POLITIET
KRIPOS

Politidirektoratet
politidirektoratet@politiet.no

NCIS Norway

Deres referanse:	Vår referanse:	Sted, dato
	201803536	Oslo, 18.02.2019

HØRINGSSVAR – FORSLAG TIL NY LOV OM ETTERRETNINGSTJENESTEN

Det vises til høringsbrev fra Forsvarsdepartementet av 12. november 2018 med forslag om ny lov om Etterretningstjenesten, samt tilhørende e-post fra Politidirektoratet av 5. desember. Kripos beklager sen innsendelse.

1. Innledende merknader

Departementets lovforslag innebærer en gjennomgang og oppdatering av rettsgrunnlaget for hele informasjonsinnhentingsvirksomheten til Etterretningstjenesten. Etterretningstjenestens metodebruk foreslås lovfestet, samt reglene for behandling av personopplysninger, deling av informasjon og annen saksbehandling.

Lovforslaget som nå er sendt på høring er omfattende og komplekst. Etter vår oppfatning er departementets utredning til dels uklar og generelt vanskelig tilgjengelig. Selve lovteksten fremstår på flere områder som rettsteknisk mindre god. Kripos har, med den korte høringsfrist som ble gitt, ikke hatt mulighet til å sette seg inn i alle sider ved forslaget. Fokus for oss er det som har tydeligst grensesnitt mot politiets rolle og oppgaveutførelse.

Etter det opplyste er hensikten i stor grad å kodifisere gjeldende regelverk og praksis. Det er vanskelig å se i hvilken grad denne hensikt oppnås, idet Etterretningstjenestens praksis av naturlige grader er lite kjent. I tillegg er både lovutkastet og motivene på sentrale områder relativt diffuse.

I tillegg foreslår departementet at Etterretningstjenesten skal gis tilgang til såkalt grenseoverskridende elektronisk kommunikasjon. Denne delen av lovforslaget tar utgangspunkt i Lysne II – utvalgets rapport om digitalt grenseforsvar av 26. august 2016, som innenfor strenge rammer anbefalte dette innført også i Norge. Utvalgets rapport ble sendt på høring 5. oktober s.å. Kripos avga høringssvar 13. januar 2017.

Politiet har sentrale oppgaver knyttet til etterretning, forebygging, avverging og krisehåndtering, i tillegg til tradisjonell reaktiv etterforskning. Herunder er terrorbekjempelse primært et polisiært ansvar. For Kripos er det derfor særlig relevant å kommentere

lovforslagets begrensinger i adgangen til å dele overskuddsinformasjon fra tilrettelagt innhenting med politiet, samt det foreslåtte bevisforbudet for opplysninger fra slik metodebruk. På dette området innebærer lovforslaget en særregulering for informasjon som Etterretningstjenesten innhenter ved tilgang til grenseoverskridende elektronisk kommunikasjon.[1]

Kripos er positiv til at Etterretningstjenestens oppgaver, innhentingshjemler og metodebruk blir nærmere lovregulert. I utgangspunktet er vi også positive til at tjenesten, på nærmere vilkår, gis tilgang til grenseoverskridende elektronisk kommunikasjon. Samtidig er det klart at denne delen av lovforslaget utgjør et inngripende tiltak, der tunge kryssende hensyn forutsettes grundig vurdert.

I fortsettelsen vil Kripos først knytte noen merknader til de foreslåtte rettslige rammene for Etterretningstjenestens virksomhet (pkt. 2). Samlet sett synes lovforslaget her å fremstå noe fragmentarisk og uklart. Deretter følger merknader knyttet til innføringen av tilrettelagt innhenting, og som nevnt med særlig fokus på spørsmålet om delingsadgang og bruk (pkt. 3). Kripos' utgangspunkt er at lovforslaget etablerer en for snever adgang til deling av overskuddsinformasjon og bruk av opplysninger som bevis, med negative konsekvenser for politiets mulighet til forebygging, avverging og straffeforfølgning av alvorlig og samfunnsskadelig kriminalitet. Avslutningsvis vil vi også knytte noen merknader til utformingen av konkrete bestemmelser i lovutkastet (pkt. 4).

2. Hjemmelsgrunnlaget for informasjonsinnhenting og metodebruk

Ved lovforslaget gis Etterretningstjenesten vidtrekkende fullmakter til å benytte inngripende metoder for informasjonsinnhenting, også på norsk jord. Hensynene bak legalitetsprinsippet får dermed stor betydning ved utformingen av virksomhetens hjemmelsgrunnlag. Ny lov må ha en oversiktlig og forståelig systematikk, og det nærmere innholdet i bestemmelsene må fremgå tilstrekkelig klart. Samtidig må det etableres rettssikkerhetsgarantier mot misbruk og vilkårlighet. Kravene til forutsigbarhet og rettssikkerhetsmekanismer vil normalt korrespondere med graden av inngrep og faren for misbruk.

Med dette utgangspunkt stiller Kripos spørsmål ved om vilkårene for informasjonsinnhenting og metodebruk angis med tilstrekkelig klarhet. Samtidig er praktiseringen av de vide fullmaktene i begrenset grad underlagt legalitetskontroll. Kanskje særlig problematisk fremstår slike mangler knyttet til tjenestens innhentingsvirksomhet her i landet, der lovforslaget etter vårt syn etablerer en for uklar grenseflate mot ansvarsområdet til PST.

2.1 Grunnvilkår

Grunnvilkårene for informasjonsinnhenting og metodebruk er inntatt i lovutkastet kap. 5. Informasjonsinnhenting ved målsøking og målrettet innhenting skal bare kunne skje dersom det er "*grunn til å undersøke*" om innhentingen "*kan*" bidra til å frembringe informasjon relevant for etterretningsformål.

Utformingen av bestemmelsen gir lite veiledning i hvordan dette vilkåret skal forstås. Samtidig synes departementets redegjørelse i begrenset grad egnet til å presisere innholdet nærmere. Vedrørende betydningen av grunnvilkåret uttaler departementet blant annet:

---

[1] Lovutkastet §§ 7-12 og 7-13

> [2]*"Etterretningstjenesten skal ikke innhente informasjon basert på ren vilkårlighet eller «magefølelse». En eller annen ledetråd vil alltid måtte ligge til grunn. Dette er begrunnet både i personvernhensyn og av hensyn til forsvarlig ressursbruk. Det skal ikke søkes vilkårlig etter informasjon gjennom simpel gjetting."*
>
> [3]*"For kontrollformål må Etterretningstjenesten i ettertid kunne vise til et kvalifiserende faktum eller en begrunnet hypotese eller assosiering som holdepunkt for innhenting. Departementet vil understreke at et slikt faktum eller en slik hypotese imidlertid ikke vil måtte kreve dokumentasjon med en spesiell bevisgrad. Det vil heller ikke kunne kreves at holdepunktet må bygge på objektive eller kvalitetssikrede opplysninger. På dette stadiet i innhentingsprosessen mener departementet i tråd med fast og langvarig praksis, at inngangsparametret for å iverksette innhenting kan være basert på etterretningsfaglig begrunnede antagelser."*

For målrettet innhenting kreves i tillegg at det må være "*konkrete holdepunkter*" som tilsier at det er grunn til å undersøke. Dette tilleggsvilkåret gir i følge departementet anvisning på et høyere sannsynlighetskrav for at innhentingen vil frembringe relevant informasjon, uten at det synes å fremgå klart hva dette faktisk innebærer. I forlengelsen uttales også at innhenting kan skje selv om sannsynligheten for å frembringe informasjon med etterretningsverdi er relativ lav, anslagsvis i området 10 – 40 % sannsynlighet.

