POLITIETS EFTERRETNINGSTJENESTE
DANISH SECURITY AND INTELLIGENCE SERVICE

Udkast til tale til brug for den offentlige høring den 28. august 2025 i Folketingets Retsudvalg vedrørende lovforslag nr. L218 om ændring af PET-loven

[Indledning]

Tak for ordet og tak for invitationen til at deltage i denne høring om det lovforslag om ændring af PET-loven, som blev fremsat i april i år.

Jeg vil ligesom ministeren koncentrere mit indlæg om den del af lovforslaget, som vedrører en ny ordning for større sammenhængende datasæt.

Vi forstår godt i PET, at forslag om ændringer af rammerne for PET's arbejde afføder offentlig debat. PET opererer i vidt omfang i "det skjulte" for at passe på "det åbne". Der kan derfor ikke være fuld transparens om, hvilke metoder og værktøjer vi anvender i det daglige. Og dermed kan der hurtigt opstå misforståelser eller fejlopfattelser af, hvad nye redskaber kan eller vil blive brugt til.

PET hilser derfor også en åben og nuanceret debat om vores redskaber velkommen. Og vi sætter pris på muligheden for at være med her i dag.

[Behov for tilpasninger af PET-loven]
Som ministeren var inde på i sin tale, blev PET-loven evalueret i 2022, og der blev i den forbindelse peget på behovet for at opdatere loven i forhold til behandlingen af store datamængder.

Når det er sagt, er det relevant at slå fast – som det også fremgår af evalueringen af PET-loven – at loven generelt er velfungerende og generelt understøtter en effektiv efterretningstjeneste.

Men PET-loven er udformet i en tid, hvor computere i vid udstrækning fungerede som registreringsværktøjer, der hjalp os med at organisere vores oplysninger, og vores arkiv var nogle skabe langt nede i PET's kælder. I dag er computeren adgangen til verden, og efterretningsarbejde foregår i dag i stor udstrækning bag en skærm. Mængden af data gør det i praksis ganske vanskeligt manuelt at gennemgå og analysere samtlige indsamlede oplysninger. Og mange af de trusler, vi skal forholde os til, eksisterer helt eller delvist i den virtuelle verden.

For at være på forkant med og kunne afværge disse trusler, er det nødvendigt, at PET under klare og tydelige regler kan operere i den digitale verden – og i store datamængder identificere forbindelser, mønstre og trusler, efterhånden som de opstår. Det forudsætter, at vi kan indsamle store klumper af data og uden at

gennemgå dem systematisk opbevare dem "på indersiden" i længere tid.

Når jeg siger, at PET-loven generelt er velfungerende og generelt understøtter en effektiv efterretningstjeneste, så skyldes det bl.a., at loven har fornuftige regler for indsamling og indhentning af oplysninger. Regler, som også giver mulighed for at arbejde databaseret.

Og lad mig i den forbindelse slå fast; PET arbejder i dag i større og større grad databaseret. Også med større datasæt. Og vi har da også i flere tilfælde afværget terrorangreb, som havde en virtuel dimension.

Men de nuværende regler i PET-loven har fokus på oplysninger om enkeltpersoner og forudsætter grundlæggende, at PET indsamler og indhenter oplysninger fokuseret på enkeltpersoner og i mindre skala. Disse data skal så inden for 4 uger gennemgås ift. det videre arbejde – og oplysningerne skal derefter enten journaliseres eller slettes.

De nuværende regler forhindrer os som sagt ikke i at arbejde i den digitale verden og med større klumper af data, men den eksponentielt stigende datamængde og det mere og mere komplekse trusselbillede kalder på en opdatering af reglerne.

Så PET fortsat kan varetage sin opgave med at passe på Danmark og danskerne. Men også for at sikre klare rammer for det tilsyn og den kontrol, en myndighed som PET naturligvis skal være underlagt.

[Udvikling i trusselsbilledet]

Som efterretnings- og sikkerhedstjeneste skal PET være på forkant med både den samfundsmæssige og teknologiske udvikling. Vores opgave er – på et tidligt stadium – at forebygge og afdække trusler mod Danmark og Rigsfællesskabet. Trusler fra bl.a. terrorisme, spionage, sabotage og udenlandsk påvirkning.

