede elektroniske kommunikationstjenester (telefonnumre)"

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.

3. Målrettet geografisk logning – kun mobiltjenester

TI anmoder om, at det præciseres i den nye regel i § 786 c om målrettet geografisk logning, at forpligtelsen kun omfatter udbydere af mobiltjenester, og at målrettet geografisk logning således kun omfatter logning af, hvilke mobiltelefonnumre der benytter mobilmasterne, som dækker et fokusområde. Det har således været en arbejdshypotese og forudsætning i alle drøftelser mellem telebranchen og Rigspolitiet og Justitsministeriet om mulige tekniske løsninger til målrettet geografisk logning, at regler og løsninger til målrettet geografisk logning kun omfatter mobiltjenester.

Denne forudsætning fremgår allerede af side 39 nederst i lovudkastet, hvor det er anført, at geografisk målrettet logning indebærer, at udbyderen skal udpege de master, som dækker fokusområdet og på den baggrund iværksætte målrettet geografisk logning af de mobilnumre, der benytter masterne i fokusområdet.

At de nye regler om målrettet geografisk logning umiddelbart kun kan omfatte trafikdata fra mobilnettet, følger endvidere af, at den parallelle udleveringsregel vedrørende politiets adgang til at indhente "oplysning om, hvilke telefoner eller tilsvarende kommunikationsapparater inden for et nærmere angivet område, der sættes i forbindelse med andre telefoner eller kommunikationsapparater" ('udvidet teleoplysning'), jf. RPL § 780, stk. 1, nr. 4, kun vedrører oplysning om, hvilke numre der har kommunikeret via masteceller, som dækker et fokusområde, samt kaldsdata for disse numre. Dette følger bl.a. af lovforslagsbemærkningerne til RPL § 780, stk. 1, nr. 4 om "udvidet teleoplysning" (lovforslag L194, fremsat 21. marts 2001). "Udvidet teleoplysning" blev således oprindeligt kaldt "masteoplysning" (dvs. oplysning om hvem der har kommunikeret via master, der dækker et fokusområde). Der findes derimod ingen udleveringsregler, der tager stilling til udlevering af teleoplysning fra fastnettelefoner i et givet område. Udlevering af teleoplysning for fastnet- og ip-telefonnummer bestilles af politiet efter kendelse pr. nummer.

Modsat mobilområdet, findes der ikke it-løsninger, der giver fastnetoperatørerne et samlet overblik over, hvilke fastnet- og ip-telefoner der findes i et geografisk område.

Hvis politiet har behov for at sikre logning af trafikdata for fastnettelefoner (herunder IP-telefoni med fast installationsadresse) i udvalgte geografiske områder (gader og steder), har politiet dog selv[7] mulighed for via opslag i 118-databasen at samle et

[7] Teleudbyderne har ikke adgang til den udtømmende nummerfortegnelser med samtlige numre i den samlede danske nummerplan, som er tildelt til slutkunder, inkl. hemmelige numre (118-databasen) – dvs. hverken tjenesteudbyderne, der sælger abonnementer til slutkunder, eller politigrupperne hos netværksoperatørerne, som yder praktisk bistand til politiet i det daglige, har adgang til 118-databasen. 118-databasen er alene et værktøj, som stilles til rådighed for politiet (og andre myndigheder), jf. reglerne herom i telelovens § 14, stk. 2, nr. 4 og § 31, stk. 6.

overblik over, om der leveres fastnet- eller ip-telefoni til adresser på de gader og veje, der findes i fokusområdet (installationsadresser). Og på baggrund af søgningen efter installationsadresser vil politiet herefter også via 118-databasen kunne finde frem til telefonnumrene og etablere en liste over fastnet- og ip-telefoni-telefonnumre med installationsadresse i fokusområdet. Hvis en sådan liste med fastnet- og IP-telefoni-telefonnumre gives til de relevante fastnetoperatører, vil fastnetoperatørerne kunne iværksætte målrettet geografisk logning for disse numre for både fastnetoperatørens egne numre og for gensælgere af operatørens tjeneste.

Det bemærkes, at hvis politiet ønsker at etablere en ordning til brug for målrettet geografisk logning af fastnet- og ip-telefonnumre, vil det desuden være nødvendigt, at politi og domstole også i kendelser om efterfølgende udlevering af trafikdata for sådanne numre (teleoplysning, jf. RPL § 780, stk. 1, nr. 3) angiver de telefonnumre, der er omfattet af kendelsen om udlevering. Også ift. udlevering er det således kun politiets adgang 118-databasen, der kan give et samlet overblik over fastnet- og ip-telefonnumre med installationsadresse i fokusområdet.

Samlet set anbefaler TI, at der ikke ændres på den hidtidige forudsætning om, at geografisk målrettet logning kun omfatter logning af, 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 videre 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 de 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.

4. Tidspunkt for iværksættelse af logning (frafiltrering af loggede 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, jf. princippet om dataretention, som er den engelske oversættelse af "logning" ("at bevare data som ellers skulle slettes"). Præciseringen kan fx ske ved tilføjelse af fx følgende nye stykke til de foreslåede § 786 a-786 e om hastesikring hhv. logning:

> Stk. x. Udbyderens forpligtelse til at registrere og opbevare trafikdata, som nævnt i § 786 b, § 786 c, § 786 d og § 786 e, indtræder på det tidspunkt, hvor udbyderen ellers ville slette data, og ophører [x måneder] efter kommunikationen har fundet sted.

TI anmoder i forlængelse heraf om, at følgende afsnit på side 48 i lovudkastet slettes:

> *"Endelig bemærkes det, 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, fra oplysninger, der ikke er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven, således at det er muligt også ved politiets adgang til data at tage højde for, om der er tale om oplysninger, der er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven, eller ej."*

Afsnittet vedrører Justitsministeriets forslag om frafiltrering af data på enkeltnummerniveau og er ikke nævnt andre steder i lovudkastet end på side 48. Forslaget var ikke en del af Justitsministeriets lovskitse i april 2021, og har heller ikke været en del af de tekniske drøftelser mellem telebranchen og Rigspolitiet om mulige tekniske løsninger til målrettet logning.

Forslaget 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[8], der registreres i teleudbydernes net til brug for fejl-

[8] Lokaliseringsdata (hvilke masteceller en mobilterminal har været registreret på) er kun delvist omfattet af de gældende logningsregler, og ifølge lovudkastet (side 13 og 46), skal denne ordning videreføres, således at der fortsat kun skal logges lokaliseringsdata ifm. brug af telefoni og sms. Hvis der eksempelvis foretages 3 opkald og 4 sms pr. dag, sker der ca. 10 registreringer af lokaliseringsdata/celle-ID for telefonen, som skal logges. Men til brug for fejlretning, kan teleudbyderne registrere alle lokaliseringsdata i en kort periode (fx 14 dage) – dvs. både ifm. telefoni-, sms- og data-kommunikation (brug af apps og internet), og i visse tilfælde også når telefonen er tændt, men ikke anvendes aktivt. Registreringen af lokaliseringsdata i fejlretningssystemerne sker kun efter "best effort". Antallet af registreringer af lokaliseringsdata i fejlretningssystemerne afhænger af antal aktive apps på telefonen samt telefonens geografiske bevægelse, og kan variere fra ca. 100 til over 1000 registreringer af celle-ID pr. telefonnummer pr. døgn. "Lokaliseringsdata" fra teleudbydernes fejlretningssystemer kan i dag kun udleveres til politiet som samlede udtræk, der omfatter alle registrerede lokaliseringsdata (for et nummer eller for et område). For yderligere fakta om registrering af lokaliseringsdata i mobilnettene henvises til TI's brev til Domstolsstyrelsen, marts 2021, som ligger på TI's hjemmeside: https://www.teleindu.dk/brancheholdninger/logning-og-teledata/

retningsanalyse, 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 i den i forvejen meget komplekse og kapacitetstunge it-løsning, der skal etableres hos teleudbyderne til brug for målrettet logning.

Til illustration af kompleksiteten i forslaget om frafiltrering kan gives følgende eksempel: Hvis politiet ifm. efterforskning af en sag, som ikke er grov kriminalitet, beder om udlevering af lokaliseringsdata/mastepositioner fra fejlretningssystemerne for en person, som er omfattet af krav om personbestemt logning, skal politiet efter forslaget om frafiltrering afskæres fra at få oplyst hvilke master personen benyttede ifm. eventuelle telefonopkald eller sms – men politiet skal ikke afskæres fra at få at oplyst masteposition ifm. personens brug af datakommunikation (brug af apps og internet). Hvis personen bevæger sig ind i et område omfattet af krav om målrettet geografisk logning, skal politiet efter forslaget om frafiltrering endvidere afskæres fra at få oplysning om alle registrerede mastepositioner for personen i logningsområdet.

Et andet eksempel kunne være, at politiet ifm. efterforskning af en sag, som ikke er grov kriminalitet, beder om få oplyst, hvilke telefoner der været registreret på mobilmaster, der dækker et fokusområde, hvor fokusområdet ikke samtidig er omfattet af krav om målrettet geografisk logning. I en sådan sag vil den foreslåede frafiltreringsmekanisme afskære politiet fra at få adgang til oplysninger om, hvorvidt en person omfattet af krav om personbestemt logning, har været registreret på en mast i fokusområdet, hvis personen eventuelt benyttede telefoni eller sms i fokusområde – men politiet skal ikke afskæres fra at få at vide, om personen har været registreret på samme mast, hvis personen benyttede sin telefon til datakommunikation (brug af apps og internet).

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, hvilket i begge tilfælde vil være problematisk, jf. "teledata-skandalen".

TI må på denne baggrund stærkt fraråde en frafiltreringsmekanisme og opfordrer til, at Justitsministeriet sletter afsnittet på side 48 i lovudkastet.

Telebranchen anser sig i øvrigt ikke 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,

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. Der findes ikke regler i gældende ret, der pålægger telebranchen en sådan byrde, jf. Telelovens § 10 modsætningsvis[9].

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 mv., 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 mv. i de mange domme om adgang til trafik- og lokaliseringsdata omfattet af logningspligt. Se også pkt. 6.2 nedenfor.

5. Klare regler om logning af teledata – hvilke udbydere – hvilke teletjenester – hvilke trafikdata

TI har længe efterlyst klarere og enklere regler om logning af teledata, jf. bl.a. TI's notat til Justitsministeriet fra februar 2020[10]. I forlængelse heraf anmoder TI om, at det tydeliggøres i lovforslaget, hvilke udbydere, hvilke tjenester og hvilke datatyper, der er omfattet af de nye regler, jf. nærmere herom nedenfor:

5.A. Hvem skal logge – hvilke udbydere (pligtsubjekt)?

Vedrørende spørgsmålet om pligtsubjekt fremgår følgende på side 34 og 59 i lovudkastet (svarende til § 7 i den gældende logningsbekendtgørelse):

> *"Hvis de omfattede oplysninger kan registreres af flere udbydere, skal oplysningerne registreres og opbevares af mindst én af udbyderne."*

Det følger desuden af § 10 i Teleloven (som ikke er nævnt i lovudkastet), at logningsforpligtelsen[11], mv. 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 på side 34 og 59 i lovudkastet og i gældende TL § 10 skaber således usikkerhed hos teleudbyderne om, hvem der er forpligtet til at sikre, at logning af trafikdata er en mulighed, jf. de foreslåede nye RPL §§ 786 b-786 e.

---

[9] Se lovforslagsbemærkninger til TL § 10 (tidligere TL § 15), jf. § 1, nr. 1 i L 219 fremsat 31. marts 2006 samt § 1, nr. 1 i L 63 fremsat 3. november 2006.

[10] Notat om logning og udlevering af teledata til politiet (TI's forslag og ønsker til ændring og præcisering af gældende regler), februar 2020. Notatet ligger på TI's hjemmeside https://www.teleindu.dk/brancheholdninger/logning-og-teledata/

[11] Jf. ændring af teleloven i 2006 – se fodnote 9.

”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, idet trafik- og lokaliseringsdata opstår i netværkene og behandles i netværkselementer, herunder centraler, og videregives kun delvist til ”udbydere af tjenester *til slutbrugere*” til brug for fakturering mv. Det er derfor ikke logisk, at det i Telelovens § 10 er anført, at forpligtelsen mv påhviler ”udbydere af elektroniske kommunikationsnet eller -tjenester *til slutbrugere*”. Det bemærkes, at tilføjelsen ”… til slutbrugere” ikke indgik i bestemmelsens oprindelige ordlyd (tidligere TL § 15), men blev tilføjet ved L 219 fremsat 31. marts 2006 uden nærmere begrundelse.

