12. marts 2021

BILAG 1

Notat om tekniske fakta og opmærksomhedspunkter i sager om udlevering til politiet af "lokaliseringsdata for et nummer" ('Masteoplysning')

Lokaliseringsdata for et nummer ('Masteoplysning')
– historiske oplysninger om hvilke masteceller et fokusnummer har været registreret på

Teleselskaberne registrerer lokaliseringsdata i form af celle-ID, som identificerer, hvilke celler (antenner på master) i mobilnettet en slutbrugers mobilterminaludstyr har været i kontakt med, og lokaliseringsdata kan således belyse en mobilterminals overordnede geografiske placering og bevægelsesmønster (dvs hvilke masteceller en mobilterminal har været registreret på).

Teleselskaberne registrerer følgende typer af lokaliseringsdata[1] om mobilterminaler:
1. Lokaliseringsdata, som er trafikdata[2] ifm. telefoni- og sms/mms-kommunikation. Denne type lokaliseringsdata logges generelt til brug for efterforskning og opbevares af teleudbyderne i 1 år, jf. logningsreglerne.
2. Lokaliseringsdata, som er trafikdata ifm. mobildata-kommunikation (internetforbrug – som kan være initieret enten af brugeren eller af telefonens apps). Denne type lokaliseringsdata opbevarer teleudbyderne i kort tid til brug for fejlretning (fx 14 dage) – men dataene kan efter pålæg fra politiet hastesikres og lagres af teleudbyderne i op til 3 måneder (svarende til logning), jf. retsplejelovens § 786a om hastesikring af elektronisk data til brug for efterforskning.
3. Lokaliseringsdata, som ikke er trafikdata, dvs lokaliseringsdata om tændte telefoner, der ikke anvendes aktivt – fx hvis telefonen opdaterer sig på nettet (location update). Denne type lokaliseringsdata opbevarer teleudbyderne i kort tid til brug for fejlretning (fx 14 dage) – men dataene kan efter pålæg fra politiet hastesikres og lagres af teleudbyderne i op til 3 måneder (svarende til logning), jf. retsplejelovens § 786a om hastesikring af elektronisk data til brug for efterforskning.

---

[1] "Lokaliseringsdata" (masteoplysninger i form af Celle-ID) er defineret i teleregulering i § 2, nr. 3 i bekendtgørelse om udbud af elektroniske kommunikationsnet og -tjenester (herefter "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.

[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)

I det daglige samarbejde mellem politiet og teleselskaberne og i retspraksis kaldes lokaliseringsdata af ovennævnte type 1 for "masteoplysning"; og lokaliseringsdata af type 1, type 2 og type 3 kaldes samlet[3] for "lokaliseringsdata for et nummer"[4].

Idet lokaliseringsdata belyser en persons geografiske færden, er der tale om fortrolige data omfattet af principperne om privatlivsbeskyttelse. Antallet af registreringer pr. telefonnummer pr. døgn for lokaliseringsdata af type 1 afhænger af antal opkald og sms til og fra nummeret (fx 5 kald pr. dag medfører 10 registreringer af celle-ID). Antallet af registreringer pr. telefonnummer pr. døgn for lokaliseringsdata af type 2+3 afhænger derimod af antallet af aktive apps på telefonen samt telefonens geografiske bevægelse, og kan variere fra ca. 100 til over 1000 registreringer af celle-ID pr. telefonnummer pr. døgn.

Opmærksomhedspunkter
Teleselskaberne har selv kun brug for at registrere lokaliseringsdata i kort tid til brug for fejlretning, og lagringen af lokaliseringsdata i længere tid sker derfor udelukkende for at opfylde politiets pålæg om hastesikring (op til 3 måneder) eller kravet i logningsbekendtgørelsen (1 år).

Teleeudbyderne har hidtil udleveret masteoplysning/lokaliseringsdata i form af celle-ID for én bestemt mobiltelefon til politiet alene efter editionskendelse, jf. bl.a. U.2009.2610H.

Teleselskaberne finder det uhensigtsmæssigt, at der findes regler i retsplejeloven kapitel 71, som pålægger teleselskaber at logge og hastesikre lokaliseringsdata, uden at der samtidig er fastsat regler i retsplejeloven, der definerer rammerne for udlevering af disse lagrede data til politiet, herunder kriminalitetskrav – ligesom dette er tilfældet for indgreb i meddelelseshemmeligheden, jf. RPL § 780, og teleobservation/fremadrettet lokaliseringsdata, jf. RPL § 791a, stk. 5. Logningsreglerne og reglerne om hastesikring fastsætter således regler om, at teleudbyderne skal lagre data om historisk observation/overvågning af kundernes færden, hvorefter teleudbyderen kan pålægges at udlevere disse data til politiet alene efter reglerne om edition – dvs også ifm. mindre lovovertrædelser.