Den nedre grense for iverksettelse av informasjonsinnhenting etter utkastet §§ 5-1 og 5-2 forstås således som lav. I tillegg kommer at innhentingen etter en konkret vurdering må være forholdsmessig. Slik kravet til forholdsmessighet angis i høringsnotatet er Kripos imidlertid noe usikre på hvilken betydning denne vurderingen i realiteten vil få ved siden av grunnvilkåret, eller hvordan kravet vil kunne følges opp i en pågående innhenting og senere etterprøving.

I lovutkastet kap. 6 er så inntatt de metodene som Etterretningstjenesten kan benytte til den aktuelle informasjonsinnhentingen. Samtlige metoder kan benyttes både til målsøking og målrettet innhenting. Dersom den lave terskelen for informasjonsinnhenting er oppfylt, vil en følgelig ha tilgang til svært inngripende virkemidler, og med beskjeden legalitetskontroll. Beslutningen om metodebruk synes da fortrinnsvis å måtte basere seg på forholdsmessigheten av det aktuelle inngrepet. For bruk av metodene i utkastet §§ 6-6 og 6-8, slik som gjennomsøking og avlytting, kreves riktignok at tiltaket i tillegg anses "*strengt nødvendig*" for ivaretakelse av tjenestens oppgaver.[4] Etter vårt syn fremgår det imidlertid ikke klart hva et slikt forhøyet terskelkrav faktisk vil innebære ved siden av en alminnelig forholdsmessighetsvurdering.

Kripos forstår at det ikke kan stilles for høye krav til grunnlaget for innhenting og metodebruk dersom Etterretningstjenesten skal kunne motvirke avanserte utenlandske trusselaktører og ivareta sitt samfunnsoppdrag. Beslutningsgrunnlaget for tjenesten vil ofte være usikkert. Samlet sett etterlater imidlertid vilkårene og departementets redegjørelse usikkerhet rundt hvor terskelen for tjenestens metodebruk faktisk går. Skjønnsmessige kriterier for denne typen inngrep i den private sfære bør etter Kripos' syn ha en klarere ramme for anvendelse enn det som nå fremgår. Hensynet til forutberegnelighet på dette området underbygges også av at den fremtidige praktiseringen av tjenestens hjemmelsgrunnlag naturlig nok vil skje uten særlig grad av innsyn.

---

[2] Høringsnotatet pkt. 9.4.5.2 s. 154
[3] Høringsnotatet pkt. 9.4.5.2 s. 156

[4] § 6-6 omhandler gjennomsøking, avlytting, skjult bildeovervåkning og annen innhenting med tekniske midler. § 6-8 omhandler endepunktinnhenting.

Samtidig korresponderer tjenestens vidtrekkende fullmakter i liten grad med forslag til mekanismer for legalitetskontroll av innhentingsvirksomheten. Beslutningskompetansen for metodebruk er lagt til sjefen for Etterretningstjenesten, eller den han eller hun bemyndiger, uten at det fremgår noe ytterligere krav til formalkompetanse. Til sammenligning tildeles dermed større fullmakter enn det som i dag er lagt til politimesternivå for tilsvarende inngrep, der skjult metodebruk etter straffeprosessloven og politiloven er underlagt domstolskontroll.

Riktignok vil EOS-utvalget føre tilsyn med Etterretningstjenestens virksomhet, med dette kan ikke likestilles med rettsikkerhetsmekanismene rundt politiets metodebruk. Uklare rettslige rammer for informasjonsinnhentingen vil også kunne gjøre tilsynet med tjenestens praksis mer krevende og mindre reell.[5] Samtidig har Kripos forståelse for at regelverket må legge til rette for tjenestens mulighet til effektiv oppgaveløsning og ivaretakelse av sikkerhetshensyn, og at en domstolskontroll med større deler av innhentningsvirksomheten verken vil være hensiktsmessig eller mulig. Likevel mener vi at mulighetene for en bedre legalitetskontroll burde vært vurdert nærmere.

2.2 Territoriell begrensing

Bakgrunnen for revisjonen av tjenestens territorielle begrensning er blant annet EOS-utvalgets oppfatning av at gjeldene bestemmelser i etterretningstjenesteloven § 4 og e-instruksen § 5 var utydelige.[6] Forbudet i etterretningstjenesteloven § 4 første ledd er utformet slik:

> *"Etterretningstjenesten skal ikke på norsk territorium overvåke eller på annen fordekt måte innhente informasjon om norske fysiske eller juridiske personer".*

Bestemmelsen utfylles blant annet av e-instruksen § 5 tredje ledd:

> *"Lovens § 4 er ikke til hinder for at tjenesten kan innhente opplysninger om fremmed etterretningsvirksomhet i Norge, herunder om norske fysiske og juridiske personer som driver slik virksomhet, i den utstrekning tjenesten har behov for slik informasjon. Innhenting av slik informasjon skal skje gjennom eller etter samtykke fra Politiets sikkerhetstjeneste."*

Gjeldende regelverk nedsetter således et forbud mot på norsk territorium å overvåke eller på annen fordekt måte å innhente informasjon om norske personer, med unntak for norske personer som driver utenlandsk etterretningsaktivitet i Norge.

EOS-utvalget var imidlertid usikre på rekkevidden av bestemmelsen, og stilte blant annet spørsmål ved betydningen av begrepet "*fordekt*" innhenting for den nærmere fastleggelsen. Tjenestens praksis, med søk i lagrede metadata etter selektorer tilhørende norske rettssubjekter i Norge, stod etter utvalgets syn dermed i en rettslig uavklart stilling. Selv om formålet med slike søk var å finne andre selektorer for utenlandsetterretningsformål, kunne slik innhenting inneholde opplysninger om norske borgere i Norge.[7] Etterretningstjenesten selv tolket forbudet til kun å ramme innhentning *"mot"* norske personer, og følgelig at det måtte innfortolkes en forutsetning om "*overvåkningshensikt*". Utvalget viste til at det kunne argumenteres for en slik forståelse, men at dette uansett reiste spørsmål om når slik hensikt inntrer og hvor inngripende tiltaket er i forhold til personvernet.

---

[5] I utkastet § 1-1 bokstav b fremgår at et av formålene med loven er å sikre grunnlaget for kontroll med tjenesten.
[6] EOS-utvalgets særskilte melding til Stortinget om rettsgrunnlaget for Etterretningstjenestens overvåkningsvirksomhet av 17. juni 2016.
[7] EOS-utvalgets særskilte melding til Stortinget pkt. 1.2 og kap. 5.

I høringsnotatet gir departementet uttrykk for å dele EOS-utvalgets oppfatning om at den territorielle begrensningen kan formuleres tydeligere i lovteksten. Samtidig anføres at den rettslige uklarhet først og fremst beror på gjeldende lovs ordlyd og begrepsbruk. Det tydelige territorielle skillet gjenspeilet dessuten datidens trusselbilde og teknologiske utvikling. Departementet viser til at om tjenesten skal kunne varsle om ytre trusler mot Norge, er utenlandske trusselaktørers aktivitet i Norge av åpenbar utenlandsetterretningsinteresse, inkludert kommunikasjon med norske personer. I enkelte tilfeller vil det også være nødvendig å bruke informasjon om norske personer i målsøking etter utenlandske etterretningsmål.