Truslerne er i stigende grad digitale. Det er i dag ikke nok blot at forlade sig på traditionelle metoder, såsom aflytning af telefoner eller observation af mistænkelige personer i den fysiske verden. Radikaliserede personer og medlemmer af terrorgrupperinger mødes ikke nødvendigvis fysisk, og megen radikalisering og kontakt foregår i dag online.

PET arbejder inden for de gældende regler allerede i vidt omfang med den digitale dimension af trusselsbilledet. Vi er så at sige ”online”, og vi interesserer os selvsagt for, hvad der foregår i f.eks. åbne og lukkede fora på visse dele af de sociale platforme. Det er vi nødt til.

På terrorområdet foregår radikalisering og rekruttering af unge i stigende grad digitalt og på sociale medier. Virtuelle fællesskaber og algoritmer, der forstærker ekstremistiske budskaber, gør det lettere at sprede radikaliseret indhold og tiltrække unge til ekstremistiske miljøer.

Også truslen fra de såkaldte statslige aktører har en klar digital dimension. Det vil jeg fokusere lidt mindre på i dag, men det er et meget vigtigt aspekt. Vi taler navnlig om spionage og forsøg på at anskaffe sig produkter, viden og teknologi for at udvikle de fremmede staters militære kapaciteter.

Vi taler om truslen fra fremmede efterretningstjenesters påvirkningsvirksomhed, og sabotagetruslen fra Rusland mod f.eks. kritisk infrastruktur er skærpet.

Det er en kerneopgave for PET at passe på Danmark og danskerne. Det gør vi ved at forebygge og afdække bl.a. spionage og sabotage. Det arbejde handler i høj grad om at kunne identificere enkeltpersoners tilknytning til udenlandske efterretningstjenester – enten som deciderede ansatte spioner eller som mere løst tilknyttede operative mellemled. Og det handler om at kunne udpege tilrejsende sabotører og dermed forhindre angreb på f.eks. dansk kritisk infrastruktur.

Svarene på disse udfordringer ligger i høj grad gemt i utroligt store datamængder. Kun ved at arbejde med større sammenhængende datasæt er det muligt at konstatere sammenhænge, mønstre og forbindelser. Det kan ske ved samkøring af f.eks. identitetsoplysninger, pasoplysninger, oplysninger fra sociale medier og rejsedata om rejseruter og ved at sammenholde disse oplysninger med andre efterretningsoplysninger hos os selv eller hos partnere. En opgave, som det i lyset af mængden af data og kompleksiteten i informationer ikke er muligt at udføre manuelt.

På den baggrund kan vi få det nødvendige grundlag for at arbejde videre – grundlaget for at sortere irrelevante personer fra så hurtigt så muligt og arbejde fokuseret videre med blik på de relevante målpersoner.

Og lad mig i den forbindelse slå én vigtig ting fast én gang for alle; når PET har begrundet mistanke mod konkrete enkeltpersoner og finder grundlag for at indlede en efterforskning, så sker det efter reglerne i retsplejeloven. Det vil sige, at vi – ligesom det øvrige politi – skal ned i retten og over for en dommer godtgøre mistankegrundlaget og argumentere for, hvorfor der f.eks. er behov for at aflytte en telefon eller ransage en bopæl. Og den mistænkte person har en advokat beskikket til at varetage sine interesser.

Det ændrer de foreslåede regler ikke ved.

[Eksempler på datasæt og behandling heraf]
Med det fremsatte lovforslag får PET mulighed for at indhente og arbejde på en anden måde med forskellige typer af store datasæt.

Vi får ikke adgang til andre eller nye typer af data, end dem vi kan indsamle og indhente i dag. Og vi får heller ikke adgang til uden retskendelse at indhente oplysninger, som i dag kræver retskendelse.

Og hvad kan PET så bruge disse større datasæt til? Lad mig forsøge at komme med et par eksempler.

Med de foreslåede regler får PET f.eks. adgang til at indsamle dele af åbne sociale medieplatforme. Det kan vi bruge til at opbygge et datamæssigt "normalbillede", som f.eks. kunne være relevant, når vi skal identificere statslige online-påvirkningskampagner.

