Til Justitsministeriet og Rigspolitiet
c.c.: Rigsadvokaten, Erhvervsstyrelsen, Energistyrelsen, MKEF

Notat om logning og udlevering af teledata til politiet – juridiske emner
(Teleindustriens forslag og ønsker til ændring og præcisering af gældende regler)
Februar 2020

Indholdsfortegnelse

1. Indledning

I forlængelse af Teleindustriens dialog med Justitsministeriet og Rigspolitiet i 2. halvår 2018 om tekniske løsninger ifm. logning af teledata og med henvisning til justitsministerens breve til Teleindustrien (TI) senest ved brev af 12. november 2019 om revisionen af logningsreglerne, vender Teleindustrien (TI) hermed tilbage med TI’s forslag og ønsker til ændring og præcisering af de gældende regler om logning[1] af teledata og om udlevering af teledata til politiet.

Målet med dette notat er, at stille forslag til mere veldefinerede begreber om logning af teledata samt klarere regler om udlevering af teledata med henblik på at lette samarbejdet mellem politiet og

[1] I dette notat bruges begrebet ”registrering” om teleudbydernes opsamling og registrering af data til eget brug, mens begrebet ”logning” bruges om registrering og opbevaring af data en bestemt periode (1 år efter de gældende logningsregler). Begreberne ”logning” og ”registrering” er således synonymer, idet begrebet ”logning” dog indebærer, at teleudbyderne i stedet for at slette opsamlede data, skal gemme og opbevare dataene i en bestemt periode (data retention).

teleudbydere samt sikre optimal retssikkerhed for både teleudbyderne og vores kunder. TI finder, at der generelt er behov for at skabe en bedre sammenhæng mellem logningsreglerne på den ene side og på den anden side retsplejelovens regler om indgreb i meddelelseshemmeligheden og politiets generelle anvendelse af reglerne om edition. Det er TI's ønske, at TI's forslag til ændringer kan indgå som baggrundsmateriale for Justitsministeriet i forbindelse med ministeriets udarbejdelse af lovudkast til kommende ændring i Folketingssamlingen 2020/2021 af retsplejelovens regler om logning og udlevering af teledata, herunder indgå som input til Strafferetsplejeudvalgets arbejde med udmøntningen af pkt. 10 i Justitsministerens Tryghedspakke ("Tryghed og sikkerhed i det offentlige rum", oktober 2019). TI's forslag kan desuden danne udgangspunkt for videre drøftelser mellem Teleindustrien, Justitsministeriet, Rigspolitiet og Rigsadvokaten som led i det lovforberedende arbejde.

For god ordens skyld bemærkes, at Teleindustrien på ingen måde har interesse i, at der fastsættes regler om logning af teledata – og som udgangspunkt ønsker Teleindustrien, hverken at de gældende regler om logning af teledata opretholdes eller udvides. Hvis der imidlertid er politisk ønske og juridisk mulighed for at opretholde og eventuelt udvide krav om logning af teledata, anbefaler TI, at opbevaringsperioden for loggede teledata fastsættes så kort som overhovedet mulig, og at de kommende regler om logning og udlevering tager højde for TI's input som beskrevet i dette notat.

Teleindustrien vil naturligvis altid gerne inden for lovens rammer bistå politiet, og igennem mange årtier har der eksisteret et godt samarbejde mellem teleselskaberne og politiet, hvor teleselskaberne har givet politiet adgang til de data, som teleselskaberne har besiddet, hvis betingelserne for indgreb i meddelelseshemmeligheden har været opfyldt. Frem til ca. år 2000 var der primært tale om indgreb i form af telefonaflytning samt udlevering til politiet af de forbrugsdata i form af opkaldslister (teleoplysning), som teleselskaberne registrerer til brug for regninger.

Imidlertid har teleselskaberne i de seneste år – siden ikrafttrædelsen af logningsbekendtgørelsen i 2007 – været pålagt at logge data, som teleselskaberne enten slet ikke selv har brug for, eller som teleselskaberne selv kun har brug for at registrere i en ganske kort periode. Disse loggede data er efterfølgende blevet udleveret til politiet alene efter reglerne om edition, dvs. uden at der er fastsat præcise regler om tvangsindgreb i forhold til disse loggede data. Dette gør sig bl.a. gældende for data om telekunders historiske lokalisering i telenettet – altså data om kundens geografiske færden op til 1 år tilbage.

Fastsættelse af regler om logning
Teleindustrien finder det uhensigtsmæssigt, at regler om logning af teledata, som teleselskaberne enten ikke selv har brug for, eller som teleselskaberne selv kun har brug for at registrere i en ganske kort periode, hidtil har været fastsat på bekendtgørelsesniveau. Logning af sådanne data, indebærer et element af overvågning, og regler om sådan overvågning bør efter TI's opfattelse fastsættes med direkte lovhjemmel med henblik på Folketingets direkte stillingtagen til spørgsmålet om overvågning.

Fastsættelse af regler om udlevering
På samme måde finder TI det uhensigtsmæssigt, at der findes regler i dansk ret, der pålægger teleudbyderne at logge visse typer af data, som teleselskaberne ikke selv har brug for, eller som teleselskaberne kun har brug for at registrere i en ganske kort periode, hvorefter disse data kan udleveres til politiet alene efter reglerne om edition – dvs også ifm. mindre lovovertrædelser. Teleindustrien ønsker, at der for hver type af data, som Teleindustrien pålægges at opbevare i en længere periode end Teleindustrien selv har brug for (logning), skal fastsættes klarere og præcise regler om de nærmere

betingelser for politiets adgang til den pågældende datatype, herunder tages stilling til graden af kriminalitet, der kan udløse politiets indgreb. Sådanne regler bør fastsættes ved lov i form af regler om præcist definerede tvangsindgreb – svarende til reglerne i retsplejelovens kapitel 71 om indgreb i meddelelseshemmeligheden og om teleobservation. Tilsvarende gør sig gældende i forhold til fortrolige data, som ikke er omfattet af logningskrav, jf. nærmere herom i pkt. 4.

Konkret anbefaler TI således, at der skabes præcis og direkte lovhjemmel både med hensyn til, hvilke typer af teledata, der skal logges, og med hensyn til veldefinerede tvangsindgreb, der fastslår rammerne for udlevering af teledata til politiet – både mht. teledata omfattet af logningsreglerne og mht. andre fortrolige teledata.

Veldefinerede begreber
I dette notat gennemgår TI de typer af teledata, som teleselskaberne registrerer og logger i dag – og TI vil fremkomme med forslag til præcise definitioner for hver enkelt type af data omfattet af logningsreglerne **(se pkt. 2 og bilag A)** samt forslag til formulering af ny hjemmelsbestemmelse i retsplejeloven om logning af teledata, herunder særligt teledata, som teleselskaberne ikke selv har brug for, eller som teleselskaberne selv kun har brug for at registrere i en ganske kort periode **(se pkt. 3)**. Desuden vil TI fremkomme med forslag til nye definitioner af tvangsindgreb for de typer af loggede teledata, hvortil der ikke i dag findes veldefinerede tvangsindgreb **(se pkt. 4)**. Endelig vil TI fremkomme med forslag til en mere hensigtsmæssig afgrænsning af 2 eksisterende tvangsindgreb: udvidet teleoplysning hhv. teleobservation **(se pkt. 5)**.

Overensstemmelse med EU-retten
TI forudsætter naturligvis, at danske regler om teleselskabernes pligt til at logge teledata samt reglerne om teleselskabernes udlevering af teledata til politiet tilpasses mhp. efterlevelse af EU-domstolens afgørelser i bl.a. EU-dom om logning fra 2016 (C-203-15, Tele2-Watson), herunder mht. proportionalitet og mht. fastsættelse af regler om (a) kriminalitetskrav for enhver indgrebsmulighed, (b) adgang til data om andre personer end den mistænkte, og (c) myndighedernes efterfølgende underretning af de berørte personer. Teleindustrien imødeser Justitsministeriets forslag til, hvordan de danske regler bør tilpasses mhp. efterlevelse af EU-domstolens afgørelser på de nævnte punkter.

TI forudsætter desuden, at danske regler om logning ikke går videre end kommende logningsregler fastsat i andre europæiske lande. Det er således efter TI's opfattelse vigtigt, at der vedtages logningsregler, som udspringer af en fælles EU-forståelse.

Med hensyn til nye regler om udlevering af teledata til politiet, jf. TI's forslag i pkt. 4 i dette notat, kan TI tilslutte sig, at nye regler om indgreb og rammer for udlevering at teledata fastsættes hurtigst muligt og gerne forud for ændring af reglerne om logning.

2. Definitioner af data-typer

De datatyper, som oplistes i den gældende logningsbekendtgørelse, henholdsvis de datatyper, som omtales i domspraksis, er i flere tilfælde anderledes end de sædvanlige teletekniske begreber, og dette kan give anledning til begrebsforvirring.

TI anbefaler, at omtale af teledata i de kommende nye logningsregler ændres så begreberne for de enkelte typer af teledata svarer til de definitioner, som benyttes i telereguleringen eller som i øvrigt benyttes som normale teletekniske begreber.

I **Bilag A** gennemgår TI de typer af teledata, som teleselskaberne behandler og registrerer i dag. **Konkret anbefaler TI**, at omtale af teledata i de kommende nye logningsregler – herunder omtale af teledata i retsplejeloven og i lovforslagsbemærkninger til retsplejeloven ifm revisionen af logningsreglerne – sker ved brug af de betegnelser for hver datatype, som er oplistet i **Bilag A, 1. kolonne**. I de tilfælde, hvor betegnelsen for datatyper i Bilag A, 1. kolonne ikke er selvforklarende, er betegnelsen markeret med BLÅ i Bilag A, 1. kolonne, og TI's forslag til nærmere definition af datatypen er herefter angivet under oversigten i Bilag A. **TI anbefaler**, at de foreslåede nye betegnelser og definitioner af teledata benyttes ved den kommende revision af logningsreglerne.

Særligt for så vidt angår data, som angiver den geografiske placering af en slutbrugers mobilterminaludstyr – har det igennem tiderne været særlig meget begrebsforvirring. TI anbefaler, at sådanne data overordnet og samlet fremover kaldes "lokaliseringsdata", jf. definitionen heraf i telereguleringen. Se nærmere herom i pkt. 3.2 nedenfor.

Øvrige opmærksomhedspunkter ift. regler om logning og udlevering af data til politiet
Udover spørgsmålet om definition af begreber og datatyper i logningsreglerne ønsker Teleindustrien at pege på nogle opmærksomhedspunkter, som er markeret med RØD tekst i Bilag A:

For hver datatype angives det i **Bilag A, 2. kolonne**, om teleselskaberne selv har brug for at registrere den pågældende datatype samt hvor længe teleselskaberne i givet fald selv har brug for at registrere den pågældende datatype samt formålet hermed – fx til brug for debitering eller fejlretning. Desuden angives i **Bilag A, 3. kolonne**, hvor lang tid teleselskaberne aktuelt opbevarer den pågældende datatype. Endelig angives i Bilag A for hver datatype det gældende hjemmelsgrundlag for registrering/logning af den pågældende datatype (**Bilag A, 4. kolonne**) samt det gældende hjemmelsgrundlag for udlevering af den pågældende datatype til politiet (**Bilag A, 5. kolonne**).