TI anmoder derfor om, at tilføjelsen ”… til slutbrugere” slettes i Telelovens § 10.

For at skabe klarhed om pligtsubjektet anmoder TI desuden om, at det præciseres i lovforslagsbemærkningerne, jf. side 34 og 59 i lovudkastet, 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.

En præcisering i lovforslagsbemærkningerne kunne fx ske ved at erstatte det ovenfor citererede afsnit på side 34 og 59 i lovudkastet med følgende tekst:

> Pligtsubjektet for registrering og opbevaring af trafikdata er de udbydere af elektroniske kommunikationsnet eller -tjenester, der producerer de elektroniske kommunikationstjenester, der genererer de registrerings- og opbevaringspligtige oplysninger (den tjenesteproducerende udbyder). Afhængig af, hvilken tjenestetype registrerings- og opbevaringspligten omfatter, er den tjenesteproducerende udbyder normalt følgende:
> - Udbydere, der er mobilnetværksoperatører, skal for mobiltjenester registrere og opbevare trafik- og lokaliseringsdata, der genereres og behandles i udbyderens net.
> - Udbydere, som er fastnettelefonioperatører med egne centraler, skal for nummerbaserede talekommunikationstjenester (fastnet- og IP-telefoni) registrere og opbevare trafikdata, der genereres og behandles i udbyderens net.
> - Udbydere, som er tildelt IP-adresser hos RIPE, skal for internetadgangstjenester registrere og opbevare oplysning om slutbrugeres adgang til internettet (kilde-IP-adresse mv.)
>
> På den anden side, er en aktør, der alene udbyder et elektronisk kommunikationsnet, som ikke genererer registrerings- og opbevaringspligtige oplysninger, ikke pligtsubjekt i forhold til bestemmelserne i loven. Det kunne f.eks. være en aktør, der alene udbyder infrastrukturen imellem en andens aktørs master.

> I forhold til kundedata (nummeroplysningsdata mv, som er registreret i kunderegistre hos tjenesteudbyderne), vil pligtsubjektet være de ca. 100 tjenesteudbydere og gensælgere, som udbyder abonnementer til slutbrugerne.

Med ovennævnte præcisering, vil det stå klart, at det primært er netværksoperatørerne og de udbydere, der driver centralerne, herunder de fire store danske mobilnetværkoperatører 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.

Det bemærkes, at det kan slås op i OCH for hvert aktive telefonnummer i den danske nummerplan, hvem der er netværksoperatør, hhv. hvem der er tjenesteudbyder til slutbrugeren (sidstnævnte kaldes "serviceoperatør" i OCH).

TI anmoder om, at der for at undgå enhver tvivl om, at det er den tjenesteproducerende udbyder, der er forpligtet til at varetage logning af de logningspligtige oplysninger, tilføjes en overordnet bestemmelse i lovforslaget, som fastslår, at det er de udbydere, der producerer de elektroniske kommunikationstjenester, der genererer de registrerings- og opbevaringspligtige oplysninger, der er forpligtet til at foretage logning (den tjenesteproducerende udbyder).

Et forslag til en bestemmelse kunne fx være følgende:

> § Y. §§ 786 b-786 f gælder kun for udbydere, der producerer de elektroniske kommunikationstjenester, der genererer de registrerings- og opbevaringspligtige oplysninger.

Vi henviser desuden til TI's brev den 16. juni 2021[12] til Justitsministeriet og Energistyrelsen for en uddybning af problemstillingen vedrørende pligtsubjekt, idet vi dog bemærker, at anvendelsen af betegnelsen "den dataansvarlige udbyder" kan skabe forvirring, da der potentielt kan være flere dataansvarlige. TI foreslår derfor i stedet, at betegnelsen "den tjenesteproducerende udbyder" anvendes, jf. forslaget til tekst i lovbemærkningerne ovenfor.

I tilknytning til ovennævnte bemærkes, at begrebet "den dataansvarlige" på side 153 og 197 i lovudkastet om udlevering af data tilsvarende bør rettes til følgende (ændringsforslag markeret):

> *"Anmodning om adgang til registrerings- og opbevaringspligtige oplysninger vil efter den foreslåede bestemmelse skulle rettes til den <u>tjenesteproducerende</u> ~~dataansvarlige~~ udbyder*".

[12] TI's brev af 16. juni 2021 om pligtsubjekt findes på TI's hjemmeside: https://www.teleindu.dk/brancheholdninger/logning-og-teledata/

Forslag til forenklet henvisning til teleloven – erhvervsmæssige udbydere
Det fremgår mange steder i både lovteksten og bemærkningerne til lovforslaget, at pligtsubjektet i forhold til reglerne om målrettet logning er "… *udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden …*". Teksten er en gengivelse af definitionen af 'erhvervsmæssig udbyder' i telelovens § 2, nr. 2.

Den omfattende brug af definitionen gør læsning af lovforslaget ganske vanskelig. TI foreslår derfor, at der i stedet indsættes en bestemmelse, som definerer pligtsubjektet for §§ 786 b-d, hvorefter pligtsubjektet kan omtales som "… udbydere af elektroniske kommunikationsnet eller -tjenester" i lovforslaget.

Et forslag til en bestemmelse kunne fx være følgende:

> § X. §§ 786 b-786 d [om målrettet registrering og opbevaring af trafikdata] gælder kun for erhvervsmæssige udbydere af elektroniske kommunikationsnet eller -tjenester, jf. lov om elektroniske kommunikationsnet og -tjenester § 2, nr. 2.

TI bemærker desuden, at der formentlig kun findes ganske få (måske slet ingen) eksempler på ikke-erhvervsmæssige udbydere, der udbyder fastnet- og mobiltelefoni og dermed omfattet af de foreslåede §§ 786 b-786 d om målrettet logning. Ikke-erhvervsmæssige udbydere, som fx hoteller og campingpladser, udbyder således som nævnt i lovudkastet side 33 primært internetadgangstjenester (hotspots), som ikke er omfattet af reglerne om målrettet logning af trafik- og lokaliseringsdata, men derimod kun omfattet af den foreslåede nye § 786 f om generel logning af kilde-IP-adresser (som ikke-erhvervsmæssige udbydere ifølge lovudkastet ikke er undtaget fra).

5.B. Hvad skal logges – hvilke teletjenester?
Det er ikke beskrevet hverken i de foreslåede §§ 786 b-786 f eller bemærkningerne hertil, 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 (jf. nærmere herom nedenfor pkt. 5.C), som er omfattet af de gældende regler i logningsbekendtgørelsen.

Det fremgår af de gældende regler i logningsbekendtgørelse, at § 4 i bekendtgørelsen vedrører telefonitjenester, herunder mobiltelefoni, samt sms/mms-kommunikation, og at § 5 vedrører internetadgangstjeneste.

TI anmoder om, at det på samme måde i de foreslåede nye regler i §§ 786 b-786 f tydeligt anføres, hvilke teletjenester – og dermed hvilke udbydere – reglerne omfatter.

En præcisering i lovteksten kunne fx være følgende (forslag til den nævnte § 786 x findes nedenfor i pkt. 5.C):

Ad § 786 b – målrettet personbestemt logning:

> Stk. 4. Det påhviler [udbydere af elektroniske kommunikationsnet eller -tjenester] at foretage personbestemt målrettet registrering og opbevaring af trafikdata, som nævnt i § 786 x, om fastnet- og mobiltelefoni samt sms-kommunikation[13] [fra telefonnumre eller kommunikationsapparater (imei), der benyttes af personer, der har været genstand for indgreb i meddelelseshemmeligheden] …

Ad § 786 c – målrettet geografisk logning:

> Stk. 2. Det påhviler [udbydere af elektroniske kommunikationsnet eller -tjenester] at foretage geografisk målrettet registrering og opbevaring af trafikdata, som nævnt i § 786 x, om mobiltelefoni samt sms-kommunikation [foretaget fra telefonnumre eller kommunikationsapparater (imei) i særligt sikringskritiske områder, såsom …

Ad § 786 d – målrettet logning efter kendelse:

> § 786 d. Der kan meddeles [udbydere af elektroniske kommunikationsnet eller -tjenester] pålæg om at foretage målrettet registrering og opbevaring af trafikdata, som nævnt i § 786 x, om fastnet- og mobiltelefoni samt sms-kommunikation …

Ad § 786 e – generel og udifferentieret logning efter kendelse:

> § 786 e. Justitsministeren kan efter forhandling med erhvervsministeren fastsætte regler, der pålægger udbydere af elektroniske kommunikationsnet eller -tjenester at foretage generel og udifferentieret registrering og opbevaring af trafikdata, som nævnt i § 786 x, om fastnet- og mobiltelefoni samt sms-kommunikation …, 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.

Ad § 786 f - generel logning af kilde-IP-adresser:

> § 786 f. Det påhviler udbydere af internetadgangstjenester, jf. art. 2, andet afsnit, nr. 2 i forordning (EU) 2015/2120, at foretage generel og udifferentieret registrering og opbevaring af oplysninger om en slutbrugers adgang til internettet, jf. § 786 x, stk. 2.

[13] Alternativt: "… nummerbaseret talekommunikation samt sms-kommunikation

5.C. Hvad skal logges – hvilke trafikdata?
Det er ikke anført i de foreslåede lovtekster i §§ 786 b–786 e, hvilke typer af trafikdata, der er omfattet af logningsforpligtelsen. Det fremgår således blot i de fire bestemmelserne, at det påhviler udbyderne at foretage registrering og opbevaring af "trafikdata". Rækkevidden af teleudbydernes forpligtelse er således ikke klart beskrevet i reglerne.

Som beskrevet flere steder i lovforslagsbemærkninger dækker begrebet "trafikdata" over en lang række typer af data, herunder lokaliseringsdata ifm. kundens mobildatakommunikation (internetadgang fra mobilen). Af bemærkningerne til lovforslaget (bl.a. side 47 i lovudkastet) fremgår det, at sidstnævnte datatype *ikke* er omfattet af logningskravet.

Det bemærkes, at der i de specifikke bemærkninger til lovudkastet, s. 159 (og tilsvarende på side 176 og side 46), fremgår følgende:

> *"Det foreslås således, at der kan iværksættes målrettet registrering og opbevaring for alle typer trafikdata.*
> *Begrebet trafikdata skal forstås i overensstemmelse med e-databeskyttelsesdirektivets artikel 2, litra b og c. Ved trafikdata forstås data, som behandles med henblik på overførsel af kommunikation i et elektronisk kommunikationsnet eller debitering deraf."*

Det citerede kan læses således, at målrettet logning (kan) udvides til at omfatte al trafikdata, hvilket omfatter meget mere og andet end "[…] de data, der er registrerings- og opbevaringspligtige i dag", som fremgår af samme side i lovudkastet. Dette skaber betydelig uklarhed omkring omfanget af registrerings- og opbevaringsforpligtelsen, såfremt den logningspligtige data ikke fastlægges entydigt.

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. De præcise regler om, hvilke datatyper, der skal logges, er således en vigtig retsakt i forhold til fastlæggelsen af teleudbydernes forpligtelse til at indrette tekniske systemer til logning af trafikdata og bør derfor fremgå eksplicit af teksten i reglerne.

Konkret anmoder TI om, at der enten tilføjes en regel om afgrænsningen af logningspligtige trafikdata som ny regel direkte i lovforslaget, eller alternativt, at der indsættes hjemmelsbestemmelse i §§ 786 b, 786 c, 786 d, 786 e og 786 f til at udstede en ny "logningsbekendtgørelse", hvor afgrænsningen af de logningspligtige datatyper oplistes, svarende til §§ 4 og 5 i den gældende logningsbekendtgørelse.

En præcisering kunne fx være følgende:

§ 786 x. Registrerings- og opbevaringspligten som nævnt i § 786 b-§ 786 e omfatter følgende typer af trafikdata om fastnet- og mobiltelefoni samt sms- og mms-kommunikation:
1) opkaldende nummer (A-nummer),
2) opkaldte nummer (B-nummer),
3) ændring af opkaldte nummer (C-nummer),
4) kvittering for modtagelse af meddelelser,
5) identiteten på det benyttede kommunikationsudstyr (IMSI- og IMEI-numre),
6) Registreret celle ved mobiltelefoni- og sms-kommunikation (lokaliseringsdata)[14], samt de tilhørende masters præcise geografiske eller fysiske placering på tidspunktet for kommunikationen,
7) tidspunktet for kommunikationens start og afslutning.