Hvis PET skal afdække afvigelser – f.eks. desinformationskampagner – er PET nødt til at sammenholde udviklingen på f.eks. sociale medier med normalsituationen. Vores modstandere er professionelle og dygtige til at skjule sig. Med de foreslåede regler vil PET kontinuerligt kunne vedligeholde et sådant bagtæppe og normalbillede og ved hjælp af it-understøttelse identificere afvigelser. Dermed vil vi hurtigere kunne afsløre potentielt

ulovlig statslig indblanding i forbindelse med f.eks. valghandlinger.

Adgangen til at arbejde på større datasæt er lige så afgørende på terrorområdet.

På terrorområdet vil PET kunne indsamle oplysninger fra offentligt tilgængelige kilder, herunder åbne sociale medier, hvor eksempelvis højreekstremistiske eller militant islamistiske individer og grupperinger færdes og kommunikerer. Og vi ved, at radikaliserede personer og grupper bruger digitale platforme til at planlægge og forberede terrorangreb.

Herefter vil PET kunne foretage generelle analyser for at kortlægge tendenser og udviklinger i disse miljøer og derved udarbejde efterretningsanalyser og -vurderinger. De analyser og vurderinger vil f.eks. kunne have fokus på trends inden for særlige fokusområder – er der f.eks. en udvikling i, hvilke narrativer som fylder? – eller fokusere på nye symboler, som kan associeres med ekstremistiske grupperinger – f.eks. bestemte tegn eller memes.

De generelle analyser vil derefter kunne understøtte PET's mulighed for at udfinde relevante enkeltpersoner, som PET bør interessere sig mere konkret for. F.eks. fordi disse personer aktivt deler eller på anden måde spreder de identificerede narrativer eller memes.

Der er altså ikke tale om, at PET vil indsamle store klumper af data og derefter ved hjælp af f.eks. kunstig intelligens eller algoritmer foretage en såkaldt ”profilering”. Vi agter på ingen måde at få it-systemer til at udføre det analytiske efterretningsarbejde, som vores dygtige medarbejdere laver hver eneste dag.

Derimod vil vores analytikere kunne bruge de generelle analyser af data til at ”arbejde videre”. Analyserne kan sætte retning for det videre arbejde og medvirke til, at vi anvender vores ressourcer bedst muligt.

Derudover vil analyserne og vurderingerne kunne anvendes i forhold til PET’s eller det åbne politis forebyggende indsats.

Det handler for PET grundlæggende om at kunne identificere den næste Breivik. Eller den næste Omar Hussein. Og det skal vi helst kunne gøre, inden de begår deres terrorangreb.

I et andet tænkt eksempel vil arbejdet med større datasæt kunne understøtte PET’s evne til f.eks. at forhindre skoleskyderier.

Lad mig give et helt konkret tænkt eksempel.

Forestil jer, at PET får oplysninger fra f.eks. en SSP-konsulent i en kommune på Sydsjælland om, at der blandt unge i kommunen tales om, at der deles højreekstremt indhold på en gamingplatform. Og at der bliver talt om et "muligt" angreb.

Er det bare "trash talk" – som man i gamingmiljøer kalder det? Eller er det begyndelsen på noget langt mere alvorligt?

Sproget på sociale medier er ofte voldsomt. Det ved vi godt. Det meste er tomme trusler. Men indimellem gemmer der sig netop dét ene forløb, der kan udvikle sig til det næste terrorangreb. Den næste skoleskydning. Den tragedie, vi alle frygter. Og sandheden er, at forskellen – mellem tomme ord, hård retorik og egentlig planlægning – kan være uhyre svær at se.

Derfor har vi i den situation brug for at kunne indsamle en større mængde af den åbne kommunikation på gamingplatformen og analysere den i vores egne systemer.

På baggrund af de foreslåede regler ville vi kunne indsamle relevant data fra gamingplatformen vedrørende brugerprofiler på Sydsjælland i eksempelvis de seneste seks måneder. På samme måde som enhver anden borger ville kunne logge på platformen og downloade dataen. Der er således ikke

tale om, at vi ville kunne indsamle data om kommunikation, som i dag ville kræve en dommerkendelse.