Opmærksomhedspunkter ift. regler om logning og udlevering af data til politiet er markeret med RØD tekst i Bilag A. Opmærksomhedspunkter omfatter følgende situationer:

(1) Situationer, hvor teleselskaberne er pålagt at logge data, som teleselskaberne ikke selv har brug for, eller som teleselskaberne kun har brug for at registrere i en ganske kort periode. Dette gælder bl.a. for lokaliseringsdata og for mobile dynamiske IP-adresser. For disse situationer anbefaler TI, at reglerne om logning fastsættes med direkte lovhjemmel og ikke som hidtil kun på bekendtgørelsesniveau. Se nærmere under **pkt. 3.1** i dette notat.
(2) Situationer, hvor der mangler hjemmel til logning af bestemte datatyper (visse lokaliseringsdata) m.fl.), og hvor politiet erfaringsmæssigt har stort behov for indsigt i teledata. For denne datatype anbefaler TI, at eventuelle nye regler om logning fastsættes enkelt og teknologineutralt mhp. at sikre, at nye logningsregler tager højde for den teknologiske udvikling. Se nærmere under **pkt. 3.2** i dette notat.
(3) Situationer, hvor gældende hjemmel til logning er uklar (logning af brugeridentitet i form af IP-adresse). Se nærmere under **pkt. 3.3** i dette notat.
(4) Situationer, hvor der mangler veldefinerede tvangsindgreb, der fastslår rammerne for udlevering af registrerede data til politiet. Dette gælder bl.a. for lokaliseringsdata og for udlevering af data om ikke-mistænkte. For disse situationer anbefaler TI, at der skabes præcis og direkte lovhjemmel til veldefinerede tvangsindgreb i retsplejelovens kapitel 71, der fastslår rammerne for udlevering af registrerede data til politiet. Se nærmere under **pkt. 4 og 5** i dette notat.

2.1. Særligt om brug af begrebet "signaleringsdata"

TI finder det uhensigtsmæssigt at benytte begrebet "signaleringsdata" om lokaliseringsdata for mobilterminaler, idet al udveksling af data (bortset fra indholdsdata) i et telenet, teknisk set er signalering. Den almindelige tekniske forståelse af begrebet 'signaleringsdata' er således enhver form for data (trafikdata[2] og lokaliseringsdata[3]), der indgår i signaleringen i telenet, både når telefonen bruges aktivt til telefoni, sms, mms eller mobildata/internetadgang, og når telefonen ikke bruges aktivt.

Derfor har det heller ikke været retvisende, når begrebet "signaleringsdata" i visse tilfælde har været brugt som betegnelse for lokaliseringsdata i form af registrerede celle-ID for mobilterminaler uden aktivitet – det vil sige når telefonen er tændt, men ikke anvendes aktivt.

Fx fremgår følgende forståelse af begrebet "signaleringsdata" af U.2017.1934Ø. Beskrivelsen i Østre Landsrets kendelse er en gengivelse af anklagemyndighedens forståelse (se også TI's vurdering af rækkevidden af kendelsen i pkt. 4.2):

> "***Kendelse*** *[Retten i Glostrup]*
> *Retten har forstået, at en tændt mobiltelefon løbende har forbindelse med en eller flere af de master, som den passerer, selv om der ikke er en faktisk aktivitet på telefonen. Teleselskaberne kan således udlevere oplysning om, hvorvidt en mobiltelefon er registreret som have været i forbindelse med en mast på et nærmere angivet tidspunkt. Denne oplysning kaldes signaleringsdata eller lagrede location updates. …*
>
> ***Østre Landsrets kendelse …***
> *… signaleringsdata giver kun adgang til oplysninger om, hvorvidt telefonen har været tændt, og i givet fald om brugeren er tilknyttet et af de tre teleselskaber, der gemmer signaleringsdata. Der vil således ikke fremgå oplysninger om, hvorvidt telefonerne har været brugt og hvilke apparater de eventuelt har været i kontakt med …"*

En aktiv forbindelse vil altid medføre signalering både i mobiludbydernes radionet (masterne) og i kernenettet (centraler og trafiknoder mv.). Hvis en mobiltelefon derimod blot er tændt, men ikke bruges aktivt, herunder ikke har mobildata aktiveret, vil der som udgangspunkt kun ske signalering i radionettet, og i så fald kun i begrænset omfang fx når terminaludstyret bevæger sig ind i et nyt overordnet område i radionettet – eksempelvis ved 'location update' i 2G- og 3G-radionettet. Brug af begrebet "signaleringsdata" om kun sidstnævnte lille del af den samlede mængde signaleringsdata i en teleudbyders net – som anklagemyndigheden gør i ovennævnte Østre Landsrets kendelse – kan give anledning til begrebsforvirring, og bør derfor undgås.

TI anbefaler, at begrebet "signaleringsdata" fremover helt undgås i relation til registrering/logning og udlevering af data. TI anbefaler, at alle typer af lokaliseringsdata, som teleudbyderne er i besiddelse af, fremover samlet benævnes "lokaliseringsdata" (data om anvendte master), og at der ikke sondres mellem

---

[2] "Trafikdata" er defineret i § 2, nr. 2 i udbudsbekendtgørelsen: "Trafikdata: Data, som behandles med henblik på overførsel af kommunikation i et elektronisk kommunikationsnet eller debitering heraf". Trafikdata omfatter både forbrugsdata, lokaliseringsdata ifm. kommunikation samt mere tekniske data (fx data om protokol og format).

[3] "Lokaliseringsdata" (data om anvendte masteceller) er defineret i § 2, nr. 3 i udbudsbekendtgørelsen: "Lokaliseringsdata: Data, som behandles i et elektronisk kommunikationsnet, og som angiver den geografiske placering af det terminaludstyr, som brugeren af en offentlig elektronisk kommunikationstjeneste anvender". Lokaliseringsdata (celle-ID) kan både være trafikdata, der behandles med henblik på overførsel af kommunikation (telefoni, sms, mms, mobildata), og data, som ikke er trafikdata.

forskellige typer af lokaliseringsdata ved en eventuel kommende revision af regler om logning af lokaliseringsdata og ved fastsættelse af regler om udlevering af sådanne data. Se nærmere herom i pkt. 3.2 og pkt. 4.1 og 4.2 i dette notat.

3. Regler om logning af teledata

3.1. Forslag til ny formulering af hjemmel i retsplejeloven om logning af teledata

Indledningsvis, og som også anført i pkt. 1, ønsker TI at understrege, at Teleindustrien på ingen måde har interesse i, at der fastsættes regler om logning af teledata – og som udgangspunkt ønsker Teleindustrien, hverken at de gældende regler om logning af teledata opretholdes eller udvides. Hvis der imidlertid er politisk ønske og juridisk mulighed for at opretholde og eventuelt udvide krav om logning af teledata, anbefaler TI, at de kommende regler om logning og udlevering tager højde for TI's input som beskrevet nedenfor.

TI anbefaler, at der i hjemmelsbestemmelsen i retsplejeloven (RPL § 786, stk. 4) skabes direkte lovhjemmel til logning af teledata, som teleudbydere selv kun har brug for at registrere i en ganske kort periode, og at der samtidig skabes overblik i hjemmelsbestemmelsen over sammenhængen mellem retsplejelovens tvangsindgreb og de datatyper, der skal logges.

Baggrunden for anbefalingen er følgende:

Følgende fremgår af den gældende hjemmelsbestemmelse om logning i retsplejelovens § 786, stk. 4:

> *"§ 786. …*
> *Stk. 4. Det påhviler udbydere af telenet eller teletjenester at foretage registrering og opbevaring i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. Justitsministeren fastsætter efter forhandling med erhvervsministeren nærmere regler om denne registrering og opbevaring."*

TI foreslår følgende ændringer til reglen i retsplejelovens § 786, stk. 4:

a. DIREKTE LOVHJEMMEL til logning af data, som teleselskaberne ikke selv har brug for:
Som anført i pkt. 1 i dette notat indebærer logning af teledata, som teleselskaberne ikke selv har brug for, eller som teleselskaberne selv kun har brug for at registrere i en ganske kort periode, et element af overvågning. Med henblik på lovgivers direkte stillingtagen til spørgsmålet om sådan overvågning bør regler om sådan overvågning efter TI's opfattelse fastsættes med direkte lovhjemmel og ikke som hidtil kun på bekendtgørelsesniveau. **Konkret anbefaler TI**, at regler om logning af følgende typer af teledata – som teleselskaberne ikke selv har brug for, eller kun har brug for at registrere i en ganske kort periode – fastsættes med direkte lovhjemmel og ikke som hidtil kun på bekendtgørelsesniveau:
- Lokaliseringsdata (alle slags)
- IMEI-nummer
- Dynamiske IP-adresser (som bruges af flere).

b. SAMMENHÆNG mellem tvangsindgreb og datatyper, der skal logges:
Som det fremgår af pkt. 2 i dette notat samt oversigten i Bilag A eksisterer der i dag et virvar af begreber både i logningsreglerne og retsplejeloven. For at skabe klarhed og understøtte samarbejdet og dialogen

mellem teleudbyderne og politiet, anbefaler TI, at der via hjemmelsbestemmelsen om logning i retsplejeloven § 786, stk. 4 skabes sammenhæng mellem de datatyper, som er omfattet af logningsreglerne, og de tvangsindgreb i retsplejelovens kapitel 71, som knytter sig til teleområdet. I den forbindelse foreslår TI, at der defineres 3-4 nye tvangsindgreb, som matcher de typer af teledata, som teleselskaberne ikke selv har brug for at registrere, eller som teleselskaberne selv kun har brug for at registrere i en ganske kort periode, jf. ovenfor pkt. a. **Konkret foreslår TI**, at følgende nye tvangsindgreb defineres, jf. nærmere herom i pkt. 4 i dette notat:

- 'Masteoplysning', (oplysning om lokalisering af én bruger)
- 'Udvidet masteoplysning', (oplysning om alle de brugere, der har anvendt en mast)
- 'Udvidet IP-adresse oplysning' (oplysning om flere brugere bag en dynamisk IP-adresse).
- 'IMEI-søgning' (oplysning om hvilke terminaler der har været anvendt til fokus-abonnementet).