Stk. 2 Registrerings- og opbevaringspligten som nævnt i § 786 f, omfatter følgende typer af trafikdata om internetadgangstjenester[15]:
1) den tildelte brugeridentitet, herunder den anvendte offentlige IP-adresse (kilde), samt portnummer (kilde), hvis den tildelte IP-adresse, er tildelt flere abonnenter samtidig,
2) identifikation af det benyttede abonnement, fx telefonnummer, som identificerer det benyttede mobilabonnement ved internetadgang via mobildatatjenester, eller ID-nummer (fx kredsløbsnummer), som identificerer det benyttede bredbåndsabonnement ved internetadgang via faste net,
3) tidspunktet for tildelingen af brugeridentitet,
4) navn og adresse på abonnenten eller den eventuelle registrerede bruger.

Stk. 3 Registrerings- og opbevaringspligten som nævnt i § 786 xx, omfatter følgende typer af trafikdata om mobiltjenester:
[se pkt. 5.C.1 nedenfor med liste med 'IMEI-oplysning']

Det bemærkes, 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/nummeroplysningsdata 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.

[14] Se nedenfor pkt. 5.C.2 og 5.C.3 om baggrund for forslag til ændret formulering ift. § 4 i logningsbekendtgørelsen.

[15] Se pkt. 3.3 i TI's notat om logning og udlevering af teledata, feb 2020, om baggrunden for forslaget til ændret formulering ift. § 5 i logningsbekendtgørelsen. Notatet ligger på TI's hjemmeside https://www.teleindu.dk/brancheholdninger/logning-og-teledata/

5.C.1. Særligt om logning af IMEI-oplysninger
TI har hidtil fortolket det gældende krav i logningsbekendtgørelsen § 4, nr. 5 om logning af "identiteten på det benyttede kommunikationsudstyr" således, at der – ud over sammenhængen mellem IMEI, IMSI, telefonnummer *og* kommunikation (i form af opkald/sms) – desuden logges trafikdata om sammenhængen mellem IMEI og IMSI og telefonnummer *uden* samtidig registrering af kommunikation. Sidstnævnte sammenhæng kaldes "IMEI-oplysning", det vil sige 'oplysning om hvilke mobilabonnementer, der har været anvendt til en mobilterminal og omvendt', og kan bl.a. benyttes til sporing af stjålne mobilterminaler.

Til brug for "IMEI-oplysning" er det således normal praksis hos mobilnetværksudbyderne at logge følgende data i en særskilt tabel med unikke kombinationer af følgende trafikdata fra mobilnetværket:

- Telefonnummer
- IMSI (sim-kortnummer)
- IMEI (terminalens unikke nummer)
- Timestamp for første gang, hvor kombinationen af de 3 ovenstående numre er registreret i mobilnetværket.
- Timestamp for seneste tidspunkt, hvor kombinationen af de 3 ovenstående numre er registreret i mobilnetværket.

Når sammenhængen mellem IMEI og telefonnummer er fundet, kan politiet via 118-databasen finde sammenhængen mellem telefonnummer og slutbrugerens navn/adresse (nummeroplysningsdata).

"IMEI-oplysning" opsamles generelt, dvs også i de tilfælde, hvor en telefon anvendes til datakommunikation (men som nævnt sker opsamlingen uden samtidig registrering af kommunikationen). Det bemærkes, at datakommunikation via apps i dag er den primære form for kommunikation via mobilterminaler. Hvis IMEI-oplysning kun opsamles for telefoner, der anvendes til tale og sms, vil der fremover ikke blive registreret IMEI-oplysning for terminaler, som kun anvendes til datakommunikation.

TI bemærker, at det følger af Ministerio Fiscal-dommen, at politiets adgang til trafikdata i form af "IMEI-oplysning", udgør en indgreb, der ikke er så alvorligt, at politiets adgang skal begrænses til sager om grov kriminalitet (se også pkt. 6.D nedenfor om udlevering af IMEI-oplysning).

TI anbefaler på denne baggrund, at det overvejes at fastsætte en selvstændig regel (§ 786 xx) 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 logning 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.

5.C.2. Lokaliseringsdata for internetadgang/datakommunikation (MMS)
TI har noteret lovudkastets afgrænsning af, at lokaliseringsdata/masteoplysninger ved internetadgang fra mobiltelefoner (datakommunikation) ikke er omfattet af krav om logning (side 47 i lovudkastet).

Lokaliseringsdata/masteoplysninger ved internetadgang fra mobiltelefoner registreres kun i teleudbydernes analysesystemer til brug for fejlretning (prober). 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 (CDR – Call detail record).

For MMS-kommunikation, som er omfattet af de gældende logningsregler, registreres følgende trafikdata i CDR: A-nummer, B-nummer og tidsstempling. I CDR registreres der ikke lokaliseringsdata (Celle-ID) ved MMS-kommunikation. Dette skyldes, at MMS-kommunikation er datakommunikation (brug af internettet).

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.

5.C.3. Første og sidste mast ved mobiltelefoni
I opremsningen på side 47 i lovudkastet over 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, som er fra 2006. 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 datatrafik), 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 af basere logning på CDR-data (som beskrevet ovenfor pkt. 5.C.2), anmoder TI konkret om, at teksten om registrering af lokaliseringsdata ifm. mobiltelefoni og sms formuleres enkelt og teknologineutralt på følgende måde (se også samlet forslag i pkt. 5.C. ovenfor):

> "Registreret celle ved mobiltelefoni- og sms-kommunikation (lokaliseringsdata)"

5.C.4. e-mailadresser
TI bemærker, at det ikke giver mening at inddrage e-mailadresser i afgrænsningen af trafikdata, som telefoni-udbyderne skal logge, jf. pkt. 8 og 9 i opremsningen over logningspligtige trafikdata på side 13 og side 46 i lovudkastet. Kravet om logning af mailadresse efter § 6 i 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 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 lovgivningen.

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 om logning af kilde-IP-adresser, som også retter sig mod udbydere af internetadgangstjenester.

5.D. Slutbrugeres indsigtsret i loggede trafikdata
Spørgsmålet om slutbrugernes indsigtsret i trafikdata, som er logget efter reglerne om målrettet logning, er ikke 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 – fx med en tilføjelse på side 51, hvor spørgsmålet om aktindsigt behandles.

I bilaget pkt. C findes en uddybning af TI's bekymring for sammenstødet mellem lovforslaget og de registreredes grundlæggende databeskyttelsesretlige rettigheder.

6. Klare og enkle regler om udlevering af teledata
TI har længe efterlyst klarere og enklere regler om udlevering af teledata, jf. bl.a. TI's notat til Justitsministeriet fra februar 2020[16], hvor TI bl.a. 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:

a. **Masteoplysning**: Oplysning om, hvilke masteceller ét fokusnummer har været registreret på (dvs. registrerede lokaliseringsdata om et bestemt nummer). Antallet

[16] Notat om logning og udlevering af teledata til politiet (TI's forslag og ønsker til ændring og præcisering af gældende regler), februar 2020. Notatet ligger på TI's hjemmeside https://www.teleindu.dk/brancheholdninger/logning-og-teledata/

af registreringer af lokaliseringsdata i teleudbydernes fejlretningssystemer afhænger af antal aktive apps på telefonen samt telefonens geografiske bevægelse, og kan variere fra ca. 100 til over 1000 registreringer af celle-ID pr. telefonnummer pr. døgn.

b. **Udvidet masteoplysning**: Oplysning om, hvilke numre, der har været registreret på masteceller, som dækker et fokusområde.
c. **Udvidet IP-adresse-oplysning**: Oplysning om telefonnumrene bag en mobil dynamisk IP-adresse, hvor politiet ikke har oplysning om portnummer (op til 1000 samtidige brugere).
d. **IMEI-oplysning**: Oplysning om, hvilke mobilabonnementer der har været anvendt til en mobilterminal og omvendt.

TI beklager derfor, at lovudkastet nu lægger op til endnu mere komplicerede regler om udlevering af teledata end nogensinde før – og uden at imødekomme TI's ønske om klare og enkle regler.

6.A. Udlevering af trafikdata, som er "teleoplysning" – ny § 781 a

TI finder det besynderligt, at der i lovudkastets forslag til ny § 781a 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 endnu mere komplekse end i dag.

Uanset reglerne om logning, opbevarer teleudbyderne trafikdata om telekunders tale- og sms/mms-kommunikation (samtalelister med opkald/tilkald/sms/mms) til brug for fakturering og samtrafikafregning i mindst 1 år, jf. bogføringslovens regler herom, og sådanne trafikdata udleveres til politiet efter kendelse om teleoplysning efter de gældende regler om indgreb i meddelelseshemmeligheden, som er vedtaget længe før de gældende regler om logning.

TI opfordrer til, at Strafferetsplejeudvalget inddrages i overvejelsen om, hvorvidt der skal gælde særlige regler for politiets adgang til teleoplysning og udvidet teleoplysning, hvis der er tale om loggede trafikdata.

6.B. Udlevering af lokaliseringsdata – ny § 804 a

TI finder det positivt, at der med lovudkastets forslag til ny § 804 a fastsættes rammer for udlevering af 'masteoplysning' og 'udvidet masteoplysning', jf. ovenfor litra a og b, 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, jf. nærmere herom lovudkastets side 117 (og side 122), hvor følgende fremgår:

> *"Politiet vil efter forslaget fortsat kunne få adgang til ikke-registrerings- og opbevaringspligtige oplysninger samt dynamiske IP-adresser mv. efter de gældende regler om edition, dvs. uden at der stilles krav om, at politiet skal anvende oplysningerne til bekæmpelse af grov kriminalitet, herunder beskyttelse af den nationale sikkerhed."*

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 RPL § 804. TI bemærker til støtte herfor, at definitionen af tvangsindgreb som 'teleoplysning, jf. RPL § 780, stk. 1, nr. 3 og 'udvidet teleoplysning', jf. RPL § 780, stk. 1, nr. 4, således er blevet defineret i retsplejelovens kapitel 71 længe før logningsreglerne blev til. Trafikdata og lokaliseringsdata indeholder desuden altid elementer, der enten indgår i meddelelseshemmeligheden, eller er fortrolige oplysninger om brugerens geografiske færden.

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 heller 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 (fremadrettede lokaliseringsdata), jf. retsplejelovens § 791a, stk. 5.

TI opfordrer til, at Strafferetsplejeudvalget inddrages i overvejelsen om, hvorvidt der bør gælde samme regler og samme kriminalitetskrav for udlevering af loggede og hastesikrede lokaliseringsdata hhv. lokaliseringsdata, som ikke er omfattet af logningskrav.

6.C. Udlevering af loggede kilde-IP-adresser – ny § 804 a

Den foreslåede nye § 804 a, hvorefter loggede data kun kan udleveres til politiet i sager om efterforskning af grov kriminalitet, omfatter ikke loggede kilde-IP-adresser, idet den nye § 786 f om generel og udifferentieret logning af kilde-IP-adresser ikke er nævnt i opremsningen i lovudkastets nye § 804 a. Baggrunden herfor er Justitsministeriets fortolkning af La Quadrature du Net-dommens præmis 152-159, som gennemgås på side 63-67 i lovudkastet (pkt. 3.3.3.) samt side 117 midtfor, 119 nederst, side 125 nederst. Centralt for Justitsministeriets fortolkning er præmis 153, som nævner "sporing af en internetbrugers søgemønster".

TI er ikke umiddelbart enig i JM's fortolkning, og TI anmoder Justitsministeriet om at genoverveje fortolkningen.

Det er TI's opfattelse, at den omtalte sporing i præmis 153 vedrører sporing af IP-adresser tilbage til kilden, og at præmis 152-156 *ikke* vedrører sessionslogning, som JM overvejer på side 66 i lovudkastet (præmis 153 nævner slet ikke sessioner). Det bemærkes desuden, at afsnittet i La Quadrature du Net-dommen med præmis 152-159 omfatter to separate dele: Først en del om kilde-IP-adresser (præmis 152-156) og dernæst en del om civile identitetsoplysninger (præmis 157-158). Opdelingen i disse to dele fremgår desuden af domskonklusionerne, hvor det tillige tydeligt fremgår, at oplysning om kilde-IP-adresser kun må logges med henblik på bekæmpelse af grov kriminalitet (vor fremhævelse):

> *"Artikel 15, stk. 1, i direktiv 2002/58 … er derimod ikke til hinder for lovgivningsmæssige foranstaltninger … – der med henblik på beskyttelse af den nationale sikkerhed, bekæmpelse af grov kriminalitet og forebyggelse af alvorlige trusler mod den offentlige sikkerhed foreskriver generel og udifferentieret lagring af de IP-adresser, der er tildelt kilden til en forbindelse, i en periode, der er tidsmæssigt begrænset til det strengt nødvendige"*

Eftersom loggede data om kilde-IP-adresser ifølge Justitsministeriets gennemgang i lovudkastet netop bruges til efterforskning af grov kriminalitet (børneporno mv), finder TI 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 RPL § 804 (dvs uden særlige kriminalitetskrav).

