Eksternt review af risikoen for teknisk forvanskning af tekniske bevismidler forbundet med øget fortrolighed

Endelig afrapportering

Notat

9. april 2021

1 Formål, baggrund og scope for det eksterne review

Justitsministeren orienterede den 2. juli 2019 Folketingets Retsudvalg om, at der skulle iværksættes et eksternt review af politiets indhentning, opbevaring og behandling af tekniske bevismidler, herunder af de kontrolforanstaltninger som politiet og anklagemyndigheden har etableret. Denne orientering blev fulgt op af et brev til Retsudvalget af 4. oktober 2019, hvori der er beskrevet en række tiltag til opfølgning på teledatasagen, herunder iværksættelsen af et eksternt review af tekniske bevismidler.

Formålet med reviewet er at undersøge risikoen for at der sker teknisk forvanskning som et led i håndteringen af tekniske bevismidler hos politiet og anklagemyndigheden, herunder sikre at de fornødne kontrolforanstaltninger til at minimere sådanne risici er etableret hos myndighederne med henblik på fremover at forhindre/forebygge teknisk forvanskning af bevismidlerne. Reviewet skal dertil identificere eventuelle anbefalinger til kvalitetsforbedrende tiltag.

Det eksterne review af tekniske bevismidler forbundet med øget fortrolighed er gennemført af en ekstern konsulentvirksomhed i perioden oktober 2020 til marts 2021 og omfatter en kortlægning og uvildig vurdering af risikoen for teknisk forvanskning i forbindelse med politiets indhentning, opbevaring og behandling af tekniske bevismidler forbundet med øget fortrolighed. Dertil er overleveringen af bevismidlerne fra politiet til anklagemyndigheden og de pågældende kontrolforanstaltninger hos hhv. politiet og anklagemyndigheden blevet kortlagt.

Det eksterne review af tekniske bevismidler forbundet med øget fortrolighed har omfattet følgende bevismidler:

Tabel 1: Oversigt over de omfattede bevismidler

Bevistype	Omfattede tekniske bevismidler
1. Telekommunikation	• Aflytning • Teleobservation

2. Digital forensics	• Bevismiddel 1
	• Bevismiddel 2
	• Bevismiddel 3
	• Bevismiddel 4, herunder
	  ○ Bevismiddel 4a
	  ○ Bevismiddel 4b
	  ○ Bevismiddel 4c
	  ○ Bevismiddel 4d
	  ○ Bevismiddel 4e

Dette notat er udformet, så det ikke skal klassificeres, jf. sikkerhedscirkulærets bestemmelser. Det betyder, at anvendte processer, it-systemer og konklusioner alene er beskrevet på et overordnet niveau.

2 Konklusion

Det er på baggrund af det eksterne review af tekniske bevismidler forbundet med øget fortrolighed vurderingen, at de undersøgte bevismidler håndteres på en måde af politiet og anklagemyndigheden, der i overvejende grad vurderes at reducere risikoen for teknisk forvanskning, og at bevismidlernes nødvendige karakteristika ikke utilsigtet ændres som led i håndteringen.

Med teknisk forvanskning forstås en utilsigtet registrering og/eller forandring af digitale data om bevismidlet, således at disse data ikke længere fuldt repræsenterer bevismidlets oprindelige tilstand, og som betyder, at der i yderste konsekvens kan opstå usikkerhed i forhold til anvendelsen af bevismidlet i en straffesag.

Vurderingen af risikoen for teknisk forvanskning er baseret på en fempunktsvurdering, hvor der er foretaget en systematisk gennemgang af relevante processer, kontroller, it-systemer, data og kompetencer til håndteringen af de omfattede bevismidler. Der er - som et led i den gennemførte dataanalyse - ikke konstateret konkrete eksempler på teknisk forvanskning af nogle af de omfattede bevismidler.

Det bemærkes, at der er taget afsæt i en gennemgang af de på tidspunktet for reviewets gennemførelse gældende processer, kontroller og anvendte systemer til håndtering af de pågældende bevismidler og endvidere taget beskik af kendte igangværende og planlagte tiltag i politiet og anklagemyndigheden. Det betyder, at risikoen for teknisk forvanskning kan ændre sig, såfremt der efterfølgende foretages ændringer i processer, kontroller og særligt de systemer, der behandler bevismidlerne.

Der er for de undersøgte bevismidler, *jf. tabel 1*, tale om bevismidler af høj teknisk kompleksitet, som tilmed er underlagt en høj teknologisk udviklingshastighed, hvorfor afrapporteringen alene giver et øjebliksbillede af risikoen for teknisk forvanskning.