Set i lyset af EU-domstolens afgørelse i EU-dom om logning fra 2016 (C-203-15, Tele2-Watson) og senest den nye afgørelse i EU-dom om logning fra oktober 2020 (C-511/18, C-512/18 og C-520/18) finder teleselskaberne det

[3] For så vidt angår lokaliseringsdata, som teleselskaberne opbevarer i kort tid til brug for fejlretning, har teleselskaberne kun mulighed for at levere samlede dataudtræk, som omfatter både type 1, type 2 og type 3.
[4] Blev også tidligere kaldt "signaleringsdata for et nummer" – et begreb som teknisk set ikke er en retvisende betegnelse for lokaliseringsdata, og som derfor helt bør undgås.

uafklaret, om udlevering af allerede registrerede lokaliseringsdata (historiske lokaliseringsdata) fortsat kan ske efter reglerne om edition uden samtidig stillingtagen til graden af den kriminalitet, der efterforskes. Det fremgår således af konklusionerne i 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 …". Tilsvarende fremgår af EU-dommen fra 2020 (præmis 166). Det bemærkes hertil, at hastesikrede data må sidestilles med loggede data, idet der i begge tilfælde er tale om lagrede data. Spørgsmålet er også behandlet af EU-domstolen i sag C-746/18.

Særligt i forbindelse med lovovertrædelser, som ikke er grov kriminalitet eller alvorlige trusler mod den nationale sikkerhed, finder teleselskaberne, at det bør afklares, om det er proportionalt og i overensstemmelse med EU-dommene fra 2016 og 2020, at politiet får adgang til lagrede lokaliseringsdata.

Til orientering kan det oplyses, at teleselskabernes branchesamarbejde, Teleindustrien (TI) på baggrund af ovenstående opmærksomhedspunkter i notat den 28. februar 2020 (pkt. 4.1 i notatet) har opfordret Justitsministeriet til, at der defineres et nyt tvangsindgreb, 'Masteoplysning', som fastsætter de nærmere rammer og betingelser for politiets adgang til lagrede lokaliseringsdata: http://www.teleindu.dk/brancheholdninger/logning-og-teledata/.

12. marts 2021

BILAG 2

Notat om tekniske fakta og opmærksomhedspunkter i sager om udlevering af 'lokaliseringsdata for et område/adresse' til politiet ('Udvidet Masteoplysning')

Lokaliseringsdata for et område/adresse ('Udvidet Masteoplysning') – historiske oplysninger om hvilke numre, der har været registreret på masteceller, der dækker et fokusområde

Teleselskaberne registrerer lokaliseringsdata i form af celle-ID, som identificerer, hvilke celler (antenner på master) i mobilnettet en slutbrugers mobilterminaludstyr har været i kontakt med, og lokaliseringsdata kan således belyse hvilke mobilterminaler (numre), der har været registreret på masteceller, der dækker et nærmere afgrænset geografisk område - typisk en adresse (fokusadressen/gerningsstedet).

Teleselskaberne registrerer følgende typer af lokaliseringsdata[5] om mobilterminaler:

1. Lokaliseringsdata, som er trafikdata[6] ifm. telefoni- og sms/mms-kommunikation. Denne type lokaliseringsdata logges generelt til brug for efterforskning og opbevares af teleudbyderne i 1 år, jf. logningsreglerne.

2. Lokaliseringsdata, som er trafikdata ifm. mobildatakommunikation (internetforbrug – som kan være initieret enten af brugeren eller af telefonens apps). Denne type lokaliseringsdata opbevarer teleudbyderne i kort tid til brug for fejlretning (fx 14 dage) – men dataene kan efter pålæg fra politiet hastesikres og lagres af teleudbyderne i op til 3 måneder (svarende til logning), jf. retsplejelovens § 786a om hastesikring af elektronisk data til brug for efterforskning.

3. Lokaliseringsdata, som ikke er trafikdata, dvs lokaliseringsdata om tændte telefoner, der ikke anvendes aktivt – fx hvis telefonen opdaterer sig på nettet (location update). Denne type lokaliseringsdata opbevarer teleudbyderne i kort tid til brug for fejlretning (fx 14 dage) – men dataene kan efter pålæg fra politiet hastesikres og lagres af teleudbyderne i op til 3 måneder (svarende til logning), jf. retsplejelovens § 786a om hastesikring af elektronisk data til brug for efterforskning.

---

[5] "Lokaliseringsdata" (masteoplysninger i form af Celle-ID) er defineret i teleregulerin-gen i § 2, nr. 3 i bekendtgørelse om udbud af elektroniske kommunikationsnet og -tjenester (herefter "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.

