CIR1H nr 9810 af 20/06/2025 (Gældende)

Rigsadvokatmeddelelsen, afsnittet: Krypteret kommunikation fra særlige tjenester

Ministerium: Justitsministeriet

Journalnummer: CMS VB 11022

Rigsadvokatmeddelelsen, afsnittet: Krypteret kommunikation fra særlige tjenester

1. Overblik

Politiet – både i Danmark og internationalt – oplever, at personer i kriminelle miljøer i stigende grad benytter krypteret kommunikation ved brug af særlige tjenester som eksempelvis EncroChat og SKY ECC til kommunikation om alvorlig kriminalitet.

Kommunikationstjenesterne er kendetegnet ved at have indbygget en lang række tekniske modforanstaltninger, som er designet til at skjule brugernes kommunikation. Samtidig bliver tjenesterne stillet til rådighed af udbydere, som typisk ikke er samarbejdsvillige i forhold til retshåndhævende myndigheder. De retshåndhævende myndigheder har derfor vanskeligt ved at få adgang til data fra kommunikationstjenesterne. Andre landes retshåndhævende myndigheder har dog i enkelte tilfælde skaffet sig adgang til indholdet af krypterede kommunikationstjenester. Derved har myndighederne fået adgang til meget store mængder data fra kommunikationstjenesterne. Disse data har myndighederne givet andre landes retshåndhævende myndigheder indblik i gennem det internationale politisamarbejde.

De krypterede kommunikationstjenester, som dette meddelelesafsnit vedrører, skal ikke forveksles med mere udbredte krypterede kommunikationsapplikationer som f.eks. iMessage, Telegram, Signal, WhatsApp m.fl. Disse applikationer vil typisk kunne installeres af alle på en almindelig smartphone, mens f.eks. EncroChat og SKY ECC kræver særligt tilvirkede telefoner. Kommunikationsplatformene EncroChat og SKY ECC adskiller sig bl.a. fra de øvrige nævnte applikationer, idet EncroChat og SKY ECC efter politiets vurdering primært anvendes af organiserede kriminelle netværk.

EncroChat

EncroChat var en ”end-to-end” krypteret kommunikationstjeneste, som var installeret på særligt tilvirkede mobiltelefoner.

I forbindelse med et samarbejde mellem fransk og hollandsk politi og Europol lykkedes det de franske myndigheder at omgå krypteringen i marts 2020. I den anledning fik myndighederne adgang til mere end 120.000.000 datatransaktioner på netværket. EncroChat blev anvendt i perioden fra 2015 til juni 2020, hvor det blev kendt i de organiserede kriminelle miljøer, at netværket var kompromitteret som følge af de franske myndigheders dekryptering. EncroChat blev herefter lukket ned og anvendes ikke længere.

EncroChat-telefonerne blev ifølge Eurojust solgt for ca. 1.000 € stykket med et abonnement på 6 måneder for ca. 1.500 €. Samtalefunktion, kamera og mikrofon var deaktiveret på telefonerne, og der var alene mulighed for at bruge telefonerne til at skrive beskeder og chatte samt til at sende billeder via EncroChats servere i Frankrig. Der var installeret særligt hurtige slettefunktioner, så indholdet på telefonerne hurtigt kunne slettes, hvis brugeren f.eks. blev anholdt af politiet.

Efter dekrypteringen blev der konstrueret to databaser i henholdsvis Frankrig og Holland. Dansk politi fik online adgang fra Danmark til at gennemse og eksportere data relateret til Danmark til efterretningsbrug via den franske database.

Det kunne efterfølgende konstateres, at en stor del af brugerne gik over til at benytte den krypterede platform SKY ECC.

SKY ECC

SKY ECC var en krypteret kommunikationstjeneste til at udveksle beskeder, der blev installeret på almindelige, men konfigurerede smartphones, typisk iPhones. Der var kun få tilgængelige applikationer i en krypteret SKY ECC-telefon, og de almindeligt kendte applikationer var fjernet, ligesom det ikke var muligt at installere nye applikationer. Det var ikke muligt at foretage almindelige taleopkald fra telefonen.

I 2016 indledte politimyndigheder fra Holland, Belgien og Frankrig en fælles efterforskning mod det canadiske selskab SKY ECC, idet politiet i Belgien mistænkte selskabet for at tilbyde krypterede kommunikationsløsninger til kriminelle.

Den 9. marts 2021 blev det offentligt kendt, at myndighederne i de førnævnte lande i et samarbejde med Europol havde aktioneret mod platformen, og at sikkerheden var blevet kompromitteret. På det tidspunkt var der ca. 70.000 brugere af SKY ECC-platformen på verdensplan, og det blev samtidig betragtet som en af verdens mest anvendte krypterede kommunikationsplatforme. I perioden fra 2019 til 2021 blev der indhentet kommunikationsdata fra platformen.

Efterretningsdata modtaget gennem internationalt politisamarbejde

Når internationale samarbejdspartnere udveksler oplysninger om strafbare forhold med Danmark, kan det pågældende land (”ejerlandet”) fastsætte betingelser for, hvordan de modtagne oplysninger må anvendes. Det kan f.eks. være, at oplysningerne er begrænset til kun at måtte anvendes til efterretningsmæssig brug. Politiet og anklagemyndigheden vil herefter være bundet af disse betingelser.

National enhed for Særlig Kriminalitet (NSK) er nationalt kontaktpunkt for modtagelse af såkaldt efterretningsdata og har mulighed for at få stillet et samlet datasæt vedrørende profiler relateret til Danmark (landepakker) til rådighed.

Efterretningsdata indgår i politiets systematiske monitering af kriminelle grupper og netværk samt til vurdering af konkrete mistankegrundlag mod enkeltpersoner, grupper og netværk. Se pkt. 2.

Teknisk bevis

Oplysningerne fra de krypterede kommunikationstjenester er et teknisk bevis. Tekniske beviser vil altid indgå som ét blandt flere beviser i en straffesag, og betydningen af et bevis i form af oplysninger fra de krypterede kommunikationstjenester vil altid bero på en konkret vurdering af det enkelte bevis samt sagens samlede omstændigheder i øvrigt.

Det vil, i overensstemmelse med princippet om den fri bevisbedømmelse, i sidste ende være retten som afgør, hvilken bevismæssig vægt et bevis skal tillægges i den enkelte sag.

I forbindelse med behandlingen af en straffesag, hvor der indgår oplysninger fra en krypteret kommunikationstjeneste, skal anklageren særligt være opmærksom på følgende under efterforskningen, i forbindelse med tiltalerejsning samt under og efter hovedforhandlingen:

Under efterforskning

- Når der er rejst sigtelse, skal alle oplysninger fra den krypterede kommunikationstjeneste, som ikke kan udelukkes at have betydning for sagen og dermed de tiltaltes/sigtedes mulighed for at tilrettelægge et effektivt forsvar, indgå i sagen, jf. retsplejelovens § 729 a, stk. 3. Se pkt. 3.1.
- Oplysninger, der er oversendt fra NSK til en politikreds eller NSK's egne efterforskningsafdelinger, som af "ejerlandet" er begrænset til efterretningsmæssig brug, og som indgår i sagen, vil skulle underlægges en konkret vurdering af, om oplysningerne skal søges foreløbigt eller endeligt undtaget fra forsvarerens adgang til aktindsigt efter retsplejelovens § 729 c. Se pkt. 3.1.
- Hvis oplysningerne fra den krypterede kommunikationstjeneste af "ejerlandet" er begrænset til efterretningsmæssig brug eller lignende, skal der i god tid inden hovedforhandlingen sendes en retshjælpsanmodning til "ejerlandet". I retshjælpsanmodningen skal der anmodes om tilladelse til at fremlægge oplysningerne under straffesagen. Se pkt. 3.2.
- Dokumentationspakken for den krypterede kommunikationstjeneste (varedeklaration mv.) og kvalitetskontrolrapporten skal være bilageret ind i sagen. Se pkt. 3.3.