TI bemærker, at ved internetadgang fra mobile datatjenester (og i visse tilfælde også fastnet bredbånd) er der mangel på dynamiske IP-adresser (IPv4), og derfor tildeles abonnenten både et portnummer og en dynamisk afsender-IP-adresse, som "oversættes" via NAT (Network Address Translation). Brugen af NAT indebærer, at én dynamisk IP-adresse kan deles mellem flere brugere – typisk flere end tusinde brugere pr. sekund. Kombinationen af dynamisk IP-adresse og portnummer identificerer entydigt abonnenten. Hvis portnummer derimod ikke kan oplyses, er der typisk flere end 1000 brugeridentiteter (mobiltelefon-numre) pr. dynamisk IP-adresse pr. sekund.

Teleselskaberne har det seneste år oplevet, at politiet i stigende omfang anmoder retten om efter reglerne om edition at pålægge teleselskaberne at udlevere oplysning om, hvem der er registreret som brugere af mobile dynamiske IP-adresser på et bestemt tidspunkt angivet med sekunds nøjagtighed – men uden at politiet har oplysning om portnummer. I disse sager har teleselskaberne hidtil udleveret oplysning om de mere end 1000 brugeridentiteter (mobiltelefonnumre), som har benyttet den mobile dynamiske IP-adresse på det oplyste tidspunkt.

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 præmis i dom 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 RPL § 786 f.

Fastholdes forslaget, opfordrer TI til, at Strafferetsplejeudvalget inddrages i overvejelsen om, hvorvidt der bør gælde samme regler og samme kriminalitetskrav for udlevering af loggede kilde-IP-adresser, som der gælder for udlevering af øvrige loggede data.

6.D. Udlevering af IMEI-oplysning – § 804

TI vil gerne kvittere for lovudkastets præcisering af kategoriseringen af IMEI-nummer på side 47 i lovudkastet:

> *"Med benævnelsen af identiteten på det benyttede kommunikationsudstyr (f.eks. IMSI- og IMEI-numre) i opremsningen ovenfor (nr. 5), sigtes der til oplysninger om identiteten på det benyttede kommunikationsudstyr (f.eks. IMSI- og IMEI-numre), når de genereres i forbindelse med trafik (som trafikdata, der er registrerings- og opbevaringspligtige i medfør af de foreslåede §§ 786 a-786 e). Det bemærkes imidlertid, at identiteten på det benyttede kommunikationsudstyr (f.eks. IMSI- og IMEI-numre) vil kunne udleveres efter den foreslåede § 804 b, stk. 1, hvis sådanne oplysninger ikke er registreret og opbevaret som trafikdata i medfør af de foreslåede §§ 786 a-786 e. Det vil således være en forudsætning for udlevering efter den foreslåede § 804 b, stk. 1, at udbyderne af elektroniske kommunikationsnet eller -tjenester er i besiddelse af oplysningerne på andet grundlag. Der henvises til pkt. 3.7.4."*

TI beder dog om, at teksten på side 47 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, nemlig de situationer, hvor oplysning om IMSI- og IMEI-nummer findes registreret som *kundedata* i tjenesteudbydernes kundeordresystemer (kundedatabaser og salgssystemer). Det drejer sig reelt om følgende situationer:

> (a) For tjenesteudbydere, der sælger mobilabonnementer, findes sim-kortets nummer (IMSI) registreret i tjenesteudbyderens kundedatabase.
> (b) For tjenesteudbydere, der sælger mobilterminaler, kan udbyderen vælge at registrere terminalens IMEI-nummer som serienummer i en tjenesteudbyders salgssystem.

Det bemærkes, at kundedata af typen (a) og (b) ikke kan bruges til at give 'oplysning om hvilke mobilabonnementer, der har været anvendt til en mobilterminal og omvendt' ("IMEI-oplysning"), idet sådan sammenhæng kun kan findes i trafikdata.

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 (som nævnt i teksten på side 47) eller trafikdata, som ikke er omfattet af krav om logning.

Som TI har beskrevet i pkt. 5.C.1. ovenfor, er trafikdata i form "IMEI-oplysning" i dag udelukkende baseret på generel logning af trafikdata, som viser sammenhængen mellem IMEI og IMSI og telefonnummer. Det følger af Ministerio Fiscal-dommen, at politiets adgang til trafikdata i form af sådan "IMEI-oplysning" (dvs uden at vise sammenhængen med terminalens kommunikation eller lokalisering), udgør et indgreb, der ikke er så alvorligt, at politiets adgang skal begrænses til sager om grov kriminalitet.

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, at disse regler ikke finder anvendelse for "IMEI-oplysning".

6.E. Den foreslåede § 804 b (overførsel af telelovens § 13 til retsplejeloven)

Det bemærker, at det ud fra lovteksten og de tilhørende bemærkninger ikke umiddelbart er muligt for TI at forstå indholdet af den foreslåede nye § 804 b, som skal overføre Telelovens § 13 til retsplejeloven.

TI anmoder om, at det anføres direkte i lovteksten i den foreslåede § 804 b, 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 TL § 13, hvilket teleudbyderne bruger mange ressourcer på at måtte afvise.

TI anmoder om, at præcisering om, at den foreslåede § 804 b ikke omhandler trafikdata, tilføjes til bestemmelsens stk. 2 – fx med følgende tekst (tilføjelse markeret):

> § 804 b. …
> Stk. 2. Oplysninger om <u>trafikdata, herunder trafikdata</u> som opbevares som følge af §§ 786 a-786 f, er ikke omfattet af stk. 1.

TI anmoder desuden om, at det – i lighed med bemærkningerne til Telelovens § 13 – præcisere i lovforslagsbemærkningerne til den foreslåede nye § 804 b, 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 bemærker, at teksten i lovudkastets bemærkninger til den foreslåede nye § 804 b på side 198-201 giver helt modsatrettede informationer om kategoriseringen af IMEI-oplysning end det ovenfor i pkt. 6.D citerede afsnit fra side 47 i lovudkastet.

Det samme gælder gennemgangen på side 117-119 af Telelovens § 13 i relation til IMEI-oplysning, som også giver helt modsatrettede informationer om kategoriseringen af IMEI-oplysning end det ovenfor i pkt. 6.D citerede afsnit fra side 47 i lovudkastet. TI bemærker, at TL § 13 netop *ikke* omfatter IMEI-oplysning, som er baseret på trafikdata opsamlet i mobilnettene.

Teksterne på side 117-119 og på side 199-201 efterlader stor tvivl og ingen afklaring af, hvad indholdet af den foreslåede nye regel i § 804 b er. TI opfordrer til, at teksterne på side 117-119 og side 199-201 udgår i deres helhed og erstattes af tydelige beskrivelse af, hvad reglen går ud på. TI foretrækker og opfordrer til, at lovforslagsbemærkninger til den gældende TL § 13 blot gentages som bemærkninger til den foreslåede § 804 b 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).

TI bemærker, at teksten på side 199-201 kan læses sådan, at politiet gives adgang til trafikdata om sammenhæng mellem IMEI, IMSI og telefonnummer, som mobilnetværksudbyderne registrerer i kort tid til brug for fejlretning (fx 14 dage), og hvor eventuel logningsforpligtelse først indtræder på det tidspunkt, hvor udbyderen ellers ville slette data (jf. pkt. 4 ovenfor). Trafikdata nævnes dog ikke teksten. TI må stærkt fraråde enhver form for overvejelse om at fastsætte regler ved lov om adgang til trafikdata uden kendelse, idet trafikdata er omfattet af de skærpede behandlingsregler og hensyn til privatlivsbeskyttelse, som følger af e-datadirektivet (2002/58/EF). Hvis det er hensigten med den foreslåede § 804 b, at politiet som noget nyt skal have adgang uden kendelse til sådanne oplysninger, opfordrer TI til, at det gøres fuldstændigt tydeligt både i lovteksten og i bemærkningerne at der tilsigtes en ændring af gældende ret, så der ikke hersker nogen som helst tvivl i den politiske proces om, hvad forslaget går ud på.

Teksten på side 125 under overskriften "telelovens § 13" anfører også fejlagtigt, at IMEI-oplysning er omfattet af den gældende bestemmelse i Telelovens § 13. I lovudkastet på side 125 nederst er det anført, at IMEI-oplysning, som er omfattet af logningspligt, kan indhentes af politiet efter den almindelige regel om edition i retsplejelovens § 804. Det anførte skaber igen tvivl om, hvad hensigten med den foreslåede nye § 804 b er. Teksten på side 125 bør ændres og tydeliggøres. Det samme gælder side 154 øverst.

TI henviser i øvrigt til TI's høringssvar[17] den 11. august 2020 til udkast til ændring af Telelovens § 13, hvor TI også redegjorde for behovet for klarhed i regeludstedelsen om politiets adgang til IMEI-oplysning.

7. Hastesikring – domstolsprøvelse og periodeafgrænsning

7.A. Hastesikring – domstolskontrol

Følgende fremgår på side 90 i lovudkastet vedrørende den foreslåede ændring af RPL § 786 a om hastesikring:

> *"Justitsministeriet har også overvejet, om der skal indføres et krav om forudgående retskendelse i forbindelse med hastesikring. Det er Justitsministeriets vurdering, at der i EU-Domstolens praksis stilles krav om en effektiv prøvelse af hastesikring, men at denne ikke behøver at være forudgående, jf. La Quadrature du Net-dommens præmis 163. Oplysninger, som er sikret i medfør af reglerne om hastesikring, vil politiet efter gældende ret kunne få adgang til efter de relevante regler i retsplejeloven Denne adgang vil som hovedregel kræve forudgående retskendelse. Der henvises til pkt. 3.7 vedrørende adgang til oplysninger."*

TI bemærker hertil, 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). I forhold til denne praksis, vil den på side 90 nævnte efterfølgende domsstolskontrol af indgreb i form af hastesikring ikke finde sted.

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.

7.B. Hastesikring – afgrænsning af periode

TI finder, at det er betænkeligt, at der efter den foreslåede ændring til RPL § 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.

[17] *https://www.teleindu.dk/brancheholdninger/horingssvar/

TI opfordrer til, at den foreslåede ændring af RPL § 786 a, stk. 2 bør angive en maksimal periode i hvilken data kan hastesikres – fx på ét år, svarende til reglerne om logning.

8. Økonomisk byrde og fælleseuropæiske regler

8.A. Økonomisk godtgørelse for teleudbydernes praktiske bistand til politiet for iværksættelse af målrettet logning
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 §§ 786a-786d, er ikke omtalt i lovudkastet.

Spørgsmålet om godtgørelse var ellers velbeskrevet i Justitsministeriets lovskitse fremlagt i marts 2021 (s. 40 i lovskitsen om standardtakster, som politiet skal betale for iværksættelse af målrettet logning) i form af en ordning som svarer til den gældende praksis for politiets betaling for teleudbydernes praktiske bistand til politiet ifm. udlevering af teledata.

TI anmoder om, at spørgsmålet om betaling for teleudbydernes praktiske bistand til politiet ifm. iværksættelse af målrettet logning og hastesikring 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).

8.B. Økonomisk byrde og fælleseuropæiske regler
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, som er et rent efterforskningsmæssigt værktøj, og de dertil knyttede væsentlige og omfattende behov for systemudvikling.

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 egen-interesse i at udvikle.

Dertil kommer etableringsomkostninger til systemunderstøttelse af registrering af Unikt ID og bruger samt indberetning heraf til 118-databasen mv., som alene os de største udbydere udgør et 3-cifret 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 finder det derfor rimeligt og anmoder om, at alle omkostninger til udvikling og drift af sådanne it-løsninger dækkes af staten.

8.C. Forenelighed med EU-retten og dommene fra EU-domstolen
På trods af Justitsministeriets arbejde med at tilpasse lovforslaget efter de afsagte domme fra EU-domstolen, er TI er bekymrede for, hvorvidt lovforslaget ligger inden for EU rettens rammer.

