EOS-UTVALGET

STORTINGETS KONTROLLUTVALG
FOR ETTERRETNINGS-, OVERVÅKINGS- OG SIKKERHETSTJENESTE

ÅRSMELDING 2018

DOKUMENT 7:1 (2018–2019)

Foto: Katja Kircher/ Maskot / NTB scanpix

Til Stortinget

I henhold til lov 3. februar 1995 nr. 7 om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-kontrolloven) § 17 tredje ledd avgir utvalget melding til Stortinget om sin virksomhet i 2018.

Årsmeldingen er ugradert, jf. EOS-kontrolloven § 17 tredje ledd. Hvorvidt informasjonen er sikkerhetsgradert skal etter sikkerhetsloven avgjøres av den som har utstedt informasjonen. Før meldingen avgis til Stortinget, sender vi de respektive delene av meldingsteksten til tjenestene for at de skal avklare om meldingen følger dette kravet. Tjenestene er også gitt anledning til å kontrollere at det ikke er feil eller misforståelser i teksten.

Oslo, 27. mars 2019

Eldbjørg Løwer

Svein Grønnern

Theo Koritzinsky

Øyvind Vaksdal

Håkon Haugli

Inger Marie Sunde

Eldfrid Øfsti Øvstedal

Henrik Magnusson

Foto: Ingar Sørensen

Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste i 2018. Fra venstre: Inger Marie Sunde, Håkon Haugli, Eldfrid Øfsti Øvstedal, Theo Koritzinsky, Eldbjørg Løwer (leder), Svein Grønnern (nestleder) og Øyvind Vaksdal.

Innhold

1. Utvalgets mandat og sammensetning

EOS-utvalget er et permanent, stortingsoppnevnt organ som kontrollerer norske virksomheter som utøver etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-tjeneste). Kontrollen gjelder bare EOS-tjeneste som utøves, styres eller settes i gang av offentlige forvaltning.[1]

Formålet med kontrollen er etter EOS-kontrolloven[2] § 2 første ledd å:

1. klarlegge om og forebygge at noens rettigheter krenkes, herunder påse at det ikke nyttes mer inngripende midler enn det som er nødvendig etter forholdene, og at tjenestene respekterer menneskerettighetene,
2. påse at virksomheten ikke utilbørlig skader samfunnets interesser, og
3. påse at virksomheten holdes innen rammen av lov, administrative eller militære direktiver og ulovfestet rett.

Utvalget skal i sin kontroll ta hensyn til rikets sikkerhet og forholdet til fremmede makter.[3] Vi skal ikke søke et mer omfattende innsyn i sikkerhetsgraderte opplysninger enn det som er nødvendig ut fra kontrollformålene[4], og vi skal så vidt mulig ta hensyn til kildevernet og vern av informasjon mottatt fra utlandet. Kontrollen med enkeltsaker og operasjoner skal være etterfølgende, men vi har rett til å bli informert om tjenestenes løpende virksomhet. Utvalget kan ikke instruere EOS-tjenestene eller brukes til konsultasjoner. Kontrollen skal være til minst mulig ulempe for tjenestenes operative virksomhet.[5]

Det er sju medlemmer i utvalget. Medlemmene velges for et tidsrom på inntil fem år av Stortinget i plenum etter innstilling fra Stortingets presidentskap.[6] Det oppnevnes ikke vara-medlemmer. Etter en lovendring i 2017 kan medlemmene gjenoppnevnes én gang og maksimalt ha vervet i ti år.

Utvalget er uavhengig av både regjeringen og Stortinget.[7] Vi kan derfor ikke instrueres av regjeringen, og medlemmer av utvalget kan ikke samtidig være stortingsrepresentanter. Utvalget har en variert sammensetning, der både ulik politisk bakgrunn og erfaring fra andre samfunnsområder er representert. Utvalgets medlemmer og ansatte i sekretariatet må ha sikkerhetsklarering og autorisasjon for høyeste nivå både nasjonalt og etter traktat Norge er tilsluttet.[8] Det vil si sikkerhetsklarering og autorisasjon for henholdsvis STRENGT HEMMELIG og COSMIC TOP SECRET.

1 Det er bestemmelser som viser til EOS-kontrolloven i lov 20. mars 1998 nr. 10 om forebyggende sikkerhet (sikkerhetsloven) § 30, lov 20. mars 1998 nr. 11 om Etterretningstjenesten (e-loven) § 6, instruks 29. april 2010 nr. 695 om sikkerhetstjeneste i Forsvaret § 14 og lov 28. mai 2010 nr. 16 om behandling av opplysninger i politi og påtalemyndigheten (politiregisterloven) § 68.

2 Lov 3. februar 1995 nr. 7 om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-kontrolloven). Loven ble sist endret i juni 2017.

3 Jf. EOS-kontrolloven § 2 andre ledd.

4 Jf. EOS-kontrolloven § 8 tredje ledd. Av EOS-kontrolloven § 8 fjerde ledd fremgår det at utvalget kan fatte bindende beslutning om innsynsretten og om kontrollens utstrekning. Eventuell protest skal inntas i årsmeldingen, og det vil da være opp til Stortinget å mene noe om tvisten, etter at innsyn er gitt som anmodet (ingen oppsettende virkning). I 1999 vedtok Stortinget ved plenarvedtak at det skulle gjelde en særskilt prosedyre for tvist om innsyn i Etterretningstjenestens dokumenter. Vedtaket førte ikke til endring i utvalgets lov eller instruks, se Dokument nr. 16 (1998-99), Innst. S. nr. 232 (1998-99) og referat og vedtak i Stortinget 15. juni 1999. Bakgrunnen for Stortingets vedtak fra 1999 er den særlige sensitiviteten som knytter seg til enkelte av E-tjenestens kilder, identiteten til personer i okkupasjonsberedskapen og spesielt sensitive opplysninger mottatt fra utenlandske samarbeidende tjenester. EOS-utvalget ba i 2013 Stortinget avklare om utvalgets innsynsrett slik den er nedfelt i lov og instruks skal gjelde fullt ut også for E-tjenesten, eller om Stortingets vedtak fra 1999 skal opprettholdes. På Stortingets anmodning ble spørsmålet behandlet i rapporten fra Evalueringsutvalget for EOS-utvalget, som ble avgitt til Stortinget 29. februar 2016, se Dokument 16 (2015-2016). Ved behandlingen av rapporten fra Evalueringsutvalget i 2017, ble begrensningen i innsynet i «særlig sensitiv informasjon» opprettholdt, men uten at lovteksten ble endret.

5 Jf. EOS-kontrolloven § 2.

6 Jf. EOS-kontrolloven § 3.

7 Stortinget i plenum kan «likevel pålegge utvalget å foreta nærmere definerte undersøkelser innenfor utvalgets kontrollmandat», jf. EOS-kontrolloven § 1 siste ledd andre punktum.

8 Jf. EOS-kontrolloven § 11 andre ledd.

Ulovfestet rett
Ulovfestet rett er gjeldende rett som ikke er lovfestet. Den skapes gjennom praksis, dels gjennom domstolsavgjørelser, men også sedvanerett.

Sikkerhetsgraderte opplysninger
Informasjon som etter reglene i sikkerhetsloven skal beskyttes av sikkerhetsmessige grunner. Informasjonen merkes med en sikkerhetsgrad, for eksempel KONFIDENSIELT.

Sikkerhetsklarering
Avgjørelse av en klareringsmyndighet om en persons antatte sikkerhetsmessige skikkethet for en angitt sikkerhetsgrad.

Autorisasjon
Avgjørelse om sikkerhetsklarert person skal gis tilgang til informasjon med en angitt sikkerhetsgrad.

Under følger en oversikt over utvalgets sammensetning og medlemmenes funksjonsperioder:

Eldbjørg Løwer, Kongsberg, leder
1. juli 2011 – 30. juni 2019

Svein Grønnern, Oslo, nestleder
13. juni 1996 – 30. juni 2021

Theo Koritzinsky, Oslo
24. mai 2007 – 30. juni 2019

Håkon Haugli, Oslo
1. januar 2014 – 30. juni 2021

Øyvind Vaksdal, Karmøy
1. januar 2014 – 30. juni 2021

Inger Marie Sunde, Bærum
1. juli 2014 – 30. juni 2019

Eldfrid Øfsti Øvstedal, Trondheim
1. juli 2016 – 30. juni 2021

Av dagens sju medlemmer har fem ulik partipolitisk bakgrunn. De to øvrige har juridisk og teknologisk faglig bakgrunn. Den brede sammensetningen bidrar til å styrke utvalgets kompetanse og legitimitet.

Vi støttes av et sekretariat. Ved utgangen av 2018 bestod sekretariatet av 14 personer i fulltidsstillinger – sekretariatsleder (jurist), seks juridiske saksbehandlere, tre teknologer, én sikkerhetsleder, én informasjonsrådgiver og to administrativt ansatte.

2.

Oversikt over utvalgets virksomhet i 2018

2.1 Sammendrag – hovedpunkter i kontrollen med tjenestene

EOS-utvalget har som sin viktigste oppgave å «klarlegge om og forebygge at noens rettigheter krenkes». Det gjør utvalget blant annet ved å kontrollere om PSTs registrering av personer er i samsvar med loven, om E-tjenesten ikke bryter forbudet mot å overvåke norske personer som oppholder seg i Norge og om saker om sikkerhetsklarering er behandlet på en rettssikker og rettferdig måte.

Politiets sikkerhetstjeneste (PST):

- PST har i en stor andel saker overlevert informasjon til klareringsmyndigheter på muntlig vis uten å dokumentere det skriftlig. Dette er et brudd på loven.
- Ved ett tilfelle har PST registrert opplysninger om politisk engasjement og utlevert det til en klareringsmyndighet. Dette er forbudt og utvalget kritiserte tjenesten.
- PST utleverte opplysninger til en klareringsmyndighet om at en person som skulle sikkerhetsklareres tilhørte det PST kaller et «ekstremt miljø med voldspotensiale». Men personen tilhørte ikke dette miljøet.
- Utvalget har kritisert PST for å innhente en chatlogg på ulovlig grunnlag.
- PST meldte inn to avvik til utvalget. Ett av dem gjaldt skjult kameraovervåking der et kamera ble slått av ni dager etter at rettens tillatelse utløp.

Nasjonal sikkerhetsmyndighet (NSM):

- I en klagesak har ikke NSM rettet seg etter utvalgets anbefaling om å gi en klager innsyn i korrespondanse mellom NSM og utvalget. Utvalget mener dette er beklagelig.
- NSM har krenket en klagers rettigheter ved å la personen gå gjennom en klareringsprosess uten at det var grunnlag for det. Personen fikk først konklusjonen «INGEN KLARERING» og det fikk negative følger for klageren.
- Utvalget har ferdigstilt prosjektet om sikkerhetsklarering av personer som har tilknytning til andre stater. Det har resultert i en særskilt melding til Stortinget.

Etterretningstjenesten:

- E-tjenesten mente de hadde hjemmel til å gå gjennom informasjon som stammer fra kommunikasjon mellom personer i Norge, selv om den var samlet inn i strid med loven. EOS-utvalget konkluderte på prinsipielt grunnlag med at E-tjenesten ikke har lov til dette. Utvalget fant ikke at E-tjenesten faktisk har gjort dette.
- Det knytter seg begrunnet tvil til lovligheten av tjenestens innhenting av informasjon fra åpne kilder om norske personer mens de oppholder seg i Norge.
- Utvalget har brukt mye tid på å jobbe med høringssvaret til Forsvarsdepartementets forslag om ny Lov om Etterretningstjenesten. Høringssvaret følger som vedlegg 3.

Annen EOS-tjeneste:

- Utvalget har kritisert Riksrevisjonen for ikke å gi dem som blir nektet sikkerhetsklarering en begrunnelse for vedtaket.

2.2 Utført kontrollvirksomhet

Utvalgets kontrollvirksomhet kan deles inn i tre hovedkategorier. For det første gjennomfører vi stedlige inspeksjoner i EOS-tjenestene. For det andre undersøker vi og uttaler oss om enkeltsaker. Slike saker er gjerne et resultat av problemstillinger vi har avdekket i inspeksjonene. For det tredje behandler vi klager fra enkeltpersoner.

Etter endringen av EOS-kontrolloven i 2017 stilles det krav om at utvalget gjennomfører minst 13 inspeksjoner årlig.

I 2018 har utvalget gjennomført 20 inspeksjoner og vært alle steder som loven krever. Politiets sikkerhetstjeneste (PST) er inspisert 7 ganger, Etterretningstjenesten (E-tjenesten) 4 ganger, Nasjonal sikkerhetsmyndighet (NSM) 2 ganger og Forsvarets sikkerhetsavdeling (FSA) 2 ganger. Etterretningsbataljonen, Nasjonal kommunikasjonsmyndighet, Forsvarets spesialkommando, Telia Norge AS og Felles cyberkoordineringssenter er inspisert én gang hver.

Utvalget kan i all hovedsak gjennomføre inspeksjoner direkte i tjenestenes elektroniske systemer. Dette innebærer at inspeksjonene inneholder betydelig uanmeldte elementer. Hvilken informasjon som kontrolleres er ikke kjent for tjenestene før vi stiller muntlige spørsmål i en inspeksjon, eller retter skriftlige henvendelser til tjenestene om funn etter en inspeksjon. Det ble i 2018 gjennomført én inspeksjon med kort varsel – av PST-kontoret ved Oslo lufthavn Gardermoen.

For å gjøre utvalgets kontroll målrettet og effektiv, gjør sekretariatet grundige forberedelser i tjenestene. Inspeksjonsforberedelser er ressurskrevende, og forbere-

Klareringsmyndighet
Offentlig organ som har myndighet til å avgjøre om en person skal få sikkerhetsklarering.

delsene er stadig styrket de siste 10 årene. I 2018 ble en ny milepæl nådd ved etableringen av en teknologisk enhet i sekretariatet. Les mer om dette i punkt 3.1.

I 2018 opprettet utvalget 22 saker av eget tiltak, mot 31 i 2017. Sakene utvalget har tatt opp på eget tiltak er hovedsakelig oppfølging av funn fra utvalgets inspeksjoner. Utvalget avsluttet i 2018 22 saker som var tatt opp av eget tiltak, mot 30 saker i 2017. Sakene som ble undersøkt i 2018 har generelt vært mer arbeidskrevende enn sakene i 2017.

Utvalget undersøker klager fra enkeltpersoner og organisasjoner. Det kom inn 19 klager på EOS-tjenestene i 2018, mot 26 klager i 2017.[9] Klager som faller inn under utvalgets kontrollområde undersøkes i den eller de tjenestene som klagen retter seg mot. Utvalget har en lav terskel for å ta klagesaker til behandling.

Utvalgets medlemmer møtes flere dager hver måned, med unntak av juli. Vervet som leder tilsvarer opp mot 30 prosent stilling og medlemsvervet opp mot 20 prosent stilling. Vi har i 2018 hatt 12 interne arbeidsmøter på utvalgets kontor, i tillegg til interne arbeidsmøter på stedet i tilknytning til inspeksjonene. I disse møtene drøfter vi planlagte og gjennomførte inspeksjoner. Utvalget behandler i møtene også klagesaker, saker tatt opp av eget tiltak, meldinger til Stortinget og administrative forhold.

EOS-tjenestene har gjennomgående vist forståelse for vår kontroll. Erfaringene har vist at kontrollen bidrar til å sikre enkeltindividets rettssikkerhet – og til å skape tillit i befolkningen til at tjenestene opererer innenfor sine rettslige rammeverk.

EOS-utvalgets leder Eldbjørg Løwer overleverte 10. april årsmeldingen for 2017 til stortingspresident Tone Wilhelmsen Trøen.
Foto: Stortinget

9 Noen av klagene er rettet mot flere av tjenestene samtidig.

3.

Utviklingstrekk, rammebetingelser og internasjonalt kontrollsamarbeid

3.1 Sekretariatets teknologiske enhet er styrket, men mangler fortsatt ressurser

I årsmeldingen for 2017 skrev utvalget om planene for opprettelse av en teknologisk enhet med minst fem ansatte. Det er antallet vi mener enheten bør ha ut fra dagens kontrollbehov. I sin behandling av årsmeldingen for 2017 understreket også Stortinget viktigheten av mer teknologisk kompetanse til utvalget. Tildelingen fra Stortinget for 2018 ga rom for å starte dette arbeidet og vi har ansatt de to første teknologene til den nye enheten. Men i Stortingets budsjett for 2019 ble ikke dette fulgt opp, og det er i 2019 ikke noen mulighet for ytterligere å styrke den teknologiske enheten på veien mot fem ansatte.

Høsten 2018 ble en fagdirektør og en senioringeniør ansatt i den teknologiske enheten. Sammen med et halvt årsverk som allerede var på plass teller enheten nå 2,5 årsverk. Det er nok til å komme i gang med bedre teknologisk støtte til både utvalget og resten av sekretariatet. Det er viktig at den teknologiske enheten har nødvendig oversikt og innsikt i systemene slik at teknologene kan gi utvalget støtte både i forkant av og under inspeksjoner, samt bidra i oppfølgingen av problemstillinger som kommer fra inspeksjonene.

Fremover blir det viktig å se på effektivisering av kontrollen med automatisering og andre moderne verktøy. Dette krever både kunnskap om tjenestenes systemer, og kunnskap om gode verktøy for å utføre denne effektiviserte kontrollen.

Den teknologiske enheten har startet på en samlet kartlegging og dokumentasjon av systemene i de forskjellige tjenestene.

Teknologene er også i gang med å knytte nettverk med eksisterende IT-miljøer i Norge, spesielt på sikkerhetsområdet. Den teknologiske enheten får nyttig kunnskap gjennom seminarer og andre samlinger, og ved å prate med fagfolk. Et annet mål er å gjøre EOS-utvalget bedre kjent i fagmiljøet, slik at vi forhåpentligvis får mange gode søkere i fremtiden.

Høringen om ny lov om Etterretningstjenesten har tatt mye tid mot slutten av 2018. Forslaget om tilrettelagt innhenting (TI) (Digitalt grenseforsvar) introduserer begrepet «styrket kontroll» og peker på EOS-utvalget både i den løpende kontrollen, som er en helt ny rolle, og den etterfølgende kontrollen, som er en utvidelse av dagens rolle.

En eventuell innføring av en ny og omfattende e-lov inkludert TI vil kreve ytterligere styrking av den teknologiske enheten utover fem ansatte som er behovet i dag.

En nærmere beskrivelse av utvalgets behov i forbindelse med TI og ny e-lov er beskrevet i utvalgets høringssvar til lovforslaget, se punkt 4.1 og vedlegg 3.

3.2 Internasjonalt samarbeid om kontroll

EOS-tjenestene samarbeider stadig mer internasjonalt, og de deler også mer og mer data over landegrensene – en god del av disse dataene er sensitive personopplysninger. Denne utviklingen gir også kontrollorganene nye utfordringer. Vi har derfor behov for å ha kontakt med utenlandske kontrollkollegaer for å utveksle erfaringer og få innspill til å bedre kontrollen.

EOS-utvalget har siden 2015 deltatt i et samarbeidsprosjekt med kontrollorganene fra Danmark, Sveits, Nederland og Belgia. I prosjektet undersøkte kontrollorganene sine nasjonale tjenesters internasjonale utveksling av personopplysninger om fremmedkrigere. EOS-utvalget har i undersøkelsen ikke funnet kritikkverdige forhold hos norske tjenester, men har merket seg at oppbyggingen av tjenestenes systemer har gjort det vanskelig å få full oversikt på ett sted over opplysninger som er delt om en enkeltperson.

Alle møtene med andre lands kontrollorganer har foregått på ugradert nivå og møtene er omtalt i årsmeldingene for 2015 - 2017.

Vi har en intensjon om å samarbeide mer med de fire kontrollorganene, og forhåpentligvis andre som slutter seg til, i årene fremover.

Den 14. november 2018 kom gruppa med en felles offentlig uttalelse om erfaringene fra prosjektet.

Tilrettelagt innhenting (TI) (Digitalt grenseforsvar)
Forslaget om TI går i hovedsak ut på at E-tjenesten skal ha mulighet til å innhente grenseoverskridende elektronisk kommunikasjon mellom Norge og utlandet. Forslag om TI er en del av forslaget til ny lov om Etterretningstjenesten som ble sendt på høring i 2018.

Sensitive personopplysninger
I personopplysningsloven, som er basert på EU-forordningen GDPR, er noen opplysninger definert som sensitive (kalt «særlige kategorier» i loven) – opplysninger om rasemessig eller etnisk bakgrunn, politisk, filosofisk eller religiøs oppfatning, opplysninger om fagforeningsmedlemsskap, genetiske opplysninger, biometriske opplysninger med formål om å identifisere noen, helseopplysninger, seksuell legning og informasjon om seksuelle forhold og opplysninger om straffedommer og lovovertredelser.

Fremmedkrigere
En person som kjemper i en væpnet konflikt utenfor sitt eget land av ideologiske eller idealistiske grunner, og ikke som en betalt leiesoldat.

Uttalelsen og en pressemelding om den følger som vedlegg 6 til årsmeldingen. I uttalelsen peker vi blant annet på risikoen for at kontrolltomrom kan oppstå når delingen av personopplysninger mellom tjenester er internasjonal, mens kontrollen bare er nasjonal. Når en norsk tjeneste deler informasjon med en partner i utlandet, kan vi se alt som skjer hos den norske tjenesten, men vår kontroll stopper når informasjonen er sendt ut av landet.

I uttalelsen tar vi til orde for et styrket samarbeid mellom kontrollorganene. Et verdifullt steg mot et nærmere samarbeid vil være å minimere hemmeligholdet mellom kontrollorganene, slik at noe informasjon kan deles. Når data allerede er utvekslet mellom tjenestene, kunne også kontrollorganene ha delt de samme opplysningene. Dette kunne redusert risikoen for et kontrolltomrom.

Vi peker i uttalelsen også på viktigheten av å utvikle nye kontrollmetoder, både juridiske og tekniske, som skal kunne bidra til bedre og mer effektiv kontroll av internasjonal datautveksling.

Organet IPCO, som blant annet kontrollerer Storbritannias hemmelige tjenester, har i etterkant sendt ut en offentlig støtteerklæring til vår uttalelse.

Det er for tiden flere initiativ til økt samarbeid om kontroll av internasjonalt samarbeid mellom tjenester. EOS-utvalget følger med på disse.

3.3 Anonymitet for varslere

I en artikkel på *aldrimer.no* 5. mars 2018 fikk utvalget kritikk for at det «tilsynelatende ennå ikke er etablert rammer for at utvalget kan tilby de ansatte i de hemmelige tjenestene kildevern dersom de ønsker å varsle om kritikkverdige forhold». Utvalgsleder svarte i et innlegg på *aldrimer.no* 18. april at utvalget har en plikt til å sørge for at identiteten til personer som i fortrolighet har gitt informasjon til EOS-utvalget beskyttes og ikke eksponeres når vi undersøker mulige kritikkverdige forhold i tjenestene:

> «Om vi får et varsel må vi vurdere om og hvordan informasjonen fra varsleren kan brukes av utvalget uten at varslerens identitet blir avslørt. Utvalget kan ta opp saker av eget initiativ, uten å måtte begrunne årsaken til undersøkelsene overfor tjenestene.»

Utvalget har likevel måtte opplyse om risikoen for at en varsler kan bli utpekt som kilde til informasjonen om utvalget satte i gang en undersøkelse.

Men vi vil ikke uten samtykke bruke informasjon fra varslere som vil forbli anonyme. Vi avslører heller ikke overfor Stortinget identiteten til varslere eller klagere.

Vi mener også at personer som er ansatt i virksomheter som er underlagt utvalgets kontrollområde fritt skal kunne varsle oss om mulig kritikkverdige forhold internt, uten hinder av taushetsplikt.

Utvalget mener at vern av varslere bør vurderes regulert i EOS-kontrolloven og eventuelt også i de respektive EOS-tjenestenes regelverk.

4.

Utvalgets høringsuttalelser

4.1 Høring om forslag til ny lov om Etterretningstjenesten

Den 12. november 2018 mottok EOS-utvalget Forsvarsdepartementets høringsnotat om ny lov om Etterretningstjenesten.

Utvalget praktiserer en høy terskel for å inngi høringssvar. Det ligger ikke til utvalgets mandat å mene noe om hvilke overvåkingsmetoder (som f.eks. tilrettelagt innhenting) E-tjenesten skal gis av Stortinget som lovgiver. Men forslaget har betydning for EOS-utvalgets kontroll. I tillegg ser vi konsekvenser av forslaget som Stortinget bør kjenne til før de behandler et lovforslag.

Utvalget har merket seg at høringsnotatet gjennomgående viser til EOS-utvalget som en sikringsmekanisme. Det er viktig å understreke at EOS-utvalget ikke er en garantist for at feil ikke kan skje i EOS-tjenestene. Vår kontroll er stikkprøvebasert og legger ikke opp til en fullstendig gjennomgang av all overvåkingsvirksomhet i EOS-tjenesten. Men vår vide innsynsrett har trolig en sterk disiplinerende og dermed preventiv effekt.

Vi vil overordnet påpeke at forslaget ikke løser sentrale uklarheter for Etterretningstjenestens overvåking av personer i Norge. Videre er flere av utvalgets kritiske merknader blitt omgjort til unntak fra forbudet mot overvåking av personer i Norge. Konsekvensen av dette er at Etterretningstjenesten vil få utvidede fullmakter i Norge.

Vi vil også fremheve forslaget om at E-tjenestens hensikt skal være avgjørende for tjenestens mulighet til å innhente informasjon om personer i Norge. For det første er kriteriet lite egnet for kontroll. For det andre synes kriteriet å tilsløre det at Etterretningstjenesten kan benytte metoder mot personer i Norge – så lenge «hensikten» er rettet mot forhold eller personer i utlandet.

Det er i høringsnotatet foreslått to endringer i EOS-kontrolloven. Vi mener de foreslåtte endringene utløser behov for avklaringer av konsekvensene for utvalgets virksomhet.

Utvalget mener også at om tilrettelagt innhenting blir innført, bør sekretariatet styrkes med mer enn de fire stillingene som Forsvarsdepartementet foreslår.

Høringssvaret følger som vedlegg 3 til meldingen.

4.2 Høring om forslag til forskrifter til ny sikkerhetslov

Den 2. juli 2018 mottok vi Forsvarsdepartementets høring om forslag til forskrifter til ny sikkerhetslov. Departementet foreslår nye forskrifter om myndighetens roller og ansvar for nasjonal sikkerhet, om virksomhetenes arbeid med forebyggende sikkerhet og om klarering av leverandører og personell.

Utvalget avga høringssvar 6. september 2018. Utvalget ba departementet vurdere om rettssikkerhetsgarantiene som gjelder for klareringssaker også bør gjelde for avgjørelser om autorisasjon for BEGRENSET. Vi viste til at negative avgjørelser om både klarering og autorisasjon kan få betydning for personens yrkeskarriere. Utvalget har tidligere[10] tatt opp dette problemet.

Høringssvaret følger som vedlegg 4 til meldingen.

4.3 Høring om sikkerhetslovens anvendelse for Stortingets eksterne organer

Stortinget skal vurdere på hvilken måte ny lov om nasjonal sikkerhet skal gis anvendelse for Stortingets eksterne organer og ba i den forbindelse om synspunkter fra blant andre EOS-utvalget.

Utvalget avga høringssvar 31. januar 2019. Utvalget stilte seg positivt til at sikkerhetsloven gis anvendelse for vår virksomhet. Vi uttalte at konstitusjonelle hensyn gir grunn til å unnta enkelte bestemmelser i sikkerhetsloven fra anvendelse. Vi foreslo en regulering tilsvarende de bestemmelser som er gitt om sikkerhetslovens anvendelse for Stortingets administrasjon. Utvalget hadde også enkelte synspunkter på hvilken klareringsmyndighet som skal klarere utvalgets medlemmer og sekretariatets ansatte.

Høringssvaret følger som vedlegg 5 til meldingen.

10 Saken ble først omtalt i utvalgets årsmelding for 2005, Dokument nr. 20 (2005–2006), side 13. Oppfølgingen av saken er også omtalt i årsmeldingene for 2011 og 2012 (henholdsvis Dokument 7:1 (2011–2012) kapittel V punkt 3 og Dokument 7:1 (2012–2013) kapittel V punkt 3).

5. Politiets sikkerhetstjeneste (PST)

5.1 Generelt om kontrollen

I 2018 har utvalget gjennomført fire inspeksjoner i Den sentrale enhet (DSE). I tillegg er PST-enhetene i politidistriktene Agder og Innlandet inspisert, samt PST-kontoret på Oslo lufthavn Gardermoen. Vi har fulgt opp inspeksjonen av PST-kontoret på Oslo lufthavn Gardermoen, men saken er ikke ferdig behandlet i meldingsåret.

Som én av partene i Felles cyberkoordineringsssenter (FCKS) har PST også i den sammenheng blitt inspisert.

I inspeksjonene i tjenesten kontrollerer vi særlig følgende:

- Tjenestens innhenting og behandling av personopplysninger.
- Tjenestens nye og avsluttede forebyggende saker og etterforskingssaker.
- Tjenestens bruk av skjulte tvangsmidler (for eksempel telefon- og romavlytting, dataavlesing og hemmelig ransaking).
- Tjenestens utveksling av informasjon med innenlandske og utenlandske samarbeidspartnere.

Utvalget deler inspeksjonene i en orienteringsdel og en inspeksjonsdel. PSTs orienteringer til oss er nyttige for å få tjenestens syn på dens oppgaver, vurderinger og utfordringer. Orienteringstemaene er i hovedsak valgt av utvalget selv, men tjenesten bes også om å orientere om øvrige forhold de mener er relevante for utvalgets kontroll. Ved å ha et bredt innblikk i tjenestens virksomhet, settes vi i stand til å foreta en mer spisset kontroll. Under inspeksjonene blir vi orientert om blant annet PSTs løpende virksomhet, tjenestens nasjonale og internasjonale samarbeid og saker det har vært offentlig debatt om. Utvalget stiller muntlige spørsmål på stedet og eventuelle skriftlige spørsmål i etterkant.

I inspeksjonsdelen søker vi direkte i tjenestens elektroniske systemer. PST varsles ikke om hvilke søk vi gjør. Det innebærer at inspeksjonsdelen inneholder betydelige uanmeldte elementer. Sekretariatet forbereder våre inspeksjoner grundig og det setter oss i stand til å gjennomføre mer målrettede inspeksjoner.

5.2 PSTs utlevering av opplysninger i klareringssaker

5.2.1 Innledning

Formålet med sikkerhetsklarering er å vurdere om personer er skikket til å behandle sikkerhetsgradert informasjon. Når en person skal sikkerhetsklareres, kan klareringsmyndigheten innhente opplysninger om vedkommende fra en rekke offentlige registre til sin vurdering av personens sikkerhetsmessige skikkethet. Dette kalles personkontroll. PST er blant dem det hentes inn opplysninger fra.

Utvalget kontrollerer jevnlig hvilke opplysninger PST utleverer til klareringsmyndigheten i klareringssaker.[11] Funn i inspeksjonene i PST, NSM og FSA i 2017 og 2018 ga grunn til nærmere undersøkelser av hvilke opplysninger PST formidler til klareringsmyndigheten. Vi har også undersøkt i hvilken form opplysningene utleveres og om det er godt nok dokumentert hvilke opplysninger som er utlevert.

Vi har gått gjennom opplysningene som PST har utlevert om i underkant av tjue personer fra 2015 til 2017.[12] I tillegg har vi undersøkt hvilke opplysninger PST har registrert om disse personene i tjenestens systemer og registre, samt hvordan klareringsmyndigheten har behandlet opplysningene i klareringssaken.

5.2.2 Hvordan PST utleverer informasjonen – bruk av møter og manglende dokumentasjon

Det fremgår av sikkerhetsloven 1998[13] at PST plikter å utlevere registeropplysninger til klareringsmyndigheten uten hinder av taushetsplikt. Opplysningene skal gis skriftlig.[14]

Utvalget stilte en rekke spørsmål til PST om skriftlighet ved utleveringer, bruk av møter og dokumentasjon av hva som ble formidlet. PST opplyste i sitt svar at tjenesten «… som hovedregel [utleverer] informasjon skriftlig, og i enkelte tilfeller har det blitt gitt ytterligere informasjon i et møte med klareringsmyndigheten».

Det er utvalgets oppfatning at tjenesten rutinemessig har lagt opp til at det holdes møter med klareringsmyndigheten om tjenesten har «flere detaljer enn det som gjengis i brevet eller at fagseksjonen ønsker å presisere informasjonene som blir gitt».[15] Utvalget viste til at flere av de skriftlige utleveringene fra PST til klareringsmyndigheten avsluttes med «for ytterligere opplysninger kontakt PST».

Forebyggende sak (f-sak)
Sak opprettet for å undersøke om noen forbereder et straffbart forhold som PST har til oppgave å forebygge.

Etterforskingssak (e-sak)
Sak opprettet for å undersøke om det er et straffbart forhold som faller inn under PSTs ansvarsområde.

Dataavlesing
En metode som gjør at en mobil/datamaskin blir tatt kontroll over ved bruk av datainnbrudd. Metoden, som gjør at alt som skjer på maskinen vil overvåkes, kan brukes av PST etter kjennelse fra domstolen.

I *omkring halvparten* av sakene som utvalget undersøkte, gjennomførte PST møter med klareringsmyndigheten. Dette betyr sannsynligvis at utlevering av informasjon i møter skjer i større utstrekning enn det PST beskrev i sitt svar til oss.

Vi mener at gode grunner taler for at personkontrollopplysninger skal utleveres skriftlig.

For det første taler hensynet til en korrekt og komplett formidling av personkontrollopplysninger for at disse skal utleveres skriftlig. Opplysninger fra PST vil normalt være særlig relevante og tungtveiende i en klareringssak. Den som utleverer opplysningene har best forutsetning for å nedtegne disse korrekt.[16]

For det andre bør utlevering skje skriftlig av hensyn til etterprøvbarheten. Manglende skriftlighet ved utleveringene fra PST gjør det vanskelig for både klageinstansen, en eventuell særskilt oppnevnt advokat[17] og EOS-utvalget å kontrollere hvilke opplysninger klareringsmyndigheten har hatt tilgang til og lagt til grunn for sin avgjørelse. Den som skal klareres har i enkelte tilfeller ikke krav på begrunnelse.[18] Dette gjelder for eksempel opplysninger fra PST. At alle sakens sider kan ettergås er særlig viktig siden personen som skal klareres ikke får vite om at opplysninger fra PST utgjør hele eller deler av begrunnelsen for nektelsen.

PST har uttalt at tjenesten med fordel kunne gitt mer informasjon skriftlig til klareringsmyndigheten i enkeltsaker. PST opplyste også at dokumentasjonen av hvilke personkontrollopplysninger som ble utlevert i møter ikke har vært tilfredsstillende. Tjenesten har skjerpet praksisen.

Vi delte tjenestens syn og la til grunn at PST heretter i all hovedsak vil utlevere informasjon til klareringsmyndigheten skriftlig. Skriftlig utlevering av opplysninger vil redusere behovet for møter mellom PST og klareringsmyndigheten. I den grad møter er nødvendige, forutsatte utvalget at PST sørger for tilfredsstillende dokumentasjon av hvilke opplysninger som utleveres.[19]

Utvalget kritiserte PST for at tjenestens praksis for utlevering av personkontrollopplysninger ikke har fulgt lovens krav om skriftlighet.

5.2.3 Kan PST la være å utlevere relevante opplysninger?

PST besvarte ikke utvalgets spørsmål om tjenesten har hjemmel til å holde tilbake opplysninger som er relevante for klareringssaken fra klareringsmyndigheten.

På generelt grunnlag ga tjenesten likevel uttrykk for at den i hvert tilfelle må vurdere hvilken informasjon som kan utleveres. PST uttalte at hensynet til tjenestens virksomhet, operative hensyn, hensynet til pågående etterforsking og vern av kilder og tredjepartsinformasjon må ivaretas, samtidig som klareringsmyndigheten får tilstrekkelig informasjon.

Vi uttrykte forståelse for denne type hensyn. Men utvalget bemerket at vi vanskelig kan se at sikkerhetslovens regler om personkontroll åpner for at PST kan gjøre sin egen vurdering av om opplysninger skal utleveres, så fremt opplysningene er relevante for personkontrollen. Utvalget uttalte at det bør være tydelig regulert hvordan man skal vekte hensynet til PSTs oppgaveløsning opp mot å utlevere negative opplysninger om personer som søkes klarert.

Utvalget uttalte at unntak fra utleveringsplikten bør reguleres i sikkerhetsloven eller forskrift til sikkerhetsloven.

Utvalget merker seg at det i klareringsforskriften[20] som trådte i kraft 1. januar 2019 er inntatt i § 12 at politiet og PST skal inngå avtale med NSM om politiets og PSTs utlevering av opplysninger som innhentes fra etterretnings- og arbeidsregistre til bruk i klareringssaker. Bestemmelsen skal ivareta hensynet til operative og forebyggende behov hos politiet og PST på den ene siden, og NSM og klareringsmyndigheten på den andre. Uenighet om bruk og utlevering av opplysningene skal avgjøres av Justis- og beredskapsdepartementet.

11 Utvalget har uttalt seg om utlevering fra PST til klareringsmyndigheten i utvalgets årsmeldinger til Stortinget for 1998 s. 11 og 2001 s. 7.

12 Kriterier for utvelgelsen var blant annet om det var fattet endelig avgjørelse i klareringssaken og om sakens dokumenter var tilgjengelige i Mimir – saksbehandlingssystemet for klareringssaker.

13 Lov 20. mars 1998 om forebyggende sikkerhetstjeneste (Sikkerhetsloven 1998) § 20 fjerde ledd. Sikkerhetsloven 1998 ble opphevet 1. januar 2019 – samme dag som lov 1. juni 2018 om nasjonal sikkerhet (Sikkerhetsloven) trådte i kraft.

14 Krav til skriftlighet følger både av sikkerhetsloven 1998 § 20 fjerde ledd og politiregisterforskriften § 11-3 første ledd, jf. politiregisterloven § 30 og politiregisterforskriften § 9-6 første ledd nr. 11.

15 Dette fremgår av PSTs notat som ble fremlagt for utvalget i inspeksjonen i DSE i desember 2017.

16 Dette kommer også til uttrykk i NSMs veiledning som tilrår at muntlig mottatte opplysninger som skal anvendes i saksbehandlingen av klareringssaker, «må klareringsmyndigheten be om å få … bekreftet skriftlig», jf. NSMs veiledning til sikkerhetsloven 1998 kapittel 6 og forskrift om personellsikkerhet, fra veiledningen til § 20.

17 Det følger av sikkerhetsloven 1998 § 25b andre ledd at klareringssaker der det ikke gis begrunnelse på nærmere vilkår kan oversendes til en særskilt oppnevnt advokat som skal gi råd om hvorvidt den omspurte bør klage på avgjørelsen. Advokaten skal ha tilgang til sakens faktiske opplysninger og den begrunnelse som er ukjent for den som har vært vurdert sikkerhetsklarert. Advokaten vil ikke kunne representere vedkommende i en eventuell klagesak.

