RIGSPOLITIET

POLITI

17. april 2020
J.nr.: 2020-033380

POLITIOMRÅDET

Redegørelse vedrørende politiets håndtering af signaleringsdata fra Telenor mv.

Indhold

1. Indledning

1.1. Justitsministeriets bestilling

Justitsministeriet har den 30. januar 2020 anmodet Rigspolitiet – efter behov med inddragelse af Rigsadvokaten – om at redegøre for politiets håndtering af en sag, hvor et teleselskab (Telenor) i forbindelse med kendelser om levering af signaleringsdata til politiet ved en fejl har videregivet oplysninger om SMS-indhold og B-numre.

Justitsministeriet har i den forbindelse anmodet myndighederne om at redegøre for, om politiet i andre tilfælde i forbindelse med kendelser om edition mere systematisk har modtaget oplysninger fra teleselskaber, som må anses for omfattet af reglerne om indgreb i meddelelseshemmeligheden.

1.2. Rigspolitiets og Rigsadvokatens konklusioner på baggrund af sagen

Sagen handler i sit udgangspunkt om, at en teleudbyder fejlagtigt har udleveret teleoplysninger til politiet, som ikke har været omfattet af de underliggende retskendelser. Oplysningerne har kun i begrænset omfang været læsbare for efterforskerne, og de har i vidt omfang været uden efterforskningsmæssig betydning.

Det er ikke ualmindeligt, at politiet i forbindelse med en efterforskning kommer i besiddelse af flere oplysninger, end der er relevant for den konkrete efterforskning, eller at oplysninger kan indgå i en efterforskning ved en fejl eller tilfældighed. Det kendes således fra en række andre områder. Politiet har dog omvendt et ansvar for som myndighed at reagere, hvis politiet bliver opmærksom på, at der på mere systematisk vis fejlagtigt indgår oplysninger i politiets efterforskning. Dette ansvar skærpes endvidere, når der er tale om oplysninger, som politiet almindeligvis kun har adgang til med retskendelse.

I den konkrete sag reagerede politiet og anklagemyndigheden, da man blev opmærksom på problemet. I første omgang var fokus imidlertid primært på at udvikle

en operativ løsning, og der gik derfor for lang tid, før Rigspolitiet rettede henvendelse til Telenor om problemet.

Som led i arbejdet med denne redegørelse er det afdækket, at også andre teleudbydere har udleveret flere oplysninger, end hvad der var omfattet af de konkrete retskendelser.

Det rejser en række spørgsmål i forhold til både teleloven og lovgivningen om databeskyttelse, at der fra teleudbydernes side er udleveret teleoplysninger til politiet, som ikke har været omfattet af de indhentede retskendelser. Disse spørgsmål – og de retssikkerhedsmæssige aspekter der kan være forbundet hermed – henhører imidlertid under de relevante ressortmyndigheder. Derimod er der ikke grundlag for at antage, at fejlagtigt udleverede oplysninger konkrete har været anvendt i straffesager på en måde, der giver anledning til retssikkerhedsmæssige betænkeligheder.

Fremadrettet er det vigtigt i samarbejde med telebranchen at få sikret, at der ikke videregives oplysninger fra teleudbyderne til politiet, som ikke må udleveres på en kendelse om edition. Det er herudover vigtigt at være opmærksom på, at det uanset iværksættelse af relevante tiltag til imødegåelse af uberettiget og/eller fejlagtige videregivelser er vanskeligt helt at gardere sig mod, at der kan opstå fejl i fremtiden.

Der er bl.a. i forlængelse af teledatasagen og denne sag dog iværksat en række tiltag, som efter Rigspolitiets og Rigsadvokatens opfattelse vil medvirke til at minimere denne risiko.

2. Lokaliseringsoplysninger og signaleringsdata

Allerede registrerede oplysninger om lokaliseringen af en tændt mobiltelefon er oplysninger om, hvilke telemaster en mobiltelefon er registreret på i et bestemt tidsrum. Disse oplysninger omhandler:

- lokaliseringsoplysninger hidrørende fra aktiv brug af telefonen til eksempelvis tale, sms og mms, som skal logges af teleudbyderne.
- lokaliseringsoplysninger hidrørende fra en tændt telefon, der ikke er i aktiv brug, men som kommunikerer sin position til mobilnetværket. Disse *skal* ikke logges af teleudbyderne, men *må* godt opbevares – i en begrænset periode – med henblik på eksempelvis fejlretning.

Allerede registrerede lokaliseringsoplysninger logges ikke i et ensartet format hos de enkelte teleudbydere, ligesom indholdet og detaljeringsgraden af oplysningerne er forskellig fra udbyder til udbyder.

Hvis politiet anmoder om udlevering af signaleringsdata, vil datasættene efter omstændighederne i praksis indeholde såvel oplysninger, der hidrører fra aktiv brug af telefonen, som oplysninger, der er genereret ved, at en tændt telefon kommunikerer sin position til mobilnetværket, jf. ovenfor. Det skyldes, at teleudbyderne ved deres registrering af disse oplysninger ikke skelner mellem aktiv og passiv kommunikation.

I det følgende anvendes betegnelsen ”signaleringsdata” som en generel betegnelse for de data, der er udleveret fra teleselskaberne på editionskendelse om udlevering af signaleringsdata. Som redegjort for i det følgende må ”signaleringsdata” dog ikke indeholde modpartsnumre, når udlevering til politiet alene er hjemlet ved en kendelse om edition.

2.1. Politiets anvendelse af signaleringsdata

Signaleringsdata er et relativt nyt efterforskningsmiddel, som må forventes at få stigende anvendelse fremadrettet, også fordi alle fire teleselskaber nu kan levere disse data. Signaleringsdata vil ofte have væsentlig værdi for politiets efterforskning af alvorlige strafbare forhold såsom manddrab, voldtægt mv., herunder til hurtigt at målrette efterforskningen mod en afgrænset personkreds og udelukke andre

fra efterforskningen. Endvidere kan signaleringsdata anvendes til at følge en mistænkts færden i et relevant tidsrum. Den efterforskningsmæssige merværdi af signaleringsdata set i forhold til andre tilgængelige oplysninger ligger i, at disse data (også) opsamles, selv om en person ikke anvender sin telefon til at foretage eller modtage opkald.

For nuværende er signaleringsdata fra nogle af teleselskaberne ikke umiddelbart læsbart, når politiet modtager data, og brugen heraf forudsætter derfor i visse tilfælde, at data bearbejdes af medarbejdere med særlige kompetencer.

2.2. Politiets rekvisition af signaleringsdata

Politikredsene indhenter typisk signaleringsdata via Rigspolitiets Telecenter ved fremsendelse af en anmodning til telecenteret med afgrænsning af et område eller med oplysning om et fokusnummer samt med oplysning om den relevante tidsperiode for dataudtrækket. Telecentret bestiller herefter data fra teleoperatøren. Indhentelse af signaleringsdata er et straffeprocessuelt tvangsindgreb, der er omfattet af retsplejelovens kapitel 74 om edition, og sker på baggrund af rettens kendelse eller på øjemedet efterfulgt af rettens kendelse, hvis det af efterforskningsmæssige grunde har været nødvendigt at iværksætte indgrebet straks.

Når telecentret modtager data fra teleoperatøren, videresender telecentret disse til politikredsen.

Telecentret foretager ingen behandling af de modtagne data.

Politikredsene kan også bestille signaleringsdata direkte hos teleudbyderen. Leverancen af signaleringsdata sker da typisk via telecentret, men det forekommer også, at data sendes direkte fra udbyderen til den rekvirerende politikreds.

Politikredsene afregner særskilt over for teleoperatørerne for hver rekvisition.

Teleudbyderne leverer signaleringsdata i forskellige formater. Data kan være opdelt i flere forskellige filer, ligesom der er forskel på det data, der leveres fra de forskellige teleudbydere. Politikredsene vil derfor som nævnt have behov for at oversætte og/eller strukturere data, før de kan anvendes i efterforskningen.

3. Det retlige grundlag

3.1. Oplysninger omfattet af indgreb i meddelelseshemmeligheden

Indgreb i meddelelseshemmeligheden er reguleret i retsplejelovens kapitel 71. Telefonaflytning er i § 780, stk. 1, nr. 1, defineret som at politiet kan aflytte telefonsamtaler eller anden tilsvarende telekommunikation. Endvidere er teleoplysning i § 780, stk. 1, nr. 3, defineret som oplysning om, hvilke telefoner eller andre tilsvarende kommunikationsapparater der sættes i forbindelse med en bestemt telefon eller andet kommunikationsapparat. Telefonaflytning omhandler indholdet af kommunikationen, mens teleoplysning omhandler oplysninger om, hvilke telefoner der sættes i forbindelse med andre bestemte telefoner.

Endelig er udvidet teleoplysning – også kaldet mastesug – i § 780, stk. 1, nr. 4, defineret som oplysning om, hvilke telefoner eller andre tilsvarende kommunikationsapparater inden for et nærmere angivet område, der sættes i forbindelse med andre telefoner eller kommunikationsapparater.

Fælles for disse indgreb i meddelelseshemmeligheden er, at der som udgangspunkt gælder et kriminalitetskrav på fængsel i 6 år eller derover, ligesom der er skærpede krav til indhentelse af udvidede teleoplysninger. Oplysningerne kan således ikke indhentes på en editionskendelse, jf. nedenfor.

3.2. Signaleringsdata mv.

Retsplejeloven indeholder ikke bestemmelser, der definerer allerede registrerede lokaliseringsoplysninger (herunder signaleringsdata), eller bestemmelser, der sær-

ligt regulerer politiets adgang til at indhente allerede registrerede lokaliseringsoplysninger. Den retlige ramme for indhentelse af disse oplysninger er derfor udviklet gennem retspraksis.

Det følger af Højesterets kendelse gengivet i UfR 2009.2610 H, at allerede registrerede lokaliseringsoplysninger fra en tændt mobiltelefon kan indhentes med hjemmel i retsplejelovens regler om edition, jf. § 806, stk. 2, jf. § 804, stk. 1. Det er i den forbindelse uden betydning, om lokaliseringsoplysningerne er blevet registreret i forbindelse med aktiv brug af en telefon, eller om de er genereret ved, at en tændt telefon (automatisk) har kommunikeret sin position til mobilnetværket. Herudover fremgår det af Østre Landsrets kendelse gengivet i UfR 2017.1934 Ø, at allerede registrerede lokaliseringsoplysninger tillige kan indhentes for masteceller, der dækker en bestemt adresse, dvs. alle de telefoner, som har kommunikeret med en bestemt mast.

