FD
FORSVARSDEPARTEMENTET

Høringsnotat

Forslag til ny lov om Etterretningstjenesten

12. november 2018

Forslag til ny lov om Etterretnings-tjenesten

1 Bakgrunn

1.1 Hovedhensynene bak lovrevisjonen

Lov om Etterretningstjenesten («etterretningstjenesteloven») ble vedtatt i 1998.[1] Utviklingen i trusselbildet, styrkingen av menneskerettighetenes stilling i norsk rett og digitaliseringen av samfunnet har siden den gang endret forutsetningene for vår utenlandsetterretningstjeneste. Som en konsekvens av dette mener Forsvarsdepartementet at tiden er moden for en gjennomgåelse av rettsgrunnlaget for Etterretningstjenesten.

Formålet med en slik gjennomgåelse er å vurdere om regelverket i dag gir det nødvendige rettslige grunnlaget for de oppgaver Etterretningstjenesten er satt til å utføre. Videre mener departementet det er behov for å vurdere hvordan rettsgrunnlaget bør oppdateres og moderniseres i tråd med rettsutviklingen vi har sett de senere år, særlig på menneskerettighets- og personvernområdet. Lovrevisjonen vil ikke ha til hensikt å endre eller begrense Etterretningstjenestens oppgaver eller samfunnsoppdrag, men snarere å sørge for at disse har en sikker rettslig forankring.

1.2 Nærmere om EOS-utvalgets særskilte melding. Anmodningsvedtak

EOS-utvalget avga 17. juni 2016 en særskilt melding til Stortinget om rettsgrunnlaget for Etterretningstjenestens overvåkingsvirksomhet.[2] EOS-utvalget stiller i meldingen spørsmål ved om rettsgrunnlaget for Etterretningstjenesten er tilstrekkelig oppdatert, og påpeker et mulig behov for lovendringer for å sikre at tjenesten har hjemmelsgrunnlag for den aktivitet den utøver. Kontroll- og konstitusjonskomiteen avga 31. januar 2017 sin innstilling i saken til Stortinget.[3] Komiteen påpekte at regelverket for Etterretningstjenestens virksomhet må legge til rette for tjenestens mulighet til effektiv oppgaveløsning og ivaretakelse av sikkerhetshensyn. Komiteen uttalte videre at det er viktig at tjenestens hjemler for inngrep er tilstrekkelig klare for å kunne fastslå om tjenesten utfører virksomheten i tråd med lovgivers vilje. Videre fremhevet komiteen at det er viktig både for tilliten til tjenesten, og for faktisk og opplevd trygghet for landet og borgerne, at virkemidler som er forholdsmessige og nødvendige for å utføre tjenestens oppdrag, beskrives gjennom et lovverk som stemmer overens med de utfordringer vi står overfor. Komiteen var derfor av den oppfatning at det i stedet for å justere enkeltbestemmelser i etterretningstjenesteloven var mer formålstjenlig at regjeringen, med bakgrunn i de perspektiver som trekkes opp av EOS-utvalget i den særskilte meldingen og fra Etterretningstjenesten selv, la frem forslag til en revidert

[1] Lov av 20. mars 1998 nr. 11 om Etterretningstjenesten (etterretningstjenesteloven)

[2] Dokument 7:2 (2015–2016)

[3] Innst. 164 S (2016–2017)

etterretningstjenestelov for Stortinget, med vurderinger av EOS-utvalgets mulighet for kontroll.

Stortinget fattet 21. februar 2017 følgende anmodningsvedtak basert på komiteens innstilling:

> «Stortinget ber regjeringen legge frem forslag til en revidert lov om Etterretningstjenesten.»

Uttalelsene fra kontroll- og konstitusjonskomiteen og tilhørende anmodningsvedtak samsvarer godt med departementets vurdering av behovet for en lovrevisjon som beskrevet i punkt 1.1 over.

1.3 Hovedpunkter i lovforslaget

1.3.1 Generelt

Formålet med lovforslaget er å gi Etterretningstjenestens virksomhet trygg rettslig forankring, særlig med hensyn til rettsutviklingen innen menneskerettigheter og personvern. Lovforslaget er utarbeidet for å regulere Etterretningstjenestens informasjonsinnhentingsvirksomhet – altså den tradisjonelle etterretningsvirksomheten – ikke annen virksomhet som tjenesten utøver som en del av Forsvaret eller tjenestens administrative virksomhet.

Lovforslaget kodifiserer i stor utstrekning gjeldende regelverk og praksis, men det foreslås også noen nyvinninger. Etterretningstjenestens metodebruk foreslås lovfestet. Det foreslås også regler om behandling av personopplysninger som er tilpasset tjenestens virksomhet, regler for deling av informasjon og flere andre saksbehandlingsregler. Det foreslås også å gi Etterretningstjenesten tilrettelagt tilgang til grenseoverskridende elektronisk kommunikasjon («tilrettelagt innhenting»), se nærmere punkt 1.3.3.

Regler om organisering, styring og kontroll av Etterretningstjenesten er inntatt i lovforslaget kapittel 2. Dette reguleres i dag delvis av lov, delvis av instruks. Departementet foreslår at instruks 31. august 2001 nr. 1012 om Etterretningstjenesten (E-instruksen) oppheves når den nye loven trer i kraft. Flere bestemmelser fra instruksen foreslås videreført i ny lov. Lovforslaget kapittel 2 viderefører dagens innretning med Etterretningstjenesten som Norges nasjonale utenlandsetterretningstjeneste, med både sivile og militære oppdragsgivere. Det foreslås også at Etterretningstjenesten fortsatt skal være en del av Forsvaret og underlagt forsvarssjefens kommando. Samtidig er det forhold ved tjenestens oppgaver som begrunner særlige former for styring og kontroll som ikke gjelder ellers i Forsvaret. Bestemmelser knyttet til oppdragsstyring og rapportering foreslås lovfestet. De ulike former for kontroll med Etterretningstjenesten foreslås inntatt i loven. Forslaget til lovregulering innebærer en videreføring av gjeldende praksis.

1.3.2 Samfunnsoppdrag – hjemler for innhenting og metodebruk

Etterretningstjenestens lovpålagte oppgaver følger i dag av etterretningstjenesteloven § 3, og kan grovt sett kategoriseres i tre grupper:

1. Varsle om ytre trusler mot Norge og norske interesser
2. Gi etterretningsstøtte til Forsvarets operasjoner hjemme og ute i verden

3. Understøtte viktige politiske beslutningsprosesser med relevant informasjon om fokusområder for norsk utenriks-, sikkerhets- og forsvarspolitikk

Departementet mener dette fremdeles bør være Etterretningstjenestens samfunnsoppdrag, men foreslår en mer strukturert inndeling av oppgavene i utkast til ny lov. Oppgavene, formulert som innhentingshjemler, fremgår av lovforslaget kapittel 3. Departementet foreslår at tjenestens oppgaver reguleres uttømmende i loven, noe som vil avhjelpe kritikken mot at dagens regelverk har en uklar formålsavgrensning.

Varslingsoppdraget beskrevet i punkt 1, gjerne omtalt som *strategisk varsling*, vil av mange kategoriseres som Etterretningstjenestens viktigste oppgave. Oppgaven gir imidlertid ikke i seg selv hjemmel til å innhente informasjon – varsling forutsetter at man allerede har informasjon å varsle om. Departementet vurderer derfor at varslingsoppdraget passer best i lovens kapittel 2, mens hjemmelen for *innhentingen* av informasjon om utenlandske trusler følger av kapittel 3.

Lovforslaget legger opp til at informasjonsinnhenting med etterretningsformål først kan finne sted når grunnvilkårene i kapittel 5 er oppfylt. Her sondres det mellom de to hovedformene for informasjonsinnhenting, nemlig *målsøking* og *målrettet innhenting*. Utkastet til § 5-4 pålegger en forholdsmessighetsvurdering i henhold til menneskerettighetenes krav, og er dermed en sentral bestemmelse.

Innhentingshjemmelen i dagens lov er teknologi- og metodenøytral, og omtaler ikke hvilke metoder for innhenting som Etterretningstjenesten kan ta i bruk for å tilegne seg informasjon. Lovkravet i menneskerettighetene innebærer at metoder som gjør inngrep i rettighetene må være forankret i tilgjengelig og forutsigbar lovgivning. Som følge av at mye av aktiviteten pågår fordekt, bør dessuten reglene utformes på en måte som legger til rette for kontroll. Departementet foreslår at metodebruk som kan innebære inngrep i menneskerettighetene reguleres i kapittel 6. Dette gjelder både fordekt innhenting og innhenting gjennom åpne kilder, og både tekniske og menneskebaserte innhentingsdisipliner. I tillegg foreslås det særskilte personell- og prosedyrebestemmelser.

Departementet foreslår å videreføre hovedregelen om at Etterretningstjenesten ikke kan innhente informasjon om personer og virksomheter i Norge. En utfordring har vært å formulere innhentingsforbudet på en måte som er mer treffende gitt dagens trusselbilde og teknologiske forutsetninger. Departementet foreslår at det bare er informasjonsinnhenting med *overvåkingshensikt* som rammes av innhentingsforbudet. Dette formuleres i lovteksten som et forbud mot innhenting *rettet mot* personer som oppholder seg i Norge. Dette er i tråd med hvordan innhentingsforbudet praktiseres i dag, men i forslaget til ny lov vil dette komme klarere frem.

1.3.3 Nærmere om tilrettelagt innhenting

Lovutkastet foreslår at Etterretningstjenesten på nærmere vilkår får hjemmel til å lagre metadata om elektronisk kommunikasjon som passerer landegrensen. Tilbydere av elektronisk kommunikasjon pålegges en tilretteleggingsplikt. Først etter at en domstol har godkjent det i en kjennelse, vil Etterretningstjenesten kunne søke i de lagrede metadataene og innhente innholdsdata. Et grunnleggende premiss for at innhentingen skal være i overensstemmelse med menneskerettighetene, er at det oppstilles rettssikkerhetsmekanismer som verner mot misbruk og vilkårlighet. Departementet foreslår

en rekke kontrolltiltak. Ordningen med rettens forhåndsgodkjennelse står sentralt. Departementet foreslår at domstolskontrollen legges til Oslo tingrett, og anbefaler ikke å opprette en særdomstol. Det foreslås dessuten en ordning med særskilt advokat som skal ivareta rettighetene til den eller de som innhentingen retter seg mot. Videre foreslås det at EOS-utvalget skal foreta en styrket legalitetskontroll og styrket teknisk kontroll med Etterretningstjenestens innsamling, lagring og bruk av grenseoverskridende elektronisk kommunikasjon.

1.3.4 Personvern, deling av informasjon og andre bestemmelser

Etterretningstjenestens behandling av personopplysninger reguleres i dag blant annet av personopplysningsloven 2000. At 2000-loven er gitt fortsatt anvendelse er en overgangsordning i påvente av ny etterretningstjenestelov.[4] Tjenestens behandling av personopplysninger skiller seg på mange måter fra behandling av personopplysninger utført av andre aktører i samfunnet. Departementet foreslår egne regler for tjenestens behandling av personopplysninger som sikrer en forsvarlig balanse mellom personvernhensyn og etterretningsfaglige hensyn. Forslagene til bestemmelser følger av lovutkastet kapittel 9 og bygger på alminnelige personvernrettslige prinsipper.

Lovforslaget kapittel 10 regulerer nasjonalt og internasjonalt samarbeid og gir regler for utlevering av informasjon. Bestemmelsene baserer seg i stor grad på gjeldende rett og praksis. Det foreslås en ny hjemmel som åpner for at norske myndigheter kan utlevere informasjon til Etterretningstjenesten uten hinder av lovbestemt taushetsplikt. Forslaget oppstiller en rett, og ingen plikt, til å utlevere slik informasjon.

Lovforslaget kapittel 11 inneholder ulike saksbehandlingsregler. Det foreslås at det gjøres unntak fra forvaltningsloven og offentlighetsloven for tjenestens etterretningsvirksomhet. Det foreslås dessuten særskilte tiltak som skal sikre skjerming mot offentlig eksponering av tjenestens ansatte, kilder, kapasiteter, metoder og operasjoner.

Gjeldende lov inneholder ingen bestemmelser om straff. Etter departementets vurdering bør enkelte brudd på loven, først og fremst brudd på taushetsplikten og brudd på enkelte plikter knyttet til tilrettelagt innhenting, belegges med straff. Departementet har også vurdert om det bør gis en lovbestemmelse som tydeliggjør at ansatte i og kilder eller oppdragstakere for Etterretningstjenesten ikke kan straffes for lovlige tjeneste- eller oppdragshandlinger. Et slikt forslag til bestemmelse er inntatt i lovforslaget.

1.4 Arbeidet med lovforslaget

Forsvarsdepartementet har ledet arbeidet med lovforslaget. Lovavdelingen i Justis- og beredskapsdepartementet har bistått i arbeidet med forslaget til lovforankring av tilrettelagt innhenting og har også bidratt til den øvrige regelverksutformingen. Utenriksdepartementet, Justis- og beredskapsdepartementet, Samferdselsdepartementet og Kommunal- og moderniseringsdepartementet har støttet og vært konferert i utredningsarbeidet knyttet til tilrettelagt innhenting. Etterretningstjenesten har vært en viktig bidragsyter med juridisk og etterretningsfaglig ekspertise som grunnlag for forslag til ny lovgivning.

[4] Se forskrift 15. juni nr. 877 om Overgangsregler om behandling av personopplysninger § 1 første ledd bokstav c

2 Rettstilstanden i andre land

2.1 Innledning

Tilnærmet enhver stat driver fordekt etterretningsvirksomhet.[5] I moderne rettsstater innebærer dette at virksomheten er lovforankret i ulik grad og med ulikt detaljeringsnivå. Statene har innrettet sine etterretningstjenester ut fra nasjonale interesser og behov. Dette medfører at de ulike landene har organisert seg forskjellig og at rettstradisjonene knyttet til etterretningsvirksomheten varierer. Det har således gitt varierende verdi å sammenligne lovgivningene på dette området. En trend synes imidlertid å være at nyere lovgivning, eller forslag om lovgivning, på utenlandsetterretningsområdet er vesentlig mer detaljert enn det som tradisjonelt har vært vanlig. Dette gjelder for eksempel Storbritannia, Nederland, Sveits og Finland – og med forslaget her også Norge.

Departementet finner grunn til å understreke at fremstillingen under er basert på åpne kilder. Det er sannsynlig at instrukser og retningslinjer som er underordnet lovgivningen vil være sikkerhetsgraderte og dermed ikke åpent tilgjengelige. Departementet tar således forbehold om at det kan forekomme feil i fremstillingen som følge av at nyanser og praksis basert på lovtolkninger ikke synliggjøres i kildene som departementet har hatt tilgang til. Departementet gjør nærmere rede for ulike lands tilgang til grenseoverskridende elektronisk kommunikasjon i høringsnotatet punkt 11.4.

2.2 Sverige

I Sverige er forsvarsetterretning generelt regulert i lagen (2000:130) om försvarsunderrättelseverksamhet. Loven gir fullmakter til regjeringen og til de myndigheter som regjeringen bestemmer. Forhold av betydning for utenlandsetterretning er regulert i en rekke offentlig tilgjengelige lover og forordninger. Den generelle loven kompletteres av en rekke spesiallover og forordninger. Det samlede inntrykket er således at etterretningslovgivningen er fragmentarisk. Av innhentingsmetoder er det kun signalspaning som har et eget lovgrunnlag. Signalspaning innebærer innhenting av grenseoverskridende elektronisk kommunikasjon fra kabel som eies av en operatør, jf. lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet. Signalspaning er således sammenlignbart med departementets forslag om tilrettelagt innhenting, se om dette i høringsnotatets kapittel 11.

Den svenske regjeringen bestemmer hvordan etterretningsvirksomheten skal organiseres. Etterretningsoppgavene er fordelt mellom etater som utøver etterretningsvirksomhet for ulike formål, jf. lag (2000:130) § 1 tredje ledd. Disse kan etablere og opprettholde samarbeid med andre land og internasjonale organisasjoner. Slikt samarbeid skjer på betingelser gitt av regjeringen, og alltid på en måte som tjener den svenske statsledelsen og det svenske totalforsvaret.

Generelt gjelder at etterretningsvirksomheten utøves til støtte for svensk utenriks-, sikkerhets- og forsvarspolitikk for det formål å kartlegge ytre trusler mot landet og å medvirke til svensk deltakelse i internasjonalt sikkerhetssamarbeid. Etterretningsvirksomheten skal

[5] Det redegjøres nærmere for etterretningsvirksomhetens berettigelse i et internasjonalt perspektiv i høringsnotatets kapittel 3.

ikke ha kriminalitetsbekjempelse som formål, men utelukkende rettes mot utenlandske forhold. For signalspaning gjelder at innhenting kan skje også for å kartlegge «grov grensöverskridande brottslighet som kan hota väsentliga nationella intressen». Oppgavene utføres gjennom innhenting ved bruk av tekniske og personbaserte metoder, og påfølgende bearbeiding, analyse og videreformidling av den innhentede informasjon.

2.3 Danmark

I Danmark er Forsvarets Efterretningstjeneste (FE) den nasjonale utenriks- og militære etterretningstjenesten. Organisatorisk er FE underlagt Det danske forsvarsdepartementet. FEs virksomhet er regulert i lov nr. 602 af 12. juni 2013 om Forsvarets Efterretningstjeneste. Lovgivningen er kortfattet og teknologinøytral. Den beskriver ikke hvilke metoder som kan anvendes av tjenesten, men fastslår at FE kan «indsamle og indhente oplysninger, der kan have betydning for tjenestens efterretningsmæssige virksomhed», jf. § 3 første ledd. Metodene er imidlertid fremstilt i tjenestens ugraderte årsrapporter. Bestemmelsene i loven om Forsvarets Efterretningstjeneste gjelder derfor tilsvarende uavhengig av hvordan opplysningene har blitt fremskaffet.

FE fremskaffer det etterretningsmessige grunnlaget for dansk utenriks-, sikkerhets- og forsvarspolitikk og bidrar til å forebygge og motvirke ytre trusler gjennom å innhente, bearbeide, analysere og formidle opplysninger om forhold i utlandet av betydning for Danmark og danske interesser.

FEs etterretningsmessige virksomhet er rettet mot utlandet. Innhenting og bruk av opplysninger om personer som er hjemmehørende og oppholder seg i Danmark kan likevel skje dersom opplysningene tilfeldigvis fanges opp i forbindelse med utenlandsetterretning. Dette gjelder både juridiske og fysiske personer. FE kan også innhente opplysninger om en fysisk person som er hjemmehørende i Danmark men som befinner seg i utlandet. Forutsetningen for slik innhenting er at det foreligger konkrete holdepunkter som tilsier at vedkommende deltar i aktiviteter som kan innebære eller forøke en terrortrussel mot Danmark eller danske interesser.

I Danmark skilles det også mellom utenlands- og innenlandsetterretning. Politiets Efterretningstjeneste har ansvar for kriminaletterretning og landets indre sikkerhet. Videreformidling av opplysninger mellom FE og Politiets Efterretningstjeneste kan skje innenfor rammen av personvernlovgivningen dersom videreformidlingen kan ha betydning for ivaretagelsen av tjenestenes oppgaver. Som nevnt er den danske lovgivningen teknologinøytral, hvilket innebærer at informasjonsdeling tilsynelatende kan skje uavhengig hvilken kilde informasjonen stammer fra.

2.4 Finland

I skrivende stund har ikke Finland ennå lovfestet regulering av landets militære etterretningsvirksomhet, men det pågår et arbeid med å få dette på plass. Den 25. januar 2018 overleverte den finske regjeringen et lovforslag for behandling i riksdagen. Forslagene dekker ulike sider ved etterretningsvirksomhet, herunder sivil og militær. Det foreslås særskilt lovgivning for sivil etterretningsvirksomhet underlagt innenriksministeriet, og militær etterretningsvirksomhet underlagt forsvarsministeriet. Begge lovforslagene åpner for innhenting av både innenlands- og utenlandsetterretning. De øvrige to proposisjonene er et

grunnlovsforslag og et forslag om regulering av kontroll med etterretningsvirksomheten. Også behandling av personopplysninger i Försvarsmakten er regulert i egen lov. Den finske riksdagen vedtok 3. oktober 2018 en hurtigprosedyre for endring av den finske grunnloven, men endringen vil ikke kunne tre i kraft før etter neste riksdagsvalg i april 2019.

De finske forslagene angir hvilke etterretningsformål som kan berettige innhenting av informasjon. For øvrig inneholder lovforslagene bestemmelser om samarbeid med andre myndigheter, internasjonalt samarbeid, metoder for informasjonsinnhenting, prosessuelle krav til beslutningstaking, samt styring og kontroll av etterretningsvirksomheten. I tillegg foreslås bestemmelser om den tekniske gjennomføringen av innhenting av datatrafikk. Det helhetlige inntrykket er at Finland går langt i å beskrive de militære og sivile etterretningstjenestenes metoder og hvilke prosedyrer som må følges i forbindelse med metodebruk og informasjonsinnhenting.

Lovforslagene innebærer at de sivile og militære etterretningstjenestene vil få nye og betydelige oppgaver og større myndighet. Tilsvarende foreslår den finske regjeringen å fornye kontrollregimet for etterretningstjenestene. Kontrollmekanismene er ment å sørge for at etterretningsvirksomheten utføres på en forsvarlig måte som ivaretar rettssikkerheten til den enkelte. Det har vært et mål i seg selv å organisere kontrollorganene på en effektiv måte ved å gi dem en sterk posisjon og myndighet. Forslaget innebærer at etterretningsvirksomheten underlegges parlamentarisk kontroll av et nyopprettet underrättelsetillsynsutskott i riksdagen. I tillegg foreslås at et underrättelseombudsmann foretar legalitetskontroll og avvikshåndtering i form av stans av innhenting og/eller sletting av rettstridig innhentet informasjon. Ombudet vil også være klageinstans for individer som vet eller mistenker at de er eller har vært gjenstand for overvåkning.

2.5 Frankrike

I Frankrike er etterretningsvirksomheten fordelt på spesialiserte etterretningstjenester utpekt av Conseil d'Etat. Rammene for tjenestenes virksomhet er regulert i lov nr. 2015-912 av 24. juli 2015 Bok VIII: Etterretning. Loven utgjør et generelt men detaljert rammeverk for etterretningsvirksomhet, og angir blant annet hvilke metoder som kan benyttes, formålsbegrensninger og prosessuelle regler knyttet til slik metodebruk, tilsyns- og kontroll av tjenestenes virksomhet, klageadgang og straff for brudd på regelverket.

Enheten Direction générale de la sécurité extérieure (DGSE) har ansvar for innhenting av både sivil og militær utenlandsetterretning. DGSE kan innhente informasjon i den utstrekning det er nødvendig for utøvelsen av deres respektive oppgaver og innhentingen bidrar til å fremme Frankrikes grunnleggende interesser. Hvilke interesser det her er tale om følger av lovens artikkel L811-3, og kan oppsummeres som følger:

- Frankrikes uavhengighet, territoriets integritet og det nasjonale forsvar;
- kvalifiserte utenrikspolitiske, økonomiske, industrielle og vitenskapelige interesser, oppfyllelsen av Frankrikes europeiske og internasjonale forpliktelser, samt forebygging av uønsket utenlandsk påvirkning;
- forebygging av en rekke alvorlige forhold, herunder terrorisme, organisert kriminalitet og spredning av masseødeleggelsesvåpen.

Innhentingsmetodene kan benyttes på fransk territorium på nærmere bestemte vilkår. Fransk etterretningsvirksomhet er således ikke underlagt en tilsvarende forbud mot

innhenting på eget territorium slik som til sammenligning gjelder for den norske Etterretningstjenesten. I Frankrike begrenses de spesialiserte tjenestenes innhenting av deres respektive rettsgrunnlag og formålsavgrensningen som nevnt over.

2.6 Storbritannia

I Storbritannia er det Secret Intelligence Service (MI6) som har som oppgave å drive etterretningsvirksomhet rettet mot utenlandske forhold. MI6 samarbeider med de øvrige etterretnings- og sikkerhetstjenestene for ivaretakelsen av Storbritannias sikkerhet, herunder UK Government Communactions Headquarters (GCHQ) som er Storbritannias generelle signaletterretningstjeneste. MI6 og GCHQs generelle virksomhet er hjemlet i Intelligence Services Act av 1994. Etterretningsvirksomhet kan bare utføres innenfor rammen av formålsbestemmelsene i henholdsvis section 1 (2) og section 3 (2), som etter sin ordlyd er likelydende for de to tjenestene. I korte trekk kan tjenestene innhente informasjon om utenlandske forhold av hensyn til den nasjonale sikkerheten, den økonomiske velferden eller for å bidra til å avverge eller avdekke alvorlig kriminalitet.

Hva angår regulering av metodebruk er innhenting av elektronisk kommunikasjon fra kabelnettverk regulert i Investigatory Powers Act fra 2016 med tilhørende reguleringer fra 2018. Loven omfatter ulike former for innhenting av elektronisk kommunikasjon, herunder innhenting og lagring av elektronisk kommunikasjon, innbrudd i elektronisk utstyr og innsamling av data i bulk. Lovgrunnlaget for denne typen innhenting er særdeles omfattende og detaljert sammenlignet med øvrige lands lovgivning om det samme. Annen metodebruk for britisk etterretningsvirksomhet er ikke tilsvarende regulert.

MI6 og GCHQ kan samarbeide med de øvrige britiske etterretnings- og sikkerhetstjenestene. For øvrig kan tjenestene dele informasjon med andre nasjonale myndigheter på nærmere bestemte vilkår.

MI6 og GCHQ er organisert som sivile forvaltningsorganer underlagt det britiske utenriksdepartementet. De avgjørelsene som må fattes på høyt nivå tas følgelig av utenriksministeren selv. Dette gjelder for eksempel intervenerende handlinger som rammer noens eiendom eller trådløs telegrafi, jf. Intelligence Services Act section 5. For innhenting av elektronisk kommunikasjon gjelder ytterligere sikkerhetsgarantier, se nærmere om dette i punkt 11.4.6.

3 Etterretning i det internasjonale system av nasjonalstater og normer

3.1 Hva er utenlandsetterretning?

3.1.1 Generelt

Behovet for å innhente informasjon om omverdenen har eksistert til alle tider, både i fred, krise og i krig. Internasjonalt foreligger det ingen entydig definisjon av *etterretning* i betydningen etterretning rettet mot utenlandske forhold (*foreign intelligence*). I forsvarssjefens etterretningsdoktrine av mai 2013 er utenlandsetterretning definert slik:

> «Etterretning er systematisk innhenting og bearbeiding av informasjon som angår utenlandske forhold ervervet med åpne og fordekte metoder i en statlig legal ramme. Produktene skal redusere usikkerhet, skape forståelse og har ofte en prediktiv karakter. Begrepet brukes om produktet, aktiviteten og organisasjonen som utøver aktiviteten.»

Definisjonen bygger på NATOs tilsvarende definisjon, og skiller *utenlands*etterretning fra annen innsamling og bearbeiding av informasjon, enten det gjøres av andre offentlige myndigheter (slik som kriminaletterretning) eller private aktører (såkalt *business intelligence*).

3.1.2 Hvorfor bedriver Norge og andre stater etterretning?

Det *overordnede formålet* med norsk utenlandsetterretning er å beskytte Norges eksistens, territorielle integritet, borgere og viktige nasjonale interesser. Etterretning er nødvendig for å unngå strategiske overraskelser som kan utfordre den norske staten og vår suverenitet. Etterretningstjenesten skal bidra med rettidig, pålitelig og relevant kunnskap om verden rundt oss, som beslutningsgrunnlag for norske myndigheter. Tjenesten er informasjonsleverandør til militære og sivile myndigheter og organer; til de som utformer policy og til de som omsetter politikk til handling. Etterretningstjenestens motto er *Viten om verden for vern av Norge.* For en småstat som Norge, med vår geostrategiske plassering, er viten om verden særlig viktig.