18 Jf. sikkerhetsloven 1998 § 25 tredje ledd.

19 Jf. politiregisterforskriften § 11-4 andre ledd.

20 Forskrift 20. desember 2018 nr. 2054 om sikkerhetsklarering og annen klarering (klareringsforskriften).

Utvalget legger til grunn at PST i alle tilfeller vil informere klareringsmyndigheten om at PST *har* opplysninger som er relevante for en klareringssak og som tjenesten ikke vil utlevere. I motsatt fall kan ikke en uenighet om hvorvidt opplysningene *skal* utleveres komme til overflaten.

5.2.4 Utlevering av ikke-bekreftede opplysninger

Før PST utleverer opplysninger knyttet til personkontroll skal tjenesten kontrollere opplysningenes kvalitet og beskrive eventuell usikkerhet om opplysningene er riktige.[21]

PST opplyste at tjenestens bekymring for en person i mange tilfeller vil basere seg på ubekreftede opplysninger. Tjenestens register inneholder ikke faktaopplysninger på samme måte som straffesaksregistrene eller folkeregisteret.

Utvalget uttalte at PST i enkelte tilfeller ikke tydelig nok har informert om usikre opplysninger. Opplysninger til klareringsmyndigheten kan fremstå som førstehåndsinformasjon fra PST («PST er kjent med..»), mens realiteten er at PST har mottatt opplysninger fra en kontakt eller kilde, uten at opplysningene kan bekreftes.

Klareringsmyndigheten skal påse at klareringssaken er så godt opplyst som mulig. Opplysninger fra PST vil som regel veie tungt i klareringssaken, samtidig som klareringsmyndigheten selv sjelden kan bekrefte eller avkrefte opplysningene. For eksempel kan ikke klareringsmyndigheten uten videre konfrontere den som anmodes klarert med opplysningene fra PST i en sikkerhetssamtale.

Utvalget uttalte at det er spesielt viktig at PST tydeliggjør eventuell usikkerhet som hefter ved opplysningene.

5.2.5 Konklusjoner og oppfølging

Utvalgets oppgaver er blant annet å klarlegge om og forebygge at noens rettigheter krenkes og påse at tjenestenes virksomhet er i samsvar med krav i lov og forskrift.[22] Vår undersøkelse viste at PSTs praksis for utlevering av opplysninger til klareringsmyndigheten ikke er i samsvar med kravene. Tjenestens praksis innebærer også en risiko for at rettighetene til personer som anmodes sikkerhetsklarert kan krenkes. En negativ klareringsavgjørelse kan ha stor betydning for en persons yrkeskarriere.

Sikkerhetssamtale
Samtale som klareringsmyndigheten gjennomfører for å vurdere en persons sikkerhetsmessige skikkethet i en klareringssak.

Saken har demonstrert verdien av at Norge har ett utvalg som kontrollerer alle tjenestene og dermed kan vurdere både arbeidsdelingen og deling av informasjon tjenestene imellom.

Vi har merket oss at PST har endret sin praksis og revidert rutinen for utlevering av opplysninger til klareringsmyndigheten, samt at PST og NSM skal utarbeide en ny samarbeidsavtale.

Utvalget vil holde seg orientert om hvilke tiltak tjenesten gjennomfører i oppfølgingen av saken og fortsette sin kontroll av PSTs utleveringer til klareringsmyndighetene.

5.3 PSTs utlevering til klareringsmyndigheten i tre saker

5.3.1 Bakgrunn

Som redegjort for i punkt 5.2 har utvalget undersøkt PSTs utlevering til klareringsmyndigheten og som følge av den saken uttalt seg om tre konkrete tilfeller. I én av sakene ble resultatet at vedkommende ikke fikk klarering. Utvalget har ikke grunn til å tro at manglene ved PSTs utlevering har virket inn på resultatet i klareringssakene.

5.3.2 Sak 1 – Manglende dokumentasjon av hvilke opplysninger som er utlevert

I en sak fremgikk det av PSTs notater til et møte med klareringsmyndigheten at det skulle orienteres om etterretning fra en stat. At PST var bekymret for at personen kunne være tilknyttet fremmed etterretning fremgikk verken av den skriftlige utleveringen i forkant av møtet, eller av møtereferatet.

På spørsmål fra utvalget om hva som ble delt i møtet, svarte PST at tjenesten var bekymret for at personen som skulle sikkerhetsklareres kunne være etterretningsoffiser eller på annen måte samarbeide med en konkret stats myndigheter.

Utvalget uttalte at utleveringen i saken illustrerer de problematiske sidene ved PSTs praksis, som omtalt ovenfor i punkt 5.2. Hvilke opplysninger som ble utlevert var ikke dokumentert. I tillegg mente vi at PSTs utlevering kunne gi inntrykk av at tjenesten overfor klareringsmyndigheten gikk god for opplysningene i brevet, selv om opplysningene ikke var bekreftet av PST.

5.3.3 Sak 2 – Ulovlig utlevering av opplysninger om politisk engasjement

Politisk engasjement, inkludert medlemskap i, sympati med eller aktivitet for lovlige politiske partier eller organisasjoner og annet lovlig samfunnsengasjement skal ikke bety noe for vurderingen av en persons sikkerhetsmessige skikkethet, jf. sikkerhetsloven § 21 andre ledd.

PST hadde i en sak registrert opplysninger om en persons politiske engasjement og delt opplysninger om dette med klareringsmyndigheten. I oppfølgingen uttalte PST at ytringen er innenfor rammen av ytringsfriheten. Til utvalget opplyste PST at det ikke var grunnlag for behandlingen av opplysningene om personen og at registreringen derfor ble slettet.

Vi delte PSTs vurdering av registreringen, og la til at ytringen ikke går utover grensene for lovlig politisk virksomhet eller samfunnsengasjement.

Utvalget kritiserte PST for å ha utlevert opplysninger om politisk engasjement til klareringsmyndigheten, i strid med forbudet i sikkerhetsloven § 20 femte ledd.[23]

5.3.4 Sak 3 – Utlevering av uriktige opplysninger

PST utleverte opplysninger til en klareringsmyndighet om at personen som skulle klareres var medlem av en organisasjon som av PST ble beskrevet som et ekstremt miljø med voldspotensiale. Vår undersøkelse av registreringen av personen i Smart (PSTs arbeidsregister) viste at arbeidshypotesen om medlemskap i organisasjonen ikke var underbygget av informasjon.

PST opplyste at de til å begynne med hadde fått opplysninger som tilsa at personen var medlem i organisasjonen, men at nyere opplysninger viste at dette var feil. Ved en feil ble ikke arbeidshypotesen om medlemskap slettet, og de feilaktige opplysningene ble senere utlevert til klareringsmyndigheten.

Som følge av utvalgets spørsmål har PST slettet arbeidshypotesen og varslet klareringsmyndigheten om at det ble utlevert feil opplysninger om personen. For å hindre lignende saker i fremtiden skal seksjonen i PST som utleverer personkontrollopplysninger varsles når det oppdages feilregistreringer om en person tjenesten har utlevert opplysninger om.

Utvalget understreket viktigheten av at PST kontrollerer opplysningenes riktighet før de utleveres til klareringsmyndigheten.[24] *Utvalget merket seg de tiltak som PST har iverksatt.*

21 Jf. personellsikkerhetsforskriften § 3-4 fjerde ledd. Dette er også regulert i politiregisterloven, der det i § 67 tredje ledd er vist til § 20, som inneholder særlige regler og krav om skriftlighet for utlevering av ikke-verifiserte opplysninger.

22 Jf. EOS-kontrolloven § 2 første ledd.

23 Jf. sikkerhetsloven 1998 § 21 andre ledd.

24 Dette stilles det krav om i personellsikkerhetsforskriften § 3-4 fjerde ledd.

5.4 Hvor lenge kan PST lagre opplysninger før nødvendigheten av dem må vurderes?

Opplysninger som behandles i politiet og PST skal ikke lagres lenger enn det som er «nødvendig ut fra formålet med behandlingen».[25]

I årsmeldingen for 2017[26] skrev utvalget at vi i flere saker har stilt spørsmål om det fortsatt er nødvendig å lagre opplysninger om personer i arbeidsregisteret Smart. PST har på generelt grunnlag anført at registrerte opplysninger i arbeidsregisteret kan lagres i fem år før PST må vurdere om arbeidsregistreringene fortsatt er relevante og nødvendige for tjenesten. Tjenesten har vist til den såkalte femårsregelen i politiregisterforskriften § 22-3 tredje ledd. Samtidig har PST pekt på at nødvendigheten og relevansen av en arbeidsregistrering skal vurderes på nytt når det er tilført nye opplysninger på en registrert person i arbeidsregisteret Smart.

Utvalget uttalte i 2017 at arbeidsregistreringer med jevne mellomrom bør gjennomgås av den som er ansvarlig for å ha registrert opplysningene. Formålet er å sikre at arbeidsregisteret skal inneholde oppdatert, korrekt, nødvendig og relevant informasjon.

PST var uenig med utvalget i at arbeidsregistreringer må gjennomgås oftere enn hvert femte år. Vi tok derfor opp spørsmålet med Justis- og beredskapsdepartementet.

Departementet viste i brev til utvalget i 2018 til at det i politiregisterforskriften er satt forskjellige tidsintervaller for gjennomgang av opplysninger i ulike registre. Bestemmelsene er gitt fordi det ikke anses mulig å vurdere fortløpende om nødvendighetskravet er oppfylt. Lengden på intervallene beror på en konkret vurdering av hvor lenge det anses forsvarlig å behandle opplysningene uten at det foretas nye konkrete vurderinger om nødvendigheten. Departementet hadde ikke noen innvendinger mot den skisserte praksisen i PST.

Utvalget legger departementets forståelse til grunn i det videre kontrollarbeidet.

5.5 PSTs innhenting av chatlogg

Utvalget har i 2018 behandlet en sak som illustrerer hvordan nye måter å kommunisere på utfordrer det tradisjonelle skillet mellom muntlig og skriftlig kommunikasjon. I medhold av straffeprosessloven (strpl.) § 216l kan PST på bestemte vilkår «ved teknisk innretning avlytte eller gjøre opptak av telefonsamtale eller annen samtale med den mistenkte dersom politiet enten selv deltar i samtalen eller har fått samtykke fra en av samtalepartene».

PST mente at strpl. § 216l ga hjemmel for å innhente en chatlogg.

Når man chatter har det form som en samtale, men det skjer skriftlig. Utvalget stilte derfor spørsmål til PST om en chat kan anses som en «samtale» etter strpl. § 216l.

PST svarte at en naturlig språklig forståelse av ordlyden i bestemmelsen talte for at skriftlige samtaler via Internett og telefonapper som for eksempel Snapchat, Instagram og Messenger omfattes av «samtale» i strprl. § 216 l. Tjenesten viste til at ordet «chat» brukes om noe som kan sies å være en mellomting mellom muntlig og skriftlig kommunikasjon, og at bokmålsordboken definerer det som nettprat etter engelsk chat ‘prat, snakk’; samtale som foregår med tastaturet på datamaskin via internett. Dette mente PST støtter forståelsen av at samtaler ikke bare er muntlige, men at også skriftlig kommunikasjon via internett i stor grad har et muntlig element i seg. PST viste også til lovforarbeidene:

> «Avlyttingen/opptaket kan gjelde telefonsamtaler eller andre samtaler. (..) «Samtale» skal forstås vidt. Det avgjørende er om partene kommuniserer muntlig. Om det helt eller i det vesentlige bare er den ene parten som snakker, setter ikke saken i en annen stilling».[27]

PST viste til at det er om lag 20 år siden dette ble skrevet, og at de kommunikasjonsplattformene vi har i dag ikke fantes da. PST oppsummerte sin tolkning av bestemmelsen slik:

> »Det er derfor PSTs oppfatning, under henvisning til alminnelige rettskildeprinsipper, at en naturlig, samfunnskontekstuell ordlydsforståelse bør veie tungt. PST mener derfor at straffeprosessloven § 216l bør kunne anvendes på samtaler som foregår som nettprat/chat når bestemmelsens øvrige vilkår er oppfylt.»

Femårsregelen
Krav om at PSTs arbeidsregistreringer skal revurderes om de ikke er tilført nye opplysninger i løpet av de siste fem årene.

Arbeidsregistrering
Behandling av opplysninger som anses nødvendige og relevante for PSTs oppgaveløsning og som ikke kvalifiserer til opprettelse av eller behandling i forebyggende sak.

For øvrig viste tjenesten til at metoden innebar et lite inngrep overfor den det gjaldt, som allerede var underlagt annen type overvåkning besluttet av tingretten.

I avsluttende uttalelse til PST ga utvalget uttrykk for et annet syn enn hva PST har på rekkevidden av straffeprosessloven § 216l. PST har rett i at man i dagligtalen bruker «samtale» også om å «chatte», slik at tidligere klare grenser mellom muntlighet og skriftlighet er blitt mer flytende.

Verdien av å kunne kommunisere fortrolig med andre er en så verdifull rettighet at den er beskyttet i både Grunnloven og i Den Europeiske Menneskerettighetskonvensjonen (EMK). Grunnloven § 102 sier at alle har rett til respekt for kommunikasjonen sin, mens EMK artikkel 8 gir enhver rett til respekt for sin korrespondanse. Dette utgangspunktet kan bare fravikes av myndighetene om det lovfestes.

Til tross for at ordet »samtale» i strpl. § 216l skal forstås vidt, slår lovforarbeidene fast at det er avgjørende om partene kommuniserer «muntlig». Etter utvalgets syn kan derfor ikke bestemmelsen tolkes i en utvidet betydning under henvisning til en samfunnskontekstuell ordlydsforståelse av begrepet «samtale».

Det at PST etter vår mening ikke kan bruke strpl. § 216l til å få tilgang til en chatlogg, innebærer ikke at PST er avskåret fra å innhente chatlogger. Tjenesten har på visse vilkår adgang til å «avlytte samtaler eller annen kommunikasjon til og fra bestemte telefoner, datamaskiner eller andre anlegg …» etter strpl. § 216a. Bruk av denne bestemmelsen krever en kjennelse fra domstolen, mens påtalemyndigheten selv beslutter avlytting etter strpl. § 216l. Gjennom å benytte strpl. § 216l som grunnlag for å innhente chatlogger, vil PST kunne unndra seg innhentingen en lovbestemt domstolskontroll, noe som svekker den enkeltes rettsikkerhet.

På denne bakgrunn kritiserte utvalget PST og oppfordret tjenesten til å endre sin praksis.

I etterkant presiserte PST at bestemmelsen kun har blitt benyttet til å innhente chatlogger i dette ene tilfellet.

25 Jf. Forskrift 20. september 2013 nr. 1097 om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterforskriften) § 22-3 første ledd første punktum, jf. politiregisterloven § 6 første ledd nr. 3.

26 Jf. Dokument 7:1 (2017–2018) Årsmelding for 2017 fra EOS-utvalget punkt 5.4.

27 Ot.prp. nr 64 (1998–99) side 163.

PST understreket at bruken av bestemmelsen ble begrunnet i deres lovforståelse, og ikke for unndra innhentingen fra domstolskontroll.

PST har overfor utvalget bekreftet at tjenesten vil rette seg etter EOS-utvalgets oppfordring og vil avstå fra å benytte straffeprosessloven § 216l til innhenting av chatlogger i fremtiden. Dette er utvalget tilfreds med.

5.6 Avviksmeldinger – PSTs tvangsmiddelbruk

I årsmeldingen for 2017 skrev vi at PST av eget tiltak orienterte oss om ett avvik knyttet til tjenestens bruk av skjult kameraovervåking. Utvalget har i 2018 blitt orientert om PSTs oppfølging av avviket og endrede rutiner som følge av feilen.

Utvalget har i 2018 blitt orientert om to nye avvik i tjenestens tvangsmiddelbruk. Det ene avviket var knyttet til tjenestens kommunikasjonskontroll som ikke ble nedkoblet da abonnementet ikke lenger var i bruk. Det andre avviket gjaldt kameraovervåking som ikke ble nedkoblet da rettens tillatelse utløp. Kameraet ble slått av da feilen ble oppdaget ni dager senere. Det ble ikke gjort opptak i de ni dagene.

Vi har blitt orientert om tjenestens oppfølging av avvikene. Dette har ikke gitt grunn til oppfølging fra oss.

Utvalget mener det er positivt at PST rapporterer om avvik til utvalget under inspeksjoner. Vi legger til grunn at PST tar avvikene alvorlig og gjennomgår sine rutiner for å hindre at feil oppstår på nytt.

5.7 Klagesaker for utvalget

Utvalget har i 2018 mottatt 6 klager rettet mot PST, mot 12 i 2017. Enkelte av klagene var samtidig rettet mot andre EOS-tjenester.

Utvalgets uttalelser til klagere skal være ugraderte. Opplysning om at noen har vært overvåket eller ikke, anses som gradert hvis ikke annet blir bestemt. Det innebærer at en klager i utgangspunktet ikke kan få vite om vedkommende er overvåket av PST eller ikke. Av EOS-kontrolloven fremgår det at det ved klager mot tjenestene om overvåkingsmessig virksomhet kun skal uttales om klagen har gitt grunn til kritikk eller ikke.[28]

Utvalget har i 2018 avsluttet 4 klagesaker mot PST. Ingen klagesaker som ble avsluttet i 2018 har ført til kritikk av PST.

28 Jf. EOS-kontrolloven § 15 første ledd: «Uttalelser til klagere bør være så fullstendige som mulig uten at det gis graderte opplysninger. Opplysning om at noen har vært gjenstand for overvåkingsvirksomhet eller ikke, anses som gradert hvis annet ikke blir bestemt. Ved klager mot tjenestene om overvåkingsmessig virksomhet skal det bare uttales om klagen har gitt grunn til kritikk eller ikke. Mener utvalget at en klager bør gis en mer utfyllende begrunnelse, gir det forslag om det overfor den tjeneste det gjelder eller vedkommende departement.»

Kommunikasjonskontroll
En metode som overvåker en persons kommunikasjon – for eksempel telefonavlytting eller overvåking av metadata om telefon og datakommunikasjon. Metoden kan brukes av PST etter en kjennelse fra domstolen.

6.

Nasjonal sikkerhetsmyndighet (NSM)

Foto: Trond Strøm / Aftenposten / NTB scanpix

6.1 Generelt om kontrollen

I 2018 har utvalget gjennomført to inspeksjoner i NSM, hvorav den ene var i NSM NorCERT. Det er Norges nasjonale senter som koordinerer hendelseshåndtering i forbindelse med alvorlige IKT-sikkerhetshendelser.[29] Som én av partene i Felles cyberkoordineringssenter (FCKS) har NSM også i den sammenheng blitt inspisert.

NSM har status som direktorat og ivaretar de overordnede funksjoner innen forebyggende sikkerhetstjeneste etter sikkerhetsloven. NSM klarerer egne ansatte, i tillegg til å være klageinstans for klareringsvedtak fattet av andre klareringsmyndigheter.

I inspeksjonene kontrollerer vi særlig følgende:

- NSMs behandling av saker der klarering er nektet, nedsatt eller suspendert av klareringsmyndigheten, samt direktoratets behandling av klager over slike saker.
- NSMs samarbeid med andre EOS-tjenester.
- NSM NorCERTs informasjonsbehandling.

Under inspeksjonene blir vi rutinemessig orientert om NSMs løpende virksomhet, blant annet om direktoratets samarbeidssaker med andre EOS-tjenester og saksbehandlingstid i klareringssaker. I inspeksjonene søker utvalget direkte i direktoratets elektroniske systemer. Orienteringstemaene er i hovedsak valgt ut av utvalget selv, men tjenesten bes også om å orientere om øvrige forhold som de mener er av relevans for utvalgets kontroll. Utvalget stiller muntlige spørsmål på stedet og eventuelle skriftlige spørsmål i etterkant.

Klareringsmyndighetens oppgave er å vurdere personers pålitelighet, lojalitet og sunne dømmekraft, og om hun eller han er sikkerhetsmessig skikket til å behandle sikkerhetsgradert informasjon.[30] En avgjørelse om sikkerhetsklarering kan få avgjørende betydning for den enkeltes karriere, og det må derfor stilles høye krav til saksbehandlingen. Utvalget har derfor stor oppmerksomhet mot disse sakene – også fordi saksbehandlingen i klareringssaker er mer lukket enn saksbehandlingen i andre forvaltningsavgjørelser.

6.2 Særskilt melding til Stortinget om ulik praksis for sikkerhetsklarering av personer med tilknytning til andre stater

Utvalget avga 12. mars en særskilt melding til Stortinget.

EOS-utvalget har gått gjennom klareringssaker der personen som skal sikkerhetsklareres eller nærstående har tilknytning til andre stater enn Norge. Vi har funnet flere kritikkverdige forhold, som NSM som fagmyndighet har et overordnet ansvar for. Et hovedmål for prosjektet har vært å vurdere om tilnærmet like saker behandles likt.

- Utvalgets undersøkelse avdekket ubegrunnet forskjellsbehandling av saker som gjaldt klarering av personer med både norsk og et utenlandsk statsborgerskap. Forskjellene gjaldt både saksbehandlingen og sakenes resultat. Enkelte personer med tilknytning til et land ble nektet klarering, selv om andre personer med sammenlignbar tilknytning til det samme landet fikk klarering.
- Undersøkelsen viste at flere av sakene ikke var tilstrekkelig opplyst, og at personenes tilknytning til Norge ikke var godt nok vurdert.
- Utvalget har konkludert med at enkeltpersoners rettigheter er krenket, jf. EOS-kontrolloven § 2.

Majoriteten av klareringssakene i denne undersøkelsen er behandlet av klareringsmyndighetene Forsvarets sikkerhetsavdeling (FSA), Politiets sikkerhetstjeneste (PST) og Etterretningstjenesten. Dette er klareringsmyndigheter som har et stort sakstilfang. Utvalget har ikke synspunkter på hvilket resultat de aktuelle sakene skulle ha fått. Dette er en utpreget sikkerhetsfaglig vurdering. Vi er opptatt av at alle klareringsmyndighetene behandler og vurderer saker med tilnærmet samme faktum på lik måte. At det er variasjon i saksbehandlingen og resultatet hos klareringsmyndighetene, går utover rettssikkerheten til personene som søkes klarert.

Undersøkelsen av åtte saker der personer ble nektet klarering, viste at seks av personene ble nektet klarering uten at sakene deres var tilstrekkelig opplyst. Disse sakene ble avgjort av FSA. FSA har orientert om at disse negative klareringsavgjørelsene vil behandles på nytt.

Utvalgets undersøkelse avdekket også ubegrunnet forskjellsbehandling i klareringssaker der ektefellen til personen som skulle klareres manglet personhistorikk. I flere saker ble det lagt til grunn at ektefellen ikke var omfattet av kravet

Forebyggende sikkerhetstjeneste
Planlegging, tilrettelegging, gjennomføring og kontroll av forebyggende sikkerhetstiltak som søker å fjerne eller redusere risiko som følge av sikkerhetstruende virksomhet.

Nærstående
Personer som er i nær familie eller som har annen nær tilknytning til den som skal klareres, for eksempel ektefelle/partner/samboer og barn.

Personhistorikk
Det kreves opplysninger om en persons bakgrunn som er sikkerhetsmessig relevant for de siste 10 årene for å gjennomføre en personkontroll i forbindelse med sikkerhetsklarering.

til personhistorikk, og det ble dermed gitt klarering, mens Nasjonal sikkerhetsmyndighet (NSM) i sammenlignbare saker nektet klarering.

NSMs tilbakemelding i saken støtter opp under utvalgets konklusjoner. NSM erkjenner at det foreligger en uforholdsmessig og ikke faglig begrunnet variasjon knyttet til både saksbehandlingen og avgjørelsen i sakene utvalget viste til. Som mulige årsaker til dette, pekte NSM på at det ikke finnes en sporbar oversikt over praksis, og at det er utfordringer med kapasiteten til å holde sikkerhetssamtaler.

Utvalget har overfor NSM, som er fagmyndighet for klareringssaker, gjennom flere år understreket viktigheten av at et erfaringsarkiv og andre verktøy for å sikre lik behandling av tilnærmet like saker kommer på plass. Det er svært viktig at NSM etablerer løsninger som sikrer ensartet praksis. Utvalget merker seg at tiltakene ennå ikke er gjennomført.

6.3 Klagesaker for utvalget

6.3.1 Innledning

Utvalget har i 2018 mottatt 11 klager rettet mot NSM, mot 3 i 2017. 10 av disse er klager i saker om sikkerhetsklarering.

En avgjørelse i sak om sikkerhetsklarering kan være avgjørende for en persons videre yrkeskarriere og livssituasjon. Av den grunn er det essensielt at disse sakene behandles på en rettssikker og rettferdig måte av klareringsmyndighetene. I saker der utvalget uttaler kritikk, får klageren en begrunnelse for utvalgets konklusjon.

Utvalget har i meldingsåret avsluttet 8 klager over nektet sikkerhetsklarering. Av saker vi har avsluttet i meldingsåret har følgende saker gitt grunn til kritiske uttalelser fra oss:

6.3.2 Klagesak 1 – Manglende klareringsbehov

I en klagesak ba klageren utvalget om å undersøke om det i det hele tatt var behov for sikkerhetsklarering. Utvalget ba anmodende myndighet (arbeidsgiver) om å dokumentere og begrunne behovet for sikkerhetsklarering i den aktuelle stillingen.[31] Arbeidsgivers svar ga grunn til ytterligere spørsmål fra vår side, og arbeidsgivers uttalelser til utvalget ble oversendt til NSM for direktoratets vurdering.

NSM konkluderte med at klareringsbehovet ikke var tilstrekkelig dokumentert. Den manglende dokumentasjonen var en saksbehandlingsfeil som førte til at vedtaket om INGEN KLARERING var ugyldig.

Anmodningen om sikkerhetsklarering skulle vært avvist av NSM.

Ved avslutningen av saken sluttet vi oss til direktoratets ugyldighetsvurdering. Det forelå ikke et lovmessig grunnlag for å gjennomføre en klareringsprosess overfor klageren. Vi uttalte videre:

> «Den uhjemlede klareringsprosessen har fått faktiske negative følger for [klageren]. Utvalget understreker at en klareringsavgjørelse kan ha avgjørende betydning for en persons livssituasjon og videre yrkeskarriere.
>
> Utvalget bemerker også at en uhjemlet klareringsprosess er en sterk inngripen i enkeltpersonens personvern. Utvalget har merket seg at opplysningene fra klareringsprosessen gjøres utilgjengelig og anonymiseres.
>
> Det er klart kritikkverdig at klareringsmyndigheten har gjennomført et inngripende tiltak uten at det forelå reelt behov for sikkerhetsklarering».

EOS-utvalget mener NSM på en sterkt kritikkverdig måte har krenket klagerens rettigheter, jf. EOS-kontrolloven § 2 første ledd nr. 1 og 3.

I årsmeldingen for 2017 redegjorde utvalget for en lignende klage. Vi opprettet sak for å vurdere generelle spørsmål om problemstillinger rundt dokumentasjon og begrunnelse for klareringsbehov. Denne saken er fortsatt til behandling i utvalget.

29 NSM NorCERT (Norwegian Computer Emergency Response Team). NSM NorCERT er en funksjon som ivaretas av Avdeling for IKT-sikkerhet i NSM.
30 Jf. sikkerhetsloven 1998 § 21 første ledd.
31 Jf. sikkerhetsloven 1998 § 19 og personellsikkerhetsforskriften § 3-1

Nasjonal sikkerhetsmyndighet
Nasjonal sikkerhetsmyndighet (NSM) er et sivilt direktorat som har ansvar for forebyggende sikkerhet. NSM har fag- og kontrollansvaret for personellsikkerhetstjenesten innenfor sikkerhetslovens område, er Norges ekspertorgan for informasjons- og objektsikkerhet og er det nasjonale fagmiljøet for IKT-sikkerhet.

Anmodende myndighet
Et organ som anmoder om personkontroll i forbindelse med en sikkerhetsklarering.

6.3.3 Klagesak 2 – Manglende innsyn i sak der utvalget ikke er enig i NSMs begrunnelse

I årsmeldingen for 2017[32] omtalte vi en sak om tilbakekall av sikkerhetsklarering, som omhandlet grensen mellom personal- og klareringssak. I samme sak ba omspurte om innsyn i korrespondansen mellom EOS-utvalget og NSM. Vi ba derfor NSM om å vurdere om innsyn kunne gis.

NSM vurderte at det kunne gis innsyn i utvalgets brev til NSM i sin helhet, men unntok fra innsyn flere avsnitt i enkelte av NSMs brev til utvalget. Begrunnelsen for å nekte innsyn var at avsnittene «viser NSMs arbeidsmetoder og vurderinger». NSM vurderte at disse avsnittene inneholder skjermingsverdig informasjon som fortsatt skal være sikkerhetsgradert etter sikkerhetsloven § 11.[33]

Utvalget bemerket overfor NSM at det var uklart hvilke arbeidsmetoder og vurderinger som er sikkerhetsgraderte i denne konkrete saken. Vi kunne vanskelig se grunnlaget for å unnta opplysninger i de aktuelle avsnittene fra innsyn, idet de gir uttrykk for beskrivelse av faktum og regelverk, juridiske/sikkerhetsfaglige vurderinger og en gjengivelse av utvalgets uttalelser. Vi kunne heller ikke se på hvilken måte de unntatte opplysningene i saksdokumentene er sikkerhetsgraderte. Altså at opplysningene kan skade Norges, eller våre alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser, om omspurte ble gitt innsyn i disse.

NSM ble derfor bedt om å redegjøre for hvilke arbeidsmetoder og vurderinger som eventuelt er graderte. Direktoratet måtte også svare på hva som er grunnen til dette, samt helt konkret hvorfor innsyn i de aktuelle avsnittene i disse dokumentene for personen saken gjelder kan skade rikets sikkerhet.

Etter tilbakemelding fra NSM om at de fremdeles mente at opplysningene som ble unntatt fra innsyn skal være sikkerhetsgraderte, ga vi følgende avsluttende uttalelse:

> «Sikkerhetsloven § 11 tredje ledd annet punktum sier at 'sikkerhetsgradering ikke skal skje i større utstrekning enn strengt nødvendig, og det skal ikke brukes høyere sikkerhetsgrad enn nødvendig'. Bestemmelsen fastsetter en plikt å verdivurdere informasjonen med tanke på om informasjonen er sikkerhetsgradert, samt hvilken sikkerhetsgrad informasjonen ev. har. Dersom unntak fra innsyn begrunnes med at informasjonen er sikkerhetsgradert, uten at det er hjemmel for det, er dette i strid med sikkerhetsloven § 11.
>
> Utvalget merker seg at NSM fremdeles mener at opplysningene som er unntatt fra innsyn skal være sikkerhetsgraderte, 'basert på de betydelige negative konsekvenser det kan ha for nasjonale sikkerhetsinteresser dersom opplysningene sammenstilles og benyttes til manipulasjon av fremtidige klareringssaker'.

Utvalget kunne på generelt grunnlag være enig i at sammenstilling av detaljerte sikkerhetsfaglige vurderinger og metoder vil kunne skade nasjonale sikkerhetsinteresser om de blir kjent for uvedkommende. Men vi hadde fortsatt vanskelig for å se at alle opplysningene i de unntatte avsnittene sier noe om NSMs sikkerhetsfaglige vurderinger eller sikkerhetstjenestens metoder, og dermed inneholder sikkerhetsgradert informasjon etter sikkerhetsloven 1998 § 11.

Vi viste også til NOU 2016:19 kapittel 8.2.1[34] om informasjonssikkerhet, der det fremgår at '[d]en nedre grensen for informasjon som skal sikres må være av en slik art at den har et visst skadepotensial'.

Det var for oss ikke klart at alle de unntatte opplysningene er av en slik art at de har et visst skadepotensial om de blir kjent for uvedkommende.

Utvalget mener det er beklagelig at innsyn ikke ble gitt i den fullstendige korrespondansen mellom NSM og utvalget i saken.

6.3.4 Klagesak 3 – Mangler ved begrunnelsen og underretningen til klageren, samt manglende dokumentasjon

Utvalget stilte spørsmål til NSM om behandlingen av en klage over nektet sikkerhetsklarering. Førsteinstansen hadde i sin avgjørelse vektlagt en rekke forhold nevnt i sikkerhetsloven 1998 § 21 første ledd:

- straffbare handlinger (bokstav b),
- forhold som kan lede til at omspurte kan utsettes for press (c),
- feilaktig eller unnlatt fremstilling om faktiske forhold (d),
- unnlatelse av å gi autorisasjonsansvarlig løpende underretning om egne forhold (g) og
- andre forhold knyttet til klagerens væremåte og egenskaper (l).

NSMs interne samtidige begrunnelse (ISB) viste ikke hvilke av de ovennevnte forholdene som var vektlagt i klageomgangen.

I svar til oss skrev NSM at de ikke hadde tatt stilling til alle forholdene som førsteinstansen la vekt på. NSM mente at

Omspurte
Person som det etter samtykke anmodes om sikkerhetsklarering for.

Intern samtidig begrunnelse (ISB)
Et internt dokument som klareringsmyndigheten er pliktig å utarbeide i forbindelse med klareringsavgjørelser. Dette dokumentet må omhandle alle vesentlige forhold i saken, inkludert reglene avgjørelsen bygger på, hvilke forhold som er vektlagt etter sikkerhetsloven § 21 og hvilke faktiske forhold avgjørelsen bygger på.

førsteinstansens vektlegging av straffbare handlinger, pressgrunnlag, klagerens egenskaper eller væremåte ikke hadde betydning for sakens utfall. Andre forhold var nok til å nekte klarering. NSM erkjente at dette burde vært omtalt i sakens interne dokumenter og i underretningen til klageren.

Det har stor betydning for klagerens rettssikkerhet og for utvalgets mulighet til å føre etterfølgende kontroll at klareringsmyndighetens vurderinger fremkommer av sakens dokumenter.

Utvalget kritiserte NSM for manglende skriftlig dokumentasjon i saken.

NSM lot også være å informere klageren om at de ikke hadde tatt stilling til alle forhold i saken. Førsteinstansen hadde i sin vurdering av klageren vektlagt forhold av personlig og svært sensitiv karakter. Blant annet la førsteinstansen vekt på at klageren var anmeldt for alvorlige straffbare handlinger, selv om anmeldelsene var henlagt som «intet straffbart forhold bevist».

Utvalget kritiserte NSM for ikke å klargjøre overfor klager at de sensitive forholdene ikke var en del av begrunnelsen for nektet sikkerhetsklarering. At det ble gitt en mangelfull begrunnelse var i seg selv kritikkverdig, og det alvorlige vurderingstemaet forsterket utvalgets kritikk.[35]

I sitt svar til oss beklaget NSM at direktoratets vedtak fremstod som ufullstendig og var egnet til å skape frustrasjon og misforståelser. Utvalget sluttet seg til NSMs syn på vedtakets utforming.

Det er en forutsetning for enkeltpersoners mulighet til å ivareta sine interesser at klareringsmyndigheten gir en så utfyllende begrunnelser som mulig når en blir nektet sikkerhetsklarering.

6.3.5 Klagesak 4 – Lang saksbehandlingstid

I en klagesak kritiserte utvalget NSM for lang saksbehandlingstid. Da klagesaken ble sendt over fra førsteinstans til NSM, gjorde førsteinstansen en feil som klageinstansen NSM ikke kan lastes for. Det var gått 1,5 år siden klagen var avgjort i førsteinstans da NSM ble oppmerksom på saken. Saksbehandlingstiden i NSM var deretter ni måneder. I utvalgets avsluttende uttalelse til NSM ga vi uttrykk for at saken ut fra omstendighetene burde ha vært avgjort av NSM uten opphold. Saksbehandlingstiden var derfor etter utvalgets syn uforholdsmessig lang.

6.4 Saksbehandlingstid i klareringssaker

Utvalget har i mange år vært opptatt av klareringsmyndighetenes saksbehandlingstid i klareringssaker. Nedenfor følger en tabell over saksbehandlingstid for 2018 som opplyst av NSM.

NSM har i en inspeksjon orientert utvalget om sitt arbeid med å redusere saksbehandlingstiden. Utvalget vil fortsatt holde seg orientert om saksbehandlingstid i klareringssaker i 2019.

SAKSBEHANDLINGSTID NSM 2018	Gjennomsnittlig saksbehandlingstid totalt	Gjennomsnittlig saksbehandlingstid positive avgjørelser	Gjennomsnittlig saksbehandlingstid negative avgjørelser
Anmodning om innsyn	49 dager		
Anmodning om klarering	76 dager	74 dager	189 dager
Klage 1. instans	74 dager	N/A	74 dager
Klage 2. instans	75 dager	152 dager	65 dager

32 Årsmelding 2017 punkt 6.4

33 Jf. sikkerhetsloven1998 § 25a andre ledd første punktum, jf. § 25 tredje ledd.

34 NOU 2016:19 kapittel 8.2.1 side 150.

35 Krav til begrunnelse følger av sikkerhetsloven § 25 og NSMs veiledning til sikkerhetsloven kapittel 6 og forskrift om personellsikkerhet, veiledning § 25.

7.

Forsvarets sikkerhetsavdeling (FSA)

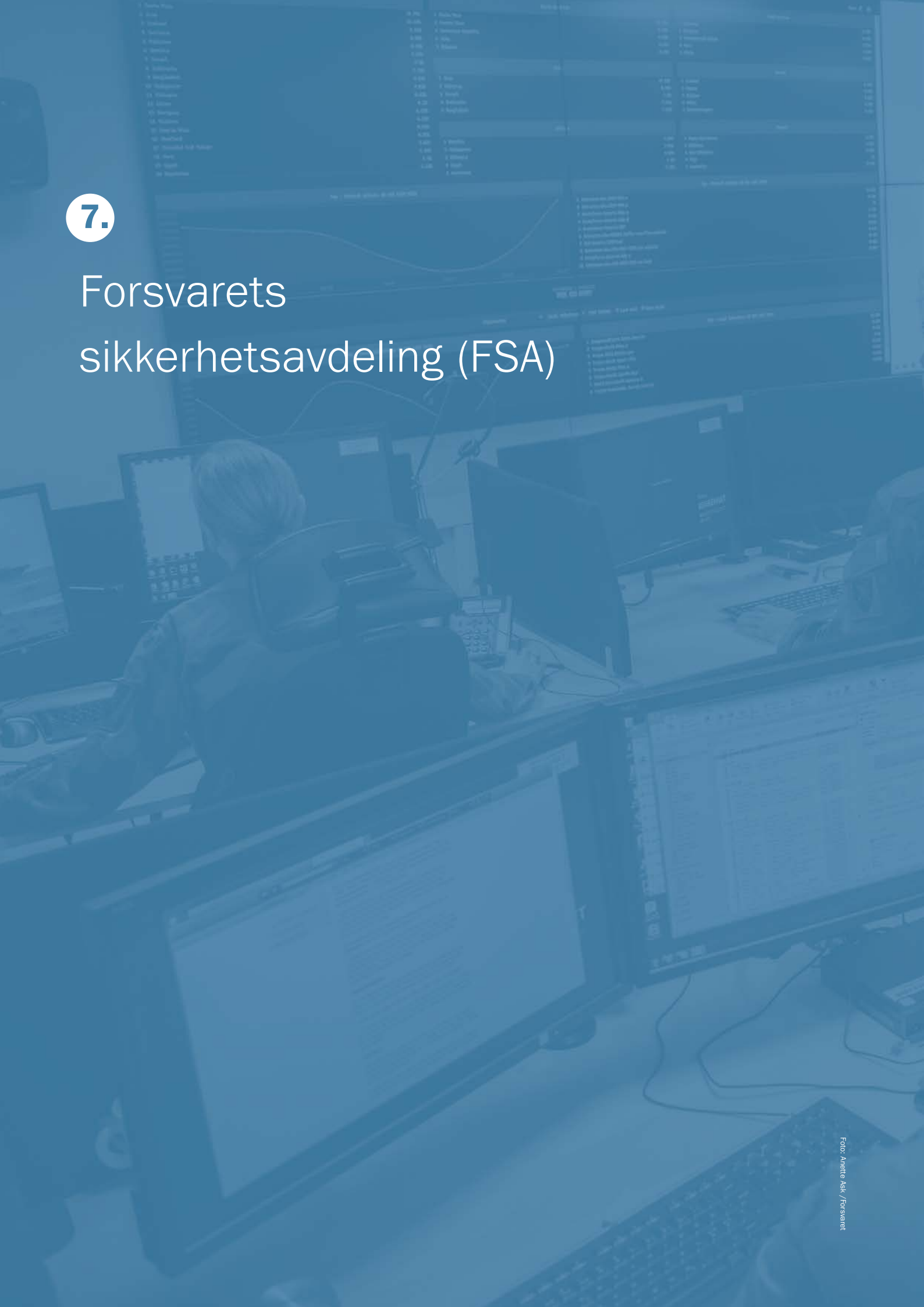


Foto: Anette Ask / Forsvaret

7.1 Generelt om kontrollen

Utvalget har i 2018 gjennomført to inspeksjoner i FSA. I inspeksjonene i avdelingen kontrollerer vi særlig følgende:

- FSAs behandling av saker der klarering er nektet, nedsatt eller suspendert av klareringsmyndigheten.
- FSAs virksomhet innenfor forebyggende sikkerhetstjeneste.
- FSAs samarbeid med andre EOS-tjenester.