Derudover bør de eksisterende tvangsindgreb i retsplejelovens kapitel 71 ('Teleoplysning' m.fl.) også nævnes i § 786, stk. 4 i sammenhæng med de typer af data, der danner grundlag for tvangsindgrebene.

c. OPBEVARINGSPERIODE for loggede data – og hastesikring:

Generelt ønsker Teleindustrien, at opbevaringsperioden for loggede data nedsættes markant ift. den nuværende regel om logning i 1 år – særligt i forhold til registrering af lokaliseringsdata og data om IP-adresser (kilde). Hvis der ved den kommende revision af logningsreglerne fastsættes regler om logning af lokaliseringsdata ifm. mobildatatrafik, jf. pkt. 3.2 i dette notat, vil mængden af registrerede data blive mangedoblet sammenlignet med de gældende regler om logning af lokaliseringsdata, som kun omfatter telefoni og sms/mms, hvilket vil øge teleselskabernes omkostninger til opbevaring af data. Som det fremgår af oversigten i Bilag A har teleselskaberne selv kun brug for at registrere lokaliseringsdata i kort tid. Generelt ønsker TI derfor, at opbevaringsperioden i logningsreglerne nedsættes fra 1 år til så kort tid som overhovedet mulig. TI peger samtidig på muligheden for helt at undlade at fastsætte regler om opbevaringsperiode for loggede data, og i stedet fastsætte regler om hastesikring af allerede registrerede trafik- og lokaliseringsdata for mistænkte og for gerningssteder svarende til reglen om hastesikring i retsplejelovens § 786 a – for på den måde at imødekomme EU-domstolens afgørelse i EU-dom om logning fra 2016 (C-203-15, Tele2-Watson) om, at der ikke kan fastsættes nationale regler om udifferentieret logning af samtlige trafikdata og lokaliseringsdata.

d. DATA RETENTION – og best effort:

Det engelske begreb "Data retention" (tilbageholdelse og opbevaring af data) er mere præcist end den lidt misvisende danske oversættelse "logning". Begrebet logning anvendes i øvrigt i de gældende regler kun i en parentes i overskriften til logningsbekendtgørelsen. Reglerne om Data retention er oprindeligt et krav om at gemme data, som teleudbyderen i forvejen besidder til brug for leveringen af teletjenester (og ikke et krav om at skaffe data på anden vis). Dvs data skal gemmes og opbevares af teleudbyderen, i stedet for at teleudbyderen sletter data, når teleudbyderen ikke længere selv har brug for disse data. Dertil kommer, at ordlyden i § 1 i den gældende logningsbekendtgørelse om, at teleudbydere skal "registrere og opbevare [data], der genereres eller behandles i udbyderens net" fra tid til anden har givet anledning til misforståelser om rækkevidden af logningsreglerne mht. skabelse af data. For at undgå, at de kommende nye logningsregler kan give anledning til nye misforståelser, **anbefaler TI**, at de nye regler blot fastslår, at teledata, som teleudbydere opsamler og registrerer til egne formål, skal gemmes og opbevares i en periode – i stedet for at blive slettet (Data retention). Det bemærkes særligt, at lokaliseringsdata, som teleudbyderne opsamler og registrerer i kort tid til brug for fejlretning, kun kan ske efter "best effort, jf. pkt. 3.2 nedenfor.

e. 'TELEDATA' i stedet for 'data om TELETRAFIK:
Derudover foreslår TI overordnet, at hjemmelsbestemmelsen om logning i retsplejeloven § 786, stk. 4 ændrer ordlyd fra det snævre begreb "oplysninger om teletrafik" til det bredere begreb "teledata". Betegnelsen "oplysninger om teletrafik" må forstås som "trafikdata", jf. definitionen heraf i eData-reglerne (se bilag A), og sådanne "trafikdata" omfatter bl.a. *ikke* lokaliseringsdata om en mobiltelefon, som er tændt, men som ikke anvendes aktivt (lokaliseringsdata, som ikke er trafikdata ("signaleringsdata"[4])), jf. nærmere herom nedenfor i pkt. 3.2 om lokaliseringsdata. I modsætning til betegnelsen "oplysninger om teletrafik" (trafikdata), kan betegnelsen "teledata" rumme alle former for data, som en teleudbyder opsamler og registrerer, og begrebet "teledata" vil derfor med fordel kunne anvendes som nyt overordnede begreb i logningsreglerne. Se også bilag A om nærmere definitioner af alle de nævnte begreber.

<u>På denne baggrund foreslår TI konkret</u>, at retsplejelovens § 786, stk. 4 ændres på følgende måde (TI's nærmere begrundelser for forslag og definition af nye tvangsindgreb findes i pkt. 4 og 5 i dette notat):

Gældende regel:

> *"§ 786. …*
> *Stk. 4. Det påhviler udbydere af telenet eller teletjenester at foretage registrering og opbevaring i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. Justitsministeren fastsætter efter forhandling med erhvervsministeren nærmere regler om denne registrering og opbevaring."*
>
> Forslag til ny regel (ændringer ift. gældende tekst er markeret):
>
> *Stk. 4. ~~Det påhviler udbydere af telenet eller teletjenester at foretage registrering og opbevaring i 1 år af oplysninger om teletrafik til brug for~~ <u>Udbydere af elektroniske kommunikationsnet eller -tjenester, som opsamler og registrerer teledata med henblik på levering af teletjenester, skal gemme og opbevare sådanne teledata i [x] måneder, således at disse teledata vil kunne anvendes som led i</u> efterforskning og retsforfølgning af strafbare forhold. <u>Opbevaringspligten omfatter følgende typer af teledata:</u>*
> *1) <u>Trafikdata, som muliggør indgreb i form af teleoplysning, som nævnt i § 780, stk. 1, nr. 3.</u>*
> *2) <u>Lokaliseringsdata (data om anvendte master), som muliggør indgreb i form af masteoplysning som nævnt i § [NY], udvidet masteoplysning, som nævnt i § [NY], samt udvidet teleoplysning, som nævnt i § 780, stk. 1, nr. 4.</u>*
> *3) <u>Trafikdata, som muliggør indgreb i form af IMEI-oplysning, som nævnt i § [NY].</u>*
> *4) <u>Trafikdata, som muliggør indgreb i form af IP-adresse-oplysning og udvidet IP-adresse-oplysning, som nævnt i § [NY].</u>*
> *Justitsministeren fastsætter efter forhandling med erhvervsministeren nærmere regler om denne registrering og opbevaring.*

TI foreslår desuden, at det herefter i bemærkningerne til lovforslag om ændring retsplejelovens § 786, stk. 4 samt i en kommende ny logningsbekendtgørelse uddybes, hvilke konkrete typer af allerede registrerede teledata, der skal gemmes og opbevares, og at TI's forslag til begreber og definitioner, som er oplistet i Bilag A, benyttes i den forbindelse – jf. nærmere herom i pkt. 2 i dette notat.

[4] Som beskrevet i pkt. 2.1 anbefaler TI, at begrebet "signaleringsdata" fremover helt undgås.

3.2. Regler om logning af lokaliseringsdata (data om anvendte master)

Indledningsvis, og som også anført i pkt. 1, ønsker TI at understrege, at Teleindustrien på ingen måde har interesse i, at der fastsættes regler om logning af lokaliseringsdata – og som udgangspunkt ønsker Teleindustrien, hverken at de gældende regler om logning af teledata opretholdes eller udvides. Hvis der imidlertid er politisk ønske og juridisk mulighed for at opretholde og eventuelt udvide krav om logning af teledata, anbefaler TI, at de kommende regler om logning og udlevering tager højde for TI's input som beskrevet nedenfor.

TI anbefaler, at eventuelle nye regler om logning af lokaliseringsdata udformes og formuleres teknologineutralt – både i hjemmelsbestemmelsen i retsplejeloven (RPL § 786, stk. 4), i bemærkningerne i lovforslaget om revision af hjemmelsbestemmelsen i retsplejeloven, samt i reglerne i den kommende nye logningsbekendtgørelse.

Baggrunden for anbefalingen er følgende:

Som det fremgår af Bilag A, findes der overordnet flere typer af lokaliseringsdata (data om anvendte master (celle-ID)):

- lokaliseringsdata, som er trafikdata ifm. telefoni- og sms/mms-kommunikation
- lokaliseringsdata, som er trafikdata ifm. mobildata-kommunikation (4G)
- lokaliseringsdata, som ikke er trafikdata (tændte telefoner, der ikke anvendes aktivt)

Den gældende regel om logning af lokaliseringsdata i logningsbekendtgørelsens § 4, nr. 6 har følgende ordlyd:

> *§ 4. En udbyder af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal registrere følgende oplysninger om fastnet- og mobiltelefoni samt SMS-, EMS- og MMS-kommunikation:*
> *…*
> *6) den eller de celler en mobiltelefon er forbundet til ved kommunikationens start og afslutning, samt de tilhørende masters præcise geografiske eller fysiske placering på tidspunktet for kommunikationen,*

De gældende logningsregler omfatter således ikke logning af lokaliseringsdata ved brug af mobildatatjenester, og heller ikke logning af lokaliseringsdata for mobilterminaler, der ikke anvendes aktivt.

Baggrunden for, at ikke alle typer af lokaliseringsdata er omfattet af de gældende logningsregler, er bl.a. detaljeringsgraden i udformningen af den gældende regel om logning af lokaliseringsdata, dels fordi bestemmelsen forholder sig til de begrænsninger i mulighederne for logning af lokaliseringsdata, som gjorde sig gældende i 2006 (første og sidste mast i en kommunikation), dels fordi den gældende regel positivt nævner telefoni, sms og mms, som var det mest udbredte teletjenester i 2006, da logningsbekendtgørelsen blev udstedt. Mobildatatjenester blev derimod ikke anvendt i stort omfang i 2006. I 2020 er kundernes forbrugsmønster imidlertid anderledes, og mobildatatjenester anvendes i betydeligt omfang.

Som det fremgår af "TI's tekniske løsningsbeskrivelser", som er sendt til Justitsministeriet og Rigspolitiet den 19. december 2018, registrerer mobiludbyderne lokaliseringsdata i form af celle-ID til brug for fejlretning og drift. Opsamlingen af lokaliseringsdata kan ske på flere forskellige måder:

a. Opsamling af lokaliseringsdata sker i form af CDR-data (xDR/CDR – call detail record), dvs opsamling via centraler og switche i mobilnettet i form af "taksttelegrammer", der registrerer kundens forbrug – primært til brug for debitering. CDR-data omfatter forbrugsdata om hver enkel telefoni-, sms-, mms- eller mobildata-kommunikation, herunder aggregerede lokaliseringsdata (data om de anvendte celler):

   Ved telefoni- og sms-kommunikation er der 100 % overensstemmelse mellem tidspunkt og Celle-ID, som registreres i CDR, og CDR giver mulighed for at opsamle start-Celle-ID og i nogle tilfælde også slut-Celle-ID i en kommunikation.

   Ved mobildata-kommunikation forholder det sig imidlertid anderledes, hvilket bl.a. skyldes, at mobildata-trafik ikke afregnes pr. tid, men pr. volumen – og desuden indgår der i en mobildata-CDR kun oplysning om den sidst rapporterede celle: Når en kunde har mobildata aktiveret (dvs dataforbindelsen står åben), vil der løbende for mobildata-forbindelsen blive dannet nye CDR'er, herunder (1) ved skift af radioteknologi (2G/3G/4G), (2) hvis dataforbruget i CDR'ens levetid når en specifik volumengrænse, fx 50 Mbyte, eller (3) hvis CDR'ens levetid når en specifik tidsgrænse, fx 1 time, uden at nå volumengrænsen. Længden på en CDR kan derfor variere fra få sekunder og indtil tidsgrænsen er nået. Hver mobildata-CDR indeholder CDR'ens starttidspunktet, volumenforbrug i CDR'ens levetid samt den sidste celle, som systemet rapporterer til CDR'en. I situation (1) og (2) rapporteres derfor celle ved CDR'ens udløb, men i situation (3) rapporteres den sidste celle, der har været ført trafik på i CDR'ens levetid (fx hvis en CDR står åben fra 12:00 til 13:00 og der alene føres trafik fra **12:03 til 12:04 under celle x** og fra **12:30 til 12:31 under celle y**, vil tidsstemplingen være kl. 12:00, men den registrerede celle vil være den celle, der blev trafikeret på kl. 12:31, dvs celle y). Registrerede Celle-ID fra mobildata-CDR'er kan derfor i situation (3) kun fortælle, at den pågældende celle har været benyttet indenfor det tidsinterval, hvor det pågældende mobildata-CDR har været aktivt. Registrerede Celle-ID fra CDR'er om mobildata-kommunikation kan derfor give anledning til fortolkningsfejl, hvis læseren ikke er opmærksom på de nævnte forhold.

b. Opsamling af lokaliseringsdata sker desuden via måleudstyr (ofte benævnt prober), som opsamler data til brug for fejlretning og drift af mobilnettet, og som ud over den kommunikationsrelaterede signalering, som opsamles parallelt i CDR i aggregeret form, også opsamler yderligere mobilitetsrelateret signalering. Generelt sker der mange flere registreringer af celle-ID i probe-systemerne end i CDR-data, og i probe-systemerne er der altid overensstemmelse mellem tidspunkt og Celle-ID, uanset hvilken type trafik, der er tale om (telefoni, sms, mms eller mobildata).