Såfremt den foreslåede model helt eller delvist underkendes, som værende uforenelige med EU-retten, vil en meget stor del af de mange millioner, som telebranchen pålægges at betale for at indrette it-systemer til opfyldelse af de nye regler, være tabt, og der vil herefter sandsynligvis skulle indføres og tilpasses et nyt system – med nye udgifter i samme størrelsesorden eller potentielt større til følge.

TI frygter således ikke blot en stor regning hørende til den foreslåede regulering, men også en mulig endnu større regning, såfremt den indførte ordning skal laves om endnu engang.

TI opfordrer derfor til, at regler om logning og udlevering af teledata udspringer af en fælles EU-forståelse. Derved styrkes retssikkerheden og indførelse af krav på et fælleseuropæisk grundlag vil sikre, at den danske telebranche ikke i forhold til teleudbydere i andre lande pålægges en ekstra byrde til udvikling af tekniske løsninger som følge af danske særregler, som ikke kan baseres på fælleseuropæiske standardløsninger.

TI bemærker desuden, at teleselskaberne efter dansk rets almindelige regler vil have mulighed for at kræve erstatning for omkostninger afholdt til efterlevelse af ulovlige regler.

TI står til rådighed for besvarelse af Justitsministeriets eventuelle spørgsmål i anledning af dette høringssvar, ligesom TI gerne uddyber høringssvaret ved et møde.

Med venlig hilsen

Jakob Willer
Direktør, TI

BILAG 1 – yderligere konkrete bemærkninger
(se vedlagte bilag)

R E T S P O L I T I S K F O R E N I N G

HØRINGSSVAR

Til Justitsministeriet

Vedr. 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.)

Høringsbrev af 27. september 2021 - med svarfrist 25. oktober 2021.

Svar fremsendt pr. mail til jm@jm.dk, hlm@jm.dk og nat@jm.dk

Sagsnr. 2020-187-0036

Dette lovforslag kommer 5-6 år efter, at den daværende regering i lyset af en EU-dom erkendte, at de danske regler om såkaldt logning var alt for vidtgående og faktisk ulovlige i henhold til EU-retten. Siden da har Folketinget flere gange og på forslag fra skiftende regeringer besluttet at udskyde den påkrævede revision uagtet kraftig kritik fra vide kredse, herunder også Retspolitisk Forening bl.a. i høringssvar ved hver udskydelse.

"Til gengæld" for forsinkelsen indeholder det nu fremsatte forslag så mange vidtgående muligheder for masseovervågning af teledata også kaldet trafikdata, at konkrete indgreb foretaget i henhold til den foreslåede ordning, hvis den vedtages, risikerer at blive underkendt af EU-domstolen.

Foreningen finder det uforsvarligt, at den udøvende magt på den måde lægger op til, at også landets lovgivende magt blot skal løbe en i realiteten betragtelig procesrisiko, som hvis overført til private forhold ville være udtryk for en meget dårlig samfundsmoral.

1: Typisk er det, at muligheden for at oprette uregistrerede taletidskort nu foreslås helt afskaffet med den begrundelse, at mange kriminelle benytter sig af denne mulighed for at undgå at blive aflyttet og overvåget mv. Men da der aktuelt findes omkring 100.000 af den slags kort, er realiteten, at masser af ganske almindelige mennesker ville blive ramt, typisk folk, som ikke har råd til at betale et almindeligt abonnement.

2: Foreningen må endvidere advare 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 ville 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.

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 samtidig bidrage til den stempling af bestemte boligområder som ghettoer, der efterhånden møder stigende kritik.

3: Konklusion.

Foreningen kan ikke anbefale vedtagelse af forslaget i dets nuværende form. Den foreslåede ordning ville placere Danmark i toppen internationalt set af overvågningsramte lande, uden at vores kriminalitetsstatistik eller terrortrusselssituation 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 at snart sagt alle og enhver skal mistænkeliggøres og overvåges, finder vi uacceptabelt.

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.

København, den 25. oktober 2021

Bjørn Elmquist	Esben Obel
Formand	Bestyrelsesmedlem

Justitsministeriet
Sikkerhedskontor II
Slotsholmsgade 10
1216 København K

RIGSADVOKATEN

RIGSADVOKATEN
FREDERIKSHOLMS KANAL 16
1220 KØBENHAVN K

TELEFON: 7268 9000
FAX: 7268 9004
E-MAIL: RIGSADVOKATEN@ANKL.DK
www.anklagemyndigheden.dk

DATO 26. oktober 2021

JOURNAL NR.
RA-2021-3200601-15

SAGSBEHANDLER: MPT/

Høring over udkast til 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.) – Justitsministeriets j.nr. 2020-187-0036

Ved brev af 27. september 2021 har Justitsministeriet anmodet om Rigsadvokatens eventuelle bemærkninger til 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.).

Jeg kan i den forbindelse oplyse, at lovudkastet ikke giver anledning til bemærkninger.

Med venlig hilsen

Marie Bindslev
Vicestatsadvokat

25. oktober 2021
MOKR
DI-2018-15718

ATT: Justitsministeriet
jm@jm.dk ; hlm@jm.dk ; nat@jm.dk

Dansk Industri
Confederation of Danish Industry

Høringssvar vedr. lovforslag om logning

DI skal hermed takke for høringen og indledningsvist henvise til høringssvaret fra Teleindustrien, som vi støtter, men samtidig nedenfor understrege en række budskaber.

Kompleksitet, overgang, EU-ret og ikrafttrædelse
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.

Omkostninger
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.

Entydig identifikation
En måde at nedbringe omkostningerne er ved at gøre det nemmere for teleselskaberne at efterkomme kravene i reguleringen. Ved målrettet logning er det fx vigtigt at teleselskaberne gøres i stand til enkelt og præcist at lokalisere en relevante telefon ved at spore på telefonnummer, IMEI eller lignende og netop ikke fx CPR-numre. Af Teleindustriens høringssvar fremgår der en række yderligere eksempler på hvordan omkostningerne konkret kan nedbringes.

H. C. Andersens Boulevard 18
1553 København V
Danmark
SAG

(+45) 3377 3377
di@di.dk
di.dk

CVR: 16 07 75 93

Fælles format
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 evt. 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 evt. på en ensrettet måde.

Tjenester omfattet at målrettet logning
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.

Afsluttende
DI vurderer grundlægende, at lovforslaget er for omfattende, komplekst, omkostningsfuldt og med en for hastig ikrafttrædelse. I medfør af ovenstående bemærkninger kan flere af disse forhold forbedres og vi 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.

DI står naturligvis til rådighed for at uddybe ovenstående.

Med venlig hilsen

Morten Kristiansen, chefkonsulent
DI Digital

Til Justitsministeriet:
Sendt pr. mail til jm@jm.dk, hlm@jm.dk, nat@jm.dk
Kopi: Energistyrelsen <tele@ens.dk>

København, 2021-10-25

Re: 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.)

Fiberby leverer højhastighedsinternet til boligforeninger, og vores høringssvar tager derfor udgangspunkt i hvordan det vil påvirke mindre internetudbydere som os.

Vi har bygget netværk siden 2000, og har været internetudbyder siden 2004. I dag er over 30.000 lejligheder tilsluttet vores fibernetværk.

Vi leverer på vores egen infrastruktur, og ude i den enkelte boligforening har vi netværksudstyr, typisk placeret i kælderen, og derfra går der netværkskabler op til de enkelte lejligheder.

Vi er generelt enige med Teleindustrien (TI) og IT-Politisk Forening (IT-Pol) i deres kommentarer til lovudkastet. og henviser derfor til disse for den dybere fortolkning af JM's vurderinger ift. EU-Domstolens praksis.

Vi har dog nogle konkrete bemærkninger omkring lovudkastet, fra en mindre internetudbyders perspektiv.

Hvem er omfattet af hvad?

Lovudkastet er generelt formuleret med stort fokus på telefoni, hvilket gør det lidt usammenhængende, når man blot udbyder internet-adgang på faste installationsadresser.

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.

Da vi driver et kommunikationsnetværk, og udbyder en kommunikationstjeneste som hovedydelse, så antager vi at vi er omfattet af begrebet.

Vi læser at trafikdata defineres som logningsbekendtgørelsens § 5, stk. 1, som ændret ved bekendtgørelse nr. 660 af 19. juni 2014. Vi læser at det foreslås, at registrering og opbevaring fremover vil kunne iværksættes for de data, der er registrerings- og opbevaringspligtige i dag.

Vi antog oprindeligt §§ 786 b-e til mest at handle om telefoni.

Restauranter, caféer, campingpladser og hoteller tilbyder typisk en delt trådløs internet-adgang, og opererer ikke et mobiltelefonnetværk, de er dog undtaget det

indskrænkede udbyder-begreb, netop for at undgå at de skulle blive omfattet af §§ 786 b-d.

Dermed må vi antage at det er meningen at §§ 786 b-d også skal omfatte internetudbydere og adgang til internettet.

§ 786 f gør dog at vi skal opsamle trafikdata uanset §§ 786 b-e, dermed giver det ikke mening at pålægge os byrden fra §§ 786 b-e.

Vi kan derfor kun få det et at give mening hvis intentionen er at §§ 786 b-d kommer til at genindføre sessionslogningen evt. på et senere tidspunkt, for i første omgang at kunne harmonere med begrænsningen til data der er registrerings- og opbevarings-pligtige i dag.

Vi læser pkt. 3.3.3 som at det ikke udelukkes at sessionslogning kan genindføres, via nogen af de nye bekendtgørelser, men blot vurderes at dette ville kræve en begrænsning mht. udlevering.

En genindførsel af sessionslogning vil være forbundet med store omkostninger til udvikling, hardware og lagring af loggede oplysninger.

Vi henviser til IT-Pol's høringssvar for argumentationen mod sessionslogning ift. EU-domstolens praksis.

Vi anbefaler at internetudbydere med fast leveringspunkt fritages for §§ 786 b-e samt at sessionslogning ikke genindføres.

Identificering af slut-bruger

Et mobiltelefonabonnement er som oftest personligt, og derfor kan det give mening med en CPR-nummer kobling.

Det er ikke klart af forslaget, om der lægges op til at vi skal registrere ét CPR-nr. eller samtlige CPR-numre der er en del af en given husstand. Det første er svært nok at få en høj datakvalitet på, og det andet er næsten umuligt. Hvor mange vil huske at melde ind at de har fået en ny sambo, og hvis vedkommende ikke har CPR gennemgå den ekstra verificering?

Det er heller ikke klart af lovskitsen hvad der skal ske med produkter solgt til erhverv, men som må benyttes privat, såsom arbejdsgiverbetalt "fri telefon" og arbejdsgiverbetalt internet. Hvordan skal den slags abonnementer registreres og verificeres? CVR, CPR eller begge.

Da vi leverer på vores egen infrastruktur, bruger vi ikke 8-cifrede telefonnumre, og har derfor ikke adgang til 118-databasen, eller andre telefoniske fossiler.

Ved erhvervsabonnementer fx. kontor eller butikslokale vil det da være et krav ifm. verificering at der er registeret et P-nummer på leveringspunktet?

Vi har også kollektivt opkrævede foreningskunder, hvor opkrævningen sker gennem deres fællesomkostninger/husleje. I dette segment har vi i dag ofte ingen registrering af slut-bruger, udover enhedsadressen og selv når vi har så er den ofte forældet, da vi ikke får besked når folk flytter.

Da vores primære forsyningsområde er København har vi en del dele-lejligheder og anden form for værelsesudlejning.

Da det må antages at tidligere fængslede, kan være bevidste om at de bliver målrettet overvåget, det er vel derfor ikke helt utænkeligt at de får andre medlemmer af deres husstand til at tegne abonnementet til deres husstand, hvis ikke de flytter ind et sted hvor der i forvejen er tegnet et internetabonnement.

Derudover kan vi ikke logge datatrafik på en enkelt person uden at logge datatrafik for den samlede husstand, samt evt. gæster.

I realiteten vil den personbestemte målrettede overvågning derfor blive til den husstandsbestemte målrettede overvågning.

Vi ser derfor ikke CPR som en egnet nøgle til den personbestemte målrettede overvågning når det gælder faste forbindelser.

Enhedsadresser som unik identifikation

Vi leverer faste bredbåndsforbindelser til danske husstande.

Alle danske husstande har et unikt ID kaldet enhedsadresse-id, registeret i Danmarks Adresseregister (DAR), som drives af Styrelsen for Dataforsyning og Effektivisering (SDFE).

Personer er i CPR tilknyttet en enhedsadresse (folkeregisteradresse). Ligeledes er virksomheder i CVR tilknyttet enhedsadresser via både CVR og P-numre.