Til inspeksjonene ber utvalget om å bli orientert om FSAs løpende virksomhet, og om enkelte særskilte temaer av kontrollmessig relevans. Orienteringstemaene er i hovedsak valgt ut av utvalget selv, men tjenesten bes også om å orientere om øvrige forhold som de mener er relevante for utvalgets kontroll. Utvalget stiller muntlige spørsmål på stedet og eventuelle skriftlige spørsmål i etterkant.

FSAs behandling av sikkerhetsklareringssaker utgjør en særlig viktig del av vår kontroll med avdelingen. FSA er landets desidert største klareringsmyndighet. Den 1. januar 2017 ble FSA klareringsmyndighet for hele forsvarssektoren, og de overtok ansvaret for klareringssakene til Forsvarsdepartementet og Forsvarsbygg. Utvalget kontrollerer de fleste negative klareringsavgjørelser fattet av FSA, samt påklagede klareringssaker der avdelingen har tatt klagen helt eller delvis til følge i klageomgangen.

Vi fører også kontroll med FSAs virksomhet innenfor forebyggende sikkerhetstjeneste, tar stikkprøver knyttet til undersøkelser av sikkerhetstruende virksomhet rettet mot Forsvaret (sikkerhetsundersøkelser) og kontrollerer operative saker som ledd i avdelingens ansvar for å drive militær kontraetterretning i Norge i fredstid. En annen sentral oppgave er å føre kontroll med FSAs behandling av personopplysninger som ledd i utøvelsen av forebyggende sikkerhetstjeneste.

Utvalget har i 2018 mottatt tre klager rettet mot FSA, mot én i 2017. Klagene var også rettet mot andre EOS-tjenester. Vi har avsluttet to klagesaker i 2018. Ingen klagesaker som ble avsluttet i 2018, har ført til kritikk av FSA.

7.2 Bruk av personkontrollopplysninger til andre formål enn vurdering av sikkerhetsklarering

Utvalget har stilt spørsmål til FSA om personopplysninger som var innhentet i klareringssaker kunne brukes til andre formål.

FSA skal holde oversikt over det sikkerhetsmessige risikobildet som omgir Forsvaret og norsk militær aktivitet både hjemme og ute.[36] For å forebygge sikkerhetstruende hendelser behandlet FSA opplysninger om et stort antall personer tilknyttet Forsvaret i en sikkerhetsundersøkelse. Av et internt notat i FSA fra 2014 fremgikk det at opplysningene som ville brukes i undersøkelsen var gitt til avdelingen som ledd i personkontroll i klareringssaker. Dette er opplysninger som etter sikkerhetsloven 1998 § 20 sjette ledd ikke kunne brukes til andre formål enn slik personkontroll. FSA har overfor utvalget i 2018 opplyst at undersøkelsen ikke baserte seg på opplysninger fra personkontroll.

Vi minnet ved avslutningen av saken FSA om at opplysninger som er gitt til klareringsmyndigheten i forbindelse med personkontroll, ikke skal benyttes til andre formål enn vurdering av sikkerhetsklarering.

7.3 Saksbehandlingstid i klareringssaker

Utvalget har i mange år vært opptatt av klareringsmyndighetenes saksbehandlingstid i klareringssaker. Nedenfor følger en tabell over saksbehandlingstid i 2018 som opplyst av FSA.

FSA har i en inspeksjon orientert utvalget om sitt arbeid med å redusere saksbehandlingstiden. Utvalget vil fortsatt holde seg orientert om saksbehandlingstid i klareringssaker i 2019.

SAKSBEHANDLINGSTID FSA 2018	Gjennomsnittlig saksbehandlingstid totalt	Gjennomsnittlig saksbehandlingstid positive avgjørelser	Gjennomsnittlig saksbehandlingstid negative avgjørelser
Anmodning om innsyn	16 dager		
Anmodning om klarering	25 dager	21 dager	151 dager
Klage 1. instans	98 dager	149 dager	70 dager

36 Jf. Instruks 29. april 2010 nr. 695 om sikkerhetstjeneste i Forsvaret § 4 første ledd bokstav e.

Sikkerhetstruende hendelse
Sikkerhetstruende virksomhet, kompromittering av skjermingsverdig informasjon og grove sikkerhetsbrudd.

8.

Etterretningstjenesten (E-tjenesten)

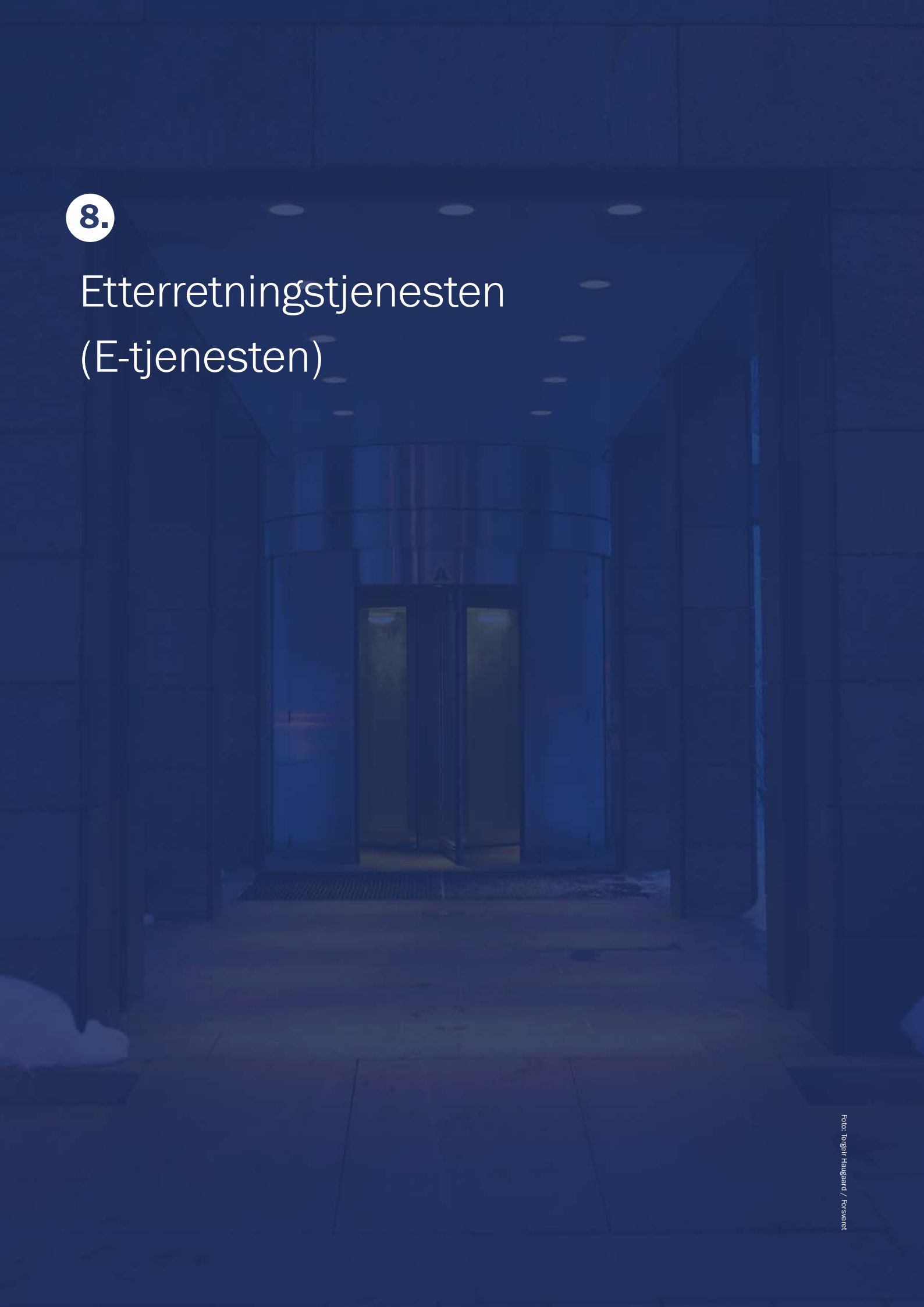


Foto: Torgeir Haugaard / Forsvaret

8.1 Generelt om kontrollen

Utvalget har i 2018 gjennomført to inspeksjoner av E-tjenesten sentralt, i tillegg til inspeksjoner av fartøyet Marjata og Forsvarets stasjon Ringerike på Eggemoen.

Som én av partene i Felles cyberkoordineringssenter (FCKS) har E-tjenesten også i den sammenheng blitt inspisert.

Kontrollen av E-tjenesten er særlig rettet inn mot å kontrollere at tjenesten ikke bryter med det lovfestede forbudet mot å overvåke eller på annen fordekt måte innhente informasjon om personer som oppholder seg i Norge.[37] To andre sentrale kontrollpunkter er å kontrollere at tjenesten er under nasjonal kontroll og at den overholder Forsvarsdepartementets bestemmelser om innsamling og/eller deling av informasjon om norske rettssubjekter utenfor Norge.

Utvalget skal sikre at virksomheten i E-tjenesten holdes innenfor rammen av tjenestens fastlagte oppgaver.[38] Videre skal kontrollen sikre at virksomheten ikke krenker noens rettigheter eller utilbørlig skader samfunnets interesser, at virksomheten i E-tjenesten holdes innenfor rammen av lov, administrative eller militære direktiver og ulovfestet rett. Andre viktige kontrollpunkt er å sjekke at det ikke nyttes mer inngripende midler enn det som er nødvendig etter forholdene og at tjenesten respekterer menneskerettighetene.[39]

Vår kontroll med E-tjenesten skal omfatte tjenestens tekniske virksomhet, inkludert overvåking og innhenting av informasjon og behandling av personopplysninger. Utvalget skal påse at samarbeidet og informasjonsutvekslingen mellom E-tjenesten og innenlandske og utenlandske samarbeidspartnere holdes innenfor rammen av gjeldende regelverk, jf. EOS-kontrolloven § 6.

I inspeksjonene i E-tjenesten fører vi særlig kontroll med følgende punkter:

- Tjenestens tekniske informasjonsinnhenting.
- Tjenestens behandling av opplysninger i dens datasystemer.
- Tjenestens informasjonsutveksling med innenlandske og utenlandske samarbeidende tjenester.
- Saker av særlig viktighet eller prinsipiell karakter som er forelagt Forsvarsdepartementet (foreleggelsessaker)[40] og interne godkjenningssaker.

Til inspeksjonene ber utvalget om informasjon om E-tjenestens løpende virksomhet, blant annet om tjenestens samarbeidssaker med andre EOS-tjenester, trusselsituasjonen, foreleggelsessaker for Forsvarsdepartementet og interne godkjenninger. Orienteringstemaene er i hovedsak valgt av utvalget selv, men tjenesten bes også om å orientere om øvrige forhold som de mener er relevante for utvalgets kontroll. Utvalget stiller muntlige spørsmål til på stedet og eventuelle skriftlige spørsmål i etterkant.

Interne godkjenninger kan være tillatelser til deling av informasjon om norske rettssubjekter til utenlandske samarbeidende tjenester eller tillatelser til å overvåke norske rettssubjekters kommunikasjon når personene er i utlandet. Som utvalget tidligere har pekt på, plikter ikke E-tjenesten å gå til retten for å få tillatelse når de skal overvåke norske personers kommunikasjon i utlandet. PST må derimot få en kjennelse fra retten når de skal utføre kommunikasjonskontroll av personer som er i Norge.

Utvalget har i 2018 mottatt fire klager rettet mot E-tjenesten, mot seks i 2017. Klagene var også rettet mot andre EOS-tjenester. Vi har avsluttet to klagesaker i 2018. Ingen klagesaker som ble avsluttet i 2018 har ført til kritikk av E-tjenesten.

Utvalget ber rutinemessig E-tjenesten om å rapportere til utvalget dersom tjenesten avdekker avvik i den tekniske informasjonsinnsamlingen. E-tjenesten har ikke rapportert noen avvik i 2018.

8.2 E-tjenestens innsamling fra åpne kilder om personer i Norge

E-tjenesten skal ikke overvåke eller på annen fordekt måte innhente informasjon om personer i Norge.

På nærmere vilkår kan E-tjenesten innhente informasjon om norske personer i utlandet (heretter kalt innhentingsmål).

37 Jf. e-loven § 4 første ledd.
38 Jf. EOS-kontrolloven § 6 tredje ledd nr. 2.
39 Jf. EOS-kontrolloven § 2.
40 Jf. Kgl. res. av 31. august 2001 nr. 1012 om instruks om Etterretningstjenesten § 13 bokstav d.

Rettssubjekt
Enhver som kan ha rettigheter og plikter, ikke bare mennesker, men også juridiske personer – f.eks. foreninger, stiftelser, selskaper, kommuner fylkeskommuner og staten.

Utvalget merket seg at tjenesten i henhold til dens interne regelverk også kan innhente opplysninger fra åpne kilder om personer i Norge – inkludert norske statsborgere. Dette forutsatt at formålet med innhentingen ikke er å innhente informasjon om innenlandske forhold, og at personen er godkjent som et innhentingsmål.

På denne bakgrunn stilte utvalget på prinsipielt grunnlag spørsmål til tjenesten om hvilke skranker e-loven § 4 setter for E-tjenestens innhenting av informasjon fra åpne kilder om personer i Norge. Tjenesten svarte at tjenestens innsamling kun skal være rettet mot utenlandske forhold innenfor E-tjenestens oppgaver, og ikke ha som formål å frembringe opplysninger om innenlandske forhold. Innsamlingen er derfor i realiteten ikke rettet mot personer i Norge. E-tjenesten anførte også at innhenting av informasjon som er åpent tilgjengelig ikke rammes av «fordekt»-begrepet i e-loven § 4 sin forstand, selv om tjenesten skjuler sin aktivitet.

Forbudet i e-loven § 4 er formulert slik:

> «Etterretningstjenesten skal ikke på norsk territorium overvåke eller på annen fordekt måte innhente informasjon om norske fysiske eller juridiske personer»

Utvalget har i særskilt melding[41] til Stortinget tatt opp hvordan begrepet «om» skal forstås. E-tjenesten mener at begrepet må forstås som rettet mot og at det altså må innfortolkes en overvåkingshensikt. I meldingen omtalte utvalget E-tjenestens søk i lagrede metadata knyttet til personer i Norge for å finne selektorer som er relevante for utenlandsetterretning.[42] Vi var i tvil om dette var lov i henhold til dagens regelverk.

Utvalget mener at tjenestens innhenting av informasjon fra åpne kilder rettet mot personer som er godkjente innhentingsmål og som oppholder seg i Norge, må vurderes på samme måte som søkene omtalt over.

Vi er opptatt av i hvilke tilfeller E-tjenesten kan samle inn opplysninger om personer som oppholder seg i Norge. Det kan vanskelig trekkes ut av forbudets ordlyd at det er tjenestens hensikt som skal avgjøre om overvåking av personer i Norge er i strid med forbudet eller ikke. At tjenesten kun har til hensikt å overvåke når personen befinner seg utenfor Norge – men ikke når vedkommende befinner seg i Norge – er et kunstig skille som vanskelig kan kontrolleres av oss.

Utvalget kan vanskelig se at tjenesten kan søke etter utenlandsrelevant informasjon via søk etter personer i åpne kilder som befinner seg i Norge – og som er innhentingsmål når de befinner seg i utlandet.

Vi uttalte til E-tjenesten at det knytter seg begrunnet tvil til lovligheten av innhentingen av informasjon fra åpne kilder om norske personer mens de oppholder seg i Norge etter dagens regelverk. Saken illustrerer at rammen for forbudet i e-loven § 4 bør avklares av Stortinget.

Utvalget har i en høringsuttalelse sendt merknader til forslag til ny e-lov, se punkt 4.1 og vedlegg 3.

8.3 E-tjenestens innhenting av innholdsdata om norsk borger

I en inspeksjon fant vi at tjenesten hadde innsamlet innholdsdata i form av personopplysninger om en norsk borger i Norge. Informasjonen var innhentet som følge av tjenestens innsamling av innholdsdata fra satellitt.

Innsamlingen var basert på et søkebegrep som var innenfor tjenestens mandat og rettsgrunnlag. Det innsamlede materialet inneholdt informasjon som ga tjenesten svar på sitt informasjonsbehov – men også irrelevant informasjon om en norsk borger.

Derfor stilte vi spørsmål til tjenesten om innhentingen av informasjon om den norske borgeren var i strid med e-loven § 4. E-tjenesten ble først oppmerksom på at de hadde samlet inn opplysningene om den norske borgeren da utvalget stilte spørsmål. E-tjenesten svarte at innsamlingen ble gjennomført for å utføre tjenestens lovpålagte oppgaver. Søkebegrepet var videre ikke *rettet* mot norske personer og dermed ikke i strid med forbudet slik tjenesten forstår det.

Som beskrevet i punkt 8.2 har utvalget i særskilt melding til Stortinget tatt opp hvordan forbudets bruk av «om» skal forstås i tilknytning til ordlyden i loven der det står «(…) innhente informasjon *om* norske fysiske eller juridiske personer». E-tjenesten mener at begrepet må forstås som *rettet mot* og at det må innfortolkes en overvåkingshensikt.

Målrettet innhenting av innholdsdata som er basert på et søkebegrep vil nettopp ikke være rettet mot spesifikke personer. Dersom E-tjenestens forståelse av forbudet skal legges til grunn, vil slik innsamling aldri rammes av forbudet – selv

Metadata
Informasjon om data, eksempelvis tidspunkt, varighet, til/fra-identifikatorer og type trafikk, som beskriver en teknisk hendelse som har funnet sted i et kommunikasjonsnettverk. Metadata kan for eksempel være informasjon om en telefonsamtale.

Selektor
I en etterretningskontekst er det et mål som det blir hentet informasjon fra, for eksempel et telefonnummer eller en e-postadresse.

om innholdsdata om norske borgere i Norge rent faktisk følger med på lasset.

På den andre siden ser vi at dersom en rent språklig forståelse av forbudets begrep «om» skal legges til grunn, vil tjenestens mulighet for innsamling av innholdsdata bli så vanskelig at tjenesten ikke kan utføre sine lovpålagte oppgaver.

I vår avsluttende uttalelse til E-tjenesten sa vi at det knytter seg begrunnet tvil til lovligheten av innhentingen av informasjon om en norsk borger etter dagens regelverk – selv om innhentingen ikke var tilsiktet. Vi mener at denne saken igjen illustrerer at rammen for forbudet i e-loven § 4 bør avklares av Stortinget.

Utvalget har i en høringsuttalelse sendt merknader til forslag til ny e-lov, se punkt 4.1 og vedlegg 3.

E-tjenesten har orientert utvalget om at informasjonen om den norske borgeren er slettet.

8.4 E-tjenesten har ikke lov til å gå gjennom innholdsdata som er samlet inn i strid med loven

Utvalget har bedt E-tjenesten gi en redegjørelse for om tjenesten kan gjennomgå innholdsdata som er innhentet i strid med e-loven § 4 første ledd:

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

Bakgrunnen for spørsmålet var at utvalget hadde fått inntrykk av at E-tjenesten hadde hørt gjennom innholdet i lydkuttene som ble feilinnsamlet i strid med e-loven § 4 første ledd. Vi redegjorde for feilinnsamlingen i årsmeldingen for 2017.[43]

E-tjenesten meldte tilbake at tjenesten ikke hadde hørt gjennom lydkuttene. Utvalget merket seg at tjenesten på generelt grunnlag anførte at «virkningen av at informasjon er erverv et i strid med § 4 … ikke automatisk [vil] være at denne ikke kan behandles med et utenlandsetterretningsformål».

Foto: Forsvaret / NTB scanpix

41 Dokument 7:2 (2015-2016) Særskilt melding til Stortinget om rettsgrunnlaget for Etterretningstjenestens overvåkingsvirksomhet.
42 Særskilt melding til Stortinget om rettsgrunnlaget for Etterretningstjenestens virksomhet, punkt 5.3.3 i meldingen.
43 Årsmelding for 2017 punkt 8.3 under «Avvikssak 1».

E-tjenesten viste blant annet til praksis i menneskerettighetsdomstolen om presisering av anvendelsen av EMK artikkel 8 (retten til respekt for privatliv), høyesterettspraksis om bruk av ulovlig ervervet bevis i straffesaker og tilsvarende for sivile saker, jf. tvisteloven § 22-7.

Utvalget skrev i avsluttende brev til tjenesten at utenlandsetterretningstjenester skiller seg grunnleggende fra politiorganers formål og virksomhet. Etterretningstjenesten skal «redusere usikkerhet hos viktige beslutningstakere, med et særlig fokus på å forutse framtida. De skal vurdere fremmede trender og handlinger hos stater, organisasjoner og personer, uavhengig av om de vil gjøre noe straffbart.»

Vi mener at viderebehandling av slikt (feil)innsamlet materiale må anses som fortsatt «fordekt innhenting» av informasjon om en norsk borger på norsk territorium. Forbudet i e-loven § 4 første ledd mot fordekt overvåking av norske personer i Norge, er en sentral begrensning for E-tjenestens virksomhet.

Videre uttalte utvalget ved avslutningen av saken:

> «Dersom materiale som er innsamlet i strid med e-loven § 4 gjennomgås av E-tjenesten, vil dette kunne utgjøre en gjentatt krenkelse av e-loven § 4, og være et fortsatt ulovlig inngrep i den overvåkedes privatliv og personvern. Utvalget bemerker at den motsatte konklusjon ville innebære stor fare for utglidning av forbudet i e-loven § 4 første ledd om overvåking av norske borgere på norsk territorium. Dette ville kunne gjøre forbudet i e-loven § 4 illusorisk og vil være problematisk for rettssikkerheten til norske personer i Norge.»

Utvalget konkluderte med at E-tjenesten ikke har hjemmel til å gjennomgå eller på annen måte behandle informasjon som stammer fra norsk kommunikasjon i Norge, og som tjenesten har samlet inn i strid med e-loven § 4 første ledd.

8.5 Innsamling av kommunikasjon der en av partene er i Norge

Utvalget har vurdert det rettslige grunnlaget for å behandle personopplysninger om personer i Norge i etterretningsrapporter vedrørende etterretningsmål i utlandet.

Vi mener at tjenesten kan rapportere om nødvendig og relevant informasjon for utenlandsetterretning som kommer frem gjennom «den norske forbindelsen» ved innsamling mot mål i utlandet. Dette vil si at lovlig innsamling mot mål i utlandet også kan omfatte målets kommunikasjon med norske personer som befinner seg i Norge. Spørsmålet i saken var om tjenesten gikk for langt i sin sammenstilling og viderebehandling av kommunikasjon med den norske forbindelsen, selv om den var innhentet på lovlig vis. Utvalget lot saken bero med den forklaring tjenesten ga.

Vi uttalte at det i arbeidet med ny lov om Etterretningstjenesten må avklares hvilke skranker som gjelder for E-tjenestens sammenstilling og viderebehandling mv. av informasjon som stammer fra «den norske forbindelsen» sett opp mot forbudet i § 4.

Fordekt innhenting
Innhenting av opplysninger i etterretningsøyemed som er gjort i skjul for personen det innhentes opplysninger om.

Særlig sensitiv informasjon
EOS-utvalget har begrenset innsyn hos E-tjenesten i det som regnes som særlig sensitiv informasjon. Med «særlig sensitiv informasjon», jf. E-tjenestens Retningslinjer for behandling av særlig sensitiv informasjon, menes:

1. Identiteten til E-tjenestens og utenlandske partneres menneskelige kilder.
2. Identiteten til utenlandske partneres særskilt beskyttede tjenestemenn.
3. Personer og operative planer i okkupasjonsberedskapen.
4. E-tjenestens og/eller utenlandske partneres særlig sensitive utenlandsoperasjoner* som ved kompromittering
    a. alvorlig kan skade forholdet til fremmed makt grunnet operasjonens politiske risiko, eller
    b. kan medføre alvorlig skade eller tap av liv for eget personell eller tredjepersoner.

*Med «utenlandsoperasjoner» menes her operasjoner rettet mot utenlandske forhold (fremmede stater, organisasjoner eller individer), inkludert aktivitet relatert til slike operasjoner som forberedes og gjennomføres på norsk territorium.

9.

Kontroll av annen EOS-tjeneste

9.1 Generelt om kontrollen

Utvalget kontroller EOS-tjeneste, uavhengig av hvilken del av offentlig forvaltning som utfører den.[44] Kontrollområdet er med andre ord funksjonelt definert. Det er ikke begrenset til bestemte organisatoriske enheter.

Etter en endring av EOS-kontrolloven i 2017 skal utvalget gjennomføre en årlig inspeksjon av Etterretningsbataljonen[45] og en årlig inspeksjon av Forsvarets spesialstyrker,[46] jf. EOS-kontrolloven § 7.

Utvalget har i 2018 avsluttet én klagesak rettet mot klareringsmyndigheten i Nasjonal kommunikasjonsmyndighet. Saken ble avsluttet uten kritikk. Etter at Stortinget i 2016 besluttet å endre klareringsmyndighetsstrukturen, er ikke Nasjonal kommunikasjonsmyndighet (Nkom) lenger klareringsmyndighet.

9.2 Felles cyberkoordineringssenter (FCKS)

Felles cyberkoordineringssenter (FCKS) ble etablert i 2017 og er et samarbeid mellom NSM, E-tjenesten, PST og Kripos. Senterets mål er å styrke den nasjonale evnen til effektivt forsvar mot og håndtering av alvorlige hendelser i det digitale rommet.

Utvalget har i 2018 gjennomført en inspeksjon av senteret. Inspeksjonen ga ikke grunnlag for oppfølging.

Vi har i flere år vært opptatt av å kontrollere samarbeidet mellom EOS-tjenestene i deres arbeid opp mot digitale trusler. Vi er særlig opptatt av at samarbeidet innrettes slik at regelverket for de enkelte tjenestene ikke omgås. Utvalget forutsetter at tjenestene dokumenterer sitt samarbeid slik at vi kan føre etterfølgende kontroll.

Utvalget vil fortsette sin kontroll av samarbeidet som finner sted i FCKS.

9.3 Inspeksjon av Etterretningsbataljonen (Ebn)

Behovet for ekstern kontroll av Etterretningsbataljonen knytter seg i følge Evalueringsutvalget for EOS-utvalget[47] til faren for at verktøy og kunnskap bataljonen har om etterretningsvirksomhet brukes på ureglementert måte.

Utvalget har i 2018 inspisert Ebn på Setermoen. Utvalget ble i inspeksjonen orientert om endringer i Ebn siden inspeksjonen i 2017, samarbeid med andre EOS-tjenester og pågående saker og aktivitet. Utvalget inspiserte Ebns datasystemer og utvalgte dokumenter, på bakgrunn av sekretariatets forberedelse. Inspeksjonen ga ikke grunnlag for oppfølging.

Foto: Anette Ask / Forsvaret

9.4 Inspeksjon av Forsvarets spesialkommando

Kontrollbehovet knytter seg ifølge Evalueringsutvalget til avdelingens kapasitet til å drive etterretningsvirksomhet, og til faren for at denne benyttes i Norge i fredstid eller på annen ureglementert måte. Det bør også kontrolleres at samarbeidet med Etterretningstjenesten skjer innenfor gjeldende regelverk.

Vi har i 2018 inspisert Forsvarets spesialkommando på Rena. Utvalget ble i orienteringen orientert om spesialstyrkenes organisering, oppgaver og kapasiteter. Inspeksjonen ga grunnlag for en viss skriftlig oppfølging.

9.5 Inspeksjon av Nasjonal kommunikasjonsmyndighet (Nkom)

Det følger av EOS-kontrolloven § 7 nr. 8 at utvalget etter eget tiltak skal utføre inspeksjon av organer som bistår PST. Utvalget har i 2018 inspisert Nkom. Inspeksjonen ga ikke grunnlag for oppfølging.

9.6 Inspeksjon av Telia Norge AS

I 2018 har vi gjennomført en inspeksjon av Telia Norge AS. Som teletilbyder har Telia etter ekomloven § 2-8 en tilrettelegginsplikt for PST i forbindelse med kommunikasjonskontroll. Inspeksjonen ga ikke grunnlag for oppfølging.

9.7 Personellsikkerhetstjenesten i Riksrevisjonen

Utvalget gjennomførte i 2017 en inspeksjon av personellsikkerhetstjenesten i Riksrevisjonen. Vi har i brev til Riksrevisjonen stilt spørsmål om manglende begrunnelser til personer som ble nektet klarering og tatt opp enkelte spørsmål til realiteten i en av sakene.

I sakene der klarering var nektet som følge av «tilknytning til andre stater», fikk personene opplyst av klareringsmyndigheten at de ikke fikk noen informasjon om begrunnelsen fordi denne er gradert.

I svar til utvalget fastholdt Riksrevisjonen at begrunnelse ikke kunne gis, med hjemmel i sikkerhetsloven 1998 § 25. I henhold til sikkerhetsloven 1998 § 25 tredje ledd første punktum skal «begrunnelse for en avgjørelse … gis samtidig med underretningen om utfallet av klareringssaken». I NSMs veiledning til bestemmelsen fremgår det at begrunnelsen til den enkelte «må utarbeides på basis av klareringsmyndighetens interne begrunnelse».

I vår avsluttende uttalelse viste vi til NSMs veiledning, som også angir at begrunnelsen «som et minimum [må] nevne de regler og faktiske forhold avgjørelsen bygger på». Det fremgår av lovteksten at «tilknytning til andre stater» kan tillegges negativ vekt – og det kan ikke anses som sikkerhetsgradert informasjon å vise til denne i begrunnelsen. Riksrevisjonens personell hadde selv opplyst om sin tilknytning til andre stater og var innforstått med det faktiske forholdet.

Det er kun i ekstraordinære tilfeller at lovgiver har akseptert at begrunnelse kan unntas. Slike hensyn forelå ikke i disse sakene.

Etter utvalgets mening er negative klareringsavgjørelser så inngripende vedtak at det skjerper kravet til at begrunnelsen må utformes på en tilstrekkelig presis og tydelig måte, slik at den reflekterer hensynene som har vært avgjørende i saken. Uteblitt begrunnelse vanskeliggjør omspurtes muligheter til å imøtegå avgjørelsen og svekker deres rettssikkerhet. I avsluttende brev til Riksrevisjonen bemerket utvalget at ingen av personene hadde påklaget de negative avgjørelsene.

EOS-utvalget kritiserte Riksrevisjonen for ikke å ha gitt begrunnelser for de negative avgjørelsene i tråd med sikkerhetslovens bestemmelser. Utvalget har oppfordret Riksrevisjonen til å bringe sin praksis i samsvar med sikkerhetslovens krav til begrunnede underretninger og gi utvalget tilbakemelding om hvilke tiltak som er gjort, jf. EOS-kontrolloven § 14 siste ledd.

44 Jf. EOS-kontrolloven § 1 første ledd.

45 EOS-kontrolloven § 7 andre ledd nr. 5 stiller krav om at utvalget skal gjennomføre minst «en årlig inspeksjon av Etterretningsbataljonen.

46 EOS-kontrolloven § 7 andre ledd nr. 6 stiller krav om at utvalget skal gjennomføre minst «en årlig inspeksjon av Forsvarets spesialstyrker».

47 Stortingets presidentskap nedsatte 27. mars 2014 et utvalg ledet av daværende førstelagmann Bjørn Solbakken til å evaluere EOS- utvalgets virksomhet og rammebetingelser. Evalueringsutvalget leverte sin rapport til Stortinget 29. februar 2016, Dokument 16 (2015-2016.)

Personellsikkerhet
Tiltak, handlinger og vurderinger for å hindre at personer som vil kunne utgjøre en sikkerhetsrisiko, får tilganger som kan føre til sikkerhetsbrudd.

I en sak stilte utvalget også spørsmål til grunnlaget for nektelsen. Personen fikk opplyst at begrunnelsen var gradert og i de interne sakspapirene fremgikk det at den negative avgjørelsen skyldtes tilknytning til annen stat. På spørsmål fra utvalget ga Riksrevisjonen uttrykk for at det var personens tilbakeholdenhet med å gi opplysninger til klareringsmyndigheten som var avgjørende for det negative utfallet. I avsluttende brev til Riksrevisjonen uttalte vi at personen skulle fått en begrunnelse som samsvarte med den reelle begrunnelsen for utfallet. Vi påpekte også overfor Riksrevisjonen at de interne sakspapirene syntes å mangle dokumentasjon for at personen ikke hadde gitt klareringsmyndigheten ønskede opplysninger. Tvert imot var det dokumentert at vedkommende hadde gitt Riksrevisjonens flere detaljer om sin kontakt med et annet lands borgere.

Vi var derfor i berettiget tvil om saken var godt nok opplyst og dokumentert til at avgjørelsen kunne etterprøves av utvalget.

Vi har bedt Riksrevisjonen om en tilbakemelding om hvilke tiltak som er blitt foretatt på grunnlag av vår kritikk, jf. EOS-kontrolloven § 14 siste ledd.

9.8 Prosjekt om sikkerhetssamtaler

I kontrollen med klareringssaker har utvalget i mange år vært særlig oppmerksom på sikkerhetssamtalen som verktøy for klareringsmyndigheten. En sikkerhetssamtale skal, slik loven lød i 2018[48], gjennomføres i saker der det ikke er «åpenbart unødvendig». Klareringsmyndigheten skal gjennom samtalen innhente opplysninger som grunnlag for å kunne vurdere om omspurte er sikkerhetsmessig skikket. Etter sikkerhetsloven § 8-4[49] er det en rekke forhold som kan være relevante i vurderingen av om en person er sikkerhetsmessig skikket.

Utvalget besluttet i 2018 å gjøre en systematisk gjennomgang av et større antall sikkerhetssamtaler. Formålet med gjennomgangen er å undersøke om sikkerhetssamtalene forberedes og gjennomføres slik at informasjon som er relevant for klareringsmyndigheten kommer frem, samt hvordan samtalen sikrer kontradiksjon for omspurte.

Prosjektet er forventet å bli ferdig i 2019.

9.9 Klage på klareringsavgjørelser i Forsvarsdepartementet

Utvalget har i 2018 avsluttet to klagesaker rettet mot klareringsmyndigheten i Forsvarsdepartementet som var klageinstans i begge sakene. Vi ba departementet om å dokumentere sine vurderinger i klagesakene. Utvalget mente at det ikke fremgikk av departementets interne saksdokumenter at departementet i klageomgangene hadde foretatt en konkret og individuell vurdering av klagerens sikkerhetsmessige skikkethet. Departementet opplyste at det delte førsteinstansens vurderinger og konklusjon, men erkjente at vurderingene i større grad burde vært dokumentert.

Vi påpekte at det har stor betydning for klagernes rettssikkerhet og for utvalgets mulighet til å føre en reell etterfølgende kontroll at klareringsmyndighetens vurderinger fremkommer av sakenes dokumenter.

48 Se § 21 tredje ledd i sikkerhetsloven 1998.
49 Se § 21 første ledd i sikkerhetsloven 1998.

10.

Informasjonsarbeid, eksterne relasjoner og media i 2018

10.1 Offentliggjøring av utvalgets uttalelser utenfor årsmeldingen

I våre offentlige og ugraderte meldinger til Stortinget tar vi hensyn til både EOS-tjenestenes behov for hemmelighold og offentlighetens behov for kunnskap. At offentligheten får informasjon om kritikk av EOS-tjenestene er en forutsetning for en opplyst debatt. Vi merker oss at fravær av kritikk fra utvalget på et område, i økende grad blir tatt til inntekt for at utvalget mener at tjenestens virksomhet er innenfor regelverket.

Etter modell fra Sivilombudsmannen mener vi det kan være et positivt bidrag til det offentlige ordskiftet om også utvalget publiserer enkelte av sine omtaler av avsluttede saker løpende. Vi mener at utvalgets behandling av saker som er av offentlig interesse – men som likevel ikke nødvendiggjør en særskilt melding til Stortinget – kan utgis som uttalelser i løpet av året. For saker som har vært offentlig omtalt og diskutert, vil det også ha en verdi at utvalgets uttalelse ikke må vente til neste årsmelding. Vi venter at det er relativt få uttalelser som vil være aktuelle for slik offentliggjøring.

Utvalgets løpende uttalelser vil være ugraderte, på samme måte som meldinger til Stortinget. Før vi publiserer en slik uttalelse, vil vi gi tjenestene mulighet til å avklare om uttalelsen inneholder gradert informasjon, samt kontrollere at teksten ikke inneholder feil eller misforståelser. Disse uttalelsene vil bare bli publisert digitalt, men vil tas med i påfølgende årsmelding.

10.2 Eksterne relasjoner, årskonferanse og studietur til USA

Utvalget har de siste årene lagt ekstra mye arbeid og ressurser i kontakt med eksterne i inn- og utland – både for å få ut budskapet om arbeidet vårt, og for å lære av andre.

Hele utvalget var på studietur i Washington DC i september. Vi hadde blant annet møter hos Justisdepartementet.

Foto: EOS-utvalget

Å få mer kunnskap ut i offentligheten om den demokratiske kontrollen med EOS-tjenestene mener vi vil føre til mer tillit og legitimitet både for oss og tjenestene. Det kan også gjøre både tjenestene og utvalget bedre.

Så fremt vi har kapasitet og ikke er begrenset av taushetsplikt, ønsker vi å stille opp for å svare på spørsmål fra media, forskere og andre, eller å holde foredrag for dem som ønsker det.

Sekretariatet har også i 2018 begynt å publisere medieoppsummeringene utvalget får om EOS-relevante nyhetssaker og rapporter – både på nettsida og via Twitter-kontoen. Eksterne kan også få disse oppsummeringene tilsendt per epost.