3 Oversigt over risikovurdering for de omfattede bevismidler

Det er samlet set vurderingen, at risikoen for teknisk forvanskning af de undersøgte bevismidler ligger på henholdsvis niveauerne lav og middel, *jf. nedenstående tabel*[1].

Det har ikke på alle de omfattede bevismidler været muligt at lave en detaljeret gennemgang af den systemmæssige databehandling af bevismidlerne, primært fordi der anvendes standardsystemer, hvor der ikke er adgang til gennemgå systemernes virkemåde i detaljer.

[1] Den anvendte risikovurderingsskala fremgår af metodeafsnittet sidst i dette notat

Tabel 2: Oversigt over vurdering af risiko for teknisk forvanskning for de enkelte bevismidler

Teknisk bevismiddel	Vurdering af risiko for teknisk forvanskning
Telekommunikation	
Aflytning	Lav til middel
Teleobservation	Lav til middel
Digital forensics	
Bevismiddel 1	Lav til middel
Bevismiddel 2	Middel
Bevismiddel 3	Lav til middel
Bevismiddel 4	
- Bevismiddel 4a	Lav til middel
- Bevismiddel 4b	Lav til middel
- Bevismiddel 4c	Lav til middel
- Bevismiddel 4d	Lav
- Bevismiddel 4e	Lav

3.1 Bevismidler afstedkommet af telekommunikation

Det vurderes på baggrund af det gennemførte review af tekniske bevismidler afstedkommet af telekommunikation, at der på tværs af aflytning og teleobservation er henholdsvis veldefinerede processer med en lav grad af kompleksitet, høj grad af systemunderstøttelse og videre en veldefineret arbejdsdeling mellem politikredsene og NC3, hvilket vurderes at bidrage til at nedbringe risikoen for forvanskning. Kontrolforanstaltningerne er mere ad hoc-prægede, fordi det er vanskeligt at kontrollere kvaliteten af data fra start til slut, fordi dele af datahåndteringsprocessen er forankret hos tele- og internetudbyderne.

Den primære databehandling hos politiet sker imidlertid i ét standardsystem, hvilket alt andet lige nedbringer risikoen for forvanskning, dog med den udfordring, at politiet ikke kan få detaljeret indblik i databehandlingsprocesserne inde i systemet, da dette af leverandøren betragtes som en forretningshemmelighed.

Risikoen for de forskellige analyserede aktiviteter, herunder aflytning af tale, internet mv. og teleobservation, varierer:

- Risikoen ses at være lavest for aflyttede samtaler, hvor det med relativ stor sikkerhed er muligt at verificere, hvilke parter, der fører en given samtale, hvad indholdet af denne samtale er, og om der evt. er udfald (datatab) i samtalen.

Endvidere sker der kun i sjældne tilfælde efterbearbejdning af aflyttede samtaler

- Risikoen ses at være højere for anvendelse af teleobservation og for de metadata (eksempelvis tidspunkt for samtalen og geolokation for start- og slutmast for samtalen), der indsamles i forbindelse med aflytning, fordi det ikke på samme måde umiddelbart er mulighed at verificerede de indsamlede data. Samtidig er anvendelsen af geolokationsdata fra teleudbyderne pr. definition forbundet med en vis usikkerhed, der er iboende i den anvendte teknologi. Endelig sker der typisk en efterbearbejdning af disse typer af data, hvilket vurderes at øge risikoen for teknisk forvanskning.

3.2 Bevismidler afstedkommet ved digital forensics metoder

Udgangspunktet for det gennemførte review af bevismidlerne afstedkommet ved **digital forensics** er, at der på baggrund af områdets høje kompleksitet vurderes at være en iboende risiko for, at der kan ske fejlfortolkning af data, hvilket medvirker til en øget risikoprofil. Området er generelt kendetegnet ved:

- Hurtig teknologisk udvikling, der stiller krav til **kontinuerlig opdatering af standard-analyseværktøjer** og dermed **versionsstyring** pga. hyppige opdateringer fra softwareleverandørernes side
- Store, uoverskuelige datasæt og datatyper, der **ikke er intuitivt forståelige, og derfor kræver særlige kompetencer at fortolke**
- **Stor bredde** i typer af analyseværktøjer, analysemetoder og datatyper på grund af det brede analyseområde.

Proceskompleksiteten vurderes generelt at være middelhøj, blandt andet fordi bevismidlerne og de sikrede data i en række tilfælde håndteres i et samspil mellem politikredsene og NC3, hvilket betyder, at data flyttes frem og tilbage. For bevismiddel 4-datakilderne ses der en større variation i proceskompleksiteten, hvilket også afspejles i risikovurderingen, der for flere af datakilderne ligger på niveauet lav og lav til middel.

