TELE INDUSTRIEN
teleselskabernes branchesamarbejde

3. maj 2021

Notat
TI's input til Justitsministeriet efter 4. møde om revision af logningsreglerne mv. (28. april 2021) – Bemærkninger til nye krav i lovskitsen, herunder omkostningsestimat

Nedenfor findes TI's bemærkninger til nye krav i lovskitsen, som ikke er blevet berørt i de løbende tekniske drøftelser mellem Telebranchen og Rigspolitiet forud for Justitsministeriets fremlæggelse af lovskitsen. Notatet følger desuden op på emner, som blevet drøftet på Justitsministeriets møder den 28. april 2021 om revision af reglerne om logning mv.

Følgende emner berøres i dette notat:
A. Hvilke lokaliseringsdata skal logges – opdeling?
B. Hastesikring – typer af data, forbud mod aggregering og domstolskontrol
C. Fælles format og dataintegritet
D. Tilstrækkelig kapacitet til opfyldelse af nye logningskrav
   - omkostningsestimat og implementeringsfrist
E. Iværksættelse af målrettet personbestemt logning efter 118-opslag (ikke CPR-opslag)
F. Brugerregistrering mhp. målrettet logning
G. Generel logning af IMEI-numre som identitetsoplysning
H. MAC-adresser
I. Teknologineutrale regler – dialog om formulering af nye regler

TI henviser desuden til de to tidligere fremsendte notater den 27. april 2021 om
(a) TI's input og svar på Justitsministeriet spørgsmål om *tekniske forhold og procedurer* (herefter 'TI's notat om tekniske forhold og procedurer'), og
(b) TI's input om *juridiske forhold, begrebsafklaring og udlevering af teledata* (herefter 'TI's notat om juridiske forhold og begrebsafklaring').

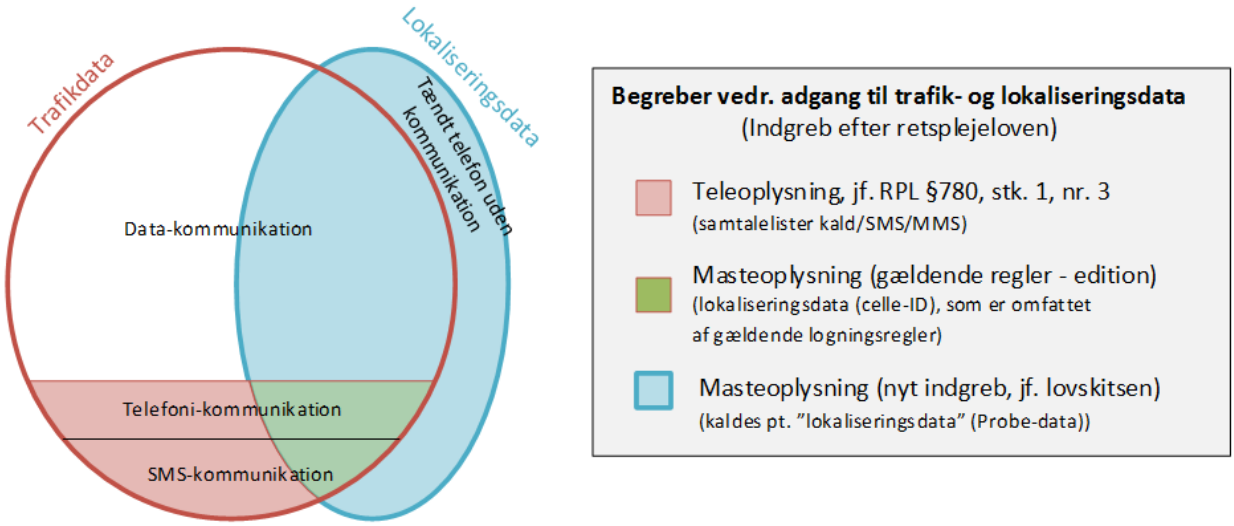
A. Hvilke lokaliseringsdata skal logges – opdeling?

I pkt. 2 i 'TI's notat om tekniske forhold og procedurer' oplyser TI, at lokaliseringsdata fra mobilnetværksudbydernes analysesystemer (prober) kun kan leveres samlet til politiet. Som drøftet på mødet den 28. februar 2021 skal det præciseres, at udtalelsen i pkt. 2 vedrørte de gældende muligheder i netudbydernes probe-systemer. Hvis der indføres nye regler om generel logning hhv. målrettet logning af trafik- og lokaliseringsdata, som findes i analysesystemerne, vil netværksudbyderne være nødsaget til at etablere IT-systemer med processorkapacitet, der understøtter de nye regler, og i den forbindelse kan der samtidig udvikles løsning til filtrering og frasortering af fx lokaliseringsdata ifm mobildatakommunikation. I en kommende ny situation, hvor der er vedtaget sådanne nye regler om logning, vil en eventuel opdeling/filtrering således kunne lade sig gøre.

TI bemærker dog, at enhver behandling med henblik på opdeling/filtrering indebærer en risiko for fejl og datatab.