I *mellomstatlig* sammenheng kan etterretningsvirksomhet ha positive effekter. Kunnskap om hverandres egentlige kapasiteter og intensjoner kan ha en stabilitetsfremmende effekt, og kan motvirke overreaksjoner blant annet fordi man misforstår en aktørs intensjoner. I forarbeidene til gjeldende lov om Etterretningstjenesten heter det at «[g]jensidig oversikt over blant annet militære forhold vil dessuten ofte ha en stabilitetsfremmende virkning.» [6] Etterretning er på sitt beste konfliktforebyggende, konfliktdempende og tillitsskapende i internasjonale relasjoner.

Etterretningens *kjerne* er den samme i dag som i tidligere tider. Etterretning benyttes for å samle inn informasjon om omverdenen, og særlig informasjon om kapasiteter og intensjoner som forsøkes holdt skjult. Om nødvendig må slik informasjon tilegnes ved fordekte metoder som ellers ikke er tillatt i samfunnet for andre formål. Metodene og etterretningsmålenes karakteristikker har forandret seg gjennom tidene. Nye oppfinnelser, herunder mer moderne kommunikasjonsformer, innebærer at etterretningstjenesters mulighet for å innhente informasjon med ulike metoder til dels har økt. Ny teknologi har samtidig økt muligheten for å skjerme kommunikasjon og informasjon gjennom blant annet kryptering, slik at den etterretningsrelevante informasjonen kan være vanskeligere tilgjengelig. Teknologiutviklingen innebærer dessuten nye utfordringer, både på grunn av nye sårbarheter, og fordi mengden informasjon har blitt så enorm.

Norges geografiske plassering i et *strategisk viktig* område gjør det særlig viktig for norske beslutningstakere å ha god oversikt over politiske utviklingstrekk og militære forhold som kan føre til spente sikkerhetspolitiske situasjoner og kriser. I våre nærområder testes konvensjonelle og kjernefysiske militære systemer, det foregår omfattende militærøvelser og annen aktivitet. Det er sentralt at vi har kjennskap til og forstår denne aktiviteten korrekt. Dette er viktig både for norske beslutningstakere, for utviklingen av Forsvaret og for vår

[6] Ot.prp. nr. 50 (1996-97) side 9

deltakelse i NATO. Det er også sentral kunnskap for å kunne håndtere oppdukkende situasjoner og kriser. En viktig lærdom fra overraskelsesangrepet 9. april 1940 var at Norge måtte bygge opp en egen effektiv etterretningstjeneste.

Etterretning er også viktig for å unngå eller redusere konsekvensene av andres etterretning. *Kontraetterretning* er nødvendig for å beskytte egen sensitiv informasjon og dermed hindre at andre stater får et informasjonsovertak tilsvarende det en selv ønsker å ha. En vedvarende og ofte usynlig etterretningsvirksomhet mellom stater er derfor i praksis akseptert, så lenge den ikke strider direkte mot folkeretten.

3.1.3 Krav til en moderne etterretningstjeneste

Satt inn i en historisk kontekst ser vi at fremveksten av nasjonalstater og det moderne diplomatiet etter middelalderen bidro til å utvide etterretningens funksjon og rolle – fra et grunnleggende selvforsvarsbehov, via en fase preget av ekspansjon og erobring – og frem til dagens politisk-strategiske understøttelsesfunksjon og oppgavespekter av både militære og sivile etterretningsbehov. 11. september 2001 ble en milepæl for vestlige etterretningstjenester. Uforutsigbarhet, ustabilitet og fremveksten av grenseoverskridende terrortrusler preger sikkerhetssituasjonen. De *sivile* etterretningsbehovene har økt.

Moderne *militære* operasjoner kan i dag ikke gjennomføres uten etterretning som fundament. I økende grad vektlegges dessuten situasjonsforståelse og etterretningsgrunnlag også for å unngå at militære operasjoner gjennomføres i strid med krigens folkerett og politiske og militære målsettinger. Etterretningens økende rolle i målutvelgelsesprosesser i væpnet konflikt underbygger dette. Rettidig varsling, god evne til å innhente og analysere informasjon samt å opprettholde en god situasjonsforståelse danner grunnmuren for et militært forsvar. God situasjonsforståelse er viktig både til lands, over og under havoverflaten, i luften, rommet og det digitale domenet.

Utøvelsen av utenlandsetterretning henger nært sammen med en stats suverenitet, og stater er i liten grad villige til å overlate ansvaret for etterretning til andre. Bare unntaksvis koordineres etterretningsinformasjon gjennom *internasjonale organisasjoner* slik som FN, NATO eller EU. Samtidig har det gjennom flere år vært en økende erkjennelse av behovet for mer internasjonalt etterretningssamarbeid for å møte aktuelle grenseoverskridende trusler, særlig gjelder dette land i det vestlige sikkerhetssamarbeidet. Nødvendigheten av å dele informasjon med partnere er økende. FNs sikkerhetsråd har flere ganger oppfordret til økt etterretningssamarbeid blant annet for å møte trusselen fra internasjonal terrorisme. Deling og samarbeid er nødvendig internasjonalt, men også nasjonalt mellom de myndigheter som har ansvar for henholdsvis utenlandsetterretning og innenlands sikkerhetsetterretning.

Det stilles store krav til Etterretningstjenesten som en *moderne utenlandsetterretningstjeneste*. Tjenesten må kunne forstå oppdragsgivernes behov, og evne å innhente den informasjonen som etterspørres. Men det holder ikke å fange inn informasjon i seg selv, enten det skjer med menneskebaserte eller tekniske sensorer. I de enorme mengdene av informasjon som befinner seg i og forflytter seg i tusenvis av nettverk må tjenesten både være i stand til å finne de relevante små informasjonsbitene, men også evne å sette bitene sammen, og tolke dem, i en større helhet. Dette kan bare oppnås gjennom kontinuerlig oppgradering, oppdatert metodebruk, avanserte tekniske løsninger, kompetente analytikere og et godt regelverk.

3.1.4 Åpenhet og skjerming

Utøvelsen av etterretningsvirksomhet er forbundet med hemmelighold, men også Etterretningstjenesten er avhengig av *legitimitet og tillit*, både på politisk nivå og ikke minst i befolkningen. En forutsetning for å holde hemmelig det som det er avgjørende å holde hemmelig, er derfor å vise åpenhet rundt det som det er mulig å være åpen om. Samtidig er balansegangen mellom åpenhet og skjermingsbehov på enkelte områder svært krevende. Det er fortsatt avgjørende å beskytte kilder, kapasiteter og metoder. Den uavhengige kontrollen som EOS-utvalget utøver bidrar til legitimitet og tillit i befolkningen. Utvalget har innsyn i de hemmelige aktivitetene og arkivene til Etterretningstjenesten, som allmennheten ikke kan ha innsyn i. Tilliten til at tjenesten utøver sin aktivitet innenfor de legale rammer som er gitt, må befolkningen derfor basere på EOS-utvalgets innsyn og deres vurderinger. I de senere år har Etterretningstjenesten også vist økende åpenhet. Årlige ugraderte etterretningsvurderinger samt deltakelse i den offentlige debatten bidrar til det. Fremstillingen i høringsnotatet her representerer en ytterligere omdreining i retning av åpenhet om hva Etterretningstjenesten er og hva den gjør.

3.2 Folkerettslige rammer

3.2.1 Akseptert aktivitet mellom stater

Etterretningsvirksomhet er en *akseptert aktivitet* mellom stater og er ikke i strid med folkeretten. Det finnes ingen traktater eller alminnelige folkerettslige prinsipper som forbyr etterretning. Det foreligger heller ingen avgjørelser fra internasjonale domstoler som konkluderer med at etterretning i seg selv er folkerettsstridig. Statspraksis, som ved siden av traktater og alminnelige folkerettslige prinsipper er en av de viktigste rettskildene i folkeretten, viser at statene i utgangspunktet aksepterer etterretningsvirksomhet. Selv om stater har protestert når det har blitt kjent at de har vært utsatt for etterretningsvirksomhet fra andre stater, er protestene ofte preget av det faktum at den protesterende stat selv utfører lignende handlinger som det de blir utsatt for. Selv om spionasje kan være straffbart etter nasjonal lovgivning, er det sjelden at stater har påberopt at etterretningsvirksomhet som sådan utgjør folkerettsbrudd i form av suverenitetskrenkelse eller brudd på maktforbudet i FN-pakten artikkel 2(4). Tradisjonell etterretning i form av informasjonsinnhenting for å ivareta nasjonale interesser er dermed ikke ulovlig etter folkeretten.

Det internasjonale samfunn synes tilfreds med å opprettholde en stilltiende enighet om at etterretningsvirksomhet ikke er folkerettsstridig. Denne *pragmatismen* gjenspeiler seg i at utenlandsetterretningsvirksomhet er lite regulert i den skrevne folkeretten. Selv om enkeltaktører har tatt til orde for at etterretningsvirksomhet helt eller delvis burde reguleres nærmere, har få om noen stater argumentert for dette.

Det betyr ikke at all aktivitet som utøves av etterretningstjenester verden over er akseptert. Aktivitet som innebærer *brudd på* grunnleggende menneskerettigheter, suverenitetskrenkelser eller brudd på intervensjonsforbudet eller maktforbudet i folkeretten er uakseptabel både av politiske og folkerettslige grunner. Dersom etterretningstjenester utøver ulike typer fordekte operasjoner som går ut over innhenting av informasjon, for eksempel påvirkningsoperasjoner i form av forsøk på påvirkning av valg eller andre indre anliggender, eller cyberangrep i fredstid med hensikt å lamme eller ødelegge infrastruktur eller funksjoner, er dette ikke akseptabelt. Operasjoner av denne karakter strider mot

folkerettslige avtaler og alminnelige folkerettslige prinsipper, og er ikke tillatt. Spionasje med formål å gi eget lands industri kommersielle markedsfordeler (industrispionasje) er også i økende grad ansett som en uakseptabel virksomhet mellom stater.[7]

Aktiviteten som utøves må holde seg innenfor grunnleggende folkerettslige rammer, blant annet innenfor rammen av maktforbudet i FN-pakten. Også de alminnelige menneskerettighetene setter enkelte begrensninger med hensyn til hvilke metoder som tas i bruk. I væpnet konflikt vil bestemmelsene i krigens folkerett gjelde som ytre ramme for hvordan etterretningsvirksomhet kan gjennomføres. For internasjonale operasjoner kan særskilte begrensninger, eksempelvis geografiske restriksjoner, følge av operasjonens mandat og engasjementsregler.

3.2.2 Metodebruken

Det ligger i etterretningens natur at *metodebruken* vil kunne medføre brudd på den nasjonale lovgivningen i en annen stat, med mindre det foreligger særskilt avtale eller annet rettslig grunnlag. Fordekt innhenting av informasjon som søkes hemmeligholdt av en annen stat vil ofte være straffebelagt internrettslig av den stat innhentingen er rettet mot. I Norge er Etterretningstjenesten den eneste offentlige myndighet som gjennom lov og instruks har myndighet til å bryte lovgivningen i andre stater. I tillegg kommer at stater vanskelig kan beskytte seg gjennom nasjonal lovgivning mot etterretningsvirksomhet som foregår utenfor dens jurisdiksjonsområde, eksempelvis fra åpent hav eller fra rombaserte etterretningsplattformer.

Selv om etterretning ikke er ulovlig etter folkeretten, må *måten* man gjennomfører etterretningsvirksomhet på, likevel vurderes konkret opp mot folkerettslige normer. Vurderingstemaene og de rettslige kildene man vurderer saken opp mot kan være forskjellige. Den relevante folkeretten i denne sammenheng kan deles inn i to hovedgrupper: Den første gruppen gjelder folkerettsregler som har til hensikt å beskytte enkeltindivider. Slike regler fremgår blant annet av internasjonal humanitærrett og menneskerettighetene. Menneskerettighetene er nærmere behandlet i høringsnotatet kapittel 4. Etterretningsvirksomhet skal aldri gjennomføres i strid med grunnleggende menneskerettigheter som staten er bundet av. Den andre gruppen gjelder folkerettsregler som regulerer statenes rettigheter og plikter vis-a-vis hverandre, blant annet prinsippene nedfelt i FN-pakten og i reglene om statsansvar. Etterretning kan for eksempel ikke gjennomføres ved metoder eller effekter som innebærer folkerettsstridige væpnede angrep eller suverenitetskrenkelser.

3.2.3 Etikk

Selv om etterretningsvirksomhet *per se* er lovlig og berettiget kan den likevel reise etiske problemstillinger. Formålet med all virksomhet Etterretningstjenesten bedriver er å bidra til å verne norsk sikkerhet og suverenitet og å sikre viktige nasjonale interesser. Etterretningens etiske paradoks er at tjenesten i denne virksomheten kan være nødt til å bruke metoder som bryter andre lands lover og fra tid til annen kan bryte med grunnleggende norske kulturelle normer for hvordan vi bør behandle hverandre som mennesker. Som et generelt prinsipp

[7] Et eksempel på slik ulovlig industrispionasje vil være å innsamle bedriftshemmeligheter om en virksomhets forsknings- og/eller patentutvikling for å utnytte disse til egen produksjon og fortjeneste.

gjelder derfor at alt som er lov ikke nødvendigvis er forsvarlig eller riktig å gjennomføre. Etiske overlegninger vil supplere de rettslige vurderingene som gjøres på de ulike stadier i etterretningsvirksomheten.

4 Forholdet til Grunnloven og menneskerettighetene

4.1 Rettslig rammeverk og utgangspunkter

4.1.1 Myndighetenes inngrep overfor den enkelte. Legalitetsprinsippet

Legalitetsprinsippet krever at myndighetenes inngrep overfor den enkelte skal ha hjemmel i lov. Etter grunnlovsendringene i 2014 er legalitetsprinsippet nå nedfelt i Grunnloven § 113. Formålet med å grunnlovsfeste legalitetsprinsippet var ikke å gjøre endringer i rettstilstanden, men å «synliggjøre prinsippet og samtidig vise at det fungerer som en reell skranke for makthavernes myndighetsutøvelse».[8] Konstitusjons- og kontrollkomiteen i Stortinget delte Menneskerettighetsutvalgets syn om at legalitetsprinsippet burde tas inn i Grunnloven, og viste til at dette er «grunnlaget for forståelsen av rettsstaten» og dermed utgjør en av «de sentrale deler av vår statsskikk».[9] Høyesterett uttaler i Rt. 2014 s. 1105 at lovkravet fremmer forutberegnelighet og legger til rette for at den enkelte kan treffe rasjonelle valg. Lovkravet motvirker således vilkårlighet og usaklig forskjellsbehandling, jf. også Grunnloven § 98 første ledd som slår fast at alle er like for loven. Lovkravet støtter Stortingets lovgiverfunksjon etter Grunnloven § 75 a og den demokratiske ideen som ligger bak ordningen med at lovgiverkompetansen er lagt til en folkevalgt nasjonalforsamling. I dette ligger at den utøvende makt ikke kan gå lenger i sin maktbruk overfor borgerne enn det fullmaktene fra lovgiver gir grunnlag for.

At inngrep i privatlivet i form av informasjonsinnhenting må ha hjemmel i nasjonal lov som må oppfylle visse kvalitative krav følger også av Den europeiske menneskerettskonvensjon (EMK) artikkel 8 med tilhørende praksis fra Den europeiske menneskerettsdomstol (EMD).[10]

I kraft av sin rolle som lovgiver kan Stortinget både vedta nye lover og endre tidligere vedtatte lover, og dermed sikre at legalitetsprinsippet overholdes. Grunnloven og menneskerettighetene setter imidlertid konstitusjonelle og menneskerettslige rammer knyttet til *innholdet* i de lover Stortinget kan vedta. Rekkevidden av dette rammeverket har betydning for utformingen av ny lov om Etterretningstjenesten, og vil vurderes i det følgende.

[8] Rapport til Stortingets presidentskap fra Menneskerettighetsutvalget om menneskerettigheter i Grunnloven Dokument nr. 16 (2011-2012) s. 248

[9] Innst.186 S (2013-2014) s. 31

[10] Jf. f.eks. *Weber og Saravia mot Tyskland* 26. juni 2006 avsnitt 84 samt en lang rekke andre EMD-dommer på området

4.1.2 Forholdet mellom Grunnlovens menneskerettighetsbestemmelser og de internasjonale menneskerettighetskonvensjonene vi er bundet av

4.1.2.1 Noen utgangspunkter - hvilke bestemmelser har hvilken rang og hvilken rettskildeverdi?

I forbindelse med grunnlovsrevisjonen i 2014 ble Grunnloven supplert med flere nye bestemmelser for å styrke menneskerettighetenes stilling i norsk rett. Menneskerettighetenes betydning trekkes frem allerede i formålsbestemmelsen til Grunnloven. Paragraf 2 sier at Grunnlovens formål er å verne om demokratiet, rettsstaten og menneskerettighetene. Paragraf 92 innleder Grunnlovens kapittel E om menneskerettigheter. Bestemmelsen fikk sin nåværende form etter grunnlovsrevisjonen i 2014 og lyder:

> Statens myndigheter skal respektere og sikre menneskerettighetene slik de er nedfelt i denne grunnlov og i for Norge bindende traktater om menneskerettigheter.

Det har vært reist spørsmål ved om bestemmelsen skal forstås slik at alle internasjonale menneskerettighetsbestemmelser som Norge var bundet av før grunnlovsendringene ble vedtatt heretter skulle gis grunnlovs rang. I Høyesteretts plenumsdom i Holship-saken[11] ble det klarlagt at Grl. § 92 ikke innebærer at de traktatene bestemmelsen viser til, skal ha grunnlovs trinnhøyde. Høyesterett gjentar dette i HR-2018-456-P i avsnitt 93 og tilføyer at «[d]et bestemmelsen innebærer, er et pålegg til domstolene og andre myndigheter om å håndheve menneskerettighetene på det nivå de er gjennomført i norsk rett.»

Den europeiske menneskerettskonvensjon (EMK) er en traktat som har hatt stor betydning for norsk og europeisk rettsutvikling. Dette skyldes for det første at EMK fastslår helt grunnleggende rettigheter som europeiske myndigheter har forpliktet seg til å ivareta overfor alle som befinner seg innenfor deres jurisdiksjon. Tyngden i EMK sin gjennomslagskraft er også et resultat av den myndighet Den europeiske menneskerettsdomstolen (EMD) er gitt til å avsi bindende dommer i konkrete saker, derigjennom til autorativt å fastsette hvordan konvensjonen til enhver tid skal forstås.

EMK ble inkorporert i norsk rett ved vedtakelsen av menneskerettsloven i 1999. EMK har status som norsk lov, jf. § 2 nr. 1, og vil i tilfelle motstrid gå foran annen norsk lovgivning, jf. § 3. FN-konvensjonen om sivile og politiske rettigheter (SP) fra 1966 er også inkorporert i norsk rett ved menneskerettsloven, og inneholder mange lignende rettighetsbestemmelser som EMK. FNs menneskerettskomité overvåker statenes etterlevelse av konvensjonen. Selv om komitéuttalelsene ikke er rettslig bindende har Høyesterett lagt til grunn at uttalelser fra Menneskerettskomitéen i individklagesaker likevel kan ha betydelig vekt som rettskilde.[12]

Samtidig vurderer departementet at EMK sin faktiske innflytelse på rettsutviklingen er og har vært større enn den fra SP, særlig når det gjelder spørsmålene som må vurderes i nærværende lovforslag. Den mer inngående drøftelsen av hvilke krav menneskerettighetene stiller til utformingen og praktiseringen av regelverket i forslag til ny etterretningstjenestelov vil derfor i første rekke knyttes til EMKs bestemmelser, med tilhørende praksis fra EMD. Det rettighetsvern som fastslås i EMK formodes også dekkende for de skranker for lovgivningen som kan utledes av SP.

---

[11] HR-2016-2554-P

[12] Se blant annet Rt. 2008 s. 1764

4.1.2.2 Tolking av bestemmelsene. Dynamisk utvikling.

Som utgangspunkt må tolkingen av menneskerettighetsbestemmelsene i Grunnloven følge de alminnelige prinsipper for grunnlovstolking. Det er imidlertid grunn til å hevde at det er to forhold som utmerker seg i forbindelse med Grunnlovens kapittel E. For det første er forarbeidene fra Menneskerettighetsutvalget og innstillingen fra kontroll- og konstitusjonskomiteen i Stortinget langt mer utførlige enn det som ellers har vært praksis for grunnlovsbestemmelser. Forarbeidene gir her viktige bidrag når innholdet i bestemmelsene skal fastslås. I tillegg er grunnlovsbestemmelsene inspirert av og i stor utstrekning utformet etter mønster av internasjonale traktatbestemmelser på menneskerettsområdet, særlig fra EMK. I dette ligger at de internasjonale forbildene vil få en sentral betydning som tolkingsbidrag.[13] Et viktig spørsmål i denne forbindelse er hvordan Grunnlovens menneskerettighetsbestemmelser skal leses sett i forhold til konvensjonsbestemmelsene i EMK, gitt EMDs rolle i å tolke og videreutvikle konvensjonen. Spørsmålet er altså om en dynamisk utvikling av forbildebestemmelsene krever at forståelsen av grunnlovsbestemmelsene må følge samme utvikling, og hva som vil skje dersom EMD og Høyesterett legger ulikt innhold i tolkingen av de respektive regelsettene. Leser man Grunnlovens § 92 og formålet med grunnlovsrevisjonen i sammenheng er det mye som tyder på at de nye grunnlovsbestemmelsene vil bli tolket i lys av utviklingen av EMDs praktisering av EMK. Praksis fra Høyesterett til nå viser at domstolen i det vesentligste har lagt seg på samme linje som EMD. Høyesterett har allerede brukt de internasjonale konvensjonsforpliktelsene som forbilde for å innfortolke en begrensningshjemmel i Grl. § 102,[14] som nærmere beskrevet under. Samtidig har Høyesterett uttalt en konstitusjonelt viktig begrensning når det gjelder betydningen av de internasjonale kildene i Rt. 2015 s. 93, avsnitt 57:

> «Jeg legger til grunn at [Grl.] § 102 skal tolkes i lys av de folkerettslige forbildene, men likevel slik at fremtidens praksis fra de internasjonale håndhevingsorganene ikke har samme prejudikatsvirkning ved grunnlovstolkningen som ved tolkningen av de parallelle konvensjonsbestemmelsene: Det er etter vår forfatning Høyesterett – ikke de internasjonale håndhevingsorganene – som har ansvaret for å tolke, avklare og utvikle Grunnlovens menneskerettighetsbestemmelser.»

Oppsummert er det grunn til å anta at Høyesterett i stor grad vil legge sin tolking av de nye menneskerettighetsbestemmelsene i Grunnlovens kapittel E nært opp til de folkerettslige forbildene, derunder at EMDs dynamiske forståelse av EMK vil gjenspeiles i Høyesteretts praksis. Likevel kan man ikke utelukke at Høyesterett, med utgangspunkt i sitatet over, kan komme til å legge et annet innhold i grunnlovsbestemmelsene enn det som følger av menneskerettskonvensjonene dersom dette settes på spissen. Det er følgelig ingen automatikk i at Høyesterett i alle saker som gjelder tolking av grunnlovsbestemmelsene, vil kopiere EMD.

Et annet moment er dersom internasjonale håndhevelsesorganer som EMD legger til grunn en i overkant dynamisk tolking av konvensjonens ordlyd basert på formålsbetraktninger og effektivitetshensyn. Dette vil i ytterste konsekvens kunne gå ut over prinsippet om folkesuverenitet og demokrati, altså prinsippet om at det er folket ved den lovgivende

[13] Se for eksempel Jørgen Aall, *Rettsstat og menneskerettigheter* (2015), s. 36-27 og s. 44-47

[14] Rt. 2015 s. 93

forsamling i nasjonalstatene som gir rettsreglene og inngår konvensjonene som borgerne og staten er bundet av.[15]

I sin lovgivningsoppgave vil Stortinget måtte forholde seg til både de skranker som følger av Grunnloven, og av menneskerettighetskonvensjonene vi er bundet av, all den tid begge disse regelverkene i tilfelle motstrid vil gå foran alminnelig norsk lovgivning, jf. trinnhøydeprinsippet og menneskerettsloven § 3.[16] De internasjonale konvensjonsforpliktelsene Norge er bundet av, med særlig vekt på EMK, vil derfor legge viktige premisser for lovreguleringen av de delene av Etterretningstjenestens virksomhet som griper inn i menneskerettighetene.

4.1.3 Nærmere om jurisdiksjonsspørsmålet

For at en stat skal kunne holdes ansvarlig etter EMK er det et grunnvilkår at personen er innenfor statens jurisdiksjon i konvensjonens forstand. Dette følger av EMK artikkel 1 som fastsetter at statspartene «skal sikre enhver innen sitt myndighetsområde [eng. «jurisdiction»] de rettigheter og friheter som er fastlagt i […] konvensjonen». FNs konvensjon om sivile og politiske rettigheter (SP) artikkel 2 inneholder en tilsvarende bestemmelse, men som er noe annerledes formulert.[17] Menneskerettskomiteen har lagt tilsvarende vurderingstema til grunn etter SP artikkel 2 som EMD har gjort etter EMK artikkel 1. SP artikkel 2 behandles ikke nærmere her.

Jurisdiksjonsbegrepet har vært gjenstand for stadig utvikling i EMDs rettspraksis. I storkammerdommen *Al-Skeini m.fl. mot Storbritannia* av 7. juli 2011 oppsummerte, og i noen grad reformulerte, EMD de generelle prinsippene som er relevant for jurisdiksjonsvurderingen. 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. Om slike eksepsjonelle omstendigheter foreligger, må besluttes utfra de særlige fakta i den foreliggende saken. EMD har oppstilt to hovedunntak fra territorialprinsippet: situasjoner hvor statlige agenter utøver «myndighet og kontroll» («authority and control») over personer utenfor eget territorium og situasjoner hvor staten utøver effektiv kontroll over et område. I *Chagos Islanders mot Storbritannia* oppsummerer EMD innholdet i de to hovedunntakene slik:[18]

> «iv. There are two principal exceptions to territoriality: circumstances of “State agent authority and control” and “effective control over an area”;
>
> v. The “State agent authority and control” exception applies to the acts of diplomatic and consular agents present on foreign territory; to circumstances where a Contracting State,

[15] Se mer om dynamisk tolking i artikkel av dr. juris Jens Edvin A. Skoghøy «Dynamisk tolking i internasjonale domstoler som fenomen, problem og effektivitetsgaranti» inntatt i Lov og rett, 2011 s. 511-530

[16] Menneskerettsloven § 3 har rang som norsk lov og kan dermed etter alminnelige prinsipper fravikes ved lov, men dette ville undergrave lovens formål og betydning og det er følgelig ingen praksis for dette.

[17] SP artikkel 2 lyder slik i norsk oversettelse: «Hver konvensjonspart forplikter seg til å respektere de rettigheter som anerkjennes i denne konvensjon, og å sikre dem for alle som befinner seg på dens territorium og er undergitt dens jurisdiksjon».

[18] *Chagos Islanders mot Storbritannia* avsagt 11. desember 2012, avsnitt 70

through custom, treaty or agreement, exercises executive public powers or carries out judicial or executive functions on the territory of another State; and circumstances where the State through its agents exercises control and authority over an individual outside its territory, such as using force to take a person into custody or exerting full physical control over a person through apprehension or detention.

vi. The “effective control over an area” exception applies where through military action, lawful or unlawful, the State exerts effective control of an area outside its national territory.”

De to alternativene forenkles gjerne til et spørsmål om konvensjonsstaten utenfor eget territorium utøver kontroll over en person eller et område. Hvor staten utøver effektiv kontroll over et område, skal i utgangspunktet alle menneskerettighetene sikres for personene innenfor det aktuelle området. Hvor jurisdiksjon er et resultat av myndighet og kontroll over en person, vil staten ha en forpliktelse til å sikre de rettighetene og frihetene som er relevante for situasjonen til den aktuelle personen.