[6] "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)

I det daglige samarbejde mellem politiet og teleselskaberne kaldes oplysninger om, hvilke mobilterminaler (numre), der har været registreret på masteceller, der dækker et nærmere afgrænset fokusområde/adresse for "lokaliseringsdata for et område/adresse"[7]. Der er tale om lokaliseringsdata, som teleselskaberne opbevarer i kort tid til brug for fejlretning, og teleselskaberne har kun mulighed for at levere samlede dataudtræk, som omfatter både type 1, type 2 og type 3.

Idet lokaliseringsdata belyser personers geografiske opholdssted, er der tale om fortrolige data omfattet af principperne om privatlivsbeskyttelse. Antallet af registreringer pr. telefonnummer pr. døgn for lokaliseringsdata af type 1 afhænger af antal opkald og sms til og fra nummeret (fx 5 kald pr. dag medfører 10 registreringer af celle-ID). Antallet af registreringer pr. telefonnummer pr. døgn for lokaliseringsdata af type 2+3 afhænger derimod af antallet af aktive apps på telefonen samt telefonens geografiske bevægelse, og kan variere fra ca. 100 til over 1000 registreringer af celle-ID pr. telefonnummer pr. døgn.

Udvælgelse af masteceller, der dækker fokusadressen
Den radiotekniske opbygning af mobilnet indebærer, at mange masteceller i mobilnettet bidrager til dækning på en given adresse. Det er således ikke muligt kun at udpege én bestemt celle eller mast, der dækker en given adresse. For hvert af teleselskabernes mobilnet findes for hvert punkt i Danmark en "bedste celle" i teleselskabets mobilnet pr. teknologi pr. frekvens. En celle kan dog også give radiodækning udenfor det geografiske område, hvor cellen er "bedste celle" – og derfor kan de omkringliggende celler/master, som ligger rundt om "bedste celle", også give radiodækning på fokusadressen – fx hvis "bedste celle" er ude af drift eller overbelastet – eller pga. vejrforhold og topografi. Sådanne omkringliggende sekundære celler er typisk celler, der peger mod fokusadressen fra andre master, der ligger i nærheden af fokusadressen – men det kan også forekomme, at sekundære masteceller, der bidrager til dækning på en given adresse, ligger flere kilometer væk fra adressen.

Dertil kommer, at der ved udlevering af "lokaliseringsdata" for en given mastecelle, sker udlevering af oplysning om alle mobilterminaler/numre, der har benyttet cellen i hele cellens dækningsområde – et område som afhængig af mastetætheden i området kan være flere kvadratkilometer stort. Dette skyldes, at oplysning om hvilke terminaler/numre, der har været registreret på en mastecelle, ikke indeholder oplysning om terminalens afstand til masten eller terminalens præcise geografiske position i øvrigt.

[7] Blev også tidligere kaldt "signaleringsdata" – et begreb som teknisk set ikke er en retvisende betegnelse for lokaliseringsdata, og som derfor helt bør undgås.

Ved teleselskabernes udlevering til politiet af "lokaliseringsdata for et område/adresse" – dvs oplysninger om, hvilke mobilterminaler (numre), der har været registreret på masteceller, der dækker et nærmere afgrænset fokusområde/adresse – udleveres således oplysning om de mange personer, som har befundet sig i hele det store område rundt om fokusadressen, som er radiodækket af alle de masteceller, der bidrager til dækning på fokusadressen. Afhængig af mastetætheden i det pågældende område udleverer hver af de 4 mobilskaber normalt oplysning om flere tusinde mobilnumre pr. time pr. fokusadresse i de større byer.

Det kan supplerende oplyses, at teleselskaberne generelt fraråder, at rekvisitioner og kendelser nævner en radius, medmindre selve gerningsstedet er et område, som er cirkelformet. Rekvisitioner og kendelser bør udpege præcist, hvilke(n) adresse(r) eller steder, der er fokus – hvorefter teleselskaberne ud fra en radioteknisk vurdering undersøger og indestår for, hvilke masteceller, der dækker fokusområdet. Hvis kendelser nævner en radius rundt om fokusadressen og pålægger teleselskaberne at udlevere lokaliseringsdata for hele det cirkelformede område – dvs oplysninger om, hvilke mobilterminaler (numre), der har været registreret på masteceller, der dækker området indenfor cirklen – vil teleselskaberne ud over masteceller, der dækker fokusadressen, også udvælge celler der dækker alle punkter i cirklen, herunder (1) celler som ligger udenfor cirklen, men som giver dækning ind i cirklen uden nødvendigvis at give dækning på fokusadressen, samt (2) celler, der ligger indenfor cirklen, men som peger væk fra fokusadressen, og som derfor ikke giver dækning på fokusadressen.

Såfremt politiet i enkeltsager har behov for, at fokusområdet fastsættes med en radius som et stort cirkelareal, opfordrer teleselskaberne til, at den efterforskningsmæssige begrundelse herfor er nøje beskrevet.