Indhentelse af allerede registrerede lokaliseringsoplysninger kan på baggrund af retspraksis ske som led i efterforskningen af en lovovertrædelse, der er undergivet offentlig påtale, jf. retsplejelovens § 806, stk. 2, jf. § 804, stk. 1. Derfor kan allerede registrerede lokaliseringsoplysninger også indhentes til brug for sager, hvor strafferammen er under 6 års fængsel.

Allerede registrerede lokaliseringsoplysninger og signaleringsdata omfatter forskelligt indhold på tværs af teleselskaberne. Begreberne allerede registrerede lokaliseringsoplysninger og signaleringsdata kan derfor næppe forstås helt entydigt. Da indhentning af disse typer af oplysninger begge er omfattet af samme hjemmel, findes en indbyrdes afgrænsning også at være af mindre betydning ud fra et straffeprocessuelt perspektiv.

Derimod giver en kendelse om udlevering af allerede registrerede lokaliseringsoplysninger, herunder signaleringsdata, alene politiet adgang til at få udleveret oplysninger om en telefons placering, men ikke til oplysninger om, hvilke telefoner mv.

der har været sat i forbindelse med telefonen – dvs. modpartsnumre – eller indhold af kommunikationen. Sådanne oplysninger er omfattet af meddelelseshemmeligheden og kræver derfor kendelse efter retsplejelovens kapitel 71, jf. også retsplejelovens § 801, stk. 3.

3.3. Signaleringsdata mv., der fejlagtigt er fremsendt til politiet

3.3.1. Den retlige ramme for teleudbydernes udlevering

Det følger af telelovens § 7, stk. 1, at ejere af elektroniske kommunikationsnet og udbydere af elektroniske kommunikationsnet eller -tjenester og deres ansatte og tidligere ansatte ikke uberettiget må videregive eller udnytte oplysninger om andres brug af nettet eller tjenesten eller indholdet heraf, som de får kendskab til i forbindelse med det pågældende udbud af elektroniske kommunikationsnet eller -tjenester.

Bestemmelsen er strafbelagt, jf. telelovens § 81, stk. 1, nr. 1.

Det fremgår af de specielle bemærkninger til den daværende telekonkurrencelovs § 13[1], der efterfølgende er videreført i den gældende telelovs § 7, at telekonkurrencelovens § 13, stk. 1 og 2, rettede sig mod opretholdelsen af "fortroligheden med hensyn til den trafik, der foregår via de pågældende telenet og teletjenester"[2]. Herudover indeholder bemærkningerne ikke bidrag til fortolkningen af, hvad der er

[1] Forslag til lov om konkurrence- og forbrugerforhold på telemarkedet som fremsat den 30. marts 2000 af forskningsministeren, Folketingstidende 1999-00, Tillæg A, 6896ff, hvor det bl.a. anføres, at "*af den gældende bestemmelse i § 3, stk. 1, nr. 5, i lov om visse forhold på telekommunikationsområdet fremgår, at forskningsministeren kan fastsætte nærmere regler for udbud af telenet eller teletjenester, med sigte på at sikre hemmeligholdelse af telekommunikation. Med hjemmel heri er det i den gældende bekendtgørelse om udbud af telenet og teletjenester fastsat, at udbyderen af et telenet eller en teletjeneste og dennes ansatte ikke uberettiget må videregive eller udnytte oplysninger om andres brug af nettet eller tjenesten eller om indholdet heraf, som de får kendskab til i forbindelse med det pågældende udbud af telenet eller teletjenester.* [……]. *Den foreslåede bestemmelse er en lovfæstet videreførelse af den ovenfor beskrevne regulering med enkelte justeringer.*

[2] Telekonkurrencelovens § 13, stk. 3, retter sig mod forpligtelsen til at træffe de nødvendige foranstaltninger med henblik på at sikre, at oplysninger om andres brug af nettet eller tjenesten eller indholdet heraf ikke er tilgængelige for uvedkommende. Denne forpligtelse ses videreført i telelovens § 7, stk. 1, sidste pkt.

omfattet af betegnelsen ”oplysninger om andres brug af nettet eller tjenesten eller indholdet heraf”.

Ud fra bestemmelsens ordlyd må den dog anses for at omfatte oplysninger, der afdækker om f.eks. en tjeneste har været ”brugt” af en slutbruger og dermed også den umiddelbare oplysning om, hvorvidt andre (i praksis en slutbruger) har etableret adgang til et net eller tjeneste. For så vidt angår fortolkningen af begrebet ”oplysninger om indholdet heraf” må bestemmelsen anses for at beskytte oplysninger, der afdækker det egentlige indhold, der har været kommunikeret som led i en slutbrugers anvendelse af et net eller en tjeneste.

Bestemmelsen i telelovens § 7 implementerer artikel 5 om kommunikationshemmelighed i direktivet om databeskyttelse inden for elektronisk kommunikation[3]. Efter denne bestemmelse kan medlemsstaterne tillade indskrænkninger i kommunikationshemmeligheden i overensstemmelse med direktivets artikel 15, stk. 1. Artikel 15, stk. 1, tillader bl.a. indskrænkninger, der er nødvendige, passende og forholdsmæssige i et demokratisk samfund af hensyn til forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager. Retsplejelovens bestemmelser om indgreb i meddelelseshemmeligheden og edition udgør sådanne indskrænkninger. Enhver behandling – og hermed også videregivelse – af personoplysninger skal dog finde sted i overensstemmelse med de generelle databeskyttelsesretlige principper fastsat i databeskyttelsesforordningens artikel 5.

Oplysninger, der må anses for omfattet af begreberne ”andres brug af elektroniske kommunikationsnet og –tjenester eller indholdet heraf”, er således som udgangspunkt tavshedsbelagte, hvilket skal ses i sammenhæng med retten til kommunikationshemmelighed.

[3] Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor.

Afgørende for, om en videregivelse af oplysninger omfattet af telelovens § 7, stk. 1, sker i overensstemmelse med bestemmelsen, er, om videregivelsen i den konkrete situation må betragtes som *berettiget*. En videregivelse må eksempelvis betragtes som berettiget, når den sker på baggrund af en kendelse efter retsplejelovens regler[4], f.eks. en kendelse om indgreb i meddelelseshemmeligheden eller edition.

Kendelsen – og det regelgrundlag, den er afsagt efter – udgør derved en konkret angivelse af, hvad der efter telelovens § 7, stk. 1, kan anses som en berettiget videregivelse af oplysninger om andres brug af elektroniske kommunikationsnet- og tjenester eller indholdet heraf. Modsætningsvist følger det, at en videregivelse af oplysninger, der omfatter andre oplysninger end fastsat i den givne kendelse, vil være uberettiget – medmindre, der kan peges på et andet retligt grundlag, som gør videregivelsen berettiget.

Er grundlaget for en konkret videregivelse et pålæg om edition, så medfører dette– foruden at gøre den konkrete videregivelse berettiget – at adressaten undergives en aktiv og domstolsbestemt[5] handlepligt til at fremkomme med de oplysninger, som pålægget omhandler.

Som nævnt skal den dataansvarlige teleudbyder altid iagttage de almindelige principper for behandling af personoplysninger i databeskyttelsesordningens[6] artikel 5, stk. 1, litra a – f. Ét af disse er dataminimeringsprincippet, jf. artikel 5, stk. 1, litra c,[7] hvorefter personoplysninger skal begrænses til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles.

---

[4] Se i den forbindelse Lasse Lund Madsen, Edition som efterforskningsmiddel, U.2017B.205, afsnit 4, for så vidt angår kendelser om edition.
[5] Herved adskiller pålæg om edition sig fra reglerne om indgreb i meddelelseshemmeligheden, hvor teleudbyderne er undergivet en lovgiverbestemt forpligtelse til at bistå politiet ved gennemførelsen af indgreb i meddelelseshemmeligheden, jf. retsplejelovens § 786, stk. 1.
[6] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse).
[7] Jf. bl.a. Datatilsynets afgørelse offentliggjort 11. februar 2019 om en teleudbyders efterlevelse af databeskyttelsesforordningens artikel 5, stk. 1, litra c (j.nr. 2018-31-0070).

3.3.1.1. Underretning om brud på persondatasikkerheden

Teleudbyderes underretning ved brud på persondatasikkerheden er reguleret i Kommissionens forordning (EU) nr. 611/2013 af 24. juni 2013 om de foranstaltninger, der skal anvendes ved underretningen om brud på persondatasikkerheden, jf. Europa-Parlamentets og Rådets direktiv 2002/58/EF vedrørende databeskyttelse inden for elektronisk kommunikation.

I medfør af forordningens artikel 2, stk. 1, skal udbyderen således underrette den kompetente nationale myndighed om samtlige brud på persondatasikkerheden. Den kompetente nationale myndighed er i denne sammenhæng Erhvervsstyrelsen. Hvis bruddet på persondatasikkerheden kan forventes at krænke personoplysninger eller privatlivets fred for en abonnent eller en fysisk person, skal udbyderen foruden den underretning, der er nævnt i artikel 2, også underrette abonnenten eller den fysiske person om bruddet, jf. artikel 3, stk. 1.

Ved brud på persondatasikkerheden forstås "et sikkerhedsbrud, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, ubeføjet videregivelse af eller adgang til persondata, der sendes, lagres eller på anden måde behandles i forbindelse med udbuddet af offentligt tilgængelige kommunikationstjenester i Fællesskabet.", jf. artikel 2, litra i, i direktivet om databeskyttelse inden for elektronisk kommunikation.

3.3.2. Regulering i forhold til straffesagen

Som nævnt i afsnit 3.2. giver en kendelse om udlevering af allerede registrerede lokaliseringsoplysninger (herunder signaleringsdata) alene politiet adgang til at få udleveret oplysninger om en telefons placering, men ikke til oplysninger om, hvilke telefoner mv. der har været sat i forbindelse med telefonen – dvs. modpartsnumre, eller indhold af kommunikationen. Sådanne oplysninger er omfattet af meddelelseshemmeligheden og kræver derfor kendelse efter retsplejelovens kapitel 71.