Spørsmålet blir hvordan jurisdiksjonsspørsmålet stiller seg ved Etterretningstjenestens aktivitet som kan innebære inngrep i noens menneskerettigheter etter EMK. Etterretningstjenestens oppdrag er rettet mot ytre trusler og utenlandske forhold. Tjenesten har på visse vilkår adgang til å innhente informasjon om fysiske og juridiske personer på norsk territorium. Informasjonen som tjenesten henter inn, er å finne både i det fysiske og i det digitale rom. I sum er det altså flere jurisdiksjonsrelaterte problemstillinger som kan reises. Utgangspunktet er klart. Personer på norsk territorium er innenfor norsk jurisdiksjon i EMKs forstand. Det legges derfor til grunn at EMK som utgangspunkt kommer til anvendelse på Etterretningstjenestens aktiviteter i den grad disse omfatter personer som bor eller oppholder seg i Norge.

Spørsmålet om jurisdiksjon kommer først og fremst på spissen der Etterretningstjenesten innhenter informasjon om utlendinger og norske borgere i utlandet.

Innhenting av informasjon om personer i utlandet kan finne sted på flere måter.

Spørsmålet om jurisdiksjon reiser seg for det første for Etterretningstjenestens innhentingsvirksomhet når innhentingen av informasjon om personer i utlandet finner sted *fra utlandet*. Spørsmålet om ekstraterritoriell anvendelse vil kunne være særlig aktuelt der norske militære styrker deltar i en internasjonal militær operasjon i utlandet. Hvis norske styrker ut fra de konkrete omstendigheter må anses å ha effektiv kontroll over et område, følger det av kriteriene beskrevet ovenfor at Norge i utgangspunktet vil ha ansvar for å sikre alle menneskerettighetene for de som befinner seg i området under norsk kontroll. Dersom de norske styrkene ikke kan anses å ha effektiv kontroll over et område, men har kontroll over en person, typisk ved frihetsberøvelse, vil også Norge ha et ansvar for å sikre de rettighetene som er relevante for situasjonen.

Hvor Norge verken utøver effektiv kontroll over et område eller har fysisk kontroll over en person, blir spørsmålet om Etterretningstjenesten ved sin innhentingsvirksomhet fra utlandet likevel kan sies å utøve myndighet og kontroll over personen innhentingen retter seg mot. Det er knyttet usikkerhet til dette spørsmålet. Tar man utgangspunkt i kriteriene EMD oppstiller som gjengitt over, taler ordvalget for at det kreves en form for *fysisk* kontroll over personen. EMD bruker ordene «circumstances where the State through its agents exercises control and authority over an individual outside its territory, such as using force to take a person into custody or exerting full physical control over a person through apprehension or

detention». Samtidig kan man hevde at sitatet bare er ment som en eksemplifisering fra EMD sin side, og at domstolen ikke nødvendigvis føler seg bundet av dette i en senere sak.

Innhentingen kan for det andre finne sted ved hjelp av innhentingsmetoder eller -kapasiteter som fysisk befinner seg på *norsk* territorium eller andre steder der det er klart at norsk jurisdiksjon gjelder, men som har *virkning* utenfor norsk territorium. Et typisk eksempel på dette vil være tekniske innhentingsdisipliner slik som kommunikasjonsetterretning. Her vil man fra norsk territorium kunne innhente informasjon om personer i utlandet, herunder kommunikasjon mellom personer i utlandet. Siden selve inngrepet, altså innhentingen, skjer på norsk territorium, kan det argumenteres for at territorialprinsippet kommer til anvendelse. Det kan imidlertid være mer nærliggende å anse informasjonsinnhentingen som en ekstraterritoriell handling fordi inngrepet i disse tilfeller har virkning for personer utenfor norsk territorium. Disse situasjonene må i så fall vurderes etter de samme kriterier som når informasjonsinnhentingen skjer fra utlandet uten at det utøves fysisk kontroll over personen innhentingen er rettet mot. Spørsmålet blir i så fall hvorvidt informasjonsinnhentingen kan anses å innebære utøvelse av myndighet og kontroll over personen som er gjenstand for informasjonsinnhentingen.

Spørsmålet ble berørt av EMD i saken *Weber og Saravia mot Tyskland* fra 29. juni 2006, hvor klagerne påberopte at Tyskland hadde brutt deres konvensjonsrettigheter i forbindelse med overvåkning av telekommunikasjon fra deres telefonforbindelser i Uruguay. Tyskland argumenterte blant annet med at:[19]

> «the monitoring of telecommunications made from abroad, however, had to be qualified as an extraterritorial act. In accordance with the Court's decision in the case of Bankovic and Others v. Belgium and Others (…) the applicants therefore did not come within Germany's jurisdiction within the meaning of Article 1 of the Convention – a concept which was primarily territorial – on account of that act"

Domstolen fant det ikke nødvendig å ta stilling til jurisdiksjonsspørsmålet i *Weber og Saravia mot Tyskland* siden klagen uansett måtte avvises fordi domstolen kom til at det ikke hadde funnet sted noe konvensjonsbrudd. I *Liberty m.fl. mot Storbritannia* fra 1. juli 2008 ble Storbritannia domfelt for brudd på EMK artikkel 8 for overvåkning av samtaler mellom en britisk og to irske organisasjoner basert i henholdsvis London og Dublin. Kommunikasjonen frem og tilbake mellom Dublin og London ble fanget opp på «Capenhurst Electronic Test Facility» på britisk territorium. Det ble ikke anført av Storbritannia i saken at EMK ikke kom til anvendelse på saksforholdet for så vidt gjaldt de irske klagerne, og EMD reiste heller ikke spørsmålet av eget tiltak.

All den tid EMD ikke har behandlet spørsmålet direkte er det vanskelig å forutsi hvordan domstolen vil forholde seg til kriteriene om myndighet og kontroll over en person eller effektiv kontroll over et område i fremtidige saker om grenseoverskridende overvåkning og utenlandsetterretning på annet lands territorium hvis spørsmålet skulle komme på spissen. Det kan ikke utelukkes at domstolen vil kunne oppstille ytterligere «eksepsjonelle omstendigheter» som kan nødvendiggjøre og berettige ekstraterritoriell jurisdiksjon utledet av EMK artikkel 1. EMD har tidligere uttalt som begrunnelse for unntakene fra hovedregelen om territorialprinsippet slik:

[19] *Weber og Saravia mot Tyskland* avsagt 29. juni 2006, avsnitt 66

> «Accountability in such situations stems from the fact that Article 1 cannot be interpreted so as to allow a State Party to perpetrate violations of the Convention on the territory of another State which it would not be permitted to perpetrate on its own territory."

Domstolen peker her på at det ikke er rimelig at konvensjonsstatene skal kunne foreta handlinger utenfor eget territorium som den ikke tillates overfor egne borgere. En slik ordning vil dessuten kunne oppmuntre til internasjonalt samarbeid, i dette tilfellet etterretningssamarbeid, for å omgå menneskerettsforpliktelsene på eget territorium. På den annen side kan slik omgåelse av konvensjonen unngås ved at statene gjør det forbudt for sine etterretningstjenester å be om informasjon fra samarbeidende tjenester som de ikke selv har hjemmel til å innhente. Dessuten kan det argumenteres for at innhenting av informasjon om personer som befinner seg på et statskontrollert territorium eller som på annen måte er underlagt statens myndighet og (fysiske) kontroll, lettere kan brukes, herunder misbrukes, mot vedkommende person av staten, enn når det gjelder informasjonsinnhenting rettet mot personer på andre staters territorium. Dette argumentet taler for at EMDs gjeldende kriterier for ekstraterritoriell jurisdiksjon ikke bør strekkes for langt.

Høyesterett uttaler i plenumsdommen inntatt i Rt. 2005 s. 833 avsnitt 45-46 med videre henvisninger at domstolene må være varsomme med å være like dynamiske som EMD i sin fortolkning av EMK. En slik praksis vil kunne føre til at norske domstoler i enkelte tilfeller går lenger enn det som er nødvendig i forhold til EMK, og således legge unødvendig bånd på norsk lovgivningsmyndighet. Av hensyn til den balanse mellom lovgivningsmyndighet og domstolsmyndighet som vår statsskikk bygger på, vil dette være uheldig. Høyesterett uttaler videre at norske domstoler, dersom det foreligger tvil om hvordan EMK skal forstås, ikke bør anlegge en for dynamisk tolking av konvensjonen. Som alminnelig regel kan norske domstoler ved tolkingen av EMK heller ikke bygge inn sikkerhetsmarginer for å sikre seg mot at Norge dømmes for konvensjonsbrudd. Uttalelsen fra Høyesterett gjelder direkte for domstolenes praktisering og tolking av menneskerettighetene. Vurderingen av om det skal bygges inn sikkerhetsmarginer for å ta høyde for en mulig utvikling av konvensjonen kan imidlertid også reises fra lovgivers perspektiv. Dersom lovgiver snevrer inn sitt demokratiske handlingsrom fordi man legger en for dynamisk tolking av konvensjonen til grunn, vil dette være uheldig ut fra demokratihensyn, samt at man kan risikere å basere seg på en forskuttert forståelse av EMK som EMD ikke nødvendigvis deler. Dette taler for at lovgiver forholder seg til den tolkningen av jurisdiksjonsbegrepet som allerede er utmeislet i EMDs praksis, og at man ikke legger antakelser om eventuell fremtidig utvidelse av konvensjonens anvendelsesområde til grunn for utformingen av nasjonalt regelverk.

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. Hva som skal til for å fastslå at det foreligger effektiv kontroll over et område eller myndighet og kontroll over person må vurderes ut fra EMDs praksis med utgangspunkt i faktum i den enkelte sak.

Når det er sagt vil Etterretningstjenestens personell være bundet av den regulering som følger av etterretningstjenesteloven uansett hvor de oppholder seg. Dette lovforslaget er utformet for å tilfredsstille menneskerettighetene uavhengig av utfallet av hver enkelt konkrete jurisdiksjonsvurdering som pekt på over. Lovforslaget er generisk og legger ikke opp til å differensiere normeringen ut ifra hvor eller overfor hvem en gitt aktivitet finner sted. I

så måte kan man si at regelverket er utformet nasjonalitets- og geografinøytralt, og at prinsipper og krav som utledes av våre menneskerettslige forpliktelser således i praksis blir anvendt overfor alle individer Etterretningstjenesten får befatning med. En nøytral utforming er ikke et resultat av en rettslig forpliktelse, men gjøres av policy- og praktiske hensyn. Det presiseres at utfallet av en konkret jurisdiksjonsvurdering i enkelte tilfeller vil kunne få betydning, slik som spørsmålet om hvem som kan påberope krav om effektive rettsmidler etter EMK. Dette spørsmålet drøftes nærmere i punkt 4.3 under.

4.1.4 Hvilke menneskerettighetsforpliktelser må vurderes i tilknytning til Etterretningstjenestens utøvelse av sin virksomhet?

En vurdering av hvilke menneskerettigheter Etterretningstjenesten kan komme i berøring med innebærer blant annet å konkretisere hvilke sivile og politiske rettigheter som kan bli krenket ved tjenestens virksomhet. Det er imidlertid også imperativt å se hen til en av statens mest grunnleggende forpliktelser overfor borgerne, nemlig å ivareta statens suverenitet og borgernes trygghet. Staten har en plikt til å ivareta borgernes rett til liv, frihet og sikkerhet. I dette ligger blant annet at staten må bygge opp nødvendige strukturer og mekanismer for å sikre borgernes grunnleggende rettigheter. I denne forbindelse kan man problematisere hvorvidt det kan kreves at staten engasjerer seg for å oppdage og avverge ytre trusler mot statens innbyggere. Dette diskuteres nærmere i punkt 4.2.2 under.

Etterretningstjenestens aktivitet kan potensielt gripe inn i flere ulike individuelle rettigheter. Retten til respekt for privatlivet står særlig sentralt, slik denne kommer til uttrykk i Grl. § 102 og EMK artikkel 8. Tjenestens virksomhet kan også tenkes å gripe inn i andre rettigheter slik som pressens rett til å verne om sine kilder, som er et viktig aspekt ved ytringsfriheten etter både Grl. § 100 og EMK artikkel 10. Visse former for overvåkning antas også å kunne gjøre et inngrep i forenings- og forsamlingsfriheten etter Grl. § 101 og EMK artikkel 11, eller religionsfriheten etter Grl. § 16 og EMK artikkel 9. Felles for alle disse er at de sikrer viktige sivile og politiske rettigheter for innbyggerne. Hvilken adgang myndighetene har til å gjøre inngrep i rettighetene vil vurderes i det følgende.

4.1.5 Begrensningshjemmel

Grunnlovens menneskerettsbestemmelser som Etterretningstjenesten kan komme til å gjøre inngrep i er etter sin ordlyd formulert som absolutte rettigheter.[20] De tilsvarende rettighetene i EMK er akkompagnert av tilhørende unntaksbestemmelser.[21] Menneskerettighetsutvalgets flertall foreslo å grunnlovsfeste en generell begrensningshjemmel i Grunnlovens menneskerettighetskapittel.[22] Utvalget mente at begrensningen i rettighetene burde fremgå av Grunnloven som sådan, og ikke bare følge av domstolenes praksis. Utvalget begrunnet dette med at en grunnlovfesting ville tydeliggjøre at de fleste rettigheter i noen utstrekning vil kunne være gjenstand for begrensninger dersom de støter an mot andres menneskerettigheter eller mot viktige samfunnsinteresser.

[20] Bare Grl. § 100 har enkelte unntak inntatt i ordlyden, men disse vil ikke være relevante for Etterretningstjenestens virksomhet.

[21] Disse bestemmelsene i EMK følger et system der rettigheten følger av bestemmelsens første ledd og unntaksadgangen reguleres i andre ledd.

[22] Dokument 16 (2011-2012) punkt 11.4 side 62

Stortinget valgte ikke å vedta begrensningshjemmelen som en egen bestemmelse i Grunnloven. Det er likevel ikke tvil om at inngrep i menneskerettighetene kan finne sted. Det følger av Grunnlovens system at de vidt formulerte rettighetene både må balanseres mot hverandre og mot fellesskapets interesser. Dette er også fastslått i rettspraksis – Høyesterett har allerede prøvd rekkevidden av rettighetsvernet av de nye menneskerettighetsbestemmelsene flere ganger. Førstvoterende uttalte i Rt 2018 s. 1105 avsnitt 28 at det gjelder en alminnelig forholdsmessighetsbegrensning for «lovhjemlede og saklig begrunnede inngrep i rettighetene og frihetene fastsatt i Grunnlovens menneskerettsbestemmelser». Førstvoterende trakk deretter parallellen til de tilsvarende bestemmelsene i EMK og SP, som også oppstiller krav til lovforankring og en forholdsmessighetsvurdering. Det samme synspunktet ble ytterlige utdypet av Høyesterett i Rt. 2015 s. 93, avsnitt 60:

> «Til forskjell fra SP artikkel 17 og EMK art. 8, inneholder Grunnloven § 102 ingen anvisning på om det overhodet kan gjøres lovlige begrensninger i privat- og familielivet. Men grunnlovsvernet kan ikke være – og er heller ikke – absolutt. I tråd med de folkerettslige bestemmelsene som var mønster for denne delen av § 102, vil det være tillatt å gripe inn i rettighetene etter første ledd første punktum dersom tiltaket har tilstrekkelig hjemmel, forfølger et legitimt formål og er forholdsmessig, jf. Rt. 2014-1105 avsnitt 28. Forholdsmessighetsvurderingen må ha for øye balansen mellom de beskyttede individuelle interessene på den ene siden og de legitime samfunnsbehovene som begrunner tiltaket på den andre.»

Det er følgelig ikke omstridt at det er adgang til å gjøre inngrep i menneskerettighetsbestemmelsene i Grunnloven.

4.2 Balansen mellom den enkeltes rettigheter og nasjonal sikkerhet

4.2.1 Generelt

Balansen mellom Etterretningstjenestens samfunnsoppdrag og hensynet til beskyttede individuelle rettigheter og andre grunnleggende verdier kommer til uttrykk allerede i dette lovforslagets § 1 om lovens formål. Formålet med loven, og dermed også formålet med Etterretningstjenestens virke, er å bidra til å trygge Norges suverenitet, territorielle integritet, demokratiske styreform og andre nasjonale sikkerhetsinteresser, herunder å forebygge, avdekke og motvirke utenlandske trusler mot Norge og norske interesser. Loven skal dessuten sørge for at Etterretningstjenestens virksomhet utøves i samsvar med menneskerettighetene og folkeretten for øvrig, og i samsvar med andre grunnleggende rettsprinsipper og verdier i et demokratisk samfunn. Det er et viktig premiss at loven bidrar til å trygge tilliten til og sikrer grunnlaget for kontroll med Etterretningstjenestens virksomhet.

Som nevnt innledningsvis i dette kapittelet setter menneskerettighetene skranker for Stortingets lovgivningskompetanse. I så måte kunne det være ønskelig å tegne opp en klar grense for hvilket handlingsrom lovgiver har til å fastsette bestemmelser på etterretningsfeltet. Kjernen i de individuelle rettighetene er nokså klare. Men en presis angivelse av rekkevidden av de enkelte rettighetene er mer krevende å fastslå én gang for alle. Menneskerettsinstrumentene er gjenstand for en dynamisk utvikling som er preget av samfunnsutvikling og rettsoppfatning ikke bare hos oss, men vel så mye internasjonalt. Dessuten vil mangfoldet av tenkte scenarioer innenfor Etterretningstjenestens

aktivitetsspekter innebære at den konkrete vektingen av individuelle rettigheter opp mot samfunnets behov vil slå ulikt ut i ulike tilfelle. Til dette kommer at det ikke bare er *utformingen* av lovverket, men også *praktiseringen* av det som må holdes innenfor de menneskerettslige krav for at nasjonale og overnasjonale domstoler ikke skal konstatere krenkelse. Høyesterett har avvist at man i norsk regelverksutforming må innbake en sikkerhetsmargin for å sikre at regelverket ikke strider mot EMK.[23] Samtidig er det ikke ønskelig å vedta regelverk som balanserer hårfint på grensen av det som antas akseptabelt etter konvensjonsforpliktelsene. Å vedta et godt og balansert regelverk som ivaretar både fellesskapets og individenes rettigheter bør derfor være den overordnede målsetningen.

I det følgende vil det gjøres rede for de mest sentrale prinsipper og rettigheter som det må tas hensyn til i utformingen av forslaget til ny etterretningstjenestelov.

4.2.2 Statens plikt til å beskytte borgernes grunnleggende rettigheter

4.2.2.1 Generelt

Nasjonalstatens mest grunnleggende oppgave er å ivareta statens suverenitet og innbyggernes sikkerhet. Grunnleggende verdier for vår stat og statsform – å sikre demokratiet, rettsstaten og menneskerettighetene – er nedfelt i Grunnloven § 2. Det overordnede formålet med Etterretningstjenestens virksomhet er å bidra til å verne om Norge som en fri og selvstendig stat, som nettopp er en forutsetning for at vi kan ha en fungerende rettsstat og et demokratisk styresett. Borgerne har således en berettiget forventning om at staten gjør det den kan for å ivareta både statens eksistens og handlefrihet og borgernes sikkerhet. Ivaretakelsen av disse forpliktelsene kan måtte balanseres mot andre rettigheter borgerne har.

4.2.2.2 Beskyttelse av grunnleggende rettigheter

Positive menneskerettighetsforpliktelser kan utledes både av Grunnloven og EMK.[24] EMK artikkel 1 pålegger konvensjonsstatene å sikre konvensjonens rettigheter for alle innenfor statens jurisdiksjon. Selv om det er statene som er pliktsubjektene etter menneskerettskonvensjonene, vil kravet i EMK artikkel 1 også etter forholdene kunne pålegge statene en plikt til å ta aktive skritt for å hindre at private krenker hverandre. Konvensjonen har i denne forstand horisontal virkning.[25]

På generelt grunnlag kan man si at staten har en plikt til å sørge for at personer ikke utsettes for unødig risiko. I denne forbindelse er det imidlertid en betingelse at staten på det relevante tidspunktet har eller burde hatt nødvendige opplysninger om en risikofaktor som burde være eliminert. Myndighetene kan altså ikke forholde seg passive til risiko som den kjenner eller burde kjenne til.[26] Forpliktelsen kan likevel ikke tolkes til å legge umulige eller

[23] Se Rt. 2000 s. 996 s. 1008 og Rt. 2005 s. 833 avsnitt 46

[24] Se blant annet Grunnloven § 93 og EMK artikkel 2, 3 og 5.

[25] Se Rt. 2013 s. 588 avsnitt 41 med videre henvisninger.

[26] Se Osman-testen i EMD, jf *Osman mot Storbritannia 28. oktober 1998* (166) «[..] it must be established to its satisfaction that the authorities *knew or ought to have known* at the time of the existence of a real and immediate risk to the life of an identified individual or individuals, from the criminal acts of a third party, and that they *failed to take measures* within the scope of their powers which, judged reasonably, might have been expected to avoid that risk."

uproporsjonale krav på staten.[27] Staten kan altså ikke forventes å hindre enhver krenkelse, og bestemmelsen kan følgelig ikke leses som en resultatforpliktelse. Vurderingstemaet er følgelig om staten i rimelig grad har iverksatt adekvate beskyttelsestiltak, og kravene som stilles til tiltakene må være realistiske og forholdsmessige. Høyesteretts avgjørelse inntatt Rt. 2013 s. 588 kaster lys over sentrale vurderingsmomenter for å klarlegge statens forpliktelser.[28]

Et særlig spørsmål er hvorvidt en stat kan sies å ha en plikt til å beskytte borgerne mot krenkelser på statens territorium, der krenkelsen har sin opprinnelse *utenfor* landets grenser, gjennom utenlandsetterretning. Utenlandsetterretning vil naturligvis ikke *i seg selv* avverge en menneskerettskrenkelse, men *tilgang til informasjon* vil alltid være en viktig faktor for å kunne oppdage en trussel, eller annet som kan resultere i en krenkelse, og anses dermed som en nødvendig forutsetning for avvergelsen.

EMD har i sin praksis særlig vektlagt statens plikt til å gi lovgivning og administrative systemer som sikrer borgernes rettigheter innenfor eget territorium. Spørsmålet er om forpliktelsene kan tolkes til å pålegge staten en plikt til å beskytte innbyggerne også mot risiko som har sitt opphav utenfor statens territorium. Det kan være ulike oppfatninger om dette. Betydningen av informasjonsinnhenting om omverdenen bør imidlertid ikke underdrives. Innhenting av informasjon er avgjørende for å kunne kartlegge potensielle trusselaktørers evner og ambisjoner og faktiske trusler mot staten eller innbyggerne. Informasjonen som innhentes fungerer som beslutningsgrunnlag for konkrete handlinger fra myndighetenes side, som igjen skal bidra til å ivareta statens og innbyggernes sikkerhet. Dersom statens reelle adgang til å innhente informasjon om omverdenen begrenses i for stor grad er det grunn til å hevde at dette vil gå ut over både statens og innbyggernes sikkerhet. Nasjonale strafferegler og nasjonalt politi vil gjennom sin preventive og avvergende effekt kunne bidra til å sikre innbyggerne mot trusler som har sin opprinnelse internt i staten, men vil i liten grad evne å motvirke eller avskrekke fremmede trusler som har sin opprinnelse utenfor landets grenser. Det er ingen grunn til å forvente at trusler med opprinnelse fra utlandet er mindre potente enn truslene med intern opprinnelse.

---

[27] «Such an obligation must be interpreted in a way which does not impose an impossible or disproportionate burden on the authorities, bearing in mind the difficulties involved in policing modern societies, the unpredictability of human conduct and the operational choices which must be made in terms of priorities and resources» jf. *Mastromatteo mot Italia* 24.10.2002 avsnitt 68, som viser til *Osman mot Storbritannia* avsnitt 116.

[28] Saken gjaldt et søksmål fra en kvinne som anførte at staten hadde gjort for lite for å hindre at hun ble utsatt for forfølgelse av en mann hun hadde hatt et kortvarig forhold til. Forfølgelsen hadde pågått i flere år og hadde medført at kvinnens livskvalitet var blitt vesentlig forringet. Høyesterett kom til at staten ikke hadde oppfylt sin plikt til å sikre kvinnen mot forfølgelse fra gjerningsmannen. Høyesterett uttalte i dommen at sikringsplikten etter EMK artikkel 1 er presisert og utviklet gjennom mange avgjørelser fra EMD, og trakk deretter frem fire hovedkomponenter som har vært gjennomgående i EMDs praksis. Disse angis av Høyesterett å være; 1) at staten plikter å reagere mot reell og umiddelbar risiko som myndighetene er kjent med, eller burde være kjent med, med de tiltak som det ut fra situasjonen er rimelig å forvente; 2) at nasjonale myndigheter er nærmest til å vurdere hva som er den beste måten å reagere på; 3) at det under EMK er en forventing om at tiltak blir gjennomført på en måte som innebærer at de bidrar til reell beskyttelse, og at det at det besluttes beskyttelsestiltak ikke i seg selv er tilstrekkelig, men at disse også må settes ut i livet og håndheves; og 4) at kravene til aktivitet fra myndighetenes side vil bero på det aktuelle saksområdet.

Grenseoverskridende terrorisme er et aktuelt eksempel på dette.[29] Gode grunner tilsier derfor at staten, i alle fall i en viss utstrekning, plikter å etablere strukturer som evner å motvirke fremmede trusler utenfra for å ivareta borgernes grunnleggende rettigheter.

Aktivitet i det digitale rom kan også fungere som et eksempel. Dersom internasjonale terrorister bryter seg inn i norske datamaskiner og benytter seg av norske identiteter og datautstyr for å rute et angrep videre mot et angrepsmål, kan det anføres at denne handlingen utgjør et inngrep i privatlivet til de som eier identitetene og datamaskinene. Spørsmålet i denne forbindelse er hvilken plikt staten har til å forsøke å avverge denne formen for krenkelse av privatlivet til landets borgere dersom staten er kjent med at slik aktivitet sannsynligvis finner sted.[30]

Det finnes ikke relevant rettspraksis fra norske eller overnasjonale domstoler som behandler forholdet mellom sikringsplikten og utenlandsetterretning direkte. Dette i seg selv betyr imidlertid ikke at spørsmålet er uten betydning. Domstolene behandler de rettsspørsmål som de får seg forelagt i den enkelte sak, og rettspraksis gir dermed ingen fullgod oversikt over hvilke problemstillinger som i praksis kan reises. At krenkelse av en individuell rettighet kan ha sin opprinnelse utenfor landets grenser er imidlertid klart. Det avgjørende bør derfor være hvilken reell og umiddelbar risiko myndighetene er eller burde være kjent med, og hvilke tiltak det er rimelig at myndighetene foretar seg for å ivareta borgernes rettigheter. Hva som konkret kreves må vurderes i det enkelte tilfellet. At vi i dag står ovenfor en situasjon der landegrensenes betydning blir satt på prøve, både på grunn av den digitale utviklingen, men også fordi mennesker og trusler forflytter seg mellom land med en annen frekvens enn tidligere, er godt kjent. Dette er trender som vil fortsette. Digitale angrep og terror vil kunne innebære en alvorlig krenkelse av private norske borgeres grunnleggende rettigheter begått av andre private borgere. Når en manglende evne til å fange opp alvorlige trusler er kjent og dokumentert, oppstår spørsmålet om hvilke tiltak det ut fra situasjonen er rimelig å forvente at norske myndigheter iverksetter for å bøte på denne svakheten. Den konkrete vurderingen av dette spørsmålet er behandlet i kapittel 11.

4.2.3 Den enkeltes rett til respekt for privatliv, familieliv, hjem og kommunikasjon

4.2.3.1 Generelt

I vurderingen av hvilke individuelle menneskerettigheter Etterretningstjenestens aktiviteter kan gripe inn i, står retten til respekt for privatlivet særlig sentralt. Denne rettigheten følger av både Grunnloven § 102, EMK artikkel 8 og SP artikkel 17. Bestemmelsene fastslår et vern for privatlivets fred og personlig integritet. Forholdet mellom Grunnlovens menneskerettighetsbestemmelser og bestemmelsene i EMK er behandlet over. SP artikkel 17 antas ikke å gi et større vern enn de to øvrige bestemmelsene, og behandles derfor ikke i det følgende.

4.2.3.2 Grunnloven § 102

Grunnloven § 102 lyder:

[29] Samtidig har EMD slått fast at artikkel 2 ikke kan fortolkes slik at den garanterer beskyttelse av enkeltpersoner mot terrorisme, se *M. mot Storbritannia og Irland* avsagt 4. mars 1985.