   Særligt i forhold til registrering af lokaliseringsdata i probe-systemerne skal det bemærkes, at registrering kun kan ske efter "best effort", idet alle data kun opsamles, hvis kapaciteten i teleudbydernes opsamlingssystemer er tilstrækkelig. Teleudbyderne har selv interesse i at opsamle flest mulige trafikdata og lokaliseringsdata i probe-systemerne til brug for fejlretning, og teleudbyderne tilpasser derfor løbende kapaciteten i probe-systemerne. I sjældne tilfælde – fx ifm uforudset øget trafik i mobilnettene – kan der dog forekomme mangel på kapacitet i probe-systemerne, og i så fald vil den opsamlede mængde af lokaliseringsdata blive reduceret. Selv i disse sjældne situationer, opsamles der dog typisk stadig langt flere registreringer af lokaliseringsdata pr. mobilterminal i probe-data end i

CDR-data. Dertil kommer, at probe-systemet primært er beregnet til støtte for driften af mobilnettet, og probe-systemerne understøttes derfor ikke med back-up og fuldt service-level 24/7, og det kan derfor også – i yderst sjældne tilfælde – forekommer, at midlertidige brugeridentiteter (temporær IMSI (TMSI)) sporadisk kan blive forvekslet med utilsigtede registreringer af mastespring til følge[5].

Som det fremgår af oversigten i Bilag A, registreres lokaliseringsdata, som ikke er omfattet af logningsreglerne, normalt kun i kort tid – til brug for drift/fejlretning. Imidlertid efterspørger Politiet erfaringsmæssigt indsigt i alle former for registrerede lokaliseringsdata – uanset om der er tale om lokaliseringsdata, der ikke er omfattet af de gældende logningsregler. Politiet benytter derfor i stort omfang muligheden for hastesikring af data, jf. retsplejelovens § 786a, for de datatyper, som udbyderne registrerer til egne formål i en kort periode (bl.a. hastesikring af lokaliseringsdata i form af "signaleringsdata"[6]). Hastesikring af data er ressourcekrævende for teleudbyderene, idet data, som ikke er omfattet af logningsreglerne, ikke overføres til teleselskabernes it-systemer til lagring af loggede data. Data, som ikke er omfattet af logningsreglerne, skal derfor hentes direkte i mobiludbydernes probe-systemer.

Som det fremgår, er de tekniske forhold omkring opsamlingen af lokaliseringsdata i mobiludbydernes net ganske komplicerede. Dertil kommer, at ovenstående beskrivelse er et øjebliksbillede af, hvordan registrering og opsamling af lokaliseringsdata sker i dag. Med kommende generationer af mobilnet (5G m.fl.) vil de tekniske forhold igen kunne ændre sig.

For at undgå, at eventuelle kommende nye logningsregler bliver afgrænset utilsigtet – lige som de gældende – **anbefaler TI**, at eventuelle nye regler om logning af lokaliseringsdata udformes fuldstændig teknologineutralt og blot fastslår, at lokaliseringsdata, som teleudbydere opsamler og registrerer til egne formål, skal hastesikres eller gemmes og således opbevares i en længere periode end teleudbyderen selv har brug for (data retention, pkt. 3.1 i dette notat). For at sikre teknologineutrale regler, bør eventuelle nye regler derimod hverken forholde sig til opsamlingsmetoder (probe-systemer, CDR-systemer osv.) eller nævne specifikke tjenestetyper (telefoni, sms, mms, data), ligesom bestemmelsen ikke bør forholde sig til, om lokaliseringsdata opsamles ifm aktiv kommunikation eller ej. Pga. den omfattende mængde af data i probe-systemerne, samt teleselskabernes omkostninger til opbevaring af data, ønsker TI som nævnt i pkt. 3 en opbevaringsperiode så kort som overhovedet mulig.

Som nævnt ønsker Teleindustrien, hverken at de gældende regler om logning af teledata opretholdes eller udvides. Hvis der imidlertid opstår politisk flertal for en ændring af reglerne om logning af lokaliseringsdata, skal **TI foreslå**, at der samarbejdes direkte med TI om et konkret forslag til formulering af ny teknologineutral regel om logning af lokaliseringsdata.

For god ordens skyld bemærkes, at hvis der indføres logningspligt for alle typer af lokaliseringsdata, der behandles i mobiludbydernes net, herunder "lokaliseringsdata, der ikke er trafikdata" – dvs lokaliseringsdata om en mobiltelefon, som er tændt, men som ikke kommunikerer aktivt – er der behov for, at § 24, stk. 1 i udbudsbekendtgørelsen om lokaliseringsdata, der ikke er trafikdata – opdateres med en

[5] Sådanne registrerede mastespring vil som altovervejende hovedregel fremstå som usandsynlige, jf. nærmere herom i beskrivelse af fejlkilder i Rigspolitiets notat vedrørende anvendelse af historiske teledata i straffesager ("Varedeklarationen").

[6] Som beskrevet i pkt. 2.1 anbefaler TI, at begrebet "signaleringsdata" fremover helt undgås.

undtagelse/henvisning til retsplejelovens § 786, stk. 4 – svarende til den henvisning til retsplejeloven, som findes i udbudsbekendtgørelsens § 23, stk. 1 om trafikdata, herunder lokaliseringsdata som er trafikdata.

3.3. Forslag til præcisering af logningsbekendtgørelsens regel om logning af brugeridentitet (IP)

TI anbefaler en præcisering af § 5 i logningsbekendtgørelsen om logning af brugeridentitet for internetbrugere. Baggrunden for forslaget er følgende:

§ 5 i den gældende logningsbekendtgørelse om, hvilke trafikdata og identifikationsdata, der skal logges, for så vidt angår internetadgangstjenester, er noget uklar.

Både § 5, stk. 1, nr. 1 og nr. 2 i logningsbekendtgørelsen omtaler således "brugeridentiteten" for en brugers adgang til internettet. I § 5, stk. 1, nr. 2 omtales desuden "telefonnummer". I Justitsministeriets oprindelige vejledning til logningsbekendtgørelsens § 5, stk. 1 er det forklaret, at kravene i § 5, stk. 1 omfatter både den tildelte IP-adresse (kilde) samt telefonnummer eller "kundenummer", som identificerer kunden overfor udbyderen.

Det må lægges til grund, at § 5, stk. 1, nr. 1 vedrører krav om logning af IP-adresse inkl. eventuelt portnummer (kilde), som identificerer en slutbrugers adgang til en internettjeneste; og at § 5, stk. 1, nr. 2 vedrører krav om logning af mobiltelefonnummer eller tilsvarende identifikationsnummer for den anvendte bredbåndsforbindelse (fx kredsløbsnummer), som har været benyttet til internetadgang. Kundenummer – som nævnt i den gamle vejledning – ses derimod ikke at være relevant.

Desuden omtaler § 5, stk. 1, nr. 4 i logningsbekendtgørelsen "tidspunktet for kommunikationens start og afslutning". Det må lægges til grund, at § 5, stk. 1, nr. 4 vedrører krav om tidsstempling af tildelingen af brugeridentiteten, som ellers mangler i § 5. Det kan i øvrigt oplyses, at der hverken i fastnet eller mobilnet sker en retvisende tidsstempling af internet-forbrug. Dette skyldes bl.a., at forbrug af data/internet-forbrug ikke registreres pr. tid, men pr. volumen målt i Mbyte.

På den baggrund, foreslår TI konkret, at reglen i logningsbekendtgørelsen om logning af IP-adresser (kilde) præciseres på følgende måde i den kommende nye logningsbekendtgørelse (ændringsforslag er markeret):

> *§ 5. En udbyder af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal registrere følgende oplysninger om en abonnents adgang til internettet:*
> *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) ~~den brugeridentitet og det telefonnummer, som er tildelt kommunikationer, der indgår i et offentligt elektronisk kommunikationsnet,~~ identifikation af det benyttede abonnement, fx telefonnummer, som identificerer det benyttede mobilabonnement ved internetadgang via mobildatatjenester, eller ID-nummer (fx kredsløbs-nummer), som identificerer det benyttede bredbåndsabonnement ved internetadgang via faste net,*
> *3) tidspunktet for tildelingen af brugeridentitet,*
> *4) navn og adresse på abonnenten samt den eventuelle registrerede bruger. ~~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.~~*

4. Regler om udlevering af teledata – Definition af nye tvangsindgreb

Teleindustrien finder det uhensigtsmæssigt – og besynderligt – at der findes regler i dansk ret, der pålægger teleudbyderne at logge visse typer af data, som teleselskaberne ikke selv har brug for, eller som teleselskaberne kun har brug for at registrere i en ganske kort periode, hvorefter disse data kan udleveres til politiet alene efter reglerne om edition – dvs også ifm. mindre lovovertrædelser.

Som anført i pkt. 1 i dette notat, ønsker Teleindustrien, at der for hver type af data, som teleudbyderne pålægges at logge, skal fastsættes klare og præcise regler om de nærmere betingelser for politiets adgang til den pågældende datatype, herunder tages stilling til (a) graden af kriminalitet, der kan udløse politiets indgreb (svarende til fx reglen i RPL § 781, stk. 1, nr. 3), og (b) spørgsmålet om byrettens efterfølgende orientering af personen om, at indgrebet har fundet sted (svarende til fx reglen i RPL § 788). Sådanne regler om betingelserne for udlevering af loggede data til politiet bør fastsættes ved lov i form af regler om præcist definerede tvangsindgreb – svarende til reglerne i retsplejelovens kapitel 71 om indgreb i meddelelseshemmeligheden og om teleobservation.

For god ordens skyld skal det tilføjes, at det desuden er Teleindustrien opfattelse, at der bør defineres tvangsindgreb for enhver form for udlevering af trafik- og lokaliseringsdata til politiet – uanset om de pågældende typer at 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 reglerne om edition. 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. Dertil kommer, at det muligvis er utilsigtet, at logningsreglerne ikke omfatter samtlige typer af lokaliseringsdata – idet sådanne data muligvis kan have efterforskningsmæssig interesse (se bl.a. pkt. 2.1 og 3.2 i dette notat om politiets behov for indsigt i lokaliseringsdata, som ikke er omfattet af de gældende logningsregler). Samlet set bør der derfor fastsættes præcist definerede tvangsindgreb i RPL kapitel 71, som angiver betingelserne for enhver form for udlevering af trafik- og lokaliseringsdata, uanset om der er tale om data omfattet af logningsreglerne.