TI bemærker endvidere, at den gruppe af lokaliseringsdata, som ikke er nævnt i lovskitsen – nemlig lokaliseringsdata ifm. mobildatakommunikation – i er den gruppe af lokaliseringsdata, som indeholder flest registreringer (i gennemsnit 1000 registreringer af masteoplysning pr. døgn, pr. kunde) – her illustreret, som den del af fællesmængden mellem trafik- og lokaliseringsdata, som er markeret med kun BLÅ:

Illustration af trafik- og lokaliseringsdata for mobiltjenester



Dertil kommer, at den gældende bestemmelse i retsplejeloven § 786, stk. 4 fra 2002, allerede giver hjemmel til at udstede regler om logning af lokaliseringsdata ifm. mobilkommunikation (inden for rammerne af EU-dommene). TI foreslår, at det undersøges i hvilket omfang de forskellige grupper af lokaliseringsdata er omfattet af logningsregler i andre EU-lande, og TI henstiller, at regler om logning ikke går videre end logningsregler fastsat i andre europæiske lande. Det er således efter TI's opfattelse vigtigt, at regler om logning af teledata udspringer af en **fælles EU-forståelse**.

TI bemærker, at hvis der udstedes regler om logning af lokaliseringsdata ifm. datakommunikation, vil netværksudbyderne være nødsaget til at etablere en langt større lagerkapacitet til opbevaring af loggede lokaliseringsdata, end hvis der ikke udstedes regler om logning af lokaliseringsdata ifm. datakommunikation. Hvis der omvendt ikke udstedes regler om logning af lokaliseringsdata ifm. datakommunikation, vil netværksudbyderne være nødsaget til at etablere it-løsning og processorkapacitet til filtrering og frasortering af fx lokaliseringsdata ifm mobildatakommunikation. Det skønnes, at omkostningerne vil være i samme størrelsesorden for de nævnte to scenarier.

TI henstiller kraftigt, at det ikke pålægges telebranchen at udvikle løsning til filtrering og frasortering af lokaliseringsdata ifm. mobildatakommunikation, hvis der så efterfølgende alligevel udstedes regler om logning af alle lokaliseringsdata. I så fald vil byrden blive dobbelt for telebranchen.

B. Hastesikring – typer af data, forbud mod aggregering og domstolskontrol

I lovskitsen (side 48) anføres følgende om tidsmæssig udstrækning af hastesikring (vores fremhævelse):

> ”Det vil også kunne påhvile politiet at vurdere og beslutte et pålægs tidsmæssige udstrækning. Ved et pålægs tidsmæssige udstrækning forstås den periode, som udbyderne forpligtes til at opbevare den pågældende data i. Fælles for både den omhandlede data og opbevaringsperioden er, at politiet skal begrænse dette til det strengt nødvendige”.

TI bemærker hertil, at hastesikring af data i sagens natur sker bagudrettet, dvs. efter at den kriminelle handling er begået. I modsætning til loggede data, som ikke nødvendigvis (og faktisk kun sjældent) skal udleveres til politiet, forventes hastesikrede data altid at skulle udleveres til politiet, så snart politiet har indhentet rettens kendelse til udleveringen. På den baggrund forudsætter TI, at hastesikringsperiodens længde maksimalt skal fastsættes til 3 måneder svarende til den gældende regel i RPL § 786a. TI anmoder om at den maksimale hastesikringsperiode som hidtil fastsættes direkte i retsplejelovens regel om hastesikring.

I lovskitsen (side 48) anføres følgende om hastesikrede data (vores fremhævelse):

> ”Der forudsættes ikke forudgående høring af adressaterne for pålægget, som endvidere vil være pligtige til at efterkomme pålægget straks efter modtagelse. Den udbyder, der mødes med et pålæg om hastesikring, vil kunne være forpligtet til at sikre integriteten af den data, som er genstand for pålægget, og pålægget vil gælde for dataen i udbyderens samlede net. Det foreslås, at dette indebærer, at der ikke må ske aggregering af dataen i forbindelse med sikringen og opbevaringen.”

Mht. sætningen (side 48) om, at pålæg om hastesikring af data vil gælde for data i udbyderens samlede net, bemærker TI, at det er nødvendigt, at politiets begæringer om hastesikring er fuldstændig præcise med hensyn til, hvilke data, der skal hastesikres.

TI henstiller og forudsætter, at pålæg om hastesikring af trafik- og lokaliseringsdata specificeres mht. hvilke konkrete datatyper, der skal sikres, og at pålæg om hastesikring benytter fuldstændig samme terminologi og definitioner, som vil blive brugt i de kommende nye regler og bekendtgørelser om logning af trafik- og lokaliseringsdata.

Det bemærkes, at TI anser logning af trafik- og lokaliseringsdata hhv. hastesikring af trafik- og lokaliseringsdata for at være to sider af samme sag, idet begge dele omfatter lagring af trafik- og lokaliseringsdata, dog således at logning sker fremadrettet, mens hastesikring sker bagudrettet. TI forudsætter derfor også, at de kommende nye regler om udlevering af trafik- og lokaliseringsdata (efter rettens kendelse herom) vil være de samme, uanset om der er tale om loggede data eller hastesikrede data. TI anmoder om, at Justitsministeriet tilkendegiver, hvis ministeriet ser det anderledes, og at der i så fald sker en afklaring og drøftelse med branchen forud for færdiggørelsen af lovforslaget.