I forbindelse med tiltalerejsning

- Senest fire uger inden hovedforhandlingen begynder, skal der tages stilling til, om oplysninger, som er foreløbigt undtaget fra forsvarerens adgang til aktindsigt efter retsplejelovens § 729 c, skal søges undtaget endeligt, eller om der skal meddeles aktindsigt efter § 729 a, stk. 3. Se pkt. 3.1.

Under hovedforhandlingen

- Dokumentationspakken, herunder varedeklarationen som politiet har udarbejdet, jf. pkt. 3.3., skal dokumenteres i relevant omfang. Se pkt. 5.1.
- Oplysninger fra en krypteret kommunikationstjeneste er et teknisk bevis, som ikke kan stå alene i straffesagen. Se pkt. 3.5.
- Der må ikke fremlægges oplysninger, som er endeligt undtaget efter retsplejelovens § 729 c, medmindre hensynene bag undtagelsen er faldet bort. Se pkt. 3.1.

Efter hovedforhandlingen

- Der skal ske underretning om endelige domme i overensstemmelse med eventuelle aftaler indgået med eksempelvis det eller de lande, som har indhentet oplysningerne fra den krypterede kommunikationstjeneste, Statsadvokaten for Særlig Kriminalitet (SSK) eller NSK. Se pkt. 6.

2. Politiets efterforskning og sagsbehandling

Det er politimyndighederne i det eller de lande, som har sikret sig adgang til en krypteret kommunikationstjeneste, som "ejer" de oplysninger, der er tilgængelige i kommunikationstjenesten. "Ejerlandene" kan dog vælge at give politimyndigheder i andre lande indblik i oplysningerne med henblik på, at disse politimyndigheder selv kan vurdere, om kommunikationstjenesten indeholder oplysninger af betydning for det pågældende land; en såkaldt efterretningsadgang. Dette sker typisk via internationalt politisamarbejde.

Der er fastsat interne retningslinjer i politiet om håndtering af modtagne oplysninger fra krypterede kommunikationsplatforme.

Oplysninger fra krypterede kommunikationstjenester, som dansk politi indhenter fra internationale samarbejdspartnere, modtages i NSK, som herefter behandler det modtagne data, dels for at dette leveres

overskueligt, ensartet og valideret, dels for at udfinde eventuelle indikatorer på visse kriminalitetsformer og dels for at fastlægge identiteten på de fysiske personer bag kommunikationstjenesternes profiler.

NSK kan på den baggrund enten sende data direkte til politikredsene eller udarbejde efterforskningsoplæg, der som udgangspunkt vil indgå i den almindelige samarbejdsmodel mellem NSK og politikredsene.

Når dansk politi indgår i et internationalt politisamarbejde vedrørende en krypteret kommunikationstjeneste, skal det besluttes, hvordan oplysninger fra kommunikationstjenesten skal visiteres og videreformidles til de relevante politikredse. I den forbindelse skal det tillige afklares med "ejerlandet", under hvilke betingelser oplysningerne må anvendes i konkrete sager. Visitationsmodellen skal godkendes af Rigspolitiet og den centrale anklagemyndighed, inden den tages i brug.

Hvis oplysninger fra en krypteret kommunikationstjeneste skal behandles fortroligt, fordi oplysningerne af "ejerlandet" er begrænset til efterretningsmæssig brug, sørger politiet for, at baggrunden herfor er beskrevet. Det skyldes, at behovet for fortrolighed skal anvendes til at vurdere, om der skal ske en foreløbig eller endelig undtagelse af oplysningerne efter retsplejelovens § 729 c. Se nærmere herom i pkt. 3.1.

Herudover skal NSK udarbejde en dokumentpakke indeholdende en varedeklaration, et terminologiskema og et teknisk skema, som skal bilageres ind i sager med oplysninger, som stammer fra den krypterede kommunikationstjeneste. Dokumentpakken skal godkendes af Rigspolitiet og den centrale anklagemyndighed, inden denne tages i brug. Politiet skal endvidere udarbejde en kvalitetskontrolrapport til den konkrete sag. Se nærmere herom i pkt. 3.3.

Politiets beslutning om at anvende oplysninger fra en krypteret kommunikationstjeneste i en efterforskning af en straffesag er som udgangspunkt ikke i sig selv et konkret efterforskningsskridt, som kan gøres til genstand for rettens legalitetskontrol efter retsplejelovens § 746, stk. 1, eller princippet heri. Det følger af Højesterets kendelse af 27. september 2022 (trykt i UfR 2022.4878 H).

3. Forberedelse

3.1. Forsvarerens adgang til aktindsigt i oplysningerne efter retsplejelovens § 729 a, stk. 3, og fravigelse af adgang efter retsplejelovens § 729 c

Hvis politiet til brug for en konkret sag har modtaget oplysninger, som stammer fra en krypteret kommunikationstjeneste, eller hvis politiet vil gøre brug af sådanne oplysninger i en konkret sag, er oplysningerne omfattet af forsvarerens adgang til aktindsigt, jf. retsplejelovens § 729 a, stk. 3. Oplysningerne skal derfor inddrages i sagen. Det gælder også, selvom oplysningerne er begrænset til efterretningsmæssig brug af f.eks. "ejerlandet". I sådanne tilfælde skal det overvejes, om der er grundlag for at undtage oplysningerne fra forsvarerens adgang til aktindsigt i medfør af retsplejelovens § 729 c.

Oplysninger, som ikke er modtaget til en konkret sag, men som ikke kan udelukkes at have betydning for en konkret sag, er ligeledes omfattet af forsvarerens adgang til aktindsigt, og skal derfor inddrages i den konkrete sag. Det gælder også, selvom oplysningerne er begrænset til efterretningsmæssig brug.

3.2. Retshjælpsanmodning om tilladelse til brug af oplysninger i en straffesag

Hvis der i en sag indgår oplysninger fra en krypteret kommunikationstjeneste, skal det med bistand fra politiet undersøges, om oplysningerne må fremlægges under en straffesag.

Hvis oplysningerne ikke må fremlægges under en straffesag, eksempelvis fordi de af "ejerlandet" er begrænset til efterretningsmæssig brug, skal anklageren sende en retshjælpsanmodning til "ejerlandet", hvori der anmodes om tilladelse til at bruge oplysningerne i straffesagen. Anklageren skal i den forbindelse være opmærksom på, om der gælder en særlig procedure for fremsendelsen af retshjælpsanmodninger i sager med oplysninger fra den pågældende kommunikationstjeneste. Typisk vil denne procedure være meldt ud til embederne i forbindelse med, at NSK har indledt et internationalt samarbejde om en kommunikationstjeneste.

Hvis de oplysninger, som retshjælpsanmodningen vedrører, er undtaget efter retsplejelovens § 729 c, skal selve retshjælpsanmodningen også søges undtaget efter retsplejelovens § 729 c. Det skyldes, at det er uvist, om "ejerlandet" vil godkende anmodningen, og at det vil kompromittere fortroligheden i de bagvedliggende oplysninger, hvis retshjælpsanmodningen fremlægges, forinden en eventuel tilladelse fra ejerlandet kan opnås.

Når "ejerlandet" giver tilladelse til at bruge oplysningerne i straffesagen, skal det altid sikres, at der er overensstemmelse mellem de oplysninger, som er foreløbigt undtaget efter retsplejelovens § 729 c, og de oplysninger, som udleveres til forsvarsadvokaten efter retsplejelovens § 729 a, stk. 3. Hvis der af "ejerlandet" ikke er givet tilladelse til at bruge alle oplysningerne i straffesagen, skal det vurderes, om der er grundlag for at søge disse oplysninger endeligt undtaget fra aktindsigt i medfør af retsplejelovens § 729 c. Se i øvrigt pkt. 3.1.

Hvis "ejerlandet" undtagelsesvis ikke vil give tilladelse til, at oplysningerne fremlægges under straffesagen, skal sagen drøftes med den tilsynshavende statsadvokat.