Retsplejelovens regler om tvangsindgreb indeholder ikke bestemmelser, der særligt regulerer det tilfælde, hvor en teleudbyder videregiver flere oplysninger til politiet, end en kendelse om edition omfatter. Spørgsmålet er herefter, hvilken praksis der gælder i relation til straffesagen, hvis en teleudbyder alligevel videregiver oplysningerne til politiet.

Retsplejeloven indeholder ikke en generel regel om bevisførelsen inden for strafferetsplejen, men den materielle sandheds princip og princippet om den fri bevisbedømmelse, jf. retsplejelovens § 880, 2. pkt., spiller en central rolle ved behandlingen af straffesager. Herudover regulerer retsplejelovens § 789 såkaldte tilfældighedsfund ved indgreb i meddelelseshemmeligheden og § 800 tilfældighedsfund i forbindelse med politiets ransagning, ligesom § 791, stk. 3, regulerer destruktion af materiale fra indgreb i meddelelseshemmeligheden hidrørende fra den mistænktes forbindelse med personer, som efter reglerne i retsplejelovens § 170 er udelukket fra at afgive forklaring som vidne. Endelig er der i retspraksis taget konkret stilling til anvendelse af beviser, som er ulovligt tilvejebragt.

Det er ikke ualmindeligt, at politiet i forbindelse med en efterforskning kommer i besiddelse af flere oplysninger, end der er relevant for den konkrete efterforskning, eller at sådanne oplysninger kan indgå i en efterforskning ved en fejl eller tilfældighed. I nogle tilfælde får politiet f.eks. i forbindelse med et tvangsindgreb kendskab til oplysninger om lovovertrædelser, der ikke dannede eller kunne danne baggrund for indgrebet. Det kan f.eks. være tilfældet, hvis politiet under en aflytning får kendskab til en lovovertrædelse, som ikke lever op til strafferammekravet i § 781. Disse såkaldte tilfældighedsfund er reguleret i retsplejelovens § 789 og § 800.

Tilfældighedsfund kan anvendes som led i politiets videre efterforskning af den pågældende lovovertrædelse, jf. retsplejelovens § 789, stk. 1. De kan imidlertid ikke anvendes som bevis i retten, medmindre retten tillader det, jf. retsplejelovens § 789, stk. 3, og § 800, stk. 2.

Ønsker anklagemyndigheden at anvende et tilfældighedsfund som bevis, medtages det i bevisfortegnelsen under udtrykkelig angivelse af, at der er tale om et tilfældighedsfund. Herefter har forsvareren mulighed for at begære spørgsmålet forelagt for retten til afgørelse efter princippet i § 841, stk. 1, inden hovedforhandlingen.

Er der udover tilfældighedsfundet tillige tilvejebragt beviser for den oprindeligt angivne kriminalitet, der dannede grundlag for indgrebet, vil det normalt være ubetænkeligt at tillade anvendelsen af tilfældighedsfund som bevis. Se f.eks. Michael Kistrup m.fl., Straffeprocessen, 3. udgave.

Selvom reglerne om tilfældighedsfund ikke finder direkte anvendelse på den foreliggende situation, hvor en teleudbyder udleverer flere oplysninger til politiet, end der er omfattet af de kendelser, anklagemyndigheden har indhentet på vegne af politiet, bør samme fremgangsmåde som udgangspunkt følges, herunder for at sikre fuld transparens for rettens aktører.

Anklagemyndigheden bør derfor – i det omfang oplysningerne er læsbare og indgået i sagen – sikre, at oplysningernes tilvejebringelse tydeligt fremgår af sagen. På den måde sikres det, at forsvareren har adgang til alt materiale af relevans for sagen, jf. retsplejelovens § 729 a, stk. 3, og at retten – ud fra principperne om den materielle sandhed og den fri bevisbedømmelse – har mulighed for at tage stilling til oplysningernes eventuelle bevismæssige betydning.

I det omfang oplysningerne indgår i sagen, er de omfattet af de almindelige regler for straffesagers behandling, herunder reglerne for arkivering, destruktion mv.

4. Det tidsmæssige forløb og underretning af berørte registrerede

4.1. Det tidsmæssige forløb

Sagen, der gav anledning til nærværende redegørelse, vedrører signaleringsdata, der er videregivet til politiet fra Telenor.

4.1.1. september 2018 – april 2019

Politiet har haft mulighed for at rekvirere signaleringsdata fra Telenor siden september 2018, hvor Københavns Politi første gang modtog signaleringsdata fra Telenor. Signaleringsdata blev leveret i binære PCAP datafiler. Det vil sige, at data var i binær kode, som ikke kunne læses, medmindre data blev oversat maskinelt, da binær kode alene består af 1-taller og 0' er

Ifølge de foreliggende oplysninger modtog Københavns Politi, Afdelingen for efterforskningsstøtte – i en anden sag end den ovennævnte – signaleringsdata fra Telenor medio november 2018. For at læse data blev disse gjort læsbare med hjælp af et open source værktøj. Dermed kunne data læses, men det var delt på mange forskellige filer, og det var ikke muligt at få et systematisk overblik over data i et samlet billede. I forbindelse med arbejdet med at udfinde de relevante data som målpersonens telefonnummer, tid og sted blev man i december 2018 opmærksom på, at der i datafilerne fandtes såkaldte modpartsnumre (hvilket omfatter – men ikke er tilsvarende med – såkaldte B-numre), som er telefonnumre, som de omhandlede telefoner har haft kontakt med, ligesom der i enkelte tilfælde også var SMS-indhold. Såvel Rigspolitiet som den lokale anklagemyndighed blev informeret om dette af medarbejdere i Afdelingen for efterforskningsstøtte i december 2018, og anklagemyndigheden i Københavns Politi gjorde opmærksom på, at politiet ikke måtte hverken tilgå eller anvende disse oplysninger i sagsbehandlingen.

Da data, selv om det blev gjort læsbart, var meget vanskelig at få overblik over og anvende i praksis, besluttede Københavns Politi at udvikle et værktøj, der kunne oversætte og strukturere data fra Telenor til et format, som kunne anvendes i efterforskningen. I løbet af de første måneder af 2019 arbejdede politikredsen på udviklingen af dette værktøj. Til brug for dette modtog Københavns Politi signaleringsdatasæt, som andre politikredse havde indhentet fra Telenor. Københavns Politi konstaterede i den forbindelse, at der ikke var SMS-indhold i alle de datasæt, som blev modtaget fra andre politikredse, idet SMS-indhold øjensynligt var isoleret til en bestemt protokol, som ikke altid blev udleveret som en del af datasættet.

Rigspolitiet kontaktede primo marts 2019 Rigsadvokaten om problemstillingen. Det blev i den forbindelse aftalt, at Rigspolitiet skulle rette henvendelse til Telenor og underrette dem om, at selskabet i nogle tilfælde havde fremsendt indholdsdata på baggrund af en editionskendelse, og samtidig anmode Telenor om, at dette ikke skete fremover.

I lyset af de oplysninger, som Rigspolitiet modtog fra Københavns Politi i forbindelse med deres arbejde med signaleringsdata fra Telenor, kontaktede Rigspolitiet den 27. marts 2019 Telenors politigruppe[8]. Telenor blev gjort bekendt med, at det leverede signaleringsdata indeholdt mere data end omfattet af editionskendelserne, herunder at der var konstateret indholdsdata i det modtagne materiale. Idet Københavns Politi havde konstateret, at der var forskelligt indhold i datasættene fra Telenor, blev det ved henvendelsen endvidere drøftet, hvordan disse datasæt blev genereret af Telenor.

Ud fra de oplysninger Telenor har afgivet, undersøgte selskabet i den forbindelse deres systemer, men fandt ingen tegn på, at disse indeholdt mere information, end politiet havde anmodet om. Telenor har efterfølgende oplyst, at selskabet meddelte dette til Rigspolitiet, ligesom selskabet anmodede om at modtage den information, som selskabet fejlagtigt skulle have sendt, men at selskabet ikke på daværende tidspunkt hørte mere fra politiet.

Rigspolitiet har ikke kunnet identificere nogen henvendelser fra Telenor, men kan ikke udelukke, at dette har fundet sted.

Oversættelsesværktøjet var færdigudviklet primo april 2019 og blev gjort tilgængeligt for alle politikredsene i den første version den 3. april 2019. I denne version

[8] "Politigruppe" anvendes som betegnelse for de medarbejdere, der forestår kontakten til politiet i forbindelse med indgreb i meddelelseshemmeligheden.

blev eventuel SMS-indhold i datasættet fra Telenor ikke vist i de læsbare data. I en senere version af oversættelsesværktøjet, som blev udsendt den 3. juli 2019, blev også oplysninger om modpartsnumre frasorteret i de læsbare data.

Det bemærkes, at Rigspolitiet den 5. februar 2020 afholdt et ITV-møde med lederne af kredsenes it-efterforskere og NC3 forposter[9] med henblik på at afdække, hvordan kredsene har behandlet signaleringsdata fra Telenor. Politikredsene og efterforskningsfællesskaberne oplyste, at de, siden oversættelsesværktøjet udviklet af Københavns Politi blev gjort tilgængeligt for kredsene, har anvendt dette værktøj til oversættelse af signaleringsdata fra Telenor. Enkelte politikredse havde i tiden forud herfor i enkelte sager anvendt andre værktøjer til læsning af data, men ved anvendelse af disse værktøjer var det ikke muligt at få et systematisk overblik over data.

4.1.2. maj 2019 – juli 2019

Rigspolitiet konstaterede ultimo maj 2019, at signaleringsdata fra Telenor fortsat indeholdt modpartsnumre og i visse tilfælde endvidere SMS-indhold, hvorfor det på et møde den 28. maj 2019 mellem Rigspolitiet og Rigsadvokaten blev aftalt, i) at Telenor på direktionsniveau skulle orienteres om problemstillingen og med henblik på, at fejlen blev rettet, ii) at det skulle sikres, at værktøjet, som Københavns Politi havde, udviklet effektivt "spærrede" for de oplysninger, som ikke var omfattet af kendelsen, og iii) at indhentning af signaleringsdata fortsat burde ske i form af editionskendelse.