Særligt for så vidt angår lokaliseringsdata bemærkes, at TI er opmærksom på, at lokaliseringsdata ikke på samme måde som trafikdata om kundens opkald og øvrige kommunikation er omfattet af meddelelseshemmeligheden og telelovens § 7. Lokaliseringsdata kan imidlertid belyse en persons geografiske færden, og er derfor 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, jf. nærmere herom i pkt. 3.2. 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.

Konkret opfordrer TI til, at der i retsplejelovens kapitel 71 fastsættes regler, der definerer følgende nye tvangsindgreb samt fastsætter de nærmere betingelser for politiets adgang til at benytte indgrebet:

- Masteoplysning (vedr. udlevering af lokaliseringsdata om en bestemt mobiltelefon)
- Udvidet masteoplysning (vedr. hvilke telefoner, der har været registreret på en mast)
- Udvidet IP-adresse-oplysning (vedr. brugerne bag en dynamisk IP-adresse, der bruges af flere)
- IMEI-oplysning (hvilke mobilterminaler har været anvendt til et abonnement – og omvendt)

4.1. Forslag til definition af nyt tvangsindgreb: Masteoplysning

TI anbefaler, at der fastsættes regler i RPL kap 71 om et nyt tvangsindgreb, 'masteoplysning', som giver politiet adgang til oplysninger om lokaliseringsdata (Celle-ID), som viser, hvilke master en bestemt mobilterminal har anvendt.

Baggrunden for forslaget er følgende:

Teleudbyderne registrerer lokaliseringsdata i form af celle-ID, jf. nærmere beskrivelse heraf i pkt. 3.2 og Bilag A, herunder både lokaliseringsdata, som er omfattet af de gældende logningsregler (opbevares i 1 år), og lokaliseringsdata, der ikke er omfattet af de gældende logningsregler (opbevares i kort tid). Lokaliseringsdata identificerer, hvilke celler (master) en slutbrugers mobilterminaludstyr har været i signaleringsmæssig kontakt med, og lokaliseringsdata kan således belyse en mobilterminals overordnede geografiske placering og bevægelsesmønster (dvs hvilke master en mobilterminal har anvendt).

Teleselskaberne har selv kun brug for at registrere lokaliseringsdata i kort tid til brug for fejlretning, og registreringen af lokaliseringsdata ifm. telefoni- og sms/mms-kommunikation i 1 år sker derfor udelukkende for at opfylde kravet i logningsbekendtgørelsen.

Teleudbyderne har hidtil udleveret lokaliseringsdata i form af celle-ID for én bestemt mobiltelefon til politiet efter editionskendelse alene, jf. bl.a. U.2009.2610H. Der er således ikke fastsat regler i retsplejelovens kapitel 71, der definerer et tvangsindgreb ift. udlevering af lokaliseringsdata til politiet – på trods af, at der i retsplejelovens kapitel 71 (§ 786, stk. 4) er fastsat regler om logning af visse lokaliseringsdata.

Set i lyset af EU-domstolens afgørelse i EU-dom om logning fra 2016 (C-203-15, Tele2-Watson) finder TI det uafklaret, om udlevering af historiske lokaliseringsdata fortsat kan ske efter reglerne om edition uden samtidig stillingtagen til graden af den kriminalitet, der efterforskes. Det fremgår således af EU-dommen fra 2016, at artikel 15, stk. 1 i e-datadirektivet (2002/58/EF) er til hinder for national lovgivning, der giver politiet adgang til lagrede data "uden i forbindelse med bekæmpelse af kriminalitet at begrænse denne adgang til målet om bekæmpelse af grov kriminalitet …".

Der henvises endvidere til begrundelserne anført indledningsvis i pkt. 4, hvorefter det er TI's opfattelse, at lokaliseringsdata generelt ikke bør kunne udleveres til politiet alene efter reglerne om edition – uanset om de pågældende typer af lokaliseringsdata er omfattet af logningsreglerne eller ej.

På den baggrund, foreslår TI konkret, at nyt tvangsindgreb i form af masteoplysning defineres på følgende måde med direkte lovhjemmel i RPL kapitel 71 – fx i tilknytning til reglerne i § 791a, stk. 5 om fremadrettet teleobservation:

> [NY § 791a, stk. X]:
> Politiet kan fra udbydere af elektroniske kommunikationsnet og -tjenester indhente historiske oplysninger om anvendte mobilmaster for en bestemt mobiltelefon eller andet tilsvarende mobilt kommunikationsapparat, der antages at have været benyttet af en mistænkt (masteoplysning), hvis indgrebet må antages at være af væsentlig betydning for efterforskningen, og efterforskningen vedrører en lovovertrædelse, der kan medføre fængsel i [x år] eller derover.

4.2. Forslag til definition af nyt tvangsindgreb: Udvidet masteoplysning

TI anbefaler, at der fastsættes regler i RPL kap 71 om et nyt tvangsindgreb, 'udvidet masteoplysning', som giver politiet adgang til oplysninger om, hvilke mobilterminaler, der har været anvendt på bestemte master, i et præcist afgrænset område og på et præcist angivet tidspunkt – uden samtidig udlevering af oplysninger om, hvem de registrerede mobilterminaler har kommunikeret med.

Baggrunden for forslaget er følgende:

Teleudbyderne registrerer lokaliseringsdata i form af celle-ID, jf. nærmere beskrivelse heraf i pkt. 3.2 og Bilag A, herunder både lokaliseringsdata, som er omfattet af de gældende logningsregler (opbevares i 1 år), og lokaliseringsdata, der ikke er omfattet af de gældende logningsregler (opbevares i kort tid). Lokaliseringsdata identificerer, hvilke celler i mobilnettet (master) en slutbrugers mobilterminaludstyr har været i signaleringsmæssig kontakt med, og lokaliseringsdata kan således belyse, hvilke mobilterminaler der har været anvendt via master i et nærmere afgrænset geografisk område (dvs hvilke mobilterminaler har været anvendt på bestemte master).

Teleselskaberne har selv kun brug for at registrere lokaliseringsdata i kort tid til brug for fejlretning, og registreringen af lokaliseringsdata ifm. telefoni- og sms/mms-kommunikation i 1 år sker derfor udelukkende for at opfylde kravet i logningsbekendtgørelsen.

Teleudbyderne har hidtil – baseret på registrerede lokaliseringsdata – udleveret oplysninger til politiet, om hvilke mobilterminaler, der har været anvendt på bestemte master, efter kendelse om 'udvidet teleoplysning', jf. RPL § 780, stk. 1, nr. 4, hvis der er tale om både trafikdata og lokaliseringsdata, og efter editionskendelse, hvis der er tale om lokaliseringsdata i form af "signaleringsdata[7]", jf. U.2017.1934Ø.

Følgende fremgår af U.2017.1934Ø for så vidt angår spørgsmålet om forholdet til retsplejelovens regler om indgreb i meddelelseshemmeligheden:

> "*Det må på baggrund af det oplyste om signaleringsdata lægges til grund, at anmodningen [fra anklagemyndigheden] alene vedrører udlevering af allerede registrerede lokaliseringsoplysninger.*
>
> *Da anmodningen således ikke angår oplysninger om, hvilke telefoner eller andre tilsvarende kommunikationsapparater der sættes i forbindelse med en bestemt telefon eller andet kommunikationsapparat, er der ikke tale om [udvidet] teleoplysninger, jf. retsplejelovens § 780, stk. 1, nr. 4.*".

Selvom kendelsen vedrører lokaliseringsdata i form af "signaleringsdata"[8] (i kendelsen forstået som lokaliseringsdata om mobilterminaler, der er tændt, men som ikke anvendes aktivt), vurderer TI, at betragtningerne i kendelsen kan gøres tilsvarende gældende ved udlevering af lokaliseringsdata ifm kommunikation, herunder lokaliseringsdata omfattet af de gældende logningsregler – så længe politiets

[7] Som beskrevet i pkt. 2.1 anbefaler TI, at begrebet "signaleringsdata" fremover helt undgås.

[8] Se forrige note.

anmodning om udlevering af data kun omfatter lokaliseringsdata, men ikke også omfatter oplysninger om, hvem mobilterminalerne har kommunikeret med (trafikdata om opkald mv.). I det daglige samarbejde mellem teleudbyderne og politiet udleveres alle registrerede lokaliseringsdata, om hvilke mobilnumre, der har været anvendt på master, der dækker et gerningssted, således alene efter kendelse om edition.

TI bemærker dog, at der en stor lighed mellem indgreb i form Udvidet Teleoplysning efter RPL § 780, stk. 1, nr. 4 og politiets indhentelse af registrerede lokaliseringsdata om, hvilke mobiltelefoner der er registreret anvendt på mobilmaster, der dækker et gerningssted. TI vurderer desuden, at det ikke kan udelukkes, at hensigten med fastsættelsen af reglen om udvidet teleoplysninger, jf. retsplejelovens § 780, stk. 1, nr. 4, primært har været, at fastsætte rammerne for politiets indhentelse af oplysninger om, hvilke mobiltelefoner, der har været registreret anvendt på mobilmaster, der dækker et gerningssted – og således ikke i lige så høj grad politiets behov for at vide, hvem disse telefoner har kommunikeret med. Fx fremgår følgende af lovforslagsbemærkningerne til lov nr. 465 fra 2001 (lovforslag L 194 fra 2001) (vores fremhævelse):

> *"4.4. Teleoplysninger om brug af mobiltelefoner mv. (udvidet teleoplysning/masteoplysninger)*
> *4.4.1. Baggrund*
> *En særlig variant af teleoplysninger er de såkaldte »masteoplysninger«. Hvor den typiske situation ved teleoplysning er, at der ønskes oplysninger om bestemte telefonnumre, er situationen ved masteoplysninger den, at der ønskes oplysninger om alle telefoner, der i et givent område og inden for et bestemt tidsrum har benyttet en bestemt sendemast."*

TI vurderer derfor, at der bør tages udgangspunkt lovforarbejderne til reglen om i retsplejelovens § 780, stk. 1, nr. 4 ved overvejelsen af hvilke rammer, der fremover bør gælde for politiets indhentelse af registrerede lokaliseringsdata der viser, hvilke mobiltelefoner, der har været registreret anvendt på mobilmaster.

Dertil kommer, at politiets indhentelse af registrerede lokaliseringsdata om, hvilke mobiltelefoner der er registreret anvendt på mobilmaster, der dækker et gerningssted, giver politiet viden om mange flere mobilkunder, end tilfældet er ved indgreb i form Udvidet Teleoplysning efter RPL § 780, stk. 1, nr. 4. Dette skyldes, at Udvidet Teleoplysning kun giver adgang til viden om mobilkunder, der har anvendt telefoni-, sms- og mms-kommunikation via masterne, mens teleudbydernes systemer til brug for fejlretning (prober) opsamler og registrerer lokaliseringsdata både ved telefoni-, sms-, mms og 4G-data-kommunikation og ved mobilitet, herunder også hvis telefonen er 'tændt men ikke aktiv', jf. nærmere beskrivelse heraf i pkt. 3.2 og Bilag A. Tendensen forstærkes af, at mobilkunderne i stigende omfang benytter mobildata, men ikke telefoni og sms. Der er således tale om udlevering af oplysninger til politiet om et stort antal ikke-mistænkte.