I den data vil der uundgåeligt være oplysninger, der er uvedkommende. Sikkert også personlige oplysninger. Men vi leder ikke efter private oplysninger. Vi leder efter mønstre. Efter ord. Efter netværk. Indikationer, der kan afsløre, om nogen er på vej fra snak til handling.

Finder vi noget – står vi over for et valg.

Ligger det i gråzonen, vil vejen frem typisk være forebyggelse. Oplæg på skoler. Dialog med kommunen og SSP. Eller måske direkte samtaler med unge, der er ved at glide for langt ud.

Er det mere alvorligt, vil vi indlede en egentlig efterforskning. I så fald efter de samme regler i retsplejeloven som i dag – hvor indgreb kræver dommerkendelse.

Eller er det ligefrem så alvorligt, at der skal reageres her og nu? Så vil vi selvfølgelig gøre det!

Pointen er, at uden muligheden for først at analysere den store datamængde, ville vi aldrig få øje på de faresignaler, der er afgørende for, at vi kan handle.

PET vil ikke i dag effektivt kunne indsamle data som skitseret i eksemplet. Vi ville slet ikke kunne arbejde med den hastighed, som efter de foreslåede regler. Og det ville slet ikke være sikkert, at vi overhovedet fandt frem til konkrete unge drenge.

Dette er som sagt ét tænkt eksempel. Og vi kunne lave mange flere.

Men de foreslåede regler vil efter PET's vurdering gøre PET bedre i stand til at forebygge terrorangreb i Danmark.

Jeg håber, at disse eksempler gør det lidt lettere at få en fornemmelse for, hvordan PET kan arbejde med større sammenhængende datasæt. Og hvordan vi ikke har tænkt os at anvende dem.

[Tilrettelæggelse af arbejdet med større datasæt – interne retningslinjer, kontrol, it-systemer]

Lad mig så også lige knytte et par ord til det tilsyn og kontrol med anvendelsen af de foreslåede regler, som helt naturligt også har fyldt i debatten siden april.

Lovforslaget forudsætter, at PET udarbejder interne retningslinjer for behandlingen af større sammenhængende datasæt. Tilsynet med Efterretningstjenesterne skal orienteres om disse retningslinjer og vil skulle føre kontrol med, at de overholdes. Derudover vil tilsynet naturligvis skulle

kontrollere, om PET's behandling sker i overensstemmelse med de betingelser, som er angivet i PET-loven.

PET har herudover noteret sig, at der i den politiske debat om lovforslaget har været interesse for, præcist hvilke it-systemer og -leverandører som PET anvender eller påtænker at anvende i forbindelse med databehandlingen.

Til det kan jeg sige så meget, at udviklingen i trusselsbilledet betyder, at PET i højere grad end tidligere er afhængig af it-løsninger i det operative arbejde. Men derfor er PET også yderst varsom med at fortælle om kapaciteter, kapabiliteter og arbejdsmetoder, da indblik heri kan udnyttes af PET's modstandere. Det gælder også oplysninger om konkrete it-løsninger og -leverandører.

Der skal dog ikke herske nogen tvivl om, at PET i en verden, der forandrer sig hastigt, og hvor PET's modstandere får stadig flere teknologiske muligheder, er konstant optaget af at passe på vores data og systemer. PET har derfor foranstaltninger på plads til at passe på de oplysninger, som behandles i PET. Det gælder selvfølgelig internt i forhold til f.eks. styring af brugeradgange og logning af adfærd i systemerne. Og det gælder naturligvis også på it-området i forhold til vores eksterne leverandører og deres adgang til vores oplysninger.

[Afslutning]
Som jeg indledte mit indlæg med at sige, så hilser PET en åben og nuanceret debat om vores redskaber velkommen. Og vi sætter pris på muligheden for at være med her i dag.

Forslag om ændringer af vores retlige rammer og redskaber afføder helt naturligt en offentlig og politisk debat. Sådan skal det være i et demokrati og en retsstat.

Jeg håber, at mit indlæg har været med til at udfolde behovet for reglerne en smule, og at de nævnte eksempler har givet "mere kød på debatten".

Tak for ordet.