3.3. Teknisk beskrivelse af kommunikationstjenesten

Inden sagen indbringes for retten, skal anklageren sikre, at der er udarbejdet følgende dokumenter, som beskriver den krypterede kommunikationstjeneste, hvordan oplysningerne er sikret og eventuelle fejlkilder ved indhentning og konvertering af data:

- Varedeklaration
- Terminologiskema
- Teknisk beskrivelse
- Kvalitetskontrolrapport

Varedeklarationen har til formål at sikre, at der er transparens for alle straffesagens aktører om tilvejebringelsen og behandlingen af data fra kommunikationstjenesten. Varedeklarationen har derudover til formål at beskrive de eventuelle fejl og usikkerheder, som knytter sig til anvendelsen af oplysninger fra kommunikationstjenesten som bevis under straffesagen. Der henvises i den forbindelse til varedeklaration for EncroChat (bilag 1) og varedeklaration for SKY ECC (bilag 2).

Terminologiskemaet beskriver visse tekniske begreber.

Den tekniske beskrivelse vedrører beskrivelse af den standardiserede databehandling af den pågældende platform og tilhørende kontroller.

Kvalitetskontrolrapporten dokumenterer, at politiet har udvist særlig opmærksomhed ved gennemgangen, kontrollen og brugen af data fra den krypterede kommunikationstjeneste, herunder i forhold til de potentielle fejlkilder og usikkerheder der kan være. Rapporten angiver således, hvilke data der er indhentet i sagen, hvordan kvaliteten af data er kontrolleret, hvis der er usikkerheder og fejlkilder, som vurderes at være særligt relevante for den konkrete sag, og i bekræftende fald hvilke efterforskningsskridt der eventuelt er foretaget for at imødegå de pågældende usikkerheder mv.

Dokumenterne skal være bilageret ind i sagen, og skal under hovedforhandlingen dokumenteres i relevant omfang, inden der gøres brug af oplysninger fra den krypterede kommunikationstjeneste. Se i den forbindelse pkt. 5.1.

3.4. Det juridiske grundlag for "ejerlandets" adgang til oplysningerne

Når de udenlandske myndigheders indsamling af oplysninger fra en krypteret tjeneste ikke sker som led i danske myndigheders efterforskning eller på foranledning af danske myndigheder, skal der ikke foretages en bedømmelse af indsamlingen efter den danske retsplejelovs regler om straffeprocessuelle indgreb. Det følger af Højesterets afgørelse af 11. januar 2023 (trykt i UfR 2023.1368 H). Derfor skal det kendelsesmateriale, som ligger til grund for "ejerlandets" indhentning af oplysninger fra den kryptrede kommunikationstjeneste som altovervejende hovedregel ikke søges indhentet til brug for danske straffesager.

Det skyldes, at det er en forudsætning inden for gensidig retshjælp, at et efterforskningsskridt, som gennemføres i en fremmed stat, foretages i overensstemmelse med den fremmede stats love og regler. Det vil være i strid med principperne i konventionsbestemt eller bilateralt aftalt gensidig retshjælp, hvis en anmodende stat foretager en juridisk prøvelse af lovligheden af det ønskede eller udførte efterforskningsskridt i udlandet. Hertil kommer, at det som udgangspunkt reelt ikke vil være muligt for en national domstol at vurdere, om en fremmed stats myndigheder har overholdt lovgivningen i den fremmede stat.

Når der indledes et internationalt politisamarbejde om en krypteret kommunikationstjeneste, vil det land, som har sikret adgang til kommunikationstjenesten, dog typisk generelt tilkendegive, at adgangen er sket i overensstemmelse med det pågældende lands lovgivning. Hvis en sådan tilkendegivelse foreligger, kan den eller selve oplysningen herom bilageres ind i sagen og skal dokumenteres under hovedforhandlingen i relevant omfang.

3.4.1. Særlige omstændigheder for så vidt angår EncroChat og SKY ECC

Hvis det bagvedliggende udenlandske kendelsesmateriale drejer sig om politiets indhentelse af oplysninger fra EncroChat eller SKY ECC, kan en anmodning fra en beskikket forsvarsadvokat om udlevering af det bagvedliggende franske kendelsesmateriale som udgangspunkt imødekommes.

Selv om udgangspunktet er, at det kendelsesmateriale, som ligger til grund for "ejerlandets" indhentning af oplysninger fra en krypteret kommunikationstjeneste, som altovervejende udgangspunkt ikke skal indhentes, jf. ovenstående pkt. 3.4, har den centrale anklagemyndighed efter en konkret vurdering besluttet

at fravige dette udgangspunkt for så vidt angår det kendelsesmateriale, der ligger til grund for de franske myndigheders indhentning af data fra EncroChat og SKY ECC.

Baggrunden for fravigelsen er, at de franske myndigheder til brug for straffesager i andre europæiske lande har udleveret dette kendelsesmateriale. Kendelsesmaterialet er derfor allerede fremlagt i sammenlignelige sager i andre europæiske lande.

3.5. Opmærksomhedspunkter ved anvendelsen af oplysningerne under en straffesag

Når der i en straffesag indgår oplysninger fra en krypteret kommunikationstjeneste, skal anklageren være opmærksom på, at der kan være en række potentielle fejlkilder og usikkerheder ved anvendelsen af oplysningerne.

Det vil altid bero på en konkret vurdering af den enkelte kommunikationstjeneste hvilke fejlkilder og usikkerheder, der kan knytte sig til anvendelsen af oplysninger fra tjenesten, og hvilken betydning disse fejlkilder og usikkerheder skal tillægges.

Varedeklaration

NSK udarbejder dokumentationspakker indeholdende bl.a. en varedeklaration for hver krypteret platform, der nedtages i de internationale efterforskninger, se også pkt. 3.3. Varedeklarationen har bl.a. til formål at beskrive de eventuelle fejl, mangler og usikkerheder, som knytter sig til anvendelsen af oplysninger fra kommunikationstjenesten som bevis under straffesagen. En varedeklaration kan løbende ændres eller tilpasses, hvis politiet f.eks. bliver opmærksom på nye fejlkilder og usikkerheder.

Teledata

Oplysninger fra krypterede kommunikationstjenester indeholder ofte teledata. Der gælder derfor de samme opmærksomhedspunkter for disse oplysningstyper, som der gælder for teledata i øvrigt. Der henvises i den forbindelse til Rigsadvokatmeddelelsen, afsnittet om anvendelse af teledata i straffesager. Den omstændighed, at oplysningerne indeholder teledata, er ikke ensbetydende med, at der er tale om logningspligtige oplysninger. Dette kan f.eks. skyldes, at oplysningerne om teledata indsamles af udbyderen af den krypterede kommunikationstjeneste, og dermed ikke sker som følge af en af myndighederne pålagt logningsforpligtelse, eller fordi teleudbyderne ikke har registreret oplysninger på baggrund af en pålagt logningsforpligtelse.

Hvis oplysninger om teledata stammer fra udenlandske teleudbydere, vil der ikke skulle foretages en vurdering af, hvorvidt det pågældende lands regler er i overensstemmelse med EU-Domstolens afgørelser om logning af trafik- og lokaliseringsdata. Dette skyldes, at oplysningerne er indhentet via international retshjælp, og det er en forudsætning inden for gensidig retshjælp, at et efterforskningsskridt, som gennemføres i en fremmed stat, foretages i overensstemmelse med den fremmede stats love og regler. Se også pkt. 3.4.

Datasæt er ikke altid komplette

Dekrypteringen af data fra krypterede kommunikationstjenester vil ofte foregå løbende. Det betyder, at de datapakker på konkrete brugerprofiler, som politiet modtager, ikke nødvendigvis er fuldt dækkende for

den kommunikation, som der har været på brugerprofilen. Det vil derfor ikke kunne afvises, at der har været kommunikation på en brugerprofil, som politiet ikke har fået adgang til.