Samme dag rettede Rigspolitiet telefonisk henvendelse til Telenors juridiske direktør og oplyste, at signaleringsdata i visse tilfælde indeholdt oplysninger om b-numre og egentlig indholdsdata (SMS-indhold). Det blev i den forbindelse oplyst, at Rigspolitiet den 27. marts 2019 orienterede Telenors politigruppe om ovenstående og drøftede de mulige årsager hertil. Det blev ved henvendelsen understreget over for

[9] IT-ingeniører, der organisatorisk er tilknyttet National Cybercrime Center, men som er stationeret i hver politikreds

Telenor, at Rigspolitiet så med stor alvor på sagen, og at Rigspolitiet ønskede problemstillingen adresseret fra Telenors side. Det blev samtidig bemærket, at det var vigtigt for politiet, at Telenor vedblev med at kunne udlevere de oplysninger, som politiet i overensstemmelse med gældende ret anmoder om at modtage.

Rigspolitiet orienterede den 29. maj 2019 telefonisk Telenors politigruppe om henvendelsen til selskabets juridiske direktør. Repræsentanten fra Telenors politigruppe oplyste i den forbindelse, at man både i forbindelse med Rigspolitiets henvendelse den 27. marts 2019 og i forbindelse med Rigspolitiets henvendelse af 28. maj 2019 havde undersøgt signaleringsdata, som Telenor havde sendt til politiet. Man havde ved de undersøgelser ikke kunnet konstatere tilfælde, hvor indholdsdata (SMS-indhold) var fremsendt til politiet, hvorfor Telenor gerne modtog eksempler på dette.

Det blev endvidere oplyst, at Telenor efter fast praksis slettede de datasæt, der blev udleveret til politiet efter afsendelsen, og at Telenor derfor ikke efterfølgende var i stand til at fastlægge hvilke oplysninger, der var blevet udleveret.

Telenor anførte samme forhold i en e-mail af 29. maj 2019 til Rigspolitiet og anmodede om at modtage et eksempel på signaleringsdata, som Telenor havde fremsendt til politiet. Telenor oplyste endvidere, at selskabet – både ved Rigspolitiets henvendelse i marts 2019 og henvendelse den 28. maj – havde undersøgt deres systemer. Selskabet fandt dog ikke tegn på, at der i de fremsendte datasæt var oplysninger om indhold af kommunikation, ligesom Telenor ved forskellige test ikke kunne konstatere, at der fremgik indholdsoplysninger i deres system.

Rigspolitiet iværksatte på den baggrund fremsøgningen af et sæt signaleringsdata modtaget fra Telenor med henblik på at kunne fremsende det til selskabet. Den 6. juni 2019 fremsendte Rigspolitiet herefter et eksempel på SMS-indhold, som var leveret i signaleringsdata til Københavns Politi i maj 2019. Ved fremsendelsen be-

mærkede Rigspolitiet over for Telenor, at Københavns Politi havde oplyst, at modpartens nummer altid er synligt for kald og SMS uafhængigt af den benyttede protokol.

Rigspolitiet anmodede i den forbindelse ved e-mail af samme dato om at blive orienteret, såfremt Telenor måtte konkludere, at der forelå et eller flere brud på persondatasikkerheden, som Telenor efter gældende ret havde pligt til at indberette til den relevante tilsynsmyndighed.

Telenor svarede ved e-mail af 7. juni 2019, at selskabet måtte konstatere, at eksemplet indeholdt SMS-indhold, og at man nu havde fundet fejlen i systemet. Telenor anførte i den forbindelse, at man havde iværksat udbedring af fejlen hurtigst muligt, og at man ville indberette forholdet til Erhvervsstyrelsen som et brud på persondatasikkerheden.

Rigspolitiet lagde på denne baggrund til grund, at forholdet knyttet til såvel udlevering af SMS-indhold som modpartsnumre ville blive løst af Telenor. Som beskrevet nedenfor blev Rigspolitiet først efterfølgende bekendt med, at Telenor ikke på dette tidspunkt havde fundet grundlag for at adressere problemstillingen knyttet til udlevering af modpartsnumre.

Det bemærkes, at Rigspolitiet som led i den e-mail korrespondance, der beskrives nedenfor under afsnit 4.2, ved e-mail af 30. januar 2020 anførte, at Rigspolitiet havde konstateret, at Telenor på dette tidspunkt regelmæssigt fortsat fremsendte signaleringsdata til politiet, der indeholdt oplysninger om B-numre. Rigspolitiet opfordrede derfor på ny Telenor til at søge dette forhold afhjulpet snarest muligt.

I perioden ultimo maj til medio juni 2019 var der løbende dialog mellem Rigspolitiet og Rigsadvokaten for at få afklaret, om SMS-indhold og modpartsnumrene var tilgængelige for politikredsene og indgik i straffesagerne, og om der var behov for udfærdigelse af retningslinjer i den anledning.

Som led i disse drøftelser fremsendte Rigspolitiet den 12. juni 2019 et notat til Rigsadvokaten, der beskrev Rigspolitiets kommunikation med flere politikredse og efterforskningsfællesskaberne Særlig Efterforskning Vest og Særlig Efterforskning Øst. Af notatet fremgik det bl.a., at der den 3. april 2019 blev uploadet et konverteringsprogram på teledata ERFA netværket[10], hvorefter samtlige teledataanalytikere havde adgang til at konvertere signaleringsdata fra Telenor til et læsbart excel-format. Det uploadede konverteringsprogram eksponerede imidlertid ikke eventuelt SMS-indhold.

Den 17. juni 2019 oplyste Rigspolitiet over for Rigsadvokaten, at Telenor havde rettet deres procedurer/software til, så der fremadrettet ikke ville indgå indhold eller modpartsnumre i materiale, som er rekvireret på baggrund af editionskendelser om signaleringsdata. Da problemstillingen var historisk, og da man på daværende tidspunkt vurderede, at der var tale om relativt få sager, vurderede Rigsadvokaten, at der ikke var grundlag for at udstede generelle retningslinjer, men at legalitetssikringen burde foretages af de lokale anklagemyndigheder i de enkelte sager.

Fejlen vedrørende SMS-indhold blev ud fra de foreliggende oplysninger først endeligt udbedret fra Telenors side den 20. juni 2019, således at politiet ikke længere modtog oplysninger herom.

4.1.3. august 2019 – december 2019

Den 2. august 2019 konstaterede Rigspolitiet, at signaleringsdata fra Telenor fortsat indeholdt oplysninger om modpartsnumre. Telenors politigruppe blev orienteret herom den 6. august 2019, og der blev på ny taget telefonisk kontakt herom til Telenors juridiske direktør, der blev anmodet om at søge forholdet løst. Telenor bemærkede i den forbindelse, at man gerne så, at politiet præciserede editionskendelserne, så det var mere entydigt, hvilke oplysninger de omfattede. Hertil bemærkede

[10] En fælles informationsplatform for teledataeksperter og sagsbehandlere i politiet.

Rigspolitiet, at det ikke virkede som en egnet løsning, idet dette bl.a. forudsatte, at Rigspolitiet udtømmende skulle opregne hvilke datafelter en given teleudbyder skulle udtrække fra netop dennes system. Endvidere tilkendegav Rigspolitiet, at spørgsmålet om, hvilke oplysninger der er omfattet af en editionskendelse, skulle søges afklaret på baggrund af retsplejelovens bestemmelser.

Ved e-mail af 8. august 2019 forespurgte Telenor, om man fra politiets side kunne præcisere, hvilken information, politiet har brug for, når politiet anmoder om "signaleringsdata". Telenor anførte bl.a. følgende i e-mailen:

> *"Desuden vil* [Telenor] *bede politiet sørge for en præcisering i de kendelser, som Telenor modtager fremover, således at kendelserne lyder på netop den data, som I har behov for (og grundlag for at indhente)."*
>
> *Således har vi fra Telenors side ikke lige nu en holdbar løsning og ej heller en hurtig løsning på at udlevere den fulde mængde signaleringsdata uden oplysninger om den modtagende eller afsendende part – og ud fra et juridisk synspunkt mener vi også at vi udleverer det, som vi får kendelser på – nemlig (al vores) signaleringsdata."*

Ved samme e-mail tilkendegav Telenor, at selskabet forstod problemstillingen med hensyn til oplysninger om den part, som havde været sat i forbindelse med personens telefon (dvs. den modtagende eller afsendende part, som ikke selv nødvendigvis har befundet sig i det pågældende område). Telenor anførte i den forbindelse følgende:

> *"Vi er enige i, at udlevering af denne information alene kan udleveres efter reglerne i Retsplejelovens kapitel 71 om indgreb i meddelelseshemmeligheden, hvilket også forudsætter en kendelse, om end kravene til at få en sådan kendelse er anderledes."*

I forlængelse heraf anførte Telenor, at denne information om modtagende/afsendende part er en dybt integreret del af signaleringsdata, som Telenor anvender til fejlretning i netværket, og at en anonymisering eller sletning af disse oplysninger vil være en meget omfattende opgave, som enten vil kræve systemudvikling for at lave en teknisk løsning eller et stort antal mandetimer for at lave en manuel anonymisering/sletning.

Rigspolitiet orienterede den 16. august 2019 Rigsadvokaten om Telenors anmodning og gjorde i den forbindelse opmærksom på, at håndteringen af problemstillingen burde afklares sammen med Rigsadvokaten. Samme dag bekræftede Rigspolitiet over for Telenor modtagelsen af anmodningen og anførte i den forbindelse, at Rigspolitiet i samarbejde med Rigsadvokaten ville afklare, hvordan problemstillingen mest hensigtsmæssigt håndteres og vende tilbage, så snart det var muligt.

Rigspolitiet lagde på baggrund af korrespondancen med Telenor umiddelbart til grund, at Telenor havde vurderet spørgsmålet nærmere og fundet, at selskabets *udlevering* af oplysninger om modpartsnumre kunne finde sted efter de retlige rammer, som Telenor er underlagt, uanset om politiet havde adgang til at *indhente* disse, jf. også afsnit 4.1.4. nedenfor.

I perioden fra primo til ultimo august 2019 var der løbende dialog mellem Rigspolitiet og Rigsadvokaten, idet politikredsene fortsat modtog oplysninger om modpartsnumre ved indhentelse af signaleringsdata fra Telenor.

Som led i heri rettede Rigspolitiet den 27. august 2019 henvendelse til Rigsadvokaten med henblik på fornyede drøftelser af behovet for udfærdigelse af de påtænkte retningslinjer.

