Til Rigsadvokaten og Rigspolitiet

Sendt pr. e-mail til:
Katrine Krejberg, Rigsadvokaten (KKR003@ANKL.DK)
Christian Svanberg, Rigspolitiet Databeskyttelsesenheden (CSV010@POLITI.DK)
Lars Mortensen, Rigspolitiet Nationalt Kriminalteknisk Center, NKC; Tele og Aflytning (LMO006@politi.dk)
Henrik Lange Blichmann, Rigspolitiet Nationalt Efterforskningscenter, NEC (HLB002@POLITI.DK)

27. marts 2020

Terminologi ifm teleudbyderenes udlevering af lokaliseringsdata til politiet efter rettens kendelse (masteoplysning)

Som drøftet på møde i Rigspolitiets Telebrancheforum (juridisk gruppe) den 9. marts 2020 vender Teleindustrien (TI) hermed tilbage med forslag til terminologi og begreber, som TI foretrækker, at politi og anklagemyndighed fremover anvender ifm anmodninger til teleselskaberne om hastesikring og udlevering af lokaliseringsdata (masteoplysninger i form af celle-ID), herunder anvendes når anklagemyndigheden anmoder om rettens kendelse om at pålægge teleudbyderne at udlevere sådanne registrerede lokaliseringsdata til politiet.

Teleindustriens anbefalinger
TI anbefaler, at politi og anklagemyndighed benytter følgende begreber ved anmodning om hastesikring og ved anmodning om edition af registrerede lokaliseringsdata[1]:

(A)
"Oplysning om registrerede lokaliseringsdata for [fokusnummer] i [tidsrum]",
– i daglig tale "Masteoplysning' eller 'Lokaliseringsdata (nummer -> master)'.

(B)
"Oplysning om, hvilke mobilterminaler, der har været registreret på mobilmaster, der dækker [fokusområde] i [tidsrum]"
– i daglig tale 'Udvidet masteoplysning' eller 'Lokaliseringsdata (master -> numre)'.

TI anmoder endvidere om, at begrebet "signaleringsdata" udgår og helt undgås i dialogen mellem politiet og teleudbyderne, herunder ved politi og anklagemyndigheds anmodning om hastesikring og ved anmodning om edition af registrerede lokaliseringsdata, jf. nærmere herom nedenfor.

[1] Lokaliseringsdata (masteoplysninger i form af celle-ID) er defineret i telereguleringen. Se note 2.

Baggrund

Teleudbyderne registrerer følgende typer af lokaliseringsdata (masteoplysninger i form af data om hvilke masteceller en mobilterminal har været registreret på):

1. Lokaliseringsdata[2], som er trafikdata[3] ifm. telefoni- og sms/mms-kommunikation.
2. Lokaliseringsdata, som er trafikdata ifm. mobildata-kommunikation via 4G.
3. Lokaliseringsdata, som ikke er trafikdata - dvs data om tændte telefoner, der ikke anvendes aktivt.

Ad 1: Denne type lokaliseringsdata logges og opbevares i 1 år, jf. logningsreglerne.
Ad 2: Denne type lokaliseringsdata opbevares i kort tid til brug for fejlretning.
Ad 3: Denne type lokaliseringsdata opbevares i kort tid til brug for fejlretning.

Teleudbyderne har kun mulighed for at levere enten samlede dataudtræk, som omfatter alle ovennævnte typer af lokaliseringsdata (både nr. 1, nr. 2 og nr. 3 ovenfor), eller dataudtræk som kun omfatter loggede lokaliseringsdata (nr. 1 ovenfor). Førstnævnte samlede dataudtræk (både nr. 1, nr. 2 og nr. 3 ovenfor) stammer fra teleudbydernes måleudstyr til brug for fejlretning (også benævnt prober), som kun muliggør samlede dataudtræk. Sidstnævnte dataudtræk (nr. 1 ovenfor) stammer fra såkaldte CDR-data, som er overført til teleudbyderens særlige systemer til opbevaring af data i år, jf. kravet herom i logningsreglerne. For uddybning se pkt. 3.2 i TI's notat om teledata sendt til Justitsministeriet og Rigspolitiet den 28. februar 2020.

Teleudbyderne har derimod ikke mulighed for at levere udtræk, som kun omfatter lokaliseringsdata om mobiltelefoner, der er tændt, men som ikke anvendes aktivt som nævnt i pkt. 3 ovenfor (tidligere benævnt "signaleringsdata", jf. U.2017.1934Ø). Teleudbyderne har således ikke mulighed for at efterleve kendelser, der indeholder betegnelsen "signaleringsdata", idet levering af det samlede dataudtræk i så fald ville medføre, at teleudbyderen leverer udtræk til politiet, der omfatter mere data, end der er hjemmel til i kendelsen. Generelt opfordrer Teleindustrien derfor til, at begrebet "signaleringsdata" helt undgås. For uddybning se pkt. 2.1 i TI's notat om teledata sendt til Justitsministeriet og Rigspolitiet den 28. februar 2020.