Opmærksomhedspunkter
Teleselskaberne har selv kun brug for at registrere lokaliseringsdata i kort tid til brug for fejlretning, og lagringen af lokaliseringsdata i længere tid sker derfor udelukkende for at opfylde politiets pålæg om hastesikring (op til 3 måneder) eller kravet i logningsbekendtgørelsen (1 år).

Teleselskaberne har hidtil – baseret på registrerede lokaliseringsdata – udleveret oplysninger til politiet, om hvilke mobilterminaler/numre, der har været registreret på masterceller, der dækker et fokusområde/adresse 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 udelukkende er tale om lokaliseringsdata, jf. U.2017.1934Ø.

Der en dog 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 på mobilmaster, der dækker et gerningssted. Det kan derfor ikke udelukkes, at hensigten med fastsættelsen af reglen om udvidet teleoplysning, jf. retsplejelovens § 780, stk. 1, nr. 4, primært har været, at fastsætte rammerne for politiets adgang til oplysninger om, hvilke mobiltelefoner, der har været registreret 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):

> *"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."*

Teleselskaberne vurderer derfor, at der bør tages udgangspunkt i lovforarbejderne til reglen i retsplejelovens § 780, stk. 1, nr. 4 ved overvejelsen af hvilke rammer (kriminalitetskrav mv), der bør gælde for politiets adgang til registrerede lokaliseringsdata, der viser, hvilke mobiltelefoner, der har været registreret på mobilmaster.

Dertil kommer, at politiets indhentelse af registrerede lokaliseringsdata om, hvilke mobiltelefoner der er registreret 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 teleselskabernes systemer til brug for fejlretning (prober) opsamler og registrerer lokaliseringsdata både ved telefoni-, sms-, mms- og datakommunikation og ved mobilitet, herunder også hvis telefonen er 'tændt men ikke aktiv'. Tendensen forstærkes af, at mobilkunderne i stigende omfang benytter mobildatakommunikation, men ikke telefoni og sms. Der er således tale om udlevering af oplysninger til politiet om et ganske stort antal ikke-mistænkte.

Teleselskaberne finder det uhensigtsmæssigt, at der findes regler i retsplejeloven kapitel 71, som pålægger teleselskaber at logge og hastesikre lokaliseringsdata, uden at der samtidig er fastsat regler i retsplejeloven, der definerer rammerne for udlevering af disse lagrede data til politiet, herunder kriminalitetskrav – ligesom dette er tilfældet for indgreb i meddelelseshemmeligheden i form af udvidet teleoplysning, jf. RPL § 780, stk. 1, nr. 4. Logningsreglerne

og reglerne om hastesikring fastsætter således regler om, at teleudbyderne skal lagre data om historisk observation/overvågning af kundernes geografiske opholdssted, hvorefter teleudbyderen kan pålægges at udlevere disse data til politiet alene efter reglerne om edition – dvs også ifm. mindre lovovertrædelser.

Det bemærkes desuden, at teleselskaberne oplever, at politiet i stigende omfang efter reglerne om edition begærer adgang til lokaliseringsdata for et område/adresse i sager, der ikke vedrører efterforskning af grov kriminalitet - eksempelvis i sager om indbrud i biler.

Set i lyset af EU-domstolens afgørelse i EU-dom om logning fra 2016 (C-203-15, Tele2-Watson) og senest den nye afgørelse i EU-dom om logning fra oktober 2020 (C-511/18, C-512/18 og C-520/18) finder teleselskaberne det uafklaret, om udlevering af allerede registrerede lokaliseringsdata (historiske lokaliseringsdata) fortsat kan ske efter reglerne om edition uden samtidig stillingtagen til graden af den kriminalitet, der efterforskes. Det fremgår således af konklusionerne i 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 …". Tilsvarende fremgår af EU-dommen fra 2020 (præmis 166). Det bemærkes hertil, at hastesikrede data må sidestilles med loggede data, idet der i begge tilfælde er tale om lagrede data.

Særligt i forbindelse med lovovertrædelser, som ikke er grov kriminalitet eller alvorlige trusler mod den nationale sikkerhed, finder teleselskaberne, at det bør afklares, om det er proportionalt og i overensstemmelse med EU-dommene fra 2016 og 2020, at politiet får adgang til lagrede lokaliseringsdata om tusindvis af ikke-mistænkte og helt tilfældige kunder.