Rigsadvokaten og Rigspolitiet drøftede i dagene herefter håndteringen af Telenors henvendelse. Der var både politiets og anklagemyndighedens opfattelse, at Telenor

var forpligtet til at sikre korrekt efterlevelse af en retskendelse om "signaleringsdata" uden en nærmere specificering af dataindholdet i kendelsen, ligesom udbyderen var forpligtet til at sikre, at den udleverede signaleringsdata ikke indeholdt teleoplysninger, hvis indhentning kræver kendelse om indgreb i meddelelseshemmeligheden, jf. retsplejelovens kapitel 71. Endelig var der enighed om, at der allerede i den eksisterende ordning er indbygget en proportionalitetsvurdering, som påses af domstolene.

Rigspolitiet oplyste samtidig, at da spørgsmålet om, hvad der udgør "signaleringsdata", bør ses som et spørgsmål, der berører alle de teleudbydere, der indsamler disse data, bør spørgsmålet med fordel drøftes med alle de relevante teleudbyderene i fællesskab. Rigspolitiet fandt på den baggrund – og da der var etableret en teknisk løsning, der udeholdt modpartsnumre fra sagsbehandlingen – at emnet burde sættes på dagsordenen for et kommende møde med repræsentanter fra telebranchen.

Spørgsmålet om fortolkning af begrebet "signaleringsdata" har efterfølgende været genstand for såvel korrespondance og telefoniske drøftelser mellem Rigspolitiet, Rigsadvokaten og enkelte teleudbydere, jf. for Telenors vedkommende det under afsnit 4.1.4. nævnte brev af 7. februar 2020 Emnet blev endvidere drøftet på mødet i den juridiske arbejdsgruppe under Rigspolitiets Telebrancheforum den 9. marts 2020.

4.1.4. januar 2020 – nu

På baggrund af medieomtale af sagen i januar måned 2020 rettede Erhvervsstyrelsen som kompetent tilsynsmyndighed på teleområdet henvendelse til Telenor og anmodede om en redegørelse om forholdene knyttet til Telenors videregivelse af b-numre[11] til politiet.

[11] "B-numre"-ses i denne sammenhæng at blive benyttet som en alternativ betegnelse for modpartsnumre, som er oplysninger, om hvilke telefoner eller andre tilsvarende kommunikationsapparater, som en bestemt telefon eller andet kommunikationsapparat har været sat i forbindelse med.

Til brug for Erhvervsstyrelsens oplysning af sagen anførte Telenor ved e-mail af 29. januar 2020, at selskabet ikke mente, at der var tale om brud på persondatasikkerheden, når Telenor havde overført information om B-nummer som del af signaleringsdata, og at Telenor således ikke mente uretmæssigt at have oversendt personoplysninger til Rigspolitiet.

Telenor anførte endvidere, at da man havde udleveret det, som kendelserne har lydt på indtil videre, har man ikke betragtet forholdet som et brud, og af denne årsag havde man ikke underrettet Erhvervsstyrelsen.

Telenor afgav den 4. februar 2020 en supplerende redegørelse til Erhvervsstyrelsen. Telenor har i den forbindelse anført, at der i den konkrete sag ikke var tale om et sikkerhedsbrud, idet det ikke var en utilsigtet hændelse, der havde ført til videregivelse af oplysninger. Endvidere har Telenor anført, at baggrunden for Telenors udlevering af data har været, at Telenor var blevet forelagt dommerkendelser om udlevering af signaleringsdata, og at Telenor derfor havde vurderet at være retligt forpligtet til at udlevere de pågældende oplysninger til politiet i overensstemmelse med ordlyden af kendelserne.

I den supplerende redegørelse har Telenor nærmere anført følgende:

> *"Efter en fornyet vurdering er Telenor imidlertid blevet opmærksom på, at der muligvis har været tale om en overfortolkning af forpligtelsen til at udlevere data fra vores side."*

Hvis det på dækningsområdet for en telemast bliver registreret, at en bestemt telefon har påbegyndt et opkald, vil denne telefon i forhold til den konkrete kommunikation være A-nummeret, mens den modtagende telefon vil være B-nummeret. B-nummeret vil i den konkrete kommunikation således være modpartsnummeret.

I forlængelse heraf har Telenor anført, at det er selskabets klare opfattelse, at Telenor har været i god tro omkring udleveringen af oplysningerne, som Telenor begyndte at udlevere i form af signaleringsdata i september 2018.

Samtidig har Telenor anført følgende:

> *"Henset til sagens udvikling og Telenors fornyede vurdering har vi imidlertid nu set os nødsaget til at begrænse de datasæt, som vi leverer til politiet efter editionskendelse."*

Ved e-mails af 31. januar 2020 og 6. februar 2020 anmodede Erhvervsstyrelsen om Rigspolitiets bemærkninger til de ovenfor omtalte redegørelser fra Telenor til Erhvervsstyrelsen omkring videregivelsen af modpartsnumre.

Telenor anmodede ved brev af 7. februar 2020 om, at politi og anklagemyndighed fremover undgik at benytte både begrebet "signaleringsdata" og begrebet "ikke-logningspligtige lokaliseringsdata", men i stedet benyttede begreberne – både ved hastesikring og edition – a) "oplysning om registrerede lokaliseringsdata for [fokusnummer] i [tidsrum]" og b) "registrerede lokaliseringsdata om, hvilke mobiltelefoner eller andre tilsvarende mobile kommunikationsapparater, der er registreret anvendt på mobilmaster, der dækker [fokusområde] i [tidsrum]".

Telenor angav i den forbindelse, at hvis andre begreber end ovennævnte a) og b) anvendtes, og disse begreber ikke var entydige, tog man forbehold for, at begæringen om udlevering af data måtte afvises. Disse forhold har efterfølgende indgået i den samlede dialog med telebranchen om afklaring af terminologien vedrørende signaleringsdata mv., jf. afsnit 6.4. nedenfor.

Som baggrund for anmodningen henviste Telenor til, at selskabet kun havde mulighed for at levere udtræk, som omfatter alle typer lokaliseringsdata, eller udtræk, som kun omfatter logningspligtige lokaliseringsdata. Endvidere henvistes der til, at

ingen af de hidtidige anvendte begreber efter Telenors opfattelse var entydige, hvorfor det for Telenor var uklart, hvad selskabet ved kendelsen eller anmodningen skulle hastesikre og/eller udlevere til politiet, og at selskabet derfor ikke var sikker på at have den nødvendige behandlingshjemmel til at hastesikre og/eller udlevere data til politiet.

Rigspolitiet afgav den 26. februar 2020 – efter høring af Rigsadvokaten – sine bemærkninger til Erhvervsstyrelsen.

Rigspolitiet anførte bl.a., at efter Rigspolitiets opfattelse skal spørgsmålet om hvilke oplysninger en teleudbyder er forpligtet til at – og dermed entydigt må – udlevere på baggrund af en kendelse, afgøres ud fra en fortolkning af ordlyden af den bestemmelse i retsplejeloven, der hjemler kendelsen og relevant retspraksis mv., og ikke ud fra overvejelser knyttet til, hvordan én eller flere teleudbydere vælger at definere begrebet signaleringsdata som led i udbyderens virksomhed.

På denne baggrund og på baggrund af den retspraksis, der også er gengivet ovenfor under afsnit 3.2., kunne Rigspolitiet tilslutte sig Telenors supplerende redegørelse af 4. februar 2020, hvor Telenor bl.a. anfører, at man i den foreliggende sag muligvis har overfortolket forpligtelsen til at udlevere data til politiet.

Endvidere anførte Rigspolitiet, at den enkelte teleudbyder må anses for at have en selvstændig forpligtelse til at sikre, at alene de oplysninger, der er omfattet af editionskendelse udleveres på baggrund af en sådan kendelse, men at det på den anden side påhviler anklagemyndigheden i relevant og passende omfang at vejlede teleudbyderen om indholdet af retsplejeloven og den pågældende kendelse.

Erhvervsstyrelsen har på nuværende tidspunkt endnu ikke truffet afgørelse om styrelsens vurdering af de forhold, der behandles i de ovennævnte redegørelser fra Telenor.

4.1.4.1. Status i forhold til modtagelse af signaleringsdata

Telenor begyndte i primo februar 2020 at fremsende signaleringsdata i et nyt format, som ikke indeholder oplysninger om modpartsnumre, og som ikke kræver anvendelse af oversættelsesværktøjet for at gøre data læsbart.

Rigspolitiet har indledt dialog med Telenor om det nærmere indhold af oplysninger i det nye format. Rigspolitiets vil endvidere indlede drøftelser med de øvrige teleudbydere om det fremtidige indhold og format for signaleringsoplysninger, der sikrer en korrekt overholdelse af editionspålæg vedrørende signaleringsdata.

Rigspolitiets Telecenter har i perioden fra den 24. september 2018 til den 28. januar 2020 registreret 262 bestillinger på signaleringsdata fra Telenor. Rekvisitionerne vedrører 96 unikke journalnumre. Telenor har i et brev af 4. februar 2020 til Erhvervsstyrelsen oplyst, at selskabet i perioden fra september 2018 til den 4. februar 2020 har udleveret 224 datasæt til signaleringsdata efter editionskendelse. Af disse 224 datasæt har der i 61% af tilfældene også foreligget en kendelse på indgreb i meddelelseshemmeligheden, hvorfor der har været udleveret 87 datasæt alene på baggrund af edition.[12]

Det fremgår af de journalnumre, som er angivet ved bestillingerne af signaleringsdata fra Telenor, at data overvejende har været rekvireret til brug for efterforskning af meget alvorlig kriminalitet som sprængninger, drab, drabsforsøg, brandstiftelse, kvalificeret vold, trusler på livet, besiddelse af skydevåben på offentligt sted, røveri og narkotikaforbrydelser. Det indebærer, at der i mange af sagerne ud over signaleringsdata også vil have været mulighed for at foretage indgreb i meddelelseshemmeligheden. Telenor har som nævnt oplyst, at der i 61% af tilfældene også har foreligget en kendelse på indgreb i meddelelseshemmeligheden. Det fremgår også af

[12] Forskellen i antallet af bestillinger og antallet af udleveringer kan bl.a. skyldes, at politikredsen anmoder om sikring af data, der ikke længere er tilgængeligt i Telenors system, eller at politikredsen, efter at have fremsendt en anmodning om hastesikring, alligevel ikke har brug for de sikrede data.

journalnumrene, at der har været indhentet signaleringsdata i sager vedrørende indbrud, tyveri og hærværk, men i et betydeligt mindre omfang.