Politiet har mulighed for at omsætte CPR-numre til enhedsadresser via CPR-registeret.

Vi ser ikke nogen grund til at vi skal forsøge at lave en dårlig kopi af CPR-registeret. Det vil være en meget kostbar øvelse, og spild af ressourcer.

Vi har også behov for fortsat at kunne levere til bygningstekniske installationer i erhverv/foreninger med CVR-nummer med hverken enhedsadresser eller P-nummer, såsom adgangssystemer, dørtelefoni, fjernaflæsning, brandanlæg, elevatorer, beboervaskerier, bestyrelses- og fælleslokaler osv. I disse tilfælde vil der dog udover CVR-nummer, oftest kunne tilknyttes en adgangsadresse.

Vi vil også helst undgå at skulle håndtere CPR-numre på vores kunder.

Vi vil derfor kraftigt opfordre 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.

Målrettet trafikdata for kommunikationsapparater

Ifm. § 786 d, må vi gøre opmærksom på at vi ikke kan identificere kommunikationsudstyr som ikke er direkte tilkoblet vores netværk.

Vores kunder ejer selv deres routere, de er ikke en del af deres abonnement hos os.

Vi kan derfor ikke identificere udstyr tilkoblet bag vores kunders routere.

Den forslåede verificering vil give problemer ifm. flytning

Da vi i forvejen har et vægstik i samtlige lejligheder, hvor vi kan levere så fungere vores tilmeldingsproces, ved at brugerne tilkobler deres stik og udfylder en tilmeldingsside,

før deres internet-adgang bliver aktiveret. Som en del af denne proces får vi også verificeret enhedsadressen.

Da vi har en del kunder der tegner deres abonnement ifm. en flytning, så vil det ofte ikke være den rigtige adresse som står i CPR-registeret, og derfor vil vi evt. skulle oprette dem på deres gamle adresse for at kunne verificere dem, da CPR-registeret endnu ikke vil være opdateret.

Et andet eksempel er forældre der vil tegne ét internet-abonnement for deres børns bopæl, men ikke selv har bopæl på adressen.

Vi anser det som en meget tung opgave, at skulle verificere vores kunder før de kan få åbnet deres internet-adgang, som vil øge mængden af support som vores kunder har behov for ifm. tilmelding og verificering.

Det er forbundet med store gener for både slut-bruger og Fiberby, hvis vi er udelukket fra at tegne abonnement og aktivere internet-adgang hvis ikke folkeregisteradresse matcher installationsadressen.

Vi vil derfor gerne undgå krav om verificering af slut-bruger data, eftersom at vi har verificeret hvilken enhedsadresse forbindelsen er leveret til.

Carrier Grade NAT

Carrier Grade NAT (CGN) er beskrevet i BCP 127 / RFC 6888, som er udgivet af Internet Engineering Task Force (IETF), som et såkaldt Best Current Practice dokument. Det er IETF der har udgivet alle de grundlæggende internetstandarder og protokoller.

For at sikre teknologineutralitet foreslår vi at følgende skal oplyses ifm. 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

Modtager IP og port bør ikke være svære at medtage i forespørgslerne, som eksempel hvis man gerne vil spore en forbindelse til "https://www.ft.dk/" så vil modtager IP være serverens IP (152.115.53.91) og modtager port være 443 og IP-protokol være TCP (pga. https:// altid er TCP/443).

Simple CGN-implementeringer med generisk server hardware, kan godt bruge samme afsender port til forskellige modtagere samtidig, på vegne af forskellige slut-brugere.

Simpel logning på denne slags CGN, vil dermed kræve at modtager og afsender logges, og er dermed næsten det samme som sessionslogning.

Da dette er på kant med BCP 127 krav nr. 12 samt GDPR, så bør disse logningsdata efterbehandles, hvorved overflødige modtager adresser kan smides væk i de tilfælde hvor samme port-nummer ikke er anvendt af flere slut-brugere. Dermed ville det kunne minimeres til kun at opbevare de minimale oplysninger.

Uden at inkludere oplysninger om modtageren, vil det være et krav at der benyttes særlig CGN hardware som understøtter Port Block Allocation (PBA), en metode til at sørge for at kunne minimere CGN logningsdata, ved at logge intervaller af afsender porte tildelt til den enkelte slut-bruger.

Hvilket vil øge omkostningerne til logning markant, og ramme mindre udbydere u-proportionelt hårdere.

Ang. BCP 127 krav nr. 15: "A CGN's port allocation scheme SHOULD make it hard for attackers to guess port numbers.":

Såfremt at modtager oplysningerne inkluderes i en forespørgsel, så kan modtager oplysningerne bruges til at sløre afsender porten, for at beskytte brugeren bedre mod angreb, uden at forringe muligheden for at politiet kan få udleveret bruger oplysninger. Vi håber ikke at slut-brugernes IT-sikkerhed skal lide pga. restriktioner i dette lovforslag.

Vi vil selvfølgelig helst undgå at skulle udføre generel udifferentieret CGN logning, jvf. IT-Pol's høringssvar.

Vores anbefaling er at modtager IP og port også bør oplyses ifm. udlevering, for at sikre ønsket om teknologineutralitet.

BCP 127 / RFC 6888: Common Requirements for Carrier-Grade NATs (CGNs)
https://www.rfc-editor.org/rfc/rfc6888

Transparens og statistik

For at gøre det muligt at have en offentlig debat omkring denne lovgivning, så foreslår vi at der skal 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 den 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 være umuligt at debattere lovgivningens anvendelighed, proportionalitet og effektivitet.

3 gange 3 km inddeling af Danmark

SDFE har i dag ikke en 3 gange 3 km inddeling af Danmark, men kun en 1 gange 1 km og en 5 gange 5 km inddeling.

Vi vil derfor opfordre til at SDFE får opgaven med at lave en ny officiel 3 gange 3 km inddeling, således at denne bliver offentlig tilgængelig på lige fod med de eksisterende inddelinger.

Dansk tid?

Det foreslås at reglerne skal sikre at "korrekt dansk realtid" registreres.

Dansk tid er dog ikke egnet til logningsformål, da denne ikke er kontinuerlig.

Ifm. med skift fra CEST til CET er der 2 timer hvor logningen ikke vil være entydig og dermed vil tjene som et svagere bevis.

Best practice er at benytte UTC tid til logningsformål, hvorved at den slags problemer undgås.

Såfremt dansk tid bliver et decideret krav, må det antages at kriminelle kan udnytte dette til deres fordel.

Derudover er det måske tid til at revidere Lov om Tidens Bestemmelse (lov nr 83 af 29/03/1893), inspiration kan evt. hentes i Sverige, som har officielle tidsservere til præcis UTC tidssynkronisering.

Revision

Endeligt bør den nye lovgivning også tilføjes en revisionsbestemmelse, gerne med et loft over hvor mange gange den kan udskydes.

Venlig hilsen

Jens Fauring

IT-chef | Direkte telefon 20 89 68 64 | E-mail jef@fiberby.dk

DANSKE IT ADVOKATER

DANSKE ADVOKATER

Justitsministeriet
Slotsholmsgade 10
1216 København K

Sendt til: jm@jm.dk, hlm@jm.dk, nat@jm.dk

Vesterbrogade 32
1620 København V

Telefon 33 43 70 00
dlol@danskeadvokater.dk
www.danskeadvokater.dk

Dok.nr. D-2021-034168

27. oktober 2021

Høringssvar over udkast til de nye logningsregler

Den 27. september 2021 har Justitsministeriet sendt 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.), ("Lovforslaget") i høring.

Danske Advokaters høringsnotat er udarbejdet i samarbejde med vores fagudvalg for it- og teleret. Fagudvalget består af advokater, der i væsentligt omfang beskæftiger sig med it og telekommunikation. Medlemmerne af vores fagudvalg for it- og teleret repræsenterer både udbydere, kunder og leverandører i telebranchen og er alle en del af Danske IT-Advokaters (DITA) bestyrelse.

Overordnede bemærkninger

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.

Vi har i svaret valgt at fokusere på de umiddelbart væsentligste emner:

1) Adgangen til at generel og udifferentieret logning,
2) Adgangen til målrettet logning,
3) Udbyderbegrebet,
4) Systemtekniske udfordringer,

Danske Advokater har nedenfor anført vores konkrete bemærkninger til de foreslåede ændringer i Lovforslaget. For god ordens skyld bemærkes det, at bemærkninger og emner ikke skal anses for udtømmende.

Konkrete bemærkninger til Lovforslaget

Adgangen til at generel og udifferentieret logning

Det er Danske Advokaters vurdering, at der, med de foreslåede regler, er en risiko for, at generel og udifferentieret logning kommer til at udgøre hovedregelen og ikke den begrænsede undtagelse. En sådan praksis vil være i strid med EU-retten.

Det foreslås endvidere, at vurderingen af, om der foreligger en alvorlig trussel mod den nationale sikkerhed, med deraf følgende mulighed for at iværksætte generel og udifferentieret logning ligger hos Justitsministeriet efter forhandling med erhvervsministeren. Disse kan iværksætte den generelle og udifferentierede logning udenom Folketinget. En sådan beslutning er endvidere ikke underlagt automatisk domstolskontrol. Det er efter Danske Advokaters opfattelse et retssikkerhedsmæssigt problem, som vi kraftigt vil advare imod.

EU-domstolen har i 3 hovedafgørelser, C-293/12 Digital Rights Ireland fra 2014 (”Digital Rights Ireland”), C-2013/15 og C-698/15 Tele2/Watson fra 2016 (”Tele2”), og C-512/18 La Quadrature Du Net i 2020 (”La Quadrature”) slået fast, at *generel og udifferentieret logning* strider mod EU-Chartrets grundlæggende rettigheder om art. 7 (retten til privatliv), 8 (beskyttelse af personoplysninger), 11 (retten til ytringsfrihed) og at sådan indgreb går videre, end hvad der kan begrundes under proportionalitetsprincippet i Charterets art. 52, stk. 1.

Se eksempelvis, La Quadrature, præmis 141:

> *”[…] national lovgivning, der foreskriver generel og udifferentieret lagring af trafikdata og lokaliseringsdata med henblik på bekæmpelse af grov kriminalitet, overskrider det strengt nødvendige og kan i et demokratisk samfund ikke anses for at være begrundet, således som det er påkrævet i henhold til artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1 (jf. i denne retning dom af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 107).”*

EU-Domstolen udtalte i Tele2, (præmis 108) og La Quadrature (præmis 147), at EU-retten ikke er til hinder for, at en medlemsstat vedtager lovgivning, der som en forebyggende foranstaltning muliggør en *målrettet lagring af trafikdata og lokaliseringsdata* med henblik på *bekæmpelse af grov kriminalitet eller for at forhindre en alvorlig fare for den offentlige sikkerhed,* forudsat at lagringen af

disse data *begrænses til det strengt nødvendige* for så vidt angår kategorierne af data, der skal lagres, de omhandlede kommunikationsmidler, de berørte personer og den fastsatte varighed af lagringen. Endvidere (præmis 111), at sådan logning skal være *baseret på objektive forhold* der gør det muligt at fokusere målrettet på en personkreds, hvis data kan afsløre *en forbindelse, i det mindste indirekte, til grov kriminalitet, bidrage til bekæmpelse af grov kriminalitet på den ene eller den anden måde eller forhindre en alvorlig fare for den offentlige sikkerhed*.

Målrettet logning kan således indføres under iagttagelse af særlige krav.

La Quadrature introducerede en *begrænset undtagelse for kvalificeret trussel mod national sikkerhed*, hvor hensynet til en kvalificeret trussel mod national sikkerhed i visse – afgrænsede – tilfælde kan begrunde et generelt og udifferentieret logningspåbud.

Domstolen udtaler, at følgende omstændigheder skal være til stede, før der er tale om en kvalificeret trussel mod den nationale sikkerhed. Først når disse kvalificerende omstændigheder foreligger, aktualiseres muligheden for en generel og udifferentieret logning, jf. præmis 137:

Der er tilstrækkelige og konkrete omstændigheder, som indikerer, at

1. en medlemsstat står overfor en alvorlig fare for den offentlige sikkerhed, og
2. denne fare er reel, aktuel eller forudsigelig.

Der er derudover 5 kumulative krav:

1. Ethvert påbud om at foretage forebyggende logning skal *"tidsmæssigt begrænses til det strengt nødvendige"*, jf. præmis 138.