På denne bakgrunn foreslår departementet i utkastet § 4-1 at tjenesten som hovedregel ikke kan rette innhenting mot fysisk person i Norge, eller mot virksomhet i Norge som utøves av juridisk person. Bestemmelsen gjelder all form innhenting, og skiller ikke etter statsborgerskap. Ved å bruke formuleringen "*rettet mot*" ønsker man imidlertid å tydeliggjøre at det er innhenting med nevnte "*overvåkningshensikt*" som omfattes av forbudet. Dette i motsetning til der informasjon innhentes for målsøking. Samtidig oppstilles en rekke unntak i § 4-2 knyttet til fremmed etterretningsvirksomhet. Departementet opplyser at lovforslaget er i tråd med gjeldende hovedregel og langvarig praksis, og innebærer ingen endringer i den etablerte arbeidsfordelingen mellom Etterretningstjenesten og PST.

Etter Kripos' syn er det hensiktsmessig at territorielle begrensninger forsøkes klargjort i en ny hovedregel. Imidlertid er vi usikre på i hvilken grad dette har blitt resultatet. Herunder fremstår det uklart hvordan forutsetningen om "*overvåkningshensikt*" vil gi anvisning på grensen for innhentingsvirksomheten i praksis. Høringsnotatet synes ikke å gå særlig i dybden på dette. Eksempelvis antas at skillet mellom målsøking og målrettet innhenting ikke alltid vil være like tydelig i en pågående innhenting. Særlig vil dette gjelde der tjenesten i søken etter etterretningsmål benytter selektorer tilhørende norske rettssubjekter i Norge. I slike tilfeller vil det kanskje ikke utelukkende være tilfellet at "*norsk informasjon uintendert kan følge med på lasset*".[8] For de som rammes av innhenting vil dette uansett formål utgjøre et inngrep i den private sfære.

I utkastet § 4-2 inntas forholdsvis omfattende unntak fra den territorielle begrensingen. På nærmere vilkår åpnes for vidtrekkende metodebruk også på norsk jord. Etter unntaksbestemmelsen kan Etterretningstjenesten rette innhenting mot utenlandske statsborgere eller mot norsk eller utenlandsk virksomhet i Norge, dersom det foreligger "*konkrete holdepunkter*" for at personen opptrer eller virksomheten utøves på vegne av fremmed makt. Sannsynlighetskravet er dermed tilsvarende vilkåret for målrettet innhenting i utkastet § 5-2. Departementet uttaler at det ikke kreves sannsynlighetsovervekt for tilknytning til fremmed makt, men at det må foreligge ett eller flere objektive holdepunkter for dette.

Etter Kripos' oppfatning synes det hensiktsmessig at unntaksbestemmelsen ikke gir adgang til innhenting mot norske borgere i Norge, men at innhenting mot virksomheter som sådan står i et annet lys. Imidlertid synes lovforslaget likevel å etablere en noe uklar grenseflate mot ansvarsområdet til PST, idet den nærmere rekkevidden av unntaksbestemmelsen kan være vanskelig å få tak på.

Herunder anses kravet om tilknytning til fremmed makt som en noe uforutsigbar terskel, der en skjønnsmessig vurdering i praksis kan gi adgang til inngripende metodebruk. En pågående innhenting rettet mot virksomhet i Norge, til forskjell fra norske borgere i virksomheten, antas også etter omstendighetene å kunne utfordre grensen. Dernest synes innholdet i begrepet "*fremmed makt*" uklart utenfor dets kjerneområde, ettersom det synes noe vagt beskrevet

[8] Høringsnotatet s. 124.

hvilke internasjonale organisasjoner som kan tenkes å falle innenfor. Terrororganisasjoner omtales ikke direkte, men grenseoverskridende terrorisme er samtidig en del av tjenestens oppgaver etter utkastet § 3-1 bokstav f. I høringsnotatet uttaler departementet også at det aktive innhentingsfokuset til Etterretningstjenesten vil og bør være rettet mot den utenlandske etterretningsvirksomheten og *"eventuelt deres styring av og kommunikasjon med norske borgere som er vervet av den fremmede aktøren. Videre oppfølging og innhenting mot norske personer vil være PSTs ansvar"*. Etter Kripos' oppfatning synliggjør uttalelsen faren for en utfordrende grensedragning.

Under Stortingets behandling av EOS-utvalgets melding ble det vist til at regelverket må legge til rette for en effektiv oppgaveløsning og ivaretakelse av sikkerhetshensyn. Videre ble uttalt at dagens trusselaktører er oppdaterte på den teknologiske utviklingen, og at Etterretningstjenesten er nødt til å være utrustet med de virkemidler som behøves for å utføre oppdraget sitt. Kripos støtter dette, og har forståelse for at utøvelsen av fremmed etterretningsvirksomhet i Norge må ligge innenfor tjenestens innhentingsfokus.

Uklare rettslige rammer knyttet til Etterretningstjenestens fullmakter fremstår imidlertid særlig problematisk i forhold til ansvarsområdet på norsk jord. Denne grensen bør være tilstrekkelig forutsigbar. Selv om tjenestens og PSTs formål ikke er sammenfallende, har "sporvalget" ved innhenting betydning for vilkår og krav til legalitetskontroll. Samlet sett gir lovforslaget potensielt tjenesten fullmakter til omfattende metodebruk på norsk jord, basert på til dels uklare skjønnsmessige rammer, og med lav grad av legalitetskontroll.

3. Innføring av tilgang til grenseoverskridende elektronisk kommunikasjon

Som nevnt innledningsvis foreslår departementet at Etterretningstjenesten gis tilgang til grenseoverskridende elektronisk kommunikasjon, såkalt "tilrettelagt innhenting".

I praksis omfatter dette tilgang til kommunikasjon som med dagens teknologi transporteres i fiberkabler over den norske landegrensen, omtalt som kommunikasjon i transitt. Kjernen i tiltaket er at metadata fra slik kommunikasjon lagres i bulk, og at tjenesten på nærmere vilkår skal kunne gjennomføre søk eller målrettet innhente utvalgt kommunikasjon.

Slik forstått vil systemet i korte trekk bestå av tre forskjellige datasett, betegnet som kortidslageret, metadatalageret og spesifiserte innholdsdata. Den tekniske innretningen vil inneholde en løsning for filtrering, som for det første skal redusere mengden data som flyter inn i systemet, samt filtrere bort trafikk som enkelt lar seg identifisere til å falle utenfor Etterretningstjenestens oppgavesett. Systemet vil også i størst mulig grad filtrere bort metadata som ikke er relevant for tjenestens samfunnsoppdrag. Samtidig viser departementet til at en fullstendig filtrering av metadata er teknisk vanskelig, slik at metadatalageret vil inneholde store mengder overskuddsinformasjon.

Videre anvendelse av tilgangen vil imidlertid være underlagt nærmere vilkår og domstolskontroll, og basert på rettens godkjennelse av angitte modus- eller personselektorer. Selve søkene skal kun utføres av utpekt personell, og det vil være maskinell kontroll med at både søk i metadata og innhenting av innholdsdata er i henhold til rettens tillatelse. Dernest foreslås også etableringen av et styrket og løpende tilsyn med at tjenestens bruk skjer i henhold til de rammene som er fastsatt.