Det bemærkes desuden, at mobiludbyderne oplever, at politiet i stigende omfang anmoder retten om efter reglerne om edition at udlevere oplysninger til politiet om hvilke mobiltelefoner, der har været registreret anvendt på mobilmaster, der dækker et gerningssted. Blandt disse sager er der også tale om sager der *ikke* vedrører efterforskning af grov kriminalitet. Eksempelvis er mobiludbyderne i februar 2020 i en sag om indbrud i biler i Ringkøbing blevet pålagt at udlevere tusindvis af lokaliseringsoplysninger om de mange mobilabonnenter, der havde anvendt de mange mobilmaster, der dækkede gerningsstedet.

TI finder det generelt uafklaret, om udlevering af tusindvis af lokaliseringsoplysninger om ikke-kriminelle og helt tilfældige kunder er proportionalt, jf. proportionalitetsbetragtningen i RPL § 805, stk. 1, hvis der ikke er tale om efterforskning af grov kriminalitet.

Set i lyset af EU-domstolens afgørelse i EU-dom om logning fra 2016 (C-203-15, Tele2-Watson) finder TI det desuden uafklaret, om udlevering af historiske lokaliseringsdata om, hvilke mobilterminaler, der har været anvendt på bestemte master, fortsat kan ske efter reglerne om edition uden samtidig stillingtagen til graden af den kriminalitet, der efterforskes. Det fremgår således af EU-dommen fra 2016, at artikel 15, stk. 1 i e-datadirektivet (2002/58/EF) er til hinder for national lovgivning, der giver politiet adgang til lagrede data "uden i forbindelse med bekæmpelse af kriminalitet at begrænse denne adgang til målet om bekæmpelse af grov kriminalitet …".

Der henvises endvidere til begrundelserne anført indledningsvis i pkt. 4, hvorefter det er TI's opfattelse, at lokaliseringsdata generelt ikke bør kunne udleveres til politiet alene efter reglerne om edition – uanset om de pågældende typer af lokaliseringsdata er omfattet af logningsreglerne eller ej.

TI foreslår på denne baggrund, at der fastsættes regler i RPL kap 71 om et nyt tvangsindgreb, 'udvidet masteoplysning', som fastslår de nærmere betingelser for politiets adgang til oplysninger om, hvilke mobilterminaler, der har været anvendt på bestemte master, og herunder tager stilling til graden af kriminalitet, der kan udløse dette indgreb.

Det bemærkes, at udlevering af historiske lokaliseringsdata om, hvilke mobilterminaler, der har været anvendt på bestemte master, kan omfatte tusindvis af tilfældige personer – alt afhængig af fokusområdets størrelse (og dermed antallet af mulige master) og fokusperiodens længde. For at sikre, at indgrebet er proportionalt i forhold til, at politiet får adgang til data om andre personer end den mistænkte, bør det ved fastsættelse af regler om et nyt tvangsindgreb, sikres, at indgrebet skal være nøje og præcist afgrænset mht. fokusområde og fokustidsrum. Som udgangspunkt finder TI, at et præcist afgrænset fokustidsrum og et præcist afgrænset fokusområde, ikke bør overskride 10 timer og én adresse (eller fx op til 25 masteceller), for derved at sikre, at udgangspunktet for brug af indgrebet er passende afgrænset og dermed proportionalt. Se også nærmere om behovet for afgrænsning mht. fokusområde og fokustidsrum nedenfor i pkt. 5.1 om det tilsvarende eksisterende tvangsindgreb "udvidet teleoplysning", hvor Teleindustrien i 2018 og 2019 har oplevet en meget omfattende og uafgrænset brug af tvangsindgreb. TI foreslår, at spørgsmålet om proportionalitet og afgrænsning præciseres enten via lovforslagsbemærkninger eller direkte i bestemmelsen.

<u>På den baggrund foreslår TI konkret</u>, at et nyt tvangsindgreb i form af 'udvidet masteoplysning' defineres på følgende måde med direkte lovhjemmel i RPL kapitel 71 – f.eks. i tilknytning til reglerne i § 791a, stk. 5 om fremadrettet teleobservation:

> [NY § 791a, stk. Y]:
> Politiet kan fra udbydere af elektroniske kommunikationsnet og -tjenester indhente oplysning om, hvilke mobiltelefoner eller andre tilsvarende mobile kommunikationsapparater, der er registreret anvendt på mobilmaster, der dækker et præcist angivet område [svarende til én adresse], og indenfor en præcist angivet tidsperiode [maksimalt 10 timer] (udvidet masteoplysning), hvis indgrebet må antages at være af

> væsentlig betydning for efterforskningen, og efterforskningen vedrører en lovovertrædelse, der kan medføre fængsel i [x år] eller derover.

Det bemærkes, at TI samtidig foreslår, at det eksisterende tvangsindgreb "udvidet teleoplysning" udgår, jf. nærmere herom nedenfor pkt. 5.2.

4.3. Forslag til definition af nyt tvangsindgreb: Udvidet IP-adresse-oplysning

TI anbefaler, at der fastsættes regler i RPL kap 71 om et nyt tvangsindgreb, 'udvidet IP-adresse-oplysning', som fastlægger betingelserne for politiets adgang til loggede data om, hvilke abonnenter, der har været tildelt en (mobil) dynamisk IP-adresse samtidig, og hvor den unikke abonnenten ikke kan udpeges entydigt, fordi port-nummeret er uoplyst.

Baggrunden for forslaget er følgende:

Teleudbydere tildeler IP-adresser til kunder, der abonnerer på internetadgangstjenester (abonnenten). Dette gælder både ved internetadgangstjenester via faste bredbåndsforbindelser og internetadgangstjenester via mobile datatjenester. IP-adressen identificerer en abonnents adgang til internettet, og svarer således til telefonnummeret for en telefonitjeneste. IP-adressen for et bredbåndsabonnement kan være enten statisk tildelt (fast IP-adresse) eller dynamisk tildelt, mens IP-adresser for et mobilabonnement altid er tildelt dynamisk[9] (mobile dynamiske IP-adresser).

Faste IP-adresser er statisk tildelt et abonnement – typisk mod betaling – og til brug for debitering registrerer teleudbydere i op til 5 år oplysninger om faste IP-adresser på kundens abonnement. Oplysninger om abonnenten bag en fast IP-adresse (både nummer-til-navn og navn-til-nummer) udleveres til politiet uden retskendelse efter reglen i telelovens § 13. Politiet har således direkte adgang til oplysninger, der identificerer abonnenten bag faste IP-adresser, jf. telelovens § 13, på samme måde som politiet har direkte adgang til 118-data om oplysninger, der identificerer abonnenten bag et telefonnummer, jf. telelovens § 31.

Oplysninger om dynamisk tildelt afsender-internetprotokoladresser (dynamisk IP-adresse), registreres når en abonnent påbegynder en internet-session, jf. kravet herom i § 5 i logningsbekendtgørelsen. Opbevaringen af de registrerede oplysninger om dynamiske IP-adresser i 1 år sker udelukkende for at opfylde kravet i logningsbekendtgørelsen, idet teleudbyderne selv kun har brug for at gemme disse data i en kort periode til brug for fejlretning.

Ved internetadgang fra mobile datatjenester er der p.t. mangel på 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 af mobildatatjenesten – typisk flere end tusinde brugere pr. sekund. Kombinationen af dynamisk IP-adresse og portnummer og tidspunkt identificerer normalt entydigt abonnenten. Hvis portnummer derimod ikke kan oplyses, er der typisk flere end 1000 brugeridentiteter (mobiltelefonnumre) pr. dynamisk IP-adresse pr. sekund.

---

[9] Dog undtaget visse privatabonnerede APN'er med dedikerede forbindelser mellem mobilnettet og kundens eget IP-net, hvor faste IP-adresser kan tilvælges.

Registrering af dynamiske IP-adresser er omfattet af § 5 i logningsbekendtgørelsen, og det fremgår af bemærkningerne til telelovens § 13, at udlevering til politiet af dynamiske IP-adresser mv. skal ske efter reglerne i retsplejeloven. Der er imidlertid ikke fastsat nærmere regler i retsplejeloven om betingelserne for politiets adgang til loggede data om brugerne bag dynamiske IP-adresser, og udleveringen sker derfor i dag udelukkende efter reglerne om edition.

Set i lyset af reglen i telelovens § 13, som giver politiet direkte adgang til faste IP-adresser tildelt en entydig abonnent, har TI ingen indvendinger imod, at udlevering af 'almindelig IP-adresse-oplysning', hvor abonnenten er entydig, fortsat sker alene efter edition-kendelse. Dette er ofte tilfældet for dynamisk tildelte IP-adresser i fastnettet.

Mobiludbyderne har imidlertid det seneste år oplevet, at Politiet i stigende omfang anmoder retten om efter reglerne om edition at pålægge mobiludbyderne 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 mobiludbyderne hidtil udleveret oplysning om de mere end 1000 brugeridentiteter (mobiltelefonnumre), som har benyttet den mobile dynamiske IP-adresse på det oplyste tidspunkt.

I disse sager er der ofte *ikke* tale om efterforskning af grov kriminalitet. Eksempelvis er en mobiludbyder blevet pålagt at udlevere oplysninger om flere hundrede brugere af en mobil dynamisk IP-adresse i en sag om misbrug af betalingskort til køb på internettet for beløb under 3000 kr. (databedrageri), og i en anden sag om uberettiget adgang til en idrætsklubs medlemskartotek (hacking). I nogle af sagerne er det tale om navngivne mistænkte, og i andre af sagerne er der tale om ukendte gerningsmænd.

TI finder det generelt uafklaret, om udlevering af oplysninger om tusindvis af brugeridentiteter på ikke-kriminelle og helt tilfældige kunder er proportionalt, jf. proportionalitetsbetragtningen i RPL § 805, stk. 1, hvis der ikke er tale om efterforskning af grov kriminalitet.

Set i lyset af EU-domstolens afgørelse i EU-dom om logning fra 2016 (C-203-15, Tele2-Watson) finder TI det desuden uafklaret, om udlevering af loggede data om, hvilke abonnenter, der har været tildelt en (mobil) dynamisk IP-adresse, fortsat kan ske efter reglerne om edition uden samtidig stillingtagen til graden af den kriminalitet, der efterforskes. Det fremgår således af EU-dommen fra 2016, at artikel 15, stk. 1 i e-datadirektivet (2002/58/EF) er til hinder for national lovgivning, der giver politiet adgang til lagrede data "uden i forbindelse med bekæmpelse af kriminalitet at begrænse denne adgang til målet om bekæmpelse af grov kriminalitet …".