TI bemærker desuden, at et eventuelt krav om ”dobbelt” hastesikring af trafik- og lokaliseringsdata, som opsamles parallelt både i netværksudbydernes analysesystemer (prober) og i CDR-data

ikke vil være acceptabelt. Det skal således være teleudbyderens eget valg ud fra en teleteknisk og it-mæssig vurdering at beslutte, hvordan og hvor de forskellige grupper af data, omfattet af et krav om enten logning eller hastesikring, skal opsamles og lagres.

TI henstiller på denne baggrund, at sætningen "*pålægget vil gælde for dataen i udbyderens samlede net*" ikke indgår i det kommende lovforslag, da det ikke står klart, hvad hensigten med formuleringen er.

I lovskitsen (side 48) anføres følgende om hastesikrede data (vores fremhævelse):

> "Der forudsættes ikke forudgående høring af adressaterne for pålægget, som endvidere vil være pligtige til at efterkomme pålægget straks efter modtagelse. Den udbyder, der mødes med et pålæg om hastesikring, vil kunne være forpligtet til at sikre integriteten af den data, som er genstand for pålægget, og pålægget vil gælde for dataen i udbyderens samlede net. Det foreslås, at dette indebærer, at der ikke må ske aggregering af dataen i forbindelse med sikringen og opbevaringen."

TI er uforstående over det anførte på side 48 om, at hastesikrede data ikke må aggregeres. Der sker således ikke en aggregering af de lokaliseringsdata fra mobilnetværkudbydernes analysesystemer (prober), som hastesikres i dag efter de gældende regler. Lokaliseringsdata fra mobilnetværkudbydernes analysesystemer (prober) er således "rå data".

Det bemærkes, at mobiludbyderne til takseringsformål registrerer aggregerede data om volumenforbrug af mobildatakommunikation baseret på CDR-data. Tidsstemplingen af sådanne data relaterer sig til takseringstidspunktet og ikke til de enkelte datasessioner. Ifm "teledatasagen" i 2019 er Rigspolitiet blevet gjort opmærksom på, at disse takseringsdata ikke har efterforskningsmæssig værdi og ikke bør indgå i levering af teleoplysning til politiet.

Hvis det anførte i sidste sætning indebærer krav om logning/hastesikring af ikke-aggregeret volumenforbrug af mobildata, herunder tidsstempling af datasessioner, må telebranchen kraftigt protestere over forslaget, som i så fald svarer til logning af datasessioner blot uden IP-IP og dermed en genindførelse af sessionslogning.

Hvis der menes noget andet, opfordrer TI til en afklaring og drøftelse med telebranchen forud for fremsættelsen af lovforslag.

Under alle omstændigheder henstiller TI, at det sidste punktum i det citerede afsnit om forbud mod aggregering af data ikke indgår i det kommende lovforslag, da det ikke står klart, hvad hensigten med formuleringen er.

I lovskitsen (side 48) anføres følgende om domstolskontrol ifm. hastesikring (vores fremhævelse):

> "Endelig vil der kunne sikres mulighed for, at et pålæg om hastesikring på begæring kan indbringes for domstolene med henblik på at opnå rettens stillingtagen til, hvorvidt betingelserne for at pålægge hastesikring i den konkrete situation er opfyldt. Indbringelse for retten foreslås dog ikke at have

opsættende virkning."

Det bemærkes hertil, at teleudbyderne ikke på nogen måde ønsker at påtage sig ansvaret for at vurdere om politiets iværksættelse af hastesikring opfylder kriterierne herfor (grov kriminalitet). La Quadrature du Net-dommen synes endvidere at konkludere, at afgørelser om hastesikring skal være underlagt en effektiv domstolsprøvelse.

TI anmoder derfor om, at der fastsættes regler om, at afgørelser om hastesikring altid efterfølgende automatisk skal forelægges for retten til godkendelse – svarende til princippet i retsplejelovens § 783, stk. 4 om rettens godkendelse af øjemed-indgreb.

C. Fælles format og dataintegritet

I lovskitsen anføres følgende (vores fremhævelse):

> (side 27 og 39): "Det er endvidere Justitsministeriets opfattelse, at der vil kunne fastsættes nærmere tekniske krav til udbydernes logning, herunder nærmere regler om opbevaringsformat, foranstaltninger med henblik på at sikre oplysningernes integritet og beskyttelse mod uautoriseret adgang, opbevaringssted mv. Det vil medvirke til at sikre, at der løbende kan ske den fornødne tilpasning i lyset af den teknologiske udvikling".
>
> (side 27 og 40): "Det foreslås, at i det omfang, der måtte blive fastsat regler om et fælles opbevaringsformat, og dette adskiller sig fra det af teleudbyderen anvendte, vil det påhvile udbyderen at foretage konvertering af den relevante data, herunder sikring af den fornødne dataintegritet og -kvalitet. …"

Baggrunden for forslaget om fælles opbevaringsformat er ikke nærmere begrundet. 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.