2. *Varigheden af hvert enkelt påbud må ikke "overstige et forudsigeligt tidsrum*" og lagringen må under alle omstændigheder *ikke have "systematisk karakter*", jf. præmis 138.

3. Lagring af data skal være *"omfattet af begrænsninger og underlagt strenge garantier*, der gør det muligt effektivt at beskytte personers personoplysninger mod risikoen for misbrug", jf. præmis 138.

4. Logningen skal *"rent faktisk begrænses til de situationer, hvor der foreligger en trussel mod den nationale sikkerhed"*, jf. præmis 139.

5. En afgørelse, hvorved udbydere pålægges en logningsforpligtelse skal kunne gøres til genstand for "[...] en *effektiv prøvelse enten ved en domstol eller en uafhængig administrativ enhed*, der træffer bindende afgørelser, med henblik på at kontrollere, om en af disse situationer foreligger, samt om de betingelser og garantier, der skal være fastsat, er overholdt", jf. præmis 139.

EU-Domstolen fastlægger således klare, stringente og kumulative betingelser for lovligheden af et påbud om generel og udifferentieret logning. Det er med andre ord ikke i sig selv tilstrækkeligt, at en medlemsstat kan sandsynliggøre eller sågar påvise en kvalificeret trussel mod den nationale sikkerhed.

Med Lovforslaget introducerer Ministeriet de to former for logning:

1. Målrettet logning
2. Generel og udifferentieret logning.

Lovforslaget er opbygget således, at udgangspunktet er målrettet logning, mens generel og udifferentieret logning er undtagelsen.

Danske Advokater mener imidlertid, at udformningen af Lovforslaget indebærer en væsentlig risiko for, at realiteten omvendt bliver, således at generel og udifferentieret logning bliver hovedreglen. Det er blandt andet tilfældet idet:

1. La Quadrature undtagelsen for generel og udifferentieret logning anvendes udover sine rammer og medfører en fortsættelse af den status quo, der netop er underkendt af EU-domstolen i de afsagte domme;
2. 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.

Den begrænsede undtagelse om generel og udifferentieret logning

Ministeriet lægger op til, at der ved en alvorlig trussel mod den nationale sikkerhed, der er reel, aktuel eller forudsigelig, kan iværksættes generel og udifferentieret logning ved bekendtgørelse for en periode på 1 år ad gangen, jf. Lovforslagets § 786 e.

Ministeriet angiver, at vurderingen af en alvorlig trussel mod den nationale sikkerhed kan omfatte:

1. Antallet og karakteren af verserende eller afgjorte straffesager om overtrædelse af straffelovens kapitel 12 og 13 (Lovforslaget s. 55).

2. "Vurderingen af Terrortruslen mod Danmark" (VTD), som årligt udarbejdes af Center for Terroranalyse (CTA).

3. En række andre uklassificerede analyseprodukter udgivet af Politiets Efterretningstjeneste, Forsvarets Efterretningstjeneste eller Center for Cybersikkerhed. Det kunne f.eks. være Center for Cybersikkerheds årlige "Trusselsvurdering 2020: Cybertruslen mod Danmark", men også andre relevante trusselsvurderinger vil kunne indgå. (Lovforslagets s. 58).

Vurderingen af, om der foreligger en alvorlig trussel mod den nationale sikkerhed vil skulle foretages regelmæssigt (Lovforslagets s. 58).

CTA har i VTD'en vurderet truslen som alvorlig mod den nationale sikkerhed i hele perioden 2014-2020. Det samme har været tilfældet for Center for Cybersikkerheds årlige Trusselsvurdering.

Beslutningskompetencen ligger hos Justitsministeriet efter forhandling med erhvervsministeren, der kan iværksætte den generelle og udifferentierede logning udenom Folketinget.

Beslutningen om at overgå til/fastholde generel og udifferentieret logning er ikke underlagt automatisk domstolskontrol. Ministeriet har angivet, at beslutningen efterfølgende *kan* 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 (Lovforslaget s. 84). 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.

Ministeriets bemærkninger i Lovforslaget s. 84 giver 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.

> *"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, jf. pkt. 3.1.3.4."*

Ministeriet angiver det også selv mere direkte i Lovforslagets s. 15:

> *"Målrettet registrering og opbevaring af trafikdata vil være udgangspunktet, når der ikke foreligger en alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig."*

Tilgangen synes at stride mod EU-domstolens afgørelse i La Quadrature (præmis 139) om, at

> *"en afgørelse, hvorved udbydere pålægges en logningsforpligtelse skal kunne gøres til genstand for "[...] en effektiv prøvelse enten ved en domstol eller en uafhængig administrativ enhed, der træffer bindende afgørelser,*

med henblik på at kontrollere, om en af disse situationer foreligger, samt om de betingelser og garantier, der skal være fastsat, er overholdt".

Danske Advokater anbefaler i den forbindelse, at der indføres krav om i) mandat fra Folketinget, og ii) domstolsprøvelse ved iværksættelse, eller iii) tilsyn fra en uafhængig administrativ myndighed.

Ad varighed

EU-domstolen har anført (præmis 139), at en La Quadrature ordning bør "tidsmæssigt begrænses til det strengt nødvendige". Ministeriet har 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.

Ad formålsforskydning

Der er ikke kongruens mellem det, der kan udløse en pligt til at foretage generel og udifferentieret logning (i.e. at Danmark "*står over for en alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig*", jf. § 786 e), og det at der kan ske udlevering af de pågældende oplysninger for (i.e. "*hvis efterforskningen angår en lovovertrædelse, som efter loven kan straffes med fængsel i 3 år eller derover eller en lovovertrædelse, som kan medføre strafforhøjelse efter straffelovens § 81 a*", jf. § 781 a)

Dertil kommer, at det i forlængelse heraf foreslås, at oplysninger, der er registreret og opbevaret som følge af en pligt til generel og udifferentieret registrering og opbevaring, vil skulle opbevares i 1 år fra registreringstidspunktet, også efter overgangen til målrettet registrering og opbevaring (Lovforslaget s. 60). 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 at være uforenelig med EU-retten, såvel som persondataretten, eks. GDPR art 5. Ministeriet kategoriserer da også selv dette som en "væsentlig procesrisiko" (Lovforslaget s. 106).

Danske Advokater anbefaler, at formålsforskydningen slettes, og at de pågældende oplysninger tilsvarende slettes, eller "vaskes" igennem kravene til målrettet logning, hvis en sådan er i kraft parallelt med den generelle og udifferentierede logning.

Målrettet logning

Ad geografisk afgrænset målrettet logning

Lovforslaget indebærer mulighed for målrettet geografisk logning efter § 786c, stk. 1 i 3x3 km's zoner, hvor:

1. antallet af *anmeldelser af lovovertrædelser begået i området, som efter loven kan straffes med fængsel i 3 år eller derover,* forsætlige overtrædelser af straffelovens kapitel 12 eller 13, overtrædelser afstraffelovens § 124, stk. 2, § 125, § 127, stk. 1, § 235, § 266 eller § 281, overtrædelser af udlændingelovens § 59, stk. 8, nr. 1-5, krænkelser eller overtrædelser som omfattet af § 781, stk. 2 eller 3, *udgør mindst 1,5 gange landsgennemsnittet opgjort som gennemsnit over de seneste 3 år,* eller
2. *antallet af beboere dømt* for 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 omfattet af § 781, stk. 2 eller 3, eller som er dømt efter straffelovens § 81 a, udgør *mindst 1,5 gange landsgennemsnittet opgjort som gennemsnit over de seneste 3 år.*

Indledningsvis bemærkes det, at de opstillede krav vil kunne medføre logning af store persongrupper, der ikke har tilknytning til udførelse af grov kriminalitet. Områdernes fastlæggelse vil have afgørende betydning for, hvem der konkret rammes af logning.

Området for geografisk logning kan demografisk set være endog meget stort. Det er uklart, om Lovforslaget i den nuværende form indebærer, at logning kan ske med udgangspunkt i et nedslag i et konkret område, eks. den absolut yderligste del af Christiania. I givet fald vil det indebære, at der kan/skal logges i et større område - eksempelvis helt til Østerbro – eller om kravene om 1½ gangs overrepræsentation af dømte eller anmeldte lovovertrædelser skal være gældende for hele det omfattede område.

Endvidere vil tyndt befolkede områder risikere at kunne opfylde kravene uden at overskridelsen af landsgennemsnittet reelt er statistisk signifikant.

Danske Advokater anbefaler, at reglerne genovervejes med henblik på at sikre klare kriterier for, om et konkret nedslagspunkt med en overrepræsentation kan medføre geografisk logning i en 3x3 km radius, eller om sådan zone alene kan etableres, hvis kriterier er opfyldt for hele den fastlagte zone.

Området for den målrettede geografiske logning kan endvidere ved pålæg de facto udvides endnu mere. Det er tilfældet, idet *"afhængig af den konkrete forbindelse til grov kriminalitet kan det udtrækkes f.eks. til en hel bydel eller en*

landsdel" (Lovforslaget s. 44). Ligesom samtidige zoner på 3x3 km hurtigt kan udstrækkes til det meste af København.

Derudover er der markante praktiske udfordringer for teleudbyderne med at indramme den pågældende zone. Det er tilfældet, idet antennernes (cellernes) rækkevidde udbredes i "cirkler", således at området i realiteten vil blive meget større. Ministeriet anerkender da også *"at det ikke er muligt at frasortere data inden for de enkelte cellers rækkevidde, som stammer fra telefoner, der reelt har befundet sig uden for de udpegede område*r" (Lovforslagets s. 52).

Det fremgår imidlertid af Lovforslaget, at:

> *"Er dette tilfældet, vil de oplysninger, der registreres og opbevares, være omfattet af den målrettede geografiske registrering og opbevaring. Det betyder, at Politiet og anklagemyndigheden vil kunne få adgang til disse trafikdata, og at disse oplysninger på samme vis som øvrige oplysninger, der registreres og opbevares som følge af en af de foreslåede registrerings- og opbevaringspligter, kan anvendes i efterforskninger og som bevis i straffesager" (s. 52)*

Sådan formålsforskydning vil også være problematisk i henhold til EU-domstolens krav om, at relatere logningen til det "strengt nødvendige", ligesom det kan være persondataretligt problematisk i medfør af GDPR, art. 5.

Efter § 786c, stk. 2 kan der også iværksættes målrettet logning af særligt sikringskritiske områder, såsom kongehusets residenser, Christiansborg Slot, statsministerboligen Marienborg, ambassader, politiets ejendomme, kriminalforsorgens institutioner, bro-, tunnel- og færgeforbindelser, trafikknudepunkter og større indfaldsveje, grænseovergange, busterminaler, fjernbanestationer, stationer på bybaner, militære områder, kolonne 3-virksomheder og offentligt godkendte flyvepladser.

Samlet efterlader det en risiko for, at det meste af København, Aarhus og Odense kan blive underlagt målrettet logning. Hvilket efterlader den risiko, at alternativet til den generelle og udifferentierede logning er "generel og udifferentieret" logning af store dele af Danmark.

Oversigten over de pågældende geografiske områder vil ikke være offentlig, men det enkelte påbud vil dog være genstand for domstolsprøvelse.

Danske Advokater anbefaler, at det præciseres, at domstolene i deres prøvelse kan lade verserende påbud indgå, herunder om det pågældende påbud alene *eller* i sammenhæng med verserende påbud, går udover hvad der kan indeholdes indenfor kravene til målrettet logning, henholdsvis forbuddet om generel og udifferentieret logning.

Ad personafgrænset målrettet logning

Danske Advokater anser generelt tilgangen med den personafgrænsede målrettede logning for positiv for at sikre en nærmere forbindelse, i det mindste indirekte, til 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.

Lovforslaget introducerer endvidere en øget varighed af registreringspligt for de pågældende. Perioden kan, afhængig af overtrædelsens karakter baseret på strafferammen, strækkes fra 3 til 10 år. Det rejser umiddelbart overvejelser omkring, hvorvidt en sådan tilgang er i overensstemmelse med afsoneres grundlæggende rettigheder. Det ligger udenfor DITA's kompetencer at tage stilling til foreneligheden heraf, men DITA og Danske Advokater støtter Ministeriets høring af synspunkter på området fra relevante organisationer med kompetencer indenfor området.

Edition

Danske Advokater støtter, at reglerne for udlevering af indsamlede og opbevarede logningsdata i høj grad sidestilles med indgreb i meddelelseshemmeligheden, såvel som for edition, jf. § 806, stk. 10.