Rigspolitiet er ikke bekendt med det præcise antal datasæt, hvori der er indgået oplysninger om SMS-indhold, idet det udarbejdede oversættelsesværktøj netop havde til formål at frasortere sådanne oplysninger. Det ville kræve, at politiet fremfandt alle rådatasæt modtaget fra Telenor før d. 20. juni 2019 og oversatte disse på en sådan måde, at oplysninger om SMS-indhold *ikke* blev frasorteret. Politiet ville derved gøre sig bekendt med oplysninger, som politiet ikke har hjemmel til at behandle på baggrund af en editionskendelse.

4.2. Underretning af de berørte

Som nævnt ovenfor anførte Telenor i e-mail af 7. juni 2019, at man ville indberette forholdet til Erhvervsstyrelsen som et brud på persondatasikkerheden.

Det fremgår af Telenors indberetning af 7. juni 2019 til Erhvervsstyrelsen, at der ikke ville ske underretning af de berørte personer, idet man ikke længere havde datasættene og ikke kunne identificere personerne. Telenor ses at have tilkendegivet i indberetningen, at det ville være umuligt eller uforholdsmæssigt vanskeligt at underrette de berørte personer.

De berørte personer forstås i denne sammenhæng som de abonnenter eller fysiske personer, hvis oplysninger har været omfattet af et brud på persondatasikkerheden, f.eks. de personer, hvis SMS'er uberettiget er blevet videregivet.

Det kan i den forbindelse oplyses, at Telenor i starten af juli 2019 rettede telefonisk henvendelse til Rigspolitiet vedrørende Erhvervsstyrelsens håndtering af den anmeldelse om et brud på persondatasikkerheden, som Telenor havde indgivet til styrelsen. Telenor forespurgte i den forbindelse om en underretning af de berørte registrerede måtte antages at have konsekvenser for politiets efterforskning. Rigspoliti et oplyste, at dette ikke er et forhold, der kan afklares generelt, men altid vil bero

på en konkret vurdering af, bl.a. hvor fremskreden en given efterforskning er og hvilken rolle den enkelte person, som Telenor ønsker at underrette, har i sagen. Det blev i den forbindelse bemærket, at denne afklaring alene kan foretages ved, at der rettes en anmodning herom til den enkelte politikreds, der forestår efterforskningen.

Efter de for Rigspolitiet foreliggende oplysninger har Telenor ikke rettet henvendelse til politikredsene.

Erhvervsstyrelsen har i et brev af 6. februar 2020 til bl.a. Telenor og Rigspolitiet oplyst, at Erhvervsstyrelsen, omkring tidspunktet for indberetningen, ikke mente, at der var grundlag for at pålægge Telenor at underrette de berørte abonnenter eller personer om bruddet. Samtidig anbefalede Erhvervsstyrelsen, at Telenor kontaktede Rigspolitiet for at drøfte spørgsmålet om underretning.

Telenor har i e-mail af 28. januar 2020 til Rigspolitiet anført, at Telenor ved telefonsamtalen i juli 2019 omtalt ovenfor havde fået forståelsen af, at en underretning af de berørte individer generelt ville kunne obstruere politiets efterforskning. Telenor anførte endvidere, at selskabet ikke havde modtaget dette på skrift fra Rigspolitiet, og Telenor forstod efter en telefonsamtale med Rigspolitiet den 27. januar 2020, at dette skyldes en manglende formel anmodning fra Telenors side.

Telenor fremsatte den 28. januar 2020 en formel anmodning om Rigspolitiets stillingtagen til, hvorvidt der kunne ske underretning af de berørte under hensyn til politiets efterforskning, og om politiets bistand med at identificere de berørte, i det omfang underretning kunne finde sted.

Rigspolitiet besvarede henvendelsen ved den e-mail af 30. januar 2020, der er omtalt ovenfor under afsnit 4.1.2. ovenfor, og anførte, at man gerne bistod med at identificere de berørte personer i det omfang, det var muligt, og at Rigspolitiet havde iværksat undersøgelser med henblik på afdække om, og i givet fald, hvordan man kunne bistå.

Samtidig anførte Rigspolitiet, at det – uanset udfaldet af undersøgelsen – altid ville bero på en konkret vurdering, om hensynet til efterforskning tilsiger, at underretning ikke finder sted, herunder at der skulle iværksættes en høring af den enkelte politikreds for at afdække dette i forhold til hver enkelt sag.

Rigspolitiet anførte endvidere, at i det omfang, Rigspolitiet kunne tilvejebringe de relevante oplysninger, ville Rigspolitiet dog ikke kunne foretage en gennemgang af oplysningerne med henblik på at identificere de berørte personer, idet dette ville indebære en behandling af oplysninger, der ikke tilkom Rigspolitiet at forestå. I stedet ville Rigspolitiet kunne tilbagesende det fulde datasæt til Telenor med henblik på, at Telenor selv foretog den fornødne fremsøgning, underretning mv.

4.2.1. Erhvervsstyrelsens vurdering af Telenors pligt til at underrette berørte personer

Ved det ovennævnte brev af 6. februar 2020 orienterede Erhvervsstyrelsen om, at styrelsen som uafhængig teletilsynsmyndighed havde foretaget en fornyet vurdering af spørgsmålet om underretning. Det bemærkes, at Erhvervsstyrelsens vurdering kun relaterer sig til eventuelt SMS-indhold i signaleringsdata.

Erhvervsstyrelsen fastholdt på baggrund af en konkret vurdering af de forhold, der er angivet i artikel 3 i Kommissionens forordning (EU) nr. 611/2013 af 24. juni 2013 sin opfattelse af, at styrelsen i henhold til forordningen ikke havde belæg for at meddele Telenor en pligt til at underrette de berørte. Samtidig fastholdt styrelsen sin opfordring til, at Telenor drøftede spørgsmålet om underretning med Rigspolitiet, herunder om efterforskningsmæssige hensyn talte mod underretning, såfremt Telenor ønskede at underrette de pågældende personer.

Erhvervsstyrelsen lagde i den forbindelse bl.a. vægt på, at videregivelsen er sket til det danske politi, som er den rette modtager, og som myndighed er vant til at håndtere private, fortrolige og følsomme oplysninger, og at der absolut ikke foreligger

risiko for, at bruddet kan medføre identitetstyveri eller svig, fysisk skade, psykologisk forstyrrelse, tort eller skade af omdømme.

Rigspolitiet bemærker, at det er Erhvervsstyrelsen, der som uafhængig teletilsynsmyndighed foretager den endelige vurdering af, hvorvidt en teleudbyder har en underretningspligt, og at denne pligt alene påhviler teleudbyderen, der har videregivet oplysningerne.

Som nævnt anmodede Erhvervsstyrelsen om Rigspolitiets bemærkninger til de ovenfor omtalte redegørelser fra Telenor om videregivelsen af modpartsnumre. Telenor gentog ved sin supplerende redegørelse af 4. februar 2020, at man ikke betragter videregivelsen af modpartsnumre som et brud på persondatasikkerheden efter Kommissionens forordning (EU) nr. 611/2013 af 24. juni 2013.

I sine bemærkninger den 26. februar 2020 til Erhvervsstyrelsen, jf. ovenfor under afsnit 4.1.4., anførte Rigspolitiet bl.a., at man ikke finder anledning til at afgive bemærkninger til Telenors redegørelse vedrørende spørgsmålet om, hvorvidt der konkret foreligger et brud på persondatasikkerheden, der udløser indberetningspligt, da afgørelsen af dette forhold ses at henhøre under Erhvervsstyrelsens ansvarsområde.

Erhvervsstyrelsen ses som nævnt endnu ikke at have truffet afgørelse om, hvorvidt videregivelsen af modpartsnumre er at betragte som et indberetningspligtig brud på persondatasikkerheden, og i givet fald om der skal ske underretning af de berørte.

Det bemærkes afslutningsvis, at Rigspolitiet ikke har pålagt eller på anden måde instrueret Telenor om at undlade at orientere de berørte registrerede om, at deres oplysninger har indgået i et brud på persondatasikkerheden hos Telenor. Rigspolitiet har imidlertid efter telefonisk forespørgsel fra Telenor oplyst, at Rigspolitiet på daværende tidspunkt (sommeren 2019) ville undtage oplysninger om, hvilken teleudbyder, der var omfattet af sagen, idet det på det tidspunkt ikke var alle udbydere,

der indsamlede signaleringsdata. Identifikationen af, hvilke teleudbydere der på tidspunktet konkret indsamlede signaleringsdata – og dermed også kunne pålægges at udlevere disse oplysninger til politiet – kunne således afsløre konkrete forhold om politiets efterforskningsteknikker, jf. offentlighedslovens § 33, nr. 1. Dette hensyn til politiets efterforskning er ikke længere aktuelt.

5. Andre tilfælde, hvor politiet har modtaget for mange eller forkerte oplysninger mv.

5.1. Modtagelse af oplysninger uden relevans for efterforskningen

Politiets efterforskning – særligt i de indledende stadier af efterforskningen – er ofte kendetegnet ved en meget bred indsamling af oplysninger, herunder oplysninger der umiddelbart eller over tid viser sig ikke at have betydning for sagen.

Det gør sig blandt andet gældende ved ransagning af telefoner og computere, hvor politiet indledningsvist sikrer al data på enheden for efterfølgende at analysere og sortere i data, således at det alene er de for sagen relevante oplysninger, der inddrages. Det resterende – og i den forstand irrelevante – data, bliver ikke inddraget i sagen.

Et andet eksempel er politiets ransagninger i sager vedrørende grov økonomisk kriminalitet, hvor politiet ofte beslaglægger et stort antal dokumenter og andre effekter, der umiddelbart kan være relevante for sagen, idet det ikke er praktisk muligt at gennemgå alle dokumenter mv. på lokationen for en given ransagning.

Endvidere kan politiet i forbindelse med en anmeldelse fra en borger eller virksomhed modtage store mængder oplysninger fra anmelderen, der ved en nærmere gennemgang viser sig ikke at være relevante for en strafferetlig vurdering.