Mht. (3) koordinatsystem har TI i forlængelse af TI's svar på pkt. 18 i 'TI's notat om tekniske forhold og procedurer' undersøgt, hvilke koordinatsystemer de 4 mobilnetværksudbydere benytter i dag i de basestation-tabeller, som løbende sendes til Rigspolitiet. Det viser sig, at 3 ud af de 4 mobilnetværksudbydere allerede benytter det koordinatsystem, WGS84, som Rigspolitiet efterspørger. Den fjerde mobilnetværksudbyder, TDC Net, har oplyst, at selskabet kan tilbyde at skifte fra det nuværende koordinatsystem ED50 til koordinatsystem WGS84, som Rigspolitiet ønsker. TDC's skifte af koordinatsystem vil kunne iværksættes efter nærmere aftale mellem TDC og Rigspolitiets Telecenter. TI kan i øvrigt oplyse, at der i praksis tilsyneladende er 1:1 overensstemmelse mellem WGS84 og det fælleseuropæiske ETSR89, som TI pegede på i pkt. 18 i 'TI's notat om tekniske forhold og procedurer'.

Mht. (4) kundedata, som registreres i tjenesteudbydernes administrative systemer, i form af navn, adresse og telefonnummer (nummeroplysningsdata) indberettes allerede i et fælles format til 118-databasen, som også benyttes af Rigspolitiets Telecenter.

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 trafik- og lokaliseringsdata (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 lokaliseringsdata (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 <u>som hidtil</u> 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** på side 27 og 40 i lovskitsen 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.

Der findes over 100 tjenesteudbydere, der udbyder mobiltjenester. Der henvises til TI's høringssvar fra december 2006 om samkøring (vedhæftet).

På denne baggrund opfordrer telebranchen til, at krav om fælles opbevaringsformat ikke indgår i det kommende lovforslag.

Det bemærkes i øvrigt, at lovskitsen taler om "opbevaringsformat", mens Rigspolitiets forslag og ønsker, som Justitsministeriet har rundsendt 23. april 2021, taler om "leveringsformat". Det bør afklares, hvad forslaget reelt vedrører. TI henviser desuden til de parallelt fremsendte konkrete input til Rigspolitiets forslag og ønsker.

D. Tilstrækkelig kapacitet til opfyldelse af nye logningskrav - omkostningsestimat og implementeringstid

I lovskitsen anføres følgende (vores fremhævelse):

> (side 27 og 40) "… Det følger af telelovens § 10, stk. 1, nr. 1, at det påhviler udbyderne uden udgift for staten at sikre, at deres tekniske systemer og tekniske udstyr er indrettet således, at politiet kan få adgang til oplysninger om bl.a. teletrafik. Det foreslås, at denne ordning videreføres. Udbyderne vil således være forpligtede til at indrette deres tekniske systemer og tekniske udstyr således, at de har kapaciteten til at understøtte de krav, som forslagene medfører."
>
> (side 40) "Det vil dog kunne fastsættes nærmere regler om økonomisk godtgørelse for udgifter forbundet med et konkret pålæg om personbestemt eller geografisk målrettet logning. De nærmere regler vil kunne omfatte regler om betingelserne for at yde godtgørelse for udgifter forbundet med et konkret pålæg mv., om standardtakster for godtgørelsen og eventuelt om betingelser for at yde godtgørelse ud over standardtaksterne. I det omfang sådanne regler fastsættes, forudsættes det, at der ikke ydes godtgørelse ud over standardtaksterne, medmindre der ekstraordinært måtte være tale om, at et konkret pålæg mv. medfører uforholdsmæssige udgifter for en udbyder."

TI forstår bemærkningen om "kapacitet" på side 27 og 40 således, at teleudbyderne skal sikre it-systemer, herunder processorkapacitet og lagerkapacitet, som kan understøtte lovskitsens krav om generel logning hhv. målrettet logning af trafik- og lokaliseringsdata, herunder logning af lokaliseringsdata fra analysesystemerne (prober), som ikke er omfattet af de gældende logningskrav. Hvis bemærkningen om "kapacitet" på side 27 og 40 skal forstås på en anden måde, opfordrer TI til en afklaring og drøftelse forud for færdiggørelsen af lovforslaget. TI henviser i øvrigt til pkt. 4 i 'TI's notat om tekniske forhold og procedurer' om, at registreringen af lokaliseringsdata i netudbydernes analysesystemer (prober) sker efter "best effort".

TI bemærker, at de kommende nye regler især vil stille store krav til processorkraft til opsamling, filtrering og udlevering af lokaliseringsdata fra analysesystemerne. Sådanne it-systemer vil være rene efterforskningsmæssige værktøjer, som teleselskaberne på ingen måde har egen-interesse i

at udvikle. TI henstiller derfor, at alle omkostninger til udvikling og drift af sådanne it-løsninger dækkes af staten.