Utvalget og sekretariatet har i 2018 vært på flere konferanser i utlandet, både i regi av kontrollorganer og sivilsamfunnet. Blant annet har vi vært på en konferanse i Paris i desember der representanter fra 14 europeiske kontrollorganer var til stede – med sikte på å få til et tettere europeisk kontrollsamarbeid. Dette er særlig aktualisert av at tjenestene samarbeider stadig mer, og at mer og mer data deles over landegrenser.

Vi har også bidratt til internasjonale publikasjoner, og vi har for første gang publisert en uttalelse sammen med utenlandske kontrollorganer. Les mer om det arbeidet i punkt 3.2 og vedlegg 6.

I april arrangerte vi en årskonferanse for andre gang. Det var rundt 100 deltakere. Noen av temaene var «åpenhet i tjenestene», «automatisert kontroll» og «5 år etter Snowden».

Også i 2019 arrangerer vi en årskonferanse i forbindelse med offentliggjøringen av denne årsmeldingen. Årskonferanse skal avholdes årlig fremover som en del av utvalgets arbeid for å gjøre offentligheten kjent med kontrollen av EOS-tjenestene og for å bidra til en debatt om kontrollen og resultatene av den. De gode tilbakemeldingene på konferansene de siste årene gjør oss trygge på at det er verdt ressursbruken.

EOS-utvalget er særlig opptatt av å lære hvordan andre land utfører sin kontroll for å bli bedre i sitt kontrollarbeid. Som en del av dette arbeidet reiste hele utvalget og fire ansatte i sekretariatet til Washington DC i september på en studietur over fem dager.

USA har 17 etterretningstjenester, og budsjettet til USAs e-tjenester er mange ganger større enn hva de norske tjenestene har. Det er også mange flere kontrollorganer og mennesker som jobber med kontroll. Likevel er det problemstillinger som er felles for kontrollorganer i USA og EOS-utvalget.

Noen av dem vi møtte i USA var:
- senator Ron Wyden (D) som sitter i Senatets kontrollkomité for etterretningstjenestene,
- sekretariatsledelsen i Senatets kontrollkomité,
- NSAs Deputy Inspector General,
- Privacy and Civil Liberties Oversight Boards' sekretariat,
- Office of the Director of National Intelligence,
- Justisdepartementets Office of Intelligence,
- representanter fra tenketanken New America og NGO-ene Access Now og Center for Democracy and Technology.

Noen av problemstillingene vi diskuterte var:
- gode systemer for varslere,
- åpenhet om hva tjenestene og kontrollørene gjør,
- forholdet mellom internkontroll og uavhengig ekstern kontroll,
- direkte tilgang på datasystemene til tjenestene,
- hvordan domstolene kontrollerer etterretningen,
- hvordan veldig polarisert politisk debatt påvirker kontrollen,
- konkrete metoder og tilnærming til legalitetskontroll.

En oversikt over utvalgets og sekretariatets møter, besøk og konferanser i 2018 gis i vedlegg 1.

10.3 EOS-utvalget i media i 2018

EOS-utvalget stiller opp for media når vi har mulighet og lov til det. Vi ønsker også å få oppmerksomhet i mediene om våre meldinger til Stortinget. Dette bidrar til økt kunnskap og åpenhet om kontrollen med EOS-tjenestene.

I mars hadde NRK flere saker om E-tjenestens stasjon på Eggemoen og overvåkingen av satellitter som skjer derfra. Dette var blant annet basert på dokumenter fra Snowden-lekkasjen i 2013. Utvalgsleder Løwer viste i intervjuer med NRK til vår særskilte melding fra 2016 der vi stilte spørsmål om rettsgrunnlaget for deler av E-tjenestens overvåkingsvirksomhet – som var relevant for problemstillingene NRK tok opp.

I forbindelse med den saken gikk også Løwer ut i Dagbladet mot forsvarsminister Frank Bakke Jensen og sa at han «skyver oss foran seg», da statsråden ifølge Dagbladet hevdet at «EOS-utvalget har konkludert med at aktiviteten er innenfor norsk lov». Den konklusjonen kom vi aldri med.

Sakene som fikk oppmerksomhet i flere medier etter at årsmeldingen for 2017 ble publisert i april, var særlig:
- PST som ved et par tilfeller hadde overvåket enkeltpersoner lenger enn hva retten hadde tillatt.
- NSM og en klareringsmyndighet som fikk sterk kritikk fordi de hadde gjennomført en prosess for sikkerhetsklarering av en person, som det ikke var grunnlag for å starte. Dette førte til store personlige, arbeidsmessige og økonomiske konsekvenser for vedkommende.

Ellers skrev NRK om PSTs endrede åpenhet om internasjonalt samarbeid som påvirket uttalelsen vi skrev sammen med fire andre kontrollorganer. Les mer i punkt 3.2 og vedlegg 6. I en lederartikkel i Morgenbladet i november, som handlet om forslaget til ny e-lov, ble også denne uttalelsen nevnt.

ABC Nyheter brakte en nyhetsartikkel om PSTs ulik bruk av overskuddsinformasjon. Utvalget påpekte at det er tvilsomt om det skal være ulik adgang til å bruke overskuddsinformasjonen fra kommunikasjonskontroll avhengig om avlyttingen er brukt som en del av en etterforskingssak eller en forebyggende sak.

I april skrev også utvalgsleder Eldbjørg Løwer et svar til Kjetil Stormark, redaktør for aldrimer.no, der hun påpekte at vi gjør alt vi kan for å beskytte anonymiteten til varslere som kommer til EOS-utvalget, jf. punkt 3.3.

10.4 Administrative forhold

Utvalgets utgifter i 2018 har vært på kr 18 951 810 mot budsjett, inkludert overførte midler, på kr 19 550 000. Mindreforbruket skyldes i hovedsak permisjoner i utvalgets sekretariat og at det har tatt tid å rekruttere ansatte – særlig til teknologstillinger. Det har ført til ubrukte lønnsmidler. Av ubrukte midler er kr 598 089 søkt overført til budsjettet for 2019.

Utvalget fikk 18. desember 2018 ved Stortingets vedtak 305 bevilget 29 000 000 til nytt lokale over statsbudsjettet for 2019. Vi er tilfredse med Stortingets bevilgning. Det er medgått mye tid til planlegging av nytt lokale i 2018. Utvalget forventer å kunne flytte inn våren 2019.

Det er fortsatt behov for å utvide sekretariatet med flere ansatte. Utvalget kommer tilbake til dette i forbindelse med budsjettprosessen for 2020.

Legalitetskontroll
Kontroll av at rettsregler er fulgt.

Overskuddsinformasjon
Opplysninger innhentet for eksempel ved bruk av skjulte tvangsmidler, og som har relevans for andre straffbare forhold enn det som begrunnet tvangsbruken eller opplysninger som ikke har relevans for det straffbare forhold.

11.

Vedlegg

VEDLEGG 1 – Møter, besøk og deltakelse på konferanser mv.

Møte med Teknologirådets sekretariat
En ansatt i sekretariatet var i januar hos Teknologirådet for å fortelle hvordan EOS-utvalget utfører sin kontroll.

Møte med sekretariatsleder for Kontrollutvalget for kommunikasjonskontroll (KK-utvalget)
Tre fra sekretariatet møtte i januar den nye sekretariatslederen for KK-utvalget. De har fått utvidet mandat – blant annet skal de kontrollere det ordinære politiets dataavlesing. Møtet var for å utveksle erfaringer med et utvalg som har et mandat med flere grenseflater opp mot EOS-utvalget.

Deltakelse på KK-utvalgets fagdag
Et utvalgsmedlem og to fra sekretariatet deltok i februar på KK-utvalgets fagdag. Vi orienterte dem om EOS-utvalgets oppgaver og diskuterte mulig samarbeid og felles problemstillinger.

Kontaktmøte med journalister
Ni journalister kom i februar på besøk til utvalgsleder og to fra sekretariatet etter at EOS-utvalget inviterte journalister som er opptatt av «EOS-saker». Målet med møtet var å knytte kontakt med interesserte journalister og gi informasjon til journalistene som kunne bidra til forståelsen for vår kontrolloppgave.

Presentasjon for Norsk PEN
Utvalgsleder var i mars invitert av Overvåkingsutvalget til Norsk PEN for å presentere EOS-utvalgets arbeid og diskutere problemstillinger.

Konferanse i regi av den tyske forbundsdagen i Berlin
Et utvalgsmedlem og en fra sekretariatet deltok i mars på en konferanse som handlet om etterretningstjenester i en rettsstat.

Møte med Sivil klareringsmyndighet
To ansatte i sekretariatet møtte i april den nye lederen av den nye virksomheten Sivil klareringsmyndighet.

Presentasjon på Beredskapskonferansen
Utvalgsleder holdt i april et innlegg på Nasjonal Beredskapskonferanse 2018 om EOS-utvalgets virksomhet og problemstillinger rundt overvåking og personvern.

EOS-utvalgets årskonferanse
Utvalget arrangerte 11. april sin årskonferanse. I 2018 var det over 100 deltakere, og temaene i 2018 var i tillegg til årsmeldingen for 2017 blant annet «Åpenhet i tjenestene», «5 år etter Snowden» og «Smart etterretning og automatisert kontroll».

Sikkerhetskonferanse i Trondheim
Et utvalgsmedlem deltok i mai på informasjonssikkerhetskonferansen Sikkerhet og sårbarhet i Trondheim.

Deltakelse på debatt om åpenhet i Forsvaret
Utvalgsleder var invitert til å holde innlegg på en konferanse i mai i regi av Institutt for forsvarsstudier (IFS) og Senter for integritet i forsvarssektoren (SIFS). Temaet var åpenhet og akademisk frihet i forsvarssektoren.

Deltakelse på arbeidsverksted i Berlin
En fra sekretariatet dro i mai til den tyske hovedstaden for å delta på et arbeidsverksted. Det var i regi av den tyske tenketanken Stiftung Neue Verantwortung som hadde samlet flere kontrollorganer og eksperter for å utveksle «best practices». Dette arbeidsverkstedet var noe av grunnlaget for tenketankens publikasjon «*Upping the ante on bulk surveillance – An international compendium of good legal safeguards and oversight innovations*».

EOS-utvalgets årskonferanse har både innledere fra inn- og utland. Debatten som er avbildet her handlet om 5 år etter Snowden og åpenhet i tjenestene.

Fra venstre: Journalist Ryan Gallagher i The Intercept, Tidligere sjef E Kjell Grandhagen, Sjef PST Benedicte Bjørnland, Gerald Folkvord fra Amnesty, professor Iain Cameron og ordstyrer Anne Grosvold.

Foto: EOS-utvalget

Presentasjon i Ukraina
Utvalgets nestleder var i Kiev i mai på et seminar for ukrainske parlamentarikere som handlet om ny lov for sikkerhetstjenestene og kontroll med tjenestene. Nestlederen holdt et foredrag om den norske modellen for kontroll med hemmelige tjenester. Seminaret var i regi av Ukrainas parlament, NATO, EU og DCAF.

Besøk fra Datatilsynet
Datatilsynets direktør og en fagdirektør var i juni på besøk for å fortelle EOS-utvalget om problemstillinger knyttet til kunstig intelligens og personvern.

Møter med andre kontrollorgan om felles prosjekt
I juni (København) og oktober (Bern) var ansatte i sekretariatet og utvalgsleder (Bern) i møte med kontrollorganer fra Danmark, Belgia, Nederland og Sveits i forbindelse med prosjektet de fem kontrollorganene har hatt siden 2015. Dette ledet til at vi i november publiserte en felles uttalelse – «*Strenghtening oversight of international data exchange between intelligence and security services*». Les mer i punkt 3.2 og vedlegg 6.

Arbeidsverksted og presentasjon i England
I juli deltok en fra sekretariatet på et arbeidsverksted om kontroll med hemmelige tjenester i Colchester. Det var i regi av University of Essex og det britiske kontrollorganet IPCO. Det var deltakere fra Storbritannia, Israel, Norge og Nederland.

Presentasjon for armensk delegasjon
Utvalgets nestleder holdt i september et innlegg for en delegasjon fra Armenia om EOS-utvalgets virksomhet. Delegasjonen var på besøk hos Ombudsmannen for Forsvaret.

Konferanse i Berlin om kontrollsamarbeid
En ansatt i sekretariatet deltok i september på en konferanse om muligheter for samarbeid mellom kontrollorganer i Europa. Konferansen ble arrangert av tre forskjellige organisasjoner fra det tyske sivilsamfunnet.

Studietur til USA
Hele utvalget og fire fra sekretariatet var på studietur i Washington DC i fem dager i september for å lære mer om USAs kontroll med etterretningstjenestene. Les mer om denne studieturen i kapittel 10.2.

Møte med Ombudsmannen for Forsvaret
Utvalgsleder og representanter fra sekretariatet møtte i oktober ombudsmannen for å diskutere metoder og felles problemstillinger.

Lansering av bok med forordet av EOS-utvalget
Utvalgsleder holdt i oktober et innlegg hos NUPI ved lanseringen av boken «*Intelligence oversight in the twenty-first century*». Utvalgsleder har skrevet forordet til boka. Boka har blant annet sin bakgrunn i presentasjoner på EOS-utvalgets konferanse i anledning 20-årsjubileet i 2016.

Møte med Advokatforeningen
Utvalgsleder og to fra sekretariatet møtte i oktober Advokatforeningen, representert ved blant annet leder og generalsekretær. EOS-utvalgets arbeid generelt og behandling av klagesaker spesielt ble diskutert.

Foredrag for Stortingets administrasjon
Sekretariatsleder holdt et innlegg i november om EOS-utvalgets virksomhet.

Deltakelse på Nasjonalt internettforum
En fra sekretariatet deltok i november på en konferanse om internett i Norge som var arrangert av Nasjonal kommunikasjonsmyndighet og Norid.

Foredrag ved Forsvarets Høgskole
Utvalgsleder og leder for sekretariatets teknologiske enhet holdt i november hvert sitt foredrag for studenter ved Etterretningsemnet hos Forsvarets Høgskole.

Møte hos Norsk informasjonssikkerhetsforum (ISF)
I november deltok en fra sekretariatet på julemøtet til ISF, der EOS-utvalget er medlem.

Internasjonal kontroll-konferanse på Malta
En fra sekretariatet deltok i november på den tredje utgaven av International Intelligence Oversight Forum. FNs spesialrapportør for personvern, Joe Cannataci, stod for arrangementet. Den ansatte holdt også et foredrag om EOS-utvalgets kontrollfunksjon. I 2018 var konferansen på Malta og deltakere fra over 20 land og alle verdensdeler utenom Sør-Amerika var representert. Samarbeid mellom kontrollorganer var et av flere sentrale temaer på konferansen. I tillegg til kontrollorganer deltok også representanter fra akademia, sivilsamfunnet, påtalemyndigheter, datatilsyn, parlamentariske komiteer og byråkratiet.

Møte mellom kontrollorganer i Paris
I regi av Frankrikes og Belgias kontrollorganer dro utvalgsleder og leder for sekretariatets teknologiske enhet i desember til Paris sammen med representanter fra 13 andre europeiske land. Målet med konferansen var å få til tettere samarbeid og flere møter mellom kontrollorganer i Europa.

Der det ikke står definert noe stedsnavn har arrangementet vært i Oslo.

VEDLEGG 2 – Nyheter fra kontrollorganer i andre land

Danmark
Tilsynet for Efterretningstjenesterne fant ut at i hver femte stikkprøve hos Forsvarets Efterretningstjeneste var det søkt i rådata om dansker uten rettsgrunnlag. Politiets Efterretningstjeneste fikk blant annet kritikk for ikke å ha overholdt slettefrister.

Nederland
En ny lov om etterretningstjenestene, som gir dem større fullmakter – inkludert en form for «digitalt grenseforsvar» – ble implementert i 2019.

Kontrollorganet CTIVD har sett på hvordan landets to tjenester har implementert den nye loven og har kritisert dem for å mangle gode systemer for både internkontroll og systemer som skal sikre at ikke mer data enn nødvendig lagres.

CTIVD har også laget en rapport der de undersøkte det multilaterale samarbeidet i Counter-Terrorism Group (et europeisk samarbeid som har hovedsete i Nederland.) De fant flere forbedringsmuligheter og mente kontrollmulighetene ikke var gode nok.

I årsmeldingen for 2017 skrev de blant annet om lovbrudd ved tjenestenes bruk av dataavlesing/hacking. De kontrollerte også masse-innsamling av data fra det åpne nettet. CTIVD kontrollerte fire store datasett. Et par av dem inneholdt personlige data som navn, e-post-adresser, postadresser og passord. CTIVD mente at ett av datasettene var ulovlig innsamlet fordi det ikke var tilstrekkelig politisk godkjenning bak.

Storbritannia
Parlamentets The Intelligence and Security Comittee beskrev i to rapporter hvordan britiske etterretningstjenester medvirket til tortur og bortføring av terrormistenkte etter angrepene mot USA 11. september 2001.

New Zealand
I årsmeldingen for 2017/2018 skriver Inspector-General for Intelligence and Security at de har sjekket alle som har klaget på grunnlag av mistanke om at de er under overvåking av landets hemmelige tjenester. Generalinspektøren skriver at hun har fått bekreftet at tjenestene ikke har lagret noe informasjon om dem. For å sammenligne med Norge – EOS-utvalget har i utgangspunktet bare lov å si om det er grunn til å kritisere tjenesten eller ei.

Finland
En lov som vil gi e-tjenestene flere fullmakter ligger til behandling i parlamentet. Lovforslaget inkluderer også et forslag om at landet for første gang vil få et uavhengig spesialisert kontrollorgan for de hemmelige tjenestene.

USA
For første gang publiserte National Security Agencys Inspector General en offentlig versjon av en halvårsrapport. Blant annet skriver generalinspektøren at bare 12 av 72 anbefalinger fra ham om «intelligence oversight» var implementert da rapporten ble levert. Halvparten av anbefalingene hadde ligget på vent i minst ett år hos NSA.

Canada
Et lovforslag i det kanadiske parlamentet foreslår at det skal opprettes ett kontrollorgan – National Security and Intelligence Review Agency (NSIRA) – som skal føre kontroll med alle tjenestene. Nå har hver tjeneste hvert sitt kontrollorgan. NSIRA vil trolig bli verdens største uavhengige kontrollorgan. Det er også opprettet en egen komite i det kanadiske parlamentet som skal føre kontroll med de hemmelige tjenestene.

VEDLEGG 3 – Høring om forslag til ny lov om Etterretningstjenesten

Forsvarsdepartementet
Postboks 8126 Dep
0032 OSLO

12. februar 2019

Høringssvar fra EOS-utvalget – høring om forslag til ny lov om Etterretningstjenesten

Del I – Innledning og overordnede merknader

1. Innledning

EOS-utvalget viser til Forsvarsdepartementets (FD) høringsbrev 12. november 2018 om forslag til ny lov om Etterretningstjenesten og inngir med dette vår høringsuttalelse.

EOS-utvalget praktiserer en høy terskel for å inngi høringssvar. Det ligger ikke til utvalgets mandat å ha synspunkter på hvilke overvåkingsmetoder E-tjenesten gis av Stortinget som lovgiver. Men forslaget til ny e-lov griper direkte inn i EOS-utvalgets kontroll og gir dermed grunn til enkelte merknader herfra. I tillegg ser utvalget konsekvenser av forslaget som bør fremkomme før Stortinget behandler et lovforslag.

Utvalget har merket seg at høringsnotatet gjennomgående viser til EOS-utvalget som en sikringsmekanisme. Det er viktig å understreke at EOS-utvalget ikke er en garantist for at feil ikke skjer eller ikke kan skje i EOS-tjenestene. Vår kontroll er stikkprøvebasert og legger ikke opp til en fullstendig gjennomgang av all overvåkingsvirksomhet i EOS-tjenestene. En grunnleggende forutsetning for vår kontroll er vår innsynsrett – som trolig har en sterk disiplinerende og dermed preventiv effekt.

Utvalgets kapasitet er i dag fullt utnyttet.[50] Flere kontrolloppgaver vil medføre behov for ytterligere prioriteringer for utvalgets medlemmer. Som et minimum bør sekretariatet styrkes vesentlig, for at utvalget skal kunne møte de forventningene som stilles til kontrollen. Det kan være grunn til å foreta en mer overordnet gjennomgang av kontrollmodellen, jf. punkt 2 nedenfor.

2. Kontroll som forutsetning for lovlighet

Evalueringsutvalget konkluderte med at «den norske modellen for demokratisk og parlamentarisk forankret kontroll med EOS-tjenestene er internasjonalt anerkjent som god».[51] Departementet viser til at kontrollmodellen nylig er evaluert og opprettholdt av Stortinget.[52] På bakgrunn av avgjørelser fra EMD oppfatter departementet at kontrollmekanismene er blant forutsetningene for at bulkinnsamling skal være i samsvar med EMK.[53]

50 Stortingets presidentskap nedsatte 27. mars 2014 et utvalg som skulle evaluere EOS-utvalgets virksomhet og rammebetingelser («Evalueringsutvalget»). Evalueringsutvalget leverte sin rapport til Stortinget 29. februar 2016: *Rapport til Stortinget fra Evalueringsutvalget for Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste*, Dokument 16 (2015-2016) («Evalueringsrapporten»). Om utvalgets kapasitet, se Evalueringsrapporten punkt 31.2.

51 Evalueringsrapporten punkt 1.

52 Høringsnotatet punkt 11.12.5.2.

53 Høringsnotatet punkt 11.23.3.

Departementet drøfter deretter hvilke kvalitetskrav som må stilles til kontrollen og hvilke kontrolloppgaver som må kunne utføres.

I lys av dette vil utvalget fremheve Stortingets tidligere forventning om utredning av kontrollmodellen. I kontroll- og konstitusjonskomiteens innstilling til Evalueringsrapporten står følgende:[54]

> «En raskt akselererende teknologiutvikling, økt globalisering og et stadig mer sammensatt trusselbilde endrer forutsetningene for overvåking og dermed for EOS-utvalgets kontroll med metodene. Komiteen har merket seg at Evalueringsutvalget peker på sannsynligheten for økt kompleksitet og omfang av kontrolloppgavene, blant annet med henvisning til eventuelle konsekvenser av 'digitalt grenseforsvar' som Forsvarsdepartementet har varslet en gjennomgang av. Komiteen registrerer at Evalueringsutvalget vurderer det som **vanskelig å utvide den parlamentariske kontrollen med de hemmelige tjenestene uten en gjennomgang av hele modellen for kontroll**.
>
> Komiteen registrerer videre at Evalueringsutvalget ikke har foretatt denne gjennomgangen, men nøyer seg med å peke på behovet for nytenkning. I lys av de utviklingstrekkene Evalueringsutvalget beskriver, **mener komiteen at nettopp kontrollmodellen burde vært med i dette utvalgsarbeidet, men tar til etterretning at Stortinget må komme tilbake til dette spørsmålet**» (utvalgets uthevinger).

Etter disse merknadene fra komiteen 15. desember 2016 er nettopp et «digitalt grenseforsvar» (nå kalt tilrettelagt innhenting) blitt utredet og sendt på høring. Videre har EMD i sine avgjørelser lagt vekt på kontrollmekanismer som en forutsetning for lovligheten av overvåkingstiltak.[55]

Utvalget mener at flere aspekter ved kontrollmodellen kontinuerlig kan vurderes – uten å rokke ved modellens grunnleggende styrke i kraft av parlamentarisk forankring, uavhengighet, innsynsrett og utvalgets sammensetning.

Det vises for øvrig til Evalueringsutvalgets vurderinger av utvalgsmodellen og forholdet til det samlede kontrollsystemet.[56] Utvalget legger Evalueringsutvalgets redegjørelse for de konstitusjonelle rammene for utvalgets virksomhet til grunn, som blant annet innebærer at virksomheten er rent kontrollerende.[57]

I lys av de hjemler som foreslås gitt til Etterretningstjenesten, reiser utvalget spørsmål om kontrollmodellen er vurdert i slik bredde som synes forventet av Stortinget.

Del II – Merknader til forslag til ny lov om Etterretningstjenesten

- Vi vil overordnet påpeke at forslaget ikke løser sentrale uklarheter for Etterretningstjenestens overvåking av personer i Norge. Videre er flere av utvalgets kritiske merknader blitt omgjort til unntak fra forbudet mot

54 Innstilling fra kontroll og konstitusjonskomiteen om Rapport fra Evalueringsutvalget for Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget) om evaluering av EOS-utvalget, Innst. 146 S (2016–2017) s. 47.

55 *Centrum for rättvisa mot Sverige* avsagt 19. juni 2018 (ikke rettskraftig) og *Big Brother Watch mfl. mot Storbritannia* avsagt 13. september 2018 (ikke rettskraftig).

56 Se Evalueringsrapporten punkt 31 og 37.

57 Se Evalueringsrapporten punkt 1, 10 og 29. I punkt 10 uttalte Evalueringsutvalget følgende: «EOS-utvalgets forankring i Stortinget er avgjørende for å forstå utvalgets rolle, oppgaver og handlingsrom. Konstitusjonelt har det som konsekvens at utvalget er reelt uavhengig av de tjenestene det kontrollerer. På den annen side begrenser det utvalgets myndighet overfor tjenestene, blant annet ved at det kan påpeke og kritisere kritikkverdige forhold, men ikke instruere tjenestene, eller fungere som rådgiver for dem».

overvåking av personer i Norge. Konsekvensen av dette er at Etterretningstjenesten vil få utvidede fullmakter i Norge.

- Vi vil særlig fremheve forslaget om at E-tjenestens *hensikt* skal være avgjørende for dens mulighet til å innhente informasjon om personer i Norge. For det første er kriteriet lite egnet for reell, etterfølgende kontroll fra vår side. For det andre synes kriteriet å tilsløre den omstendighet at Etterretningstjenesten kan benytte metoder mot personer i Norge – så lenge altså «hensikten» er rettet mot andre.

3. Merknader til forslagets § 2-8 – Tilretteleggingsplikt og innsyn

Høringsnotatet tar opp behovet for rettsregler som legger til rette for effektiv kontroll med Etterretningstjenestens virksomhet.[58] Dette gjenspeiles i forslaget til formålsbestemmelse i § 1-1 b, om at *loven skal bidra til å trygge tilliten til og sikre grunnlaget for kontroll med Etterretningstjenestens virksomhet.*

Utvalget mener at det bør inntas en bestemmelse om *tilretteleggingsplikt* fra E-tjenestens side overfor EOS-utvalget, for eksempel i foreslåtte § 2-8. Dette vil tydeliggjøre tjenestens plikt til å bidra til å sikre grunnlaget for effektiv kontroll med tjenestens virksomhet. Utvalget må få spille en aktiv rolle i utviklingen av tilretteleggingen for kontroll. Utvalget mener at en forutsetning for effektiv kontroll, spesielt for eventuell fremtidig kontroll med tilrettelagt innhenting, er at utvalget får egne verktøy for kontroll i tjenestens systemer.

Videre mener utvalget at unntaket fra utvalgets innsynsrett i informasjon som E-tjenesten selv har definert som særlig sensitiv informasjon (SSI), bør vurderes inntatt i forslaget til § 2-8, og eventuelt i EOS-kontrolloven § 8.[59]

4. Merknader til forslagets § 2-10 – Behandling av personopplysninger

I høringsnotatet skriver departementet at den foreslåtte videreføringen av dagens regel om at E-tjenesten er unntatt fra Datatilsynets og Personvernnemdas tilsynsmyndighet, uavhengig av formålet med behandlingen, «også er begrunnet i hensynet til et enhetlig kontrollregime som innebærer at EOS-utvalget også kontrollerer Etterretningstjenestens behandling av personopplysninger uavhengig av formål».[60]

EOS-utvalget presiserer at utvalget kun kontrollerer behandling av personopplysninger som faller inn under kontrollområdet; etterretnings-, overvåkings- og sikkerhetstjeneste. Lovteksten bør reflektere dette.

5. Merknader til forslagets § 4-1 – Problemstillinger knyttet til etterretningsvirksomhet og forholdet til personer og virksomheter som oppholder seg i Norge

5.1 Territoriell begrensing – bakgrunn

Forbudet i gjeldende lov om etterretningstjenesten § 4 lyder slik:

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

58 Høringsnotatet punkt 6.6.

59 Stortinget besluttet i et plenarvedtak i 1999 at det skulle gjelde en særskilt prosedyre for tvist om innsyn i E-tjenestens dokumenter. Vedtaket førte ikke til endring i utvalgets lov eller instruks, se Dokument nr. 16 (1998–99), Innst. S. nr. 232 (1998–99) og referat og vedtak i Stortinget 15. juni 1999. Bakgrunnen for Stortingets vedtak fra 1999 er den særlige sensitiviteten som knytter seg til enkelte av E-tjenestens kilder, identiteten til personer i okkupasjonsberedskapen og spesielt sensitive opplysninger mottatt fra utenlandske samarbeidende tjenester. EOS-utvalget ba i 2013 Stortinget avklare om utvalgets innsynsrett slik den er nedfelt i lov og instruks skal gjelde fullt ut også for E-tjenesten, eller om Stortingets vedtak fra 1999 skal opprettholdes. På Stortingets anmodning ble spørsmålet behandlet i rapporten fra Evalueringsutvalget for EOS-utvalget, som ble avgitt til Stortinget 29. februar 2016, se Dokument 16 (2015–2016). Ved behandlingen av rapporten fra Evalueringsutvalget i 2017, ble begrensningen i innsynet i «særlig sensitiv informasjon» opprettholdt, men uten at lovteksten ble endret.

60 Høringsnotatet punkt 12.3.2.2.

Departementet viser til at forslaget bygger på dagens prinsipielle utgangspunkt og hovedregel om at Etterretningstjenesten ikke skal drive rettet innhentingsvirksomhet mot personer og virksomheter som befinner seg i Norge.[61] Departementet viser til at «[d]et er gjeldende oppfatning i dag at forbudet mot fordekt innhenting «om» norske personer i etterretningstjenesteloven § 4 første ledd, må forstås som fordekt innhenting «rettet mot» norske personer», samt at «[f]ordekt-begrepet relaterer seg til selve innsamlingsmetoden og fokuset for innsamlingen, og ikke til den etterfølgende analysen og sammenstillingen av allerede innsamlet informasjon».[62]

Utvalget er uenig i at forbudet mot fordekt innhenting «om» norske personer i etterretningstjenesteloven § 4 første ledd, må forstås som fordekt innhenting «rettet mot» norske personer». Vi har tidligere tatt opp hvordan begrepet «om» i någjeldende § 4 skal forstås. I Særskilt melding til Stortinget om rettsgrunnlaget for Etterretningstjenestens overvåkingsvirksomhet, omtalte utvalget E-tjenestens søk i lagrede metadata knyttet til norske rettssubjekter i Norge for å finne selektorer for utenlandsetterretningsrelevante formål.[63] Etter utvalgets mening kunne en slik metodikk vanskelig utledes av dagens regelverk. Utvalget var *ikke* enig i at «fordekt-begrepet» relaterer seg til selve innsamlingsmetoden og fokuset for innsamlingen, og ikke til den etterfølgende analysen og sammenstillingen av allerede innsamlet informasjon. Utvalget uttalte:[64]

> «E-tjenesten peker på at begrepet «fordekt» i forbudet viser til selve innhentingen av informasjon, og ikke etterfølgende søk og sammenstilling. Utvalget deler ikke denne forståelsen. Aktive søk i, og sammenstilling av opplysninger fra selektorer tilhørende identifiserte norske rettssubjekter som stammer fra en fordekt innhentingskapasitet, kan ikke anses som noe annet enn målrettet informasjonsinnhenting mot disse, selv om formålet ikke er å innhente informasjon om de norske rettssubjektene. Ved søk og analyse behandles alltid ny informasjon. Dette vil gjelde uavhengig av E-tjenestens faglige vurdering av relevansen isolert sett. Forbudet i e-loven § 4 begrenser tjenestens mulighet til å innhente informasjon av utenlandsetterretningsmessig relevans. Hvorvidt E-tjenesten *bør* eller *ikke bør* være pålagt en slik innskrenking, er etter utvalgets oppfatning en lovgiveroppgave å ta stilling til.»

Utvalget konstaterer at våre merknader til hvordan begrepet «om» i någjeldende § 4 skal forstås, ikke er tatt i betraktning i høringsnotatet.

Utvalget er fortsatt av den oppfatning at någjeldende forbud i e-loven § 4 begrenser tjenestens mulighet til å innhente informasjon i Norge av utenlandsetterretningsmessig relevans. Utvalget registrerer at lovforslaget ikke legger opp til en slik innskrenking når det innfortolkes en begrensing om innhentingsvirksomhet med overvåkingshensikt i bestemmelsen.

Etter utvalgets oppfatning innebærer reguleringen en utvidelse av E-tjenestens mulighet til å innhente informasjon av utenlandsetterretningsmessig relevans i Norge, sammenlignet med dagens rettstilstand. Om E-tjenesten bør eller ikke bør være pålagt en begrensing i muligheten til å innhente informasjon av utenlandsetterretningsmessig relevans i Norge, må Stortinget som lovgiver ta stilling til.

5.2 Nærmere om «overvåkingshensikt»

Den foreslåtte territorielle begrensingen i ny § 4-1 omhandler bruk av E-tjenestens metoder «rettet mot» personer i Norge. Med «rettet mot» innfortolkes det en *overvåkingshensikt*.

61 Høringsnotatet punkt 8.4.3.4.

62 Høringsnotatet punkt 8.2.2.5 side 117.

63 Dokument 7:2 (2015–2016) *Særskilt melding til Stortinget om rettsgrunnlaget for Etterretningstjenestens overvåkingsvirksomhet*, punkt 5.3.3. Meldingen omtales heretter som «Særskilt melding 2016»

64 Særskilt melding 2016, punkt 5.3.3.

Som utvalget uttalte i Særskilt melding 2016, «er utfordringen med en slik forståelse at lovgivningen ikke gir anvisning på hvor grensen likevel må gå. Dette reiser spørsmål om når overvåkingshensikt inntrer og hvor inngripende tiltaket er i personvernet».[65]

Innhentingsforbudet i dagens lov for E-tjenesten setter forbud mot «*all innhenting, herunder gjennom åpne kilder og fordekte innhentingsdisipliner, av informasjon rettet mot personer eller virksomheter i Norge*».[66] Etter utvalgets oppfatning kan det vanskelig trekkes ut av ordlyden i forbudet i gjeldende § 4 at det er tjenestens *hensikt* som skal avgjøre om overvåking av personer i Norge er i strid med forbudet eller ikke. Utvalget bemerker også at det kan bli vanskelig å kontrollere hva slags *hensikt* E-tjenesten har i det enkelte tilfellet, noe som kan illustreres med følgende tenkte eksempel:

> En person returnerer til Norge etter at vedkommende har vært et etterretningsmål for E-tjenestens innsamling i utlandet. På grunn av innhentingsforbudet i foreslåtte § 4-1, må all innhenting mot personen stoppes når vedkommende oppholder seg i Norge. Men ettersom lovforslaget forutsetter at innhentingsforbudet bare skal gjelde der det foreligger *overvåkningshensikt* fra Etterretningstjenestens side, kan E-tjenesten fortsette å gjennomføre søk i rådata med utgangspunkt i vedkommendes personselektorer,[67] samt fortsette å innhente informasjon gjennom åpne kilder tilhørende den returnerte personen.[68] Forutsetningen for denne videre metodebruken/innsamlingen er at den ikke er «rettet mot» den returnerte personen, men «rettet mot forhold eller personer i utlandet». Dette vil det være vanskelig for utvalget å kontrollere.

I forbindelse med Særskilt melding 2016 uttalte E-tjenestens selv at «[f]okus er på informasjon og ikke på individer, og i utgangspunktet er det intet stigmatiserende for en person å bli gjenstand for E-tjenestens søkelys».[69] Dette taler etter utvalgets syn for at kriteriet *overvåkingshensikt* er et lite egnet kriterium for et territorielt innhentingsforbud. Uttrykket «rettet mot» kan tilsløre det faktum at E-tjenestens metoder rent faktisk kan benyttes i etterretningsøyemed på kommunikasjonen til personer som oppholder seg i Norge.

Dersom «overvåkingshensikt» skal være kriteriet for å vurdere om tjenesten kan rette sine metoder mot personer i Norge eller, åpner dette i prinsippet for at alle tjenestens metoder, herunder fordekte innhentingsdisipliner, kan benyttes opp imot kommunikasjonen til personer som oppholder seg i Norge, så lenge innsamlingen anses «rettet mot forhold eller personer i utlandet». Skiftende tider, nye samfunnsutfordringer og uventede trusler kan skape endrede behov for å innhente informasjon av utenlandsetterretningsmessig relevans i Norge. Et kriterium om overvåkingshensikt i innsamlingen av kommunikasjonen til personer som oppholder seg i Norge vil dermed kunne medføre en fare for uthuling av den forslåtte «territorielle begrensingen» for E-tjenestens overvåkingsvirksomhet.

Dersom det ikke skal begrenses hva E-tjenesten kan innhente av informasjon om norsk kommunikasjon av utenlandsetterretningsmessig relevans i Norge, bør dette gå klart frem av loven.

5.3 Konklusjon

Utvalget mener at *overvåkingshensikt («rettet mot»)* er et lite egnet kriterium for et territorielt innhentingsforbud for E-tjenesten. Utvalget mener at innhentingsforbudet for E-tjenesten på norsk territorium må klargjøres i det videre arbeidet med ny lov om Etterretningstjenesten.

65 Særskilt melding 2016, punkt 5.2.3.2.
66 Høringsnotatet punkt 8.4.3.4.
67 Jf. forslaget § 4-2 syvende ledd.
68 Jf. forslaget § 4-2 siste ledd.
69 Særskilt melding 2016, punkt 1.5 om E-tjenestens overordnede vurderinger.

6. Merknader til forslagets § 4-2 – Unntak fra og presiseringer av forbudet i § 4-1

6.1 Merknader til forslagets§ 4-2 første ledd – Innhenting av informasjon om fremmed etterretningsvirksomhet i Norge

Utvalget merker seg departementets vurdering om at innhenting mot *norske statsborgere*[70] i Norge som driver med fremmed etterretningsvirksomhet, ikke lenger skal tilligge Etterretningstjenestens oppgavesett.

I dag omfatter ikke utvalgets kontrolloppgave virksomhet «som angår utlendinger hvis opphold er knyttet til tjenesten for fremmed stat».[71] Gitt at denne begrensningen bortfaller med forslaget til ny EOS-kontrolloven § 5 femte ledd, mener utvalget det bør vurderes en eksplisitt *varslingsplikt* til EOS-utvalget når PST har gitt samtykke til at E-tjenesten kan bedrive etterretningsvirksomhet i Norge etter unntaksbestemmelsen i forslagets § 4-2 første ledd siste punktum. Det samme bør gjelde der E-tjenesten eventuelt iverksetter innhenting uten samtykke fra PST, mot personer som opptrer på vegne av fremmed makt eller virksomhet som utøves av fremmed makt i Norge (annen «fremmed aktivitet»).

6.2 Merknader til forslagets§ 4-2 andre og tredje ledd – kilder og kildeverifikasjon

I *særskilt melding om utvalgets undersøkelse av opplysninger om norske kilder mv. i Etterretningstjenesten*[72], var en av konklusjonene at utvalget ikke hadde avdekket at tjenesten har overtrådt forbudet i e-loven § 4 mot å overvåke eller på annen fordekt måte innhente informasjon om norske fysiske og juridiske personer på norsk territorium.