[30] Statens plikt til å hindre at statens territorium brukes som utgangspunkt for å utøve angrep mot andre stater er et annet spørsmål. Dette har imidlertid ingen direkte sammenheng med menneskerettighetene og behandles derfor ikke i dette kapittelet.

Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller.

Statens myndigheter skal sikre et vern om den personlige integritet.

Menneskerettighetsutvalget var opptatt av betydningen av å grunnlovsfeste retten til privatlivets fred, personvernet og personopplysningsvernet. De uttaler på side 175 i rapporten:

> «En grunnlovsfesting av privatlivets fred, personvern og personopplysningsvern vil i første rekke ha den konsekvens at disse prinsippene får en generell forankring i Grunnloven. Dette vil synliggjøre at den fragmentariske lovgivningen på området og det ulovfestede vernet etablert av domstolene, springer ut av en grunntanke om at det finnes en privatsfære som omverdenen ikke har krav på innsyn i, men som tvert imot har krav på beskyttelse mot slikt innsyn.»

Det generelle vernet for privatlivets fred i § 102 første ledd første punktum er utformet som en individuell rettighet. Menneskerettighetsutvalget fremhever i sin rapport at inngrep i disse rettighetene normalt vil oppleves som så krenkende at det er viktig at slike inngrep vurderes nøye i lovgivningsprosessen og at de kan prøves for domstolene dersom lovgiver har gått for langt i å tillate slike inngrep. Utvalget uttaler at «[i] en viss forstand kan man si at dette utgjør kjernen i den private sfære, der den enkelte har krav på et særlig vern mot krenkelser.»[31] At rettigheten følger av Grunnloven innebærer at den fungerer som en skranke og rettesnor for lovgiver.

Det er samtidig klart at vernet om den private sfære etter § 102 første ledd ikke kan forstås som at den enkelte har en udelt rett til å ha sitt privatliv i fred. Som på de fleste andre områder i samfunnet må man balansere ulike og ofte motstridende hensyn. Menneskerettighetsutvalget legger dette til grunn i sin vurdering der de uttaler at:[32]

> «Formuleringen utelukker derfor ikke at enkelte personer kan utsettes for overvåkning og kontroll, men da må vilkårene for dette være tilstede[..]».

Utvalget går videre til å minne om at under utøvelsen av slik overvåkning og kontroll må det utvises respekt for privatlivet:

> «I dette ligger at overvåkning og kontroll kun kan finne sted så langt det er nødvendig for å avdekke alvorlige kriminelle forhold, av hensyn til rikets sikkerhet el.l.»

De samme hensyn blir også fremhevet av flertallet i kontroll- og konstitusjonskomiteens innstilling:[33]

> «Det alternativ flertallet stiller seg bak, gjør retten til privatliv mv. i første rekke til en rettighet for den enkelte. Når retten er til «respekt for» privatlivet, er det likevel grunn for å synliggjøre at lovlig etterretning ikke er utelukket, som også diskutert av Menneskerettighetsutvalget.»

Grunnloven § 102 første ledd annet punktum, det såkalte husransakelsesforbudet, gir en særskilt beskyttelse av privatlivssfæren i det private hjem. Forbudet innebærer at offentlige myndigheter ikke kan foreta undersøkelser i private hjem på en måte som er egnet til å medføre krenkende mistanke mot den undersøkelsen rettes mot. Slike husransakelser

[31] Dokument 16 (2011-2012) s. 177

[32] Ibid s. 178

[33] Dette gjaldt representantene fra AP, Høyre og Frp, se Innst. 186 S (2013-2014)

tillates bare i «kriminelle tilfeller». Justis- og beredskapsdepartementet vurderte rekkevidden av forbudet sett opp mot politiets adgang til å bruke skjulte tvangsmidler i avvergende og forebyggende øyemed i forarbeidene til endringer i straffeprosessloven.[34] Spørsmålet der var om slike kriminalitetsforebyggende tiltak faller innenfor «kriminelle tilfeller» eller om det gjelder krav om at en straffbar handling må være påbegynt eller begått.

Det finnes lite rettspraksis på området. Høyesterett fastholder i Rt 2004 s. 1723 at forvaltningskontroller som har til hensikt å etterse oppfyllelsen av regelverk ikke kommer i strid med husransakelsesforbudet. Det samme har vært forutsatt i lovgivning og juridisk teori.

Etterretningsvirksomhet for utenlandsformål har ikke sammenheng med straffeforfølgelse og har ikke til hensikt å samle bevis, forberede rettslig forfølgelse eller på annen måte medføre krenkende mistanke mot den undersøkelsen rettes mot. Utenlandsetterretning innebærer heller ikke noen form for forvaltningskontroll. Det er nærliggende å legge til grunn at utøvelsen av utenlandsetterretning ikke var i lovkonsipistenes tanker ved utformingen av bestemmelsen i 1814.[35] Departementet vil samtidig ikke forskuttere hvordan domstolene ville tolket bestemmelsen dersom denne skulle komme på spissen i en konkret sak. Departementet anser dette imidlertid som lite sannsynlig all den tid Etterretningstjenesten verken etter dagens lov eller lovforslaget her vil ha anledning til å foreta husransakelser i Norge som krenker borgernes private hjem.

4.2.3.3 EMK artikkel 8

EMK artikkel 8 lyder:

> 1. Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.
>
> 2. Det skal ikke skje noe inngrep av offentlig myndighet i utøvelsen av denne rettighet unntatt når dette er i samsvar med loven og er nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter.

EMK artikkel 8 nr. 1 oppstiller et generelt vern for privatlivets fred. Det fremgår av bestemmelsen at vernet omfatter den enkeltes privatliv og familieliv, sitt hjem og sin korrespondanse. Det kan være utfordrende å skulle trekke et presist skille mellom disse alternativene, og EMD har heller ikke bestrebet seg på noen klar grensegang mellom begrepene. Alternativene blir snarere oppfattet som delvis overlappende sekkebegreper enn som konkrete angivelser, hvorav det første, «privatliv», er vidt nok til å konsumere de øvrige.

Som andre bestemmelser vil også artikkel 8 ha en kjerne og en yttergrense. Akkurat hvor grensen går lar seg ikke uten videre fastslå, og fremstillingen av bestemmelsen i juridisk teori konsentrerer seg heller om eksempler fra en rikholdig EMD-praksis, enn et forsøk på presis ordlydstolking. Man kan se begrepene som innbyrdes styrkende, og at det finnes en form for overordnet «privatlivsbegrep» som bygges opp av de fire begrepene. Vi ser også at rekkevidden av artikkel 8 kan overlappe med andre rettigheter etter EMK, slik som

[34] Prop. 68 L (2015-2016) Endringer i straffeprosessloven mv. (skjulte tvangsmidler) i punkt 5.1.3.2 side 34-38

[35] Det gjøres nærmere rede for lovbestemmelsens bakgrunn og formål i Rt. 2004 s. 1723 avsnitt 43-44.

ytringsfrihet, trosfrihet, forsamlingsfrihet mv. På engelsk sammenfattes rettighetene etter artikkel 8 gjerne som en rett til «privacy».

EMD tolker EMK i lys av reglene i Wienkonvensjonen om traktatretten.[36] Dette betyr at domstolen avklarer den vanlige meningen av begrepene i sin sammenheng og i lys av konvensjonens gjenstand og formål. Etter sin ordlyd favner artikkel 8 nr. 1 vidt. Når det gjelder hvilken type opplysninger som er omfattet av bestemmelsen har EMD sett hen til Europarådets personvernskonvensjon. Etter denne omfattes «enhver opplysning som gjelder en bestemt eller identifiserbar enkeltperson».[37]

Etterretningstjenestens ulike former for fordekt innhenting av informasjon om personer og påfølgende registrering av personopplysninger vil utgjøre et inngrep såfremt innhentingen finner sted i den private sfære. Innhenting av opplysninger fra åpne kilder eller det offentlige rom vil som utgangspunkt ikke dekkes av retten til privatliv. EMD har omtalt at begrepet «privatliv» og «hjem» ikke får anvendelse på steder der offentligheten har fri adgang og som dermed ikke tilhører individets privatsfære.[38] Å samle inn åpent tilgjengelig informasjon om personer eller holde dem under oppsikt på offentlig sted vil normalt ikke utgjøre et inngrep.[39] Dette er handlinger som enhver, inklusive myndighetene, kan gjøre med hjemmel i den alminnelige handlefrihet. Mer systematiske former for innhenting og spaning vil derimot utgjøre et inngrep i privatlivet. [40] Dessuten vil systematisk innsamling og systematisering av offentlig tilgjengelige opplysninger etter forholdene kunne utgjøre et inngrep, særlig dersom opplysningene vedrører forhold som ligger langt tilbake i tid.[41] I saken *Uzun mot Tyskland* uttaler EMD at en person utenfor sitt private hjem og sfære må kunne forvente å være synlig for andre, men ved mer systematisk innsamling vil privatlivsbetraktningene gjøre seg gjeldende jf. domstolens uttalelse i avsnitt 44-45:

> «Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain [..].
>
> Further elements which the Court has taken into account in this respect include the question whether there has been compilation of data on a particular individual, whether there has been processing or use of personal data or whether there has been publication of the material concerned in a manner or degree beyond that normally foreseeable. ”

Domstolen uttaler videre i avsnitt 46 i samme sak:

> “[T]he Court has considered that the systematic collection and storing of data by security services on particular individuals, even without the use of covert surveillance methods, constituted an interference with these persons’ private life.” [42]

---

[36] Vienna Convention on the Law of Treaties, May 23 1969

[37] Se bla. EMDs avgjørelse *Rotaru mot Romania* avsagt 4. mai 2000. avsnitt 42-43

[38] *Steel and Morris mot Storbritannia* avsagt 22. oktober 2002

[39] Se Jørgen Aall, *Rettsstat og menneskerettigheter* (2015), s. 123

[40] *Peck mot Storbritannia* avsagt 28. januar 2003

[41] Se Kjølbro, *Den europæiske menneskerettigheds konvention for praktikere*, (2017) s. 859 og EMDs avgjørelse i *Rotaru mot Romania* avsagt 4. mai 2000 om en etterretningstjenestes registrering av opplysning om studier, politiske aktiviteter og tidligere straff.

[42] *Uzun mot Tyskland* avsagt 2. september 2010

Ikke bare individer, men også selskaper er vernet etter EMK art. 8.[43] Innhenting av opplysninger som ikke retter seg mot fysiske eller juridiske personer, omfattes ikke av artikkel 8.

Avlytting eller annen form for innhenting av kommunikasjon i transitt vil omfattes av begrepet «korrespondanse» i artikkel 8 første ledd. Uttrykket «korrespondanse» favner bredt og omfatter umiddelbar kommunikasjon med andre. Begrepet er teknologinøytralt, og mange nye kommunikasjonsformer har kommet til siden bestemmelsens vedtakelse. Det må som utgangspunkt gjelde et krav om at avsender og mottaker forventer at kommunikasjonen blir formidlet uten at andre kan gjøre seg kjent med innholdet. Følgelig vil for eksempel kommunikasjon ved bruk av radiosender som anvender en frekvens som også andre lovlig kan benytte, neppe være omfattet.[44] EMD har lagt til grunn at ikke bare innsamling av innhold i kommunikasjon, men også av trafikkdata og metadata (som er data om kommunikasjon) er et inngrep i privatlivet.[45]

Innsamling av kommunikasjon utgjør et inngrep i seg selv, men det gjør også senere lagring og bruk av informasjonen.[46] Å dele informasjonen man har samlet inn vil utvide gruppen som har kjennskap til de personlige opplysningene og dette utgjør dermed et selvstendig inngrep i privatlivet.[47] Også selve eksistensen av lovgivning som tillater hemmelig overvåkning av kommunikasjon kan utgjøre et inngrep i privatlivet selv om klageren selv ikke har vært overvåket.[48]

Både en persons fysiske og psykiske integritet er omfattet av vernet mot inngrep i den private sfæren etter EMK artikkel 8. Formålet med bestemmelsen er å gi individene rett til selv å råde over seg og sitt, uten innblanding utenfra, også kalt integritetsperspektivet. Bestemmelsen tolkes dessuten til å favne det å forholde seg til andre og å utvikle sin egen personlighet.

Informasjonsinnhenting om enkeltpersoner kan potensielt lede til inngrep i alle fire kategorier i artikkel 8 nr. 1. Oftest vil inngrep i privatlivet være aktuelt, gjerne kombinert med korrespondanse. Inngrepet som gjøres vil være i den psykiske og ikke i den fysiske integritet.

4.2.4 Andre rettigheter

Det er ikke skarpe grenser mellom hva som utgjør en rett til privatliv og hva som er forbundet med andre individuelle rettigheter slik som tanke-, samvittighets- og religionsfrihet og forsamlings-, organisasjons- og ytringsfrihet. Sett i en større sammenheng kan alle disse rettighetene gripe inn i hverandre og en klar grensedragning kan være vanskelig å trekke. Det vil føre for langt å gi noen grundig redegjørelse av de enkelte rettigheter her. Retten til

[43] *Societé Colas Est mfl. mot Frankrike* avsagt 16. april 2002

[44] Kjølbro, *Den europæiske menneskerettigheds konvention for praktikere* (2017), s. 794

[45] *Malone mot Storbritannia* avsagt 2. august 1984, avsnitt 84

[46] Se bla. *Leander mot Sverige* avsagt 26. mars 1987, avsnitt 48

[47] Se *Weber og Savaria mot Tyskland* avsagt 29. juni 2006, avsnitt 79

[48] Dette er fastslått av EMD i flere saker, se blant annet *Weber og Savaria mot Tyskland avsagt* 29. juni 2006, avsnitt 78 med videre henvisninger

privatliv er den mest sentrale rettigheten å vurdere opp mot Etterretningstjenestens virksomhet, og dermed også den som vies mest oppmerksomhet.

Ytringsfriheten, og som del av denne, kommunikasjonsvernet,[49] er temaer som må vurderes. Etterretningstjenestens virksomhet vil ikke fysisk eller direkte hindre noen fra å ytre seg. Spørsmålet er imidlertid om Etterretningstjenestens adgang til å innhente informasjon kan ha en nedkjølende effekt på folks vilje til å ytre seg fritt fordi de frykter at ytringene ufrivillig kan komme Etterretningstjenesten i hende. Dette betegnes som *nedkjølingseffekten* («chilling effect»). Nedkjølingseffekten indikerer at noen avstår fra å ytre noe de ellers ville gjort, eventuelt modifiserer eller sensurerer egne ytringer, fordi de frykter at ytringene overvåkes av myndighetene. Problemstillingen ble reist i Lysne II-utvalgets rapport om digitalt grenseforsvar, og er av mange løftet frem som viktig i den offentlige høring og debatt av Lysne II-utvalgets forslag.

Lysne II-utvalget påpeker at dersom nedkjølingseffekten er reell vil dette ha en negativ innvirkning på den demokratiske debatten, og vil særlig kunne ramme de som befinner seg i randsonene for hva som er gjengs oppfatning i samfunnet. Dette er en ikke ønskelig utvikling for et demokrati som Norge. Lysne II-utvalget viser til at det så langt finnes få objektive studier av fenomenet, men at det i kjølvannet av Snowden-avsløringene har kommet noen undersøkelser som taler i retning av at fenomenet eksisterer. Det vises til omtale av disse i Lysne II-rapporten. Det vises også til teorien om Panoptikon der *muligheten* for overvåkning bidrar til endret adferd. Det at innsatte i fengsler som er bygget etter panoptikon-modellen oppfører seg *som om* de er overvåket, selv om de vet at overvåkningen ikke er konstant, er et eksempel på dette. Spørsmålet om nedkjølingseffekt kommer først og fremst på spissen ved aktivitet som omfatter mye overskuddsinformasjon. Overskuddsinformasjon er informasjon som ikke er relevant i henhold til Etterretningstjenestens oppgavesett. Problemstillingen vil derfor drøftes nærmere i kapittel 11 om særregler for tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon.

Et fungerende demokrati og åpen debatt forutsetter at det foreligger ytringsfrihet. Ytringsfrihet forutsetter på sin side tilgang til kommunikasjonskanaler, både i det fysiske, men også i det digitale rom. Kommunikasjonsvernet beskytter informasjon som er i transitt og har en side både til ytringsfriheten og til personvern. Også pressens kildevern har sammenheng med ytringsfriheten. Kommunikasjons- og kildevernet er omtalt i høringsnotatet punkt 11.8.2.1 og punkt 12.10 og i punkt 6.5 i Lysne II-utvalgets rapport.

4.2.5 Myndighetenes adgang til å gjøre inngrep i borgernes rettigheter

4.2.5.1 Generelt

Som redegjort for i punkt 4.1.5 over, er de ulike menneskerettighetene ikke uttømmende balansert mot hverandre, og det enkelte individs rettigheter kan dermed komme i konflikt med en annens menneskerett eller med fellesskapets og allmennhetens interesser. Inngrep i de individuelle rettighetene kan bare tillates dersom det foreligger hjemmel i nasjonal lov, inngrepet forfølger et legitimt formål og anses nødvendig i et demokratisk samfunn.[50]

[49] Se rapport fra Lysne II-utvalget om Digitalt grenseforsvar av 26. august 2016 s. 34

[50] Se hhv. EMK artikkel 8 nr. 2, artikkel 9 nr. 2, artikkel 10 nr. 2 og artikkel 11. nr 2

Den nedre grensen for hva som utgjør et menneskerettslig inngrep kan være vanskelig å trekke og det vil avhenge av hvilken individuell rettighet det er snakk om. Normalt må det foreligge et konkret inngrep rettet mot klageren.

Som beskrevet i punkt 4.1.5 fremgår ikke adgangen til å gjøre inngrep i menneskerettighetene uttrykkelig av Grunnloven, men må innfortolkes i praksis. Grunnlovens kapittel E om menneskerettigheter er dessuten et forholdsvis nytt kapittel. Selv om Grunnloven har trinnhøyere rang, er EMDs praksis knyttet til myndighetenes inngrepsadgang etter EMK derfor langt mer rikholdig enn Høyesteretts praksis knyttet til Grunnloven. For drøftelsens del er det derfor mest hensiktsmessig å ta utgangspunkt i EMDs praksis for å fastslå de rettslige rammene for inngrepsadgangen.

4.2.5.2 Lovkravet

Inngrep i borgernes rettssfære må ha hjemmel i lov. Legalitetsprinsippet er behandlet i punkt 4.1.1 over. Også EMK oppstiller som et grunnvilkår at et inngrep i konvensjonens rettigheter og friheter må være «in accordance with the law»/«prescribed by law».[51] Når Høyesterett har innfortolket en tilsvarende inngrepsadgang i Grunnloven som etter EMK, har forutsetningen vært at inngrepet har «tilstrekkelig hjemmel».[52] Dette innebærer at Grunnlovens hjemmelskrav i § 113 på dette området må tolkes og anvendes i samsvar med lovkravet i EMK.

Som beskrevet over gjelder det en nedre grense for hvilke handlinger som utgjør et inngrep i en individuell rettighet, og som derfor krever hjemmel i eller i medhold av lov. Når det gjelder legalitetsprinsippet etter norsk rett har Høyesterett til sammenligning på straffeprosessens område uttalt at det som kalles ulovfestede politimetoder ikke har vært ansett tilstrekkelig inngripende til å utløse et lovkrav.[53] I forslaget til ny straffeprosesslov har likevel straffeprosessutvalget tatt til orde for å lovfeste enkelte tidligere ulovfestede metoder. Dette begrunnes blant annet med at det ikke er fullt ut avklart i hvilke tilfeller «observerende og manipulerende» metoder krever lovhjemmel for å oppfylle vilkårene i EMK artikkel 8 nr. 2, men at flere av de metoder som i dag praktiseres, kan falle inn under den vernede sfæren etter nr. 1 i konvensjonsbestemmelsen.[54]

Metodene som foreslås regulert i lovforslaget her er i hovedsak handlinger som departementet vurderer at krever hjemmel i lov. Reguleringen vil oppfylle kravet om at det må foreligge rettslig grunnlag i eller i medhold av nasjonal lov. Neste spørsmål blir dermed hvilke *kvalitative* krav EMK stiller til lovgivningen. Dette vil bli vurdert i det følgende.

EMD stiller i sin praksis krav om at lovgivningen må være tilstrekkelig *klar* og *forutberegnelig*. I dette ligger blant annet at lovgivningen må være tilgjengelig og utformes i

---

[51] Se hhv. EMK artikkel 8 nr. 2, artikkel 9 nr. 2, artikkel 10 nr. 2 og artikkel 11. nr 2. At et inngrep må være i samsvar med loven innebærer etter EMDs praksis at tiltaket må ha et grunnlag i nasjonal lov, se for eksempel *Uzun mot Tyskland* avsagt 2. september 2010, avsnitt 60 med videre henvisninger. Det er ikke grunn til å problematisere forholdet mellom legalitetsprinsippet i Grunnloven (som krever hjemmel i formell lov) og lovkravet etter EMK (der også andre rettsgrunnlag som ulovfestet rett og rettspraksis kan kvalifisere) i høringsnotatet fordi inngrep i den enkeltes rettssfære her foreslås regulert i formell lov.

[52] Jf. Rt. 2015 s. 93 avsnitt 60 og Rt. 2014 s. 1105 avsnitt 23-30 som begge gjaldt Grunnloven § 102 og EMK artikkel 8

[53] Se Rt. 1984 s. 1076

[54] Se NOU 2016:24 *Ny straffeprosesslov*, punkt 14.10.2 s. 342.

tråd med alminnelige rettsstatsprinsipper. Lovkravet har som formål å verne mot vilkårlige myndighetsinngrep. Dess større inngrepet anses for å være, desto strengere krav har EMD stilt til lovgrunnlaget.[55]

EMD uttalte følgende om hva det betyr at lovgivningen må være tilstrekkelig klar og forutberegnelig i *Roman Zakharov mot Russland* i avsnitt 228:[56]

> «The law must thus meet quality requirements: it must be accessible to the person concerned and foreseeable as to its effects.»[57]

Det at lovgivningen skal være *tilgjengelig* innebærer for det første at borgerne må kunne ha adgang til reglene for å kunne sette seg inn i dem. Videre betyr det at rettsreglene må være formulert så klart og presist at borgerne skal ha mulighet til å forstå innholdet. For eksempel vil fragmentert og sterkt skjønnsmessig lovgivning kunne være både vanskelig å finne frem til og vanskelig å forstå rekkevidden av. Det at forslaget til ny etterretningstjenestelov nå utformes med en langt større detaljgrad enn gjeldende lov, bidrar i seg selv til å gjøre regelverket klarere og mer tilgjengelig for borgerne. En rekke bestemmelser som tidligere har vært å finne i internt regelverk foreslås nå vedtatt som lovtekst. Dette gir større innsikt i tjenestens oppgaver og metoder og dermed større demokratisk legitimitet.

En annen grunntanke ved klarhetskravet er at den enkelte skal ha mulighet for å *forutse* sin rettsstilling og kunne innrette sin handlemåte deretter. Dette utgangspunktet krever imidlertid noen presiseringer. Hovedhensynet og begrunnelsen bak kravet om forutberegnelighet, i betydning av individets innrettelsesbehov, gjør seg først og fremst gjeldende for adferdsregulerende bestemmelser. Det klassiske eksempelet på adferdsregulering er straffebestemmelser eller andre former for regulering der ikke-overholdelse av regelverket kan få en uønsket konsekvens. Et eksempel på sistnevnte er at man mister krav på et gode. Innenfor kategoriene av regler der individets innrettelsesbehov gjør seg særlig gjeldende, er det helt grunnleggende at borgerne på en klar og forutberegnelig måte kan gjøre seg kjent med hvilke handlinger som kan føre til hvilke konsekvenser. Ulike former for fordekt informasjonsinnhenting eller andre skjulte metoder, det være seg som ledd i utenlandsetterretning stiller seg i en annen situasjon. Her vil ikke formålet være å forsøke å påvirke individets handlingsmønster. Ved for eksempel et tiltak som kommunikasjonsetterretning vil detaljert informasjon om tiltaket gi dem aktiviteten retter seg mot mulighet til å tilpasse handlingsmønsteret sitt, som igjen vil undergrave selve formålet med informasjonsinnhentingen. EMD uttaler seg om dette i blant annet *Roman Zakharov mot Russland* i avsnitt 229:[58]

> «The Court has held on several occasions that the reference to «foreseeability» in the context of interception of communications cannot be the same as in many other fields. Foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee

[55] Se for eksempel EMDs avgjørelse *Malone mot Storbritannia* avsagt 26. april 1985

[56] *Roman Zakharov mot Russland* avsagt 4. desember 2015

[57] Dette følger av langvarig praksis fra EMD, se blant annet *Rotaru mot Romania* avsagt 4. mai 2000, *S. and Marper mot Storbritannia* 4. desember 2008 og *Kennedy mot Storbritannia* avsagt 18. mai 2010

[58] Det samme følger også av tidligere avsigelser, se for eksempel *Kruslin mot Frankrike* avsagt 24. april 1990 mfl.

> when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly."

I denne forbindelse er det et viktig poeng at etterretningstjenester, hvis oppgave er å oppfylle myndighetenes informasjonsbehov på overordnet nivå, ikke har – i motsetning til politi- og sikkerhetstjenester – håndhevelses- eller beslutningsmyndighet overfor enkeltpersoner. Selv om etterretningstjenesters virksomhet i seg selv kan være inngripende, innebærer dette at informasjon som innhentes om personer, aldri vil bli brukt til å treffe beslutninger som direkte berører disse uten at dette først vurderes, besluttes og effektueres av en eller flere uavhengige tredjeparter (f.eks. av politiet som grunnlag for å be retten om kjennelse for bruk av tvangsmidler).

Som følge av at innretningshensynet ikke gjør seg gjeldende på samme måte for skjulte metoder, er det først og fremst *kontrollhensynet* som fungerer som den sterkeste begrunnelsen for legalitetskravet i ny lov om Etterretningstjenesten. For inngrep som gjøres i hemmelighet skjerpes kravet til rettsgrunnlaget, og reglene må inneholde rettssikkerhetsgarantier for å beskytte borgerne mot vilkårlighet og misbruk. EMD har i mange saker understreket betydningen av kontrollhensynet og viktigheten av å hindre myndighetsmisbruk:[59]

> «However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated."

Når det gjelder normeringen av rammene for Etterretningstjenestens aktivitet er det den allmenne interessen i å kontrollere og sette klare grenser for myndighetenes virksomhetsutøvelse som står sentralt. Ved å sørge for at inngrep bare kan skje i henhold til fastsatte normer som tilfredsstiller minstekrav til notoritet og publisitet, så vil dette bidra til å redusere faren for myndighetsoverskridelse.[60] Det at lovreglene skal være utformet tilstrekkelig klart vil bidra til å forhindre vilkårlighet og sikre kontrolladgangen, og er dermed en mekanisme for å hindre myndighetsmisbruk. Som en generell rettesnor oppstiller EMD krav om at lovgivningen må være «particularly precise».[61] I dette ligger det at lovreglene må være så klare at de gir borgerne en indikasjon om i hvilke situasjoner og på hvilke vilkår myndighetene kan ty til denne typen skulte inngrep. EMD uttaler i *Roman Zakharov* i avsnitt 229:

> «The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures."

EMD har gjennom praksis utmeislet visse minstekrav til hva et lovverk som hjemler skjulte innhentingsmetoder må regulere. Det følger av disse minstekravene at bestemmelsene må si noe om karakteren av de handlinger som kan begrunne et tiltak, hvem tiltaket kan ramme, varighet av tiltaket, prosedyreregler for innsamling, bruk og lagring av informasjon, samt

[59] Se for eksempel *Roman Zahkarov mot Russland* avsagt 4. desember 2015, avsnitt 229

[60] Se om dette i Jørgen Aall, *Rettsstat og menneskerettigheter* (2015) s. 120

[61] *Kruslin mot Frankrike* avsagt 24. april 1990

bestemmelser om deling og sletting av informasjon. EMD uttalte følgende i *Roman Zakharov mot Russland* avsnitt 231 og i *Centrum for rättvisa mot Sverige*[62] avsnitt 103:

> "In its case-law on secret measures of surveillance in criminal investigations, the Court has developed the following minimum safeguards that should be set out in law in order to avoid abuses of power: a description of the nature of offences which may give rise to an interception order; a definition of the categories of people liable to have their communications intercepted; a limit on the duration of the measures; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed."