Løsningen som departementet har falt ned på følger kjernen i Lysne II – utvalgets anbefaling. Imidlertid inneholder forslaget flere endringer i hvordan tilgangen til informasjon nærmere

innrettes og for organiseringen av kontrollmekanismene. Kripos støtter i denne sammenheng at det likevel ikke foreslås etablert særordninger for domstolskontroll og tilsyn på dette området, men at rettsikkerhetsgarantiene i stedet ivaretas av ordinær domstol og et styrket EOS-utvalg.[9]

3.1 Nærmere om rettslige rammer

I høringsnotatet gjøres grundig rede for utfordringer knyttet til eskaleringen av digitale trusler mot Norge og norske interesser.[10] Aktørene bak slike trusler inkluderer etter det opplyste både statlige etterretnings- og sikkerhetstjenester, terrorist- og ekstremistgrupper og organiserte hackergrupper. Per i dag anses etterretningsvirksomhet i statlig regi å utgjøre den mest alvorlige trusselen i det digitale rom, der angrep kan ramme både nasjonale beslutningsprosesser og utfordre samfunns- og statssikkerheten. Digitale kommunikasjonsplattformer brukes også til planlegging og koordinering av terrorhandlinger. Samtidig vises til at det stadig utvikles nye og sofistikerte metoder for nettverksoperasjoner. Departementet anser det alvorlig at norske myndigheter per i dag ikke er rustet til å avdekke og avverge de mest alvorlige truslene mot Norge i det digitale rom. I denne sammenheng vil imidlertid tilrettelagt innhenting gi Etterretningstjenesten mulighet til selvstendig og formålsrettet innhenting av kritisk informasjon, fra en helt sentral informasjonskilde man i dag er avskåret fra.

Etter Kripos' syn viser departementet og tidligere utredninger til tunge hensyn som underbygger behovet for å innføre en tilgang til grenseoverskridende elektronisk kommunikasjon også i Norge. Kripos har ikke noe informasjonsgrunnlag som tilsier en annen vurdering av den underliggende situasjonen som beskrives. Tvert imot er vi gjennom egne ansvarsområder oppmerksom på de utfordringer som utviklingen av kommunikasjonsteknologi medfører, i forhold til å kunne forebygge, avdekke, avverge eller etterforske alvorlig kriminalitet i det digitale rom.

En av statens grunnleggende oppgaver er å sikre landets suverenitet og innbyggernes sikkerhet. Den teknologiske utviklingen har imidlertid gjort både samfunns- og statssikkerheten mer sårbar. At vår etterretningstjeneste ikke er i stand til å avdekke, varsle og motvirke de alvorlige trusler det vises til, fremstår for Kripos som urovekkende, og synes å legge begrensninger på tjenestens evne til å løse sitt samfunnsoppdrag.

Samtidig er lovforslaget utfordrende i et personvern- og menneskerettighetsperspektiv. Grunnloven og EMK setter skranker for lovgivers handlingsrom. Tiltaket vil angå kommunikasjonen til svært mange mennesker, uavhengig av mistankegrunnlag eller relevans for etterretningsformål, og uansett tekniske løsninger for filtrering. Grunnleggende hensyn må derfor balanseres, der det stilles krav til rettslige rammer og forholdsmessighet. Av betydning for vurderingen vil blant annet være de rettssikkerhets- og kontrollmekanismer som etableres. Lysne II - utvalgets anbefalinger var da også betinget av et bestemt teknisk oppsett og etablering av et strengt kontrollregime.

Særlig retten til respekt for privatliv og kommunikasjon utgjør en sentral ramme for vurderingen av lovforslaget. I tillegg har tiltaket en side til ytrings- og informasjonsfriheten. Som departementet viser til er imidlertid ikke grunnlovsvernet her absolutt. Etter Høyesteretts

---

[9] Høringssvar fra Kripos til Lysne II – utvalgets rapport, s. 2
[10] Høringsnotatet pkt. 7.5.2.5 og 11.6

og EMDs praksis kan inngrep i vernet skje når dette har hjemmel i lov, har et legitimt formål og er forholdsmessig.

Kripos antar at det foreslåtte tiltaket vil kunne tilfredsstille de ulike sider av lovskravet. Som nevnt ovenfor under pkt. 2 mener vi imidlertid at grunnvilkårene for målsøking og målrettet innhenting generelt sett burde vært angitt mer presist. Konkret for tilrettelagt innhenting vil det ha direkte betydning for rettens mulighet til å ivareta en reel legalitetskontroll. Retten skal herunder prøve om bruken er i henhold til tjenestens oppgaver, oppfyller grunnvilkårene og ikke er uforholdsmessig.[11] Selv om departementet redegjør nærmere for vurderingstemaene, etterlates likevel et inntrykk av at den konkrete terskelen for bruk er for vanskelig tilgjengelig.

Kripos vil her også bemerke at tidsrammen for rettens tillatelser på inntil 1 år (målsøking) og 6 måneder (målrettet innhenting) fremstår for vid. Selv om tillatelse i henhold til bestemmelsen ikke skal gis for lengre tid enn nødvendig, vil lange tidsperioder uten domstolsprøving etter omstendighetene kunne svekke kontrollen med metodebruken.[12] Kripos mener også at retten "skal" oppnevne særskilt advokat ved alle begjæringer og ikke bare "kan" gjøre dette, slik lovforslaget legger opp til.[13]

3.2 Nærmere om delingsadgang for overskuddsinformasjon

Med utgangspunkt i Lysne II-utvalgets rapport drøfter departementet hvorvidt det bør oppstilles et helt eller delvis forbud mot deling av overskuddsinformasjon fra tilrettelagt innhenting.

Overskuddsinformasjon defineres som *"informasjon som er uten selvstendig interesse for etterretningsformål"*.[14] Hovedregelen i dag, og etter lovforslaget, gir Etterretningstjenesten adgang til å dele slike opplysninger med andre myndigheter hvis det er nødvendig for å bidra til mottakerens oppgaveløsning, og behandling anses forholdsmessig og sikkerhetsmessig forsvarlig.[15] Spørsmålet er altså om en særregulering av overskuddsinformasjon fra tilrettelagt innhenting skal innskrenke delingsadgangen.

Lysne II – utvalget fremhevet at reglene må redusere faren for misbruk av informasjon fra tilrettelagt innhenting. Utvalgets anbefaling var å lovfeste at Etterretningstjenesten skal slette all overskuddsinformasjon som stammer fra tilrettelagt innhenting. Fra utvalgets rapport inntas:[16]

> *"Utvalget vurderer at overskuddsinformasjon fra DGF bør slettes og ikke deles. Dette er viktig for å hindre formålsglidning. Utvalget anbefaler derfor at det for DGF lovfestes at all overskuddsinformasjon som ikke er relevant for E-tjenestens oppgaveløsning skal slettes. Klare instrukser og kontrollmekanismer må sikre at dette blir ivaretatt. Tiltaket vil sammen med øvrige tiltak bidra til at publikum vil ha tillit til at DGF ikke misbrukes for andre formål enn det informasjonstilgangen er ment for. I praksis vil dette si at dersom E-tjenesten – mot formodning og uten hensikt – skulle komme over informasjon om at en person har begått et drap, seksuelle overgrep mot barn eller deltatt i annen alvorlig kriminalitet som ikke er av relevans for E-*

---

[11] Høringsnotatet pkt. 9.5 og 11.11.4.3. Lovutkast §§ 7-1, 7-8 og 7-9, jf. § 8-4 og kap. 5
[12] Høringsnotatet pkt. 11.11.4.5. Lovutkast § 8-6, jf. § 8-1
[13] Høringsnotatet pkt. 11.11.4.4. Lovutkast § 8-5
[14] Lovutkastet § 1-4 nr. 10
[15] Lovutkastet § 10-8
[16] Lysne II-utvalgets rapport punkt 9.4.2 s. 60

tjenestens ansvarsområde, vil slik informasjon bli slettet uten videre oppfølging. Hensynet til rikets sikkerhet er viktigere enn å tillate bruk av denne overskuddsinformasjonen."