Derudover bemærkes generelt – også i forhold til sager om grov kriminalitet – at udlevering af historiske lokaliseringsdata for et område/adresse, dvs oplysning om hvilke mobilterminaler/numre, der har været registreret i et område, som beskrevet ovenfor kan omfatte mange tusinde tilfældige personer – alt afhængig af fokusperiodens længde og fokusområdets størrelse. For at sikre, at politiets adgang til de lagrede data er proportionalt i forhold til, at politiet får adgang til data om tusindvis af personer ud over mistænkte, bør politiets adgang til data være nøje og præcist afgrænset mht. fokusområde og fokustidsrum, jf. de persondataretlige princippet om dataminimering. Teleselskaberne har imidlertid de seneste år oplevet, at politiet har intensiveret brugen af 'lokaliseringsdata for et område/adresse', hvor afgrænsningen af område og tidsrum er usædvanlig bred. Fx er der indhentet kendelse til udlevering af oplysninger for en fokusperiode på 3½ måned for et stærkt trafikeret punkt (motorvej), hvor lokaliseringsdata om hundredetusindevis af kunder blev ud-

leveret til politiet. I et andet eksempel blev der indhentet kendelse til udlevering af data for et fokusområde med en radius på 11 km rundt om gerningsstedet.

Teleselskaberne finder, at det bør afklares, om udlevering af omfattende datamængder om ikke-mistænkte er tilstrækkeligt afgrænset og proportionalt, jf. 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).

Generelt – også i forhold til sager om grov kriminalitet – finder teleselskaberne, at et præcist afgrænset fokustidsrum og et præcist afgrænset fokusområde, som udgangspunkt ikke bør overskride én adresse og 1-2 timer (og maksimalt 10 timer), for derved at sikre, at udgangspunktet for politiets adgang til lokaliseringsdata for et område/adresse er afgrænset og dermed proportionalt.

Til orientering kan det oplyses, at teleselskabernes branchesamarbejde, Teleindustrien (TI) på baggrund af ovenstående opmærksomhedspunkter i notat den 28. februar 2020 (pkt. 4.2 i notatet) har opfordret Justitsministeriet til, at der defineres et nyt tvangsindgreb, 'Udvidet Masteoplysning', som fastsætter de nærmere rammer og betingelser for politiets adgang til lagrede lokaliseringsdata for et område/adresse:
http://www.teleindu.dk/brancheholdninger/logning-og-teledata/.

12. marts 2021

10

BILAG 3

Notat om tekniske fakta og opmærksomhedspunkter i sager om udlevering af 'Udvidet Teleoplysning' til politiet

'Udvidet Teleoplysning', jf. RPL § 780, stk. 1, nr. 4 – historiske oplysninger om hvilke numre, der har kommunikeret via masteceller, der dækker et fokusområde, samt teleoplysning for disse numre

Teleselskaberne registrerer lokaliseringsdata i form af celle-ID, som identificerer, hvilke celler (antenner på master) i mobilnettet en slutbrugers mobilterminaludstyr har været i kontakt med, og lokaliseringsdata kan således belyse hvilke mobilterminaler (numre), der har været registreret på masteceller, der dækker et nærmere afgrænset geografisk område - typisk en adresse (fokusadressen/gerningsstedet).

Teleselskaberne registrerer følgende typer af lokaliseringsdata[8] om mobilterminaler:

1. Lokaliseringsdata, som er trafikdata[9] ifm. telefoni- og sms/mms-kommunikation. Denne type lokaliseringsdata logges generelt til brug for efterforskning og opbevares af teleudbyderne i 1 år, jf. logningsreglerne.

2. Lokaliseringsdata, som er trafikdata ifm. mobildatakommunikation (internetforbrug via – som kan være initieret enten af brugeren eller af telefonens apps). Denne type lokaliseringsdata opbevarer teleudbyderne i kort tid til brug for fejlretning (fx 14 dage) – men dataene kan efter pålæg fra politiet hastesikres og lagres af teleudbyderne i op til 3 måneder (svarende til logning), jf. retsplejelovens § 786a om hastesikring af elektronisk data til brug for efterforskning.

3. Lokaliseringsdata, som ikke er trafikdata, dvs lokaliseringsdata om tændte telefoner, der ikke anvendes aktivt – fx hvis telefonen opdaterer sig på nettet (location update). Denne type lokaliseringsdata opbevarer teleudbyderne i kort tid til brug for fejlretning (fx 14 dage) – men dataene kan efter pålæg fra politiet hastesikres og lagres af teleudbyderne i op til 3 måneder (svarende til logning), jf. retsplejelovens § 786a om hastesikring af elektronisk data til brug for efterforskning.

---

[8] "Lokaliseringsdata" (masteoplysninger i form af Celle-ID) er defineret i teleregulerin-gen i § 2, nr. 3 i bekendtgørelse om udbud af elektroniske kommunikationsnet og -tjenester (herefter "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.