Høyesterett bygger på samme forståelse av klarhetskravet i Rt. 2014 s. 1105.[63] Førstvoterende uttaler her at for å gi en hjemmel som Grunnloven og menneskerettskonvensjonene krever, holder det ikke at loven er formelt sett i orden og at den etter alminnelige tolkningsprinsipper gir grunnlag for lagringen:

> «Loven må være tilgjengelig og så presis som forholdene tillater. Den må dessuten – i lys av den forhøyede risikoen for misbruk og vilkårlighet som erfaringsmessig kan foreligge når myndigheter tillates å operere i hemmelighet – gi rimelige garantier knyttet til blant annet formen for lagring, bruken av materialet, mulighetene for å gi innsyn, sikkerhet og sletting.»

Samtidig går det en grense for hvor klart et lovverk faktisk kan formuleres og samtidig fylle sin funksjon, både når det gjelder muligheten for å fungere over tid uten stadig å måtte endres, og for å unngå at lovverket får en uønsket høy detaljeringsgrad og dermed blir svært omfattende. Virkeligheten kan være for kompleks og i tillegg i stadig endring til at det er mulig med en helt presis regulering. For rigide krav til hvordan lovtekst kan utformes kan potensielt føre til at lovgiver avstår fra å vedta lover som det er et samfunnsmessig behov for. Dette vil igjen kunne ha en negativ effekt på folks rettsoppfatning. Referanse til terrortrussel eller redningsoperasjoner kan i prinsippet være tilstrekkelig, EMD uttaler om dette i *Szabo og Vissy mot Ungarn* avsnitt 64-65:[64]

> «The Court [..] recalling that the wording of many statutes is not absolutely precise, and that the need to avoid excessive rigidity and to keep pace with changing circumstances means that many laws are inevitably couched in terms which, to a greater or lesser extent, are vague. [..] For the Court, the requirement of "foreseeability" of the law does not go so far as to compel States to enact legal provisions listing in detail all situations that may prompt a decision to launch secret surveillance operations. The reference to terrorist threats or rescue operations can be seen in principle as giving citizens the requisite indication."

Domstolen uttaler mye av det samme i avsnitt 247 i *Roman Zakharov mot Russland* og tilføyer:

> «By the nature of things, threats to national security may vary in character and may be unanticipated or difficult to define in advance.»[65]

---

[62] Dommen er i skrivende stund ikke rettskraftig.

[63] Saken gjaldt bruk av overskuddsmateriale fra kommunikasjonskontroll som bevis i en straffesak.

[64] *Szabo og Vissy mot Ungarn* avsagt 12. januar 2016

[65] Se også *Kennedy mot Storbritannia* avsagt 18. mai 2010 avsnitt 159

Men særlig bestemmelsenes rekkevidde og handlingsrom må reguleres med tilstrekkelig klarhet for å forebygge vilkårlighet og myndighetsmisbruk. Domstolen er generelt på vakt mot skjønnsmessige vilkår som legger stor diskresjonær kompetanse til utøvende myndighet som dermed selv kan fylle begrepene med innhold:[66]

> «The law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference."

Generelt kan man si at lovverket alltid må tilpasses det som skal reguleres, og at jo større inngrepet i menneskerettighetene er, desto strengere vil lovkravet være. EMD har samtidig understreket at det ikke er grunn for å stille noen lavere krav til tilgjengeligheten og klarheten av regler som gjelder strategisk overvåkning enn til kontroll av individuell kommunikasjon, selv om krav til rettssikkerhetsgarantier her kan variere og dermed også spillerom for bruk av skjønn.[67]

Av overstående drøftelse kan det utledes at lovgrunnlaget for Etterretningstjenestens virksomhet må utformes med et tilstrekkelig presisjonsnivå for å tilfredsstille klarhetskravet. Dette innebærer at lovverket tilstrekkelig klart må angi hvilke oppgaver som Etterretningstjenesten er pålagt å løse. Dernest må regelverket så presist som mulig angi hvilke fremgangsmåter som griper inn i borgernes rettssfære og som tjenesten kan anvende for å løse disse pålagte oppgavene. Dette innebærer også en tilstrekkelig presis regulering av hvilke prosedyreregler som skal gjelde for innhenting og behandling av informasjon, herunder tilpassede regler for bruk, deling og sletting av informasjon som kan knyttes til identifiserte eller identifiserbare personer. Det er dessuten av avgjørende betydning at reglene utformes på en slik måte at de legger til rette for en aktiv og effektiv kontroll med tjenestens virksomhet.

4.2.5.3 Legitimt formål

For at et inngrep skal kunne tillates må det forfølge et legitimt formål. I EMK er formålene listet opp i hver enkelt unntaksbestemmelse. EMK artikkel 8 om privatlivets fred kan tjene som eksempel. Her oppstilles det krav om at inngrepet må være nødvendig av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landet økonomiske velferd, for å forbygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter eller friheter.

Hvilke formål som listes opp i de aktuelle rettighetene i EMK som Etterretningstjenesten kan komme til å gjøre inngrep i kan variere noe. Generelt kan man si at etterretningsvirksomhet rettet mot utenlandske forhold i form av det å innhente, bearbeide og analysere informasjon som har betydning for Norges suverenitet og sikkerhet og viktige nasjonale interesser, klart faller inn under formålene «nasjonal sikkerhet» og «offentlig trygghet» («national security» og «public safety») i EMK artiklene 8 til 11. Dette vil derfor ikke problematiseres ytterligere her. Likevel er det klart at Etterretningstjenesten som sådan ikke har fullmakt til å gjøre inngrep i noens rettigheter bare fordi tjenesten har en oppgave i å ivareta nasjonens

---

[66] *Roman Zakharov mot Russland* avsagt 4. desember 2015, avsnitt 230 og 247 og *Szabó og Vissy mot Ungarn* avsagt 12. januar 2016, avsnitt 65

[67] Se *Liberty mot Storbritannia* avsagt 1. juli 2008 og *Kennedy mot Storbritannia* avsagt 18. mai 2010, avsnitt 162. Se også Erling Johannes Husabøs betenkning i Dokument 16 (2015-2016) *Rapport til Stortinget fra Evalueringsutvalget for Stortingets kontrollutvalg for etterretnings- overvåknings- og sikkerhetstjeneste (EOS-utvalget)*, vedlegg 4, s. 248.

sikkerhet. Alle tiltak Etterretningstjenesten foretar som gjør inngrep i noens menneskerettigheter må ha betydning for nasjonal sikkerhet og offentlig trygghet, og dette må vurderes og begrunnes i det enkelte tilfellet. Det er heller ikke nok at lovverket som sådan er ment å ivareta et legitimt formål. De aktuelle metodene og den konkrete bruken av dem må også være *egnet* til å oppnå et av de legitime formålene. Dette må vurderes konkret fra tiltak til tiltak, både når det gjelder selve utformingen av regelverket og ved den faktiske anvendelsen av det, se mer om dette under.

4.2.5.4 Forholdsmessighetsvurderingen

Det tredje grunnkravet for at et inngrep i individuelle rettigheter kan tillates etter EMK er at inngrepet må være *nødvendig i et demokratisk samfunn*. Dette innebærer at tiltaket må være egnet til å ivareta det legitime formålet som beskrevet over, og at interessene som begrunner inngrepet i en samlet vurdering anses som mer tungtveiende enn de interessene som krenkes. Ordlyden sier «nødvendig». Dette er ikke det samme som «absolutt nødvendig» eller «uunnværlig», men på samme tid kreves mer enn at det er «ønskelig». Det sies gjerne at inngrepet må komme som en følge av et presserende eller tvingende samfunnsbehov.

At inngrepet må være egnet til å oppnå det legitime formålet betyr at tiltaket må forventes å ha effekt. Inngripende tiltak som settes i verk for sikkerhets skyld, eller fordi de kanskje kan være effektfulle vil derfor vanskelig aksepteres. På den annen side vil det etter omstendighetene i det konkrete tilfelle og i lys av trusselbildet være akseptabelt å treffe inngripende tiltak i preventivt øyemed. Menneskerettighetene krever ikke at trusselen først må manifestere seg gjennom konkrete handlinger. For etterretningstjenesters vedkommende ligger det også i sakens natur at inngrep kan være nødvendig selv om effekten på inngrepstidspunktet er usikker.

Det er videre et krav at formålet ikke kan ivaretas gjennom andre rimelige og mindre inngripende tiltak. Hele tiden vil det være en avveining mellom viktigheten av det som søkes oppnådd og alvorligheten av inngrepet. Selv fatale inngrep kan være konvensjonsmessige hvis behovet er tilstrekkelig tungtveiende, jf. EMK art. 2.[68] Hvorvidt inngrepet er forholdsmessig må derfor vurderes konkret i den enkelte sak, og en rekke faktorer tas i betraktning. Det er det sammenlignende perspektivet som står i sentrum for vurderingen der de legitime hensynene som taler for inngrepet må være tunge nok og godt nok begrunnet for å kunne forsvare inngrep i de rettigheter som krenkes.

I forholdsmessighetsvurderingen må det tas hensyn til hvilken skjønnsmargin («margin of appreciation») EMD normalt tilkjenner statene på det aktuelle samfunnsområdet, dvs. hvilken prøvingsintensitet EMD legger til grunn i den aktuelle type saker.

Tradisjonelt har EMD lagt til grunn at statene har en nokså vid skjønnsmargin når det gjelder tiltak som er begrunnet i statens vitale interesser, særlig ivaretakelsen av nasjonal sikkerhet. I *Klass m. fl. mot Tyskland*[69] aksepterte domstolen systemer for hemmelig avlytting under henvisning til den rådende nasjonale terrortrusselen. I *Weber og Savaria mot Tyskland*[70] uttalte domstolen i avsnitt 106:

---

[68] Se mer om dette Jørgen Aall, *Rettsstat og menneskerettigheter*, 2015 s. 157

[69] *Klass m. fl. mot Tyskland* avsagt 6. september 1978

[70] *Weber og Savaria mot Tyskland* avsagt 29. juni 2006

> «[W]hen balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life, it has consistently recognized that the national authorities enjoy a fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security.."

I *Centrum för Rättivsa mot Sverige* av 19. juni 2018[71] uttaler EMD i avsnitt 112 under henvisning til *Weber og Saravia* avsnitt 106:

> «The Court has expressly recognised that the national authorities enjoy a wide margin of appreciation in choosing how best to achieve the legitimate aim of protecting national security.»

Samtidig har domstolen understreket at siden det foreligger en risiko for at alle systemer for hemmelig innhenting av informasjon kan misbrukes under dekke av å ivareta nasjonal sikkerhet, og dermed kan ende opp med å undergrave demokratiet og til og med ødelegge det, er det behov for effektive rettsikkerhetsgarantier mot misbruk:

> «Nevertheless, in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist adequate effective guarantees against abuse […]. This assessment depends on all the circumstances of the case such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them, and the kind of remedy provided by the national law. The Court has to determine whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the "interference" to what is "necessary in a democratic society".»[72]

EMD har derfor lagt til grunn at selv om statene har en vid skjønnsmargin når det gjelder å velge hvilken type etterretningsregime som er nødvendig av hensyn til nasjonal sikkerhet, vil skjønnsmarginen være snevrere når det gjelder den nærmere utformingen av tiltakene. EMD uttalte i *Centrum för Rättvisa mot Sverige* avsnitt 113:

> «[W]hile States enjoy a wide margin of appreciation in deciding what type of interception regime is necessary to protect national security, the discretion afforded to them in operating an interception regime must necessarily be narrower.»

Deretter sier EMD samme sted:

> «In this regard, the Court has identified six minimum safeguards that […] interception regimes must incorporate in order to be sufficiently foreseeable to minimize the risk of abuses of power»

Hva disse seks rettsikkerhetsgarantiene er, er beskrevet i *Centrum för rättvisa mot Sverige* avsnitt 103 med referanse til *Roman Zakharov mot Russland* avsnitt 231. Disse er omtalt i høringsutkastets punkt 4.2.5.2. Det understrekes at statene i utformingen av konkrete tiltak har en viss skjønnsmargin («certain margin of appreciation»).[73]

I sin helhetsvurdering vil domstolen gå inn og vurdere hvordan den konkrete etterretningstjenestens oppgaver og fremgangsmåter er regulert. Den indre sammenhengen

---

[71] Dommen er i skrivende stund ikke rettskraftig.

[72] *Weber og Savaria mot Tyskland* avsagt 29. juni 2006, avsnitt 106 og tilsvarende i *Roman Zakharov mot Russland* avsagt 4. desember 2015, avsnitt 232

[73] Se nærmere omtale av dommen *Centrum for rättvisa mot Sverige* avsagt 19. juni 2018 i punkt 11.8.2.5

mellom lovkravet og forholdsmessighetsvurderingen trer her frem; for at domstolen skal kunne ta stilling til om et inngrep er forholdsmessig må den ta utgangspunkt i hvordan tiltaket er regulert – det vil si de materielle vilkår, så vel som personelle og prosessuelle bestemmelser. I tillegg har forholdsmessighetsvurderingen avgjørende betydning for om, og i tilfellet hvordan, tiltaket kan reguleres; det er bare inngrep som er nødvendige i et demokratisk samfunn for å ivareta et legitimt formål som det er tillatt å regulere.

Helt sentralt i proporsjonalitetsvurderingen er om det eksisterer tilstrekkelige og effektive rettssikkerhetsgarantier for å beskytte individet mot misbruk og hindre vilkårlighet. Den som er gjenstand for fordekt informasjonsinnhenting vil som utgangspunkt ikke selv være kjent med at dette skjer, og vil dermed ikke kunne påklage inngrepet. EMD har innfortolket et krav til effektiv og uavhengig kontroll for å hindre myndighetsmisbruk. I *Rotaru mot Romania* uttaler domstolen i avsnitt 59:[74]

> «In order for systems of secret surveillance to be compatible with Article 8 of the Convention, they must contain safeguards established by law which apply to the supervision of the relevant services' activities. Supervision procedures must follow the values of a democratic society as faithfully as possible, in particular the rule of law […]."

Ved vurderingen av om det finnes tilstrekkelige garantier til beskyttelse mot misbruk foretar domstolen en samlet bedømmelse av blant annet karakter, omfang og varighet av inngrepet, betingelser for å iverksette tiltaket, hvilke myndigheter som har kompetanse til å bemyndige, utføre og kontrollere inngrep og hvilke rettsmidler som finnes etter nasjonal rett. Den berørte skal ha adgang til en «effektiv kontroll» der det sikres at inngrepet begrenses til hva som er nødvendig i et demokratisk samfunn.[75] Reguleringen vil følgelig måtte omfatte vilkår for innsamling, kompetansebestemmelser, saksbehandlingsregler, varighet mv. Det er relevant å vurdere om det er fastsatt begrensninger med hensyn til karakteren av de opplysninger som kan innsamles og oppbevares, hvilke persongrupper som kan utsettes for tiltaket, hvilke betingelser som må være oppfylt, hvilken fremgangsmåte som kan benyttes, og hvordan og hvor lenge opplysningene blir oppbevart.[76]

Det må eksistere kontrollinstanser som bidrar til å sikre overholdelse av regelverket. Aller helst mener EMD at kontrollen bør være judisiell og ligge til den dømmende myndighet, i alle fall i siste instans, fordi domstolene gir de beste garantier for uavhengighet og upartiskhet.[77] EMD har imidlertid lagt til grunn at fravær av rettslig kontroll ikke automatisk fører til brudd på artikkel 8, såfremt andre kontrollmekanismer oppfyller kravene til effektiv, uavhengig og permanent kontroll.[78]

Kontrolltiltakene spiller inn i alle stadier i prosessen; når inngrepet igangsettes, mens det utføres og etter at det er avsluttet. EMD beskriver flere sider av kontrolltiltakene i *Roman*

---

[74] *Rotaru mot Romania* avsagt 4. mai 2000

[75] Se Kjølbro, *Den europæiske menneskerettigheds konvention for praktikere* (2017), s. 878 med videre henvisning til *Roman Zakharov mot Russland* avsagt 4. desember 2015 avsnitt 232

[76] Se Kjølbro «Den europæiske menneskerettigheds konvention for praktikere» 2017 s. 860

[77] Se EMD i *Klass m.fl. mot Tyskland* avsagt 6. september 1978, avsnitt 55-56 og *Kennedy mot Storbritannia* avsagt 18. mai 2010, avsnitt 167

[78] Se *Klass m.fl. mot Tyskland* avsagt 6. september 1978 der en parlamentarisk komité med balansert politisk sammensetning og en uavhengig myndighetskommisjon som gjennomførte kontrollen, var tilstrekkelig.

Zahkarov mot Russland.[79] EMD gjentar tidligere uttalelser om at det ligger i sakens natur at kontrollen når inngrepet beordres og utføres må finne sted uten at den som tiltaket retter seg mot kjenner til dette. Dette stiller ekstra strenge krav til kontrollens kvalitet. Domstolen uttaler i denne forbindelse i avsnitt 233:

> «Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights. In addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 § 2, are not to be exceeded."

Samme avgjørelse går langt i å kreve at aktivitet loggføres som grunnlag for kontroll, og at kontrollmyndigheten må ha tilgang til relevant informasjon og dokumentasjon. I tillegg antyder domstolen at kontrollmyndigheten bør ha en viss myndighet som sikrer at dersom den kommer til at inngrepet var ulovlig, må dette kunne føre til at inngrepet avsluttes og at ulovlig innhentet materiale slettes.

Når det gjelder det tredje kontrollstadiet, nemlig etterfølgende kontroll, legger EMD særlig vekt på hvilken mulighet den enkelte har til å få prøvd lovmessigheten av et mulig eller faktisk inngrep. Igjen er utfordringen manglende kunnskap om hvilke eventuelle fordekte innhentingsmetoder som er benyttet mot individet utført av de hemmelige tjenestene. Spørsmålet om effektive rettsmidler, herunder klagerett og notifikasjon, behandles i punkt 4.3 under. I denne forbindelse er det tilstrekkelig å nevne at EMD har lagt stor vekt på individets etterfølgende klageadgang som en viktig faktor for å sikre effektive kontrolltiltak mot myndighetsmisbruk. Dette behovet kan ivaretas ved notifikasjon til den enkelte etter at inngrepet er avsluttet, forutsatt at det ikke foreligger tungtveiende hensyn til hinder for dette. En vid klageordning som ikke stiller strenge krav til sannsynliggjøring av at et inngrep har funnet sted kan avhjelpe manglende notifikasjon.

Oppsummeringsvis vil forholdsmessighetsvurderingen omfatte alle sider av saken der alvorligheten av inngrepet veies opp mot nødvendigheten av det. Rettssikkerhetsgarantier må bygges inn i regelverket og inngrepsadgangen reguleres i faste rettslige rammer. For å sikre at proporsjonalitetsvurderingen blir ivaretatt i alle enkeltsaker som kan innebære et inngrep i noens individuelle rettigheter, mener departementet at det er formålstjenlig å innta en egen bestemmelse om forholdsmessighet i loven. Bestemmelsen bør stå i kapittelet som angir grunnvilkår for innhenting for å synliggjøre at dette er en vurdering som alltid skal foretas. Departementet mener at det må fremgå av lovverket at inngrep ikke er tillatt dersom disse vurderes å være uforholdsmessige. Dersom mindre inngripende tiltak i tilstrekkelig grad kan ivareta formålet skal disse velges. Departementet understreker at praktiseringen av forholdsmessighetsvurderingen må utføres på en slik måte at den er egnet for kontroll, både i form av løpende forvaltningskontroll og etterfølgende kontroll av EOS-tilsynet.

[79] EMD bruker uttrykket «review and supervision» av hemmelige overvåkningstiltak, se *Roman Zakharov mot Russland* avsagt 4. desember 2015, avsnitt 233

4.3 Krav til effektive rettsmidler

4.3.1 Generelle utgangspunkter

Det følger av EMK artikkel 13 at enhver som har fått sine konvensjonsrettigheter krenket, skal ha rett til et effektivt rettsmiddel, eller en effektiv prøvningsrett, for en nasjonal myndighet.[80] En liknende bestemmelse finnes også i FNs konvensjon om sivile og politiske rettigheter (SP) artikkel 2 nr. 3. I det følgende redegjøres det bare for EMDs rettspraksis etter EMK artikkel 13.

Rekkevidden av forpliktelsen etter EMK artikkel 13 vil variere med den aktuelle konvensjonsrettighetens karakter og hvilken type myndighetsutøvelse det er stilt spørsmål ved lovligheten av.[81] Saker som angår nasjonal sikkerhet skiller seg ut fra andre saker når det gjelder EMK artikkel 13.[82] I denne type saker har statene vist til at det bare kan være begrenset grad av overprøving i lys av nasjonale sikkerhetshensyn. EMD har derfor akseptert betydelige begrensninger når det gjelder hvilken prøvingsrett som kan kreves når det gjelder artikkel 8 og 10 på områdene hemmelig overvåkning. EMD uttalte i tråd med dette følgende i *Klass m.fl. mot Tyskland*:[83]

> «For the purposes of the present proceedings, an "effective remedy" under Article 13 must mean a remedy that is as effective as can be having regard to the restricted scope for recourse inherent in any system of secret surveillance. It therefore remains to examine the various remedies available to the applicants under German law in order to see whether they are "effective" in this limited sense."

EMDs tilnærming kan være svært kontekstavhengig, noe som har medført at ulik standard har vært satt i noen av sakene som gjelder nasjonal sikkerhet og artikkel 13.[84]

Vurderingene knyttet til en effektiv prøvingsrett vil inngå som en integrert del av den helhetlige forholdsmessighetsvurderingen som må foretas blant annet etter EMK artikkel 8 andre ledd. EMD anså det derfor f.eks. i *Roman Zakharov mot Russland* unødvendig å behandle spørsmålet om rett til en effektiv prøvingsrett separat.[85]

Det er nærliggende å legge til grunn, i lys av subsidiaritetsprinsippet, at jo mer effektiv nasjonal prøvingsrett som foreligger, jo mindre intensiv vil EMDs prøving av om det foreligger et konvensjonsbrudd etter EMK artikkel 8 og evt. andre bestemmelser være.[86]

---

[80] Den norske oversettelsen av EMK artikkel 13 oversetter «right to an effective remedy» med «en effektiv prøvingsrett». Den norske oversettelsen av SP artikkel 2 nr. 3 er derimot «adgang til effektive rettsmidler».

[81] Harris, O'Boyle & Warbrick, *Law of the European Convention on Human Rights*, Third Edition, 2014, s. 766

[82] Harris, O'Boyle & Warbrick, op.cit., s. 766, *Klass mot Tyskland* avsagt 6. september 1978, avsnitt 69 og *Leander mot Sverige* avsagt 26. mars 1987, avsnitt 84.

[83] *Klass m.fl. mot Tyskland* avsagt 6. september 1978, avsnitt 69.

[84] Harris, O'Boyle & Warbrick, op.cit., s. 769.

[85] EMD nøyde seg i punkt II (avsnitt 306-307) om EMK artikkel 13 med å vise til funnene sine i punktet I om EMK artikkel 8 avsnitt 286 til 300 vedrørende «notification of interception of communication and available remedies».

[86] Se Harris, O'Boyle & Warbrick, op.cit., s. 764-765, som antyder dette.

4.3.2 Hvem skal ha en effektiv prøvingsrett?

4.3.2.1 Krav om prosedabel grunn

I henhold til EMK artikkel 13 skal «enhver hvis rettigheter og friheter fastlagt i denne konvensjon blir krenket», ha en effektiv prøvningsrett. EMD tolket dette i *Klass m.fl. mot Tyskland* slik at enhver som *hevder* at vedkommendes konvensjonsrettigheter er blitt krenket, har en slik rett.[87] I senere saker har imidlertid EMD presisert dette til at klager må ha *an arguable claim*, eller en prosedabel grunn til å hevde at vedkommende er blitt utsatt for en konvensjonskrenkelse.[88]

EMD har ikke ansett det hensiktsmessig å gi noen definisjon av begrepet "arguable", men vist til at om dette vilkåret er oppfylt må avgjøres «in light of the particular facts and the nature of the legal issue or issues raised».[89] Det er på det rene at det ikke må ha forekommet et konvensjonsbrudd, for at det skal foreligge en prosedabel grunn til å hevde at det foreligger et konvensjonsbrudd etter EMK artikkel 13. På den annen side gir EMK artikkel 13 ikke en rett til å påklage statens lovgivning som sådan som konvensjonsstridig.[90] En klage som er åpenbart grunnløs etter EMK artikkel 35, vil heller ikke kunne være «arguable».[91]

4.3.2.2 Klager må være innenfor statens myndighetsområde (jurisdiksjon)

EMK artikkel 13 må også leses sammen med EMK artikkel 1. Det er et grunnvilkår for at en stat skal kunne holdes ansvarlig etter EMK at staten utøver jurisdiksjon over den aktuelle personen og således har konvensjonsforpliktelser overfor denne.

Spørsmålet om rekkevidden av EMK artikkel 1 er drøftet under punkt 4.1.3 over. Som nærmere beskrevet der, er personer innenfor statens territorium klart nok innenfor statens jurisdiksjon i EMK artikkel 1 sin forstand, mens det foreligger mer usikkerhet knyttet til i hvilken utstrekning EMK får anvendelse på Etterretningstjenestens informasjonsinnhenting som skjer eller får virkning utenfor norsk territorium. Spørsmålet er om adgangen til rettsmidler etter gjeldende norsk rett, for de som gjøres gjenstand for Etterretningstjenestens informasjonsinnhenting der Norges konvensjonsforpliktelser gjelder jf. artikkel 1, er i overensstemmelse med EMKs krav.

---

[87] *Klass m.fl. mot Tyskland* avsagt 6. september 1978, avsnitt 64: ""Thus Article 13 must be interpreted as guaranteeing an "effective remedy before a national authority" to everyone who *claims* that his rights and freedoms under the Convention have been violated" (vår kursivering).

[88] Se f.eks. *Leander mot Sverige* av 26. mars 1987 avsnitt 63, hvor EMD uttalte: "Moreover, such a remedy is required only in respect of grievances which can be regarded as arguable[…]".

[89] Harris, O'Boyle & Warbrick, op.cit., s. 767 med videre henvisning til bl.a. Boyle and Rice mot Storbritannia avnsitt 55, hvor EMD uttalte: "The Court does not think that it should give an abstract definition of the notion of arguability. Rather it must be determined, in the light of the particular facts and the nature of the legal issue or issues raised, whether each individual claim of violation forming the basis of a complaint under Article 13 was arguable and, if so, whether the requirements of Article 13 were met in relation thereto".

[90] EMD uttalte i *Leander mot Sverige* av 26. mars 1987 avsnitt 77: "Article 13 does not guarantee a remedy allowing a Contracting State's laws as such to be challenged before a national authority on the ground of being contrary to the Convention or equivalent domestic norms..."

[91] Harris, O'Boyle & Warbrick, op.cit., s. 768 med videre henvisning til *Conka mot Belgia* av 5. februar 2002 avsnitt 76.

4.3.3 Hvem har klageadgang etter gjeldende norsk rett?

Det foreligger etter norsk rett klageadgang til EOS-utvalget og til domstolene.

Lov om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-kontrolloven) § 5 annet ledd lyder:

> 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.

EOS-kontrolloven § 5 femte ledd lyder[92]:

> 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.

Klageadgangen til domstolene er grunnlovsfestet i Grunnloven § 95 og er nærmere regulert i tvisteloven § 1-3.

Grunnloven § 95 første setning lyder:

> Enhver har rett til å få sin sak avgjort av en uavhengig og upartisk domstol innen rimelig tid.

Tvisteloven § 1-3 lyder:

§ 1-3. Søksmålsgjenstand, partstilknytning og søksmålssituasjon

(1) Det kan reises sak for domstolene om rettskrav.