Udbyderbegrebet

Lovforslaget introducerer et nyt udbyderbegreb under logningsreglerne, således at reglerne om målrettet logning alene gælder for "*udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikke-accessorisk del af virksomheden*", jf. § eks. 786 b. Hermed undtages de virksomheder, der har givet anledning til diskussioner omkring logningsforpligtelsen for campingpladser, hotel og konferencefaciliteter og udbydere af wifi hotspot. Det nye udbyderbegreb svarer reelt til begrebet "erhvervsmæssige udbydere", som defineret i teleloven.

Det brede udbyderbegreb "*udbydere af elektroniske kommunikationsnet eller -tjenester*", der også omfatter udbydere såsom campingpladser, hotel og konferencefaciliteter og udbydere af wifi hotspot finder imidlertid stadig anvendelse for så vidt angår den generelle og udifferentierede logning ved "alvorlig trussel" mod den nationale sikkerhed, jf. § 786 e.

Det nye udbyderbegreb sondrer ikke mellem udbud af teleydelser på henholdsvis engros- og detailbasis. De gældende logningsregler har udbydere til slutbrugere som pligtsubjekt. Ved ikke at tage dette led med i afgrænsningen spredes forpligtelsen ud på en række aktører, som ikke har kundeforhold og dublerer dermed reelt forpligtelsen til flere teleselskaber.

I Lovforslaget er det, som i dag, ganske vist anført, at "*hvis de omfattede oplysninger kan registreres af flere udbydere, skal oplysningerne registreres og opbevares af mindst én af udbyderne*", men for at denne begrænsning skal kunne bruges, vil det kræve, at der imellem operatørerne kan træffes aftaler.

Dertil kommer, at der ikke, som i de nuværende logningsregler, omtales muligheden for outsourcing til eksempelvis en netoperatør (MNO) således, at tjenesteudbydere (service providere) ikke forpligtes til at etablere egne funktioner, hvad de i mange henseender ikke vil være i stand til.

Endelig er det med til at skabe forvirring, at det anføres, at "*anmodning om adgang til registrerings- og opbevaringspligtige oplysninger vil efter den foreslåede bestemmelse skulle rettes til den dataansvarlige udbyder*". Danske Advokater formoder, at der herved sigtes til den registrerende udbyder.

Lovforslaget lægger op til, at de relevante udbydere skal iværksætte omfattende tekniske og praktiske foranstaltninger, som Ministeriet har anslået til 206 mio. kr. i omstillingsomkostninger og 107 mio. kr. i årlige administrationsomkostninger for udbyderne og tilsvarende ca. 200 mio. kr. for myndighederne.

Udbyderne får adgang til væsentlige persondata for at kunne iværksætte målrettet logning af personer, såvel som geografiske områder. Det er tale om oplysninger om enkeltpersoners strafbare forhold eller relationer til strafbare personer. Det er uklart, hvordan det praktisk kan/skal håndteres hos udbyderne. Dette bør overvejes særdeles grundigt, idet der er tale om potentielle databaser, der udgør en art strafferegister for personer med grove straffe. Sådanne databaser, som må anses for særligt fortrolige og genstand for øget sikkerhed skal herefter håndteres af private virksomheder.

Ministeriet udstrækker udbyderbegrebet til det yderste ved at lade alt fra netværksejere til campingpladser og hoteller være omfattet.

Størstedelen af udbyderne ligger imidlertid i den store mellemgruppe af udbydere med elektroniske kommunikationstjenester som sit hovederhverv, men med en begrænset størrelse. I Danmark er der en omfattende mængde af udbydere i SMV-størrelsen, såvel som internationale aktører med et salgskontor i Danmark. Der er måske tale om anslået mellem 50-100 udbydere. Der lægges op til, at de på samme måde skal håndtere disse persondata, sikkerheden heromkring og opdateringen heraf. Det forudsætter et højt sikkerhedsniveau, systemer og en organisation i et omfang, der ikke forefindes hos de fleste udbydere i dag. Risici i den forbindelse omfatter sikkerhedsrisici for de pågældende persondata, såvel som et fravalg af at være på det danske marked, og deraf mangel på innovation og konkurrence på markedet.

I dag skal de udbydere, der håndterer logningsdata også sikkerhedsgodkendes. Det er PET, der foretager sikkerhedsgodkendelsen. I praksis kan sådan sikkerhedsgodkendelse kun ske af dansk bosiddende personer. Varigheden af processen for at opnå sikkerhedsgodkendelse er uklar, men perioden anslås i praksis til at udgøre mellem til 3-12 måneder.

I dag håndteres dette ofte ved at outsource det sikkerhedsgodkendte kontaktpunkt, eller ved at PET meddeler, at sådan sikkerhedsgodkendelse først sker, hvis der anmodes om indgreb i meddelelsen. Det sidste giver ikke mening, men er omvendt ofte forekommende i praksis. Det er også en tilgang, der reflekterer, at det i praksis alene er netværksejerne, og/eller de helt store udbydere, der modtager kendelser om indgreb i meddelelseshemmeligheden fra politiet, herunder idet netværksejerne vil have adgang til de fleste (om ikke alle) data.

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), og 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.

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

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

Systemtekniske udfordringer

Ministeriet anslår, at myndighedernes omstilling til målrettet logning kræver udvikling af it-mæssig understøttelse.

Omstillingen forudsætter videre en analyse af it-systemer på tværs af flere myndigheder, der først vil foreligge i 2023. Først herefter vil Rigspolitiet kunne skønne, hvordan og hvornår sådan it-understøttelse kan være klar (Lovforslaget s. 53).

I den mellemliggende periode, hvilket som absolut minimum må blive 1 år før *"Rigspolitiets it-løsning m.v. er etableret og klar til at blive sat i drift – vil [Ministeriet] kunne fastsætte nærmere regler om registrering og opbevaring af trafikdata for så vidt angår den foreslåede ordning med målrettet personbestemt registrering og opbevaring af trafikdata. Det forudsættes, at bemyndigelsen udnyttes til at fastsætte regler om bl.a. politiets adgang til at pålægge registrering og opbevaring af trafikdata baseret på politiets konkrete anmodninger. Der lægges i den forbindelse ikke op til at bemyndige justitsministeren til at fastsætte andre betingelser for den målrettede registrering og opbevaring af trafikdata end dem, som fremgår af de foreslåede §§ 786 b og 786 d i retsplejeloven",* (Lovforslagets side 53).

Der er således 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. Ministeriet anfører selv:

> *"Det bemærkes, at udmøntningen af de foreslåede regler om målrettet personbestemt og geografisk registrering og opbevaring vil være forbundet med en risiko for eventuelle fejl enten i form af, at der registreres og opbevares oplysninger om personer eller områder, der ikke er omfattet af den foreslåede ordning, eller i form af, at der ikke registreres oplysninger for alle personer eller områder, der er omfattet af ordningen. Det skyldes bl.a., at udmøntningen vil være afhængig af en række ældre it-systemer og overbygninger herpå. Der vil også være risiko for fejl i overgangsperioden, hvor der vil være tale om at udmønte reglerne i en manuel løsning."* (Lovforslaget s. 53)

Dette er endvidere kun de systemtekniske udfordringer, som Lovforslaget rejser på myndighedssiden.

Der er lige så store, hvis ikke flere, tekniske implementeringsbehov og udfordringer på udbydersiden. I den mellemliggende periode, vil udbyderne tilsvarende skulle håndtere at modtage oplysninger fra myndighederne og udlevere oplysninger på en midlertidig manuel måde. Dette virker hverken sikkert eller proportionelt i forhold til at varetage borgernes personoplysninger og iagttage deres grundlæggende rettigheder til privatliv på en proportionel og sikker måde.

* * *

Som anført i indledningen finder Danske Advokater, at arbejdet med ændringen af logningsreglerne meget værdifuldt, og Danske Advokater håber, at Ministeriet finder dette høringsnotat brugbart for at arbejde yderligere med revisionen af Lovforslaget. Danske Advokater, herunder vores fagudvalg for it-ret, stiller i den forbindelse gerne op i forhold til en uddybning af elementerne i høringssvaret.

Med venlig hilsen

Danielle Løw
Juridisk konsulent
Danske Advokater

Herunder fremgår en ikke udtømmende liste over Danske Advokaters anbefaling:

Danske Advokater anbefaler, at der ved beslutning om at overgå til/fastholde generel og udifferentieret logning indføres krav om i) mandat fra Folketinget, og ii) domstolsprøvelse ved iværksættelse, eller iii) tilsyn fra en uafhængig administrativ myndighed.

Danske Advokater anbefaler, at formålsforskydningen slettes, og at de pågældende oplysninger tilsvarende slettes, eller "vaskes" igennem kravene til målrettet logning, hvis en sådan er i kraft parallelt med den generelle og udifferentierede logning.

Danske Advokater anbefaler, at reglerne genovervejes med henblik på at sikre klare kriterier for, om et konkret nedslagspunkt med en overrepræsentation kan medføre geografisk logning i en 3x3 km radius, eller om sådan zone alene kan etableres, hvis kriterier er opfyldt for hele den fastlagte zone.

Danske Advokater anbefaler, at det præciseres, at domstolene i deres prøvelse kan lade verserende påbud indgå, herunder om det pågældende påbud alene *eller* i sammenhæng med verserende påbud, går udover hvad der kan indeholdes indenfor kravene til målrettet logning, henholdsvis forbuddet om generel og udifferentieret logning.

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.

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), og 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.

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

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

DANSKE JURISTER ADVOKATER

DANSKE ADVOKATER

Justitsministeriet
Slotsholmsgade 10
1216 København K

Sendt til: jm@jm.dk, hlm@jm.dk, nat@jm.dk

Vesterbrogade 32
1620 København V

Telefon 33 43 70 00
dlol@danskeadvokater.dk
www.danskeadvokater.dk

Dok.nr. D-2021-034162

27. oktober 2021

Danske Advokaters holdning til forslaget om nye lognings regler

Hvis lovforslaget bliver vedtaget i sin nuværende form, risikerer vi 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. Sagt på jævnt dansk: I stedet for at fiske med fiskestang, kommer staten til at fiske med trawl.

Samtidig er det vores opfattelse, at der er en meget stor risiko for, at forslaget vil krænke telebrugeres grundlæggende rettigheder, der er sikret af EU-retten.

Med forslaget kan Justitsministeriet efter forhandling med erhvervsministeren iværksætte generel og udifferentieret logning, hvis det vurderes, at der forelægger en alvorlig trussel mod den nationale sikkerhed. Dette kan ske udenom Folketinget, og en sådan beslutning vil ikke være underlagt domstolskontrol.

Danske Advokater mener, at det retssikkerhedsmæssigt er stærkt betænkeligt, og vi vil kraftigt advare imod, at man vedtager lovforslaget i sin nuværende form.

Vi anerkender naturligvis, at der er en vanskelig balance mellem sikkerhed og personlig frihed.

Danske Advokater har en række konkrete anbefalinger og tekniske bemærkninger, som er udfoldet i vedlagte høringsnotat. Vi håber, at man fra ministeriets side vil se positivt og konstruktivt på disse.

Vi står naturligvis til rådighed med vores faglighed, hvis det ønskes.

Med venlig hilsen
Danske Advokater
Danielle Løw
Juridisk konsulent

Bemærkninger om ændring af retsplejeloven og logning

til JM

Vi vil henholde os til bemærkninger indsendt af it-politisk forening.

mvh
Keld Simonsen
Formand, KLID

Fra: Anette Høyrup <ah@fbr.dk>
Sendt: 4. november 2021 11:05
Til: Justitsministeriet <jm@jm.dk>
Cc: Forbrugerrådet <hoeringer@fbr.dk>
Emne: SV: Høring over udkast til ,lovforslag on ændring af retsplejeloven og lov om elektroniske kommunikationsnet og -tjeneste (Revision af logningsreglerne m.v.) J.nr. 2020-187-0036

Til Justitsministeriet

Forbrugerrådet Tænk har desværre ikke haft ressourcer til at prioritere nærværende høring, men vi vil gerne opmærksom på – trods fristoverskridelsen – at vi til fulde støtter Rådet for Digital Sikkerheds høringssvar. Vi er repræsenteret i Rådet, hvor forslaget har været diskuteret og høringssvaret udarbejdet.

Med venlig hilsen

Anette Høyrup
Chefjurist / Chief Legal Adviser

T +45 7741 7738 / M +45 2715 7432 / taenk.dk
Fiolstræde 17 B / Postboks 2188 / 1017 København K

Forbrugerrådet
Tænk
Danish Consumer Council