For at undgå nævnte usikkerhed – og henset til, at der er tale om udlevering af loggede data, som teleudbyderne selv kun har brug for at gemme i en kort periode – anmoder TI om, at der fastsættes regler i retsplejelovens kapitel 71 om de nærmere betingelser for politiets adgang til loggede data om, hvilke abonnenter, der har været tildelt en (mobil) dynamisk IP-adresse samtidig, og hvor den unikke abonnent ikke kan udpeges. Udlevering af oplysninger om kunder bag en IP-adresse udspringer oftest af, at politiet har fundet et spor i form af en afsender-IP-adresse (kilde) på en hjemmeside, som er blevet undersøgt ifm efterforskning. TI vurderer derfor, at oplysningerne om afsender-IP-adresse vedrører meddelelseshemmeligheden, idet oplysningerne skaber et billede af, hvilke hjemmesider kunden har eller kan have besøgt.

På den baggrund, foreslår TI konkret, at nyt tvangsindgreb i form af 'Udvidet IP-adresse-oplysning' defineres på følgende måde med direkte lovhjemmel i RPL kapitel 71 – fx i tilknytning til reglerne i § 780 om indgreb i meddelelseshemmeligheden:

> *[NY § i RPL kap 71]:*
> *Politiet kan fra udbydere af elektroniske kommunikationsnet og -tjenester indhente oplysninger om, hvilke abonnenter, der har været tildelt en dynamisk IP-adresse, som kan være tildelt flere abonnenter samtidig (udvidet IP-adresse-oplysning), hvis indgrebet må antages at være af væsentlig betydning for efterforskningen, og efterforskningen vedrører en lovovertrædelse, der kan medføre fængsel i [x år] eller derover.*

4.4. Forslag til definition af nyt tvangsindgreb: IMEI-oplysning

TI foreslår, at der fastsættes regler i RPL kap 71 om et nyt tvangsindgreb, 'IMEI-oplysning', som giver politiet adgang til oplysninger om, hvilke mobilterminaler der har været anvendt til et bestemt telefonnummer og omvendt.

Baggrunden for forslaget er følgende:

Teleudbyderne registrerer oplysninger om diverse numre, der identificerer en mobilbrugers adgang til elektroniske kommunikationsnet eller -tjenester, jf. reglerne herom i logningsbekendtgørelsen:
- IMEI-nummer (en mobilterminals "stelnummer"), jf. logningsbekendtgørelsens § 4, nr. 5
- IMSI-nummer (sim-kort-nummer), jf. logningsbekendtgørelsens § 4, nr. 5
- telefonnummer (MSISDN), jf. logningsbekendtgørelsens § 4, nr. 1 og § 5, stk. 1, nr. 2

Registreringen af data om IMEI-nummer i 1 år sker udelukkende for at opfylde kravet i logningsbekendtgørelsen, idet teleselskaberne selv kun har brug for at registrere data om IMEI-nummer[10] i en ganske kort periode til brug for fejlretning.

Ved en IMEI-oplysning oplyser teleselskabet til politiet, hvilke mobilterminaler, der har været anvendt til et bestemt telefonnummer (fokusnummeret) – og desuden om de identificerede mobiltelefoner omvendt har været anvendt sammen med andre telefonnumre og sim-kort end fokusnummeret. Oplysninger om, hvem der har været kommunikeret med, er ikke omfattet af IMEI-oplysning og kræver særskilt kendelse om teleoplysning, jf. RPL § 780, stk. 1, nr. 3.

Teleselskabernes udlevering af oplysninger til politiet om IMEI-numre og IMSI-numre er hidtil sket efter reglerne om edition. Der er således ikke fastsat regler i retsplejelovens kap 71, der definerer et tvangsindgreb ift. udlevering af oplysninger om IMEI-nummer mv. til politiet – på trods af, at der i medfør af retsplejelovens kapitel 71 (§ 786, stk. 4) er fastsat regler om logning af IMEI-nummer.

[10] Teleudbydere har kun brug for at registrere de første 8 cifre i IMEI-nummeret – i en kort periode til brug for fejlretning. De første 8 cifre i IMEI-nummeret angiver terminaltypen, mens det fulde IMEI-nummer er terminalens unikke "stelnummer".

Dertil kommer, at det har været drøftet i samarbejdsgruppen mellem TI og Rigspolitiet, om der findes situationer, hvor teleselskaberne kan udlevere IMEI-oplysning uden retskendelse. TI lægger til grund, at dette vedrører situationen nævnt i retsplejelovens § 806, stk. 4, som har følgende ordlyd:

> *Stk. 4. Såfremt indgrebets øjemed ville forspildes, hvis retskendelse skulle afventes, kan politiet træffe beslutning om beslaglæggelse og om edition, jf. dog stk. 6. Fremsætter den, mod hvem indgrebet retter sig, anmodning herom, skal politiet snarest muligt og senest inden 24 timer forelægge sagen for retten, der ved kendelse afgør, om indgrebet kan godkendes.*

TI kan hertil bemærke, at det er TI's opfattelse, at der skal foreligge kendelse (eller samtykke) i enhver situation, hvor der skal udleveres loggede data til politiet. Hvis data udleveres "på øjemed" vil der derfor altid være behov for, at politiet efterfølgende forelægger sagen for retten.

Det er TI's opfattelse, at der altid som minimum skal foreligge en editionskendelse, når der udleveres teledata til politiet, da det som nævnt i pkt. 4 i dette notat, er TI's opfattelse, at der bør defineres tvangsindgreb for enhver form for udlevering af trafik- og lokaliseringsdata til politiet.

Set i lyset af EU-domstolens afgørelse i EU-dom om logning fra 2016 (C-203-15, Tele2-Watson) finder TI det desuden uafklaret, om udlevering af loggede data om IMEI-nummer fortsat kan ske efter reglerne om edition uden samtidig stillingtagen til graden af den kriminalitet, der efterforskes. Det fremgår således af EU-dommen fra 2016, at artikel 15, stk. 1 i e-datadirektivet (2002/58/EF) er til hinder for national lovgivning, der giver politiet adgang til lagrede data "uden i forbindelse med bekæmpelse af kriminalitet at begrænse denne adgang til målet om bekæmpelse af grov kriminalitet …".

På den baggrund, foreslår TI konkret, at nyt tvangsindgreb – som fx kan benævnes 'IMEI-oplysning' eller 'terminal-oplysning' – defineres på følgende måde med direkte lovhjemmel i RPL kapitel 71 – f.eks. i tilknytning til reglerne i § 780 om indgreb i meddelelseshemmeligheden:

> *[NY § i RPL kap 71]:*
> *Politiet kan fra udbydere af elektroniske kommunikationsnet og -tjenester indhente oplysninger om, hvilke mobiltelefoner eller andre tilsvarende kommunikationsapparater, der har været anvendt til et mobilabonnement, og omvendt (IMEI-oplysning), hvis indgrebet må antages at være af væsentlig betydning for efterforskningen.*

5. Regler om udlevering af teledata – Afgrænsning af eksisterende tvangsindgreb

5.1. Forslag til ændring af definition af 'Udvidet teleoplysning'

Følgende fremgår af den gældende bestemmelse i RPL § 780, stk. 1, nr. 4 om 'udvidet teleoplysning':

> § 780. Politiet kan efter reglerne i dette kapitel foretage indgreb i meddelelseshemmeligheden ved at
> …

> 4) indhente oplysning om, hvilke telefoner eller andre tilsvarende kommunikationsapparater inden for et nærmere angivet område der sættes i forbindelse med andre telefoner eller kommunikationsapparater (udvidet teleoplysning),

Generelt foreslår TI, at reglen i RPL § 780, stk. 1, nr. 4 om 'udvidet teleoplysning' udgår og erstattes af et nyt tvangsindgreb "udvidet masteoplysning", som beskrevet ovenfor i pkt. 4.2. Alternativt anmoder TI om, at indgrebet afgrænses tidsmæssigt og arealmæssigt.

Baggrunden for TI's forslag er følgende:

Forslag om at lade reglen om 'udvidet teleoplysning' udgå
Tvangsindgrebet 'udvidet teleoplysning' giver politiet adgang til data om, både hvilke mobilterminaler, der har været anvendt på bestemte master til kommunikation (telefoni, sms og mms), men også oplysninger om, hvem mobilterminalerne har kommunikeret med. Sidstnævnte trafikdata er omfattet af meddelelseshemmeligheden, mens oplysningen om, hvilke mobilterminaler, der har været anvendt på bestemte master, ikke i sig selv er omfattet af meddelelseshemmeligheden.

TI finder, at indgrebet 'udvidet teleoplysning" er uforholdsmæssigt indgribende ved både at oplyse, hvilke kunder/mobilterminaler, der har befundet sig i området, men også oplyse, hvem alle disse kunder har kommunikeret med. Et alternativ til en så omfattende udlevering af data til politiet kunne være, at der alene udleveres oplysning om hvilke mobilterminaler, der har været anvendt på bestemte master, jf. TI's forslag i pkt. 4.2 i dette notat om nyt indgreb i form af 'udvidet masteoplysning', og på baggrund af en analyse af disse oplysninger, kunne der herefter udleveres opkaldslister efter behov om kun de mobiltelefoner, som politiet identificerer som fokusnumre (dvs almindelig teleoplysning, jf. RPL § 780, stk. 1, nr. 3). En sådan fremgangsmåde ville samtidig være i overensstemmelse med principperne om dataminimering og proportionalitet.

På den baggrund foreslår TI, at RPL § 780, stk. 1, nr. 4 om 'udvidet teleoplysning' udgår.

Alternativt forslag om at afgrænse reglen om 'udvidet teleoplysning' tidsmæssigt og arealmæssigt.
Afhængig af fokusområdets størrelse og fokusperiodens længde kan indgrebet 'udvidet teleoplysning' omfatte tusindvis af personer og tusindvis af opkald – herunder data om de mange tilfældige personer, som har været til stede i fokusområdet i fokusperioden.

I samarbejdsaftalerne mellem teleudbyderne og Politiet er det for nogle udbydere aftalt, at tvangsindgrebet "udvidet teleoplysning", normalt omfatter en fokusperiode på op til 10 timer hhv. et fokusområde på op til 25 masteceller. Teleudbyderne har imidlertid de seneste år oplevet en intensiveret brug af tvangsindgrebet "udvidet teleoplysning", hvor afgrænsningen af område og tidsrum er usædvanlig bred. Fx blev der i 2018 indhentet kendelse til udlevering af oplysninger for en fokusperiode på 3½ måned for et stort og stærkt trafikeret geografisk område ved Køge Bugt, som er dækket af over 100 masteceller, og hvor lokaliseringsdata (og opkaldsdata) om hundredetusindevis af kunder blev udleveret til politiet. I et andet eksempel fra 2019 blev der indhentet kendelse til udlevering af data fra én bestemt mast ved Rødby Havn, men for udvalgte tidspunkter, som strakte sig over 10 måneder. Og i et tredje eksempel fra 2019 blev der indhentet kendelse til udlevering af data for et fokusområde i Give med en radius på 11 km rundt om gerningsstedet.

Teleindustrien finder det uafklaret, om udlevering af omfattende datamængder om ikke-kriminelle er tilstrækkeligt afgrænset og proportionalt, jf. proportionalitetsbetragtningen i RPL § 782, stk. 1 og i RPL § 805, stk. 1 – og om udleveringen kan ske indenfor for rammerne af EU-domstolens afgørelse i EU-dom om logning fra 2016 (C-203-15, Tele2-Watson).