Der vurderes at være et tilstrækkeligt, om end meget manuelt, kontrolniveau for bevismidlerne afstedkommet ved digital forensics metoder. Særligt i politikredsene ses der for visse områder et forbedringspotentiale. Dertil indgår i håndteringen af bevismidlerne generelt et antal forskellige it-systemer – både i forhold til sags- og datahåndtering og til selve analyserne af data. Analyserne af data indebærer særligt at fortolke data, der er udlæst fra forskellige typer af enheder, og i at kunne søge og sammenstille relevante oplysninger i nogle meget store datamængder. Standardanalyseværktøjerne og anvendelsen af resultaterne fra samme er afgørende for vurderingen af risikoniveauet.

Risikoprofilen varierer på tværs af de omfattede tekniske bevismidler:

- Risikoprofilen ses at være højest – middel – for data udlæst fra bevismiddel 2 blandt de omfattede bevismidler på digital forensics området. Dette skyldes, at data udlæst fra bevismiddel 2 er teknisk kompliceret, hvortil håndteringen af

data hovedsagligt sker decentralt i politikredsene, der generelt har færre tekniske ressourcer til rådighed, hvilket efterlader et større ansvar hos de enkelte efterforskere, der ikke nødvendigvis har de fornødne kompetencer til at forstå faldgrupper mv. på området.
- For de øvrige tre områder (bevismiddel 1, 3 og 4) ses risikoprofilen at ligge lidt lavere (lav til middel).

4 Anbefalinger til håndtering af bevismidlerne

Der er identificeret henholdsvis tre anbefalinger til bevismidlerne afstedkommet ved telekommunikation og tre anbefalinger til bevismidlerne afstedkommet ved digital forensics. Anbefalingerne vurderes at kunne reducere risikoen for teknisk forvanskning i den nuværende behandlingstilgang, *jf. tabel 3*.

Tabel 3: Oversigt over anbefalinger

Telekommunikation
Anbefaling 1: **Etablering af en fælles efterbehandlingsløsning for teleoplysninger m.m.** Der er på tværs af politikredse, efterforskningsfællesskaber m.m. konstateret et behov for at kunne efterbehandle og sammenstille store datamængder, herunder historiske teleoplysninger, metadata fra aflytning, teleobservationsdata mv. Efterbehandlingen har til formål dels at gøre data mere anvendelige i selve efterforskningen (eksempelvis ved at fremsøge forbindelser mellem personer på tværs af meget store datamængder), dels præsentere data, så de eksempelvis kan anvendes som bevismiddel i retten.
Anbefaling 2: **"End to end kontrol" af data fra teleudbyderne** På nuværende tidspunkt gennemføres der ikke en systematisk "end to end kontrol" af data fra teleudbyderne, hvor det kontrolleres, om data ser ud som forventet, når det udstilles for slutbrugeren (efterforskere). Teledatasektionen gennemfører to daglige kontroller, men her er fokus udelukkende på at sikre, at der modtages data i systemet fra alle teleudbydere, og ikke på at kontrollere, om informationerne er, som de må forventes at være. Mangler i datakvaliteten bliver således som udgangspunkt identificeret af slutbrugerne.
Anbefaling 3: **Øget kompetenceniveau i forhold til Aflytningssystemet og datafeltet** Henset til analysefeltets kompleksitet og Aflytningssystemets omfattende funktionalitet, vurderes der at være behov for at øge kompetencerne i forhold til Aflytningssystemet, først og fremmest blandt efterforskerne i politikredsene mv., så de kan udnytte systemets fulde funktionalitet og forstå de begrænsninger, der er i forhold til teleobservation.