Utvalget registrerer at forslaget til § 4-2 andre ledd oppstiller unntak fra innhentingsforbudet for E-tjenesten. Det foreslås hjemler for fordekt innhenting av opplysninger om potensielle kilder, samt for kildeverifiseringsformål. Utvalget merker seg spesielt at E-tjenesten vil kunne iverksette fordekte HUMINT-operasjoner mot disse i Norge i en begrenset periode, når det foreligger «tungtveiende sikkerhetsmessige grunner». Slike operasjoner «kan inkludere infiltrasjon og provokasjon», samt fordekt «systematisk innhenting av informasjon gjennom samhandling mellom mennesker», jf. §§ 6-3 og 6-4.

Forslaget synes å innebære en utvidelse av hjemlene etter gjeldende rett. Det er opp til lovgiver å avgjøre hva slags etterretningsmetoder tjenesten skal kunne anvende *i Norge* for «å frembringe relevant informasjon for å finne potensielle kilder eller gjennomføre kildeverifikasjon». For utvalget vil det bli utfordrende å kontrollere de utpregede skjønnsmessige vurderingene paragrafen oppstiller, blant annet med tanke på hva som vil være «strengt nødvendig» og når det foreligger «tungtveiende sikkerhetsmessige grunner» som tilsier bruk av inngripende metoder for de nevnte formålene overfor tjenestens kilder/potensielle kilder.

6.3 Merknader til forslagets § 4-2 sjette ledd – Innhenting av rådata i bulk som inneholder informasjon om personer og virksomheter som befinner seg i Norge

Særskilt melding 2016 ble det stilt spørsmål ved Etterretningstjenestens nåværende hjemmelsgrunnlag for innhenting av metadata som kan inkludere kommunikasjon til og fra norske rettssubjekter i Norge. Dette var særlig knyttet til tjenestens metadatainnsamling fra satellittkommunikasjon, der det fanges opp kommunikasjonssignaler i transitt mellom en avsender og en mottaker gjennom såkalt midtpunktsinnhenting, jf. forslaget § 6-7. Utvalget konkluderte med at det knyttet seg rettslig usikkerhet til innhenting av metadata som kan inneholde opplysninger om norske borgere i Norge.

70 Se utvalgets årsmelding for 2017 punkt 8.2 side 41-43, jf. Innst. 389 S (2017–2018) – 2. Komiteens merknader.

71 Se EOS-kontrolloven § 5 femte ledd.

72 Dokument 7:1 (2013–2014), avgitt 16. desember 2013.

Utvalget konstaterer at våre merknader til E-tjenestens praksis med innhenting av metadata i bulk som kan inkludere kommunikasjon til og fra norske rettssubjekter i Norge, er omgjort til et unntak fra innhentingsforbudet for E-tjenesten i forslaget § 4-2 sjette ledd.

Utvalget merker seg at det foreslåtte unntaket fra innhentingsforbudet om innhenting av *rådata*[73] *i bulk,* ikke synes å være begrenset til metadata eller innsamling av kommunikasjonssignaler i transitt mellom en avsender og en mottaker. Utvalget merker seg videre at departementet skriver at innsamling av rådata i bulk kan «*skje ved bruk av enhver innhentingsmetode*», herunder innhenting av informasjon fra åpne kilder. Hvorvidt bulkinnsamling «*ved bruk av enhver innhentingsmetode*» vil være forholdsmessig i det enkelte tilfellet, vil kunne avhenge av innhentingsmetoden som benyttes.

Det er viktig å styrke utvalgets etterfølgende kontroll også av E-tjenestens innhenting av rådata i bulk, blant annet ved at utvalget får egne verktøy for kontroll i tjenestens systemer.

6.4 Merknader til forslagets § 4-2 syvende ledd – Søk i rådata med utgangspunkt i en personselektor som kan knyttes til en person i Norge

Utvalget ble i 2014 gjort kjent med at E-tjenesten gjennomfører søk i lagrede *metadata*[74] knyttet til norske rettssubjekter i Norge, for å finne selektorer[75] som er relevante for å løse tjenestens oppdrag. Utvalget uttalte i Særskilt melding 2016 at søkene stod i et problematisk forhold til e-loven § 4.[76]

Utvalget konstaterer at våre kritiske merknader til E-tjenestens praksis med å søke i lagrede metadata knyttet til norske rettssubjekter i Norge, er omgjort til et unntak fra innhentingsforbudet for E-tjenesten i forslaget til § 4-2 syvende ledd.

Forslaget til territoriell begrensing innebærer at E-tjenesten må stanse all innsamling «rettet mot» personer i Norge. Men regelverket legger opp til at E-tjenesten kan fortsette å søke etter personselektorer som tilhører personer som oppholder seg i Norge, så lenge tjenesten ikke har «overvåkingshensikt» mot personene i Norge. Disse rådataene er innsamlet fordekt gjennom tjenestens tekniske innsamlingssystemer. Det er derfor noe vanskelig for utvalget å se at søkene ikke også er «rettet mot» personen mens vedkommende er i Norge. Selv om det anføres at søk i slike rådata ikke er «rettet mot» personen i Norge, vil i hvert fall personens kommunikasjon rent faktisk være gjenstand for E-tjenestens aktive etterretningsvirksomhet.

Det vil som nevnt i punkt 5 være vanskelig for utvalget å kontrollere at søkene i realiteten ikke er «rettet mot» personen i Norge («overvåkingshensikt»).

6.5 Merknader til forslagets § 4-2 åttende ledd – Innsamling fra åpne kilder

Hjemmelen for innhenting av informasjon fra åpne kilder fremgår av forslag til § 6-2. Departementet foreslår et unntak i § 4-2 siste ledd, om innhenting av informasjon gjennom åpne kilder tilhørende personer *i Norge*. Det åpnes også for å samle inn informasjon fra åpne kilder *i bulk*, jf. forslaget til § 4-2 sjette ledd over. Departementet viser til at bulkinnsamling i prinsippet kan «*skje ved bruk av enhver innhentingsmetode*», «[e]ksempelvis kan også innhenting i åpne kilder innebære innhenting i bulk».[77]

73 «Rådata» er i foreslåtte § 1-4 nr. 13 definert som «ubearbeidet eller automatisk bearbeidet informasjon i enhver form hvis etterretningsverdi ikke er vurdert».

74 Med metadata forstås informasjon om data, eksempelvis tidspunkt, varighet, til/fra-identifikatorer, type trafikk og andre parametere som kan beskrive en teknisk hendelse som har funnet sted i et kommunikasjonsnettverk.

75 En selektor kan være et telefonnummer, en e-postadresse, Facebook-kontonavn etc.

76 Særskilt melding 2016, punkt 6.

77 Høringsnotatet punkt 9.5.6.3.

Departementet skriver:

> «Innhenting fra åpne kilder har tradisjonelt ikke vært ansett som en «fordekt» etterretningsdisiplin, og som metode har den etter norsk rett ikke krevd særskilt lovhjemmel etter legalitetsprinsippet. Dette fordi informasjonen som innsamles typisk vil være fritt delt på Internett eller på et annet offentlig tilgjengelig medium, og det ikke foreligger en berettiget forventning fra de som har delt informasjonen om at denne informasjonen er beskyttet. Innsamling fra åpne kilder kan imidlertid i et visst omfang eller intensitet kunne vurderes som et inngrep etter EMK artikkel 8 om rett til privatliv. I disse tilfellene må innsamlingen være hjemlet i lov og anses nødvendig i et demokratisk samfunn av hensyn til et legitimt formål.»

Forslaget innebærer at E-tjenesten vil kunne samle inn informasjon fra åpne kilder, fra for eksempel sosiale medieplattformer som angår personer som oppholder seg *i Norge*, for å finne informasjon om utenlandske forhold eller personer i utlandet. Som ledd i etterretningsvirksomheten vil det kunne samles inn informasjon som man ikke selv har delt åpent.

Dersom en person i Norge for eksempel har «kontakt med terroristnettverk i utlandet»[78], er det vanskelig å se at innsamlingen fra åpne kilder *ikke også* vil være «rettet mot» denne personen.

I 2018 reiste utvalget spørsmål om hjemmelen for E-tjenestens innsamling av informasjon fra nettopp åpne kilder, tilhørende personer som var godkjente innhentingsmål i utlandet, men som oppholder seg i Norge. Etter utvalgets oppfatning må innsamling av opplysninger om disse vurderes på samme måte som E-tjenestens søk i lagrede metadata knyttet til norske rettssubjekter i Norge for å finne selektorer for utenlandsetterretningsrelevante formål, jf. punkt 6.4.

EOS-utvalget er videre ikke enig i E-tjenestens forståelse av fordekt-begrepet. Så lenge informasjonen innhentes i skjul av E-tjenesten, må dette anses som «fordekt».

Utvalget konstaterer at våre kritiske merknader til E-tjenestens praksis med innhenting fra åpne kilder knyttet til norske rettssubjekter i Norge, er omgjort til et unntak fra innhentingsforbudet for E-tjenesten i forslaget til § 4-2 åttende ledd.

6.6 Konklusjon

Utvalget mener at forbudet ikke er tilstrekkelig klart til å danne grunnlag for kontroll.

7. Merknader til forslagets kapittel 5 – Grunnvilkår for informasjonsinnhenting

Grunnvilkårene for målsøking og målrettet innsamling følger av henholdsvis forslåtte §§ 5-1 og 5-2, hvis vurderingstemaer er utpreget etterretningsfaglige. Både målsøking og målrettet innsamling innebærer innsamling av informasjon om personer gjennom bruk av samme etterretningsmetoder. Den flytende overgangen mellom målsøking og målrettet innhenting, herunder at «begge formene for innhenting gjennomføres som søk i metadata eller innholdsdata, eller begge deler»,[79] gjør at det kan bli utfordrende å kontrollere om grunnvilkårene er oppfylt.

78 Høringsnotatet punkt 8.8.2.
79 Høringsnotatet punkt 9.3.1.

Kravet om forholdsmessighet, jf. forslaget § 5-4, vil «komme til anvendelse både for spørsmålet om informasjon kan innhentes i det hele tatt, på hvilken måte informasjon kan innhentes (metodebruk) og om innhentet informasjon kan utleveres til andre».[80] Det vil være en utpreget etterretningsfaglig vurdering å ta stilling til «om informasjon kan innhentes i det hele tatt» og «på hvilken måte informasjon kan innhentes (metodebruk)».[81]

Utvalget ser positivt på lovfesting av grunnvilkår for innhenting av og søk i rådata i bulk (foreslåtte § 5-3), for målsøking og målrettet innsamling, samt forholdsmessighetskravet for innhentingen. Tjenesten må kunne dokumentere overfor utvalget at grunnvilkår er oppfylt, samt at metodebruk er innrettet på minst mulig inngripende måte overfor individene som er utsatt for tjenestens metodebruk. Dette vil utvalget kunne kontrollere.

8. Merknader til forslagets § 6-9 – Forberedende tiltak

I forslagets § 6-9 om forberedende tiltak, foreslås følgende lovbestemmelse:

> «§ 6-9 *Forberedende tiltak*
> Etterretningstjenesten kan treffe forberedende tiltak som er nødvendige for å gjennomføre metoder etter kapittelet her, herunder forsere eller omgå faktiske og tekniske hindre, installere, gjennomsøke eller tilegne seg tekniske innretninger og programvare, og ta kontroll over, modifisere eller utplassere elektronisk eller annet teknisk utstyr.»

I høringsnotatet fremgår følgende om såkalte forberedende tiltak:[82]

> «Det foreslås en generell fellesbestemmelse i loven, jf. forslaget til § 6-9, om at Etterretningstjenesten kan treffe forberedende tiltak som er nødvendige for å gjennomføre innhentingen, herunder å forsere eller omgå faktiske og tekniske hindre, installere, gjennomsøke eller tilegne seg tekniske innretninger og programvare, og ta kontroll over, modifisere eller utplassere elektronisk eller annet teknisk utstyr. Dette er ikke en selvstendig hjemmel for metodebruk, men kun ment å synliggjøre i lov at gjennomføringen av metodebruk krever en rekke forutgående faktiske handlinger. Forslaget kodifiserer og presiserer gjeldende praksis, og slike faktiske tiltak vil gjennomgående være en åpenbar forutsetning for at Etterretningstjenesten i det hele tatt skal kunne skaffe seg fysisk eller logisk tilgang og dermed mulighet til å kunne benytte innhentingsmetodene som reguleres. Bestemmelsen må for øvrig sees i sammenheng med lovutkastet § 11-5, som omhandler faktiske tiltak for å ivareta sikkerheten for eget personell, egne kilder og operasjoner.»

Slike forberedende tiltak vil, etter utvalgets oppfatning, være å regne som utøvelse av etterretningstjeneste fordi det gjøres som *ledd i* E-tjenestens aktive innhentingsvirksomhet/overvåkingsvirksomhet. Utvalget merker seg at høringsnotatet ikke inneholder noen vurderinger av hvorvidt, og eventuelt i hvilken utstrekning, slike «forberedende tiltak» kan gjennomføres overfor fysiske og juridiske personer og deres eiendeler *i Norge*. Dermed er heller ikke grensen opp mot den foreslåtte territorielle begrensingen for E-tjenestens overvåkingsvirksomhet drøftet.

Det er videre uklart om eventuelle «forberedende tiltak» *i Norge,* for å forberede innhenting mot en person *i utlandet*, kan innebefatte for eksempel hemmelige ransakinger, innbrudd/datainnbrudd, forstyrring av signaler/kommunikasjon, manipulering av personer, tredjepersoner eller deres elektroniske hjelpemidler og annet teknisk utstyr.

80 Høringsnotatet punkt 9.1.
81 Høringsnotatet punkt 9.1.
82 Høringsnotatet punkt 10.5.3.

Dersom det er tiltenkt at slike og andre «forberedende tiltak» kan gjennomføres *i Norge* og innebærer at E-tjenesten gis hjemmel til å gjennomføre tiltak som PST måtte hatt rettens godkjenning for å gjennomføre, bør tiltakene vurderes opp i mot legalitetsprinsippet, ovennevnte territorielle begrensing for E-tjenestens overvåkingsvirksomhet, samt også PSTs mandat og rettsgrunnlag.[83]

Utvalget mener at disse forholdene bør avklares nærmere før en eventuell hjemmel for «forberedende tiltak» gis.

9. Sammenstilling og viderebehandling av innhentet informasjon som stammer fra den «norske forbindelsen» av kommunikasjonen

E-tjenestens lovlige innsamling mot etterretningsmål i utlandet kan også omfatte målets kommunikasjon med personer som oppholder seg i Norge («den norske forbindelsen»). Utvalget vurderte i 2018 Etterretningstjenestens rettslige grunnlag for å behandle opplysninger som *kun* stammet fra den «norske forbindelsen» av kommunikasjonen, det vil si utelukkende fra personen som befant seg *i Norge*. Utvalget var av den oppfatning at tjenesten kan rapportere om nødvendig og utenlandsetterretningsrelevant informasjon som fremkommer gjennom «den norske forbindelsen» ved *lovlig* innsamling mot mål i utlandet. Spørsmålet var om tjenesten gikk for langt i sin sammenstilling og viderebehandling av kommunikasjon med den norske forbindelsen, selv om den var innhentet på lovlig vis. Utvalget mente at det i arbeidet med ny lov om Etterretningstjenesten må avklares nærmere hvilke skranker som eventuelt gjelder for E-tjenestens sammenstilling og viderebehandling av informasjon som stammer fra «den norske forbindelsen», jf. forbudet i § 4, herunder hva som i den forbindelse eventuelt skal anses som «overskuddsinformasjon» for E-tjenesten.

Utvalget etterlyser departementets vurderinger av dette.

10. Merknader til høringsnotatets omtale av forhåndsautorisasjon

Departementet skriver at det «har vurdert hvorvidt det bør etableres en generell mekanisme for forhåndsautorisering av metodebruk av en uavhengig instans (domstol eller uavhengig administrativt organ) utenfor Etterretningstjenesten, men har kommet til at dette verken er mulig, nødvendig eller ønskelig».[84]

Utvalget har tidligere vist til at lovgivningen for E-tjenesten ikke stiller krav om tillatelse fra retten til for eksempel å overvåke en norsk persons kommunikasjonsmidler i utlandet. Dette i motsetning til PST, som må ha rettens tillatelse til kommunikasjonskontroll av den samme personens telefonnummer i Norge. Utvalget viser særlig til kontraterrorfeltet, der det allerede er tett og utstrakt samarbeid og informasjonsdeling mellom PST og E-tjenesten om personer med tilknytning til Norge.

Utvalget mener forhåndskontroll av innhenting i utlandet rettet mot personer med tilknytning til Norge kan utredes.

83 Årsmelding for 2009 kapittel VI punkt 2 side 37. Utvalget viser til årsmeldingene for 2007 til 2009, der vi kritiserte sider ved en samarbeidsoperasjon i Norge mellom PST og E-tjenesten. Utvalget bemerket blant annet at det var flere forhold som talte for at enkelte av de tiltakene E-tjenesten iverksatte i Norge, stod i et tvilsomt forhold til legalitetsprinsippet.

84 Høringsnotatet punkt 10.6.2.

11. Merknader til forslagets kapittel 7 og 8 – Tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon

11.1 Innledning

EOS-utvalget har ikke noe synspunkt på om E-tjenesten bør gis tilgang til grenseoverskridende elektronisk informasjon som beskrevet i lovforslagets kapittel 7 og 8, og heller ikke på vilkårene for bruken av metoden. Utvalgets merknader knytter seg til kontrollen med innhentingen og til den kontrolloppgaven som foreslås lagt til EOS-utvalget.

11.2 E-tjenestens internkontroll

Departementet viser i høringsnotatet[85] til at det gjelder strenge regler for internkontroll i tjenesten og at egen innmelding av avvik allerede er gjeldende praksis hos Etterretningstjenesten.

Utvalget slutter seg til departementets oppfatning om at tjenesten bør pålegges å melde fra til EOS-utvalget om avvik i egne systemer for tilrettelagt innhenting.

Departementet har ikke spesifisert nærmere hvordan E-tjenestens egen kontroll med tilrettelagt innhenting bør legges opp og hvilke sider av innhentingen som bør underlegges internkontroll. Utvalget antar at en rekke aktiviteter innenfor tilrettelagt innhenting kan underlegges forskjellige internkontrollprosedyrer. For eksempel vises det til at én kjennelse fra domstolen kan innebære tillatelse til et ukjent antall søk i datalagrene, uten at disse søkene er individuelt vurdert av domstolen.[86] Utvalget mener det vil være naturlig at de ulike søkene må gjennom en form for internkontrollprosedyre og at tjenesten etablerer særskilte rutiner for selv å avdekke avvik.

Utvalget understreker viktigheten av at kontrollsystemet settes opp med flere kontrollelementer. Internkontrollsystemet bør fange opp svikt eller mangler på et så tidlig tidspunkt og på et så lavt nivå som mulig. Tjenesten må etablere gode mekanismer for å kontrollere om den overholder vilkårene for bruk av tilrettelagt innhenting.

Utvalget savner en nærmere utredning og eventuell lovfesting av tjenestens internkontroll.

11.3 Merknader til forslagets § 7-11 – EOS-utvalgets kontroll av tilrettelagt innhenting

Forslaget legger opp til at EOS-utvalget skal føre «styrket» kontroll med E-tjenestens innhenting på området. Utvalget skal ha uhindret adgang til all informasjon og utstyr som benyttes for innhentingen. Kontrollen skal ifølge departementet være «løpende» og bør foretas «relativt hyppig» og på utvalgets «eget initiativ».

Utvalget forstår forslaget dithen at «styrket» kontroll innebærer en mer intensiv kontroll enn den kontrollen som utvalget regelmessig fører med E-tjenestens øvrige etterretningsvirksomhet. For øvrig vil det være opp til utvalget å vurdere kontrollintensiteten.

EOS-utvalgets kontroll med EOS-tjenestene, inkludert E-tjenesten, er ikke innrettet slik at den innebærer en full kontroll av alle sider av tjenestenes EOS-virksomhet. En fullstendig kontroll ville være for omfattende for utvalget, og det er et spørsmål om en slik kontroll overhodet er mulig eller ønskelig. Utvalget velger hvilke av tjenestens aktiviteter som skal undersøkes nærmere, blant annet basert på kriterier i EOS-kontrolloven og utvalgets vurderinger av hvor risikoen for rettighetskrenkelser og regelbrudd med alvorlige konsekvenser er størst. Selv om utvalget har full innsynsrett i E-tjenesten, med unntak for særlig sensitiv informasjon, vil ikke alle tjenestens aktiviteter bli kontrollert.

85 Høringsnotatet punkt 11.12.8.

86 Departementet foreslår at begjæringene til domstolen ikke må individualiseres, men kan bestå av «sakskompleks», jf. høringsnotatet punkt 11.11.4.4.

Evalueringen av EOS-utvalget i 2016 viste at utvalgets kapasitet allerede da var presset. Utvalgsmodellen begrenser utvalgets kapasitet og dermed omfanget av kontrollvirksomheten.[87] En utvidelse av kontrolloppgaven til å omfatte en styrket kontroll med tilrettelagt innhenting vil føre til flere oppgaver for utvalget. Det vil redusere utvalgets kapasitet til å kontrollere de andre EOS-tjenestene og andre sider ved E-tjenestens virksomhet.

Etter utvalgets syn vil det være essensielt å bygge inn kontrollmekanismer i systemene for datainnhenting allerede under utviklingene av disse.

I tillegg er det en nødvendig forutsetning for kontrollen at det settes av tilstrekkelig datakraft og andre ressurser til kontrollfunksjonalitet i systemene som tjenesten utvikler. Tilrettelegging for kontrollen bidrar til å underlette kontrollen og sikrer at kontrollen kan foretas på en så hensiktsmessig måte som mulig.

11.4 Merknader til forslagets § 8-1 – Kjennelse om tillatelse til tilrettelagt innhenting

Av forslag til § 8-1 femte ledd fremgår at rettens kjennelse skal meddeles E-tjenesten, som skal gjøre den tilgjengelig for EOS-utvalget. EOS-utvalget foreslår at kjennelsen og begjæringen som ligger til grunn for kjennelsen skal *meddeles* til utvalget. For å være i stand til å føre en dekkende kontroll med om tjenestens søk er i samsvar med kjennelsens innhold, må utvalget kjenne de forutsetninger som kjennelsen bygger på. Praktisk tilrettelegging fra tjenestens side gjør utvalget i stand til å føre en tettere kontroll.

Utvalget foreslår følgende endring i § 8-1 femte ledd:

> «§ 8-1 *Kjennelse om tillatelse til tilrettelagt innhenting*
> …
> Kjennelsen skal meddeles Etterretningstjenesten. Tjenesten skal *meddele kjennelsen og den underliggende begjæringen til* EOS-utvalget».

11.5 Administrative og økonomiske konsekvenser for EOS-utvalget

Utvalget er enig med departementet i at lovforslaget vil medføre behov for å utvide den tekniske og juridiske kompetansen i EOS-utvalgets sekretariat. Utvalget mener videre det er viktig, slik departementet påpeker, at sekretariatet styrkes med dedikert kapasitet allerede på utviklingsstadiet. Utvalget vil bemerke at den styrkingen med teknologisk kompetanse i sekretariatet som nylig har skjedd og som bør skje i 2020, har vært begrunnet i dagens behov for styrking av utvalgets ordinære kontroll. Behov som følge av en eventuell vedtakelse av et system for tilrettelagt innhenting, vil komme i tillegg.

Departementet anslår at 4 årsverk vil være tilstrekkelig for å ivareta kontrollfunksjonen. Det er vanskelig å gi et konkret overslag over hvilke økonomiske og administrative konsekvenser innføring av metoden vil få for utvalget. Høringsnotatet gir ikke en konkret beskrivelse av omfanget av bruken av den nye innhentingskapasiteten. Omfanget av den virksomheten som skal kontrolleres er dermed ukjent.

Beskrivelsen av ressursbehovet i forhåndskontrollen gir en pekepinn. Departementet anslår at retten vil behandle 1–2 saker i uken. Anslaget er basert på at tjenestens begjæringer til retten kan omfatte et sakskompleks fremfor å individualiseres, samt at søk etter personselektorer reguleres på en måte som vil «bidra til at antall rettsavgjørelser kan holdes på et håndterlig nivå». Utvalget legger derfor til grunn at antallet søk mv. som kan kontrolleres, kan bli omfangsrikt. I tillegg kommer at utvalgets kontroll også vil omfatte andre sider av systemet for tilrettelagt innhenting, for eksempel bruken av korttidslageret, aktivitetslogger og hvordan filtrene settes opp.

87 Evalueringsrapporten side 127 og 130.

Utvalget mener på denne bakgrunn at departementets anslag på 4 årsverk er for beskjedent. Utvalget anser at en kontroll av tilrettelagt innhenting kan ivaretas ved at utvalgets sekretariat så raskt som mulig tilføres minst 6 årsverk dersom tilrettelagt innhenting vedtas. Deretter må behovet for ressurser i sekretariatet vurderes løpende. Utvalget kan ikke se bort fra at det er nødvendig med en betydelig styrking også utover de nevnte 6 årsverkene, for å styrke kompetansen og kapasiteten til denne kontrollen. Utvalget ser for seg at hovedtyngden ligger i personer med teknologisk kompetanse. Men det vil også være behov for å styrke sekretariatets juridiske kompetanse og noe på administrativ side. De ekstra ressursene må på plass så tidlig som mulig etter en eventuell vedtakelse av ny e-lov med hjemmel til tilrettelagt innhenting.

Også den teknologiske kompetansen til medlemmene i utvalget bør styrkes. Selv om deler av den rutinemessige kontrollen kan foretas av sekretariatet, er det utvalget som avgjør om det skal rettes kritikk mot tjenesten. Det er avgjørende for at utvalget kan føre en effektiv og reell kontroll at medlemmene kan vurdere den tekniske dokumentasjonen som danner grunnlag for tjenestens bruk av tilrettelagt innhenting. Den samlede teknologiske kompetansen i utvalget kan styrkes ved at slik kompetanse vektlegges ved valg av nye medlemmer eller ved at medlemmene tilbys kompetansehevende tiltak. Det vises til spørsmål om utredning av kontrollmodellen som er omtalt ovenfor i punkt 2.

Ved vurderingen av økonomiske og administrative kostnader for E-tjenesten vises det til at forslaget medfører behov for administrative rutiner knyttet til EOS-utvalgets styrkede kontroll av tilrettelagt innhenting. Utvalget legger til grunn at utviklingskostnader knyttet til å bygge inn kontrollmekanismer i systemer for datainnhenting også vil ligge hos tjenesten.

For i størst mulig grad å ivareta utvalgets uavhengighet av tjenesten, foreslår utvalget at det legges til rette for at den løpende (styrkede) kontrollen i størst mulig grad kan utføres fra utvalgets egne lokaler. Det vil det etter utvalgets vurdering være mulig å få til i utvalgets nye lokale fra 2019, sett ut fra tilgjengelig grad av plass, sikkerhet og tekniske forhold. Også kostnaden ved å tilrettelegge for systemtilgang fra utvalgets lokale, må ligge hos tjenesten.

Del III – Merknader til forslag til endringer i EOS-kontrolloven

- Det er i høringsnotatet foreslått to endringer i EOS-kontrolloven. Vi mener de foreslåtte endringene utløser behov for avklaringer av konsekvensene for utvalgets virksomhet.

12. Merknader til EOS-kontrolloven § 5 – Jurisdiksjon som kriterium for EOS-utvalgets kontrolloppgaver

12.1 Jurisdiksjonsvilkårets betydning for utvalgets kontrolloppgaver

EOS-utvalgets kontrolloppgaver omfatter i dag ikke «virksomhet som angår personer som ikke er bosatt i riket…», jf. EOS-kontrolloven § 5 femte ledd. Utvalget kan «likevel» utøve slik kontroll «når særlige grunner tilsier det».

Som ledd i departementets vurdering av EMKs krav til effektive rettsmidler[88] reises spørsmålet om klageadgangen til EOS-utvalget etter norsk rett er tilstrekkelig vid[89]. Etter en drøftelse av denne

88 Høringsnotatet punkt 4.3.

89 Høringsnotatet punkt 4.3.4.

klageadgangen[90], foreslås den någjeldende territorielle begrensningen for utvalgets kontrolloppgaver erstattet med en jurisdiksjonsbegrensning.

Departementet foreslår EOS-kontrolloven § 5 femte ledd endret til følgende ordlyd:

> «Kontrolloppgaven omfatter enhver person, uavhengig av bosted eller statsborgerskap, som er underlagt norsk jurisdiksjon».

Jurisdiksjonsbegrepet er tradisjonelt knyttet til et lands fysiske kontroll over et område.[91] For utvalgets kontrolloppgaver vil den tradisjonelle forståelsen i stort være sammenfallende med dagens vilkår i EOS-kontrolloven om at personen må være «bosatt i riket».

For utvalget blir det mer uklart hvilke konsekvenser for kontrollen departementet ser for seg når det drøftes om E-tjenestens overvåking av personer i utlandet kan anses å innebære utøvelse av myndighet og kontroll over personer – slik at *ekstraterritoriell jurisdiksjon* må anses etablert og dermed utløse plikter etter EMK.[92] Departementet konkluderer slik:[93]

«Frem til det foreligger andre holdepunkter må det kunne konstateres at det foreligger rettslig usikkerhet knyttet til rekkevidden av EMKs anvendelsesområde for hva gjelder informasjonsinnhenting rettet mot personer i utlandet utført av en utenlandsetterretningstjeneste».

For EOS-utvalgets del foreslås nettopp jurisdiksjon som et vilkår for utvalgets kontrolloppgaver – samtidig som det det etter departementets egen vurdering knytter seg rettslig usikkerhet ved EMKs rekkevidde for utenlandsetterretningstjenestens overvåking av personer i utlandet. For Etterretningstjenestens del løses det ved at lovforslaget er «generisk og legger ikke opp til å differensiere normeringen ut fra hvor eller overfor hvem en gitt aktivitet finner sted».[94]

Inntil jurisdiksjonsspørsmålet avgjøres av domstolen (nasjonalt eller EMD) vil det med forslaget bli opp til utvalget å ta stilling til om E-tjenestens overvåking av personer i utlandet utløser plikter etter EMK, og i tilfelle kontrollere deretter.[95]

På denne bakgrunn ber utvalget departementet om å avklare følgene av endringsforslaget i EOS-kontrolloven § 5:

- Det bes avklart om departementet foreslår at EOS-utvalget på eget tiltak skal kontrollere E-tjenestens overvåking av personer (både med og uten tilknytning til Norge) i utlandet.
- Det bes avklart om departementet foreslår at EOS-utvalget skal behandle klager fra personer (både med og uten tilknyting til Norge) i utlandet som hevder at E-tjenesten har krenket deres rettigheter.

Dersom EOS-utvalget er tiltenkt kontroll av E-tjenestens overvåking av alle personer i utlandet vil det innebære en betydelig utvidelse av kontrolloppgaven. Dette vil igjen legge press på kontrollmodellen, jf. punkt 2 ovenfor.

90 Høringsnotatet punkt 4.3.4.1.

91 Departementet skriver i høringsnotatet punkt 4.1.3 at «[det] følger av EMDs rettspraksis at en stats jurisdiksjon etter EMK art. 1 hovedsakelig er territoriell, og at handlinger begått av en statspart utenfor statens territorium, eller som har virkninger utenfor statens territorium, bare unntaksvis kan utgjøre utøvelse av jurisdiksjon etter EMK art. 1».

92 Departementets drøftelse av jurisdiksjon fremgår i hovedsak i punkt 4.1.3 i høringsnotatet.

93 Høringsnotatet punkt 4.1.3.

94 Departementet presiserer at loven vil gjelde all informasjonsinnhenting som følge av praktiske hensyn – og ikke som følge av en rettslig forpliktelse.

95 I Særskilt melding 2016 punkt 3 siteres E-tjenestens påpekning av behovet for en utgreiing av «menneskerettighetenes ekstraterritoriale anvendelse for innhentingsmetoder som ikke innebærer at E-tjenesten har territoriell kontroll eller faktisk eller effektiv kontroll over en person». Utvalget uttalte det bør skje som en del av en lovutredningsprosess.

Utvalget legger i dag til grunn at E-tjenestens overvåking i utlandet av personer med tilknytning til Norge utgjør en «særlig grunn», som dermed underlegges vår kontroll. Dersom departementet mener E-tjenestens informasjonsinnhenting i utlandet etter forslaget *ikke* omfattes – vil tjenestens overvåking i utlandet av personer med tilknytning til Norge falle utenfor utvalgets mandat. Det fremgår ikke av høringsnotatet om dette i tilfellet er en tilsiktet konsekvens fra departementets side. Utvalget mener gode grunner taler for at E-tjenestens overvåking i utlandet av personer med tilknytning til Norge ikke bør ekskluderes fra utvalgets kontrolloppgaver.

Utvalget mener Stortinget bør ha en så konkret og fullstendig som mulig oversikt over hvilke kontrolloppgaver som tillegges dets kontrollorgan, dette også i lys av punkt 2 ovenfor. På denne bakgrunn ber vi departementet avklare konsekvensen av dets forslag om jurisdiksjon som vilkår for utvalgets kontrollvirksomhet.

12.2 Jurisdiksjonsvilkårets betydning for utvalgets klagesaksbehandling

Utvalget vil gjøre oppmerksom på mulige følger jurisdiksjonsvilkåret kan få for utvalgets klagesaksbehandling. Disse følgene har sammenheng med og vil delvis kunne bortfalle avhengig av departementets avklaring som etterspurt ovenfor i punkt 12.1.

Utvalget tar i dag enhver klage fra personer som er bosatt i Norge til behandling, uten å kreve annet enn at klagen er rettet mot en EOS-tjeneste.[96] For personer med tilknytning til Norge som er bosatt i utlandet legger utvalget til grunn at klagen må begrunnes (jf. kravet om «særlige grunner» i EOS-kontrolloven § 5 femte ledd).

Det fremheves at utvalget tar klager til behandling *uten at det først gjøres undersøkelser i tjenesten*. EOS-utvalgets beslutning om å ta eller ikke ta en klage til behandling vil aldri bero på en forutgående undersøkelse av hva som måtte finnes eller ikke finnes om klageren i tjenesten(e). Dette fordi *ethvert* resultat av utvalgets undersøkelser i tjenestene anses som sikkerhetsgradert informasjon:[97]

(i) Det er sikkerhetsgradert informasjon at en person er ukjent for tjenesten.

I disse tilfellene opplyser utvalget til klageren at klagen er undersøkt og at utvalget ikke har funnet at tjenesten har gjort noe ulovlig eller kritikkverdig. Det opplyses altså *ikke* til klageren at han eller hun er ukjent for tjenesten.

(ii) Det er sikkerhetsgradert informasjon at en person er blitt lovlig overvåket av tjenesten.

I disse tilfellene opplyser utvalget til klageren at klagen er undersøkt og at utvalget ikke har funnet at tjenesten har gjort noe ulovlig eller kritikkverdig. Det opplyses altså *ikke* til klageren at han eller hun er blitt *lovlig* overvåket.

Det er kun dersom utvalgets undersøkelser viser at klager er blitt utsatt for krenkelser at utvalget kan bekrefte overfor klageren at klageren er kjent for tjenesten – ved at EOS-kontrolloven bestemmer at utvalget kan meddele at det er uttalt «kritikk».[98]

Departementets forslag om at utvalget kan ta klager til behandling *dersom* personen faller inn under «norsk jurisdiksjon» synes å bryte med den forutsetning om sikkerhetsgradering som EOS-kontrolloven hviler på, jf. punkt (i) og (ii) ovenfor.

96 Utvalget praktiserer en lav terskel for å ta klager til behandling. Det kan ikke forventes at klagere skal treffe spikeren på hodet når det ikke er innsyn i EOS-tjenestens eventuelle overvåkingstiltak mot dem. Dersom en klager er bosatt i Norge (eller viser til «særlige grunner») og anfører at en EOS-tjeneste har begått urett mot ham eller henne – vil klagen tas til behandling av utvalget.

97 EOS-kontrolloven § 15 første ledd andre punktum lyder slik: «Opplysning om at noen har vært gjenstand for overvåkingsvirksomhet eller ikke, anses som gradert hvis annet ikke bli bestemt».

98 Utvalget har tidligere opplyst at dette kan være krevende, se Evalueringsutvalgets rapport punkt 38.6. I årsmeldingen for 2017 uttalte utvalget at det er en utfordring at det er rettslig forhindret fra å gi ytterligere opplysninger om grunnlaget for kritikken i klagesaker, se punkt 3.

Hvorvidt en person i utlandet må anses å være eller ikke være under norsk jurisdiksjon som følge av E-tjenestens overvåking eller fravær av sådan – vil nødvendiggjøre at utvalget *før klagen tas til behandling* foretar undersøkelser i E-tjenesten og konkluderer på bakgrunn av dets funn der.

Utvalget ber departementet om å avklare hvorvidt en konklusjon fra utvalget om at en person i utlandet faller under norsk jurisdiksjon (hvorpå det meddeles til vedkommende at klagen dermed tas til behandling), vil kunne anses som en bekreftelse av en skjermingsverdig opplysning. En slik konklusjon kan vanskelig forstås som annet enn en bekreftelse av norsk etterretningstjenestes tilstedeværelse eller interesse for et område, land eller person. Dersom departementet mener at resultatet av utvalgets jurisdiksjonsvurdering i en klagesak kan blottlegge skjermingsverdig informasjon, mener utvalget at et jurisdiksjonsvilkår ikke bør inntas i EOS-kontrolloven som vilkår for utvalgets mandat, eller at klageadgangen må sikres på annen måte.

Dersom departementet mener at utvalget kan meddele utvalgets resultat av en jurisdiksjonsvurdering til en klager i utlandet uten å komme i konflikt med forbudet mot å dele sikkerhetsgradert informasjon, har utvalget ingen innsigelser mot at jurisdiksjon gjøres til vilkår for dets mottak av *klager* fra personer i utlandet.[99] Utvalget mener at en slik klageadgang rent lovteknisk kan etableres uten samtidig å utvide utvalgets øvrige kontrolloppgaver.

Utvalget ber departementet avklare konsekvensen av jurisdiksjonsvilkåret for utvalgets klagesaksbehandling.

13. Merknader til EOS-kontrolloven § 15 – Utvalgets mulighet til å uttale seg om det offentliges erstatningsansvar

I årsmeldingen for 2016 ba utvalget Stortinget om å vurdere om utvalget kan ytre seg om det offentliges erstatningsansvar. Utvalgets redegjørelse og anmodning var basert på kontroll av saker om sikkerhetsklarering (klareringssaker). Kontroll- og konstitusjonskomiteen uttalte i sin innstilling til Stortinget at utvalgets forslag burde utredes nærmere og ba regjeringen komme tilbake til Stortinget med sin vurdering.[100]

Departementet har under henvisning til blant annet nevnte årsmelding foreslått følgende endring i EOS-kontrolloven § 15 første ledd tredje punktum:

> «Ved klager mot tjenestene om overvåkingsmessig virksomhet skal det bare uttales om klagen har gitt grunn til kritikk eller ikke, samt om utvalget mener det er grunnlag for erstatningsansvar fra det offentlige overfor klageren».

For det første synes den foreslåtte ordlyden å utelate utvalgets behandling av klager på klareringssaker, i det det vises kun til «overvåkingsmessig» virksomhet. Selv om høringsnotatet synes å forutsette at også klareringsklager omfattes, bør dette inntas i lovens ordlyd.