Som efterspurgt af Justitsministeriet på mødet den 14. april 2021 har TI – på det foreløbige grundlag – regnet på branchens omkostninger forbundet med opfyldelsen af de forventede nye krav, og TI skønner, at etableringsomkostningerne til it-systemer, der understøtter lovskitsens krav om generel logning hhv. målrettet logning af trafik- og lokaliseringsdata, herunder logning af lokaliseringsdata fra analysesystemerne (prober), som ikke er omfattet af de gældende logningskrav, vil være ca. 50 mio. kr. Der tages forbehold for, at selskaberne endnu ikke kender detaljerne i de mulige nye krav, og derfor heller ikke kan foretage en mere præcis omkostningsvurdering.

Dertil kommer etableringsomkostninger til systemunderstøttelse af CPR-opslag mv., som alene os de største udbydere kan løbe op i yderligere et større to-cifret millionbeløb, jf. nærmere herom nedenfor pkt. E.

TI vil gerne kvittere for lovskitsens beskrivelse på side 40 af muligheden for økonomisk godtgørelse for udgifter ifm. løbende iværksættelse af målrettet logning. Dette vil svare til den gældende praksis for udgifter ifm. teleudbydernes bistand til politiet, jf. princippet i RPL § 786, stk. 8 og § 804, stk. 5, hvilket TI finder meget positivt.

Med hensyn til implementering af de nye regler, bemærkes, at teleselskaberne – til brug for udvikling og indretning af it-løsninger til understøttelse af nye regler om målrettet logning samt til brug for understøttelse af nye regler om generel logning hhv. målrettet logning af nye grupper af lokaliseringsdata, som ikke er omfattet af de gældende logningsregler – har behov for en implementeringsfrist på ca. 15 måneder fra datoen, hvor de nye krav og regler er endelig kendt.

E. Iværksættelse af målrettet personbestemt logning efter politiets 118-opslag (ikke CPR-opslag)

I lovskitsen (side 33) anføres følgende (vores fremhævelse):

> ”Der foreslås endvidere, at der fastsættes nærmere regler om, hvordan det afgøres hvilke telefoner eller kommunikationsenheder, der konkret vil være omfattet af den personbestemte målrettede logning. Dette kan f.eks. indebære, at teleudbydere modtager CPR-numre på de personer, som er genstand for målrettet logning, hvorefter det vil påhvile udbyderne at foretage logning af de abonnementer og enheder, der er tilknyttet den pågældende person. En sådan indretning vil således imødegå, at målpersoner skifter telefoner eller abonnementer.”

Som drøftet på møderne med Justitsministeriet i april 2021, og som forklaret i TI’s skriftlige svar på Justitsministeriet spørgsmål nr. 5, stillet den 14. april 2021, henstiller TI, at politiets identifikation af fokusnumre, der skal logges målrettet sker via politiets efterforskning bl.a. via 118-opslag – og IKKE på baggrund af CPR-opslag i teleselskabernes kundedata. TI henstiller derfor, at en ordning med CPR-opslag i kundedata i teleudbydernes administrative systemer IKKE indgår i det kommende lovforslag,

TI henstiller, at iværksættelse af personbestemt målrettet logning af trafik- og lokaliseringsdata skal ske ved angivelse af personens telefonnumre i politiet pålæg – på samme måde som kendelser om udlevering af trafik- og lokaliseringsdata efter de gældende regler skal indeholde oplysning om telefonnummer, jf. RPL § 783. En sådan ordning vil kun involvere de fire udbydere af mobilnetværk, samt eventuelt udbydere af fastnet, hvis reglerne om målrettet personbestemt logning også skal omfatte fastnet- og IP-telefoni.

En ordning baseret på, at teleudbyderne skal foretage opslag af CPR-numre og kundenavne i de registrerede kundedata, som findes i tjenesteudbydernes administrative systemer, vil udgøre en stor administrativ byrde, der vil ramme hver af de mere end 100 danske udbydere af nummerbaserede telefoni- og mobiltjenester. Samtidig vil en sådan ordning reelt indebære, at teleudbyderne inddrages i efterforskningsmæssige overvejelser om fortolkningen af registrerede kundedata, som ikke svarer præcist til de data registreret i Folkeregisteret, som politiet kan fremlægge. Som fiktivt eksempel man forestille sig, at en kunde er registreret hos teleudbyderen som ”Renée Rasmussen” på ”Sortevej 47”, men i Folkeregisteret er samme person registreret som ”René Rasmussen” på ”Sortevej 47B”, jf. eksemplet som indgår i TDC’s mail omtalt nedenfor. Teleudbyderne ønsker i en sådan situation ikke at påtage sig nogen form for ansvar for, om der skal iværksættes målrettet logning eller ej.

Desuden vil iværksættelse af personbestemt målrettet logning på baggrund af CPR-nummer eller kundenavn forhindre, at der kan etableres automatiserede løsninger (API) for iværksættelse af målrettet personbestemt logning, som er stort ønske for telebranchen, jf. vores svar på Justitsministeriets spørgsmål 10, stillet den 14. april 2021.