Forud for en eventuel hovedforhandling kan det undersøges, om der er dekrypteret yderligere data vedrørende sagens relevante brugerprofiler. Det vil bero på en konkret vurdering, om eventuelt yderligere data skal indhentes til brug for sagen.

Bevismæssig vurdering

Oplysninger fra krypterede kommunikationstjenester vil altid skulle indgå som ét blandt flere beviser i en sag, og betydningen af et bevis i form af oplysninger fra en af disse kommunikationstjenester vil altid bero på en konkret vurdering af dels det enkelte bevis og dels sagens samlede omstændigheder i øvrigt.

Det vil i sidste ende være retten, som afgør, hvilken bevismæssig vægt et bevis i form af oplysninger fra krypterede kommunikationstjenester skal tillægges i den enkelte sag, jf. princippet om den fri bevisbedømmelse.

4. Anvendelse af oplysningerne som grundlag for tiltalerejsningen

Inden anklageren tager stilling til tiltalespørgsmålet, skal anklageren kontrollere, om politiet har udfærdiget kvalitetskontrolrapporten med de nødvendige oplysninger om usikkerheder og fejlkilder, der vurderes at være særligt relevante i sagen.

Herefter kan anklageren tage stilling til tiltalespørgsmålet. I den forbindelse skal anklageren forholde sig til relevante data og de opmærksomhedspunkter, der er forbundet med anvendelse af oplysninger fra krypteret kommunikation i straffesager, jf. pkt. 3.5.

I forbindelse med sin stillingtagen til tiltalespørgsmålet skal anklageren også vurdere, om der er foretaget de nødvendige efterforskningsskridt for at imødegå de usikkerheder, der er ved anvendelse af oplysninger fra krypteret kommunikation i den konkrete sag, eller om der skal iværksættes yderligere efterforskningsskridt.

I de tilfælde, hvor der rejses tvivl om validiteten af oplysninger fra krypteret kommunikation, kan det bl.a. være relevant at indkalde vidner, der kan belyse, hvordan og med hvilken sikkerhed de centrale oplysninger kan tolkes i den konkrete sag. Dette vil typisk være politiansatte, som arbejder med krypterede kommunikationstjenester.

Anklageren skal ved sin vurdering af tiltalespørgsmålet generelt være opmærksom på, at oplysningerne kan være mangelfulde. Hvis forklaringer eller andre oplysninger i sagen giver anledning til det, bør der i relevant omfang iværksættes yderligere efterforskning for at afdække, om oplysningerne er mangelfulde, og om der er forhold, som kan belyses på anden vis.

Særligt i sager, hvor oplysninger fra krypteret kommunikation udgør et centralt bevis, skal anklageren i forbindelse med udfærdigelse af bevisfortegnelsen og eventuel tidsplan overveje – eventuelt efter forudgående drøftelse med forsvareren – om der skal afsættes yderligere tid til dokumentation af oplysninger fra krypteret kommunikation.

5. Hovedforhandlingen

5.1. Dokumentation af oplysningerne under hovedforhandlingen

Højesteret har ved afgørelse af 11. januar 2023 (trykt i UfR 2023.1368 H) udtalt, at oplysninger fra det krypterede netværk EncroChat, der er tilvejebragt af udenlandske myndigheder, kan bruges som bevis i en straffesag.

I alle straffesager, hvor oplysninger, som stammer fra en krypteret kommunikationstjeneste, fremlægges som bevis under sagen, skal de relevante dele af varedeklarationen i fornødent omfang dokumenteres. Det samme gælder kvalitetskontrolrapporten.

NSK's tekniske beskrivelse kan i fornødent omfang anvendes af anklageren til at "oversætte" oplysninger, som stammer fra en krypteret kommunikationstjeneste.

Varedeklarationen, kvalitetsrapporten, terminologiskemaet og den tekniske beskrivelse er beskrevet i pkt. 3.3.

Det er de oplysninger fra den krypterede kommunikationstjeneste, som dansk politi har bearbejdet, der skal dokumenteres i retten. De originale oplysninger modtaget fra "ejerlandet" til brug for sagen bør dog være til stede i retten – medmindre oplysningerne er endeligt undtaget fra forsvarerens adgang til aktindsigt i medfør af retsplejelovens § 729 c, se pkt. 3.1 – til brug for behandling af eventuelle spørgsmål fra straffesagens aktører om uoverensstemmelser mellem de bearbejdede og de originale oplysninger.

6. Efter dom

Ofte ønsker "ejerlandet" og/eller det internationale politisamarbejde feedback vedrørende brugen af oplysninger fra den krypterede kommunikationstjeneste i konkrete sager. Anklageren skal derfor være opmærksom på, om der gælder en særlig indberetningsordning, herunder til SSK eller NSK.

Bilag

Bilag 1 – Varedeklaration for EncroChat: Politiets "Anvendelse af data sikret fra den krypterede kommunikationsplatform EncroChat i straffesager" af den 30. august 2021

POLITI

30. august 2021

Anvendelse af data sikret fra den krypterede kommunikationsplatform EncroChat i straffesager

Notatet har til formål at beskrive data sikret fra kommunikationsplatformen EncroChat samt eventuelle fejl og usikkerheder ved anvendelse af denne data i straffesager.

Historik – Kriminelles kommunikation via krypterede netværk

Politi- og andre efterforskningsmyndigheder oplever globalt, at organiserede kriminelle miljøer i stigende grad benytter sig af krypterede netværk til at kommunikere omkring alvorlig kriminalitet, herunder kommunikation før, under og efter drab i bandemiljøerne, samt i organiseringen af narko- og våbenhandel.

Når data krypteres, betyder det, at der anvendes en algoritme til kodning af data, så de ikke længere er i deres oprindelige form og derfor ikke kan læses. Dataene kan kun afkodes tilbage til deres oprindelige form ved at anvende en specifik dekrypteringsnøgle.

Typisk benytter man sig af asymmetrisk kryptering, hvilket betyder, at man gør brug af forskellige nøgler til kryptering samt dekryptering.

1

Hver bruger er i besiddelse af en offentlig og en privat nøgle. Når en besked sendes, anmodes automatisk om modtagerens offentlige nøgle og denne bruges til at kryptere beskeden inden afsendelse. Herefter kan beskeden kun dekrypteres, hvis man er i besiddelse af den private nøgle, hvilket betyder, at afsender i princippet heller ikke kan dekryptere beskeden igen.

EncroChat

EncroChat er en "end to end" krypteret kommunikations-app. App'en kan installeres på en mobiltelefon eller tablet og giver brugerne mulighed for at kommunikere indbyrdes i krypterede beskeder.

EncroChat blev i 2020 betragtet som en af verdens mest anvendte krypterede kommunikationsplatforme, og personerne bag EncroChat solgte krypterede telefonenheder til mere end 120 lande. EncroChat blev under OTF EMMA[1] i Europol kompromitteret i juni måned 2020, og herefter kunne det konstateres, at en stor del af brugerne gik over til at benytte den ligeledes krypterede platform, SkyECC.

Fransk politi begyndte under OTF EMMA i 2018 at arbejde med at dekryptere EncroChat, og i 2019 blev arbejdet forankret i en JIT i Europol mellem Frankrig, Holland og Europol. Det lykkedes at omgå krypteringen i netværket i marts 2020, og i den anledning fik myndighederne adgang til mere end 120.000.000 datatransaktioner på netværket. I juni måned 2020 blev det kendt i de organiserede kriminelle miljøer, at EncroChat netværket var kompromitteret, og enhederne blev derfor ikke anvendt mere.

Netværket havde ca. 60.000 aktive enheder, der var blevet solgt til kunder med garanti for anonymitet og diskretion. Enhederne var indrettet således, at de retshåndhævende myndigheder ville have meget svært ved at få adgang til data fra enhederne, idet der var indbygget en lang række af tekniske modforanstaltninger.