Som det fremgår var et sentralt hensyn for utvalget å hindre formålsglidning. Et delingsforbud kombinert med andre tiltak ville ifølge utvalget bidra til publikums tillit til at slik informasjon ikke blir misbrukt. Samtidig ble det vist til at hensynet til rikets sikkerhet er viktigere enn å tillate bruk av overskuddsinformasjon.

Kripos var i sitt høringssvar til rapporten kritisk til flere av utvalgets vurderinger. Generelt ble utvalgets beskrivelser av politiets virksomhet oppfattet som mangelfulle, særlig i forhold til forståelsen av politiets oppgaver knyttet til etterretning, forebygging, avverging og krisehåndtering.[17] Videre ble det særlig stilt spørsmål ved utvalgets anbefalinger om et absolutt delingsforbud sett i forhold til den aktivitetsplikt som følger av straffeloven §§ 196 og 226 samt barnevernloven § 6-4. Bestemmelsene gjelder uavhengig av taushetsplikt. Herunder fastsetter straffeloven § 196 en plikt til å anmelde eller på annen måte søke å avverge bestemte straffbare handlinger, eller følgene av disse.

I høringsnotatet uttaler departementet at deling av overskuddsinformasjon fra tilrettelagt innhenting, for å avverge at et straffbart forhold realiserer seg, eller der noens liv er i fare, kan hevdes ikke å være uttrykkelig drøftet av utvalget. Etter en fornyet gjennomgang er det imidlertid også departementets vurdering at faren for formålsglidning tilsier et strengt forbud mot deling av overskuddsinformasjon fra tilrettelagt innhenting. Erfaring skal vise at når informasjon først er innsamlet, kan det komme spørsmål om bruk til annet formål. Et forbud som derimot rendyrker utenlandsetterretningsformålet vil ifølge departementet gi et tydelig signal om at informasjonen ikke skal gjenbrukes til andre formål. Dette vil også motvirke et press på lovgiver om mulige fremtidige lovendringer.

Samtidig viser departementet til at enkelte rettslige forhold kan utfordre et absolutt forbud. I likhet med flere høringsinstanser trekkes frem den strafferettslige avvergingsplikten, prinsippet om at uskyldige ikke skal bli dømt og statens sikringsplikt. Herunder uttales at plikten etter straffeloven § 196 kan gi grunnlag for unntak, idet et absolutt delingsforbud kan gi uønskede utfall i enkeltsaker. Tungtveiende personvernhensyn gjør etter departementets syn at en delingsadgang i så fall må begrenses til å gjelde kun enkelte straffbare forhold.

På denne bakgrunn konkluderer departementet med at en delingsadgang kun skal omfatte straffbare forhold etter straffeloven kap. 17 og 18, og forutsatt at handlingen fortsatt kan avverges. Det vektlegges her at disse straffbare forholdene er nært beslektet med Etterretningstjenestens samfunnsoppdrag, noe som tilsier at opplysninger bør kunne deles selv om de viser seg ikke å ha tilknytning til utlandet.

Kripos er sterkt i mot at det - utover forholdene etter straffeloven kap. 17 og 18 - innføres et absolutt fritak fra i det hele tatt å vurdere om konkret informasjon utløser en aktivitetsplikt. Vårt prinsipielle utgangspunkt er, som ved høringen av Lysne II-utvalgets rapport, at kunnskap forplikter. Kryssende hensyn er ikke noe særegent for det digitale området generelt, eller for tilrettelagt innhenting konkret.

Aktivitetsplikten etter straffeloven § 196 bygger i denne sammenheng på helt sentrale hensyn i et samfunn. Personvernhensyn har her også en side til statens grunnleggende plikt til å

[17] Politiets oppgaver følger av politiloven § 2

beskytte sine borgere, og således ivaretakelse av «offerets personvern». Herunder setter Grunnloven, EMK og FNs barnekonvensjon krav til at myndighetene sikrer borgernes integritet og rettigheter. Alvorlige forhold vil forsterke en forventning om tiltak og oppfølgning. Herunder viser vi til uttalelse i Høyesterett i Rt-2013-588 om at EMK art. 1 *"....innebærer blant annet at staten har en plikt til, etter forholdene, å ta aktive skritt for å hindre at private krenker hverandre – konvensjonen har i denne forstand også horisontal virkning"*.

Barn er i en særstilling. Barn skal beskyttes. Vi finner her grunn til å minne om at barns sterke krav på beskyttelse blant annet fremgår av FN's barnevernkonvensjon og Grunnloven § 104 uten at det fremgår at departementet har hensyntatt dette i vurderingen av handleplikt når man kommer til kjennskap om barn som utsettes for overgrep. Kripos finner det så vel rettslig som etisk uholdbart at offentlige myndigheter skal kunne komme til kunnskap om eksempelvis pågående seksuelt misbruk av barn, for så å slette informasjonen uten videre oppfølgning.

Kripos er som nevnt enig i at eksistensen av betryggende prosessuelle rammer og kontrollmekanismer, egnet til å motvirke misbruk og vilkårlighet, er et sentralt element ved forholdsmessighetsvurderingen av tilrettelagt innhenting. Det er ikke tvilsomt at slik informasjonsinnhenting utelukkende må finne sted med utenlandsetterretningsformål. Vi er da også enig i at bruken av innhentet informasjon, som et utgangspunkt, må være begrenset av de samme formål. I en samlet vurdering kan Kripos imidlertid ikke se at lovforslagets innskrenking av delingsadgangen, og dermed aktivitetsplikten, verken er nødvendig for at ordningen med tilrettelagt innhenting anses forholdsmessig og kan innføres, eller er rettslig holdbar.

I denne sammenheng mener Kripos at kjernen i hensynet til formålsglidning er knyttet til selve informasjonsinnhentingen. En vurdering av risiko for formålsglidning ved sekundærbruk må da ta utgangspunkt i at informasjon det er snakk om å dele allerede vil være innhentet utelukkende med etterretningsformål. Innføringen av strenge rettssikkerhets- og kontrollmekanismer sikrer dette. Politiet vil således ikke ha noen innvirkning på hverken målsøking eller målrettet innhenting, eller noen kunnskap om hvilken overskuddsinformasjon som måtte eksistere.

Dermed vil heller ikke politiet ha noen forutsetning for å etterspørre informasjon fra tjenesten. Det anses da ikke treffende når departementet uttaler at et fremtidig press for tilgang til opplysninger underbygges ved at politiet i lang tid har ønsket seg ordinær datalagring fra elektronisk kommunikasjon til kriminalitetsbekjempelse. Likeså stilles spørsmål ved at departementet mener en slik risiko også synliggjøres av høringsuttalelser til utvalgets rapport fra Riksadvokaten, Politidirektoratet, PST og Kripos. At det i en høring fremmes et ulikt syn på vektingen av sentrale hensyn bør ikke gi grunnlag for en slik slutning. I denne sammenheng må det også kunne legges til grunn at involverte myndigheter opptrer ansvarlig, uavhengig av hvor grensen settes for delingsadgang. Samtidig vil forsøk på misbruk bli avdekket gjennom kontrollmekanismene som innføres.