[9] "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)

Teleselskaberne registrerer desuden trafikdata om kundernes kommunikation (teletrafik) i form af A-nummer (den der kalder op), B-nummer (det kaldte nummer) samt forbrugets begyndelsestidspunkt og varighed. Registreringen af trafikdata sker til brug for overførslen af kommunikationen i telenettet og til beregning og taksering af kundernes forbrug af udgående kald. Registreringen af indkommende kald i 1 år sker udelukkende for at opfylde logningsreglerne.

Teleselskaberne registrerer følgende typer af trafikdata om mobilterminalers kommunikation:
a. Trafikdata ifm telefoni-kommunikation: Denne type trafikdata logges og opbevares i 1 år, jf. logningsreglerne.
b. Trafikdata ifm sms/mms-kommunikation: Denne type trafikdata logges og opbevares i 1 år, jf. logningsreglerne.
c. Trafikdata ifm datakommunikation (internet mv): Volumenforbrug registreres til brug for debitering. Oplysning om brugerens konkrete datakommunikation, herunder hvilke internetadresser/IP-adresser, brugeren kommunikerer med (færden på internettet) registreres ikke.

De registrerede trafikdata om, hvem en mobilterminal har kommunikeret med (trafikdata af type a og b) kan sammenholdes med de registrerede lokaliseringsdata af type 1, og vil herefter kunne vise, hvilke numre, der har kommunikeret via masteceller, der dækker et fokusområde, samt teleoplysning for disse numre (udvidet teleoplysning).

I det daglige samarbejde mellem politiet og teleselskaberne kalder politiet nogle gange udvidet teleoplysning for ”mastesug”. Betegnelsen ”mastesug” er misvisende, idet udvidet teleoplysning ikke omfatter oplysning om lokaliseringsdata af type 2 og 3. Betegnelsen ”mastesug” bør derfor undgås.

Udvælgelse af masteceller, der dækker fokusadressen
Den radiotekniske opbygning af mobilnet indebærer, at mange masteceller i mobilnettet bidrager til dækning på en given adresse. Det er således ikke muligt kun at udpege én bestemt celle eller mast, der dækker en given adresse. For hvert af teleselskabernes mobilnet findes for hvert punkt i Danmark en ”bedste celle” i teleselskabets mobilnet pr. teknologi pr. frekvens. En celle kan dog også give radiodækning udenfor det geografiske område, hvor cellen er ”bedste celle” – og derfor kan de omkringliggende celler/master, som ligger rundt om ”bedste celle”, også give radiodækning på fokusadressen – fx hvis ”bedste celle” er ude af drift eller overbelastet – eller pga. vejrforhold og topografi. Sådanne omkringliggende sekundære celler er typisk celler, der peger mod fokusadressen fra andre master, der ligger i nærheden af fokusadressen – men det kan også forekomme, at sekundære masteceller, der bi-

drager til dækning på en given adresse, ligger flere kilometer væk fra adressen.

Dertil kommer, at der ved udlevering af udvidet teleoplysning , sker udlevering af oplysning om alle mobilterminaler/numre, der har benyttet hver af de udvalgte celler i hele cellens dækningsområde – et område som afhængig af mastetætheden i området kan være flere kvadratkilometer stort. Dette skyldes, at oplysning om hvilke terminaler/numre, der har været registreret på en mastecelle, ikke indeholder oplysning om terminalens afstand til masten eller terminalens geografiske position i øvrigt.

Ved teleselskabernes udlevering til politiet af udvidet teleoplysning udleveres således oplysning om de mange personer, som har befundet sig i hele det store område rundt om fokusadressen, som er radiodækket af alle de masteceller, der bidrager til dækning på fokusadressen. Afhængig af mastetætheden i det pågældende område udleverer hvert teleselskab normalt oplysning om flere tusinde mobilnumre pr. time pr. fokusadresse.

Det kan supplerende oplyses, at teleselskaberne generelt fraråder, at rekvisitioner og kendelser nævner en radius, medmindre selve gerningsstedet er et område, som er cirkelformet. Rekvisitioner og kendelser bør udpege præcist, hvilke(n) adresse(r) eller steder, der er fokus – hvorefter teleselskaberne ud fra en radioteknisk vurdering undersøger og indestår for, hvilke masteceller, der dækker fokusområdet. Hvis kendelser nævner en radius rundt om fokusadressen og pålægger teleselskaberne at udlevere udvidet teleoplysning for hele det cirkelformede område, vil teleselskaberne ud over masteceller, der dækker fokusadressen, også udvælge celler der dækker alle punkter i cirklen, herunder (1) celler som ligger udenfor cirklen, men som giver dækning ind i cirklen uden nødvendigvis at give dækning på fokusadressen, samt (2) celler, der ligger indenfor cirklen, men som peger væk fra fokusadressen, og som derfor ikke giver dækning på fokusadressen. Såfremt politiet i enkeltsager har behov for, at fokusområdet skal fastsættes som et stort cirkelareal, opfordrer teleselskaberne til, at den efterforskningsmæssige begrundelse herfor er nøje beskrevet.