For det andre omfattet ikke utvalgets anmodning til Stortinget i 2016 klager i overvåkingsaker, men var begrenset til klareringssaker. At anmodningen var begrenset til å gjelde klareringssaker var en bevisst avveining fra utvalgets side, basert på de utfordringer utvalget har erfart med å i det hele tatt å få gitt *begrunnelser* i overvåkingsklager som har endt med kritikk.

99 Klager fra personer bosatt i Norge vil kunne tas til behandling på samme måte som i dag, da det er utvilsomt at statens myndighetsområde omfatter eget territorium.

100 Innst. 418 S (2016–2017).

Utvalget har over lengre tid tatt opp spørsmål om utvalgets uttalelser til klagere i overvåkingssaker – og hvilke utfordringer det skaper at utvalget bare kan uttale «om det er uttalt kritikk eller ikke». I høringsnotatet er det ikke utredet hvordan en uttalelse om «grunnlag for erstatningsansvar» skal kunne forenes med utvalgets manglende mulighet til å oppgi grunnlaget for kritikken i overvåkingsklager. Ut fra den foreslåtte ordlyden vil en klager kunne få beskjed om at det er «uttalt kritikk» og at det er «grunnlag for erstatningsansvar» uten å få vite *noe* mer.

Utvalget ser i utgangspunktet positivt på at det skal få mulighet til å uttale seg om erstatningsansvar i overvåkingsklager, men understreker at en slik ordning må utredes grundig, og antakelig også regelfestes i mer detalj. Det kan nevnes at overvåkingsklager forutsetningsvis[101] angår utvalgets kontroll av PST i større utstrekning enn kontrollen med E-tjenesten.

Utvalget mener at utvalgets adgang til å uttale seg om det offentliges erstatningsansvar i overvåkningssaker må utredes nærmere.

Med vennlig hilsen

Eldbjørg Løwer
utvalgsleder

101 Det er PST som har hjemler til å overvåke personer i Norge.

VEDLEGG 4 – Høring om forslag til forskrifter til ny sikkerhetslov

Forsvarsdepartementet
Postboks 8126 Dep
0032 OSLO

6. september 2018

Høringssvar fra EOS-utvalget – forskrifter til ny sikkerhetslov

1. Innledning

EOS-utvalget viser til Forsvarsdepartementets (FD) høringsbrev 2. juli 2018 vedrørende forslag til forskrifter til ny sikkerhetslov.

Til utkast til forskrift om virksomhetens arbeid med forebyggende sikkerhet § 58
Utkast til virksomhetsforskriften § 58 andre ledd lyder:

> »En person som ikke er gitt sikkerhetsklarering, jf. sikkerhetsloven § 8-4, kan ikke autoriseres for BEGRENSET, uten tillatelse fra klareringsmyndigheten.»

Utvalget tok i 2005 opp med NSM spørsmål om klagemulighet når en person får avslag på søknad om dispensasjon for autorisasjon for BEGRENSET, etter en negativ avgjørelse om sikkerhetsklarering. Saken ble omtalt i utvalgets årsmelding for 2005.[102] På denne bakgrunn sendte NSM et forslag til Forsvarsdepartementet om regelverksendring slik at det gis klagemulighet. NSMs forslag ble vurdert i departementets rapport *Evaluering av sikkerhetsloven* punkt 6.2.9.2 (levert av arbeidsgruppen i november 2012). Fra forslaget hitsettes:

> »I tråd med EOS-utvalgets merknader har NSM utarbeidet endringsforslag til aktuelle bestemmelser i forskrift om personellsikkerhet, herunder er det foreslått å gi mer utførlige regler om dispensasjon for autorisasjon for BEGRENSET og at bestemmelsene om begrunnelse, underretning, innsyn og klage får tilsvarende anvendelse for avgjørelser om dispensasjon. Arbeidsgruppen anser det helt sentralt at det foreliggende forslaget blir tatt med i en eventuell revisjon av sikkerhetsloven.»

Det fremgår ikke av merknaden til virksomhetsforskriften § 58 i høringsnotatet hvordan spørsmålet om klageadgang mv. er vurdert ved utformingen av bestemmelsen. Utvalget ber om at departementet vurderer om bestemmelsene om begrunnelse, underretning, innsyn og klage som gjelder for klareringssaker bør får tilsvarende anvendelse for avgjørelser om nektet tillatelse til autorisasjon for BEGRENSET. Det vises til at en negativ avgjørelse kan få betydning for personens arbeidsforhold og videre yrkeskarriere.

Med vennlig hilsen

Eldbjørg Løwer
Utvalgsleder

102 Dokument nr. 20 (2005–2006) side 13. Oppfølgingen av saken er også omtalt i årsmeldingene for 2011 og 2012 (henholdsvis Dokument 7:1 (2011–2012) kapittel V punkt 3 og Dokument 7:1 (2012–2013) kapittel V punkt 3).

VEDLEGG 5 – Høring om sikkerhetslovens anvendelse for Stortingets eksterne organer

Stortinget
Postboks 1700 Sentrum
0026 OSLO

31. januar 2019

Ny lov om nasjonal sikkerhet – Sikkerhetsloven – Innspill fra EOS-utvalget

1. Bakgrunn

Det vises til tidligere korrespondanse, sist Stortingets brev 20. november 2018, der det anmodes om synspunkter fra blant andre EOS-utvalget på behov for endringer i lover og instrukser som følge av ny sikkerhetslov. Utvalget takker for at det er gitt utsatt frist for å besvare henvendelsen.

2. Utvalgets innspill

2.1 Sikkerhetslovens anvendelse for EOS-utvalget og behov for unntak og tilpasninger

EOS-utvalget stiller seg positivt til at sikkerhetsloven gis anvendelse for vår virksomhet. Vårt arbeid innebærer regelmessig kontroll av etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-tjeneste).[103] Selv om sikkerhetsloven ikke har hatt anvendelse for utvalget, er utvalget bundet av regler om behandling av dokumenter mv. som må beskyttes av sikkerhetsmessige grunner, jf. EOS-kontrolloven § 11 andre ledd. Utvalget har innrettet sin virksomhet *som om* sikkerhetsloven har anvendelse, så langt dette passer. At loven også formelt gis anvendelse for utvalgets virksomhet kan bidra til økt tillit til utvalget fra EOS-tjenestene og samfunnet for øvrig.

Stortingets vurderinger av de konstitusjonelle forhold i Innst. 122 S (2018–2019) punkt 3.2 er i det vesentlige overførbare til EOS-utvalgets virksomhet, og utvalget viser til disse. Vi mener det er grunn til å unnta fra anvendelse bestemmelser i sikkerhetsloven som legger kompetanse og myndighet til andre organer enn Stortinget, samt gjøre tilpasninger til bestemmelser som følge av at EOS-utvalget ikke er underlagt noe departement.

Enkelte særlige hensyn gjør seg gjeldende for EOS-utvalgets virksomhet.

For det første viser utvalget til at vi besitter skjermingsverdig informasjon om og fra EOS-tjenestene og andre som utøver EOS-tjeneste. Å gi adgang til informasjonen vil være i strid med utvalgets og sekretariatets taushetsplikt etter gjeldende lov.[104] En plikt til å gi sikkerhetsmyndigheten uhindret tilgang til utvalgets informasjon, kan redusere EOS-tjenestenes tillit til at opplysninger som utleveres til utvalget ikke blir kjent for andre.

For det andre er det prinsipielt sett uheldig om en virksomhet som utvalget er satt til å kontrollere, Nasjonal sikkerhetsmyndighet (NSM), gis myndighet over sider ved utvalgets virksomhet.

Utvalget foreslår at sikkerhetslovens anvendelse reguleres i nytt fjerde og femte ledd i EOS-kontrolloven § 1:

103 Slik tjeneste utøves i dag i hovedsak av Politiets sikkerhetstjeneste, Etterretningstjenesten, Nasjonal sikkerhetsmyndighet og Forsvarets sikkerhetsavdeling.

104 Jf. EOS-kontrolloven § 11.

«**§ 1 Kontrollområdet**

Stortinget velger et utvalg til å kontrollere etterretnings-, overvåkings- og sikkerhetstjeneste (tjenestene) som utføres av den offentlige forvaltning eller under styring av eller på oppdrag fra denne (EOS-utvalget). Kontrollen utføres innenfor rammene av §§ 5, 6 og 7.

Kontrollen omfatter ikke overordnet påtalemyndighet.

Offentleglova og forvaltningsloven, med unntak av reglene om ugildhet, gjelder ikke for utvalgets virksomhet.

Lov 1. juni 2018 nr. 24 om nasjonal sikkerhet (sikkerhetsloven) gjelder for EOS-utvalget med de unntak og presiseringer som følger av bestemmelsen her, jf. sikkerhetsloven § 1-4 første ledd.

Følgende bestemmelser i sikkerhetsloven gjelder ikke for EOS-utvalget: § 1-3, § 2-1, § 2-2 og § 2-5, kapittel 3, § 5-5, § 7-1 andre til sjette ledd, § 7-5, § 8-3 første ledd andre punktum, § 8-9 tredje ledd, § 9-4 andre til femte ledd, kapittel 10 og § 11-1, § 11-2 og § 11-3.»

Stortinget kan gi instruks om virksomheten til utvalget innenfor rammen av denne lov og fastsetter bestemmelser om dets sammensetning, funksjonsperiode og sekretariat.

Innenfor rammen av denne lov utfører utvalget sitt verv selvstendig og uavhengig av Stortinget. Stortinget i plenum kan likevel pålegge utvalget å foreta nærmere definerte undersøkelser innenfor utvalgets kontrollmandat, og under iakttakelse av de regler og innenfor de rammer som for øvrig ligger til grunn for utvalgets virksomhet.»

2.2 Klareringsmyndighet og klageinstans over klareringsmyndighetens avgjørelser

EOS-utvalgets sekretariat skal være klarert og autorisert for høyeste sikkerhetsgrad nasjonalt og etter traktat Norge er tilsluttet og klareres i dag av NSM.[105] Stortinget etterspør utvalgets syn på en modell der Stortingets administrasjon er klareringsmyndighet og presidentskapet er klageinstans.

På generelt grunnlag mener utvalget at en reduksjon av antall klareringsmyndigheter kan gi et bedre grunnlag for likebehandling av saker og en mer effektiv saksbehandling.[106]

Prinsipielle grunner taler for at sekretariatets ansatte klareres av Stortingets administrasjon. Det vil eliminere risikoen for at den utøvende makt kan påvirke hvem utvalget skal ansette i sitt sekretariat. Utvalget mener presidentskapet i så fall bør være klageinstans.

Dersom Stortinget finner grunn til å endre dagens praksis, foreslås endringer inntatt i EOS-kontrolloven § 11 andre ledd.

105 Jf. EOS-kontrolloven § 11 andre ledd.

106 Dette har utvalget gitt uttrykk for ved flere anledninger, for eksempel i våre årsmeldinger til Stortinget og i brev til Forsvarsdepartementet 27. august 2015 der utvalget ga høringssvar om endringer i sikkerhetsloven.

2.3 Sikkerhetsklarering av virksomhetens øverste ledelse

EOS-utvalgets medlemmer skal være klarert og autorisert for høyeste sikkerhetsgrad nasjonalt og etter traktat Norge er tilsluttet.[107] Utvalget mener at hensynet til kontrollens legitimitet taler sterkt for fortsatt å stille krav om klarering for utvalgets medlemmer.

I vårt brev 13. januar 2009[108] til Stortinget tok vi opp spørsmål om hvem som skulle klarere utvalgets medlemmer. Dette med bakgrunn i at medlemmene på den tiden ble klarert av NSM, altså en av tjenestene utvalget er satt til å kontrollere. Ved en lovendring vedtok Stortinget at utvalgets medlemmer skal klareres av Stortingets presidentskap.[109]

Utvalget mener det bør være en klageadgang også der klarering nektes for et valgt medlem til EOS-utvalget. Dette taler for at Stortingets administrasjon også her er klareringsmyndighet med Stortingets presidentskap som klageinstans.

Dersom Stortinget finner grunn til å endre dagens løsning, foreslås endringer inntatt i EOS-kontrolloven § 11 andre ledd.

2.4 Ikrafttredelsestidspunkt og behov for eventuelle overgangsregler

Den 1. januar 2020 anses som et hensiktsmessig ikrafttredelsestidspunkt for endringer i EOS-kontrolloven.

2.5 Økonomiske og administrative konsekvenser

Utvalget mener at de administrative og økonomiske konsekvenser av sikkerhetslovens anvendelse for EOS-utvalget kan håndteres innenfor virksomhetens eksisterende rammer. Vi viser særlig til at Stortinget i 2018 bevilget midler til nye og sikrere lokaler for utvalget, som både ivaretar utvalgets behov i dag og fremtidige forpliktelser etter sikkerhetsloven.

***

Ta kontakt dersom det er ønskelig med ytterligere synspunkter eller avklaringer.

Utvalget imøteser Stortingets behandling av saken.

Med vennlig hilsen

Eldbjørg Løwer
Utvalgsleder

107 Jf. EOS-kontrolloven § 11 andre ledd.

108 Brevet er inntatt som vedlegg 4 til *Dokument nr. 18 (2008–2009)*, utvalgets årsmelding til Stortinget for 2008.

109 Jf. endring i dagjeldende EOS-kontrollov § 9, vedtatt 19. juni 2009 nr. 87.

VEDLEGG 6 – Pressemelding fra fem europeiske kontrollorganer

Felles uttalelse: Styrking av kontrollsamarbeid

Etterretnings- og sikkerhetstjenester i ulike land samarbeider stadig mer. Det fører til at mye mer data blir utvekslet mellom landenes tjenester. Dette har særlig vist seg de siste årene. Trusselen fra islamske terrorister har økt, og ekstremistgrupper har gjennomført flere angrep i Europa.

Den økende internasjonale utvekslingen av data mellom etterretnings- og sikkerhetstjenester skaper en rekke utfordringer for nasjonale kontrollorganer. Kontrollen med etterretningstjenestene er bare nasjonal – ikke internasjonal. Det nasjonale kontrollorganet kan ikke kontrollere utenfor sin landegrense, og kan derfor bare vurdere den siden av datautvekslingen som skjer i eget land.

Kontrollorganene kunne samarbeidet om å kontrollere internasjonal datautveksling, men dette begrenses av de nasjonale reglene for hemmelighold. Vi finner det også mer og mer utfordrende å holde tritt med utviklingen i etterretningstjenestene mot raskere og mer effektive måter å utveksle data på. Disse og andre utfordringer for nasjonale kontrollorganer gir en risiko for at det utvikler seg et kontrolltomrom når etterretnings- og sikkerhetstjenester samarbeider internasjonalt.

Kontrollorganene i Belgia, Danmark, Nederland, Norge og Sveits har samarbeidet for å møte disse utfordringene og takle risikoen for et kontrolltomrom. Vi bestemte oss for å undersøke bruk og deling av informasjon knyttet til fremmedkrigere i tjenestene vi kontrollerer. De siste tre årene har vi møttes regelmessig for å dele kunnskap om våre metoder og erfaring på dette og andre tema.

Ingen gradert informasjon har blitt delt mellom kontrollorganene.

I denne felles uttalelsen peker vi på måter å komme videre på. For å minimere risikoen for et kontrolltomrom, må samarbeidet mellom kontrollorganene bli tettere. Et verdifullt og nødvendig steg mot et nærmere samarbeid vil være å minimere hemmeligholdet mellom kontrollorganene, slik at noe informasjon kan deles. Når data allerede er utvekslet mellom tjenestene, er det ikke noen grunn for kontrollen til å henge etter. Kontrollorganer burde da kunne diskutere hvordan informasjon blir utvekslet. Et annet skritt er å utvikle nye juridiske og tekniske kontrollmetoder, for å kunne drive bedre og mer effektiv kontroll med internasjonal datautveksling.

Kontrollorganene i Belgia, Danmark, Nederland, Norge og Sveits vil fortsette samarbeidet for å møte utfordringene for kontroll med internasjonal datautveksling, og inviterer kontrollorganer fra andre land med i arbeidet vårt.

EOS-utvalget har over mange år fulgt med på PSTs og E-tjenestens deling av informasjon med internasjonale partnere. Vår undersøkelse av tjenestenes behandling og deling av informasjon knyttet til fremmedkrigere i dette prosjektet har ikke avdekket noe som har gitt grunnlag for kritikk. Tjenestenes systemer er ikke tilrettelagt slik at utvalget kan finne én samlet oversikt på ett sted over alle utleverte opplysninger om den enkelte fremmedkriger. Kontrollen er derfor ressurskrevende for utvalget.

Den vedlagte uttalelsen er skrevet i samarbeid mellom:

Belgia:	Comité permanent de contrôle des services de renseignements et de sécurité/ Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten – www.comiteri.be
Danmark:	Tilsynet med Efterretningstjenesterne – www.tet.dk
Nederland:	Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten – www.ctivd.nl
Norge:	EOS-utvalget – www.eos-utvalget.no
Sveits:	Unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND – www.ab-nd.admin.ch

Strengthening oversight of international data exchange between intelligence and security services

Written in cooperation between:

Belgian Standing Intelligence Agencies Review Committee
(Comité permanent de contrôle des services de renseignements et de sécurité / Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten)
www.comiteri.be

Danish Intelligence Oversight Board
(Tilsynet med Efterretningstjenesterne)
www.tet.dk

Review Committee on the Intelligence and Security Services – The Netherlands
(Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten)
www.ctivd.nl

EOS Committee – The Norwegian Parliamentary Intelligence Oversight Committee
(EOS-utvalget)
www.eos-utvalget.no

Independent Oversight Authority for Intelligence Activities (OA-IA)
(Unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND)
www.ab-nd.admin.ch

Belgian Standing Intelligence Agencies Review Committee

tet
Danish Intelligence Oversight Board

CTIVD Review Committee on the Intelligence and Security Services

EOS COMMITTEE NORWEGIAN PARLIAMENTARY OVERSIGHT COMMITTEE ON INTELLIGENCE AND SECURITY SERVICES

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

1. Content

Five European intelligence oversight bodies have begun a new form of cooperation.
In this statement, we will:

Describe our project, which entailed each of us conducting an investigation into our respective countries' services' use of information regarding foreign terrorist fighters and sharing our methods, best practices and experiences.

- Address the challenges we met when overseeing international data exchange, including the risk of an oversight gap when intelligence and security services cooperate internationally.
- Identify ways to move forward towards strengthening oversight cooperation, for example through minimizing secrecy between oversight bodies so that certain information can be shared, in order to improve our oversight of international data exchange.

2. Introduction

Recent terrorist attacks, such as in Paris, Brussels and London, were carried out by persons directed, encouraged or inspired by ISIS, Al-Qaeda or similar terrorist groups. To identify and investigate the threat of homegrown and returning foreign terrorist fighters is an important task for intelligence and security services across Europe.

The threat of jihadist terrorism has become more complex and widespread in recent years. Investigating this threat requires international cooperation between intelligence and security services, either bilaterally or multilaterally. Such cooperation exists within Europe and with other countries. As this cooperation has intensified, the exchange of personal data between services has increased. The exchange of data with foreign services is part of the intelligence and security services' day-to-day activities. Data may be exchanged in various ways, either orally or in writing.

The oversight bodies have naturally followed the development of international cooperation between intelligence and security services. As our respective oversight mandate is strictly national, we have been concerned with the risk of an "oversight gap" occurring. In an ideal situation, the national systems of oversight would be complementary to each other: where one oversight body reaches the boundaries of its national mandate, the other is competent to effectively oversee. However, national legislation regarding exchange of data and the oversight of such exchanges may not meet these requirements. Moreover, international cooperation between intelligence services could develop in such a way, that national oversight can no longer keep up. Then an "accountability deficit" or "oversight gap" could emerge.

In light of this, the five oversight bodies from Belgium, Denmark, the Netherlands, Norway and Switzerland decided to start a joint project to exchange experiences and methods. Each of the oversight bodies conducted a national investigation into the international exchange of data on foreign terrorist fighters by the intelligence and security services they oversee.[1]

We conducted the national investigations more or less at the same time, each from our national context and within the framework of our national mandate. We have met regularly to compare investigation methods, interpret legal frameworks, discuss legal and practical problems and to collate our findings and conclusions. Classified information was not exchanged.

[1] The report from CTIVD (The Netherlands) about the investigation in English – https://english.ctivd.nl/latest/news/2018/04/26/index
The annual reports from the Danish Intelligence Oversight Board in English – http://www.tet.dk/redegorelser/?lang=en

3. Current practices in oversight of data exchange

The participating oversight bodies oversee data exchange between intelligence and security services in several ways. We may

- assess cooperative relations or arrangements between intelligence and security services,
- assess the legitimacy and quality of specific data exchanges with foreign services,
- review the system of data exchange as a whole, including the safeguards,
- be involved in procedures concerning individual remedies and complaints.

Although the mandates of the oversight bodies are different, we all have a diverse range of instruments for overseeing international data exchange.

Assessment of the cooperative relationship

Oversight bodies may assess whether or not the cooperative relationship between their country's service and partner services in other countries meets certain criteria. Legislation governing the intelligence and security services may specifically state criteria for cooperation. Typically, criteria include the necessity for cooperation, the respect for human rights, the existence of legislation on data protection and/or reliability. The threshold for cooperating with services that do not meet the criteria should be high. The oversight bodies of Belgium, the Netherlands, Norway and Switzerland review the considerations made in that respect by their national services.

Cooperative relationships between the services can be based on agreements, for example letters of intent or memorandums of understanding. Such agreements are usually not legally enforceable but offer a practical framework on the exchange of data by services. Even the existence of some of these agreements is classified. Other agreements are made public by governments or the services. Nevertheless, they may draw the outline of the cooperative relationship by addressing issues like the purpose of the cooperation, how the cooperation is expected to function, limitations concerning disclosure to third parties or procedural aspects of the cooperation. The oversight bodies of all five countries may either review or report on whether these agreements comply with national laws and regulations.

Assessment of the legitimacy of specific data exchanges

Oversight bodies may assess whether individual data exchanges meet the legal requirements imposed by national laws and regulations.

The national legislations of our countries share certain characteristics, most notably the principles of necessity and proportionality. These shared principles originate from international legal frameworks such as the European Convention on Human Rights. The principle of necessity includes the requirement of a clear and legal purpose for the data exchange and the reasonable expectation that this purpose will be

met by exchanging the data. The principle of proportionality requires the service to balance the purpose of the exchange against the gravity of the infringement of fundamental rights. Most national legislation contains other requirements as well, such as the reasonableness, correctness, effectiveness and reliability of data exchange.

The internal policy of the services may provide additional rules for data exchange. Such policy may, for example, further specify which type of data exchange is allowed under which circumstances, which authorisation level is required and which use may be made of data received. When national law or bilateral and multilateral agreements are absent or silent on a specific matter, internal policy can provide additional safeguards.

Assessment of the quality of specific data exchanges

Quality may relate to the content of the data or the format of the data. When it comes to content, quality means the data is correct, sufficiently clear and precise in its wording, confirmed by underlying data, up to date and with an indication of probability or reliability. As for format, quality aspects relate to the inclusion of a classification level, the date of exchange, the designated receiving partner service(s) and caveats regarding further use of data. All five oversight bodies can review the quality of data exchange in this respect.

Quality may also have a different meaning. It may relate to efficiency or effectiveness, that is whether the data exchange is relevant, whether the exchange happened in a timely manner and whether it fulfilled its purpose. This type of quality review is less common for oversight bodies. The oversight bodies of Belgium and Switzerland are expressly authorised to review whether data exchange has been effective and efficient.

Review of the system of data exchange as a whole

Oversight bodies may adopt a broader approach when reviewing the legitimacy of data exchange. In reviewing certain multilateral cooperative frameworks, the oversight body in the Netherlands expressly looks at the system of data exchange as a whole and at the protection of individual rights within that system. Even though certain specific data exchanges may be legitimate, there can still be insufficient safeguards in the system to ensure the legitimacy of data exchange in the longer run. This type of review may help prevent unlawful data exchange between intelligence and security services.

One could take a similar approach when reviewing the quality of data exchange. When the purpose of exchanging data is to counter jihadism, the general quality of data exchange could be measured by investigating the amount of shared information that led to prosecution and conviction, or even to a direct prevention of a terrorist attack. However, measuring the usefulness of exchanged data in this way can be challenging. Such reviews are often initiated after a terrorist attack has occurred. Then the oversight body assesses if the relevant data had sufficiently and adequately been exchanged with national and international partners. The oversight body of Belgium has been involved in this type of review.

Involvement in individual remedies and complaints

In general, oversight bodies in all five countries can receive complaints from individuals regarding the activities of the national intelligence and security services. Usually oversight bodies may offer non-legally binding opinions or recommendations to the intelligence and security services and/or the ministers who are politically responsible. The services usually comply with such opinions or recommendations. A

new law was adopted in the Netherlands in 2017, granting the oversight body the power to take binding decisions on complaints. This may also include ordering the exercise of a power to be terminated or the destruction or removal of processed data.

The secrecy that is necessary for the intelligence and security services to conduct their activities usually limits the right of the individual to access personal data. Some countries explicitly afford individuals the right to request the national oversight body to review the personal data their services have processed about them. In Denmark, any person may ask the Danish oversight body to investigate whether the security service is unlawfully processing personal data about them. In case of the military intelligence service, this review is limited to residents of Denmark. In both cases, the Danish oversight body may order the deletion of personal data regarding the applicant.

In Belgium the oversight body has an obligation to investigate all complaints that are not manifestly unfounded. The complainant will receive the findings of the investigation in general terms. The complainant then has the possibility to use these findings before the court or an administrative authority. In some specific cases the oversight body must give an official advice to a criminal court following a complaint and regarding two other topics of complaint (use of special methods and data protection), the committee may take binding decisions.

In Norway, residents have the same right to complain to the oversight body if a citizen suspects that he/she is subject to unlawful surveillance. However, the Norwegian oversight body does not have the authority to order deletion of data. In Switzerland, the Federal Data Protection and Information Commissioner (FDPIC) handles individual requests on data processing.

4. Challenges for oversight of international data exchange

In the course of our project we have found that the increased cooperation between intelligence and security services and the exchange of data between these services, especially on the multilateral level, may pose legal and practical challenges to the oversight bodies.

Oversight does not cross national borders

National legislation often promotes the cooperation and exchange of information between intelligence and security services, both bilaterally and multilaterally. However, it usually does not provide a specific legal basis for oversight bodies to cooperate or exchange information on individuals. None of the five oversight bodies working together in the context of this common publication has an explicit legal basis to exchange data with another oversight body, certainly not when this information is classified.

Where intelligence and security services cross national borders, oversight bodies cannot. Oversight is limited to national mandates. This reflects one side of data exchange: either oversight will focus on the provision of data and its prior collection, or it will focus on the reception of data and its use. National oversight bodies will not independently be able to acquire a full picture of personal data exchange, let alone review the lawfulness of the entire process of exchange.

Such a limit to national oversight does not necessarily constitute an oversight gap. When oversight is exhaustive and effective on both sides of the border, no gap exists between the mandates of the oversight bodies. However, when it comes to cooperation between intelligence and security services - predominantly multilateral cooperation - the cooperation of oversight bodies is only as strong as its weakest link.

The challenge of cooperation in the face of secrecy

Oversight bodies are limited to national rules on secrecy and cannot share and discuss the substance of their investigations beyond what is designated as public information. In practice, this means that oversight bodies have very limited insight into whether 'the other side' of data exchange is effectively overseen or whether an oversight gap exists. Therefore, oversight activities are not only unable to cross borders; they are also largely unable to share with other oversight bodies what occurs within their borders.

As the joint project between the five oversight bodies progressed, we found ourselves on numerous occasions aware of the fact that we were not even in a position to discuss matters known to us all, e.g. the content of agreements between the services we oversee. In addition, we became aware that what is public information in one country might be deemed confidential in another. This has led to difficulties for this project, limiting the possibility to reach substantial discussion on the matter in question.

Assessment of necessity and proportionality

As mentioned above, oversight bodies continuously assess whether the exchange of data is necessary for a specific purpose and proportionate to the aim pursued. This requires that oversight bodies consider the level of protection of individual rights provided by the receiving service. As the volume of data exchanges and the number of foreign services with which the data is shared increase, this will be more and more challenging for oversight bodies. This test of necessity and proportionality can become more abstract and can lose value as the data exchanged is less specific or if it is exchanged within a larger group of intelligence and security services.

Different national legal regimes may include different legitimacy and quality standards for data collection, processing, retention and exchange. The level of protection of individual rights afforded by the service receiving the data is an important element in assessing the proportionality of a particular data exchange. This is not always easy to determine as intelligence and security services may not be open about all aspects of the legal framework in place and the standards they apply.

In the context of multilateral data exchange, common standards and definitions could help define under which circumstances data exchange is regarded as necessary and proportionate, and which minimum level of data protection needs to be in place to sufficiently safeguard individual rights. There is a common interest of all parties – intelligence and security services and oversight bodies – in having such common standards and a common interpretation of existing legal safeguards. This may also add to the legitimacy of the multilateral exchange in question.

Some countries differentiate between citizens and foreigners

Some national legal frameworks offer nationals or residents a higher level of protection and more privileged access to individual remedies than foreigners or non-residents. The distinction between these groups may result in limited or no access to individual remedies for foreigners or non-residents whose data has been exchanged by the respective intelligence or security service.

A similar distinction may determine the mandate of the oversight body. Some oversight bodies only have the mandate to review data exchange with regard to nationals or residents. The provision of data with regard to other persons may lie beyond their reach. If no other oversight body may effectively review this part of the data exchange, an oversight gap exists.

Means and methods of data exchange

Intelligence and security services exchange data in various ways. Some means and methods of data exchange pose further challenges for oversight bodies. An example of such a challenge is the informal exchange of data, and how to provide efficient oversight of data exchanged during conferences and meetings, by phone and so on. The increase in international data exchange may require oversight bodies to come up with more advanced methods of oversight, as it is no longer feasible to review each exchange of data. With regard to data protection, developments in multilateral data exchange may invoke responsibilities for each of the participating services as well as the oversight bodies. To safeguard individual rights adequately, it may be required that intelligence and security services discuss the standards they apply and work towards an equal minimum level of protection offered by all participating services.

5. Oversight of international data exchange – moving forward

Our project has shown us that the efforts of the intelligence and security services to find new ways to exchange data effectively, especially on a multilateral level, and the large increase in the volume of data exchanged, have in turn led to new challenges for the oversight bodies. This applies both to the limits of the oversight bodies' national mandates, their inability to adequately discuss international data exchange with other oversight bodies as well as to their own efforts to innovate their procedures and methods to ensure effective oversight.

National sovereignty and interests dictate the international cooperation between intelligence and security services. It is to be expected that, unlike other areas of international cooperation, oversight of the intelligence and security services will continue to be carried out by national oversight bodies. However, where intelligence and security services cross national borders, oversight bodies cannot. Consequently, oversight always reflects on one side of data exchange. Moreover, oversight bodies are largely unable to share with other oversight bodies their review of a particular data exchange. Because of these limits to national oversight, there is a risk of an oversight gap with regard to international data exchange by intelligence and security services. The question remains how to tackle such a risk.

By exchanging knowledge, experience and investigation methods, and by comparing their findings, conclusions and recommendations, oversight bodies may come closer together. Our experience is that this is precisely what this common project has accomplished. We have learned from each other's best practices, developed more understanding of each other's legal systems and we have built a level of trust. In order for oversight bodies to keep up with developments in international cooperation between intelligence and security services, we need to do just that: intensify our cooperation.

A valuable and necessary step towards closer cooperation is to minimize secrecy when sharing information between oversight bodies. At the minimum, oversight bodies could be able to discuss concrete bilateral and multilateral cooperative arrangements between the intelligence and security services they oversee. A logical additional step could be to share information with other oversight bodies that has already been shared by the intelligence and security services themselves. Once data has been exchanged, there is no need for oversight to lag behind. We do not suggest that all national secrecy limitations should be set aside, to the contrary. Cooperation between oversight bodies should take place within the limits and according to the standards set by national legislators.

Being able to discuss international cooperative arrangements and data exchange with other oversight bodies also comes with certain responsibilities. Adequately safeguarding individual rights while cooperating internationally, not only requires that intelligence and security services discuss the standards they apply and work towards an equal minimum level of protection offered by all participating services. It also requires oversight bodies to uphold such a minimum level of data protection and try to find common ground in interpreting existing legal safeguards.

Due to technological development and increased cooperation, the data exchange between intelligence and security services is intensifying, resulting in an increase of the number of individual data exchanges. The sheer volume of data exchanged may become a challenge in itself. To assess the legitimacy and quality of each individual exchange can become an overwhelming task for the oversight bodies. In addition to

conducting spot checks, it is becoming increasingly important to assess the system and framework for data exchange and the existence and functioning of safeguards for the protection of fundamental rights.

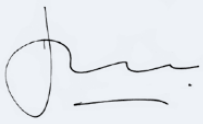
To do this effectively, oversight bodies will need to develop new methods. One way forward may be to increasingly use computerized automation and tools developed for conducting oversight of large volumes of data. In order to achieve this, oversight bodies need to expand their IT expertise and knowledge of the services' systems. Another way to facilitate a more effective oversight would be to take the needs of the oversight bodies into account when the services implement new systems and to strengthen mechanisms of internal and external control.

The oversight bodies of Belgium, Denmark, the Netherlands, Norway and Switzerland will continue to exchange methods and best practices, as well as discuss international challenges to oversight, and the best approaches to overcoming these challenges. We invite oversight bodies from other countries to join us in our efforts to limit the risk of an oversight gap and to improve oversight of international data exchange between intelligence and security services.

Signed in Bern on 22 October 2018,

Mr. Serge Lipszyc, Chair of the Belgian Standing Intelligence Agencies Review Committee

Mr. Michael Kistrup, Chair of the Danish Intelligence Oversight Board



Mr. Harm Brouwer, Chair of the Dutch Review Committee on the Intelligence and Security Services

Mrs. Eldbjørg Løwer, Chair of the EOS Committee – The Norwegian Parliamentary Intelligence Oversight Committee

Mr. Thomas Fritschi, Director of the Independent Oversight Authority for Intelligence Activities

From left to right: Harm Brouwer (chair CTIVD, the Netherlands), Thomas Fritschi (director OA-IA, Switzerland), Eldbjorg Lower (chair EOS Committee, Norway), Serge Lypszyc (chair Comité I, Belgium). Michael Kistrup, chair of the Danish oversight board, could not be present when this photo was taken.

VEDLEGG 7 – EOS-kontrolloven[110]

§ 1. Kontrollområdet

Stortinget velger et utvalg til å kontrollere etterretnings-, overvåkings- og sikkerhetstjeneste (tjenestene) som utføres av den offentlige forvaltning eller under styring av eller på oppdrag fra denne (EOS-utvalget). Kontrollen utføres innenfor rammene av §§ 5, 6 og 7.

Kontrollen omfatter ikke overordnet påtalemyndighet.

Offentleglova og forvaltningsloven, med unntak av reglene om ugildhet, gjelder ikke for utvalgets virksomhet.

Stortinget kan gi instruks om virksomheten til utvalget innenfor rammen av denne lov og fastsetter bestemmelser om dets sammensetning, funksjonsperiode og sekretariat.

Innenfor rammen av denne lov utfører utvalget sitt verv selvstendig og uavhengig av Stortinget. Stortinget i plenum kan likevel pålegge utvalget å foreta nærmere definerte undersøkelser innenfor utvalgets kontrollmandat, og under iakttakelse av de regler og innenfor de rammer som for øvrig ligger til grunn for utvalgets virksomhet.

§ 2. Formål

Formålet med utvalgets kontroll er:

1. å klarlegge om og forebygge at noens rettigheter krenkes, herunder påse at det ikke nyttes mer inngripende midler enn det som er nødvendig etter forholdene, og at tjenestene respekterer menneskerettighetene.
2. å påse at virksomheten ikke utilbørlig skader samfunnets interesser.
3. å påse at virksomheten holdes innen rammen av lov, administrative eller militære direktiver og ulovfestet rett.

Utvalget skal iaktta hensynet til rikets sikkerhet og forholdet til fremmede makter. Kontrollen bør innrettes slik at den er til minst mulig ulempe for tjenestenes løpende virksomhet.

Formålet er rent kontrollerende. Utvalget skal følge prinsippet om etterfølgende kontroll. Utvalget kan ikke instruere de kontrollerte organer eller nyttes av disse til konsultasjoner. Utvalget kan likevel kreve innsyn i og uttale seg om løpende saker.

§ 3. Utvalgets sammensetning

Utvalget skal ha syv medlemmer medregnet leder og nestleder, alle valgt av Stortinget etter innstilling fra Stortingets presidentskap, for et tidsrom av inntil fem år. Et medlem kan gjenoppnevnes en gang og maksimalt inneha vervet i ti år. Det bør unngås at flere enn fire medlemmer skiftes ut samtidig. Personer som tidligere har virket i tjenestene, kan ikke velges som utvalgsmedlemmer.

Godtgjørelse til utvalgets medlemmer fastsettes av Stortingets presidentskap.

§ 4. Utvalgets sekretariat

Leder for utvalgets sekretariat tilsettes av Stortingets presidentskap etter innstilling fra utvalget. Tilsetting av det øvrige personalet i sekretariatet foretas av utvalget. Nærmere regler om fremgangsmåten ved tilsetting og adgang til delegering av utvalgets myndighet fastsettes i et personalreglement godkjent av Stortingets presidentskap.

§ 5. Utvalgets oppgaver

Utvalget skal gjennomføre kontroll og regelmessige inspeksjoner av etterretnings-, overvåkings- og sikkerhetstjeneste som utøves i den sivile og militære forvaltning i henhold til §§ 6 og 7.

Utvalget mottar klager fra enkeltpersoner og organisasjoner. Når en klage mottas, avgjør utvalget om klagen gir grunn til behandling, og foretar i så fall de undersøkelser som klagen tilsier.

Av eget tiltak skal utvalget ta opp alle saker og forhold som det ut fra formålet finner riktig å behandle, og særlig slike som har vært gjenstand for offentlig kritikk. Med forhold menes også regelverk, direktiver og praksis.

Utvalgets undersøkelser kan gå ut over de rammer som følger av § 1 første ledd, jf. § 5 når det tjener til å klarlegge saker eller forhold som utvalget undersøker i kraft av sitt mandat.

Kontrolloppgaven omfatter ikke virksomhet som angår personer som ikke er bosatt i riket og organisasjoner som ikke har tilhold her, eller som angår utlendinger hvis opphold er knyttet til tjeneste for fremmed stat. Utvalget kan likevel utøve kontroll i tilfeller som nevnt i første punktum når særlige grunner tilsier det.

Det departement Kongen bestemmer kan helt eller delvis suspendere kontrollen under krise og krig inntil Stortinget bestemmer annet. Ved slik suspensjon skal Stortinget straks underrettes.

§ 6. Utvalgets kontroll

Utvalget skal kontrollere tjenestene i samsvar med formålet i lovens § 2.

Videre skal kontrollen omfatte tjenestenes tekniske virksomhet, herunder overvåking og innhenting av informasjon og behandling av personopplysninger.

Utvalget skal påse at samarbeidet og informasjonsutvekslingen mellom tjenestene og med innenlandske og utenlandske samarbeidspartnere holdes innenfor rammen av de tjenstlige behov og gjeldende regelverk.