Faren for formålsglidning må også vurderes i forhold til hvilket omfang av deling man kan stå ovenfor. I høringsnotatet understreker departementet at utlevering av overskuddsinformasjon sjelden eller aldri vil aktualiseres, ettersom innretningen av metoden nettopp har til hensikt å sikre at tjenesten får tilgang til etterretningsrelevant informasjon. Mengden av overskuddsinformasjon vil ifølge departementet derfor være svært begrenset. Tilsynelatende brukes dette som et argument for en restriktiv delingsadgang, ved at deling da uansett ikke vil ha særlig praktisk betydning. Etter Kripos' oppfatning er imidlertid dette vel så relevant for å

vurdere hensynet til formålsglidning. Om bruken av en delingsadgang i realiteten vil høre til sjeldenhetene, kan dette vanskelig ses å underbygge risikoen for formålsglidning i særlig grad.

Til sammenligning kan også vises til at bruk av denne typen innhenting i Sverige synes å ha et noe videre formål. I høringsnotatet viser departementet til at den svenske lovgivningen gir signaletterretningstjenesten (FRA) i oppgave å innhente opplysninger om *"other serious cross-border crimes that may threaten essential national interests"*, som ifølge departementet kan gjelde narkotikatrafikk og menneskesmugling.[18] Videre opplyses at det svenske sikkerhetspolitiet og enkelte andre deler av svensk politi kan gi FRA detaljerte oppdrag om innsamling. Etter departementets syn medfører denne forskjellen at lovforslaget vil gjøre risikoen for formålsglidning mindre i Norge.

Den svenske ordningen har vært undergitt prøving av EMD[19], der spørsmålet blant annet var om bulkinnsamling fra grenseoverskridende kommunikasjon for strategiske etterretningsformål innebar et brudd på EMK art. 8. Enkelte uttalelser fra domstolen indikerer en aksept for legitime formål utover det departementets drøftelse tar utgangspunkt i. Den konkrete rekkevidden av uttalelsene kan samtidig være usikre. Imidlertid synes domstolen å trekke inn flere typer alvorlig kriminalitet i sin vurdering av statenes informasjonsbehov og skjønnsmargin ved innføring av denne typen inngripende tiltak, ved at det vises til "*other serious crime, such as drug trafficking, human trafficking, sexual exploitation of children and cybercrime*"[20] *samt* "present-*day threats being posed by global terrorism and serious cross-border crime*".[21]

På denne bakgrunn mener Kripos samlet sett at departementet trekker hensynet til formålsglidning for langt, og at argumentasjon og premisser rundt selve risikoen ikke er treffende. Aktuell overskuddsinformasjon vil som nevnt allerede være innhentet med etterretningsformål, og det praktiske omfanget av deling vil være svært lite. Således synes dette hensynet å ha fått for stor vekt i forhold til hensynet til statens aktivitetsplikt ved positiv kunnskap om alvorlig og samfunnsskadelig kriminalitet. Etter dette kan Kripos ikke se at den foreslåtte begrensningen i delingsadgangen av overskuddsinformasjon er nødvendig for innføringen av tilrettelagt innhenting. Relevansen av Lysne II-utvalgets premiss om at hensynet til rikets sikkerhet er viktigere enn å tillate bruk av overskuddsinformasjon, synes således begrenset.

Etter Kripos' vurdering etablerer lovforslaget således en for snever adgang til deling av overskuddsinformasjon. Spørsmålet bør ikke være om ytterligere informasjon bør kunne deles, men hvilke øvrige straffbare forhold som kvalifiserer, hvordan informasjonsdelingen kan skje og til hvilken bruk. Faren for misbruk og vilkårlighet vil kunne motvirkes ved utforming av et klart hjemmelsgrunnlag for bruk av delingsadgangen, og kontrollordninger med hvilken overskuddsinformasjon som faktisk deles.

Den nærmere avgrensingen av kvalifiserte straffbare forhold kan imidlertid være vanskelig å fastsette. Til sammenligning har flere av forholdene i straffeloven kap. 17 lav strafferamme. Utgangspunktet for nærmere grensedragning bør imidlertid være alvorlig kriminalitet mot en persons liv, helse eller frihet. Man kan ikke – etter Kripos' vurdering – lovfeste en hovedregel

---

[18] Høringsnotatet s. 219
[19] Centrum for rättvisa mot Sverige avsagt 19. juni 2018. Omtalt i høringsnotatet pkt. 11.8.2.5
[20] Avsnitt 112
[21] Avsnitt 179

som innebærer at offentlige tjenestemenn er avskåret fra å varsle relevante myndigheter om de groveste brudd på straffeloven kap. 24 (vern av personlig frihet og fred), kap. 25 (voldslovbrudd mv) eller kap. 26 (seksuallovbrudd). Dette vil stride mot den beskyttelse borgerne har krav på og i alminnelighet vil forvente, det vil være etisk vanskelig å forsvare og vil utfordre tillitten til myndighetene generelt.

I praksis kan det forøvrig fremstå usikkert om det konkrete skillet mellom terrorhandlinger og drap er hensiktsmessig. Hva som etter omstendighetene kvalifiserer som en forestående terrorhandling, i motsetning annen alvorlig handling mot noens liv eller helse, kan være vanskelig å fastslå. Eksempelvis kan her nevnes såkalt skoleskyting. Her kan det ha betydning hvor nært man er selve utførelsen samt det nærmere innholdet i opplysningene. Det kan gi uheldige utslag dersom informasjon ikke deles med politiet basert på uklarhet om handlingen ville oppfylle de strafferettslige vilkår for terrorhandling.

Hvordan delt informasjon skal brukes vil også kunne ha betydning for den nærmere grensedragningen. Som Kripos har vist til tidligere, vil avverging og skadereduksjon være viktigere enn straffeforfølgning ved bruk av opplysninger. Flere av politiets oppgaver løses utenfor det straffeprosessuelle sporet. Også i etterforskning har man hjemler for å beskytte sensitiv informasjon. På denne bakgrunn kan man tenke seg at overskuddsinformasjon i mange situasjoner kun vil brukes til å avverge eller stanse pågående kvalifiserte straffbare forhold.

Også den foreslåtte delingsadgangen knyttet til straffeloven kap. 17 og 18 forutsetter som kjent at handlingen kan avverges. Samtidig kan en slik forutsetning etter Kripos' syn være krevende å praktisere, uten nærmere kriterier. Hvorvidt avverging er mulig kan etter omstendighetene være uklart. Eksempelvis kan et terroranslag være det første i rekken av flere planlagte aksjoner. Når det gjelder seksuelle overgrep mot barn vil dette ofte være pågående virksomhet over tid. Gjentakelsesfaren vil også fort være så stor at det gir liten mening å skille mellom behovet for å følge opp pågående eller avsluttede forhold.

Avslutningsvis gjentas at det for Kripos er åpenbart at opplysninger om alvorlig kriminalitet mot en persons liv, helse eller frihet må følges opp. Spørsmålet er hvordan dette best kan gjennomføres. Utgangspunktet for en løsning vil naturlig være forslaget til unntaksbestemmelse som allerede foreligger. Deling vil kunne ha som formål å avverge eller stanse en pågående straffbar virksomhet, herunder inngå som grunnlag for metodebruk.

Det stilles imidlertid spørsmål ved om alternative løsninger og kriterier burde vært noe mer utredet av departementet, med fokus på hvilke straffbare forhold som bør kvalifisere, samt hvordan og til hvilken bruk informasjonsdeling kan skje. Departementets drøftelser har i stor grad har rettet seg mot selve faren for formålsglidning ved sekundærbruk.