Følgende fremgår af U.2017.1934Ø for så vidt angår spørgsmålet om proportionalitet (vores fremhævelse):

> *"Det er anklagemyndighedens opfattelse, at indgrebet på grund af sit relativt begrænsede tidsrum sammenholdt med den alvorlige kriminalitet er proportionalt".*

Teleindustrien finder det desuden uklart, om bred og intensiv brug af tvangsindgrebet "udvidet teleoplysning" er i overensstemmelse med de oprindelige rammer og formålet med bestemmelsen i retsplejelovens § 780, stk. 1, nr. 4, som bl.a. forudsatte en præcis afgrænsning mht. område og tidsrum. Det fremgår således af lovforslagsbemærkningerne til lov nr. 465 fra 2001 (lovforslag L 194 fra 2001): (vores fremhævelse)

> *"4.4.3.3. Retskendelsen og dens form*
> *Efter den gældende bestemmelse i retsplejelovens § 783, stk. 1, sker indgreb i meddelelseshemmeligheden efter rettens kendelse. I kendelsen anføres de telefonnumre, lokaliteter, adresser eller forsendelser, som indgrebet angår. Herved sikres, at den bemyndigelse, som kendelsen giver politiet, får en præcis afgrænsning. […].*
>
> *Hvor den typiske situation ved f.eks. teleoplysninger er, at der ønskes oplysninger om bestemte telefonnumre, er situationen ved udvidet teleoplysning (masteoplysninger) den, at der ønskes oplysninger om alle telefoner, der i et givet område og inden for et bestemt tidsrum har benyttet en bestemt sendemast.*
>
> *I sagens natur vil det således i kendelsen om udvidet teleoplysning typisk ikke være muligt at angive det eller de telefonnumre, som indgrebet angår, jf. retsplejelovens § 783, stk. 1. I stedet vil det præcist skulle angives, hvilken sendemast (hvilken lokalitet) og hvilket tidsrum indgrebet angår."*

Udenfor det juridiske kan det i øvrigt oplyses, at eksemplerne fra Give, Rødby Havn og Køge Bugt er stærkt belastende for teleudbydernes it-systemer, og det kan tage timer og dage at foretage udtræk af så store datamængder.

For at sikre, at indgrebet 'udvidet teleoplysning' er proportionalt i forhold til, at politiet får adgang til data om andre personer end den mistænkte, bør reglen i RPL § 780, stk. 1, nr. 4 præciseres med henblik på at sikre, at indgreb er nøje og præcist afgrænset mht. fokusområde og fokustidsrum. Som udgangspunkt finder TI, at et præcist afgrænset fokustidsrum og et præcist afgrænset fokusområde, ikke bør overskride 10 timer og én adresse (eller fx 25 masteceller), for derved at sikre, at udgangspunktet for brug af indgrebet er passende afgrænset og dermed proportionalt. TI foreslår, at spørgsmålet om proportionalitet og afgrænsning præciseres enten via lovforslagsbemærkninger eller direkte i bestemmelsen.

På denne baggrund foreslår TI konkret – som alternativ til at lade bestemmelsen om 'udvidet teleoplysning udgå helt – at reglen i RPL § 780, stk. 1, nr. 4 ændres på følgende måde (ændringsforslag er markeret):

> § 780. Politiet kan efter reglerne i dette kapitel foretage indgreb i meddelelseshemmeligheden ved at
> …
> 4) indhente oplysning om, hvilke mobiltelefoner eller andre tilsvarende mobile kommunikationsapparater inden for et ~~nærmere~~ præcist angivet område [svarende til én adresse], og indenfor en præcist angivet tidsperiode [maksimalt 10 timer], der sættes i forbindelse med andre telefoner eller kommunikationsapparater (udvidet teleoplysning),

5.2. Forslag til ændring af definition af 'Teleobservation'

TI anmoder om, at retsplejelovens § 791a, stk. 5 og 6, som er ændret ved lov om ændring af retsplejeloven m.fl. (Freds- og æreskrænkelser), jf. Lovforslag L20 fremsat 3. oktober 2018, ændres tilbage til den oprindelige formulering.

Baggrunden for TI's ønske er følgende:

På et møde i samarbejdsgruppen mellem TI og Rigspolitiet i marts 2019 gjorde Rigspolitiet Teleindustrien opmærksom på lovforslag L20 om ændring af retsplejeloven. TI blev herved opmærksom på ændringen af retsplejelovens § 791a, stk. 5 og 6 om teleobservation, som er trådt i kraft 1. januar 2019. TI var ikke blevet hørt om udkastet til lovændring.

Følgende fremgår af den oprindelige bestemmelse i retsplejelovens § 791a, stk. 5 og 6 om teleobservation:

> *Stk. 5. Politiet kan fra udbydere af telenet eller teletjenester indhente oplysninger vedrørende lokaliseringen af en mobiltelefon, der antages at benyttes af en mistænkt (teleobservation), hvis indgrebet må antages at være af væsentlig betydning for efterforskningen, og efterforskningen vedrører en lovovertrædelse, der kan medføre fængsel i 1 år og 6 måneder eller derover.*
> *Stk. 6. Det påhviler udbydere af telenet eller teletjenester at bistå politiet ved gennemførelse af teleobservation, herunder ved at give de i stk. 5 nævnte oplysninger.*

Følgende fremgår af den nu ændrede bestemmelse i retsplejelovens § 791a, stk. 5 og 6 om teleobservation (ændringer i forhold til den oprindelige tekst er markeret):

> *"Stk. 5. Må indgrebet antages at være af væsentlig betydning for efterforskningen, og vedrører efterforskningen en lovovertrædelse, der kan medføre fængsel i 1 år og 6 måneder eller derover, kan politiet foretage teleobservation ved*
> *1) at indhente oplysninger fra udbydere af telenet eller teletjenester vedrørende lokaliseringen af en mobiltelefon, der antages at benyttes af en mistænkt eller*
> *2) på anden måde ved hjælp af en gps eller et andet lignende*

apparat at registrere
a) en mistænkts færden eller
b) en anden persons færden, hvis den pågældende har tilknytning til en mistænkt eller til samme køretøj eller ejendom som en mistænkt eller lignende.
Stk. 6. Det påhviler udbydere af telenet eller teletjenester at bistå politiet ved gennemførelse af teleobservation, herunder ved at give de i stk. 5, nr. 1 nævnte oplysninger.

Følgende fremgår af L 20 side 69 i lovforslaget:

Det foreslåede nr. 1 viderefører den gældende bestemmelse om teleobservation forstået som indhentelse af oplysninger fra udbydere af telenet og teletjenester, der gør det muligt løbende at stedfæste en tændt mobiltelefon. Det vil uændret navnlig dreje sig om oplysninger om, hvilke mobiltelefonmaster den pågældende mobiltelefon er i forbindelse med ved opdateringer, hvilken celle der er anvendt ved opdateringen, og i hvilken retning og afstand fra masten mobiltelefonen befinder sig. Bestemmelsen angår den fremadrettede og løbende udlevering af sådanne oplysninger til politiet vedrørende en bestemt mobiltelefon. Indhentelse af oplysninger, som en udbyder af telenet og teletjenester tidligere har lagret om en mobiltelefons forbindelse med master, vil uændret ikke være omfattet af bestemmelsen, men derimod i givet fald kunne ske efter reglerne om edition, jf. retsplejelovens § 804 (der ikke foreslås ændret) og UfR 2009.2610 H.

Følgende fremgår af § 10 i teleloven (vores fremhævelse):

§ 10. Udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal uden udgift for staten sikre,
1) at det tekniske udstyr og de tekniske systemer, som udbyderen anvender, er indrettet således, at politiet kan få adgang til oplysninger om teletrafik og til at foretage indgreb i meddelelseshemmeligheden i form af historisk teleoplysning og historisk udvidet teleoplysning, fremadrettet teleoplysning og fremadrettet udvidet teleoplysning, aflytning og teleobservation, jf. retsplejelovens kapitel 71 og 74, herunder, for så vidt angår fremadrettet teleoplysning og udvidet teleoplysning, at politiet kan få adgang umiddelbart efter, at disse oplysninger registreres.

TI har følgende bemærkninger til ændringerne i retsplejelovens § 791a, stk. 5 og 6:

1. TI finder det ganske uhensigtsmæssigt, at definitionen af teleobservation i RPL § 791a, stk. 5 er blevet udvidet til også at omfatte GPS-observation, som nævnt i RPL § 791a, stk. 5, nr. 2. GPS-observation som

beskrevet i nr. 2 har således intet at gøre med teletjenester. Der kan derfor hurtigt opstå begrebsforvirring og fortolkningstvivl om teleudbydernes forpligtelser. GPS-observation burde have været defineret selvstændigt og burde have haft sin egen selvstændige bestemmelse i retsplejeloven.

2. Teleudbydere er efter telelovens § 10 forpligtet til – uden udgift for staten – at indrette teleudbydernes systemer, så politiet har adgang til at foretage indgreb i form af bl.a. teleobservation. Telelovens § 10 indeholder en krydshenvisning til RPL kap 71, hvor reglen om teleobservation findes. Den ændrede definition af teleobservation i RPL § 791a, stk. 5 kan fortolkes til, at teleudbyderne bliver forpligtet til at indrette systemer til GPS-observation. Dette har næppe været hensigten, og Teleindustrien ønsker under ingen omstændigheder at indrette systemer med henblik på GPS-observation som nævnt i RPL § 791a, stk. 5, nr. 2.

3. Teleudbydere er efter ordlyden af RPL § 791a, stk. 6 forpligtet til at bistå politiet ved gennemførelse af teleobservation. Eftersom definitionen af teleobservation er ændret i den nye § 791a, stk. 5 til også at omfatte GPS-observation, kan reglen fortolkes til, at teleudbyderne er forpligtet til at bistå politiet med at gennemføre GPS-observation. Dette er næppe tilsigtet. Den ændrede formulering i § 791a, stk. 6, ses ikke at afbøde problemet. Teleindustrien ønsker under igen omstændigheder at bistå politiet med GPS-observation som nævnt i RPL § 791a, stk. 5, nr. 2.

Teleindustrien anmoder Justitsministeriet om at bekræfte, at teleudbydere ikke er forpligtet til at bistå ved GPS-observation.

Konkret anmoder TI om, at RPL § 791a, stk. 5 og 6 ændres tilbage til den oprindelige ordlyd, og at regler om GPS-observation flyttes til en særskilt bestemmelse. Ved en sådan ændring, kan det overvejes at præcisere RPL § 791a, stk. 5 på følgende måde (ændringsforslag i forhold til den oprindelige tekst er markeret):

> *Stk. 5. Politiet kan fra udbydere af ~~telenet eller teletjenester~~ elektroniske kommunikationsnet og -tjenester indhente oplysninger vedrørende lokaliseringen af en mobiltelefon eller andre tilsvarende mobile kommunikationsapparater, der antages at benyttes af en mistænkt (teleobservation), hvis indgrebet må antages at være af væsentlig betydning for efterforskningen, og efterforskningen vedrører en lovovertrædelse, der kan medføre fængsel i 1 år og 6 måneder eller derover.*