I forbindelse med Europol's arbejde i OTF Emma, blev der konstrueret to databaser i henholdsvis Frankrig og i Holland. Dansk politi fik online adgang fra Danmark til at gennemse og eksportere data relateret til Danmark til efterretningsbrug via den Franske database. Til styring af flow og

[1] OTF: Operational Task Force ved Europol

sagsgange blev Operation Pandora iværksat i Danmark i et samarbejde mellem efterforskningsfællesskaberne Særlig Efterforskning Øst (SEØ) og Særlig Efterforskning Vest (SEV). Operationen er ledelsesmæssigt forankret i en efterforskningssektion i SEØ.

Der er tilgået medarbejdere til den danske desk i Europol med henblik på at bidrage til indhentningen af data til Danmark. Medarbejderne har en udvidet adgang til konkret at søge efter internationale data i begge databaser. Hvis en politikreds ønsker at benytte data vedrørende en eller flere EncroChat profiler i en straffesag, skal politikredsen rekvirere data via en international retshjælpsanmodning til Frankrig.

Behandling af krypteret data

Hvis retshjælpsanmodningen godkendes af de franske myndigheder modtages EncroChat data til brug for efterforskning fra Frankrig på en CD-rom.

Den relevante politikreds fremsender herefter de modtagne franske data elektronisk til behandling hos SEØ/SEV, idet visse data kræver bearbejdning før de har et format, som er egnet til fremlæggelse som bevis i en straffesag. Efter endt behandling sendes en samlet datapakke med originaldata, behandlet data samt dokumentation retur til politikredsen.

På baggrund af efterretningsoplysninger udarbejdes en international retshjælpsanmodning om udlevering af data til efterforskningsbrug.

Kendelse fra Frankrig, som svar på den international retshjælpsanmodning.

Databaseudtræk fra franske OTF EMMA med franske data.

Behandling af data til brug for efterforskning.

Det modtagne original data er organiseret i mapper, således at der er én mappe pr. bruger og EncroChat enhed. Dermed vil data for et brugernavn, der har benyttet flere EncroChat enheder, blive modtaget i flere mapper. I hver mappe forefindes de rekvirerede data i Excel-ark. Fotos fremgår af arket med deres MD5 hashværdier[2], eller forkortede[3] udgaver heraf. Fotos foreligger desuden i en separat mappe ved siden af Excel-arkene.

---

[2] Hashværdier er identifikationsværdier for billeder. I dette tilfælde er der tale om hash værdier beregnet ved MD5 algoritmen.

[3] I enkelte tilfælde ses hashværdien forkortet og "tronkeret" i forbindelse med navngivningen

Excel-filer med data fra indhentede profiler ses desuden at indeholde separate dataark med de forskellige typer af data, som eksempelvis lokationsdata, indhold fra beskeder, kontakter med videre. Samtlige linjer i Excel-filen ses knyttet direkte til den pågældende brugers profil.

Excel-filer med data fra en generel søgning efter data relateret til profilen indeholder et eller flere dataark, alle inden for emnet "Messages". Den generelle søgning er foretaget af Frankrig på baggrund af rekvisition af data relateret til en konkret profil. Den pågældende bruger fremgår som part, dvs. enten afsender eller modtager, til samtlige datalinjer. Den enkelte datalinje kan være knyttet enten direkte til den pågældende brugers profil, eller til en anden brugers profil.

Bearbejdningen af data finder sted i SEØ. Ved modtagelse kontrolleres dataenes struktur og indhold for at sikre, at datasyntaks på en række punkter er som forventet.

Tekstindhold og fotos kopieres uredigeret ind i det bearbejdede datasæt. Hvis tekstindholdet er for omfangsrigt, vedlægges det i en separat tekstfil. Fotos valideres gennem den hashværdi, som fremgår af det originale datasæt.

Ved den følgende behandling af data sker der en bearbejdning og validering af data, ligesom der tilføjes oplysninger i form af lokationer for de telemaster, der er anvendt af enheden. Lokationer tilføjes på baggrund af Antenna ID værdier i originaldata, der via en omregning[4] giver nøjagtige oplysninger om den celle, der er anvendt i forbindelse med transmissionen. Disse oplysninger sammenholdes med danske mastelister for at udfinde placeringen af cellen. Den beskrevne databearbejdning er dokumenteret i metafilerne, vedlagt de enkelte datapakker.

Datasættene

Excel-ark	**Specifikke opmærksomhedspunkter** Særlige forhold omkring oplysninger i det specifikke ark.[5]	**Data, der er konverteret eller beriget** Se beskrivelse i vedlagte tekniske beskrivelse over databehandling og berigelse af data
Messages	Tidsstempler modtaget til brug for efterforskning er forbundet med usikkerhed, da enhedens geografiske lokation ikke med sikkerhed er konstateret, ligesom ejeren af enheden manuelt kan have indstillet tiden på enheden.	Informationerne vedr. tidszone og datotidsstempler angives i kolonnen "Device date" ud fra Datotid og GMT. Datotidsformaterne korrigeres for format, men tidsværdier korrigeres ikke.

[4] Se teknisk dokumentation (bilag) vedrørende omregning af Antenna ID til opslag i mastelister behandlet af Rigspolitiets Sektion for Teledata

[5] Beskrevet i notatet, "Teknisk beskrivelse vedr. databehandling og berigelse af EncroChat data til efterforskningsbrug".

	I kolonnen "Body" kan værdien i beskeden være forkortet grundet begrænsninger i Excel. Der kan være uoverensstemmelser i angivelsen af MD5 hashværdien i forhold til vedlagte mediefiler.	Den fulde værdi fra kolonnen "Body" udlæses separat og vedlægges data i en tekstfil. I cellen anføres teksten "Lang besked – se separat txt-fil". Når der ikke er uoverensstemmelser linkes mellem den oplyste MD5 hashværdi og den vedlagte mediefil.
Traceability	Data modtaget til efterforskning indeholder ikke en specifik GPS lokation for den geografiske lokation.	Grundet manglende GPS lokation i de modtagne data, beriges arket med en kolonne med "Masteliste" ud fra en beregning på værdien i kolonnen "Antenna ID".
Notes	I kolonnen "Note" kan værdien i beskeden være forkortet grundet begrænsninger i Excel.	Den fulde værdi fra kolonnen "Note" udlæses separat og vedlægges data i en tekstfil. I cellen anføres teksten "Lang note – se separat txt-fil".

Dokumentationen for databehandlingen omfatter nævnte terminologiskemaer samt den generelle beskrivelse af databehandling og berigelse. Den specifikke dokumentation for den konkrete databehandling i de enkelte sager genereres i metadatafiler, der følger med sagen.

Generelle opmærksomhedspunkter

Ved anvendelse af EncroChat data i straffesager er der en række potentielle fejlkilder og usikkerheder, som man bør være opmærksom på.

Allerede i den data, der leveres fra de franske myndigheder, er der en række iboende usikkerheder og fejlkilder. Data der modtages som svar på en international retshjælpsanmodning fra Frankrig er sikret af de udenlandske myndigheder, som deltager i JIT-samarbejdet. Det er ikke oplyst nærmere, hvordan data er sikret, og det kan som følge heraf ikke udelukkes, at data kan være helt eller delvist mistet eller forvansket i forbindelse med sikringen.

Idet dansk politi ikke har den tekniske dokumentation for den indledende datasikring af EncroChat data, kan fravær af data ikke tages som udtryk for, at der ikke kan have fundet kommunikation/aktivitet sted.

På den baggrund, kan et fravær af kommunikation/aktivitet på en eller flere enheder, ikke anvendes til entydigt at udelukke, at en enhed eller flere enheder har været aktive eller i kontakt med hinanden.

Nedenfor gennemgås de væsentligste fejlkilder og usikkerheder i forbindelse med anvendelse af EncroChat data.

Tidsstempler

EncroChat er et stykke software, der kan installeres på en mobiltelefon, tablet eller lignende. Tidsangivelserne i data er genereret på baggrund af det ur, som er indbygget i den enkelte enhed. Tidsangivelserne er derfor kun korrekte, i det omfang uret i enheden har været indstillet korrekt på tidspunktet for kommunikationen.