(2) Den som reiser saken, må påvise et reelt behov for å få kravet avgjort i forhold til saksøkte. Dette avgjøres ut fra en samlet vurdering av kravets aktualitet og partenes tilknytning til det.

4.3.4 Er klageadgangen etter gjeldende norsk rett tilstrekkelig vid?

4.3.4.1 EOS-utvalget

Det følger av EOS-kontrolloven § 5 andre ledd at EOS-utvalget skal motta klager fra enkeltpersoner og organisasjoner, og at EOS-utvalget skal gjøre nærmere undersøkelser av enhver klage «som gir grunn til behandling». Dette må i utgangspunktet anses å samsvare med EMDs krav om at klageorganet må kunne behandle klager fra personer som har en prosedabel grunn («an arguable claim») til å mene at de kan ha vært utsatt for ulovlig overvåking.

Etter EOS-kontrolloven § 5 femte ledd omfatter ikke EOS-utvalgets kontrolloppgave virksomhet «som angår personer som ikke er bosatt i riket og organisasjoner som ikke har tilhold her». Det kan gjøres unntak fra dette «når særlige grunner tilsier det». Praksis fra EOS-utvalget viser at terskelen er lav for å ta klagesaker under behandling.[93] Man kan likevel hevde at bestemmelsen i EOS-kontrolloven § 5 femte ledd skaper en viss uklarhet om i hvilken grad EOS-utvalgets klagebehandling er åpen for personer som ikke er bosatt i Norge. Dersom bestemmelsen utelukker adgangen til et effektivt rettsmiddel for personer som må anses å være innenfor norsk jurisdiksjon etter EMK artikkel 1 er det problematisk. Dette gjelder for eksempel personer som oppholder seg i Norge, uten å være «bosatt» her. Spørsmålet ble vurdert av det stortingsoppnevnte Evalueringsutvalget som ble nedsatt 27.

[92] Dette fulgte tidligere av Instruks om kontroll med etterretnings-, overvåknings- og sikkerhetstjeneste av 30. mai 1995 nr. 4295 (EOS-kontrollinstruksen) § 4. Instruksen er nå opphevet.

[93] Lysne II-utvalgets rapport om Digitalt grenseforsvar, side 65

mars 2014 med oppgave om å evaluere EOS-utvalget.[94] Utvalget uttaler på side 139 i rapporten:

> «Etter Evalueringsutvalgets syn er det, på bakgrunn av den utvikling av menneskerettighetenes geografiske virkeområdet som har, og antakelig fortsatt vil finne sted, fornuftig at EOS-utvalget ikke er fullstendig avskåret fra å kontrollere EOS-tjenestenes handlinger overfor personer som ikke er bosatt i Norge og organisasjoner som ikke har tilhold her.»

Evalueringsutvalget uttalte på denne bakgrunn at dersom EOS-utvalget kommer over forhold som kan utgjøre krenkelser overfor personer som ikke er bosatt i Norge eller dersom utvalget mottar klager fra slike personer, tilsier Norges menneskerettslige forpliktelser at disse bør kunne undersøkes nærmere. Evalueringsutvalget kunne imidlertid ikke se at Norge i dag er forpliktet til å la disse delene av EOS-tjenestenes virksomhet vies en større del av EOS-utvalgets oppmerksomhet enn de gjør i dag, og det ble derfor ikke foreslått noen endringer i regelverket på denne bakgrunn. Evalueringsutvalget presiserte samtidig at det måtte tas høyde for at det kan komme nye rettsavgjørelser fra EMD som vil kunne kaste lys over dette spørsmålet.[95]

Evalueringsutvalgets uttalelser synes å legge til grunn at EOS-utvalgets adgang til å gjøre unntak fra hovedregelen der «særskilte grunner tilsier det» i tilstrekkelig grad åpner for at de som befinner seg innenfor norsk jurisdiksjonsområde har en klageadgang til EOS-utvalget, selv om disse personene ikke er bosatt eller har tilhold i Norge. Departementet vurderer derfor at den *reelle klageadgangen* til EOS-utvalget etter gjeldende rett er tilstrekkelig vid fordi bestemmelsen tolkes i lys av menneskerettsforpliktelsene.

Det kan vurderes om det likevel er grunn til å endre ordlyden i EOS-kontrolloven, slik at den formelle klageadgangen formuleres mer i tråd med den reelle. En eventuell endring i EOS-kontrolloven vil få betydning ikke bare for kontroll med Etterretningstjenesten, men også med de andre EOS-tjenestene. Konsekvensene av mulige lovendringer må derfor også vurderes opp mot disse tjenestenes virksomhet. En utfordring ved å skulle endre ordlyden i EOS-kontrolloven er at klageadgangen fremgår som en del av reguleringen av EOS-utvalgets oppgaver, og ikke er formulert som en egen bestemmelse. En endring av lovteksten vil derfor enten måtte utvide kontrollområdet for EOS-utvalget, med de ringvirkninger det måtte få for andre områder. Eventuelt vil man kunne endre lovens oppbygning og system på dette punkt og foreslå en egen bestemmelse om klageadgang. Departementet vurderer i den forbindelse at en eventuell endring i EOS-kontrolloven først og fremst har til hensikt å tydeliggjøre at kontrollområdet ikke er snevrere enn det menneskerettighetene tilsier. En slik endring vil neppe ha konsekvenser for innretting og prioritering av kontrolltiltak innenfor rammen av kontrollområdet. En slik justering vil dessuten ha mindre betydning for de andre EOS-tjenestene, hvis oppgaver og fokus er mindre innrettet mot personer og organisasjoner i utlandet enn tilfellet er for Etterretningstjenesten. Departementet har oppstilt to alternative løsninger, og ber særlig om høringsinstansenes synspunkter på disse.

På den ene siden er det for departementet et tungtveiende moment at Evalueringsutvalget og Stortinget helt nylig har vurdert spørsmålet om EOS-utvalgets kontrollområde og kommet til at det ikke er grunn til å utvide dette. Etter at Evalueringsutvalget avga sin rapport ble den

[94] Utvalget ble nedsatt 27. mars 2014 og avga sin rapport til Stortingets presidentskap 29. februar 2016 og var ledet av daværende førstelagmann i Gulating lagmannsrett Bjørn Solbakken

[95] Evalueringsutvalget viser her videre til Sårbarhetsutvalgets vurderinger i NOU 2015:13 s. 82

behandlet i Stortinget.[96] Med dette som utgangspunkt ble EOS-kontrolloven oppdatert på bakgrunn av et representantforslag fra medlemmer i kontroll- og konstitusjonskomiteen, og hele loven ble gitt på nytt ved en lovendring 21. juni 2017.[97] I forbindelse med oppdatering av lovverket ble EOS-kontrollinstruksen opphevet og relevante bestemmelser innarbeidet i selve loven. En bestemmelse som ble flyttet fra instruksen og innarbeidet i loven var nettopp instruksens § 4 om begrensning i utvalgets kontrolloppgave overfor personer og organisasjoner uten tilknytning til riket, som nå utgjør EOS-kontrollovens § 5 femte ledd. Bestemmelsen er gjengitt over.

Det faktum at Stortinget nylig har vurdert og tatt stilling til spørsmålet om EOS-utvalgets kontrolloppgave, og dermed også klageadgangen til EOS-utvalget, kan tilsi at det ikke er nødvendig å reise dette spørsmålet på nytt. Gjeldende bestemmelse om klageadgang må harmoniseres med våre menneskerettsforpliktelser i tråd med menneskerettsloven § 3. Dette innebærer at i den grad EOS-tjenestenes aktivitet innebærer norsk jurisdiksjonsutøvelse etter EMK artikkel 1, vil det være nærliggende å innfortolke en klageadgang for EOS-utvalget. En klage vil i disse tilfeller bli behandlet så fremt det foreligger prosedabel grunn for at konvensjonskrenkelse har funnet sted. Det vil etter dette alternativet være opp til EOS-utvalget å vurdere om klager må anses å være innenfor norsk jurisdiksjon og om klager har en prosedabel grunn til å hevde at hans eller hennes menneskerettigheter er blitt krenket, jf. EOS-kontrolloven § 5 annet ledd annet punktum der det følger at utvalget avgjør om klagen gir grunn til behandling.

På den annen side taler gode grunner for at lovverket bør oppdateres slik at den formelle og reelle klageadgangen til EOS-utvalget samsvarer. Slik lovteksten er formulert i dag kan den gi inntrykk av en snevrere klageadgang enn det som er etablert praksis, noe som igjen kan lede til at potensielle klagere avstår fra å klage. All den tid det er krav om tilgang til effektive rettsmidler der norsk jurisdiksjon etter EMK artikkel 1 gjelder, taler gode grunner for at dette bør fremgå av loven, og at det ikke skal være nødvendig å foreta en harmoniserende tolking av klageadgangen sett opp mot våre folkerettsforpliktelser.

Departementet foreslår derfor eventuelt å gjøre følgende endringer i EOS-kontrolloven:

§ 5 femte ledd i lov 3. februar 1995 nr. 7 om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-kontrolloven) skal lyde:

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

I valget mellom de to alternativene heller departementet til at sistnevnte alternativ tydeligst ivaretar menneskerettighetenes krav om tilgang på effektive rettsmidler, men vil legge stor vekt på hva EOS-utvalget selv og høringsinstansene for øvrig mener om spørsmålet.

4.3.4.2 Domstolene

Kravet om effektive rettsmidler etter EMK artikkel 13 vil kunne være oppfylt med en effektiv klageadgang for domstolene. Grunnloven § 95 sier at enhver har rett til å få sin sak avgjort av en uavhengig og upartisk domstol innen rimelig tid. De nærmere vilkårene for å kunne fremme en sivil sak for domstolene er regulert i tvisteloven § 1-3, som gjengitt over. Kravet

[96] Se Innst. 146 S (2016-2017) fra kontroll- og konstitusjonskomiteen som ble behandlet i Stortinget 13. mars 2017.

[97] Se Innst. 431 L (2016-2017)

er at den som reiser saken, har et «rettskrav» og kan påvise et «reelt behov» for å få kravet avgjort i forhold til saksøkte. Det siste beror på en samlet vurdering av «kravets aktualitet og partenes tilknytning til det». Det må kunne legges til grunn at tvisteloven § 1-3, jf. Grl. § 95, sett i sammenheng med menneskerettsloven, vil gi adgang til norske domstoler for enhver person som har en prosedabel grunn til å hevde at vedkommende er blitt utsatt for en menneskerettskrenkelse, og som må anses å være innenfor den norske statens jurisdiksjon etter EMK artikkel 1, slik EMD til enhver tid tolker sistnevnte bestemmelse. Imidlertid kan det etter forholdene være et problem at det kan reises spørsmål om det foreligger en reell adgang til domstolsbehandling etter gjeldende norsk rett, jf. nærmere punkt 4.3.6 nedenfor.

4.3.5 Institusjonelle og materielle krav til en effektiv prøvingsrett

4.3.5.1 Summen av nasjonale rettsmidler

I vurderingen av hvorvidt det foreligger effektiv prøvingsrett i nasjonal rett, vil summen av nasjonale rettsmidler være avgjørende. Dette ble formulert av EMD i saken *Leander mot Sverige* av 26. mars 1987:

> "[A]lthough no single remedy may itself entirely satisfy the requirements of Article 13, the aggregate of remedies provided for under domestic law may do so".[98]

Det er videre et krav om at klageorganet må være *uavhengig*. Dette innebærer at organet må ha en uavhengig stilling i forhold til de myndigheter som beslutter å gjennomføre overvåkningen. EMD har uttalt at det er ønskelig at myndigheten etter EMK artikkel 13 ligger til den dømmende myndighet, i alle fall i siste instans, da domstolene gir de beste garantier for uavhengighet og upartiskhet.[99] EMD har imidlertid lagt til grunn at myndigheten ikke trenger å være en domstol («judicial authority»), men at hvis den ikke er det, vil graden av uavhengighet og garantiene som er tillagt den aktuelle myndigheten, være relevant for vurderingen av om prøvingsretten er effektiv.[100]

I *Klass m.fl. mot Tyskland* fant EMD at en parlamentarisk komité med balansert politisk sammensetning var tilstrekkelig.[101] I *Kennedy mot Storbritannia* kom EMD til at den britiske *Investigatory Powers Tribunal (IPT)* oppfylte kravene til et effektivt rettsmiddel.

---

[98] *Leander mot Sverige* av 26. mars 1987 avsnitt 77 (c), jf. også avsnitt 84.

[99] *Klass m. fl. mot Tysland* av avsnitt 55-56 og *Kennedy mot Storbritannia* av 18. mai 2010 avsnitt 167.

[100] Se f.eks. *Leander mot Sverige* av 26. mars 1987 avsnitt 77 og 83 og *Rotaru mot Romania* av 4 mai 2010 avsnitt 69. EMD uttalte sistenevnte sted følgende under henvisning til *Klass m.fl. mot Tyskland* av 6. september 1978: "The "authority" referred to in Article 13 may not necessarily in all instances be a judicial authority in the strict sense. Nevertheless, the powers and procedural guarantees an authority possesses are relevant in determining whether the remedy before it is effective (see the Klass and Others judgment cited above, p. 30, § 67). "

[101] I *Klass m.fl. mot Tyskland* 6. September 1978 avsnitt avsnitt 70, jf. avsnitt 21 og 23, uttalte EMD: "Although, according to the G 10, there can be no recourse to the courts in respect of the ordering and implementation of restrictive measures, certain other remedies are nevertheless open to the individual believing himself to be under surveillance: he has the opportunity of complaining to the G 10 Commission and to the Constitutional Court (see paragraphs 21 and 23 above). Admittedly, the effectiveness of these remedies is limited and they will in principle apply only in exceptional cases. However, in the circumstances of the present proceedings, it is hard to conceive of more effective remedies being possible."

Videre må klageorganet ha kompetanse til å vurdere klagens *materielle innhold* samt til å gi passende *oppreisning* («appropriate relief»).[102] Dette betyr at klageorganet må ha kompetanse til å vurdere om det har forekommet en menneskerettskrenkelse, samt til å forhindre videre krenkelse eller rette opp for begåtte krenkelser.[103] EMD vil også legge vekt på om klageorganet har tilgang til sikkerhetsgradert materiale nødvendig for å foreta en reell overprøving.[104]

I EMDs rettspraksis kan man lese ut et krav om at klagebehandlingen må kunne munne ut i at eventuelle menneskerettskrenkelser *opphører*. Spørsmålet er om dette innebærer at klageorganet skal måtte ha kompetanse til treffe en formelt bindende avgjørelse som stanser eller kompenserer for krenkelser. Enkelte har hevdet at utviklingen i EMD går i den retning.[105]

I *Centrum för Rättvisa mot Sverige* av 19. juni 2018[106] fant EMD etter en helhetsvurdering at summen av de tilgjengelige rettsmidlene i Sverige var effektive selv om ingen av klageorganene (Justititeombudsmannen eller Justitiekansleren) hadde kompetanse til å avsi rettslig bindende avgjørelser. EMD uttalte i avsnitt 176:

> «While their decisions are not legally binding, their opinions command great respect in Sweden. They also have the power to initiate criminal or disciplinary proceedings against public officials for actions taken in the discharge of their duties. As regards the Chancellor of Justice, it is also of relevance that (…) the Chancellor may receive and resolve individual compensation claims for alleged violation of the Convention."

Retten la vekt på at kontrollorganets uttalelser ble respektert tilnærmet fult ut av den svenske etterretningstjenesten. I tillegg viste retten til at dersom en menneskerettskrenkelse har fått alvorlige følger for klager som hadde medført økonomisk tap, kunne kontrollorganet også vurdere erstatning.

---

[102] *Leander mot Sverige* av 26. mars 1987 avsnitt 63 og *Rotaru mot Romania* avsnitt 67. EMD uttaler i *Rotaru mot Romania* avsnitt 67: "Article 13 guarantees the availability at national level of a remedy to enforce the substance of the Convention rights and freedoms in whatever form they might happen to be secured in the domestic legal order. This Article therefore requires the provision of a domestic remedy allowing the "competent national authority" both to deal with the substance of the relevant Convention complaint and to grant appropriate relief, although Contracting States are afforded some discretion as to the manner in which they conform to their obligation under this provision. The remedy must be "effective" in practice as well as in law (…).»

[103] Harris, O'Boyle & Warbrick, *Law of the European Convention on Human Rights*, third edition (2014), s. 769 og Erling Johannes Husabø i Dokument 16 (2015-2016) *Rapport til Stortinget fra Evalueringsutvalget for Stortingets kontrollutvalg for etterretnings- overvåknings- og sikkerhetstjeneste (EOS-utvalget)*, vedlegg 4, punkt 4.1.

[104] *Kennedy mot Storbritannia* av 18. mai 2010, hvor EMD kom til at det ikke forelå brudd på EMK.

[105] Under henvisning til EMDs frifinnelsesdom i *Leander mot Sverige* av 26. mars 1987 og senere domfellelse i *Segerstedt-Wiberg mot Sverige* av 6. juni 2006, har Husabø op.cit punkt 4.1 uttalt at det har vært en viss rettsutvikling i EMDs rettspraksis når det gjelder krav til bindende vedtak i klagesaker. Han mener at senere tids rettspraksis fra EMD tyder på at det må finnes en mulighet for bindende vedtak i klagesaker, i det minste når man ser summen av nasjonale rettsmidler under ett.

[106] Når dette skrives er dommen ikke rettskraftig

4.3.5.2 Notifikasjon

Et annet særskilt spørsmål er i hvilken grad personer som er blitt utsatt for informasjonsinnhenting må underrettes om dette for å legge til rette for en effektiv prøvingsrett.

EMD har lagt til grunn at den nasjonale lovgivningen må være tilstrekkelig klar til å gi borgerne en adekvat indikasjon på under hvilke omstendigheter offentlige myndigheter kan anvende hemmelige overvåkningstiltak, men at det selvfølgelig ikke kan kreves at den enkelte skal varsles eller på annen måte kunne forutse når overvåkningen vil bli gjennomført. I *Roman Zakharov mot Russland* uttalte EMD:[107]

> "The Court has held on several occasions that the reference to "foreseeability" in the context of interception of communications cannot be the same as in many other fields. Foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures."

EMD har lagt til grunn at hvis, og så snart, det kan skje uten å undergrave formålet med overvåkningstiltaket eller etterretningstjenestens virksomhet, bør i utgangspunktet den overvåkede personen notifiseres om overvåkningen i etterkant. Begrunnelsen for dette er å gi en reell klageadgang.[108] EMD kom i *Roman Zakharov mot Russland* til at klager ikke hadde tilgang til et effektivt rettsmiddel fordi rettsmidlene bare var tilgjengelige for personer som kunne dokumentere at deres kommunikasjon var blitt overvåket. I en slik situasjon mente EMD at det forelå en plikt til å etterhåndsunderrette om overvåkningen for å oppfylle kravene til et effektivt rettsmiddel.[109]

Forpliktelsen til etterhåndsvarsling er imidlertid *ikke* et absolutt krav hvor det foreligger en klageadgang som ikke er avhengig av at klager er underrettet om informasjonsinnhentingen eller av at klager beviser at denne har funnet sted. I *Roman Zakharov mot Russland* uttaler EMD med videre henvisning til *Kennedy mot Storbritannia*:[110]

> "By contrast, in the case of Kennedy the absence of a requirement to notify the subject of interception at any point in time was compatible with the Convention, because in the United Kingdom any person who suspected that his communications were being or had been intercepted could apply to the Investigatory Powers Tribunal, whose jurisdiction did not depend on notification to the interception subject that there had been an interception of his or her communications (see Kennedy, cited above, § 167)."

Dette bekreftes av EMD i *Centrüm för Rättvisa mot Sverige* (jf. bl.a. avsnitt 177-176).[111]

---

[107] *Roman Zakharov mot Russland* avsagt 4. desember 2015 avsnitt 229.

[108] Ibid. avsnitt 287.

[109] Ibid. avsnitt 298

[110] Ibid. avsnitt 234 og 288.

[111] Dommen er når dette skrives ikke rettskraftig.

EMD har også uttalt at så lenge det er et effektivt kontrollregime på plass, trenger man ikke nødvendigvis å ha et system for underretning om at hemmelig overvåkning har funnet sted:

> "Where secret surveillance is concerned, objective supervisory machinery may be sufficient as long as the measures remain secret. It is only once the measures have been divulged, that legal remedies must become available to the individual".[112]

Departementet forstår EMDs rettspraksis slik at etterhåndsunderretning om hemmelig overvåkning ikke er noe absolutt krav dersom det foreligger en vid, effektiv klageadgang kombinert med en effektiv kontrollmekanisme.

Justis- og beredskapsdepartementet konkluderte på lignende måte i sin vurdering av om det burde innføres krav om underretning ved bruk av skjulte tvangsmidler i forebyggende øyemed etter politiloven § 17 e.[113] Justis- og beredskapsdepartementet kom til at særtrekkene ved PSTs forebyggende virksomhet som regel vil gjøre det nødvendig å holde opplysninger om bruken av tvangsmiddelet og opplysningene som bruken resulterte i hemmelig for den som ble utsatt for inngrepet. Departementet fremhevet at det her var snakk om handlinger som truer sikkerheten i samfunnet og som ofte blir begått av lukkede og profesjonelle miljøer. Det å oppdage og avverge slike mulige trusler tidligst mulig utgjør kjernevirksomheten til sikkerhetstjenestene. Justis- og beredskapsdepartementet kunne ikke se at det kunne utledes noe absolutt krav til underretning etter EMK artikkel 8, og kom til at kontrollen med bruken av skjulte metoder var godt ivaretatt i og med domstolskontrollen og den offentlig oppnevnte advokaten i forkant, og forvaltningskontrollen og den parlamentariske kontrollen i etterkant av tvangsmiddelbruken. I tillegg ble det vektlagt at tillatelse for bruk av skjulte tvangsmidler ble gitt på strenge vilkår og at disse bare gjaldt for et meget begrenset saksområde, nemlig terrorhandlinger, ulovlig etterretningsvirksomhet og de mest alvorlige formene for vold eller trusler mot representanter for de øverste statsmyndigheter mv. Disse oppgavene ble ansett for å være i kjernen av den nasjonale handlefrihet. Forsvarsdepartementet mener at de samme hensyn må gjøre seg gjeldende for utenlandsetterretning, som er i kjerneområdet av nasjonal sikkerhet.

Spørsmålet i det følgende blir dermed om klageadgangen etter norsk rett for de som mener seg utsatt for et uforholdsmessig inngrep fra Etterretningstjenesten, oppfyller de institusjonelle og materielle kravene om effektiv prøvingsrett som beskrevet over, herunder om klageadgangen er tilstrekkelig vid til at det ikke må oppstilles krav om etterfølgende underretning.

4.3.6 Vurdering av om EOS-utvalgets og domstolenes klagebehandling er tilstrekkelig til å oppfylle de institusjonelle og materielle kravene om effektiv prøvingsrett

4.3.6.1 Uavhengighet

Det er klart at både EOS-utvalget og domstolene oppfyller kravet til uavhengighet fra de myndighetene som beslutter å gjennomføre informasjonsinnhentingen. EOS-utvalget utnevnes av Stortinget, og det er ikke tvil om at utvalget er selvstendig. Dette følger eksplisitt

[112] Se slik f.eks. *Segerstedt-Wiberg m.fl. mot Sverige* avsagt 6. juni 2006, avsnitt 117

[113] Se Prop. 68 L Endringer i straffeprosessloven mv. (skjulte tvangsmidler) (2015-2016) punkt 13.5.8 side 122-123

av EOS-kontrolloven § 1 femte ledd om at utvalget skal «uføre sitt verv selvstendig og uavhengig».

4.3.6.2 Kompetanse til å prøve sakens materielle innhold

Det er heller ikke tvil om at EOS-utvalget har kompetanse til å vurdere sakens materielle innhold, dvs. om det har funnet sted en menneskerettskrenkelse. I henhold til EOS-kontrolloven § 5 annet ledd skal utvalget foreta «de undersøkelser som klagen tilsier». I henhold til § 2 første ledd nr. 1 skal formålet med utvalgets kontroll blant annet være «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». Videre har utvalget tilstrekkelig innsyn i Etterretningstjenestens virksomhet til å foreta en reell prøving av klagene, jf. blant annet EOS-kontrolloven § 8 som gir utvalget rett til innsyn i graderte opplysninger i den grad det er nødvendig ut fra kontrollformålet.

Det kan reises spørsmål ved om domstolene har den samme kompetansen til fullt ut å prøve sakens materielle innhold. Spørsmålet har vært reist om tvisteloven § 22-1 vil kunne være til hinder for en reell domstolsprøving.[114] I henhold til denne bestemmelsen kan det ikke føres bevis om noe som holdes hemmelig av hensyn til rikets sikkerhet eller forholdet til fremmed stat. Føring av slike bevis krever samtykke fra Kongen (regjeringen i statsråd). Det har vært anført at den utøvende makt dermed kan blokkere at slike bevis føres for retten, og at dette kan være et faktisk hinder for domstolsprøvingen. Det må påpekes at bevisforbudsregelen *kan* utgjøre et hinder for materiell vurdering av saken, men den *må* ikke gjøre det. Det må forventes at regjeringen vurderer en forespørsel konkret, derunder hvilke tiltak som kan gjøres for å sikre forsvarlig informasjonssikkerhet knyttet til eventuell bevisføring, samt at regjeringen tar stilling til hvilken annen adgang til effektive rettsmidler som finnes for klager, før den konkluderer i den enkelte sak. Selv om bevisforbudsregelen reiser enkelte konkrete utfordringer mener departementet at dette *ikke i seg selv* betyr at adgangen til domstolen er stengt i denne typen saker og at domstolen dermed ikke fyller kravet til et effektivt rettsmiddel.

I alle tilfeller vil eksistensen av bevisforbudsregelen heller ikke bety at det ikke foreligger et effektivt rettsmiddel etter norsk rett dersom EOS-utvalget alene kan anses som et tilstrekkelig effektivt rettsmiddel. Som det følger ovenfor, må det kunne legges til grunn at EOS-utvalget har tilstrekkelig kompetanse til å foreta en reell overprøving av saken.

4.3.6.3 Kompetanse til å sikre at en krenkelse opphører

Neste spørsmål er om domstolenes og EOS-utvalgets klagebehandling tilfredsstiller kravet om at klagebehandlingen må munne ut i at en eventuell menneskerettskrenkelse opphører eller rettes opp.

Domstolene har kompetanse til å sikre at en menneskerettskrenkelse opphører og dette behandles derfor ikke videre her.

EOS-utvalget har bare «rett til å uttale sin mening», jf. EOS-kontrolloven § 14 første ledd, altså ikke til å treffe bindende vedtak. EOS-utvalget skal riktignok, når det avgir uttalelser som oppfordrer til å iverksette tiltak eller treffe beslutninger, be mottaker om å gi

[114] Erling Johannes Husabø reiser denne problemstillingen i sin betenkning til Evalueringsutvalgets rapport, se Dokument 16 (2015-2016) *Rapport til Stortinget fra Evalueringsutvalget for Stortingets kontrollutvalg for etterretnings- overvåknings- og sikkerhetstjeneste (EOS-utvalget)*, vedlegg 4, punkt 4.3.

tilbakemelding om hva som blir foretatt, jf. § 14 siste ledd. Dette innebærer at dersom utvalget ber om at en feil rettes opp, vil utvalget få en tilbakemelding om dette er blitt gjort eller ikke.

Den norske modellen bygger på kontroll utført av et parlamentarisk oppnevnt organ som på vegne av Stortinget kontrollerer etterretnings-, overvåknings- og sikkerhetstjeneste som utføres av den offentlige forvaltning. EOS-utvalgets kontroll skiller seg fra den direkte parlamentariske kontrollen som bare Stortinget selv kan utøve, ved at utvalgets kontroll hovedsakelig er rettet mot EOS-tjenestene som del av den underliggende forvaltning, mens Stortingets kontroll er rettet mot statsrådenes handlinger og ansvar.[115] EOS-utvalgets kontroll er både ment å legge grunnlag for Stortingets behandling av kontrollsaker og utgjøre et selvstendig kontrollelement. Utvalget er således et hjelpemiddel for Stortinget til å sikre at den etterfølgende parlamentariske kontrollen blir effektiv, og til å verne borgerne mot urett.[116] Selv om utvalget på denne måten er en viktig ressurs for Stortinget, er EOS-utvalget et selvstendig og uavhengig organ jf. EOS-kontrolloven § 1 siste ledd, som presisert over.