Utvalget skal:

1. for Politiets sikkerhetstjeneste: sikre at virksomheten holdes innenfor rammen av tjenestens fastlagte oppgaver og føre kontroll med tjenestens behandling av

110 Lov 3. februar 1995 nr. 7 om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-kontrolloven). Loven ble sist endret i juni 2017.

forebyggende saker og etterforskningssaker, dens bruk av skjulte tvangsmidler og andre skjulte metoder for informasjonsinnhenting.
2. for Etterretningstjenesten: sikre at virksomheten holdes innenfor rammen av tjenestens fastlagte oppgaver.
3. for Nasjonal sikkerhetsmyndighet: sikre at virksomheten holdes innenfor rammen av direktoratets fastlagte oppgaver, å føre kontroll med klareringssaker for personer og bedrifter hvor klarering er nektet, tilbakekalt, nedsatt eller suspendert av klareringsmyndighetene.
4. for Forsvarets sikkerhetsavdeling: føre kontroll med at avdelingens utøvelse av personellsikkerhetstjeneste og annen sikkerhetstjeneste holdes innenfor rammen av lov og forskriftsverk og avdelingens fastlagte oppgaver og påse at ingens rettigheter krenkes.

Kontrollen skal skje med innføring i den løpende virksomheten og slik besiktigelse som finnes nødvendig.

§ 7. Inspeksjoner

Inspeksjonsvirksomheten skal skje i samsvar med formålet i lovens § 2.

Inspeksjonene skal gjennomføres ut fra behov og minst omfatte:

1. flere inspeksjoner årlig av Etterretningstjenesten sentralt.
2. flere inspeksjoner årlig av Nasjonal sikkerhetsmyndighet.
3. flere inspeksjoner årlig av Den sentrale enhet i Politiets sikkerhetstjeneste.
4. flere inspeksjoner årlig av Forsvarets sikkerhetsavdeling.
5. en årlig inspeksjon av Etterretningsbataljonen.
6. en årlig inspeksjon av Forsvarets spesialstyrker.
7. en årlig inspeksjon av PST-enhetene i minst to politidistrikter og av minst en av Etterretningstjenestens stasjoner eller etterretnings-/sikkerhetstjeneste ved militære staber og avdelinger.
8. inspeksjon av eget tiltak av det øvrige politi og andre organer eller institusjoner som bistår Politiets sikkerhetstjeneste.
9. for øvrig slik inspeksjon som lovens formål tilsier.

§ 8. Innsynsrett mv.

For å utføre sitt verv, kan utvalget kreve innsyn i og adgang til forvaltningens arkiver og registre, lokaler, installasjoner og anlegg av enhver art. Like med forvaltningen regnes virksomhet mv. som eies med mer enn en halvdel av det offentlige. Utvalgets rett til innsyn og adgang etter første punktum gjelder tilsvarende overfor virksomheter som bistår ved utførelse av etterretnings-, overvåkings- og sikkerhetstjeneste.

Enhver som tjenestegjør i forvaltningen plikter på anmodning å tilveiebringe alt materiale, utstyr mv. som kan ha betydning for gjennomføring av kontrollen. Andre har samme plikt med hensyn til materiale, utstyr mv. som de har mottatt fra offentlige organer.

Utvalget skal ikke søke et mer omfattende innsyn i graderte opplysninger enn det som er nødvendig ut fra kontrollformålene. Utvalget skal så vidt mulig iaktta hensynet til kildevern og vern av opplysninger mottatt fra utlandet.

Utvalgets beslutninger om hva det skal søke innsyn i og om omfanget og utstrekningen av kontrollen, er bindende for forvaltningen. Mot slike beslutninger kan det ansvarlige personell på vedkommende tjenestested kreve inntatt begrunnet protest i møteprotokollen. Etterfølgende protest kan gis av sjefen for vedkommende tjeneste og av forsvarssjefen. Protester som her nevnt, skal inntas i eller følge utvalgets årsmelding.

Mottatte opplysninger skal ikke meddeles annet autorisert personell eller andre offentlige organer som er ukjente med dem uten at det er tjenestlig behov for det, er nødvendig ut fra kontrollformålene eller følger av saksbehandlingsreglene i § 12. I tilfelle tvil bør avgiveren av opplysningene forespørres.

§ 9. Forklaringer og møteplikt mv.

Enhver plikter etter innkalling å møte for utvalget.

Klagere og andre privatpersoner i partsliknende- stilling kan på ethvert trinn i saken la seg bistå av advokat eller annen fullmektig i den utstrekning det kan skje uten at graderte opplysninger derved blir kjent for fullmektigen. Samme rett har ansatte og tidligere ansatte i forvaltningen i saker som kan ende med kritikk mot dem.

Alle som er eller har vært i forvaltningens tjeneste har forklaringsplikt for utvalget om alt de har erfart i tjenesten.

Pliktmessig avgitt forklaring må ikke foreholdes noen eller fremlegges i retten i straffesak mot avgiveren uten dennes samtykke.

Utvalget kan begjære bevisopptak etter domstolloven § 43 annet ledd. Tvisteloven §§ 22-1 og 22-3 gjelder ikke. Rettsmøtene skal være lukket og forhandlingene holdes hemmelige. Forhandlingene holdes hemmelige inntil utvalget eller vedkommende departement bestemmer annet, jf. §§ 11 og 16.

§ 10. Om statsrådene og departementene

Reglene i §§ 8 og 9 gjelder ikke statsrådene, departementene og deres embets- og tjenestemenn, unntatt i forbindelse med klarering og autorisasjon av personer og bedrifter for behandling av graderte opplysninger.

Utvalget kan ikke kreve innsyn i departementenes interne dokumenter.

Dersom EOS-utvalget ønsker opplysninger eller uttalelser fra et departement eller dets personell, i andre saker enn slike som gjelder departementets befatning med klarering og autorisasjon av personer og bedrifter, innhentes disse skriftlig fra departementet.

§ 11. Taushetsplikt mv.

Med de unntak som følger av §§ 14 til 16, har utvalget og dets sekretariat taushetsplikt.

Utvalgets medlemmer og sekretariat er bundet av regler om behandling av dokumenter mv. som må beskyttes av sikkerhetsmessige grunner. De skal være sikkerhetsklarert og autorisert for høyeste sikkerhetsgrad nasjonalt og etter traktat Norge er tilsluttet. Stortingets presidentskap er

klareringsmyndighet for utvalgets medlemmer. Personkontroll utføres av Nasjonal sikkerhetsmyndighet.

Hvis utvalget er i tvil om graderingen av opplysninger i uttalelse eller meldinger, eller mener at av- eller nedgradering bør skje, forelegger det spørsmålet for vedkommende etat eller departement. Forvaltningens avgjørelse er bindende for utvalget.

§ 12. Saksbehandling

Samtaler med privatpersoner skal skje i avhørsform med mindre de er av orienterende art. Samtaler med forvaltningens personell skal skje i avhørs form når utvalget finner grunn til det eller tjenestemannen ber om det. I saker som kan ende med kritikk mot bestemte tjenestemenn, bør avhørs form i alminnelighet nyttes.

Den som avhøres skal gjøres kjent med sine rettigheter og plikter, jf. § 9. Forvaltningens personell, og tidligere ansatte kan under avhør i saker som kan ende med kritikk mot dem også la seg bistå av en tillitsvalgt som er autorisert etter sikkerhetsloven med forskrifter. Forklaringen skal oppleses til vedtakelse og undertegning.

Personer som kan bli utsatt for kritikk fra utvalget, bør varsles om de ikke allerede kjenner til saken. De har rett til å gjøre seg kjent med utvalgets ugraderte materiale og med gradert materiale som de er autorisert for, alt såframt det ikke vil skade undersøkelsene.

Enhver som gir forklaring skal foreholdes beviser og påstander som ikke samsvarer med vedkommendes egne, såframt bevisene og påstandene er ugraderte eller vedkommende er autorisert for dem.

§ 13. Beslutningsdyktighet og arbeidsform

Utvalget er beslutningsdyktig når fem medlemmer er til stede.

Utvalget skal være beslutningsdyktig på inspeksjoner av tjenestene sentralt som omtalt i § 7, men kan møte med færre medlemmer på inspeksjoner utover dette eller i lokale enheter. Utvalget skal alltid være representert ved minst to medlemmer på inspeksjoner.

Ved særlig omfattende undersøkelser kan innhenting av forklaringer, besiktigelser på stedet mv. overlates til sekretariatet og ett eller flere medlemmer. Det samme gjelder dersom slik innhenting av et samlet utvalg vil kreve uforholdsmessig arbeid eller kostnad. Ved avhør som nevnt i dette ledd, kan utvalget anta bistand.

§ 14. Generelt om kontrollen og uttalelser

EOS-utvalget har rett til å uttale sin mening om forhold som omfattes av kontrollområdet.

Utvalget kan påpeke at det er gjort feil eller utvist forsømmelige forhold i tjenestene. Kommer utvalget til at en avgjørelse må anses ugyldig eller klart urimelig, eller klart strider mot god forvaltningspraksis, kan det gi uttrykk for dette. Mener utvalget at det knytter seg begrunnet tvil til forhold av betydning i saken, kan det gjøre vedkommende tjeneste oppmerksom på dette.

Blir utvalget oppmerksom på mangler ved lover; administrative forskrifter eller administrativ praksis, kan det gi vedkommende departement underretning om det. Utvalget kan også foreslå forbedringer i administrative og organisatoriske ordninger og rutiner når det kan tjene til å lette kontrollen eller verne mot at noens rettigheter krenkes.

Før det gis uttalelse i saker som kan ende med kritikk eller meningsytringer rettet mot forvaltningen, skal den ansvarlige sjef gis anledning til å uttale seg om de spørsmål saken reiser.

Uttalelser til forvaltningen rettes til sjefen for vedkommende tjeneste eller organ eller til forsvarssjefen eller vedkommende departement hvis det gjelder forhold disse bør kjenne til som instruksjons- og kontrollmyndighet.

Ved uttalelser som gir oppfordring til å iverksette tiltak eller treffe beslutninger, skal mottakeren bes om å gi tilbakemelding om hva som blir foretatt.

§ 15. Uttalelser til klagere og forvaltningen

Uttalelser til klagere bør være så fullstendige som mulig uten at det gis graderte opplysninger. Opplysning om at noen har vært gjenstand for overvåkingsvirksomhet eller ikke, anses som gradert hvis annet ikke blir bestemt. Ved klager mot tjenestene om overvåkingsmessig virksomhet skal det bare uttales om klagen har gitt grunn til kritikk eller ikke. Mener utvalget at en klager bør gis en mer utfyllende begrunnelse, gir det forslag om det overfor den tjeneste det gjelder eller vedkommende departement.

Hvis en klage gir grunn til kritikk eller meningsytringer for øvrig, skal begrunnet uttalelse om dette rettes til sjefen for den tjeneste det gjelder eller vedkommende departement. Også ellers skal uttalelser i klagesaker alltid meddeles sjefen for den tjeneste klagen er rettet mot.

Uttalelser til forvaltningen graderes etter sitt innhold.

§ 16. Meddelelser til offentligheten

Utvalget avgjør i hvilken utstrekning dets ugraderte uttalelser eller ugraderte deler av uttalelsene skal offentliggjøres.

Hvis offentliggjøring må antas å medføre at en klagers identitet vil bli avdekket, skal dennes samtykke foreligge. Ved omtalen av personer skal hensynet til personvernet iakttas også om det ikke gjelder klagere. Tjenestemenn skal ikke navngis eller identifiseres på annen måte uten med vedkommende departements godkjennelse.

For øvrig kan lederen eller den utvalget bemyndiger i vedkommendes sted gi meddelelser til offentligheten om hvorvidt en sak er under undersøkelse og om den er ferdigbehandlet, eller når den vil bli det.

For saksdokumenter som er utarbeidet av eller til EOS-utvalget i saker som det vurderer å legge fram for Stortinget som ledd i den konstitusjonelle kontroll, skal innsyn først gis når saken er mottatt i Stortinget. EOS-utvalget varsler vedkommende forvaltningsorgan om at saken er av en slik art. Er en slik sak ferdigbehandlet uten at den oversendes Stortinget, inntrer offentlighet når utvalget har varslet vedkommende forvaltningsorgan om at saken er ferdigbehandlet.

§ 17. Forholdet til Stortinget

Bestemmelsen i § 16 første og annet ledd gjelder tilsvarende for utvalgets meldinger og årsmeldinger til Stortinget. Hvis utvalget anser at hensynet til Stortingets kontroll med forvaltningen tilsier at Stortinget bør gjøre seg kjent med graderte opplysninger i en sak eller et forhold det har undersøkt, skal det i særskilt melding eller i sin årsmelding gjøre Stortinget oppmerksom på det. Det samme gjelder dersom det er behov for ytterligere undersøkelser om forhold som utvalget selv ikke kan komme videre med.

Utvalget avgir årlig melding til Stortinget om sin virksomhet. Melding kan også gis hvis det er avdekket forhold som Stortinget straks bør kjenne til. Meldingene og deres vedlegg skal være ugraderte. Årsmeldingen avgis innen 1. april hvert år.

Årsmeldingen bør omfatte:

1. en oversikt over utvalgets sammensetning, møtevirksomhet og utgifter.
2. en redegjørelse for utførte inspeksjoner og resultatene av disse.
3. en oversikt over klagesaker fordelt etter art og tjenestegren og med angivelse av hva klagene har resultert i.
4. en redegjørelse for saker og forhold tatt opp av eget tiltak.
5. en angivelse av eventuelle tiltak som er bedt iverksatt og hva det har ført til, jf. § 14 sjette ledd.
6. en angivelse av eventuelle protester etter § 8 fjerde ledd.
7. en omtale av saker eller forhold som bør behandles av Stortinget.
8. utvalgets alminnelige erfaringer med kontrollen og regelverket og mulige behov for endringer.

§ 18. Ordensforskrifter

Sekretariatet fører sakjournal og møteprotokoll. Beslutninger og dissenser skal framgå av protokollen.

Uttalelser og bemerkninger som framkommer eller protokolleres under kontroll, anses ikke avgitt av utvalget uten at de er meddelt skriftlig.

§ 19. Bistand mv.

Utvalget kan anta bistand.

Lovens regler gjelder tilsvarende for bistandspersoner. Bistandspersoner skal likevel bare autoriseres for slik beskyttelsesgrad som oppdraget krever.

Personer som er ansatt i tjenestene, kan ikke antas som bistandspersoner.

§ 20. Økonomiforvaltning, utgiftsdekning til innkalte og sakkyndige

Utvalget har ansvaret for den økonomiske styringen av utvalgets virksomhet, og fastsetter egen instruks for sin økonomiforvaltning. Instruksen skal være godkjent av Stortingets presidentskap.

Enhver som blir innkalt til utvalget har krav på å få sine reisekostnader dekket etter det offentlige regulativ. Tap i inntekt erstattes etter lov 21. juli 1916 nr. 2 om vidners og sakkyndiges godtgjørelse m.v.

Sakkyndige godtgjøres etter salærforskriften. Andre satser kan avtales.

§ 21. Straff

Forsettlig eller grov uaktsom overtredelse av § 8 første og annet ledd, § 9 første og tredje ledd, § 11 første og annet ledd og § 19 annet ledd i denne lov straffes med bøter eller fengsel inntil 1 år, hvis ikke strengere straffebestemmelse får anvendelse.

Foto: Daniel Nordby / Forsvaret

STORTINGETS KONTROLLUTVALG
FOR ETTERRETNINGS-, OVERVÅKINGS- OG SIKKERHETSTJENESTE

fdesign.no

Kontaktinformasjon
Telefon: +47 23 31 09 30
E-post: post@eos-utvalget.no

www.eos-utvalget.no

STORTINGETS KONTROLLUTVALG
FOR ETTERRETNINGS-, OVERVÅKINGS- OG SIKKERHETSTJENESTE

Årsrapport 2018

Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget)

Innhold

DEL I. Leders beretning

EOS-utvalget er et permanent kontrollorgan nedsatt av Stortinget. Hovedformålet med utvalgets kontroll er å klarlegge om og forebygge at etterretnings-, overvåkings- og sikkerhetstjenestene (EOS-tjenestene) – de hemmelige tjenestene – krenker noens rettigheter, spesielt å hindre at enkeltpersoner blir utsatt for ulovlig overvåking.

EOS-kontrolloven regulerer utvalgets virksomhet.[1] I løpet av et år skal utvalget gjennomføre minst et bestemt antall inspeksjoner i EOS-tjenestene, behandle innkomne klager, samt iverksette undersøkelser i tjenestene av eget tiltak.

Utvalget mottok i fjor 19 klager og tok opp 22 saker av eget tiltak. I løpet av 2018 var utvalget på 20 inspeksjoner. Det ble avgitt en årsmelding til Stortinget.[2]

De målbare kravene til EOS-utvalgets kontrollvirksomhet er oppnådd. Innenfor virksomhetens rammer arbeider utvalget kontinuerlig for å bedre kontrollen. I 2018 ansatte utvalget to teknologer til en ny teknologisk enhet i sekretariatet. Totalt er det nå tre teknologer i sekretariatet. Utvalget ba Stortinget om midler til ytterligere to teknologer i budsjettet for 2019, uten å få det i denne omgang. Utvalget vil forsøke å få midler til disse i budsjettet for 2020. Dette er noe utvalget ser et sterkt behov for, slik at vi kan holde tritt med den raske teknologiske utviklingen. I 2018 ansatte utvalget også en sikkerhetsleder i en nyopprettet stilling i sekretariatet. To jurister erstattet i 2018 to jurister som sluttet i 2017.

Utvalget fikk også midler i 2018 til å flytte til større og sikrere lokaler. Utvalget vil være på plass i nye lokaler våren 2019. Det har medgått noe kostnader til dette i 2018. I rapportåret har det også vært en økning i utgifter på reiser og diett. Det skyldes særlig mer internasjonalt samarbeid på kontrollsiden – inkludert en studietur til USA.

Utvalgets utgifter i 2018 var innenfor godkjent bevilgning. Det var et mindreforbruk på kr 598 089. Det skyldes i hovedsak permisjoner i utvalgets sekretariat og at det har tatt tid å rekruttere ansatte – særlig til teknologstillinger. For nærmere detaljer vises det til del VI. Årsregnskap.

EOS-utvalget består av 7 medlemmer. Utvalget har et permanent sekretariat, som per 31.desember 2018 hadde 14 ansatte, fordelt på sekretariatsleder (jurist), 6 juridiske saksbehandlere, 3 teknologer, 1 sikkerhetsleder, 1 informasjonsrådgiver og 2 administrativt ansatte. Utvalget har tidligere hatt en teknisk sakkyndig tilknyttet seg på timebasis, men han er nå ansatt som leder for sekretariatets nye teknologiske enhet.

Som leder av EOS-utvalget kan jeg konstatere at medlemmene i utvalget og de ansatte i sekretariatet har bidratt til solide og tilfredsstillende resultater i 2018.

Oslo, 11. mars 2019

Eldbjørg Løwer

Utvalgsleder

[1] Lov 3. februar 1995 nr. 7 om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-kontrolloven). Loven ble sist endret 21. juni 2017.
[2] Dokument 7:1 (2016–2017).

DEL II. Introduksjon til virksomheten og hovedtall

EOS-utvalget startet sin virksomhet i 1996. Utvalgets oppgave er å kontrollere etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-tjeneste) som utføres av den offentlige forvaltning, eller som er under styring av eller utføres på oppdrag fra offentlig forvaltning. EOS-tjeneste med andre formål enn å ivareta rikets sikkerhet, for eksempel politiets alminnelige kriminaletterretning og trafikkovervåking, omfattes ikke av kontrollområdet.

Kontrollområdet er ikke knyttet til bestemte organisatoriske enheter. Det er derfor ikke avgjørende hvilke organer eller etater som til enhver tid driver EOS-tjeneste. I dag er disse oppgavene hovedsakelig lagt til Etterretningstjenesten (E-tjenesten), Politiets sikkerhetstjeneste (PST), Nasjonal sikkerhetsmyndighet (NSM) og Forsvarets sikkerhetsavdeling (FSA). Ved en lovendring i 2017 ble utvalget også pålagt å ha minst en årlig inspeksjon hos henholdsvis Etterretningsbataljonen og Forsvarets Spesialstyrker. Utvalget kan også undersøke deler av politiet eller for eksempel private teleselskaper som bistår PST, eller andre deler av forvaltningen om det er nødvendig ut fra kontrolloppgaven. Overordnet påtalemyndighet, det vil si statsadvokatene og riksadvokaten, er unntatt fra kontrollområdet.

Formålet med utvalgets kontroll er:[3]

1) Å klarlegge om og forebygge at noens rettigheter krenkes, herunder påse at det ikke nyttes mer inngripende midler enn det som er nødvendig etter forholdene, og at tjenestene respekterer menneskerettighetene,

2) å påse at virksomheten ikke utilbørlig skader samfunnets interesser, og

3) å påse at virksomheten holdes innen rammen av lov, administrative eller militære direktiver og ulovfestet rett.

Utvalgets virkemidler for å nå hovedmålene er først og fremst gjennomføring av inspeksjoner, behandling av klagesaker og undersøkelse av saker av eget tiltak.[4]

Utvalgets erfaringer med kontrollen og resultatet av den meddeles årlig i en melding til Stortinget. Utvalget kan også avgi særskilte meldinger til Stortinget, blant annet dersom det er avdekket forhold som Stortinget straks bør kjenne til.

Utvalget har 7 medlemmer, medregnet leder og nestleder. Stortinget velger medlemmene i plenum etter innstilling fra Stortingets presidentskap. Funksjonsperioden er 5 år, og medlemmene kan gjenoppnevnes én gang. Medlemmene kan dermed maksimalt inneha vervet i 10 år. Medlemmene utfører oppdraget som et verv.

Utvalget utfører sitt løpende arbeid uavhengig av Stortinget, og stortingsrepresentanter kan ikke samtidig være medlemmer av utvalget. Personer som tidligere har arbeidet i EOS-tjenestene kan heller ikke velges som utvalgsmedlemmer.

[3] Jf. EOS-kontrolloven § 2 første ledd.
[4] Jf. EOS-kontrolloven § 5.

Per 31. desember 2018 bestod EOS-utvalget av følgende medlemmer:

- Eldbjørg Løwer (leder)
- Svein Grønnern (nestleder)
- Theo Koritzinsky
- Håkon Haugli
- Øyvind Vaksdal
- Inger Marie Sunde
- Eldfrid Øfsti Øvstedal

Utvalget møtes normalt til en møte- og inspeksjonssesjon på 3 dager hver måned. Utvalgsmedlemmenes samlede arbeid, inkludert nødvendige forberedelser innebærer opptil 20 prosent av en full stilling. Lederen har ytterligere ansvar som gjør at hun har opptil 30 prosent av en full stilling.

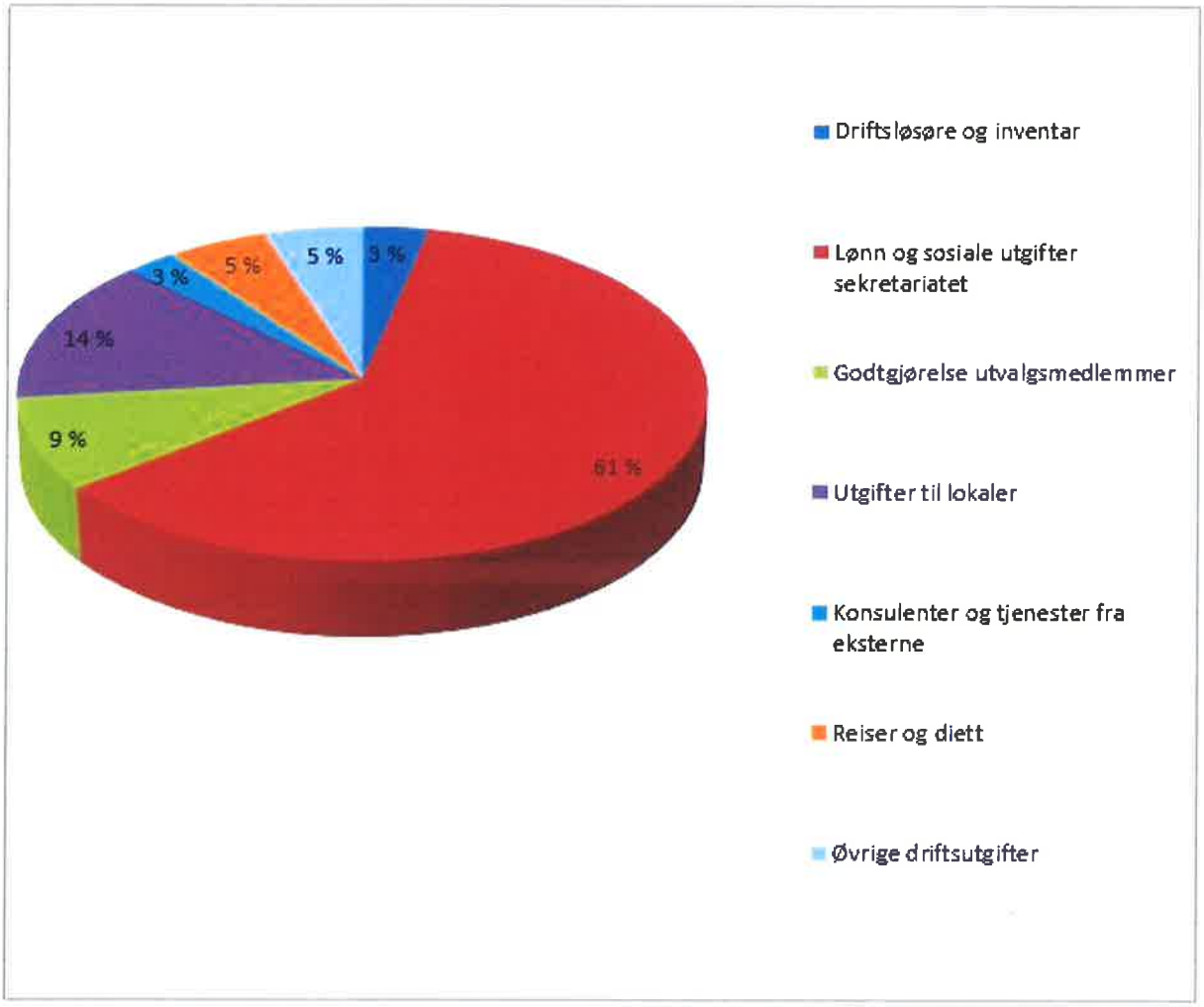
Tabell 1: Utvalgte nøkkeltall fra årsregnskapet 2016–2018

Nøkkeltall fra årsregnskapet 2016–2018	**2016**	**2017**	**2018**
Antall årsverk i sekretariatet	11	11	14
Antall medlemmer i utvalget	7	7	7
Samlet tildeling inkludert overførte midler	14 950 000	15 185 000	19 550 000
Samlet forbruk	14 764 958	13 632 788	18 951 911
Utnyttelsesgrad av samlet tildeling	99 %	90 %	97 %

Tabell 2: Utgifter etter art 2018 (se også figur 1)

Utgifter etter art 2017–2018	**2017**	**2018**
Driftsløsøre og inventar	163 301	633 084
Lønn og sosiale utgifter sekretariatet	8 297 609	11 546 607
Godtgjørelse utvalgsmedlemmer	1 610 641	1 688 371
Utgifter til lokaler	1 589 669	2 651 790
Konsulenter og tjenester fra eksterne	314 487	496 821
Reiser og diett	672 571	971 125
Øvrige driftsutgifter	984 510	964 114
SUM	**13 632 788**	**18 951 912**

Figur 1: Utgifter etter art 2018



DEL III. Årets aktiviteter og resultater

EOS-utvalgets samfunnsoppdrag er å føre en legalitetskontroll med EOS-tjenestene – det vil si å påse at de hemmelige tjenestene holder seg innenfor lover og regler.

Utvalgets kontrollvirksomhet utøves i hovedsak ved at utvalget gjennomfører anmeldte inspeksjoner i EOS-tjenestene. EOS-kontrolloven krever et minimum av 13 inspeksjoner per år, men utvalget kan ved behov gjennomføre flere inspeksjoner.[5]

Utvalget har i 2018 gjennomført 20 inspeksjoner; PST er inspisert 7 ganger, E-tjenesten 4 ganger, NSM 2 ganger og FSA 2 ganger. Etterretningsbataljonen, Nasjonal kommunikasjonsmyndighet, Forsvarets spesialkommando, Telia Norge AS og Felles cyberkoordineringssenter er inspisert en gang hver.

Utvalget har i 2018 gjennomført én inspeksjon på kort varsel. De ordinære inspeksjonene inneholder betydelige uanmeldte elementer. Utvalget kan i all hovedsak gjennomføre kontrollen direkte i tjenestens elektroniske systemer. Dette innebærer at hvilken informasjon som vil kontrolleres, ikke er kjent for tjenestene i forkant av eller under inspeksjonen. Tjenesten blir først oppmerksom på dette i etterkant av inspeksjonen når utvalget eventuelt retter skriftlige henvendelser til tjenesten om funn.

I 2018 undersøkte utvalget 22 saker av eget tiltak, mot 31 saker i 2017. Sakene som ble undersøkt i 2018 har generelt vært mer arbeidskrevende enn sakene i 2017. Sakene utvalget har undersøkt av eget tiltak er hovedsakelig funn fra utvalgets inspeksjoner.

Utvalget undersøker klager fra enkeltpersoner og organisasjoner. Det kom inn 19 klager til utvalget i 2018, mot 26 klager i 2017. Utvalget prioriterer klagesaksbehandlingen, og bruker en god del ressurser på den. Enkelte av klagene har vært rettet mot flere av EOS-tjenestene samtidig. Utvalget har på formelt grunnlag avvist noen klagesaker, blant annet under henvisning til at forholdet faller utenfor utvalgets kontrollområde. Klager og henvendelser som faller innenfor utvalgets kontrollområde undersøkes i den eller de tjenester klagen retter seg mot. Utvalget praktiserer generelt sett en lav terskel for å behandle klagesaker.

Utvalget mener at ressursbruken har vært effektiv i 2018, både med tanke på hva det er brukt ressurser på og hvordan disse er benyttet. Samlet sett er utvalget fornøyd med resultater, måloppnåelse og ressursbruk i 2018.

En nærmere redegjørelse for årets aktiviteter og resultater vil følge av utvalgets årsmelding for 2018, som overleveres til Stortinget 27. mars 2019.

Tabell 3: Antall inspeksjoner, eget tiltak-saker og klagesaker 2016–2018

	2016	2017	2018
Inspeksjoner	26	21	20
Eget tiltak-saker	51	31	22
Klagesaker	32	26	19

EOS-utvalget har i 2018 hatt kontakt med ulike eksterne miljøer. Dette inkluderer blant annet andre staters kontrollorganer, sivilsamfunnet, forsknings- og utdanningsmiljøer og nasjonale

[5] I juni 2017 ble EOS-kontrolloven endret slik at minimumskravet gikk fra 23 til 13 for å gi utvalget større fleksibilitet, jf. EOS-kontrolloven § 7.

kontrollinstanser. I 2018 publiserte også EOS-utvalget i samarbeid med kontrollorganer i Danmark, Nederland, Sveits og Belgia for første gang en felles uttalelse om styrking av internasjonalt kontrollsamarbeid

I september var utvalget på en studiereise i USA for å lære mer om kontrollsystemet der. Utvalget møtte blant annet representanter fra kontrollorganer, politiske miljøer, etterretningstjenester og sivilsamfunnet.

EOS-utvalget arrangerte for andre året på rad en årskonferanse om kontroll av hemmelige tjenester i 2018 i forbindelse med overleveringen av årsmeldingen til Stortinget. Årskonferansen var åpen for publikum. Årskonferansen for 2019 arrangeres 28. mars.

DEL IV. Styring og kontroll i virksomheten

Utvalgets virksomhet reguleres i EOS-kontrolloven. Videre kan det gis føringer fra Kontroll- og konstitusjonskomiteen i dens innstillinger om utvalgets meldinger til Stortinget, samt fra stortingsbehandlingen av meldingene. Stortinget kan også ved plenarvedtak (stortingsvedtak) pålegge utvalget å foreta nærmere definerte undersøkelser innenfor utvalgets kontrollmandat, og under iakttakelse av de regler og innen de rammer som for øvrig ligger til grunn for utvalgets virksomhet.[6]

Utvalget er som øvrige statlige virksomheter underlagt kontroll av Riksrevisjonen. Riksrevisjonen har ikke hatt merknader som har krevd oppfølging fra utvalget i 2018.

Utvalget har flere instruksdokumenter som regulerer driften i utvalget og sekretariatet. Det foreligger blant annet strenge sikkerhetsrutiner, noe som særlig har bakgrunn i utvalgets håndtering av sikkerhetsgradert informasjon. De ansatte er godt kjent med interne retningslinjer og instrukser.

IA-avtalen har høy oppmerksomhet i sekretariatet. Sykefraværet[7] i sekretariatet har vært på 5,2 prosent i 2018. I 2017 var tallet 5,6 prosent.

[6] Jf. EOS-kontrolloven § 1 femte ledd.
[7] Egenmeldinger og sykmeldinger.

DEL V. Vurdering av fremtidsutsikter

Den teknologiske utviklingen innenfor kontrollområdet til EOS-utvalget skjer veldig raskt. Utvalget har allerede tre ansatte teknologer og håper å få midler i 2020 til ytterligere to stillinger i den nye teknologiske enheten. I forbindelse med ny lov om Etterretningstjenesten som nå er på høring fra Forsvarsdepartementet kan det være at sekretariatet vil få behov for enda flere ansatte, både juridisk og især teknologisk kompetanse.

Utvalget er også opptatt av å bli mer synlige og å være tilgjengelig for intervjuer og foredrag for dem som ønsker det – gitt at det kan gjøres i tråd med taushetsplikten.

DEL VI. Årsregnskap

Ledelseskommentarer til årsregnskapet for 2018

Formål

EOS-utvalget kontrollerer EOS-tjenestene på vegne av Stortinget, men er uavhengig i sitt løpende arbeid. Utvalget fører regnskap i henhold til kontantprinsippet, slik det fremgår av prinsippnoten til årsregnskapet.

Bekreftelse

Årsregnskapet er avlagt i henhold til bestemmelser om økonomistyring i staten kapittel 2.3.3, jf. Finansdepartementets rundskriv R-115 datert 24. november 2016. Jeg mener regnskapet gir et dekkende bilde av utvalgets disponible bevilgninger og regnskapsførte utgifter.

Vurderinger av vesentlige forhold

Regnskapstallene for 2018 viser et forbruk på kr 18 951 911. Det innebærer et overskudd på kr 598 089 sammenlignet med budsjettet for 2018, som var på kr 19 550 000, inkludert overføring på kr 750 000 fra 2017. Det er anmodet om å få overført kr 598 000 til budsjettet for 2019.

Utbetalinger til lønn, godtgjørelse og sosiale utgifter til utvalgsmedlemmene og ansatte i sekretariatet beløp seg til kr 13 234 978, mot kr 9 908 250 i 2017. Utgifter til lønn og godtgjørelse utgjorde 69,8 prosent av driftsutgiftene for 2018.

Mellomværende med statskassen utgjorde per 31. desember 2018 kr 625 704.

Tilleggsopplysninger

Riksrevisjonen er ekstern revisor og bekrefter årsregnskapet for utvalget. Årsregnskapet er ikke ferdig revidert per d.d., men revisjonsberetningen antas å foreligge i løpet av andre kvartal 2019.

Oslo, 11. mars 2019

Eldbjørg Løwer
utvalgsleder

Prinsippnote årsregnskapet

Årsregnskap for EOS-utvalget er utarbeidet og avlagt etter nærmere retningslinjer fastsatt i bestemmelser om økonomistyring i staten («bestemmelsene»), fastsatt 12. desember 2003. Årsregnskapet er i henhold til krav i bestemmelsene punkt 3.4.1, nærmere bestemmelser i Finansdepartementets rundskriv R-115 fra 24. november 2016 og eventuelle tilleggskrav fastsatt av Stortinget.

Oppstillingen av bevilgningsrapporteringen omfatter en øvre del med bevilgningsrapporteringen og en nedre del som viser beholdninger virksomheten står oppført med i kapitalregnskapet.

Oppstillingen av artskontorapporeringen har en øvre del som viser hva som er rapportert til statsregnskapet etter standard kontoplan for statlige virksomheter og en nedre del som viser grupper av kontoer som inngår i mellomværende med statskassen.

Oppstillingen av bevilgningsrapporteringen og artskontorapporteringen er utarbeidet med utgangspunkt i bestemmelsene punkt 3.4.2 – de grunnleggende prinsippene for årsregnskapet:

a) Regnskapet følger kalenderåret
b) Regnskapet inneholder alle rapporterte utgifter og inntekter for regnskapsåret
c) Utgifter og inntekter er ført i regnskapet med brutto beløp
d) Regnskapet er utarbeidet i tråd med kontantprinsippet

Oppstillingene av bevilgnings- og artskontorapportering er utarbeidet etter de samme prinsippene, men gruppert etter ulike kontoplaner. Prinsippene korresponderer med krav i bestemmelsene punkt 3.5 til hvordan virksomhetene skal rapportere til statsregnskapet. Sumlinjen «Netto rapportert til bevilgningsregnskapet» er lik i begge oppstillingene.

Alle statlige virksomheter er tilknyttet statens konsernkontoordning i Norges Bank i henhold til krav i bestemmelsene punkt 3.8.1. Ordinære forvaltningsorgan (bruttobudsjetterte virksomheter) tilføres ikke likviditet gjennom året. Ved årets slutt nullstilles saldoen på den enkelte oppgjørskonto ved overgang til nytt år.

Bevilgningsrapporteringen

Bevilgningsrapporteringen viser regnskapstall som utvalget har rapportert til statsregnskapet. Det stilles opp etter de kapitler og poster i bevilgningsregnskapet som utvalget har fullmakt til å disponere. Oppstillingen viser alle finansielle eiendeler og forpliktelser utvalget står oppført med i

Statens kapitalregnskap. Kolonnen samlet tildeling viser hva virksomheten har fått stilt til disposisjon i tildelingsbrev for hver kombinasjon av kapittel/post.

Artskontorapporteringen

Artskontorapporteringen viser regnskapstall utvalget har rapportert til statsregnskapet etter standard kontoplan for statlige virksomheter. Utvalget har en trekkrettighet for disponible tildelinger på konsernkonto i Norges Bank. Tildelingene skal ikke inntektsføres og vises derfor ikke som inntekt i oppstillingen.

Note 8 til artskontorapporteringen viser forskjeller mellom avregning med statskassen og mellomværende med statskassen.

DEL II. Introduksjon til virksomheten og hovedtall

EOS-utvalget startet sin virksomhet i 1996. Utvalgets oppgave er å kontrollere etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-tjeneste) som utføres av den offentlige forvaltning, eller som er under styring av eller utføres på oppdrag fra offentlig forvaltning. EOS-tjeneste med andre formål enn å ivareta rikets sikkerhet, for eksempel politiets alminnelige kriminaletterretning og trafikkovervåking, omfattes ikke av kontrollområdet.