Opmærksomhedspunkter
Det bemærkes generelt at udlevering af udvidet teleoplysning, jf. RPL § 780, stk. 1, nr. 4, som beskrevet ovenfor kan omfatte mange tusinde tilfældige personer – alt afhængig af fokusperiodens længde og fokusområdets størrelse. For at sikre, at politiets adgang til de lagrede data er proportionalt i forhold til, at politiet får adgang til data om tusindvis af personer ud over mistænkte, bør politiets adgang til data være nøje og præcist afgrænset mht. fokusområde og fokustidsrum, jf. de persondataretlige principper om dataminimering. Teleselskaberne har imidlertid de seneste år oplevet en intensiveret brug af tvangsindgrebet ”udvidet teleoplysning”, hvor afgrænsningen af om-

råde og tidsrum er usædvanlig bred. Fx er der indhentet kendelse til udlevering af oplysninger for en fokusperiode på 3½ måned for et stærkt trafikeret punkt (motorvej), hvor udvidet teleoplysning om hundredetusindevis af kunder blev udleveret til politiet. I et andet eksempel blev der indhentet kendelse til udlevering af data for et fokusområde med en radius på 11 km rundt om gerningsstedet.

Teleselskaberne finder det, at det bør afklares, om udlevering af omfattende datamængder om ikke-mistænkte 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).

Teleindustrien finder desuden, at det bør afklares, 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):

> *"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."*

Generelt finder teleselskaberne, at et præcist afgrænset fokustidsrum og et præcist afgrænset fokusområde, som udgangspunkt ikke bør overskride én adresse og 1-2 timer (og maksimalt 10 timer), for derved at sikre, at udgangspunktet for politiets adgang til udvidet teleoplysning er passende afgrænset og dermed proportionalt, samt ligger indenfor de oprindelige rammer og formålet med bestemmelsen i retsplejelovens § 780, stk. 1, nr. 4.

14

Til orientering kan det oplyses, at teleselskabernes branchesamarbejde, Teleindustrien (TI) på baggrund af ovenstående opmærksomhedspunkter i notat den 28. februar 2020 (pkt. 5.2 i notatet) har opfordret Justitsministeriet til, at RPL § 780, stk. 1, nr. 4 om 'udvidet teleoplysning" præciseres med en forudsætning om præcis afgrænsning mht. område og tidsrum: http://www.teleindu.dk/brancheholdninger/logning-og-teledata/.

12. marts 2021

15

BILAG 4

Notat om tekniske fakta og opmærksomhedspunkter i sager om udlevering af 'Udvidet IP-adresse-oplysning' til politiet

'Udvidet IP-adresse-oplysning' (mobil IP-adresse uden portnummer) – historiske oplysninger om identiteten på alle abonnenterne bag en mobil dynamisk IP-adresse, der bruges af flere, og hvor portnummer ikke er oplyst

Teleudbydere tildeler IP-adresser (afsender-internetprotokoladresser) 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 fastnet bredbåndsabonnement kan være enten statisk tildelt (fast IP-adresse) eller dynamisk tildelt, mens IP-adresser for et mobilabonnement altid er tildelt dynamisk (mobile dynamiske IP-adresser).

En fast IP-adresse er statisk tildelt et bestemt 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.

En dynamisk IP-adresse tildeles løbende til flere forskellige abonnementer, og teleselskaberne registrerer oplysninger om hvilke dynamiske IP-adresser, der tildeles et abonnement samt tidspunkt, når en abonnent påbegynder en internet-session, jf. kravet herom i § 5 i logningsbekendtgørelsen.

Ved internetadgang fra mobile datatjenester (og i visse tilfælde også fastnet bredbånd) er der mangel på dynamiske IP-adresser (IPv4), og derfor tildeles abonnenten både et portnummer og en dynamisk afsender-IP-adresse, som "oversættes" via NAT (Network Address Translation). Brugen af NAT indebærer, at én dynamisk IP-adresse kan deles mellem flere brugere – typisk flere end tusinde brugere pr. sekund. Kombinationen af dynamisk IP-adresse og portnummer identificerer entydigt abonnenten. Hvis portnummer derimod ikke kan oplyses, er der typisk flere end 1000 brugeridentiteter (mobiltelefonnumre) pr. dynamisk IP-adresse pr. sekund.

Teleselskaberne har det seneste år oplevet, at politiet i stigende omfang anmoder retten om efter reglerne om edition at pålægge teleselskaberne at udlevere oplysning om, hvem der er registreret som brugere af mobile dynamiske IP-adresser på et bestemt tidspunkt angivet med sekunds nøjagtighed – men uden at politiet har oplysning om portnummer. I disse sager har teleselskaberne hidtil udleveret oplysning om de mere end 1000 brugeridentiteter (mobiltelefonnumre), som har benyttet den mobile dynamiske IP-adresse på det oplyste tidspunkt.