Rigspolitiet og Justitsministeriet har på møde nr. 4 om revision af logningsreglerne den 28. april 2021 oplyst, at baggrunden for Rigspolitiets ønske om, at tjenesteudbyderne skal forestå arbejdet med at identificere fokuspersonens telefonnumre via opslag på CPR og/eller kundenavn i tjenesteudbydernes administrative systemer med kundedata, i stedet for at politiet selv identificere kundens telefonnumre via politiets adgang til 118-databasen, er, at Rigspolitiet har oplevet visse udfordringer med politiets adgang til 118-databasen.

TDC, som er forsyningspligtudbyder af 118-databasen, har i mail den 3. maj 2021 til Justitsministeriet bekræftet, at Rigspolitiets Telecenter har visse problemer med politiets daglige opdatering af 118-data i politiets egne systemer, men at TDC og Rigspolitiet er i dialog om flere forskellige løsninger på denne problemstilling (problemstilling nr. 1).

TDC’s oplyser desuden i mailen (problemstilling nr. 2), at det kan forekomme, at de nummeroplysningsdata, som indberettes af udbydere af teletjenester til 118-databasen, ikke omfatter abonnentens/kundens navn og adresse, men kun navn og adresse på den bruger, som kunden har overladt telefonabonnementet til, fx kundens ægtefælle. 118-databasen giver imidlertid mulighed for flere optagelser på samme telefonnummer, og denne problemstilling vil derfor kunne løses – fx ved en præcisering af pkt. 6 i bilag til bkg. nr. 435 af 9/5/2011 om nummeroplysningsdatabaser, https://www.retsinformation.dk/eli/lta/2011/435, som TDC gennemgår i mailen. TI bemærker hertil, at det generelt ikke er muligt for teleudbydere at validere oplysninger om ”brugeren”, dvs.

hvem kunden har overladt telefonabonnementet til, medmindre der er tale om et fastnetabonnement, hvor leveringen sker til en anden installationsadresse end kundens adresse.

TDC bekræfter i mailen, at hvis ovenstående problemstilling nr. 2 adresseres, vil 118-databasen give politiet et samlet overblik over samtlige mere end 100 teleudbyderes kundedata/nummeroplysningsdata (navn/adresse/telefonnumre) for de mere end 12 mio. danske telefonnumre, som er i drift, herunder kundedata registreret med eventuelle indtastningsfejl i teleudbydernes kundedata.

Som det fremgår af mailen fra TDC, er over halvdelen af de indberettede data til 118-databasen ikke tilgængelige for offentligheden (hemmelige numre), men kun for politiet og andre myndigheder. 118-databasen er således i høj grad først og fremmest et værktøj, som har til formål at sikre politiet et overblik over teleudbydernes kundedata i form af kundenavn, kundeadresse og telefonnummer. Følgende fremgår da også af bemærkningerne til den netop reviderede § 14, stk. 2, nr. 4 i teleloven, jf. L42 fremsat 8. oktober 2020:

> (side 92) "Det skal i den forbindelse bemærkes, at politiet m.fl. anvender adgangen til nummeroplysningsdata i deres arbejde. Adgangen til nummeroplysningsdata anvendes hyppigt af politiet, f.eks. ved efterforskningen af sager om alvorlig kriminalitet. Nummeroplysningsdata anvendes således i forbindelse med blandt andet iværksættelse af aflytning eller indhentning af historiske teleoplysninger. Nummeroplysningerne anvendes også som grundlag for geografisk stedfæstelse af opkaldende part i politiets vagt- og alarmcentraler (114- og 112-opkald) med henblik på udkald."
>
> (side 95) "Som nævnt under gennemgangen af den foreslåede § 14, stk. 2, bemærkes, at politiet m.fl. anvender adgangen til nummeroplysningsdata i deres arbejde. Der er derfor behov for, at der fortsat vil være en udtømmende nummerfortegnelse svarende til den, der vedligeholdes i dag under forsyningspligten. Det er hensigten, at klima-, energi- og forsyningsministeren forlænger forsyningspligten på en udtømmende nummerfortegnelse, indtil Justitsministeriet måtte vurdere, at en udtømmende nummerfortegnelse bedre kan leveres på anden vis end under forsyningspligten."

TI finder det ikke rimeligt, hvis over 100 tjenesteudbydere pålægges administrative byrder i form af daglige CPR-opslag i deres administrative systemer med kundedata, når branchen via forsyningspligtreglerne samtidig er pålagt at etablere 118-databasen, som i høj grad er et værktøj, der opfylder politiets behov for adgang til kundedata.

TI skønner, at etableringsomkostninger til systemunderstøttelse af CPR-opslag mv. alene hos de største udbydere kan løbe op i et større to-cifret millionbeløb, og dertil kommer årlige driftsomkostninger.

At pålægge telebranchen så store økonomiske og administrative byrder forekommer både urimeligt og uhensigtsmæssigt – når politiet har en samlet adgang til præcis de samme kundedata via

118-databasen. Det vil være samfundsmæssigt spild at pålægge telebranchen opgaver, som politiet langt bedre kan klare selv ved brug af eksisterende muligheder.

For god ordens skyld bemærkes i øvrigt, at udlevering af oplysning til politiet om, hvorvidt en navngiven person eventuelt er registreret med CPR-nummer i teleselskabets administrative systemer, efter TI's opfattelse forudsætter editionskendelse.