EOS-utvalget ble opprettet i 1996. Den historiske årsaken bak opprettelsen av den norske kontrollmodellen var at det over tid hadde bygget seg opp en mistillit knyttet til EOS-tjenestene og kontrollen regjeringen drev med sine egne tjenester. Dessuten mente man at EOS-tjenestenes særegenheter og fordekte virksomhet krevet en særskilt form for kontroll. For å kompensere manglende innsyn i tjenestenes til dels inngripende virksomhet ble EOS-utvalget opprettet og gitt i oppgave å kontrollere tjenestene på vegne av Stortinget og den norske befolkning.[117] Denne ordningen har nylig blitt evaluert av Evalueringsutvalget for EOS-tjenestene. Evalueringsutvalget uttaler i sin rapport at EOS-utvalgets forankring i Stortinget først og fremst er en styrke ved dagens kontrollmodell og utvalgets arbeid, og de anbefaler at ordningen med et stortingsoppnevnt kontrollorgan bør videreføres. Kombinasjonen av et kontrollorgan som har tilstrekkelig avstand til den utøvende makt, samtidig som det fungerer som et hjelpemiddel for Stortingets parlamentariske kontroll blir trukket frem som positivt. Evalueringsutvalget uttaler på side 126 i rapporten:

> «Utvalgets kontroll av om tjenestene respekterer individuelle rettigheter og overholder gjeldende regelverk går også langt utover det Stortinget selv, eller en parlamentarisk komité, ville ha kapasitet og kompetanse til, og bidrar med dette til vern av individuelle rettigheter og samfunnsmessige interesser. I tillegg ivaretar kontrollordningen behovet for å holde sikkerhetsgradert informasjon innenfor en begrenset krets.»

Samtidig er det visse iboende begrensninger som følger av den valgte kontrollmodellen. Begrensningene har sitt utspring i vårt konstitusjonelle system og maktfordelingsprinsippene mellom den utøvende og lovgivende makt. Evalueringsutvalget uttaler dette om begrensningene i sin rapport side 126:

> «Et Stortingsoppnevnt kontrollorgan må imidlertid være underlagt enkelte begrensninger som følger av fordelingen av makt og ansvar mellom Stortinget og regjeringen. Én viktig konsekvens er at EOS-utvalget ikke kan avsi bindende avgjørelser, instruere de kontrollerte organene eller benyttes av disse til konsultasjoner, men at formålet med kontrollen er «rent kontrollerende» og at utvalget skal følge prinsipper om etterfølgende

[115] Se Evalueringsutvalgets rapport Dokument 16 (2015-2016) s. 125 og Dokument nr. 14 (2002-2003) s. 19 og 54

[116] Se Dokument 16 (2015-2016) s. 125 og NOU 1994:4 s. 48

[117] Se Dokument 16 (2015-2016) s. 126

kontroll.[118] En annen konsekvens er at EOS-utvalget må være tilbakeholdne med å overprøve EOS-tjenestenes skjønnsutøvelse.[119] Begrunnelsen for dette er at EOS-utvalget ikke skal ha styringsfunksjoner overfor tjenestene, ettersom konstitusjonelle forhold tilsier at regjeringen har styringsrett og ansvar for den offentlige forvaltningen. Videre skyldes begrensningene at EOS-utvalget ikke skal kunne tillegges ansvar for tjenestenes handlinger og at Stortingets etterfølgende handlefrihet skal opprettholdes.[120] En siste konsekvens av den parlamentariske forankringen er at EOS-utvalget skal drive legalitetskontroll, og ikke kontrollere hensiktsmessigheten og effektiviteten av tjenestenes handlinger. Kontroll med disse aspektene ved tjenestenes virksomhet er dermed i sin helhet statsrådens ansvar.»

Dersom man skulle gi EOS-utvalget beslutningsmyndighet overfor Etterretningstjenestens virksomhet ville dette rokke ved grunnleggende prinsipper i vårt statsrettslige system og maktfordelingen mellom regjering og Storting som fremhevet av Evalueringsutvalget i uttalelsen over. Departementet kan ikke anbefale en slik løsning. Dersom man skulle mene at kravene til effektiv rettergang etter EMK artikkel 13 ikke er oppfylt antar departementet derfor at hele kontrollsystemet som sådan må settes under lupen.

Evalueringsutvalget løfter selv spørsmålet om kravet til effektivt rettsmiddel etter EMK artikkel 13 er oppfylt, særlig med tanke på utvalgets manglende adgang til å avsi bindende avgjørelser, men uten å konkludere. Også Evalueringsutvalget antyder at dersom større strukturelle endringer skal gjøres, vil dette kreve en bred evaluering av det norske kontrollsystemet.[121] Slik departementet ser det vil dette kreve et selvstendig utredningsarbeid som, gitt EOS-utvalgets forankring, initieres av Stortinget selv.

Departementet mener i alle tilfeller at problemstillingen ikke kommer på spissen fordi den norske kontrollordningen bygger på et system der, selv om EOS-utvalget ikke formelt kan instruere tjenestene eller forvaltningen, det er utviklet gode og effektive systemer for oppfølging og håndtering av rapporterte avvik. Det vises i denne forbindelse til kapittel 6.10 som beskriver kontrollen av Etterretningstjenesten som EOS-utvalget utfører. Av betydning for herværende drøftelse er særlig EOS-utvalgets rolle som hjelpemiddel i Stortingets kontroll. Dersom ikke Etterretningstjenesten på eget initiativ eller etter instruks fra Forsvarsdepartementet, avslutter aktivitet EOS-utvalget mener er ulovlig, vil Stortinget kunne benytte sitt virkemiddelapparat overfor konstitusjonelt ansvarlig statsråd. I tråd med det parlamentariske system innebærer dette i sin ytterste konsekvens at Stortinget kan fremme mistillit mot statsråden, som igjen kan føre til at regjeringen går av. Det er liten tvil om at dette har en disiplinerende effekt på forvaltningen og at kritikk fra Stortingets kontrollorganer eller Stortinget selv tas på høyeste alvor i vårt konstitusjonelle system. Departementet vurderer derfor at EOS-utvalgets kontroll i praksis alltid følges opp av EOS-tjenestene og forvaltningen, eventuelt at saken blir håndtert i de formelle prosessene mellom Stortinget og regjeringen. Et krav om at klageorganet skal kunne sørge for at menneskerettighetskrenkelser opphører må derfor anses ivaretatt.

[118] Se lov av 3. februar 1996 nr. 7 om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-kontrolloven) § 2 siste ledd

[119] NOU 1994:4 *Kontrollen med de hemmelige tjenester* side 35 og Ot.prp nr 84 (1993-1994) side 11-12

[120] NOU 1994:4 *Kontrollen med de hemmelige tjenester* side 34, Ot.prp nr 84 (1993-1994) side 11 og Innst. O nr. 11 (1994-1995) s. 8

[121] Se Dokument 16 (2015-2016) s.129

4.3.6.4 Kompetanse til å sikre passende oppreisning («appropriate relief»)

Et annet spørsmål er om klageorganet har anledning til å gi passende oppreisning («appropriate relief»). Det er ingen tvil om at domstolen kan idømme krav om erstatning. Spørsmålet er om EOS-utvalget har myndighet til å sørge for passende oppreisning der det er konstatert en krenkelse. Evalueringsutvalget reiste spørsmålet om EOS-utvalget skulle gis anledning til å anbefale at EOS-tjenestene utbetalte erstatning til personer som har vært utsatt for menneskerettskrenkelser.[122] Utvalget konstaterte at problemstillingen reiser spørsmål av både prinsipiell og praktisk art, og at den derfor burde vurderes som ledd i en helhetlig vurdering av det norske systemet. Evalueringsutvalget ville derfor ikke foreslå endringer i EOS-utvalgets regelverk på daværende tidspunkt.

EOS-utvalget har imidlertid selv anbefalt at utvalget bør kunne uttale seg om det offentliges erstatningsansvar i konkrete saker, etter modell av sivilombudsmannsloven.[123] Det vises til EOS-utvalgets årsmelding for 2016 punkt 10. Det var særlig sikkerhetsklareringssakene knyttet til NSMs ansvarsområde som foranlediget anbefalingen, men anbefalingen er prinsipielt ikke begrenset til denne sakstypen. EOS-utvalget konkluderer med at det ikke foreligger konstitusjonelle hindringer for en regel om at utvalget kan uttale seg om erstatningsansvar, og mener gode grunner taler for en slik regel også ut over sammenligningen med Sivilombudsmannens regelverk og praksis.

Departementet kan i likhet med EOS-utvalget ikke se at det foreligger vesentlige innvendinger mot at utvalget kan uttale seg om og eventuelt anbefale erstatningsansvar fra det offentlige i konkrete saker, uten å instruere tjenestene eller forvaltningen som sådan. Det dreier seg om få saker, men vil kunne styrke den enkeltes adgang til effektive rettsmidler ved alvorlige krenkelser. Selv om forvaltningen kan ha en annen oppfatning av om vilkårene for erstatning foreligger, vil manglende oppfølging bli mer synlig og dermed styrke klagerens rettsstilling. Utvalget er allerede i dag neppe fullstendig forhindret fra å ytre seg overfor forvaltningen om erstatningsspørsmålet, og en formalisering av adgangen vurderes ikke til å ha vesentlige konsekvenser for verken Etterretningstjenesten eller de øvrige EOS-tjenestene.

Departementet vil derfor foreslå følgende endring i EOS-kontrolloven § 15:

§ 15 første ledd tredje punktum i lov 3. februar 1995 nr. 7 om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-kontrolloven) skal lyde:

> 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.*

Departementet mener at man med en slik lovfastsatt uttalelsesmulighet balanserer de menneskerettslige krav om å sikre passende oppreising med de overordnede hensyn som ligger til grunn for at EOS-utvalget ikke kan instruere EOS-tjenestene som redegjort for over.

4.3.6.5 Konklusjon

Oppsummeringsvis vurderer departementet at tilgangen til effektive rettsmidler etter norsk rett er tilstrekkelig å oppfylle kravet etter EMK artikkel 13.

---

[122] Evalueringsutvalgets rapport Dokument 16 (2015-2016) s. 129. Problemstillingen drøftes også i vedlegg 4 s. 253

[123] Lov om Stortingets ombudsmann for forvaltningen av 22. juni 1962 nr. 8 § 10

Klageadgangen vurderes dessuten å være tilstrekkelig vid til at det ikke kan oppstilles et krav om at Etterretningstjenesten må underrette personer som har vært gjenstand for tjenestens informasjonsinnhenting.

5 Formål og virkeområde

5.1 Formål

5.1.1 Gjeldende rett

Formålet med gjeldende etterretningstjenestelov fremgår av § 1 i loven:

Formålet med denne lov er å

a. legge forholdene til rette slik at Etterretningstjenesten effektivt kan bidra til å kartlegge og motvirke ytre trusler mot rikets selvstendighet og sikkerhet og andre viktige nasjonale interesser, og
b. trygge tilliten til og sikre grunnlaget for kontroll av Etterretningstjenestens virksomhet.

I forarbeidene ble det blant annet utdypet at begrepet «rikets selvstendighet og sikkerhet» er en utpreget rettslig standard som kan utvikle seg i takt med samfunnsutviklingen og som man blant annet gjenfinner i beredskapsloven § 3. Det samme poenget ble understreket i relasjon til begrepet «viktige nasjonale interesser».

5.1.2 Forslag til ny regulering

Departementet fremmer i lovutkastet her en presisert, revidert og uttømmende oppgavebeskrivelse for Etterretningstjenesten. Det innebærer blant annet at begrepet «andre viktige nasjonale interesser» i gjeldende oppgavebeskrivelse ikke lenger vil være et relevant vilkår. Også andre grunner taler for å gjøre enkelte språklige og strukturelle endringer i formålsbeskrivelsen. Departementet har sett hen til begrepsbruken i ny lov om nasjonal sikkerhet (sikkerhetsloven),[124] og mener formuleringene i sikkerhetslovens formålsbestemmelse om «å bidra til å trygge Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser» også er dekkende for Etterretningstjenestens samfunnsoppdrag.

Begrepet *nasjonale sikkerhetsinteresser* er et fellesbegrep som dekker både trusler mot statssikkerheten, alvorlige trusler mot samfunnssikkerheten og andre forhold som kan ha relevans for ivaretakelse av prioriterte norske og allierte utenriks-, forsvars- og sikkerhetspolitiske interesser, se mer om dette i punkt 7.4. Nasjonale sikkerhetsinteresser handler både om å verne nasjonens interesser mot trusler, samt å fremme nasjonale interesser og verdier overfor omverdenen.

I tillegg mener departementet at det i en formålsparagraf for Etterretningstjenesten bør fremkomme at en vesentlig oppgave er å bidra til å kartlegge og motvirke *utenlandske trusler* mot Norge og norske interesser.

[124] Lov av 1. juni 2018 nr. 24 om nasjonal sikkerhet (sikkerhetsloven) (foreløpig ikke trådt i kraft)

Formålet knyttet til å trygge tilliten og sikre grunnlaget for kontroll er fortsatt et viktig formål, og foreslås videreført i lovutkastet.

Departementet tilrår å tilføye et tredje element i formålsbestemmelsen, som synliggjør den relativt sett økte betydningen av menneskerettighetene og andre sentrale rettsprinsipper og demokratiske verdier i en rettsstat, herunder rettssikkerhet for den enkelte. Lovutkastet her er i seg selv et resultat blant annet av behovet for å modernisere de rettslige rammene for utenlandsetterretning i tråd med menneskerettighetenes krav til klare hjemler for inngrep og rettssikkerhetsgarantier. Også innholdet i bestemmelsene i lovforslaget vil sørge for at etterretningsvirksomheten skal utøves i samsvar med disse prinsippene.

Departementet foreslår etter dette følgende lovbestemmelse:

§ 1-1 *Formål*

Loven skal

a. bidra til å trygge Norges suverenitet, territorielle integritet, demokratiske styreform og andre nasjonale sikkerhetsinteresser, herunder forebygge, avdekke og motvirke utenlandske trusler mot Norge og norske interesser,
b. bidra til å trygge tilliten til og sikre grunnlaget for kontroll med Etterretningstjenestens virksomhet, og
c. sørge for at Etterretningstjenestens virksomhet utøves i samsvar med menneskerettighetene og øvrige grunnleggende rettsprinsipper og verdier i et demokratisk samfunn.

5.2 Lovens virkeområde

5.2.1 Innledning

Departementet foreslår at loven bare skal gjelde for Etterretningstjenestens utøvelse av *etterretningsvirksomhet*, og ikke for administrativ, forvaltningsmessig eller annen virksomhet som utøves av Etterretningstjenesten. Begrepet etterretningsvirksomhet vil derfor være gjenstand for nærmere fastleggelse i det følgende. Videre vil lovens geografiske/stedlige virkeområde omtales. Deretter tas det stilling til *hvem* loven gjelder for organisatorisk og personellmessig. Til sist redegjøres særskilt for lovens anvendelse for etterretningsvirksomhet i internasjonale militære operasjoner og under sikkerhetspolitiske kriser og væpnet konflikt som berører norsk territorium.

Hovedformålet med den foreslåtte virkeområdebestemmelsen er å kodifisere gjeldende rett og etablert praksis. I de enkelte underkapitler vil det bli redegjort for gjeldende rettstilstand og eventuelle forslag om endringer i forhold til dagens virkeområde.

5.2.2 Hva som menes med etterretningsvirksomhet (*ratione materiae*)

I forsvarssjefens etterretningsdoktrine, utgitt i mai 2013, er etterretningsvirksomhet – i betydningen *utenlandsetterretningsvirksomhet* – definert slik:

> «Etterretning er systematisk innhenting og bearbeiding av informasjon som angår utenlandske forhold ervervet med åpne og fordekte metoder i en statlig legal ramme. Produktene skal redusere usikkerhet, skape forståelse og har ofte en prediktiv karakter. Begrepet brukes om produktet, aktiviteten og organisasjonen som utøver aktiviteten.»

Definisjonen bygger på NATOs tilsvarende definisjon. Den er ment å skille utenlandsetterretning fra annen innsamling og bearbeiding av informasjon, enten det gjøres av andre offentlige myndigheter (f.eks. politiets/PSTs kriminaletterretning) eller private

aktører (f.eks. såkalt *business intelligence*). Definisjonen tar imidlertid ikke stilling til alle avgrensningsspørsmål. Det må sondres mellom etterretningsvirksomhet og annen virksomhet som kan ligne på etterretningsvirksomhet. Særlig gjelder det noen typer virksomhet i Forsvaret som benytter sensorer og metoder for informasjonsinnhenting som også kan benyttes for etterretningsformål. Typisk vil det gjelde innhenting av informasjon blant annet i den hensikt å utøve/gjennomføre rekognosering, oppklaring, styrkebeskyttelse, sikkerhetstjeneste, elektronisk krigføring, informasjonsoperasjoner og myndighetsutøvelse. Samme sensorer og metoder kan benyttes til å løse ulike oppdrag. Skillet mellom etterretningsvirksomhet og annen virksomhet går i hovedsak på aktivitetens intensjon og hva informasjonen er ment benyttet til. For eksempel vil informasjonsinnhenting for å monitorere og observere et område eller en aktør i den hensikt å bygge et sanntids situasjonsbilde, være en form for operativ overvåking eller suverenitetshevdelse. Aktiviteten anses da ikke som *etterretningsvirksomhet* i lovens forstand. Derimot vil aktiviteten være etterretningsvirksomhet dersom formålet med den samme innhentingen er å tilegne seg informasjon som skal inngå i en vurdering av en aktørs intensjoner, evner, kapasiteter, taktikk, strategi, trusselvirksomhet eller –potensiale eller utnyttelse/bruk av et objekt eller område eller lignende. Dette er oppdrag som ligger i kjerneområdet av Etterretningstjenestens samfunnsoppdrag, se høringsnotatet kapittel 7 om tjenestens oppgaver.

Departementet vurderer at det ikke er behov for å utforme en detaljert grensedragning mellom etterretningsvirksomhet og annen virksomhet i loven. I lovforslagets forstand vil all virksomhet som har et *etterretningsformål*, dvs. å ivareta en eller flere av Etterretningstjenestens oppgaver etter lovforslagets kapittel 3, være å anse som etterretningsvirksomhet. Hvis formålet er et annet, hjemles og reguleres virksomheten ikke av lovforslaget. Som en integrert del i Forsvaret kan for eksempel også Etterretningstjenesten i en militær operasjon gjennomføre tiltak for styrkebeskyttelse, men informasjonsinnhenting for dette formålet vil ikke reguleres av lovforslaget her, men av operasjonens mandat og folkeretten. Informasjonsinnhenting som ledd i forebyggende sikkerhetstjeneste reguleres heller ikke av dette lovforslaget, men reglene i sikkerhetsloven med forskrifter. I noen tilfeller har sjefen for Etterretningstjenesten et koordineringsansvar som går ut over det å drive *utenlandsetterretning*, for eksempel et koordinerende ansvar for cyberoperasjoner i Forsvaret, inkludert for defensive cyberoperasjoner (som er å anse som sikkerhetstjeneste i Forsvaret). Behandling av informasjon som ikke stammer fra etterretningsvirksomhet skal da ikke behandles etter bestemmelsene i lovforslaget her, men etter annen relevant lovgivning avhengig av type informasjon og formålet med behandlingen.

Bistand til politiet etter politiloven § 27 a og bistandsinstruksen[125] er ikke å anse som *etterretningsvirksomhet* etter lovforslaget, selv om Forsvaret – herunder Etterretningstjenesten – etter anmodning kan bistå politiet med etterretningskapasiteter. Bistand til politiet gjennomføres innenfor rammen av politiets rettsgrunnlag og instruksjonsmyndighet. Muligheten for Etterretningstjenesten til å bistå politiet er likevel omhandlet i lovforslaget. Bestemmelsen er tatt inn for å klargjøre at slik bistand ikke strider mot forbudet mot at Etterretningstjenesten utfører oppgaver med politiformål og for å klargjøre at Etterretningstjenesten ikke kan bistå politiet med informasjon som stammer fra tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon.

[125] Kongelig resolusjon av 16. juni 2017 nr. 789 om Forsvarets bistand til politiet

5.2.3 Geografisk/stedlig virkeområde (*ratione loci*)

En utenlandsetterretningstjeneste opererer over store deler av verden. Lovforslaget gjelder i utgangspunktet globalt, og uavhengig av om etterretningsvirksomheten utøves i, på eller fra et område eller overfor en person som er underlagt norsk jurisdiksjon. Loven vil således få anvendelse for all etterretningsvirksomhet som Etterretningstjenesten utøver uavhengig av hvor virksomheten geografisk utøves eller har effekt. Spørsmålet om menneskerettighetenes ekstraterritorielle anvendelse er drøftet under punkt 4.1.3. Som det fremkommer her vil jurisdiksjonsspørsmålet i utgangspunktet måtte vurderes konkret i det enkelte tilfellet. Lovforslaget er imidlertid utformet for å tilfredsstille menneskerettighetene, uavhengig av utfallet av den konkrete jurisdiksjonsvurderingen.

At lovforslaget i utgangspunktet gjelder globalt følger av at virkeområdebestemmelsen ikke angir særskilte geografiske bestemmelser. At Etterretningstjenesten er underlagt territorielle begrensninger for innhenting rettet mot personer i Norge, jf. lovforslagets kapittel 4, innebærer ikke at lovens virkeområde som sådan er geografisk avgrenset.

Ovennevnte følger etter departementets syn allerede av tolkning av gjeldende rett, og innebærer ingen materielle endringer ut over at man hittil ikke har tatt direkte stilling til om gjeldende regelverk kommer til anvendelse for etterretningsvirksomhet som utøves eller får effekt utenfor norsk jurisdiksjonsområde.

Departementet vil for øvrig presisere at gjeldende etterretningstjenestelov bruker begrepet «norsk territorium». Dette er tolket til å omfatte også Svalbard, Jan Mayen og bilandene. Departementet foreslår å videreføre denne forståelsen i lovforslaget her. Angivelsen av territoriet er av betydning for de territorielle begrensningene som følger av lovforslagets kapittel 4, se nærmere om dette i punkt 8.4.2.1 og 8.4.2.3.

5.2.4 Organisatorisk og personellmessig virkeområde (*ratione personae*)

5.2.4.1 Den strategiske Etterretningstjenesten

Gjeldende lov gjelder kun for den strategiske Etterretningstjenesten. Om dette heter det i forarbeidene:[126]

> «Med 'Etterretningstjenesten' forstås her tjenesten som organisatorisk, ikke funksjonelt, begrep. Det kan således slås fast at E-tjenesten er en integrert del av Forsvaret. Funksjonene fremgår imidlertid av de oppgaver tjenesten pålegges. Det fremgår implisitt av beskrivelsen av disse oppgavene at lovforslaget bare vil omfatte den strategiske etterretningstjeneste. Lovforslaget vil ikke få anvendelse for Forsvarets taktiske etterretningselementer (felteterretning mv); dvs. etterretningsoppgaver som den enkelte militære enhet utfører i en øvings-, beredskaps- eller stridssituasjon for å innhente informasjon om vær, lende, fiendtlige styrker osv. Det anses tilstrekkelig å klargjøre dette i motivene her.»

Departementet foreslår å videreføre denne grensedragningen i lovforslaget. Etterretningstjenesten er en integrert del av Forsvaret, men er også en nasjonal og sektorovergripende sivil og militær utenlandsetterretningstjeneste. Etterretningstjenesten er en selvstendig organisatorisk statlig enhet, men er ingen egen etat direkte underlagt Forsvarsdepartementet. Tjenesten inngår i etaten Forsvaret, med forsvarssjefen som etatssjef. Tjenesten er underlagt særlige styrings-, rapporterings- og kontrollordninger, har

[126] Ot. prp. nr. 50 (1996-1997) s. 6.

lovpålagte sektorovergripende oppgaver, har et internasjonalt samarbeidsnettverk og har en rettslig og faktisk adgang til inngripende metodebruk som skiller seg fra Forsvaret for øvrig. Dette tilsier at en særlov på området fortsatt kun bør være organisatorisk avgrenset til å gjelde for Etterretningstjenesten. Det bør likevel vurderes om loven i enkelte situasjonsbestemte tilfeller likevel bør gjøres gjeldende for etterretningsvirksomhet i andre deler av Forsvaret.

5.2.4.2 Etterretningsvirksomhet i andre deler av Forsvaret

Øvrige deler av Forsvaret kan rettslig sett ikke utøve etterretningsvirksomhet i eller fra Norge som er av en slik karakter at den krever særskilt hjemmel i lov. Øvrige avdelinger i Forsvaret har ingen innhentingshjemmel i fredstid i Norge. Det har ved ulike anledninger vært reist spørsmål om etterretningselementer i andre deler av Forsvaret likevel bør underlegges lov om Etterretningstjenesten. Departementet mener dette verken er nødvendig eller ønskelig.