Endelig kan politiet i forbindelse med indhentning af videoovervågning fra eksempelvis en dagligvarebutik i forbindelse med et anmeldelse om røveri – på grund af systemets tekniske opbygning – modtage en større mængde videomateriale end det,

der tidsmæssigt er relevant i forhold til røveriet. Det vil i det tilfælde alene være en del af videoovervågningen, der inddrages i sagen.

Det er således almindeligt, at politiet med eller uden kendelse kommer i besiddelse af flere oplysninger, end der er relevant for den konkrete efterforskning. For visse data – herunder data fra teleudbyderne – gør der sig imidlertid det særlige forhold gældende, at teleudbyderne muligt bryder persondatasikkerheden, når der udleveres flere data, end der er omfattet af rettens kendelse.

5.2. Modtagelse af modpartsnumre

Rigspolitiet har ikke tidligere været bekendt med andre systematiske fejl i de modtagne signaleringsdata end de for mange udleverede oplysninger i signaleringsdata fra Telenor. I forlængelse af det ITV-møde, som Rigspolitiet afholdt den 5. februar 2020 med lederne af kredsens it-efterforskere og NC3 forposter, jf. afsnit 4.1.1, rettede en af NC3 forposterne imidlertid henvendelse til Rigspolitiet og henledte opmærksomheden på, at den pågældende ved anden lejlighed havde konstateret, at der også fandtes modpartsnumre i signaleringsdata modtaget fra Telia. En efterfølgende analyse af tre tilfældigt udvalgte datasæt fra Telia, indhentet på baggrund af editionskendelser, viste, at der i 2 ud af de 3 datasæt forekom modpartsnumre.

5.2.1. Rigspolitiets stikprøve

På den baggrund har Rigspolitiet iværksat en stikprøvevis analyse af såvel *signaleringsdata* som *logningspligtige lokaliseringsdata* fra alle teleselskaberne. Denne stikprøve omfattede dog ikke modtaget signaleringsdata fra TDC, idet der på tidspunktet for analysen ikke var modtaget signaleringsdata fra TDC.

Rigspolitiet har dog efterfølgende undersøgt det signaleringsdata, der er modtaget fra TDC, og har ikke fundet indholdsdata i form af SMS og modpartsnumre i de i alt 3 leverede datasæt.

Stikprøven vedrørende signaleringsdata omfatter 29 datasæt fra Hi3G og Telia fra 2018-2019. Analysen viser, at der fandtes modpartsoplysninger i 10 datasæt fra Telia i perioden efter den 29. januar 2019. Der er således konstateret, at Telia i en kortere periode systematisk har udleveret modpartsoplysninger. Der blev ikke fundet modpartsoplysninger i data fra Telia fra 2018 eller i datasæt fra Hi3G. Der blev ikke fundet SMS-indhold i nogen af stikprøverne. I stikprøven for Telia blev der dog fundet information om, hvor mange tegn, der er blevet sendt i de enkelte SMS-beskeder.

På baggrund af stikprøverne rettede Rigspolitiet den 8. februar 2020 henvendelse til Telia og oplyste, at politiet havde konstateret, at der i signaleringsdata modtaget fra Telia var fundet oplysninger om modpartsnumre. Oplysningerne var del af et større ustruktureret datasæt og vanskelige at udfinde uden en særlig indsats. Rigspolitiet opfordrede Telia til hurtigst muligt at analysere de signaleringsdatasæt, Telia havde leveret til politiet med henblik på at afhjælpe ovenstående gennem en frasortering af de data, der ikke måtte udleveres.

Telia oplyste den 10. februar 2020, at selskabet allerede havde et funktionelt filter, som frasorterede modpartsnumre i data inden fremsendelse af signaleringsdata til politiet. Da Telia sletter filerne efter afsendelse til politiet, anmodede Telia politiet om at fremsende nogle yderligere oplysninger, så Telia kunne identificere de to nævnte sager og dernæst gennemgå datasættet med henblik på at afdække, om der var sket fejl i udleveringen.

Telia har den 18. februar 2020 over for Rigspolitiet oplyst, at de siden den 8. februar 2020 ikke har leveret oplysninger om modpartsnumre i deres signaleringsdata.

I februar 2020 gjorde en politikreds Rigspolitiet opmærksom på, at Hi3G i flere tilfælde havde afvist at udlevere signaleringsdata, hvis der i kendelsen var angivet et andet tidsinterval end hele klokketimer.

Rigspolitiet iværksatte på den baggrund yderligere undersøgelser af signaleringsdata fra Hi3G. Disse indledende undersøgelser viste, at Hi3G formentlig udleverede signaleringsdata for hele klokketimer, selv om rekvisitionen alene vedrørte en kortere tidsperiode. Dette skyldes formentlig, at Hi3G ikke havde teknisk mulighed for at levere signaleringsdata inden for en kortere og mere præcis angivelse end én klokketime. Der var endvidere indikation på, at Hi3G i den forbindelse havde udleveret for meget data i forhold til det i kendelsen anførte tidsinterval. Dette er dog ikke muligt at konkludere med sikkerhed, da Hi3G alene registrerer aktiviteterne i blokke af en times varighed.

Rigsadvokaten er orienteret om denne tekniske indretning i Hi3G's system, og Rigsadvokaten udsendte den 9. marts 2020 en instruks til politikredsene i forhold til fremtidige anmodninger om udlevering af signaleringsdata fra Hi3G. Heraf fremgår bl.a., at der ved indhentning af kendelser om udlevering af signaliseringsdata fra Hi3G i medfør af retsplejelovens § 804, stk. 1, både skal fremgå, hvilken periode der er relevant for efterforskningen, og hvilken periode Hi3G vurderes i stand til at levere. Dermed kan begge oplysninger indgå i rettens vurdering af, om editionsbetingelserne er opfyldt. Samtidig henledte Rigsadvokaten opmærksomheden på, at fejlagtigt modtagne oplysninger som udgangspunkt skal håndteres efter principperne om tilfældighedsfund for at sikre fuld transparens for straffesagens aktører.

5.2.1.1. Stikprøve i logningspligtige lokaliseringsdata

For så vidt angår stikprøven i *logningspligtige lokaliseringsdata* (dvs. eksklusiv signaleringsdata) – i daglig tale omtalt som historiske masteoplysninger – omfattede denne i alt 131 datasæt fra alle teleudbyderne i perioden 2013-2020. Analysen viste, at der fandtes modpartsoplysninger i 11 datasæt fra HiG3. Stikprøven vedrørende Hi3G omfattede 42 datasæt fordelt på perioden 2013-2020. De 11 datasæt med modpartsoplysninger fordelte sig med 1-2 datasæt på alle årene undtagen 2013 og 2016.

Det er på baggrund af stikprøven ikke muligt at konkludere, at der skulle være tale om en systematisk fejl hos Hi3G. Rigspolitiet har underrettet Hi3G om resultatet af undersøgelsen.

Rigspolitiets har endvidere på anmodning fra Hi3G – og efter aftale med Rigsadvokaten – den 2. marts 2020 præciseret over for Hi3G, at indholdsoplysninger og modpartsoplysninger ikke må indgå i historiske masteoplysninger.

Der fandtes ikke modpartsoplysninger i stikprøverne vedrørende logningspligtige lokaliseringsdata fra de øvrige udbydere.

5.3. Uberettiget udlevering af andre oplysninger fra teleudbyderne

Som illustreret af de ovenstående eksempler vedrørende lokaliseringsdata, herunder signaleringsdata, forekommer der ved udlevering og modtagelse af data fra teleudbyderne såvel systematiske og mere enkeltstående fejl.

Som yderligere eksempel på mere enkeltstående fejl – der ikke vedrører allerede registrerede lokaliseringsdata – kan nævnes fire indberetninger fra TDC til Erhvervsstyrelsen. De tre indberetninger omfatter udlevering af data for længere tidsrum end, hvad der er anmodet om. Kendelserne lyder på bestemte tidspunkter, mens data udleveres for 2 minutters intervaller. Den fjerde indberetning omfatter udlevering af data for et forkert tidspunkt i forhold til det tidspunkt, som er angivet i kendelsen.

Det fremgår af de foreliggende oplysninger fra TDC, at der er tale om enkeltstående fejl.

Hvis sådanne fejl bliver opdaget umiddelbart – primært af teleudbyderen – bliver det efter politiets erfaring rettet ved fremsendelse af nye data. Teleudbyderen har i sådanne situationer anmodet om, at filerne med de forkerte data slettes med det samme, samt at fremsendelsen af data til rekvirenten stoppes. I de tilfælde, hvor

data allerede er fremsendt til rekvirenten, er det normal fremgangsmåde, at telecenteret kontakter rekvirenten og oplyser, at der er afsendt forkerte data, hvorfor datasættet skal slettes. Nyt data med korrekt indhold bliver eftersendt umiddelbart, og dermed inden sletning finder sted hos teleudbyderen.

6. Vurdering og fremadrettede overvejelser

Som redegørelsen viser, har teleudbydere i en række tilfælde fejlagtigt udleveret teleoplysninger til politiet, som politiet ikke har anmodet om, og som ikke har været omfattet af de retskendelser, der har været indhentet i sagen. Oplysningerne har kun i begrænset omfang været læsbare for efterforskerne, og de har i vidt omfang været uden efterforskningsmæssig betydning. Der kan dog i det fejlagtigt udleverede materiale have været oplysninger, som politiet har kunnet anvende i efterforskningen.

Der har hovedsageligt været tale om ikke-logningspligtige data, som teleudbyderne logger med henblik på fejlretning, og dialogen med teleudbyderne peger på, at det kan have spillet ind, at der blandt teleudbyderne har været usikkerhed om, hvilke oplysninger der er omfattet af begrebet "signaleringsdata", jf. afsnit 4.1.3. og 4.1.4. ovenfor.

Som beskrevet i afsnit 5.1. er det ikke usædvanligt, at politiet i forbindelse med en efterforskning kommer i besiddelse af "for mange" oplysninger. Det er heller ikke ukendt, at oplysninger kan indgå i en efterforskning ved en fejl eller tilfældighed. Blandt andet er bestemmelserne i retsplejeloven, som er beskrevet i afsnit 3.3.2., og fremgangsmåderne, herunder i telecentret, som beskrevet i afsnit 5.3., et udtryk for, at sådanne situationer jævnligt vil opstå og herefter skulle håndteres i forbindelse med sagens videre behandling.