I disse sager er der i flere tilfælde *ikke* tale om efterforskning af grov kriminalitet. Fx er teleselskaberne blevet pålagt at udlevere oplysninger om flere hundrede brugere af en mobil dynamisk IP-adresse i sager 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.

Opmærksomhedspunkter
Teleselskaberne har selv kun har brug for at gemme oplysninger om dynamiske IP-adresser i kort tid til brug for fejlretning, og lagringen af oplysninger om, hvem der har været tildelt en dynamisk IP-adresser, og hvornår, sker derfor udelukkende for at opfylde kravet i logningsbekendtgørelsen (1 år).

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.

Teleselskaberne finder det uhensigtsmæssigt, at der findes regler i retsplejeloven kapitel 71, som pålægger teleselskaber at logge oplysninger om, hvem der har været tildelt dynamiske IP-adresser, uden at der samtidig er fastsat regler i retsplejeloven, der definerer rammerne for udlevering af disse lagrede data til politiet, herunder kriminalitetskrav – ligesom dette er tilfældet for indgreb i meddelelseshemmeligheden, jf. RPL § 780. Logningsreglerne fastsætter således regler om, at teleudbyderne skal lagre data om identiteten bag en dynamisk tildelt IP-adresse, hvorefter teleudbyderen kan pålægges at udlevere disse data til politiet alene efter reglerne om edition – dvs også ifm. mindre lovovertrædelser.

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 besøgt hjemmeside, som politiet har undersøgt ifm efterforskning. Oplysnin-

gerne om afsender-IP-adresse vedrører således på sin vis meddelelseshemmeligheden. Indgreb i meddelelseshemmeligheden kan efter reglerne i RPL kapitel 71 kun ske i sager om grov kriminalitet. Set i dette lys finder teleselskaberne det betænkeligt, at teleudbyderen kan pålægges at udlevere oplysninger om kunder bag en IP-adresse ifm. mindre lovovertrædelser.

Set i lyset af EU-domstolens afgørelse i EU-dom om logning fra 2016 (C-203-15, Tele2-Watson) og senest den nye afgørelse i EU-dom om logning fra oktober 2020 (C-511/18, C-512/18 og C-520/18) finder teleselskaberne 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 …". Tilsvarende fremgår af EU-dommen fra 2020 (præmis 166). Det fremgår desuden af EU-dommen fra 2020, at IP-adresser må logges generelt til brug for bekæmpelse af grov kriminalitet.

Særligt i forbindelse med lovovertrædelser, som ikke er grov kriminalitet, finder teleselskaberne, at det bør afklares, om det er proportionalt og i overensstemmelse med EU-dommene fra 2016 og 2020 at politiet får adgang til lagrede oplysninger om kunder bag en IP-adresse.

Teleselskaberne finder det desuden generelt uafklaret – også i forhold til sager om grov kriminalitet – om det er proportionalt, at der i sager om udlevering af brugeridentiteten bag en mobil dynamisk IP-adresse, hvor det ikke er muligt for politiet at fremskaffe både IP-adresse og portnummer, sker udlevering af oplysninger om tusindvis af brugeridentiteter på ikke-mistænkte og helt tilfældige kunder.

I sager om udlevering af brugeridentiteten bag en mobil dynamisk IP-adresse, hvor det ikke er muligt for politiet at fremskaffe både IP-adresse og portnummer, finder teleselskaberne det hensigtsmæssigt, at det afspejles i kendelsen, at det ikke er muligt at fremskaffe portnummer, og at teleselskabet derfor skal udlevere oplysning om alle abonnenter (op til 1000 abonnenter pr. sekund), der har været tildelt den mobile dynamiske IP-adresse på det angivne tidspunkt. Tidspunktet skal desuden angives præcist i dansk tid. I sager, hvor der efterforskes for flere dynamiske IP-adresser uden portnummer, bør dette iagttages pr. IP-adresse.

Til orientering kan det oplyses, at teleselskabernes branchesamarbejde, Teleindustrien (TI) på baggrund af ovenstående opmærksomhedspunkter i notat den 28. februar 2020 (pkt. 4.3 i notatet) har opfordret Justitsministeriet til, at

18

der defineres et nyt tvangsindgreb, 'Udvidet IP-adresse-oplysning', som fastsætter de nærmere rammer og betingelser for politiets adgang til oplysning om hvilke abonnenter, der har været tildelt en dynamisk IP-adresse samtidig, og hvor der ikke kan udpeges en entydig abonnement, fordi port-nummeret er uoplyst: http://www.teleindu.dk/brancheholdninger/logning-og-teledata/.