F. Brugerregistrering i form af kundedata, som registreres i administrative systemer

I lovskitsen (side 55) anføres følgende (vores fremhævelse):

> "Det vil blive nærmere overvejet, om der herudover er behov for yderligere at forpligte teleudbydere mv. til at foretage registrering og opbevaring af oplysninger om alle brugeres civile identitet, både fysiske eller juridiske personer, herunder navn, adresse og telefonnumre for både fastnet- og mobilabonnenter og SIM-kortnumre (IMSI-nummer) …"

TI vil gerne kvittere positivt for Justitsministeriets tilkendegivelse på mødet den 28. april 2021 om, at det anførte om "alle brugeres" civile identitet skal forstås som "abonnenternes" identitet, som er registreret i kundedata i tjenesteudbydernes administrative systemer – og således IKKE skal forstås som identiteten på de brugere, som kunden/abonnenten overlader abonnementet til.

Det ville have været en enorm og praktisk umulig byrde at løfte for de mere end 100 danske teleselskaber, der udbyder teletjenester til slutbrugere (tjenesteudbyderne) at registrere navn og adresse på de brugere, som kunden/abonnenten overlader mobilabonnementet til – dvs registrering af navn og adresse på erhvervskunders ansatte og privatkunders nærtstående.

Det bemærkes i øvrigt, at abonnentens/kundens eventuelle oplysninger om brugerens navn og adresse ikke kan valideres for mobilabonnementer.

Som anført i pkt. 8 i 'TI's notat om juridiske forhold og begrebsafklaring' opfordrer TI til, at det i det kommende lovforslag præciseres, at der med "bruger" menes "slutbruger", jf. telelovens § 2 nr. 3, som er den juridiske aftalepart (kunden/abonnenten), som indgår aftale med tjenesteudbyderen.

TI er i denne forståelse enig i det anførte på side 51 i lovskitsen, hvor følgende er anført:

> *"Oplysninger om identiteten på brugerne af elektroniske kommunikationsmidler må efter Justitsministeriets opfattelse omfatte abonnentoplysninger i form af den fysiske eller juridiske persons navn, adresse og telefonnumre for både fastnet- og mobilabonnenter, og for mobilabonnenters vedkommende også numre, der identificerer det anvendte mobilabonnement, f.eks. IMSI-numre."*

TI kan supplerende oplyse, at følgende "kundedata", som kan være af interesse for politiets efterforskning, registreres i de mere end 100 tjenesteudbyderes administrative systemer:

- Kundens/abonnentens navn og adresse, som oplyst ved aftaleindgåelsen
- CVR-nummer på erhvervskunder
- Evt. CPR-nummer på privatkunder
- Evt. særskilt installationsadresse (kun for abonnementer med fast installation)
- Kredsløbsnummer for bredbåndsabonnementer med fast forbindelse
- Fast IP-adresse, hvis et bredbåndsabonnement omfatter fast IP (sjældent)
- Telefonnummer/MSISDN for mobilabonnementer og telefoniabonnementer
- SIM-kortnummer/IMSI-nummer for mobilabonnementer

Bemærk, at IMEI-nummer ikke registreres som en del af kundedata i tjenesteudbyderes administrative systemer. IMEI-nummer registreres kun i netværkssystemerne.

Politiet har efter de gældende regler uden kendelse adgang til aktuelle kundedata/administrative oplysninger som oplistet ovenfor om de danske teleudbyderes egne kunder, jf. telelovens § 13 (identitetsoplysninger) hhv. telelovens § 31 (118-data). Adgang til ikke-aktuelle historiske kundedata udleveres efter kendelse.

Det bemærkes, at telefonnummer/MSISDN og IMSI-nummer for de danske teleudbyderes egne kunder registreres både som kundedata i tjenesteudbyderes administrative systemer og som trafik- og lokaliseringsdata i netudbydernes trafiksystemer og centraler. Telefonnummer og IMSI-nummer er således ”nøgle” til at sammenholde trafik- og lokaliseringsdata fra netværksudbyderens trafiksystemer og centraler med kundedata i tjenesteudbydernes administrative systemer, jf. nærmere beskrivelse i pkt. 5 ’TI’s notat om tekniske forhold og procedurer’.

G. Generel logning af IMEI-numre som identitetsoplysning

TI vil gerne kvittere for Energistyrelsens gennemgang og forklaring på mødet den 28. april 2021 om, at IMEI-nummer (mobilterminal-nummer), som kan registreres i netværkssystemerne, kan kategoriseres som ”en identitetsoplysning”, som ikke i sig selv er ”trafik- og lokaliseringsdata”. TI bemærker, at det bør afklares om samme betragtning kan gøres gældende for IMSI-nummer og for telefonnummer (MSISDN), som registreres i netværkssystemerne.