Geografisk lokalisering af en Encro-enhed

Oplysninger om Antenna ID leveres af de franske myndigheder som led i besvarelse af en retshjælpsanmodning fra en politikreds. Oplysningerne er genereret af EncroChat-softwaren i forbindelse med brug af enheden, hvorved der sker logning af oplysninger om de telemaster (celler), som enheden har anvendt. Særlig Efterforskning Øst har ved bearbejdning af disse data og sammenligning med lister over de danske telemaster udfundet de telemaster, som har været anvendt til at transmittere kommunikationen.

Bilag 2 – Varedeklaration for SKY ECC: Rigspolitiets "Anvendelse af data sikret fra den kryterede kommunikationsplatform SKY ECC som bevis i straffesager" af den 20. juni 2025

Varedeklaration – SKY ECC

20. juni 2025

RIGSPOLITIET

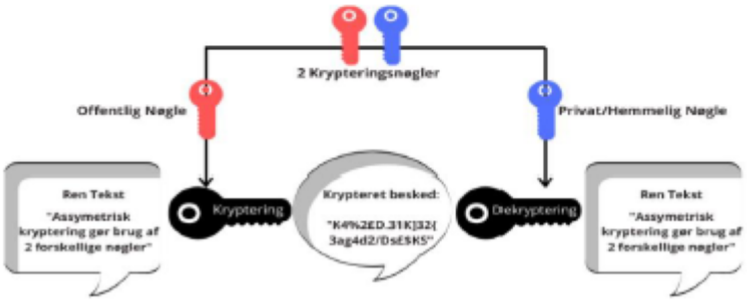
Politiområdet

Ejby Industrivej 33
2600 Glostrup
Telefon: 3314 8888

Anvendelse af data sikret fra den krypterede kommunikationsplatform SKY ECC som bevis i straffesager
Varedeklarationen har til formål at beskrive kendte fejl og usikkerheder ved anvendelse af krypteret data, sikret fra kommunikationsplatformen SKY ECC, som bevis i straffesager.

Baggrund – kriminelles kommunikation via krypterede kommunikationsplatforme
Politiet og andre efterforskningsmyndigheder oplever globalt, at organiserede kriminelle miljøer i stigende grad benytter sig af krypterede kommunikationsplatforme til at kommunikere om alvorlig kriminalitet. Det drejer sig blandt andet om kommunikation før, under og efter udførelsen af grov personfarlig kriminalitet såsom drab og organiseret narko- og våbenhandel.

Når data krypteres, anvendes en algoritme til at kode data, så data ikke længere er i den oprindelige form og derfor ikke kan læses. Data kan dekrypteres til den oprindelige form ved at anvende en specifik dekrypteringsnøgle. Typisk benyttes asymmetrisk kryptering, hvilket betyder, at der benyttes to forskellige krypteringsnøgler til kryptering samt dekryptering. Disse nøgler kaldes en privat og en offentlig nøgle, og de passer sammen i et sæt, der kan kryptere og dekryptere beskeder indbyrdes.



Hver bruger er i besiddelse af en offentlig og en privat nøgle. Når en besked sendes, anmodes automatisk om modtageres offentlige nøgle, og denne bruges til at kryptere beskederne inden afsendelse. Herefter kan beskederne kun dekrypteres, hvis man er i besiddelse af den private nøgle, hvilket betyder, at afsender heller ikke kan dekryptere beskederne igen.

SKY ECC historik

I 2016 indledte politimyndigheder fra Holland, Belgien og Frankrig en fælles efterforskning mod det canadiske selskab SKY ECC, idet politiet i Belgien mistænkte selskabet for at tilbyde krypterede kommunikationsløsninger til kriminelle.

Smartphones, der var blevet konfigureret til at kommunikere gennem SKY ECC, blev solgt til kunder med garanti for anonymitet og diskretion. Enhederne var sat op, så udenforstående ville have meget svært ved at få adgang til data på dem.

SKY ECC-platformen – funktionaliteter på en smartphone

SKY ECC er en krypteret platform til at udveksle beskeder, der er installeret på almindelige, men konfigurerede smartphones, typisk iPhones.

Første login på en SKY ECC-smartphone foregår med en kode, ligesom det kendes fra en almindelig smartphone.

Når brugeren får adgang til smartphonens menu, vil der kun være få applikationer tilgængelige. De almindeligt kendte applikationer er fjernet, og for den almindelige bruger er det ikke muligt at installere nye. Det er ikke muligt at foretage almindelige taleopkald fra smartphonen, heller ikke til særtjenester som eksempelvis 112.

Alle SKY ECC-smartphones er installeret med en UEM Client, et såkaldt Mobile Device Management. Det gør, at virksomheden, der har solgt smartphonen, har mulighed for at opdatere smartphonen eller eventuelt slette dens indhold af data uden at have fysisk adgang til den.

SKY ECC-applikationen kan efter brugerens valg skjules bag en applikation, som har et ikon, der ligner en almindelig lommeregner. I applikationen indtastes et specifikt regnestykke, hvilket bevirker, at selve SKY ECC-applikationen åbnes, hvorefter brugeren med rette kode får adgang til SKY ECC-platformen. Hver bruger er tildelt et unikt SKY ECC-ID, som benyttes til at logge ind på applikationen. SKY ECC-ID'et giver herefter adgang til at kommunikere på platformen.

Ifølge det canadiske selskab SKY ECC får brugeren adgang til følgende funktioner:

- Beskeder: Rediger, tilbagetræk, kopier eller videresend beskeder.
- Krypteret boks: Kræver endnu en kode til arkivering af notater, billeder og gemte chatbeskeder.
- Kategorier: Gruppering af kontakter.
- Foto: Send foto med "kig" eller download mulighed.
- Lydoptager: Send lydbeskeder.
- Gruppebeskeder: Send notifikationer til kontaktlisterne.

De hollandske myndigheder oplyste i en pressemeddelelse den 9. marts 2021, at der var ca. 70.000 brugere på SKY ECC-platformen på verdensplan. Efterforskningen viste, at kommunikationsdata fra SKY ECC blev opbevaret på en server af typen Blackberry BES (Business Enterprise Server), og at serveren befandt sig ved et hostingselskab i Roubaix i Frankrig.

På dette tidspunkt blev det offentligt kendt, at myndigheder i et samarbejde i Europol havde aktioneret mod SKY ECC-platformen, og at sikkerheden på platformen var kompromitteret. I perioden fra 2019 til 2021 blev der indhentet kommunikationsdata fra platformen.

SKY ECC blev på daværende tidspunkt af politimyndigheder anset som en af verdens mest anvendte krypterede kommunikationsplatforme i primært Europa, Nordamerika, Centralamerika, Colombia og i Mellemøsten.

Europol sikrede gennem sit arbejde med SKY ECC-platformen, at dansk politi via medarbejdere i Europol havde adgang til at søge i data.

National enhed for Særlig Kriminalitet (NSK) har det nationale ansvar for den overordnede styring af flow, sagsgange og databehandling af de data, der indhentes fra særlige krypterede kommunikationsplatforme, herunder SKY ECC-platformen.

Modtagelse af SKY ECC-data til efterforskningsbrug

Data modtaget fra Frankrig

Hvis dansk politi som bevis i en straffesag anvender SKY ECC data, sker dette på baggrund af en kendelse fra de franske domstole.

Indhentning af data for et specifikt SKY ECC-ID skulle frem til den 15. marts 2024 indhentes via en anmodning om international retshjælp til Frankrig. Efter godkendelse af retshjælpsanmodningen modtog dansk politi SKY ECC-data fra Frankrig til brug for efterforskning. Politiet modtog data inden for emneme: brugerinfo (user info), indeks (index), beskedtråde (conversations) samt mediefiler (media).

Til brug for indhentelsen har dansk politi modtaget en samlet liste med passwords fra de franske myndigheder. Listerne indeholder informationer om, hvilke tidsrum et password blev brugt af et givent SKY ECC-ID. Listerne er modtaget i filformatet JSON[1].