Uanset at det ikke er usædvanligt, at politiet i forbindelse med efterforskning kan kommer i besiddelse af "for mange" oplysninger, har politiet et ansvar for som myndighed at reagere, hvis man bliver opmærksom på, at der på mere systematisk vis fejlagtigt indgår oplysninger i politiets efterforskning. Dette ansvar skærpes

endvidere, når der er tale om oplysninger, som politiet almindeligvis kun har adgang til med retskendelse.

6.1. Politiets og anklagemyndighedens håndtering af sagen

Som beskrevet i afsnit 4.1.1. blev Københavns Politi Afdelingen for efterforskningsstøtte, i første omgang opmærksom på problemstillingen vedrørende SMS-data og modpartsnumre indeholdt i binære PCAP datafiler med signaleringsdata fra Telenor ultimo 2018.

Anklagemyndigheden i Københavns Politi gjorde i den forbindelse opmærksom på, at politiet ikke måtte tilgå eller anvende disse oplysninger i sagsbehandlingen.

Københavns Politi iværksatte herefter et arbejde med at udvikle et oversættelsesværktøj, der kunne oversætte og strukturere data fra Telenor til et format, som kunne anvendes i efterforskningen. Rigspolitiet havde via National Efterforskningsafdeling indsigt i udviklingen af oversættelsesværktøjet og den bagvedliggende problemstilling, og søgte i samarbejde med Københavns Politi at afdække, hvorvidt der var tale om en systematisk fejl.

Selv om politiet og anklagemyndigheden reagerede med det samme – og fra starten var opmærksom på, at der var tale om oplysninger, som politiet ikke burde have modtaget – peger forløbet på, at fokus i den indledende fase i høj grad var på at udvikle en operativ løsning i form af et oversættelsesværktøj, som kunne gøre signaleringsdata fra Telenor egnet til brug for efterforskerne og samtidig fjerne SMS-indhold.

Det var først den 27. marts 2019, at Rigspolitiet tog kontakt til Telenors politigruppe og henledte opmærksomheden på, at signaleringsdata fra Telenor indeholdt oplysninger, som ikke var omfattet af de bagvedliggende retskendelser.

Rigspolitiet har ikke kunne fastslå, om der fra politiets side blev fulgt op på denne orientering før i slutningen af maj, hvor Rigspolitiet – efter dialog med Rigsadvokaten – tog kontakt til Telenors juridiske direktør og påpegede, at politiet fortsat modtog for meget data. Det førte til, at Telenor iværksatte en fejlretning af systemet.

Det må i lyset af ovenstående konstateres, at der samlet set gik for lang tid, før Rigspolitiet rettede henvendelse til Telenor og fejlretning blev iværksat, og at der fra Rigspolitiets side mere aktivt burde have været fulgt op i forhold til teleudbyderen for at sikre, at fejlen rent faktisk var rettet.

Tilsvarende burde der – uanset at det i den indledende fase ikke stod klart for politiet, at der var tale om et mere systematisk problem – på et tidligere tidspunkt være tilvejebragt et samlet overblik over problemstillingens omfang og karakter.

Det manglende overblik fik bl.a. betydning for anklagemyndighedens håndtering af sagen, idet Rigsadvokaten i sommeren 2019 fik indtryk af, at problemstillingen var løst og derfor ikke fandt behov for at udstede generelle retningslinjer på området, hvilket ellers havde været ønskeligt.

6.2. Særligt om redegørelsen om teledatasagen

Rigspolitiet og Rigsadvokaten afgav den 28. september 2019 en redegørelse om den såkaldte "teledatasag". Sagen handlede om systematiske fejl i telecentrets behandling af teledata, samt konstateringen af fejl i (ubearbejdet) teledata, med en deraf følgende frygt for, at teledata gennem en længere årrække havde været ufuldstændige, forvanskede, fejlbehæftede eller vildledende. Formålet med redegørelsen var at beskrive disse fejl og deres mulige konsekvenser for verserende og afsluttede straffesager.

Da problemstillingen om SMS-indhold og modpartsoplysninger i Telenors data ikke omhandlede fejl i teledata – og ikke rejste spørgsmål om mulige fejlagtige afgørelser i straffesager – var der ikke overvejelser om at omtale problemstillingen

nærmere i redegørelsen. Det fremgik dog af redegørelsen, at signaleringsdata kunne være ufuldstændige i lighed med fejlkonverteret data, jf. bl.a. punkt 2.3.1 og 6.2.4.4 i redegørelsen.

6.3. Retssikkerhedsmæssige overvejelser

Spørgsmålet om, hvorvidt teleudbyderne – ved at udlevere oplysninger til politiet som ikke har været omfattet af retskendelsen – har overtrådt teleloven og lovgivningen om databeskyttelse, og de retssikkerhedsmæssige aspekter, det i givet fald rejser, falder uden for denne redegørelse.

Som anført i afsnit 6.1. ovenfor burde der efter Rigspolitiets opfattelse tidligere have været rettet henvendelse fra Rigspolitiet til Telenor og være skabt overblik over problemstillingens omfang og karakter.

Uanset at forløbet således burde have være håndteret bedre, er der efter Rigspolitiet og Rigsadvokatens vurdering ikke grundlag for at antage, at fejlagtigt udleverede oplysninger konkret har været anvendt i straffesager på en måde, der giver anledning til retssikkerhedsmæssige betænkeligheder.

Som beskrevet i afsnit 6 har der været tale om oplysninger, som politiet ikke selv har anmodet om, og som i vidt omfang har været uden nogen efterforskningsmæssig relevans. Af samme grund vurderes sandsynligheden for, at oplysningerne senere er blevet anvendt som bevis i forbindelse med en straffesag ikke at være særlig stor.

Skulle der være forekommet tilfælde, hvor fejlagtigt udleveret oplysninger er indgået som et blandt flere beviser i en straffesag, vil der ikke tale om forkerte eller fejlbehæftede oplysninger. Der er vil derfor ikke være risiko for, at nogen er dømt eller frifundet på et forkert grundlag.

Det vil i givet fald være fremgået af sagen, hvorfra oplysningerne stammede, ligesom den relevante retskendelse vil være del af sagens materiale. Sagens aktører –

herunder forsvareren – vil derfor have haft mulighed for at rejse indsigelse mod, at oplysningerne blev anvendt i sagen. Det vil i sidst ende altid være rettens vurdering, i hvilket omfang oplysningerne ville kunne indgå og tillægges bevismæssig betydning i den konkrete sag, jf. afsnit 3.3.2. ovenfor om den frie bevisbedømmelse.

6.4. Fremadrettede initiativer

Fremadrettet er det først og fremmest vigtigt, at teleudbyderne sikrer, at der ikke videregives oplysninger fra teleudbyderne til politiet, som ikke må udleveres på en kendelse om edition.

I den forbindelse bemærkes, at der er indledt et samarbejde mellem Rigspolitiet, Rigsadvokaten og teleudbyderne med henblik på at understøtte dialogen om de praktiske, tekniske og juridiske aspekter af den daglige drift mv. samt informationsudveksling om fremtidige praktiske og tekniske tiltag.

Det er herudover vigtigt at være opmærksom på, at det uanset iværksættelse af relevante tiltag til imødegåelse af uberettigede og/eller fejlagtige videregivelser er vanskeligt helt at gardere sig mod, at tilsvarende situationer kan opstå i fremtiden, og at det således også fremover vil kunne forekomme, at politiet modtager oplysninger utilsigtet.

Der er i forlængelse af teledatasagen og denne sag dog iværksat en række tiltag, som efter Rigspolitiets og Rigsadvokatens opfattelse vil medvirke til at minimere denne risiko. Det drejer sig om:

- Et nyt uafhængigt tilsyn med brugen af tekniske efterforskningsmidler og beviser.

- Certificering og akkreditering af telecentrets kvalitetskontroller.

- Telecentret styrkes med flere og specialiserede kompetencer.

- Et nyt samarbejdsforum mellem politiet og telebranchen skal sikre en systematisk dialog såvel på direktørniveau som operationelt (juridisk og teknisk).

- Målrettet uddannelse og kompetenceudvikling for brugere af teledata, dvs. efterforskere, analytikere og anklagere.

- Nye retningslinjer for sletning og kontrol med at reglerne overholdes.

Rigspolitiet og Rigsadvokaten har derudover i forlængelse af teledatasagen udarbejdet nye retningslinjer og vejledninger om anvendelse og præsentation af teledata, så de afspejler de usikkerheder, der er nævnt i det uvildige notat, ligesom de indeholder nationale retningslinjer for politikredsenes håndtering og kvalitetssikring af teledata.

En forudsætning for, at lokaliseringsdata, herunder signaleringsdata også kan blive fuldt omfattet af de mange nye initiativer på området, er, at ansvaret for disse data bliver forankret i Telecentret. Hidtil har Telecentret ikke haft anden rolle i forhold til signaleringsdata end bestilling, modtagelse og videreformidling, og dette har ikke nødvendigvis omfattet alle leveringer. Der foregår ingen behandling af signaleringsdata i Telecentret, men centret skal fremadrettet have en mere retningssættende rolle i udvikling, brug, kvalitetskontrol og godkendelse af værktøjer, som politikredsene anvender til oversættelse, analyse og systematisering af data, ligesom indhentning af signaleringsdata bliver integreret i Telecentrets rekvisitionssystem. Telecentret kan i den sammenhæng have behov for at trække på kompetencer fra andre enheder i Rigspolitiet, herunder særligt Nationalt Cybercrime Center, men bør på sigt, i takt med at styrkelsen af Telecentret bliver udmøntet, selv opbygge de nødvendige kompetencer til opgaven.

Herudover er det i forbindelse med regeringens udspil om tryghed og sikkerhed den 10. oktober 2019 besluttet at lave et grundigt og omfattende arbejde med modernisering af retsplejelovens regler om tvangsindgreb. Arbejdet forankres i Strafferetsplejeudvalget, der skal komme med et bud på ny lovgivning. Det er Rigsadvokatens forventning, at resultatet af dette arbejde vil kunne lede til klarere regler og dermed mindre usikkerhed om indholdet af afsagte kendelser.

Det kan tilføjes, at der allerede nu i arbejdsforummet mellem politiet og telebranchen er iværksat et arbejde med afklare af terminologien vedrørende signaleringsdata mv. og på den baggrund opdatere Deloittes notat vedrørende anvendelse af historiske teledata i straffesager (den såkaldte "varedeklaration" som anvendes i straffesager).