Kontrollområdet er ikke knyttet til bestemte organisatoriske enheter. Det er derfor ikke avgjørende hvilke organer eller etater som til enhver tid driver EOS-tjeneste. I dag er disse oppgavene hovedsakelig lagt til Etterretningstjenesten (E-tjenesten), Politiets sikkerhetstjeneste (PST), Nasjonal sikkerhetsmyndighet (NSM) og Forsvarets sikkerhetsavdeling (FSA). Ved en lovendring i 2017 ble utvalget også pålagt å ha minst en årlig inspeksjon hos henholdsvis Etterretningsbataljonen og Forsvarets Spesialstyrker. Utvalget kan også undersøke deler av politiet eller for eksempel private teleselskaper som bistår PST, eller andre deler av forvaltningen om det er nødvendig ut fra kontrolloppgaven. Overordnet påtalemyndighet, det vil si statsadvokatene og riksadvokaten, er unntatt fra kontrollområdet.

Formålet med utvalgets kontroll er:[3]

1) Å klarlegge om og forebygge at noens rettigheter krenkes, herunder påse at det ikke nyttes mer inngripende midler enn det som er nødvendig etter forholdene, og at tjenestene respekterer menneskerettighetene,

2) å påse at virksomheten ikke utilbørlig skader samfunnets interesser, og

3) å påse at virksomheten holdes innen rammen av lov, administrative eller militære direktiver og ulovfestet rett.

Utvalgets virkemidler for å nå hovedmålene er først og fremst gjennomføring av inspeksjoner, behandling av klagesaker og undersøkelse av saker av eget tiltak.[4]

Utvalgets erfaringer med kontrollen og resultatet av den meddeles årlig i en melding til Stortinget. Utvalget kan også avgi særskilte meldinger til Stortinget, blant annet dersom det er avdekket forhold som Stortinget straks bør kjenne til.

Utvalget har 7 medlemmer, medregnet leder og nestleder. Stortinget velger medlemmene i plenum etter innstilling fra Stortingets presidentskap. Funksjonsperioden er 5 år, og medlemmene kan gjenoppnevnes én gang. Medlemmene kan dermed maksimalt inneha vervet i 10 år. Medlemmene utfører oppdraget som et verv.

Utvalget utfører sitt løpende arbeid uavhengig av Stortinget, og stortingsrepresentanter kan ikke samtidig være medlemmer av utvalget. Personer som tidligere har arbeidet i EOS-tjenestene kan heller ikke velges som utvalgsmedlemmer.

[3] Jf. EOS-kontrolloven § 2 første ledd.
[4] Jf. EOS-kontrolloven § 5.

Per 31. desember 2018 bestod EOS-utvalget av følgende medlemmer:

- Eldbjørg Løwer (leder)
- Svein Grønnern (nestleder)
- Theo Koritzinsky
- Håkon Haugli
- Øyvind Vaksdal
- Inger Marie Sunde
- Eldfrid Øfsti Øvstedal

Utvalget møtes normalt til en møte- og inspeksjonssesjon på 3 dager hver måned. Utvalgsmedlemmenes samlede arbeid, inkludert nødvendige forberedelser innebærer opptil 20 prosent av en full stilling. Lederen har ytterligere ansvar som gjør at hun har opptil 30 prosent av en full stilling.

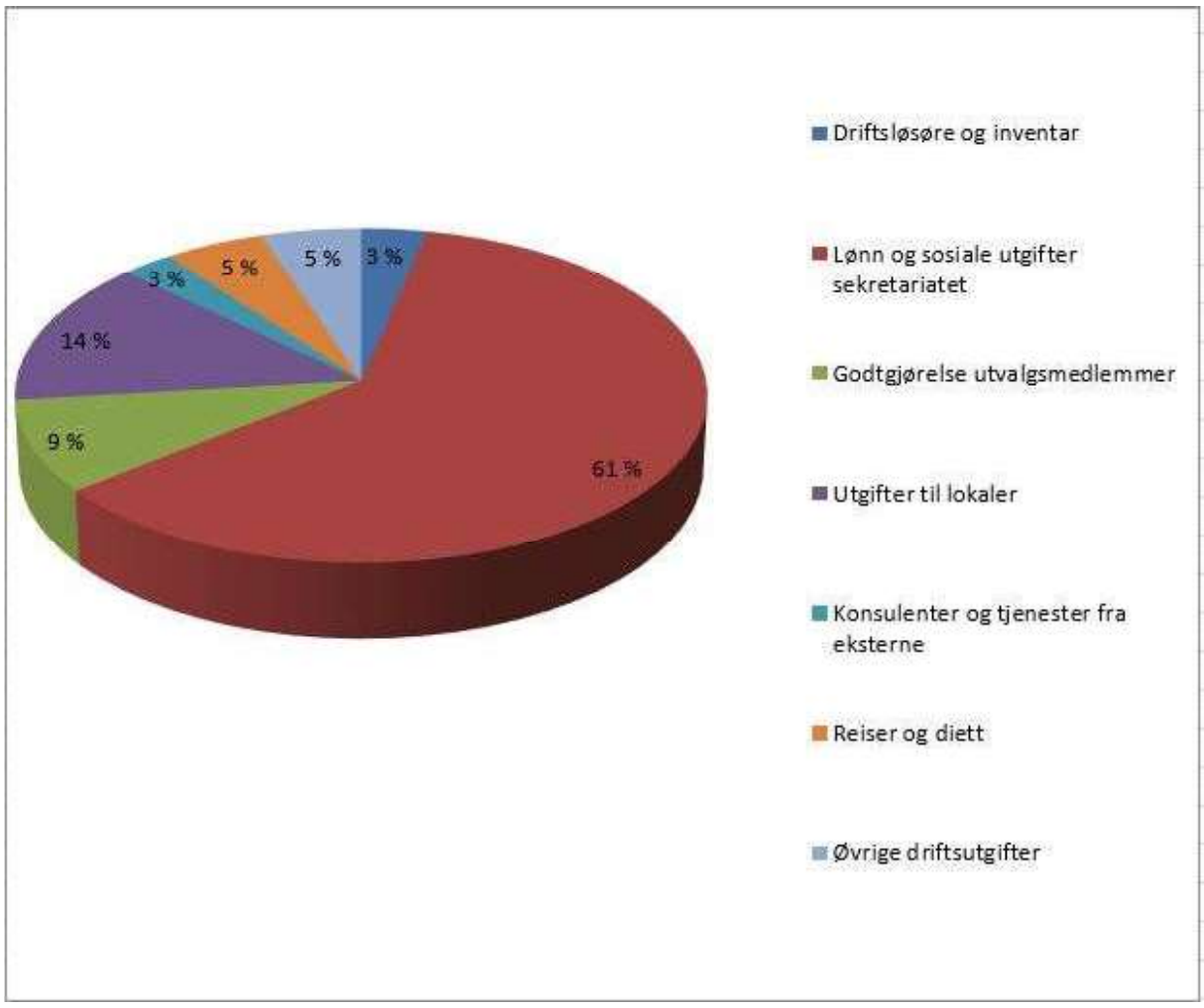
Tabell 1: Utvalgte nøkkeltall fra årsregnskapet 2016–2018

Nøkkeltall fra årsregnskapet 2016–2018	**2016**	**2017**	**2018**
Antall årsverk i sekretariatet	11	11	14
Antall medlemmer i utvalget	7	7	7
Samlet tildeling inkludert overførte midler	14 950 000	15 185 000	19 550 000
Samlet forbruk	14 764 958	13 632 788	18 951 911
Utnyttelsesgrad av samlet tildeling	99 %	90 %	97 %

Tabell 2: Utgifter etter art 2018 (se også figur 1)

Utgifter etter art 2017–2018	**2017**	**2018**
Driftsløsøre og inventar	163 301	633 084
Lønn og sosiale utgifter sekretariatet	8 297 609	11 546 607
Godtgjørelse utvalgsmedlemmer	1 610 641	1 688 371
Utgifter til lokaler	1 589 669	2 651 790
Konsulenter og tjenester fra eksterne	314 487	496 821
Reiser og diett	672 571	971 125
Øvrige driftsutgifter	984 510	964 114
SUM	**13 632 788**	**18 951 912**

Figur 1: Utgifter etter art 2018



DEL III. Årets aktiviteter og resultater

EOS-utvalgets samfunnsoppdrag er å føre en legalitetskontroll med EOS-tjenestene – det vil si å påse at de hemmelige tjenestene holder seg innenfor lover og regler.

Utvalgets kontrollvirksomhet utøves i hovedsak ved at utvalget gjennomfører anmeldte inspeksjoner i EOS-tjenestene. EOS-kontrolloven krever et minimum av 13 inspeksjoner per år, men utvalget kan ved behov gjennomføre flere inspeksjoner.[5]

Utvalget har i 2017 gjennomført 20 inspeksjoner; PST er inspisert 7 ganger, E-tjenesten 4 ganger, NSM 2 ganger og FSA 2 ganger. Etterretningsbataljonen, Nasjonal kommunikasjonsmyndighet, Forsvarets spesialkommando, Telia Norge AS og Felles cyberkoordineringssenter er inspisert en gang hver.

Utvalget har i 2018 gjennomført én inspeksjon på kort varsel. De ordinære inspeksjonene inneholder betydelige uanmeldte elementer. Utvalget kan i all hovedsak gjennomføre kontrollen direkte i tjenestens elektroniske systemer. Dette innebærer at hvilken informasjon som vil kontrolleres, ikke er kjent for tjenestene i forkant av eller under inspeksjonen. Tjenesten blir først oppmerksom på dette i etterkant av inspeksjonen når utvalget eventuelt retter skriftlige henvendelser til tjenesten om funn.

I 2018 undersøkte utvalget 22 saker av eget tiltak, mot 31 saker i 2017. Sakene som ble undersøkt i 2018 har generelt vært mer arbeidskrevende enn sakene i 2017. Sakene utvalget har undersøkt av eget tiltak er hovedsakelig funn fra utvalgets inspeksjoner.

Utvalget undersøker klager fra enkeltpersoner og organisasjoner. Det kom inn 19 klager til utvalget i 2018, mot 26 klager i 2017. Utvalget prioriterer klagesaksbehandlingen, og bruker en god del ressurser på den. Enkelte av klagene har vært rettet mot flere av EOS-tjenestene samtidig. Utvalget har på formelt grunnlag avvist noen klagesaker, blant annet under henvisning til at forholdet faller utenfor utvalgets kontrollområde. Klager og henvendelser som faller innenfor utvalgets kontrollområde undersøkes i den eller de tjenester klagen retter seg mot. Utvalget praktiserer generelt sett en lav terskel for å behandle klagesaker.

Utvalget mener at ressursbruken har vært effektiv i 2018, både med tanke på hva det er brukt ressurser på og hvordan disse er benyttet. Samlet sett er utvalget fornøyd med resultater, måloppnåelse og ressursbruk i 2018.

En nærmere redegjørelse for årets aktiviteter og resultater vil følge av utvalgets årsmelding for 2018, som overleveres til Stortinget 27. mars 2019.

Tabell 3: Antall inspeksjoner, eget tiltak-saker og klagesaker 2016–2018

	2016	2017	2018
Inspeksjoner	26	21	20
Eget tiltak-saker	51	31	22
Klagesaker	32	26	19

EOS-utvalget har i 2018 hatt kontakt med ulike eksterne miljøer. Dette inkluderer blant annet andre staters kontrollorganer, sivilsamfunnet, forsknings- og utdanningsmiljøer og nasjonale

[5] I juni 2017 ble EOS-kontrolloven endret slik at minimumskravet gikk fra 23 til 13 for å gi utvalget større fleksibilitet, jf. EOS-kontrolloven § 7.

kontrollinstanser. I 2018 publiserte også EOS-utvalget i samarbeid med kontrollorganer i Danmark, Nederland, Sveits og Belgia for første gang en felles uttalelse om styrking av internasjonalt kontrollsamarbeid

I september var utvalget på en studiereise i USA for å lære mer om kontrollsystemet der. Utvalget møtte blant annet representanter fra kontrollorganer, politiske miljøer, etterretningstjenester og sivilsamfunnet.

EOS-utvalget arrangerte for andre året på rad en årskonferanse om kontroll av hemmelige tjenester i 2018 i forbindelse med overleveringen av årsmeldingen til Stortinget. Årskonferansen var åpen for publikum. Årskonferansen for 2019 arrangeres 28. mars.

DEL IV. Styring og kontroll i virksomheten

Utvalgets virksomhet reguleres i EOS-kontrolloven. Videre kan det gis føringer fra Kontroll- og konstitusjonskomiteen i dens innstillinger om utvalgets meldinger til Stortinget, samt fra stortingsbehandlingen av meldingene. Stortinget kan også ved plenarvedtak (stortingsvedtak) pålegge utvalget å foreta nærmere definerte undersøkelser innenfor utvalgets kontrollmandat, og under iakttakelse av de regler og innen de rammer som for øvrig ligger til grunn for utvalgets virksomhet.[6]

Utvalget er som øvrige statlige virksomheter underlagt kontroll av Riksrevisjonen. Riksrevisjonen har ikke hatt merknader som har krevd oppfølging fra utvalget i 2018.

Utvalget har flere instruksdokumenter som regulerer driften i utvalget og sekretariatet. Det foreligger blant annet strenge sikkerhetsrutiner, noe som særlig har bakgrunn i utvalgets håndtering av sikkerhetsgradert informasjon. De ansatte er godt kjent med interne retningslinjer og instrukser.

IA-avtalen har høy oppmerksomhet i sekretariatet. Sykefraværet[7] i sekretariatet har vært på 5,2 prosent i 2018. I 2017 var tallet 5,6 prosent.

[6] Jf. EOS-kontrolloven § 1 femte ledd.
[7] Egenmeldinger og sykmeldinger.

DEL V. Vurdering av fremtidsutsikter

Den teknologiske utviklingen innenfor kontrollområdet til EOS-utvalget skjer veldig raskt. Utvalget har allerede tre ansatte teknologer og håper å få midler i 2020 til ytterligere to stillinger i den nye teknologiske enheten. I forbindelse med ny lov om Etterretningstjenesten som nå er på høring fra Forsvarsdepartementet kan det være at sekretariatet vil få behov for enda flere ansatte, både juridisk og især teknologisk kompetanse.

Utvalget er også opptatt av å bli mer synlige og å være tilgjengelig for intervjuer og foredrag for dem som ønsker det – gitt at det kan gjøres i tråd med taushetsplikten.

DEL VI. Årsregnskap

Ledelseskommentarer til årsregnskapet for 2018

Formål

EOS-utvalget kontrollerer EOS-tjenestene på vegne av Stortinget, men er uavhengig i sitt løpende arbeid. Utvalget fører regnskap i henhold til kontantprinsippet, slik det fremgår av prinsippnoten til årsregnskapet.

Bekreftelse

Årsregnskapet er avlagt i henhold til bestemmelser om økonomistyring i staten kapittel 2.3.3, jf. Finansdepartementets rundskriv R-115 datert 24. november 2016. Jeg mener regnskapet gir et dekkende bilde av utvalgets disponible bevilgninger og regnskapsførte utgifter.

Vurderinger av vesentlige forhold

Regnskapstallene for 2018 viser et forbruk på kr 18 951 911. Det innebærer et overskudd på kr 598 089 sammenlignet med budsjettet for 2018, som var på kr 19 550 000, inkludert overføring på kr 750 000 fra 2017. Det er anmodet om å få overført kr 598 000 til budsjettet for 2019.

Utbetalinger til lønn, godtgjørelse og sosiale utgifter til utvalgsmedlemmene og ansatte i sekretariatet beløp seg til kr 13 234 978, mot kr 9 908 250 i 2017. Utgifter til lønn og godtgjørelse utgjorde 69,8 prosent av driftsutgiftene for 2018.

Mellomværende med statskassen utgjorde per 31. desember 2018 kr 625 704.

Tilleggsopplysninger

Riksrevisjonen er ekstern revisor og bekrefter årsregnskapet for utvalget. Årsregnskapet er ikke ferdig revidert per d.d., men revisjonsberetningen antas å foreligge i løpet av andre kvartal 2019.

Oslo, 12. februar 2019

Eldbjørg Løwer

utvalgsleder

Prinsippnote årsregnskapet

Årsregnskap for EOS-utvalget er utarbeidet og avlagt etter nærmere retningslinjer fastsatt i bestemmelser om økonomistyring i staten («bestemmelsene»), fastsatt 12. desember 2003. Årsregnskapet er i henhold til krav i bestemmelsene punkt 3.4.1, nærmere bestemmelser i Finansdepartementets rundskriv R-115 fra 24. november 2016 og eventuelle tilleggskrav fastsatt av Stortinget.

Oppstillingen av bevilgningsrapporteringen omfatter en øvre del med bevilgningsrapporteringen og en nedre del som viser beholdninger virksomheten står oppført med i kapitalregnskapet.

Oppstillingen av artskontorapporeringen har en øvre del som viser hva som er rapportert til statsregnskapet etter standard kontoplan for statlige virksomheter og en nedre del som viser grupper av kontoer som inngår i mellomværende med statskassen.

Oppstillingen av bevilgningsrapporteringen og artskontorapporteringen er utarbeidet med utgangspunkt i bestemmelsene punkt 3.4.2 – de grunnleggende prinsippene for årsregnskapet:

a) Regnskapet følger kalenderåret
b) Regnskapet inneholder alle rapporterte utgifter og inntekter for regnskapsåret
c) Utgifter og inntekter er ført i regnskapet med brutto beløp
d) Regnskapet er utarbeidet i tråd med kontantprinsippet

Oppstillingene av bevilgnings- og artskontorapportering er utarbeidet etter de samme prinsippene, men gruppert etter ulike kontoplaner. Prinsippene korresponderer med krav i bestemmelsene punkt 3.5 til hvordan virksomhetene skal rapportere til statsregnskapet. Sumlinjen «Netto rapportert til bevilgningsregnskapet» er lik i begge oppstillingene.

Alle statlige virksomheter er tilknyttet statens konsernkontoordning i Norges Bank i henhold til krav i bestemmelsene punkt 3.8.1. Ordinære forvaltningsorgan (bruttobudsjetterte virksomheter) tilføres ikke likviditet gjennom året. Ved årets slutt nullstilles saldoen på den enkelte oppgjørskonto ved overgang til nytt år.

Bevilgningsrapporteringen

Bevilgningsrapporteringen viser regnskapstall som utvalget har rapportert til statsregnskapet. Det stilles opp etter de kapitler og poster i bevilgningsregnskapet som utvalget har fullmakt til å disponere. Oppstillingen viser alle finansielle eiendeler og forpliktelser utvalget står oppført med i

Statens kapitalregnskap. Kolonnen samlet tildeling viser hva virksomheten har fått stilt til disposisjon i tildelingsbrev for hver kombinasjon av kapittel/post.

Artskontorapporteringen

Artskontorapporteringen viser regnskapstall utvalget har rapportert til statsregnskapet etter standard kontoplan for statlige virksomheter. Utvalget har en trekkrettighet for disponible tildelinger på konsernkonto i Norges Bank. Tildelingene skal ikke inntektsføres og vises derfor ikke som inntekt i oppstillingen.

Note 8 til artskontorapporteringen viser forskjeller mellom avregning med statskassen og mellomværende med statskassen.

Virksomhet: **FZ - EOS-utvalget** Rapport kjørt: 01.02.2019

Oppstilling av bevilgningsrapportering 31.12.2018

Utgiftskapittel	Kapittelnavn	Post	Posttekst	Note	Samlet tildeling*	Regnskap 2018	Merutgift (-) og mindreutgift
0044	Driftsutgifter	01			19 550 000	18 951 911	598 089
1633	Nettoordning for mva i staten	01			0	666 903	
Sum utgiftsført					19 550 000	19 618 813	

Inntektskapittel	Kapittelnavn	Post	Posttekst	Samlet tildeling*	Regnskap 2018	Merinntekt og mindreinntekt(-)
5309	Tilfeldige inntekter	29		0	15 766	
5700	Arbeidsgiveravgift	72		0	1 624 120	
Sum inntektsført				0	1 639 886	
Netto rapportert til bevilgningsregnskapet					**17 978 927**	
Kapitalkontoer						
60092001	Norges Bank KK /innbetalinger				315 295	
60092002	Norges Bank KK/utbetalinger				-18 158 780	
700060	Endring i mellomværende med statskassen				-135 442	
Sum rapportert					0	

Beholdninger rapportert til kapitalregnskapet (31.12)				
		31.12.2018	**31.12.2017**	**Endring**
700060	Mellomværende med statskassen	-625 704	-490 262	-135 442

* Samlet tildeling skal ikke reduseres med eventuelle avgitte belastningsfullmakter. Se note B for nærmere forklaring.

Virksomhet: **FZ - EOS-utvalget**

Note A Forklaring av samlet tildeling utgifter			
Kapittel og post	**Overført fra i fjor**	**Årets tildelinger**	**Samlet tildeling**
530 929	750 000		750 000
4 401		18 800 000	18 800 000

Note B Forklaring til brukte fullmakter og beregning av mulig overførbart beløp til neste år

Kapittel og post	Stikkord	Merutgift(-)/ mindre utgift	Utgiftsført av andre iht. avgitte belastnings-fullmakter(-)	Merutgift(-)/ mindreutgift etter avgitte belastnings-fullmakter	Merinntekter / mindreinntekter(-) iht. merinntektsfullmakt	Omdisponering fra post 01 til 45 eller til post 01/21 fra neste års bevilgning	Innsparinger(-)	Sum grunnlag for overføring	Maks. overførbart beløp *	Mulig overførbart beløp beregnet av virksomheten
4 401	Driftsutgifter	598 089		598 089				598 089	598 000	598 000

*Maksimalt beløp som kan overføres er 5% av årets bevilgning på driftspostene 01-29, unntatt post 24 eller sum av de siste to års bevilgning for poster med stikkordet "kan overføres". Se årlig rundskriv R-2 for mer detaljert informasjon om overføring av ubrukte bevilgninger.

Forklaring til bruk av budsjettfullmakter

Mulig overførbart beløp
EOS-utvalgets ubrukte bevilgning på kapittel/post 004401 beløper seg til kr 598 000. Dette beløpet er mindre enn grensen på 5 %, og kr 598 000 kan overføres til neste budsjettår. EOS-utvalget har søkt om overføring av kr 598 000 til budsjettet for 2019.

Overføringen til 2019 er nødvendig for å dekke merkostnader i forbindelse med flytting til nye lokaler på Bryn for EOS-utvalget.

Virksomhet: FZ - EOS-utvalget

Oppstilling av artskontorapporteringen 31.12.2018

	Note	2018	2017
Driftsinntekter rapportert til bevilgningsregnskapet			
Innbetalinger fra gebyrer	1	0	0
Innbetalinger fra tilskudd og overføringer	1	0	0
Salgs- og leieinnbetalinger	1	0	0
Andre innbetalinger	1	0	0
Sum innbetalinger fra drift		0	0
Driftsutgifter rapportert til bevilgningsregnskapet			
Utbetalinger til lønn	2	13 234 977	9 908 250
Andre utbetalinger til drift	3	5 152 962	3 656 158
Sum utbetalinger til drift		18 387 939	13 564 408
Netto rapporterte driftsutgifter		**18 387 939**	**13 564 408**
Investerings- og finansinntekter rapportert til bevilgningsregnskapet			
Innbetaling av finansinntekter	4	0	0
Sum investerings- og finansinntekter		0	0
Investerings- og finansutgifter rapportert til bevilgningsregnskapet			
Utbetaling til investeringer	5	563 972	68 380
Utbetaling til kjøp av aksjer	5,8B	0	0
Utbetaling av finansutgifter	4	0	0
Sum investerings- og finansutgifter		563 972	68 380
Netto rapporterte investerings- og finansutgifter		**563 972**	**68 380**
Innkrevingsvirksomhet og andre overføringer til staten			
Innbetaling av skatter, avgifter, gebyrer m.m.	6	0	0
Sum innkrevingsvirksomhet og andre overføringer til staten		0	0
Tilskuddsforvaltning og andre overføringer fra staten			
Utbetalinger av tilskudd og stønader	7	0	0
Sum tilskuddsforvaltning og andre overføringer fra staten		0	0
Inntekter og utgifter rapportert på felleskapitler *			
Gruppelivsforsikring konto 1985 (ref. kap. 5309, inntekt)		15 766	14 480
Arbeidsgiveravgift konto 1986 (ref. kap. 5700, inntekt)		1 624 120	1 214 585
Nettoføringsordning for merverdiavgift konto 1987 (ref. kap. 1633, utgift)		666 903	369 739
Netto rapporterte utgifter på felleskapitler		-972 984	-859 326
Netto rapportert til bevilgningsregnskapet		**17 978 927**	**12 773 463**

Oversikt over mellomværende med statskassen **

Eiendeler og gjeld		**2018**	**2017**
Fordringer		0	0
Kasse		0	0
Bankkontoer med statlige midler utenfor Norges Bank		0	0
Skyldig skattetrekk		-625 704	-490 423
Skyldige offentlige avgifter		0	0
Annen gjeld		0	161
Sum mellomværende med statskassen	8	-625 704	-490 262

* Andre ev. inntekter/utgifter rapportert på felleskapitler spesifiseres på egne linjer ved behov.

** Spesifiser og legg til linjer ved behov.

Kontrollsum:
17 978 927
17 978 927
0

Virksomhet: FZ - EOS-utvalget

KONTI:

Note 1 Innbetalinger fra drift

	31.12.2018	31.12.2017
Innbetalinger fra gebyrer		
Sum innbetalinger fra gebyrer	**0**	**0**
Innbetalinger fra tilskudd og overføringer		
Sum innbetalinger fra tilskudd og overføringer	**0**	**0**
Salgs- og leieinnbetalinger		
Sum salgs- og leieinnbetalinger	**0**	**0**
Andre innbetalinger		
Sum andre innbetalinger	**0**	**0**
Sum innbetalinger fra drift	**0**	**0**

Virksomhet: FZ - EOS-utvalget

Note 2 Utbetalinger til lønn

	31.12.2018	31.12.2017
Lønn	8 887 729	7 452 940
Arbeidsgiveravgift	1 624 120	1 214 585
Pensjonsutgifter*	1 003 785	0
Sykepenger og andre refusjoner (-)	-276 458	-776 831
Andre ytelser	1 995 800	2 017 557
Sum utbetalinger til lønn	**13 234 977**	**9 908 250**
Antall årsverk:	14	11

*** Nærmere om pensjonskostnader**
Pensjoner kostnadsføres i resultatregnskapet basert på faktisk påløpt premie for regnskapsåret. Premiesats for 2018 er 12 prosent. Premiesatsen for 2017 var 0 prosent.

Virksomhet: FZ - EOS-utvalget

Note 3 Andre utbetalinger til drift

	31.12.2018	31.12.2017
Husleie	1 355 491	1 404 420
Vedlikehold egne bygg og anlegg	0	0
Vedlikehold og ombygging av leide lokaler	0	0
Andre utgifter til drift av eiendom og lokaler	1 296 299	185 249
Reparasjon og vedlikehold av maskiner, utstyr mv.	0	0
Mindre utstyrsanskaffelser	147 526	124 030
Leie av maskiner, inventar og lignende	210 674	151 288
Kjøp av fremmede tjenester	286 147	314 487
Reiser og diett	971 125	672 571
Øvrige driftsutgifter	885 699	804 114
Sum andre utbetalinger til drift	**5 152 962**	**3 656 158**

Virksomhet: FZ - EOS-utvalget

Note 4 Finansinntekter og finansutgifter

	31.12.2018	31.12.2017
Innbetaling av finansinntekter		
Renteinntekter	0	0
Valutagevinst	0	0
Annen finansinntekt	0	0
Sum innbetaling av finansinntekter	**0**	**0**

	31.12.2018	31.12.2017
Utbetaling av finansutgifter		
Renteutgifter	0	0
Valutatap	0	0
Annen finansutgift	0	0
Sum utbetaling av finansutgifter	**0**	**0**

Virksomhet: FZ - EOS-utvalget

Note 5 Utbetaling til investeringer og kjøp av aksjer

	31.12.2018	31.12.2017
Utbetaling til investeringer		
Immaterielle eiendeler og lignende	0	0
Tomter, bygninger og annen fast eiendom	0	0
Beredskapsanskaffelser	0	0
Infrastruktureiendeler	0	0
Maskiner og transportmidler	0	0
Driftsløsøre, inventar, verktøy og lignende	563 972	68 380
Sum utbetaling til investeringer	**563 972**	**68 380**

	31.12.2018	31.12.2017
Utbetaling til kjøp av aksjer		
Kapitalinnskudd	0	0
Obligasjoner	0	0
Investeringer i aksjer og andeler	0	0
Sum utbetaling til kjøp av aksjer	**0**	**0**

Virksomhet: FZ - EOS-utvalget

Note 6 Innkrevingsvirksomhet og andre overføringer til staten

	31.12.2018	31.12.2017
Sum innkrevingsvirksomhet og andre overføringer til staten	0	0

Virksomhet: FZ - EOS-utvalget

Note 7 Tilskuddsforvaltning og andre overføringer fra staten

	31.12.2018	31.12.2017
Sum tilskuddsforvaltning og andre overføringer fra staten	**0**	**0**

Virksomhet: FZ - EOS-utvalget **Rapport kjørt:** 01.02.2019

Note 8 Sammenheng mellom avregning med statskassen og mellomværende med statskassen.

Del A Forskjellen mellom avregning med statskassen og mellomværende med statskassen

		31.12.2018 Spesifisering av bokført avregning med statskassen	31.12.2018 Spesifisering av rapportert mellomværende med statskassen	Forskjell
Finansielle anleggsmidler				
	Investeringer i aksjer og andeler*	0	0	0
	Obligasjoner	0	0	0
	Sum	**0**	**0**	**0**
Omløpsmidler				
	Kundefordringer	0	0	0
	Andre fordringer	0	0	0
	Bankinnskudd, kontanter og lignende	0	0	0
	Sum	**0**	**0**	**0**
Langsiktig gjeld				
	Annen langsiktig gjeld	0	0	0
	Sum	**0**	**0**	**0**
Kortsiktig gjeld				
	Leverandørgjeld	-402 603	0	-402 603
	Skyldig skattetrekk	-625 704	-625 704	0
	Skyldige offentlige avgifter	0	0	0
	Annen kortsiktig gjeld	0	0	0
	Sum	**-1 028 307**	**-625 704**	**-402 603**
Sum		**-1 028 307**	**-625 704**	**-402 603**

* Virksomheter som eier finansielle anleggsmidler i form av investeringer i aksjer og selskapsandeler fyller også ut note 8 B

Del B Spesifisering av investeringer i aksjer og selskapsandeler

	Ervervsdato	Antall aksjer	Eierandel	Stemmeandel	Årets resultat i selskapet	Balansefort egenkapital i selskapet	Balanseført verdi i regnskap*
Aksjer							
Selskap 1							
Selskap 2							
Selskap 3							
Balanseført verdi 31.12.2018							**0**

* Investeringer i aksjer er bokført til anskaffelseskost. Balanseført verdi er den samme i både virksomhetens kontospesifikasjon og kapitalregnskapet.

Riksrevisjonen

Vår referanse 2018/00864-24

STORTINGETS KONTROLLUTVALG FOR
ETTERRETNINGS-, OVERVÅKINGS- OG
SIKKERHETSTJENESTE, EOS-UTVALGET
Org. nr.: 982110777

Riksrevisjonens beretning

Til STORTINGETS KONTROLLUTVALG FOR ETTERRETNINGS-, OVERVÅKINGS- OG SIKKERHETSTJENESTE, EOS-UTVALGET

Uttalelse om revisjonen av årsregnskapet

Konklusjon

Riksrevisjonen har revidert Stortingets kontrollutvalg for etterretnings-, overvåknings- og sikkerhetstjeneste, EOS-Utvalgets årsregnskap for 2018. Årsregnskapet består av ledelseskommentarer og oppstilling av bevilgnings- og artskontorapportering, inklusiv noter til årsregnskapet for regnskapsåret avsluttet per 31. desember 2018.

Bevilgnings- og artskontorapporteringen viser at 17 978 927 kroner er rapportert netto til bevilgningsregnskapet.

Etter Riksrevisjonens mening gir Stortingets kontrollutvalg for etterretnings-, overvåknings- og sikkerhetstjeneste, EOS-Utvalgets årsregnskap et dekkende bilde av virksomhetens disponible bevilgninger, inntekter og utgifter i 2018 og mellomværende med statskassen per 31. desember 2018, i samsvar med regelverket for økonomistyring i staten.

Grunnlag for konklusjonen

Vi har gjennomført revisjonen i samsvar med *lov om Riksrevisjonen*, *instruks om Riksrevisjonens virksomhet* og internasjonale standarder for offentlig revisjon (ISSAI 1000–2999). Våre oppgaver og plikter i henhold til disse standardene er beskrevet under «Revisors oppgaver og plikter ved revisjonen av årsregnskapet». Vi er uavhengige av virksomheten slik det kreves i lov og instruks om Riksrevisjonen og de etiske kravene i ISSAI 30 fra International Organization of Supreme Audit Institutions (INTOSAIs etikkregler), og vi har overholdt de øvrige etiske forpliktelsene våre i samsvar med disse kravene og INTOSAIs etikkregler. Etter vår oppfatning er revisjonsbevisene vi har innhentet tilstrekkelige og hensiktsmessige som grunnlag for vår konklusjon.

Øvrig informasjon i årsrapporten

Ledelsen er ansvarlig for årsrapporten, som består av årsregnskapet (del VI) og øvrig informasjon (del I–V). Riksrevisjonens uttalelse omfatter revisjon av årsregnskapet og virksomhetens etterlevelse av administrative regelverk for økonomistyring, ikke øvrig informasjon i årsrapporten (del I–V). Vi attesterer ikke den øvrige informasjonen.

I forbindelse med revisjonen av årsregnskapet er det vår oppgave å lese den øvrige informasjonen i årsrapporten. Formålet er å vurdere om det foreligger vesentlig inkonsistens mellom den øvrige informasjonen, årsregnskapet og kunnskapen vi har opparbeidet oss under revisjonen. Vi vurderer også om den øvrige informasjonen ser ut til å inneholde vesentlig feilinformasjon. Dersom vi konkluderer med at den

øvrige informasjonen inneholder vesentlig feilinformasjon, er vi pålagt å rapportere dette i revisjonsberetningen.

Det er ingenting å rapportere i så måte.

Ledelsens ansvar for årsregnskapet

Ledelsen er ansvarlig for å utarbeide et årsregnskap som gir et dekkende bilde i samsvar med regelverket for økonomistyring i staten. Ledelsen er også ansvarlig for å etablere den interne kontrollen som den mener er nødvendig for å kunne utarbeide et årsregnskap som ikke inneholder vesentlig feilinformasjon, verken som følge av misligheter eller utilsiktede feil.

Riksrevisjonens oppgaver og plikter ved revisjonen av årsregnskapet

Målet med revisjonen er å oppnå betryggende sikkerhet for at årsregnskapet som helhet ikke inneholder vesentlig feilinformasjon, verken som følge av misligheter eller utilsiktede feil, og å avgi en revisjonsberetning som gir uttrykk for Riksrevisjonens konklusjon. Betryggende sikkerhet er et høyt sikkerhetsnivå, men det er ingen garanti for at en revisjon som er utført i samsvar med *lov om Riksrevisjonen, instruks om Riksrevisjonens virksomhet* og internasjonale standarder for offentlig revisjon (ISSAI 1000–2999), alltid vil avdekke vesentlig feilinformasjon som eksisterer. Feilinformasjon kan oppstå som følge av misligheter eller utilsiktede feil. Feilinformasjon blir ansett som vesentlig dersom den, enkeltvis eller samlet, med rimelighet kan forventes å påvirke de beslutningene brukere treffer på grunnlag av årsregnskapet.

Vi utøver profesjonelt skjønn og utviser profesjonell skepsis gjennom hele revisjonen, i samsvar med *lov om Riksrevisjonen, instruks om Riksrevisjonens virksomhet* og ISSAI 1000–2999.

Vi identifiserer og anslår risikoene for vesentlig feilinformasjon i årsregnskapet, enten den skyldes misligheter eller utilsiktede feil. Videre utformer og gjennomfører vi revisjonshandlinger for å håndtere slike risikoer og innhenter tilstrekkelig og hensiktsmessig revisjonsbevis som grunnlag for vår konklusjon. Risikoen for at vesentlig feilinformasjon ikke blir avdekket, er høyere for feilinformasjon som skyldes misligheter, enn for feilinformasjon som skyldes utilsiktede feil. Grunnen til det er at misligheter kan innebære samarbeid, forfalskning, bevisste utelatelser, feilpresentasjoner eller overstyring av intern kontroll.

Vi gjør også følgende:

- opparbeider oss en forståelse av den interne kontrollen som er relevant for revisjonen, for å utforme revisjonshandlinger som er hensiktsmessige ut fra omstendighetene, men ikke for å gi uttrykk for en mening om hvor effektiv virksomhetens interne kontroll er
- evaluerer om regnskapsprinsippene som er brukt, er hensiktsmessige, og om tilhørende opplysninger som er utarbeidet av ledelsen, er rimelige
- evaluerer den totale presentasjonen, strukturen og innholdet i årsregnskapet, inkludert tilleggsopplysningene
- evaluerer om årsregnskapet representerer de underliggende transaksjonene og hendelsene på en måte som gir et dekkende bilde i samsvar med regelverket for økonomistyring i staten

Vi kommuniserer med ledelsen og informerer det overordnede departementet, blant annet om det planlagte omfanget av revisjonen og når revisjonsarbeidet skal utføres. Vi vil også ta opp forhold av betydning som er avdekket i løpet av revisjonen, for eksempel svakheter av betydning i den interne kontrollen.

Når det gjelder forholdene som vi tar opp med ledelsen, tar vi standpunkt til hvilke som er av størst betydning ved revisjonen av årsregnskapet, og avgjør om disse skal regnes som sentrale forhold ved revisjonen. De beskrives i så fall i et eget avsnitt i revisjonsberetningen, med mindre lov eller forskrift hindrer offentliggjøring. Forholdene omtales ikke i beretningen hvis Riksrevisjonen beslutter at det er rimelig å forvente at de negative konsekvensene av en slik offentliggjøring vil være større enn offentlighetens interesse av at saken blir omtalt. Dette vil bare være aktuelt i ytterst sjeldne tilfeller.

Dersom vi gjennom revisjonen av årsregnskapet får indikasjoner på vesentlige brudd på administrative regelverk med betydning for økonomistyring i staten, gjennomfører vi utvalgte revisjonshandlinger for å kunne uttale oss om hvorvidt det er vesentlige brudd på slike regelverk.

Uttalelse om øvrige forhold

Konklusjon knyttet til administrative regelverk for økonomistyring

Vi uttaler oss om hvorvidt vi er kjent med forhold som tilsier at virksomheten har disponert bevilgningene på en måte som i vesentlig grad strider mot administrative regelverk med betydning for økonomistyring i staten. Uttalelsen gis med moderat sikkerhet og bygger på ISSAI 4000-serien for etterlevelsesrevisjon. Moderat sikkerhet for uttalelsen oppnår vi gjennom revisjon av årsregnskapet som beskrevet ovenfor, og kontrollhandlinger vi finner nødvendige.

Basert på revisjonen av årsregnskapet og kontrollhandlinger vi har funnet nødvendige i henhold til ISSAI 4000-serien, er vi ikke kjent med forhold som tilsier at virksomheten har disponert bevilgningene i strid med administrative regelverk med betydning for økonomistyring i staten.

Oslo; 29.04.2019

Etter fullmakt

Tora Struve Jarlsby
ekspedisjonssjef

Ola Hollum
avdelingsdirektør

Brevet er ekspedert digitalt og har derfor ingen håndskreven signatur