De franske myndigheder overførte den 15. marts 2024 data med SKY ECC-ID'er, der relateres til Danmark. Dette data benævnes i det følgende som landepakken.

I forbindelse med modtagelsen af landepakken blev der ved fremsendelse af en fransk kendelse givet en generel tilladelse til, at de danske myndigheder efter nationale bestemmelser kan gøre brug af de leverede informationer som bevis i danske straffesager.

Data modtaget fra Holland

Hollandsk politi har fra det hollandske teleselskab KPN modtaget internationale lokationsdata (APN[2]-data og historiske teledata), som indeholder oplysninger om, hvilke telemaster SKY ECC-enheder har benyttet til at transmittere data på et givent tidspunkt.

Den 21. februar 2022 modtog dansk politi disse KPN lokationsdata fra den hollandske anklagemyndighed. Data blev leveret i datasæt i filformatet CSV[3].

---

[1] JSON – JavaScript Object Notation

[2] APN - Access Point Name

[3] CSV – Comma-separated Values

Dansk politi modtog den 2. juni 2023 data fra de hollandske myndigheder med informationer om tidsbestemte forbindelser mellem SKY ECC-ID og IMEI-numre. Data blev leveret i datasæt i filformatet Excel.

Den 10. august 2023 modtog dansk politi en ny version af KPN lokationsdata. Data blev leveret i datasæt i filformaterne Excel og CSV[3].

Ved begge fremsendelser af KPN-lokationsdata angav den hollandske anklagemyndighed, at de vedlagte data kan benyttes til brug for efterretning, og at dansk politi kan anvende specifikke datalinjer fra de modtagne KPN-lokationsdata til brug for bevis i straffesager på følgende betingelser:

1. *Dansk politi skal være i besiddelse af en tilladelse fra Frankrig vedrørende brug af data for det specifikke SKY ECC-ID som bevis.*

   Denne tilladelse har Danmark modtaget i forbindelse med en godkendt retshjælpsanmodning eller i kraft af den generelle kendelse modtaget sammen med landepakken.

2. *Dansk politi skal gennem efterforskning kunne påvise en forbindelse mellem SKY ECC-ID'et og de anvendte IMEI-numre.*

   Bemærk, at forbindelserne kan fremgå af de informationer, som dansk politi den 2. juni 2023 modtog fra de hollandske myndigheder om tidsbestemte forbindelser mellem SKY ECC-ID og IMEI-numre.

Behandling af SKY ECC-data til efterforskningsbrug
Sektionen for Dataanalyse og Krypteret Kommunikation i NSK foretager en standardiseret behandling og en række kontroller af data modtaget fra både Frankrig og Holland. Det skyldes, at visse data kræver bearbejdning, før de har et format, som er egnet til fremlæggelse som bevis i en straffesag.

Når Sektionen for Dataanalyse og Krypteret Kommunikation i NSK modtager data, kontrolleres datastruktur for at sikre, at indhold og syntaks på en række punkter er som forventet. Hvis det ikke er tilfældet, bliver afvigelsen dokumenteret, og om nødvendigt håndteret gennem en manuel kontrol af de informationer, som afvigelsen omhandler.

Efter den indledende kontrol foretages selve databehandlingen, som indebærer en række yderligere kontroller. Resultatet af kontrollerne og dokumentationen af data vedlægges i en metadatafil, der beskriver den konkrete behandling af den enkelte datapakke.

Omfanget af den indledende kontrol samt indholdet i metadatafilerne er nærmere beskrevet i den tekniske dokumentation vedrørende den standardiserede databehandling af SKY ECC-data, som vedlægges sagen. Sammenhængen mellem kolonner i originaldata og kolonner i behandlet data er beskrevet i terminologiskemaer vedrørende SKY ECC-efterforskningsdata, som vedlægges sagen.

Behandling af SKY ECC-data modtaget fra Frankrig

Særligt om behandlingen af data modtaget fra Frankrig efter konkret retshjælpsanmodning:

Datatype	Behandling
Brugerinfo (User Info)	Vedlægges ubehandlet – modtages i varierende formater og kan derfor ikke behandles med kode.
Mediefiler (Media)	Samtlige mediefiler relateret til et SKY ECC-ID samles i én mappe.
Indeks (Index)	Indeks og beskedtråde behandles og vedlægges i én samlet Excel-fil med behandlet data pr. SKY ECC-ID.
Beskedtråde (Conversations)	
Passwords	Passwords vedlægges som et ark i den samlede Excel-fil.

Særligt om behandlingen af data modtaget gennem landepakken:

Datatype	Behandling
Mediefiler (Media)	Samtlige mediefiler relateret til et SKY ECC-ID samles i én mappe.
Beskedtråde	Beskedtråde behandles og vedlægges i én samlet Excel-fil med behandlet data pr. SKY ECC-ID.
Passwords	Passwords vedlægges som et ark i den samlede Excel-fil.

Ved behandlingen af data modtaget fra Frankrig kopieres værdierne fra originaldata uredigeret ind i Excel-filen med det behandlede data. Dog foretages redigering i følgende tilfælde:

- Tekstindhold, der er for omfangsrigt til, at Excel kan håndtere det i en celle, vedlægges i en separat tekstfil. Dette beskrives i den konkrete celle.
- Celler med indhold af data, der af Excel kan forveksles med en funktion, formateres som tekst.
- I starten og slutningen af hver besked indsættes en tom værdi, så emojis kan læses i Excel.
- Celler med indhold, der ikke kan tolkes af behandlingskoden, vil blive dokumenteret separat.

Mediefilers relation til specifikke datalinjer i beskedtrådene valideres gennem de hashværdier[4], som fremgår af de originale data. Såfremt der findes overensstemmelse mellem mediefilens beregnede og den angivne hashværdi, bliver mediefilen via et hyperlink forbundet med den relevante datalinje i Excel-filen med behandlet data.

Samtlige mediefiler relateret til et given SKY ECC-ID vil fremgå af media mappen. Hvis der ikke kan konstateres en relation mellem mediefil og datalinje i beskedtrådene vil det fremgå af datapakkens metadatafil.

[4] Hashværdien, der udregnes vha. en unik algoritme, benyttes som identifikationsværdi for mediefiler. I dette tilfælde er der tale om hashværdier beregnet ved sha1 algoritmen. I landepakken er der tale om to hashværdier sha1- og md5-algoritmen.

Særligt om behandling af de tidsbestemte forbindelser modtaget fra Holland
For hvert enkelt SKY ECC-ID er der leveret en Excel-fil bestående af tre tabeller, som indeholder informationer om et givent SKY ECC-ID, et eller flere IMEI-numre og en angivelse af, hvornår IMEI-nummeret og SKY ECC-ID'et har været forbundet. En tidsbestemt forbindelse er konstateret, hvis et SKY ECC-ID og et IMEI-nummer er registreret på samme tidspunkt. Sektionen for Dataanalyse og Krypteret Kommunikation i NSK har foretaget en standardiseret behandling af ovennævnte data, hvor de tre tabeller er blevet samlet til én sammenhængende tabel.

Særligt om behandling af SKY ECC-lokationsdata modtaget fra Holland
KPN lokationsdata indeholder værdier om følgende:

- Dato/tid.
- De fysiske enheder.
- Simkort (MEID-[5] eller IMEI-nummer samt IMSI-nummer).
- Identifikationsnumre for den telecelle, der er relevant for den enkelte datalinje.
- Informationer om, hvor pågældende telecelle befinder sig geografisk.

De modtagne KPN lokationsdata fra Holland indeholder således ikke oplysninger om SKY ECC-ID'er.

Den standardiserede behandling genererer en datapakke for hvert unikt IMEI-nummer.