Digital forensics
Anbefaling 4: **Øget kompetenceniveau i politikredsene** Der er behov for at øge kompetencerne blandt efterforskerne uden for Teknisk Efterforskning i politikredsene, så de kender de gængse usikkerheder ved digital forensic-analyser. Der bør ligeledes være fokus på løbende udvikling af kompetenceniveauet blandt medarbejdere i enhederne for Teknisk Efterforskning i politikredsene og efterforskningsfællesskaberne, så deres kompetencer modsvarer den teknologiske udvikling.
Anbefaling 5: **Dokumentation af usikkerheder vedr. digital forensic-bevismidler** Der bør udformes en dokumentation af de usikkerheder, som er forbundet med brug af bevismidler afstedkommet ved digital forensics, herunder usikkerheder ved de benyttede analyseværktøjer og ved analysefeltet generelt. Dokumentationen kan ske pr. digital forensic bevismiddel eller for hele analysefeltet, hvis dette vurderes mere hensigtsmæssigt. Dokumentationen kan minimere risikoen for, at bevismidler indgår i straffesager, uden at der tages de fornødne forbehold. Dokumentationen bør være et supplement til de eksisterende erklæringer, som beskriver konkrete udfordringer ved gennemført datasikring og analyse.
Anbefaling 6: **Retningslinjer for verifikation af data fra digital forensic-analyser** Grundet de iboende usikkerheder ved bevismidler afstedkommet ved digital forensic skal politiet i videst muligt omfang verificere resultaterne af de gennemførte analyser (fx ved dual tool, sammenstilling med andre datakilder eller kontrol mod udlæst data), særligt hvis de skal indgå i en straffesag. Det oplyses, at der som udgangspunkt sker en sådan verificering af resultater hos NC3, men at der ikke er tilstrækkeligt fokus på verificering af resultater blandt efterforskere i politikredsene. Det anbefales derfor, at der udarbejdes skriftlige retningslinjer for, hvornår der bør ske verifikation af data, som videreformidles til efterforskerne, fx når efterforskerne får udleveret data fra Teknisk Efterforskning i politikredsene.

Der er udover ovenstående anbefalinger endvidere formuleret et antal "øvrige anbefalinger", der vurderes at kunne styrke den nuværende behandlingstilgang af bevismidlerne afstedkommet ved telekommunikation og digital forensics, men som ikke vurderes at have direkte betydning for at minimere risikoen for teknisk forvanskning.

5 Risikovurderingsskala og den anvendte metode

Vurderingen af risikoen for teknisk forvanskning er foretaget med afsæt i en fempunktsvurdering, der vurderer processer, kontroller, it-systemer, data og kompetencer. Metodisk tages der udgangspunkt i en korrelationsbetragtning, hvormed de fem dimensioner betragtes som potentielle årsager, der påvirker den samlede risiko for teknisk forvanskning.

Risikoen for teknisk forvanskning er vurderet ud fra følgende skala:

Tabel 4: Risikovurderingsskala

Vurdering	Uddybende beskrivelse
Meget høj	Risikovurderingen **meget høj** betyder, at det vurderes, at der er ofte sker systematiske fejl ifm. datahåndteringen af bevismidlet. Samtidig vurderes det, at der er en meget høj risiko for enkeltstående, menneskelige fejl, og at sådanne fejl forekommer.
Høj	Risikovurderingen **høj** betyder, at det vurderes, at der er sket systematiske fejl ifm. datahåndteringen af bevismidlet. Samtidig vurderes det, at der er en høj risiko for enkeltstående, menneskelige fejl, og at sådanne fejl forekommer.
Middel	Risikovurderingen **middel** betyder, at det vurderes, at der er en risiko for, at der vil opstå systematiske fejl ifm. datahåndteringen af bevismidlet. Samtidig vurderes det, at der er en øget risiko for enkeltstående, menneskelige fejl, og at sådanne fejl forekommer.
Lav	Risikovurderingen **lav** betyder, at det vurderes, at det ikke er forventeligt, at der vil opstå systematiske fejl ifm. datahåndteringen af. Samtidigt vurderes det, at der er en vis risiko for enkeltstående, menneskelige fejl, men at sådanne fejl vil være sjældne.
Meget lav	Risikovurderingen **meget lav** betyder, at det vurderes, at det ikke er forventeligt, at der vil opstå systematiske fejl ifm. datahåndteringen af bevismidlet. Samtidigt vurderes det, at der er en lav risiko for enkeltstående, menneskelige fejl, men at sådanne fejl vil være meget sjældne.

De to faktorer, der vurderes i særlig grad at påvirke risikoen for teknisk forvanskning, er sandsynligheden for systemiske it-fejl og for menneskelige fejl. I vurderingen af risikoen for teknisk forvanskning tages der således højde for omfanget og indholdet af kontroller, der kan reducere sandsynligheden for at fejl opstår, samt risikoen ved de potentielle fejlkilder, der gør sig gældende. Det bemærkes, at der med menneskelige fejl i den forbindelse ikke forstås enkeltstående manuelle fejl, der altid vil være en tilstedeværende risiko, men systematisk menneskelig fejlhåndtering, f.eks. grundet manglende retningslinjer, kontroller, procedurer for fejlhåndtering og/eller en høj grad af proceskompleksitet uden understøttende foranstaltninger.