Teleindustrien lægger til grund, at politiet efterforskningsmæssigt altid har brug for alle registrerede lokaliseringsdata om telefoner – både når telefoner bruges aktivt, og når telefoner ikke bruges aktivt. Ved at bruge betegnelserne, som angivet på side 1 i dette brev, ved anmodning om hastesikring og ved anmodning om edition vil alle sådanne registrerede lokaliseringsdata kunne sikres og udleveres.

---

[2] "Lokaliseringsdata" (masteoplysninger i form af Celle-ID) er defineret 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.

[3] "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)

Forbehold

For god ordens skyld bemærkes, at registrering af lokaliseringsdata i teleudbydernes måleudstyr til brug for fejlretning (også benævnt prober) kun kan ske efter "best effort", idet alle data kun opsamles, hvis kapaciteten i teleudbydernes opsamlingssystemer er tilstrækkelig. Teleudbyderne tilpasser løbende kapaciteten i probe-systemerne, for at sikre, at der er de nødvendige data til at foretage fejlretning. 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, som logges. 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[4].

Teleindustrien vil gerne fremhæve, at typen af data, registreringsmetoder og mængden af registrerede lokaliseringsdata kan variere fra teleselskab til teleselskab. Teleselskaberne anvender således ikke de samme systemer og tekniske set-up ifm registrering af lokaliseringsdata, og ensartet udlevering af registrerede lokaliseringsdata på tværs af teleselskaberne er derfor ikke muligt. Teleselskabernes levering af udtræk vil således være forskellige og særligt ift. registrerede lokaliseringsdata fra probe-systemer bemærkes, at der er tale om data i form af rå mastedata, som både registreres og udtrækkes forskelligt fra selskab til selskab. Dertil kommer, at der er manuelle processer forbundet med at udtrække data fra selskabernes systemer, og dette indebærer en risiko for fejl[5].

TI anmoder generelt om, at politiet afgrænser såvel fokusperiode som fokusområdet mest muligt – særligt ved udlevering af historiske lokaliseringsdata om, hvilke mobilterminaler, der har været registreret på bestemte master ("udvidet masteoplysning"). Oplysning om hvilke mobilterminaler, der har været registreret på bestemte master, kan således omfatte tusindvis af tilfældige personer – alt afhængig af fokusområdets størrelse (og dermed antallet af mulige master) og fokusperiodens længde. For at sikre, at et indgreb er proportionalt i forhold til, at politiet får adgang til data om andre personer end den mistænkte, opfordrer TI til, at politiets anmodninger om udlevering af lokaliseringsdata er nøje og præcist afgrænset mht. fokusområde og fokustidsrum, og at politiets anmodninger som udgangspunkt ikke overskrider 10 timer og én adresse.

[4] 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").
[5] Risikoen for fejl som følge af manuelle processer er nærmere beskrevet i Rigspolitiets notat vedrørende anvendelse af historiske teledata i straffesager ("Varedeklarationen").

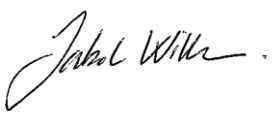
Regler om udlevering af teledata – Definition af nye tvangsindgreb

Teleindustrien finder det generelt uhensigtsmæssigt og bekymrende, at der ikke findes veldefinerede tvangsindgreb i retsplejeloven, der fastsætter de nærmere betingelser for politiets adgang til lokaliseringsdata. Lokaliseringsdata (masteoplysninger i form af celle-ID) er således fortrolige data om personers færden - både for så vidt angår lokaliseringsdata, der er omfattet af logningsreglerne og øvrige lokaliseringsdata. Bl.a. henset til EU-domstolens afgørelse i EU-dom om logning fra 2016 (C-203-15, Tele2-Watson) samt den mulige hensigt bag reglerne om "udvidet teleoplysning" finder TI det bekymrende, at udlevering af lokaliseringsdata sker alene efter reglerne om edition.

Teleindustrien opfordrer derfor til, at der snarest muligt fastsættes regler i retsplejelovens kapitel 71, der definerer følgende nye tvangsindgreb:
- Masteoplysning (vedr. udlevering af lokaliseringsdata om en bestemt mobiltelefon)
- Udvidet masteoplysning (vedr. oplysning om, hvilke mobiltelefoner, der har været registreret på en mast).

For nærmere uddybning af TI's bekymringspunker og forslag til nye tvangsindgreb se pkt. 4, 4.1 og 4.2 i Teleindustriens notat om teledata sendt til Rigspolitiet og Justitsministeriet af 28. februar 2020.

Med venlig hilsen



Jakob Willer, direktør, Teleindustrien