Datapakken består af følgende elementer:

Datatype	Behandling
Originaldatafil	Excel-filer og CSV-filer eller alene CSV-filer indeholdende samtlige datalinjer fra det modtagne KPN lokationsdata vedrørende det pågældende IMEI-nummer. Værdierne fremgår i ubehandlet stand
Behandlet data	Excel-fil indeholdende ovennævnte lokationsdata i behandlet udgave
Metadatafil	Tekstfil indeholdende resultatet af den dokumentation og kontrol, som er udført i forbindelse med selve databehandlingen
IMEI-overview Fremgår kun i behandlede datapakker genereret ud fra KPN-lokationsdata modtaget den 10. august 2023	Excel-fil indeholdende et overordnet overblik over dataindholdet vedrørende det pågældende IMEI-nummer, eksempelvis optællinger af registreringer i de forskellige lande, dato for første registrering, dato for sidste registrering, angivelse af hvilke lande der har været registreringer i osv.

[5] Et MEID-nummer er 14 karakterer langt, og er identisk med en enheds IMEI-nummer uden det sidste kontrolciffer. Fremadrettet benyttes betegnelsen IMEI, idet det alene er de 14 identiske karakterer, som har praktisk betydning i forhold til levering af data.

Informationen fra originaldata vedrørende den geografiske placering (koordinater og adresse) for de enkelte teleceller vurderes at være af varierende kvalitet. Dette er nærmere beskrevet under afsnittet *"Specifikke opmærksomhedspunkter"*. I forhold til den standardiserede databehandling bliver de geografiske placeringer håndteret på følgende måde:

- Teleceller i Danmark: Informationer fra originaldata vedrørende den geografiske placering medtages ikke i den behandlede datapakke. I stedet foretages en berigelse med oplysninger hentet fra mastelister, som er udfærdiget i Sektionen for Teledatasupport i NSK på baggrund af lister, der er leveret af de danske teleudbydere. Berigelsen foretages datorelevant og omfatter en omregning af identifikationsnumrene for telecellerne, så de matcher det format, der fremgår i nævnte mastelister.
- Teleceller i udlandet: Informationer fra originaldata vedrørende den geografiske placering medtages i den behandlede datapakke. De pågældende celler i Excel markeres med en gul farve.

Videreformidling af SKY ECC-data efter udført standardiseret behandling
Efter behandlingen af data fremsender Sektionen for Dataanalyse og Krypteret Kommunikation i NSK en samlet pakke med data og vejledninger til politikredsene.

Datapakken indeholder:

Datamappe med SKY ECC-data:
- Originaldata fra Frankrig.
- Det behandlede data.
- Metadatafil indeholdende en beskrivelse af den konkrete databehandling, herunder resultatet af de kontroller, der er udført i forbindelse med selve behandlingen af data.

Datamappe med de tidsbestemte forbindelser:
- Originaldata fra Holland.
- Det behandlede data.
- Metadatafil: Tekstfil indeholdende en beskrivelse af den konkrete databehandling.
- Visualisering: HTML[6]-fil indeholdende en visualisering af den tidsperiode hvor SKY ECC-ID'et er registreret, samt et overblik over de tidsbestemte forbindelser der er konstateret mellem et SKY ECC-ID og IMEI-numre.

Politikredsene modtager derudover en datapakke med KPN-lokationsdata vedrørende de IMEI-numre, som kan relateres til det konkrete SKY ECC-ID. Datapakkens indhold er som beskrevet under afsnittet *"Særligt om behandling af SKY ECC-lokationsdata modtaget fra Holland"*.

Generelle opmærksomhedspunkter
Dansk politi er ikke i besiddelse af en detaljeret teknisk dokumentation for den indledende databehandling af det indhentede SKY ECC-data.

[6] HTML – HyperText Markup Language

Generelt kan eventuelt fravær af data ikke tages som udtryk for, at der ikke kan have fundet kommunikation eller anden aktivitet sted. Et fravær af oplysninger kan derfor ikke anvendes til entydigt at udelukke, at en eller flere enheder har været aktive.

På samme baggrund kan det ikke udelukkes, at der kan være sket forvanskning af data i forbindelse med sikring eller behandling af data, hvilket er nærmere beskrevet nedenfor i afsnittet *"Specifikke opmærksomhedspunkter"*.

Specifikke opmærksomhedspunkter

Datotidsstempler i forbindelse med data modtaget fra Frankrig

Tidsstempler er forbundet med usikkerhed, da enhedens geografiske lokation og dermed tidszonen ikke med sikkerhed er konstateret, ligesom det ikke kan udelukkes, at tidsstemplet kan være påvirket, såfremt ejeren af enheden manuelt har indstillet tiden på enheden.

For data modtaget som en del af landepakken ses tidsstempler at fremgå i UTC+0 og er dermed ikke korrigeret i forhold til tidszonen for den relevante geografiske lokation. Ejeren af enheden kan dog stadig manuelt have indstillet tiden på enheden.

Datotidsstempler i forbindelse med KPN-lokationsdata modtaget fra Holland

Tidsstemplerne, der er angivet i den enkelte datapakke, er ikke korrigeret i forhold til tidszonen for den relevante geografiske lokation.

Geografiske informationer – lokationer i Danmark

Der må forventes en række usikkerheder vedrørende opdateringer af mastelister samt registreringer på teleceller. Usikkerhederne i det modtagne KPN-lokationsdata vurderes at kunne sidestilles med usikkerhederne i lokationsdata modtaget fra danske teleudbydere. Her gælder det – som ved andet data baseret på telecelle registreringer – at flere registreringer, der understøtter samme billede, kan opveje betydningen af usikkerheder i data.

Geografiske informationer – lokationer i udlandet

Informationerne kan være forbundet med en vis usikkerhed. Usikkerheden bunder blandt andet i, at den præcise kilde til informationerne (koordinater og adresser) er ukendt.

For KPN-lokationsdata modtaget den 21. februar 2022 er det konstateret, at informationernes præcision varierer, og at koordinatet kan angive:

- Et centralt punkt i det aktuelle land.
- Et punkt beregnet ud fra flere teleceller i et geografisk afgrænset område.
- En specifik telecelle.

Det fremgår af terminologiskemaerne vedrørende SKY ECC data, hvorledes præcisionen for hver datalinje kan findes.

KPN-lokationsdata modtaget fra Holland den 10. august 2023

I forbindelse med modtagelsen af KPN-lokationsdata fra Holland den 10. august 2023 har NSK fået oplyst, at KPN ikke har leveret registreringer fra lande uden for Holland i perioden fra maj 2019 til den 25. december 2019. Det kan derfor ikke udelukkes, at der i denne periode har været aktivitet i andre lande end Holland.

Data i perioden fra december 2019 til den 23. marts 2020 indeholder ingen information om land og område. I denne periode skelnes der kun mellem hollandske og ikke-hollandske registreringer i data.

Hashværdier

Der vil udelukkende fremgå hyperlinks til konkrete mediefiler fra datalinjerne i beskedtrådene, såfremt der i den standardiserede databehandling er fundet overensstemmelse mellem beregnet og angivet hashværdi.

Hvis der er konstateret uoverensstemmelser mellem mediefilernes beregnede hashværdier og hashværdier noteret i de specifikke datalinjer, vil det fremgå af metadatafilerne.

Henvisninger til originaldata

Vedrørende brug af henvisninger til originaldata tolker forskellige software-programmer linjeskift forskelligt, og et valgt program kan derfor vise den korrekte information fra CSV-filerne på en anden linje end det oplyste.

For at sikre, at der ikke sker fejltolkninger, skal dansk politi bruge Windows 10's notesblok i den version, der anbefales i det tekniske underdokument. Notesblok skal bruges uden funktionen "tekstombrydning" aktiveret.

Omfangsrige værdier

Såfremt der i forbindelse med behandling af originaldata findes værdier, der er mere omfangsrige, end hvad Excel kan håndtere pr. celle, vil værdien blive printet i en separat tekstfil med henvisning til og fra den pågældende celle i Excel-filen med behandlet data.

Konstaterede afvigelser

Såfremt der konstateres afvigelser i forbindelse med kontrol og behandling af data, vil disse være dokumenteret i centrale logark eller i datapakkens metadatafil.