Flere av de samme hensyn gjelder også for spørsmålet om en delingsadgang i henhold til plikten etter straffeloven § 226. Bestemmelsen bygger på grunnleggende hensyn i en rettsstat, og er forankret i Grunnloven § 95 og EMK art. 6. Igjen stilles spørsmål ved om man kan lovregulere seg bort fra en plikt til å avverge justismord. Uavhengig av dette er spørsmålet som ovenfor om et lovforbud mot deling i slike tilfeller er nødvendig for å motvirke formålsglidning. Et klart hjemmelsgrunnlag for deling, kombinert med foreslåtte kontrollordninger, vil kunne bidra til trygge rammer og motvirke misbruk og vilkårlighet.

3.3 Bevisforbud for opplysninger fra tilrettelagt innhenting

Departementet foreslår at det lovfestes et forbud mot å bruke opplysninger fra tilrettelagt innhenting som bevis i straffesaker.

Forslaget omhandler all informasjon fra tilrettelagt innhenting, både delt overskuddsinformasjon og delt informasjon med etterretningsverdi i henhold til utenlandsetterretningsformålet. Eksempelvis ved at man har delt informasjon med politiet om en terrortrussel mot Norge med tilknytning til utlandet.

En lovfesting av bevisforbud er i henhold til anbefalingene fra Lysne II-utvalget. Departementet viser til at høringen av utvalgets rapport frembrakte ulike syn på et bevisforbud. Etter departementets vurdering er det spesielt hensynet til å motvirke formålsglidning som tilsier bevisforbud i straffesaker, idet en åpning for dette anes å kunne føre til press for å benytte tilgangen i etterforskningen av straffbare handlinger. Det sentrale anførte hensyn er således tilsvarende som for spørsmålet om deling av overskuddsinformasjon.

Som bemerket ovenfor, vil opplysninger som er delt og aktuelle som bevis allerede være innhentet med utenlandsetterretningsformål, og politiet vil ikke ha hatt noen innvirkning på denne fasen. Med unntak av overskuddsinformasjon, vil aktuelle opplysninger også være vurdert til å ha etterretningsverdi i henhold til tjenestens oppgaver.

Kripos kan ikke se at en adgang til å bruke opplysninger som bevis medfører særlig økt fare for formålsglidning, dersom vilkårene for deling først er oppfylt. Tilsvarende anses ikke en slik begrensning nødvendig for å styrke tilliten til at metoden og informasjonen ikke misbrukes. Igjen forutsettes at de foreslåtte kontrollmekanismer vil kunne ivareta dette. Således fremstår et bevisforbud heller ikke nødvendig for at ordningen med tilrettelagt innhenting kan anses forholdsmessig og innføres.

Det foreslåtte bevisforbudet har en klar side til kriminalitetsbekjempelse. Kripos' prinsipielle utgangspunkt er at delt informasjon fra tilrettelagt innhenting også bør kunne benyttes som bevis i straffesaker. Manglende oppklaring og iretteføring av alvorlig kriminalitet som følge av begrensninger i bruken av opplysninger, er også egnet til å svekke tilliten til både politiet, domstolen og myndighetsapparatet. Prinsippet om fri bevisføring og hensynet til sakens opplysning, innebærer at påtalemyndigheten bør kunne føre de bevis man har. Dette vil bidra til en riktig avgjørelse og straffereaksjon.

I denne sammenheng bemerkes også at hovedbegrunnelsen for straff er dens individuelle og allmennpreventive virkning. Straffeforfølgning kan noen ganger være det beste virkemiddelet for å beskytte samfunnet mot trusler som også begrunner innføringen av tilrettelagt innhenting. Det ville herunder være lite formålstjenlig med tanke på samfunnsbeskyttelsen dersom en terrorist skulle frifinnes som følge av at informasjon fra tilrettelagt innhenting ikke kunne benyttes som bevis. I denne sammenheng kan det være grunn til å minne om reaksjonen forvaring. Forvaringsordningens formål er å beskytte samfunnet, og dette vil kunne være den mest relevante reaksjon på de trusler som behovet for tilrettelagt innhenting begrunnes i.

Etter dette er Kripos standpunkt at delt informasjon fra tilrettelagt innhenting også bør kunne benyttes som bevis i straffesak, i hvert fall i de alvorligste sakene.

Alternative tilnærminger og mulige kriterier synes også her å kunne vært noe mer utredet, også med utgangspunkt i hvordan andre land har lovregulert dette. Dette ville gjort det enklere å vurdere forskjellige løsninger.

4. Merknader til enkelte bestemmelser i lovutkastet

Til § 1-2 tredje ledd:
Det fremstår unødvendig å fastslå at loven gjelder i «fred, krise og væpnet konflikt». Så vidt vi forstår vil dette omfatte alle situasjoner. Det er begrensinger i dette utgangspunkt som eventuelt måtte fremgå av loven.

Til § 1-3:
Hele § 1-3 fremstår etter Kripos syn lite hensiktsmessig. Det grunnleggende forhold til folkeretten er ivaretatt gjennom Grunnloven og menneskerettslova. Utover det bør man kanskje være forsiktig med å lovfeste folkerettslige begrensinger. Det ligger i etterretningstjenestens natur at den vil kunne måtte operere i et grenseland her. Videre vil vi fremheve at det uklart hva som ligger i begrepet "*reell risiko*" for at ufravikelige og andre grunnleggende menneskerettigheter krenkes, og hva som ligger i kravet til å "*medvirke*". Det antas at dette vil kunne ha konkret betydning for muligheten til samarbeid med andre tjenester. Ut i fra formuleringen kan motsetningsvis også spørres hvilke grunnleggende menneskerettigheter man mener eventuelt kan fravikes.

Til § 1-4:
Det fremstår fornuftig å flytte definisjonen av "personopplysninger" fra nr. 11 til nr. 1, da denne definisjonen bør komme forut for definisjonen av "behandling av personopplysninger". Det tilføyes at definisjonen av "personopplysning" bør være identisk med definisjonen av dette begrepet i personvernforordningen artikkel 4 nr. 1, eventuelt den som fremgår av politiregisterloven § 2 nr. 1.

Det bemerkes videre at det bør søkes å finne et treffende norsk ord for begrepet "bulk". Definisjonen er etter vår vurdering uheldig. En definisjon skal fortrinnsvis angi positivt hva som menes med begrepet, og definisjonen bør derfor legges tettere på beskrivelsen i høringsnotatet.

Det bør vurderes om også "organisasjon" bør inngå i nr. 4.

Til § 4-3:
En egen bestemmelse som nedsetter et forbud mot industrispionasje er overflødig ved siden av angivelsen og begrensningen av Etterretningstjenestens oppgaver i utkastet § 3-1 og 3-2. Å se behov for positivt å forby tjenesten å tjene et åpenbart usaklig, antagelig ulovlig, formål underbygger på ingen måte troverdighet for at man vil innrette seg etter de formålsbegrensinger som ligger i loven ellers.

Til § 4-4:
Her gjelder det tilsvarende. Bestemmelsen er overflødig idet den ikke gir mer enn hva som ellers følger av lovens formålsbegrensning og gjeldende regelverk rundt Forsvarets bistand til politiet.