TI bemærker, at det er muligt, at IMEI-nummer som anført af Energistyrelsen registreres ”frivilligt” af teleudbyderne og ikke som sådan er nødvendig for trafikafviklingen, men registreringen sker dog udelukkende i ”trafikmaskinen”, og synes dermed umiddelbart også at kunne kategoriseres som trafik- og lokaliseringsdata, jf. i øvrigt definitionen af ”lokaliseringsdata” i artikel 2 i e-databeskyttelsesdirektivet (2002/58/EF), som er citeret flere steder i lovskitsen (vores fremhævelse):

> c) »lokaliseringsdata«: data, som behandles i et elektronisk kommunikationsnet og angiver den geografiske placering af det terminaludstyr, som brugeren af en offentligt tilgængelig elektronisk kommunikationstjeneste anvender

TI opfordrer til, at spørgsmålet om kategoriseringen af IMEI-nummer som en identitetsoplysning, som ikke er omfattet af definitionen af "trafik- og lokaliseringsdata" for god ordens skyld – og for at undgå begrebsforvirring i de kommende nye logningsregler – forelægges for Erhvervsstyrelsen, som er ansvarlig myndighed for reglerne i e-databeskyttelsesdirektivet.

Uanset hvilken konklusion Erhvervsstyrelsen kommer frem til henstiller TI, at der ved den kommende revision af logningsreglerne – hvis der er politisk flertal herfor – fastsættes selvstændige og klare regler om eventuel generel logning af IMEI-nummer (og sammenhængen til IMSI- og telefonnummer).

Der henvises desuden til TI's bemærkninger om logning og udlevering af IMEI-oplysning i pkt. 5 i 'TI's notat om juridiske forhold og begrebsafklaring'.

H. MAC-adresser

Det fremgår på side 51 og 55 i lovskitsen, at det vil blive pålagt krav om registrering af MAC-adresser – fx fremgår følgende på side 51 i lovskitsen:

> *Det vurderes på den baggrund, at der tillige kan pålægges registrering og opbevaring af oplysninger, der entydigt identificerer den enhed (mobiltelefon, tablet, PC mv.), som brugeren ejer eller anvender (herunder IMEInumre og MAC-adresser mv.).*

Som også anført i pkt. 7 i 'TI's notat om juridiske forhold og begrebsafklaring' bemærker TI, at det ikke er muligt at logge MAC-adresser, idet MAC-adresser hverken findes som trafik- og lokaliseringsdata i teleudbydernes offentlige net eller i tjenesteudbydernes administrative systemer. Det er derfor ikke en teknisk mulighed for udbydere af traditionelle teletjenester at logge MAC-adresser.

I visse tilfælde kan udbydere af "trådløs internetadgang" (wifi hotspots) registrere MAC-adressen på det udstyr, som trådløst tilgår adgangspunktet/hotspottet, jf. § 5, stk. 2 i den gældende logningsbekendtgørelse.

TI anmoder på den baggrund om, at omtalen af MAC-adresser ikke indgår i det kommende lovforslag. TI bemærker, at MAC-adresser heller ikke er omtalt i lovforslagsbemærkningerne til de gældende logningsregler.

I. Teknologineutrale regler – dialog om formulering af nye regler

Lovskitsen omtaler flere steder, at kommende nye regler om logning skal udformes under hensyntagen til den teknologiske udvikling. TI er helt enig heri, og opfordrer til, at reglerne formuleres bredt nok til at favne nye elektroniske kommunikationstjenester i form af nummerafhængige interpersonelle kommunikationstjenester, herunder OTT-tjenester ("over-the-top" web- og app-baserede kommunikationstjenester), som fx Skype og Messenger m.fl., som allerede på nuværende tidspunkt vurderes at stå for en ikke ubetydelig del af den elektroniske kommunikation.

TI bemærker i øvrigt generelt, at teknologineutralitet ved udformningen af de kommende nye regler om logning er væsentligt, og følgende eksempler bekræfter vigtigheden heraf:

- ➔ Ældre mobilteknologier (2G og 3G) er på vej til at blive udfaset. Med disse teknologier forsvinder bl.a. kredsløbskoblet tale og SMS og alt flyttes med tiden til pakkekoblet trafik (Voice over LTE (VoLTE), Voice over Wifi, SMS/MMS over IP), dvs ligesom datatrafik. Dette ændrer en del på, hvilke trafik- og lokaliseringsdata, der findes i teleudbydernes systemer.
- ➔ Ex 1: Der registreres ikke nødvendigvis IMEI-numre på VoLTE-kald (4G), idet dette er telefonproducent afhængigt. Krav om registrering af trafikdata- og lokaliseringsdata om anvendte mobilterminaler, skal derfor fastsættes teknologineutralt.
- ➔ Ex 2: Der registreres ikke lokaliseringsdata om sidste mast på VoLTE (4G). Kravet om registrering af "første og sidste mast" i de gældende logningsregler stammer fra en tid, hvor der kun fandtes 2G og 3G. Krav om registrering af lokaliseringsdata skal derfor fastsættes teknologineutralt.

Som bekendt ønsker telebranchen ikke, at regler om logning af trafik- og lokaliseringsdata hverken opretholdes eller udvides. Hvis der imidlertid er politisk flertal for at fastsætte regler om logning, stiller TI sig meget gerne til rådighed for en fortsat dialog om konkrete forslag til formulering af teknologineutrale regler om logning af trafik- og lokaliseringsdata og om politiets adgang hertil.