Til § 5-3:
Det fremgår av bestemmelsen at alle søk i rådata i bulk skal logges for kontrollformål, jf. annet ledd. Kripos bemerker at det positivt bør fremgå en plikt til å gjennomgå loggene regelmessig med det formål å avdekke uautorisert tilgang til opplysningene. Det vises i den forbindelse til utformingen av politiregisterforskriften § 40-13. Bakgrunnen for dette er at en ren stikkprøvekontroll hverken vil være effektiv eller innebære et element av reell kontroll med behandlingen. Ordlyden bør videre endres til at "hver bruk av opplysninger" skal logges, ikke bare søk. Det bemerkes videre at det er vanlig å angi hva opplysninger om bruk av systemet skal brukes til, se f.eks. politiregisterloven § 17.

Til § 6-1 første ledd, siste punktum:
At «Metodebruk skal avsluttes dersom det blir klart at vilkårene etter loven her ikke lenger er tilstede.» er etter vår vurdering et så selvsagt utgangspunkt at det ikke bør lovfestes.

Til § 6-3 andre ledd:
Her bør det foretas en presisering av hva som menes med «infiltrasjon» og «provokasjon». Skal disse begrepene forstås tilsvarende som i polisiær sammenheng? Hva innebærer det at slik virksomhet kan «inkluderes» i menneskebasert innhenting? Er dette et forsøk på å hjemle aktivitet som ellers ville være ulovlig?

Til § 7-7:
Til tredje ledd bemerkes det at ordlyden slettes "etter" 18 måneder er uheldig, og det bør settes inn "senest etter" for å gi bestemmelsen meningsinnhold.

Til § 8-7:
Det stilles spørsmål ved om annet ledd er overflødig sett i lys av at sikkerhetsloven gjelder for behandling av graderte opplysninger.

Til § 8-9:
Kripos forstår ikke begrunnelsen for at ikke domstolen skal kunne bestemme oppsettende virkning.

Til § 9-4:
Diskrimineringsforbudet i utkastets § 9-4 synes å ha tatt utgangspunkt i den tidligere definisjonen av sensitive personopplysninger i daværende personopplysningslov § 2 nr. 8. Det bemerkes at personvernlovgivningen nå opererer med begrepet særlige kategorier personopplysninger, som blant annet også omfatter genetiske og biometriske opplysninger. Det bør sees hen til personvernforordningen artikkel 9 og politiregisterloven § 7 ved utformingen av denne bestemmelsen.

Til § 9-5:
Ved utformingen av bestemmelsen bør det sees hen til det alminnelige nødvendighetsprinsippet i personvernlovgivningen, som formuleres slik at opplysninger kun kan behandles når det er nødvendig for å oppnå formålet med behandlingen.

Til annet ledd bemerkes det at begrepet "distribuert" bør erstattes med det allerede innarbeidede begrepet "utlevert".

Til § 9-7:
Det bemerkes at bestemmelsen slik den nå er utformet ikke gir noen føringer for behandlingen. Det må i så fall oppstilles et krav om at E-tjenesten innenfor en viss tidsfrist må søke å avklare hvorvidt vilkårene i §§ 9-2, 9-5 og 9-6 er oppfylt. Til sammenligning oppstiller politiregisterloven § 8 en tidsfrist på fire måneder. I høringsnotatets punkt 12.6.2.3 argumenteres det med at en tilsvarende frist hverken er hensiktsmessig eller praktisk fordi metodikken er annerledes enn politiets og fordi det vil kreve en økning i antall ansatte. Det er vanskelig å se at denne begrunnelsen fører til at det ikke kan oppstilles noen krav med hensyn til når kravene senest må være avklart. Slik bestemmelsen nå er utformet fremstår den som et generelt unntak fra formålsbestemthet og nødvendighet.

Til § 9-8:
Bestemmelsen definerer begrepet kvalitet til å omfatte et krav om at opplysningene skal være "korrekte og oppdaterte". Kripos bemerker i den sammenheng at kravet til kvalitet som hovedregel omfatter mer, herunder at opplysningene skal være tilstrekkelige og relevante for formålet med behandlingen, og ikke lagres lenger enn nødvendig ut fra formålet med behandlingen. Se eksempelvis politiregisterloven § 6 og personvernforordningen artikkel 5 nr. 1 bokstav c og d.

Det følger av annet ledd at det skal fremgå av Etterretningstjenestens produkter dersom ikke-verifiserte personopplysninger er behandlet. Det bør videre oppstilles et krav om at dette fremgår også når det utleveres opplysninger. Til sammenligning nevnes politiregisterforskriften § 11-4 annet ledd nr. 5.

Til § 9-9:
Kripos stiller spørsmål ved begrunnelsen for en lagringstid på 15 år for opplysninger som etter definisjonen i utkastets § 2 nr. 2 primært inneholder opplysninger som antas å være irrelevante for etterretningsformål. Til annet ledd bemerkes det at det heller bør defineres hva sletting er, ikke hva det ikke er. Til sammenligning vises det til politiregisterforskriften § 16-2.

Til § 9-12:
Kripos foreslår at ordlyden endres til: "Etterretningstjenesten skal peke ut en personvernrådgiver..." for å forenkle ordlyden i bestemmelsen. Til tredje ledd stilles det spørsmål ved om det er hensiktsmessig å begrense kretsen som kan stille personvernrådgiver spørsmål til interne.

Til § 10-2:
Kripos bemerker for ordens skyld at en utlevering av opplysninger fra behandlingsansvarlig som er underlagt personopplysningsloven må oppfylle kravene i personvernforordningen artikkel 6, og eventuelt artikkel 9 for en utlevering av særlige kategorier personopplysninger. Da henvisninger til forordningen er fraværende i høringsnotatets omtale av utlevering stiller Kripos spørsmål ved om dette har vært et vurderingstema.

Til § 10-5:
Det foreslås at det sees hen til ordlyden i politiregisterforskriften § 11-4 ved utarbeidelsen av denne bestemmelsen.

Til § 11-4:
Det kan vurderes om det er hensiktsmessig å definere begrepet "tjenstlig behov".

Til § 12-1:
Kripos kan ikke se at bestemmelsen er nødvendig idet disse forhold allerede er straffebelagt.

Til § 12-2:
Etter sin ordlyd fremstår bestemmelsen som meningsløs. At man ikke kan straffes for en lovlig tjenestehandling er åpenbart. Begrepet straffrihet brukes der man skal fritas for straff for en i utgangspunktet straffbar handling. Vi antar at tanken har vært å påpeke at den omstendighet at noe utføres som ledd i en offentlig tjenestehandling kan gjøre at en ellers straffbar handling er lovlig. Denne bestemmelsen er imidlertid ikke på noen måte egnet til å fastlegge nærmere rammene for hva som er en lovlig tjenestehandling. Når departementet begrunner forslaget i at man vil minne *«rettsanvenderen om at straffebud tidvis må tolkes innskrenkende"*, fremstår det uforståelig. At det i alle straffebud skal innfortolkes en rettstridsreservasjon følger av alminnelig strafferett. En eventuell bekymring hos departementet for om domstolene er innforstått med denne reservasjonen fremtrer ubegrunnet, og kan uansett ikke begrunne en slik regel.

Dersom forslaget er ment å berolige ansatte i (og kilder for) etterretningen om at forhold som ellers ville være straffbare kan være lovlige når de begås som ledd i offentlig tjenestehandlinger, må andre "kommunikasjonsmidler" enn lovtekst benyttes. Tilsvarende vil forøvrig også gjelde for andre, herunder ansatte i politiet.

Med hilsen

for **Ketil Haukaas**

Saksbehandler:
Espen H. Hanken
politiadvokat
Telefon: +47 23 20 80 00

Kopi: Det nasjonale statsadvokatembetet