En videreføring av anvendelsesområdet betyr imidlertid ikke at etterretningsenheter i Forsvaret må holde seg uvirksomme i påvente av en eventuell væpnet konflikt. For det første vil etterretningsenheter drive trening og øving for hovedoppdraget knyttet til etterretningsstøtte til Forsvarets operative enheter i beredskaps- og konfliktsituasjoner. For det andre kreves ingen særskilt hjemmel i lov til å drive grunnleggende og annen etterretningsproduksjon i fredstid, så lenge det ikke er tale om inngripende metodebruk for innhenting av etterretningsinformasjon som krever hjemmel i lov. For det tredje kan øvrige avdelinger og personer i Forsvaret operativt utøve etterretningsvirksomhet i følgende alternative situasjoner:

a. *Ved kommandooverføring til Etterretningstjenesten*. Det er praksis for at andre enheter og personer i Forsvaret midlertidig kan inngå som del av Etterretningstjenesten og dermed operere innenfor Etterretningstjenestens rettsgrunnlag. Dette gjøres både for å kvalifisere andre enheter og personer i Forsvaret, og for å avhjelpe ressurskrevende oppgaver i tjenesten. De vil da være underlagt lov om Etterretningstjenesten, og også ellers behandles som enhver annen i tjenesten. Det kreves i disse tilfellene at man er reelt underlagt Etterretningstjenesten og står under kontroll av sjefen for Etterretningstjenesten. For å tilfredsstille dette kriteriet kreves minimum kommandoforholdet operativ kontroll til sjefen for Etterretningstjenesten eller en formell midlertidig beordring av enkeltpersoner til Etterretningstjenesten. Kommandooverføringen kan være av midlertidig og gjentakende karakter, men det skal være tydelig skille både formelt og i praksis for når enheten/personen er under kommando av sjefen for Etterretningstjenesten og når enheten/personen ikke er det. I lovforslaget fremkommer dette som en presisering i utkast til § 1-2 andre ledd om at loven også gjelder for andre personer og enheter for det tidsrom de er under kommando av sjef Etterretningstjenesten.

b. *Ved samtykke fra sjefen for Etterretningstjenesten til å utøve etterretningsvirksomhet*. Dette alternativet medfører ikke at lov om Etterretningstjenesten og tilhørende regelverk kommer til anvendelse, og innebærer ikke at enheter eller personell underlegges kommando eller instruksjonsmyndighet fra sjefen for Etterretningstjenesten. Dette alternativet, som bygger på interne bestemmelser i Forsvaret utgitt av sjefen for

Etterretningstjenesten som fagmyndighet for all etterretning i Forsvaret, behøver derfor ikke reguleres i lovforslaget. Samtykke fra sjefen for Etterretningstjenesten er derfor kun aktuelt for etterretningsvirksomhet som ikke 1) medfører innhenting som krever hjemmel i lov, eller 2) ved tilstedeværelse innenfor annen stats jurisdiksjonsområde medfører brudd på denne statens lovgivning, eller 3) reiser prinsipielle eller politiske problemstillinger. Typisk vil dette kunne gjelde grunnleggende eller annen etterretningsanalyse som ikke forutsetter inngrep i noens rettigheter, eller etterretningsinnsamling i/fra internasjonalt farvann/luftrom rettet mot fremmede objekter. Den alminnelige handlefrihet er meget begrenset for myndighetsutøvelse av etterretningsinnhenting. Ved at sjefen for Etterretningstjenesten samtykker til virksomheten sikrer man legalitetskontroll, enhetlig etterretningsmessig ledelse og produksjonsstyring, kontroll med bruk av etterretningsressurssene i Forsvaret og kontroll med Forsvarets samhandling med tredjeparter på etterretningsområdet. All informasjon og analyseprodukter fremkommet gjennom etterretningsvirksomhet etter dette alternativet (for)blir Etterretningstjenestens eiendom, og kan ikke distribueres internt i Forsvaret eller deles med tredjeparter uten etter samtykke fra Etterretningstjenesten. Sjefen for Etterretningstjenesten kan gi stående samtykke/oppdrag til bestemte enheter blant annet gjennom årlige samvirkeplaner med forsvarsgrensjefene, f.eks. stående rapporteringsoppdrag til Garnisonen i Sør-Varanger eller fartøyer i Sjøforsvaret. For øvrig skal sjefen for Etterretningstjenesten etter gjeldende regler godkjenne alt samarbeid og kontakt som Forsvaret har innen etterretning med politiet og eventuelt andre offentlige eller private virksomheter.

c. *I internasjonale operasjoner innenfor rammen av operasjonens mandat og engasjementsregler*. Dette alternativet forutsetter at etterretningsvirksomheten skjer med hjemmel i særskilt folkerettslig mandat, altså at det foreligger rettslig grunnlag for utøvelsen av statlig selvforsvar eller at virksomheten er hjemlet i en sikkerhetsrådsresolusjon eller i samtykke fra vertsstaten. Dessuten må etterretningsvirksomheten utøves av norske styrker som er kommandooverført til annen stat eller internasjonal organisasjon. Etterretningsvirksomhet i operasjonsområdet skal ligge innenfor operasjonens mandat og engasjementsregler, og vil prinsipielt skje på vegne av operasjonen (den stat eller internasjonale organisasjon som leder operasjonen). All nasjonal bruk av etterretninger innhentet i operasjonsområdet etter dette alternativet skal godkjennes av Etterretningstjenesten. For øvrig gjelder internt regelverk i Forsvaret blant annet for å sikre ivaretakelse av Etterretningstjenestens ansvar for etterretningsstyrkestruktur/-arkitektur, samvirke og kontroll. Lovens anvendelse i internasjonale militære operasjoner er drøftet i pkt. 5.2.4.4 nedenfor.

d. *I nasjonale beredskapssituasjoner og væpnet konflikt som berører norsk territorium*. Ansvar og hjemler i fred endres ikke i krisesituasjoner, med mindre annet bestemmes i medhold av beredskapslovgivningen eller ny krisetilpasset lovgivning. Dette gjelder også for utenlandsetterretning. Krisesituasjoner som krever inngripende tiltak med et innenlandsetterretningsfokus og/eller mot personer i Norge som ikke opptrer på vegne av fremmed makt, kan verken

Etterretningstjenesten eller øvrige avdelinger i Forsvaret gjennomføre med mindre ny krisetilpasset lovgivning vedtas eller vilkårene for nødrett foreligger. Øvrige deler av Forsvaret kan likevel, uten kommandooverføring til sjefen for Etterretningstjenesten, gjennomføre etterretningsvirksomhet rettet mot en motstander i en væpnet konflikt som Norge er part i, begrenset til etterretningsvirksomhet som er nødvendig for å støtte planlagte eller pågående militære operasjoner og som ligger innenfor handlingsrommet etter krigens folkerett og politiske og militærstrategiske vedtak knyttet til operasjonen (operasjonsplan, engasjementsregler osv.). Rettslig grunnlag for etterretningsvirksomheten utledes her av folkeretten, på lik linje med andre faktiske handlinger som Forsvaret utøver i slike situasjoner rettet mot en potensiell motstander eller etablert fiende. Inngripende tiltak overfor fremmede aktører som truer med eller gjennomfører væpnet angrep mot Norge, eller som krenker norsk suverenitet eller norske suverene rettigheter, gjennomføres med hjemmel i folkeretten. Dette gjelder i prinsippet også for Etterretningstjenesten, selv om Etterretningstjenesten også har hjemmel i nasjonal lovgivning til å gjennomføre inngripende tiltak. Etterretningsstøtte til Forsvaret i nasjonale beredskapssituasjoner og væpnet konflikt som berører norsk territorium skal for øvrig gjennomføres innenfor rammen av gjeldende nasjonalt planverk og direktiver fra strategisk nivå. Sjefen for Etterretningstjenesten har et overordnet ansvar for, koordinert med sjefen for Forsvarets operative hovedkvarter, å planlegge og lede etterretningsstøtte til Forsvarets operasjoner. I og med at etterretningsinnhenting i væpnet konflikt fra andre deler av Forsvaret gjennomføres uten behov for særskilt hjemmel i norsk lov, men selvfølgelig innenfor rammen av krigens folkerett, vurderer departementet at det ikke er grunn til å regulere dette i lovforslaget.

5.2.4.3 Bistand fra andre enn forsvarspersonell

I enkelte situasjoner kan det tenkes at andre norske myndighetspersoner vil avgis midlertidig til Etterretningstjenesten, uten å ta midlertidig ansettelse i tjenesten. Disse vil utføre oppdrag for tjenesten innenfor rammen av lov om Etterretningstjenesten. Dette kan for eksempel gjelde enkeltstående tjenestepersoner i Nasjonal sikkerhetsmyndighet eller Politiets sikkerhetstjeneste med spisskompetanse som avgis til Etterretningstjenesten for å bistå i løsningen av spesielle oppgaver eller gjennomføring av spesielle operasjoner. I avgivelsesperioden vil personene være underlagt tjenestens instruksjonsmyndighet, tilsvarende som for personer i Forsvaret som midlertidig kommandooverføres til tjenesten. I og med at det ikke er vanlig å bruke kommandobegrepet utenfor Forsvaret, mener departementet at det i lovforslaget bør reflekteres at loven gjelder for personer som på denne måten underlegges Etterretningstjenestens instruksjonsmyndighet. Dette fremgår av utkast til § 1-2 andre ledd.

5.2.4.4 Særlig om etterretningsvirksomhet i internasjonale operasjoner

Departementet mener at etterretningsvirksomhet i internasjonale operasjoner med folkerettslig mandat ikke bør omfattes av lovforslaget. Forutsetningen er at informasjonsinnhentingen og -behandlingen skjer for operasjonens formål. Motsetningsvis, der informasjonen beholdes for nasjonal bruk, for eksempel for etterretningsproduksjon til bruk for norske myndigheter, bør loven derimot komme til anvendelse. Departementet begrunner denne sondringen med at etterretningsvirksomhet innenfor rammene av en

internasjonal operasjon utøves direkte med hjemmel i det internasjonale mandatet for operasjonen. Dette stiller seg annerledes dersom opplysningene behandles for nasjonale formål.

Tilsvarende sondring kan utledes av Forsvarsdepartementets instruks om sikkerhetstjeneste i Forsvaret § 18 annet ledd.[127] Her følger det at personopplysningsloven ikke kommer til anvendelse hvis opplysningene hentes inn på utenlandsk territorium i en internasjonal militær operasjon, og «dersom innhentingen skjer på vegne av annen stat eller internasjonal organisasjon og opplysningene ikke beholdes av Forsvaret.» De samme hensyn som denne regelen hviler på, nemlig at innhenting og behandling av slike opplysninger skjer med et internasjonalt mandat og med et internasjonalt avgrenset formål, tilsier at samme prinsipper vil gjelde etterretningsvirksomhet i slike operasjoner.

5.2.5 Virkeområde i tid (*ratione temporis*)

Om gjeldende lovs virkeområde i tid er følgende uttalt i forarbeidene:[128]

> «Generelt bemerkes at lovforslagets bestemmelser primært er utformet med henblikk på anvendelse under normale fredsforhold. Dersom krig truer eller rikets selvstendighet eller sikkerhet er i fare, kan eventuelle tilpasninger om nødvendig fremmes for Stortinget eller skje med hjemmel i beredskapslovgivningens fullmakter. Departementet anser det ikke nødvendig eller hensiktsmessig å regulere Etterretningstjenestens oppgaver eller beføyelser under krise og krig i det foreliggende lovforslag.»

Det er et alminnelig prinsipp i norsk rett at fredstidslovgivningen fortsetter å gjelde i en krisesituasjon, inntil noe annet eventuelt bestemmes i medhold av beredskapslovgivningen eller ny krisetilpasset lovgivning. I beredskapsloven § 3 er Kongen i statsråd gitt en hastefullmakt til å gi bestemmelser av lovgivningsmessig innhold blant annet «*for å trygge rikets sikkerhet*».[129] Om nødvendig kan det i bestemmelsene gjøres avvik fra gjeldende lov. Bestemmelser gitt i medhold av beredskapsloven § 3 skal snarest mulig meddeles Stortinget. Såfremt bestemmelsene ikke er opphevet 30 dager etter at de er meddelt Stortinget, skal de snarest mulig legges frem som lovforslag.

Departementet foreslår en videreføring av gjeldende rett i lovforslaget her, likevel slik at man for å unngå tolkningstvil foreslår å lovfeste at loven gjelder i hele krisespennet (i fred, krise og væpnet konflikt). Det anses rettsteknisk uheldig i bestemmelsen å henvise til beredskapsloven § 3 eller andre deler av beredskapslovgivningen. Departementet vurderer at det er tilstrekkelig at det følger av alminnelige rettskildeprinsipper og forarbeidene her at andre særlige fullmakter i medhold av beredskapslovgivningen kan komme til anvendelse.

5.2.6 Forslag til regulering

Departementet foreslår etter følgende angivelse av lovens virkeområde i lovutkastet § 1-2:

§ 1-2 *Virkeområde*

---

[127] Instruks av 29. april 2010 nr. 695 om sikkerhetstjeneste i Forsvaret. Instruksen er i dag opphevet. Det er ikke tvilsomt at prinsippet i den tidligere instruksen § 18 annet ledd fortsatt vurderes som gyldig for utøvelse av sikkerhetstjeneste i internasjonale operasjoner.

[128] Ot. prp. nr. 50 (1996-97) s. 14

[129] Lov av 15. desember 1950 nr. 7 om særlige rådgjerder under krig, krigsfare og liknende forhold

Loven gjelder for Etterretningstjenesten.

Loven gjelder også for andre personer og enheter for det tidsrom de er under kommando eller instruksjonsmyndighet av sjef Etterretningstjenesten.

Loven gjelder ikke etterretningsvirksomhet som gjennomføres av Etterretningstjenesten som ledd i en internasjonal operasjon med folkerettslig mandat, dersom etterretningsvirksomheten skjer for operasjonens formål og innhentet informasjon kun behandles av Etterretningstjenesten for formål som kan henføres til den internasjonale operasjonen.

Loven gjelder i fred, krise og væpnet konflikt.

6 Organisering, styring og kontroll

6.1 Innledning

Det ligger i utgangspunktet til regjeringen å bestemme organiseringen av statsforvaltningen. Departementets styring og kontroll med underlagte etater, herunder Etterretningstjenesten som en avdeling i Forsvaret, kan dermed reguleres gjennom den alminnelige instruksjonsmyndighet og eventuelt ved behov fastsettes i forskrift. I forbindelse med utformingen av nytt lovforslag kan rammene for styring og kontroll også beskrives i høringsnotatet, men uten at en nærmere regulering inntas i loven.

Departementet har allikevel etter en nærmere vurdering kommet frem til at de særlige forhold som gjør seg gjeldende for Etterretningstjenesten tilsier at de overordnede rammene knyttet til organisering, styring og kontroll bør nedfelles i loven. Flere forhold gjør en slik lovforankring hensiktsmessig. For det første er organiseringen av Etterretningstjenesten allerede i dag delvis fastlagt i lov, jf. gjeldende etterretningstjenestelov § 2. Videre er økonomi- og virksomhetsstyringen av Etterretningstjenesten gjennom K-utvalget[130] forankret i Stortinget. For det andre er Etterretningstjenestens virksomhet og samfunnsoppdrag av en slik karakter at det er behov for særskilt tilpasset styring og kontroll. Forankring i lovs form bidrar til å sikre åpenhet og allmennhetens tillit til at tjenestens virksomhet er underlagt en helhetlig overordnet styring og kontroll. For det tredje taler hensynet til sammenhengen i regelverket for en lovregulering.

Departementet vurderer at de bestemmelser som er foreslått i lovutkastet kapittel 2 ivaretar balansen mellom nødvendig regulering av viktige prinsipper og styrings- og kontrollmekanismer, og tilstrekkelig fleksibilitet i utøvelsen av forvaltningsansvaret. En hensikt bak lovforslaget er å skape åpenhet og tillit til at Etterretningstjenestens virksomhet er underlagt klare og avgrensede rettslige rammer for inngripen i individuelle rettigheter, i tillegg til å forankre og tydeliggjøre den overordnede styring og kontroll av tjenesten. Det vil redegjøres for departementets forslag i det følgende.

6.2 Organisering og ansvar

6.2.1 En nasjonal sivil og militær utenlandsetterretningstjeneste

Etterretningstjenesten er Norges eneste utenlandsetterretningstjeneste og er gitt i oppgave å bistå både sivile og militære myndigheter. Tjenestens sektoroverskridende

[130] K-utvalget er en forkortelse for «Koordineringsutvalget for Etterretningstjenesten», se mer om dette under høringsnotatet punkt 6.3.2.

samfunnsoppdrag er reflektert i dagens lovbestemmelser, og videreføres i forslag til ny lov. Organisatorisk er Etterretningstjenesten en del av etaten Forsvaret og kommandomessig underlagt forsvarssjefen.

Den militære kommandomyndighet over «forsvarsmakten» tilligger Kongen (regjeringen) etter Grunnlovens § 25. I tråd med konstitusjonell praksis er det forsvarsministeren som på vegne av regjeringen utøver kontroll over Forsvarets organisasjon og nasjonens militære styrker. Stortingets eksklusive bevilgningsmyndighet utgjør begrensinger for hva regjeringen kan beslutte uten Stortingets samtykke, og etter Grunnlovens § 25 kreves Stortingets samtykke også for enkelte disposisjoner knyttet til ressursbruk og organisering. I forbindelse med den årlige budsjettbehandlingen beslutter Stortinget de større organisatoriske endringene og oppgavene for forsvarssektoren.[131]

Etterretningstjenestens oppgaver er nærmere beskrevet i høringsnotatet kapittel 7. Det at Etterretningstjenesten er en del av Forsvaret innebærer at tjenesten også har andre oppgaver enn ren informasjonsinnhenting, -analyse og -behandling, både i fred, krise og krig.[132] De rettslige og politiske rammene for bruk av Etterretningstjenesten i utførelsen av Forsvarets hovedoppgaver utenfor tjenestens tradisjonelle etterretningsvirksomhet gjelder tilsvarende som for bruken av Forsvaret for øvrig.

Det er hverken hensiktsmessig, mulig eller i tråd med konstitusjonell praksis at Forsvarets oppgaver detaljreguleres i lov. Reguleringen av statlig maktbruk følger av folkeretten. Det anses derfor ikke hensiktsmessig å regulere denne delen av Etterretningstjenestens oppgaver, all den tid vi ikke har tilsvarende lovregulering av statlig maktbruk for øvrig.

Departementet foreslår følgende bestemmelse i lovutkastet § 2-1:

§ 2-1 *Nasjonal tjeneste*

Etterretningstjenesten er Norges nasjonale utenlandsetterretningstjeneste, og har et sektoroverskridende samfunnsoppdrag.

Rammene for EOS-utvalgets kontrollmyndighet begrenses eller utvides ikke av rekkevidden av forslag til ny lov, men det foreslås enkelte justeringer i EOS-kontrolloven, se kapittel 16.1.4. Det foreslås også at kontrollen med tilrettelagt innhenting styrkes, se nærmere om dette i kapittel 11.12. Det er klart at EOS-utvalget vil kunne kontrollere alle deler av Etterretningstjenestens virksomhet som faller inn under kontrollområdet.

6.2.2 Etterretningstjenesten integrert i Forsvaret

I Norge er Etterretningstjenesten en integrert del av Forsvarets organisasjon. Sjefen for Etterretningstjenesten har militær kommando over tjenesten, og er underlagt forsvarssjefens alminnelige kommandomyndighet. Dette innebærer blant annet at forsvarssjefens instrukser og bestemmelser som prinsipp gjelder for Etterretningstjenesten som for Forsvaret for øvrig. Som en følge av tjenestens særlige oppgave som nasjonal utenlandsetterretningstjeneste har imidlertid Forsvarsdepartementet et særlig styringsansvar. Forsvarssjefen utøver sitt kommando- og etatssjefsansvar over Etterretningstjenesten som del av Forsvaret blant annet gjennom sin rolle i styringsfora og i fastsettelsen av overordnede styringsdokumenter.

[131] Se Johs. Andenæs og Arne Fliflet, *Statsforfatningen i Norge*, 11. utgave (2017), kapittel 41 side 393

[132] Se nærmere om dette i punkt 5.2.4.

Organiseringen av Etterretningstjenesten fremgår i dag av etterretningstjenesteloven § 2 første og andre ledd. Departementet foreslår at dette videreføres, men i en noe annen språkdrakt, i utkast til § 2-2:

§ 2-2 *Organisasjon*

Etterretningstjenesten er organisatorisk en del av Forsvaret og kommandomessig underlagt forsvarssjefen.

Det er et grunnleggende prinsipp at Etterretningstjenesten skal være under norsk kontroll. Det skal således sikres norsk kontroll med hvilken informasjon som gjøres kjent for utenlandske samarbeidspartnere. Departementet mener dette viktige prinsippet bør fremgå av loven og foreslår følgende bestemmelse i utkast til § 2-3:

§ 2-3 *Nasjonal kontroll*

Etterretningstjenesten skal være under norsk kontroll. Det skal sikres norsk kontroll med hvilken informasjon som gjøres kjent for utenlandske samarbeidspartnere.

6.2.3 Forsvarsdepartementets særlige rolle ovenfor Etterretningstjenesten

Forsvarsministeren har det parlamentariske og konstitusjonelle ansvaret for hele forsvarssektoren, herunder Etterretningstjenesten som del av Forsvaret. Forsvarsdepartementet ivaretar som departementskontor ansvaret på vegne av forsvarsministeren. Etterretningstjenestens sektoroverskridende samfunnsoppdrag tilsier at Forsvarsdepartementet må ha en direkte rolle i styring og kontroll av tjenesten. Departementet vil i større utstrekning enn for annen virksomhet i Forsvaret ha en direkte styringsrolle. Dette ivaretas gjennom det særskilt etablerte styringsforumet Koordineringsutvalget for Etterretningstjenesten (forkortet K-utvalget) som ledes av departementet, i den særskilte foreleggelsesplikten tjenesten har for departementet i enkelte kategorier av saker, samt gjennom fastsettelse av overordnede styringsdokumenter. I forslaget til ny lov foreslås departementets rolle tydeliggjort i større grad enn i gjeldende lov. Departementet foreslår følgende bestemmelse om departementets styring og kontroll i utkast til § 2-5 første ledd:

§ 2-5 *Departementets styring og kontroll*

Departementet ivaretar politisk styring og kontroll med Etterretningstjenesten gjennom forsvarssjefen dersom annet ikke er fastsatt i loven her.

6.3 Nærmere om Forsvarsdepartementets overordnede ansvar for styring og kontroll

6.3.1 Generelt

Offentlighet og åpenhet er viktige elementer i tillitsforholdet mellom borgere og statsforvaltningen, og det offentliges plikt til å tilrettelegge for åpenhet følger også direkte av Grunnloven.[133] Retten til innsyn i det offentliges virksomhet er imidlertid ikke absolutt, og den

[133] Grunnloven § 100, femte ledd: «Enhver har rett til innsyn i statens og kommunenes dokumenter og til å følge forhandlingene i rettsmøter og folkevalgte organer. Det kan i lov fastsettes begrensinger i denne rett ut fra hensynet til personvern og andre tungtveiende grunner.»

både må og kan begrenses der dette er nødvendig. For Etterretningstjenestens del medfører virksomhetens karakter at majoriteten av dokumenter og prosesser har et absolutt skjermingsbehov og må være unntatt innsyn. Kompromittering av blant annet tjenestens metoder, kapasiteter og personell har et stort skadepotensiale for rikets og personellets sikkerhet, og full åpenhet er ikke mulig å praktisere. Det er derfor ekstra viktig at det er fastsatt klare, tillitsvekkende og dokumenterbare styrings- og kontrollordninger og rutiner som tilfredsstiller krav til arkivering og notoritet. Den uavhengige parlamentariske kontrollen som gjennomføres av EOS-utvalget reguleres i egen lov[134] og står her i en særstilling. I forslag til ny etterretningstjenestelov foreslår departementet at dagens formaliserte ordninger lovforankres for å ivareta åpenhet og skape tillit til rammene for styringen av Etterretningstjenesten.

6.3.2 Koordineringsutvalget for Etterretningstjenesten

Helt siden oppstarten har det vært behov for å skjerme Etterretningstjenestens budsjett og økonomiske disposisjoner. Behovet for skjerming utfordrer det parlamentariske prinsippet om at det er Stortinget som fører kontroll med bruken av de bevilgede statsmidler. For å sikre en tilpasset kontroll ble det tidlig etablert et særlig utvalg, forløperen til dagens K-utvalg, for ivaretakelse av revisjon og regnskap for Etterretningstjenestens virksomhet. Riksrevisjonen, som ivaretar revisjonen av statens regnskap på Stortingets vegne, har hatt en særskilt utpekt ekspedisjonssjef med fast representasjon i utvalget. Den utpekte ekspedisjonssjefen har gjennomført revisjonen og har hatt innsyn i alle deler av tjenestens økonomiske virksomhet. Sammensetningen av utvalget og det nærmere innholdet i dets oppgaver har tilpasset seg utviklingen i tjenestens oppgaver og Forsvarsdepartementets organisering. I 1993 formaliserte Stortinget K-utvalget i en sikkerhetsgradert stortingsproposisjon.[135] Stortingsbeslutningen er det formelle grunnlaget for dagens ordning. Utvalget ble fra 1993 benevnt Koordineringsutvalget for Etterretningstjenesten (K-utvalget). Forsvarsdepartementet implementerte Stortingets vedtak, og fastsatte en utfyllende sikkerhetsgradert instruks i 1997.

De siste årene har kravene til Etterretningstjenesten økt i takt med et tilspisset sikkerhetspolitisk bilde, en stadig akselererende teknologisk utvikling og et mer komplekst trusselbilde. Dette har blant annet medført at det er besluttet en betydelig økonomisk styrking av tjenesten for å sikre at den har de nødvendige kapasiteter og ressurser for å være i stand til å utføre sin oppgave. En styrking av tjenesten og dennes kapasiteter tilsier at styring og kontroll må være tilsvarende tilpasset.

Økonomi- og virksomhetsstyringen i staten er underlagt enhetlige prosesser gjennom blant annet reglement og bestemmelser for økonomistyring i staten[136]. For Forsvarsdepartementets underlagte virksomheter er det fastsatt utfyllende instruks for økonomi- og virksomhetsstyring basert på overordnet regelverk og Statens bevilgningsreglement. Etterretningstjenesten omfattes ikke av denne instruksen, men er

[134] Lov om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-kontrolloven) av 3. februar 1995 nr. 7

[135] For det formål å ivareta at tjenestens budsjett og regnskap behandles, kontrollers og revideres i samsvar med den praksis som er innarbeidet og beskrevet i proposisjonen.

[136] Reglement for økonomistyring i staten (RØS), fastsatt i kronprinsregentens resolusjon 12. desember 2003 og Bestemmelser for økonomistyring i staten (BØS), fastsatt av Finansdepartementet samme dag

underlagt K-utvalgets særskilt tilpassede prosesser etter stortingsbeslutningen av 1993 og tilhørende instruks for K-utvalget.

Forsvarsdepartementet har nylig oppdatert og strukturert K-utvalget som det overordnede forum for økonomi- og virksomhetsstyring av Etterretningstjenesten. Det er i 2017 fastsatt ny ugradert instruks som klargjør og formaliserer K-utvalgets funksjon og prosessuelle rammer i tråd med prinsippene som gjelder økonomi- og virksomhetsstyring i staten for øvrig.[137]

Departementet mener at økonomi- og virksomhetsstyringen gjennom K-utvalget bør fremgå av loven og foreslår følgende regulering i utkast til § 2-5 annet ledd om departementets forvaltningsstyring og kontroll:

> Departementets økonomi- og virksomhetsstyring ivaretas gjennom Koordineringsutvalget for Etterretningstjenesten (K-utvalget). Departementet kan opprette andre særlige fora og ordninger som sikrer nødvendig styring og kontroll.

6.3.3 Oppdragsstyring og styringsdokumenter

Etterretningstjenestens sivil-militære samfunnsoppdrag og det omfattende behov for unntak fra offentlig innsyn stiller særlige krav til overordnet styring og kontroll, beslutningsnotoritet og dokumenterbare prosesser. Som landets nasjonale utenlandsetterretningstjeneste skal tjenesten bistå også andre myndigheter enn Forsvarsdepartementet og Forsvaret. Det er Forsvarsdepartementet som foretar koordineringen av etterretningsbehov, og som vurderer og prioriterer disse innenfor rammen av Etterretningstjenestens samlede ressurser. Forsvarsdepartementet fastsetter årlige oppdrag til tjenesten gjennom et gradert prioriteringsdokument for nasjonale etterretningsbehov (dokumentet omtales ofte med forkortelsen PNEB). Prioriteringsdokumentet beskriver på et overordnet nivå hvilke land, regioner og temaer som Etterretningstjenesten skal prioritere i sitt arbeid. Oppdukkende informasjonsbehov dekkes gjennom såkalte «Requests for information» (RFI). Slike RFI kan blant annet omfatte behov for særlige vurderinger og orienteringer knyttet til oppdukkende særlige situasjoner, bakgrunn til politisk behandling mm. RFI formidles i all hovedsak fra Forsvarsdepartementet til Etterretningstjenesten eller etter Forsvarsdepartementets anvisning. Etterretningstjenestens innhenting og behandling av informasjon skal kunne knyttes direkte til oppgavene som er fastsatt i lov, og skal fremgå av prioriteringsdokumentet og/eller RFI. Lovforslagets kapittel 2 viderefører at det er departementet som fastsetter årlig oppdragsprioritering, og det tas sikte på å tydeliggjøre at det gjøres en helhetlig prioritering av sivile og militære etterretningsbehov.

I forbindelse med at Stortinget vedtar langtidsplanen for forsvarssektoren[138] fastsetter Forsvarsdepartementet Iverksettingsbrev for forsvarssektoren (IVB LTP). Iverksettingsbrevet er departementets overordnede styringsdokument for forsvarssektoren for den gjeldende langtidsperioden, og formaliserer langtidsplanen i et helhetlig implementeringsoppdrag til etatene i forsvarssektoren. Dokumentet konkretiserer ansvar, målsettinger, økonomiske rammer og rapporteringsplikt, og gir grunnlag for årlig styring og resultatmåling. Det utarbeides et særskilt sikkerhetsgradert vedlegg for Etterretningstjenesten med rammer for styring, resultatmåling og rapportering, tilpasset de særlige prosesser som gjelder for

[137] Instruks for Koordineringsutvalget for Etterretningstjenesten, fastsatt av Forsvarsdepartementet 29. mars 2017

[138] Gjeldende langtidsplan er langtidsplanen for 2017–2020 basert på Stortingets behandling av Innst. 62 S (2016–2017), jfr Prop. 151 S (2015–2016) Kampkraft og bærekraft

tjenesten. Dette vedlegget danner hovedgrunnlaget for den styring og kontroll som departementet og forsvarssjefen utøver gjennom K-utvalget.

Departementet foreslår at de overordnede prinsipper knyttet til oppdragsstyringen fremgår av loven i utkast til § 2-4. Forslaget lyder:

§ 2-4 *Oppdragsstyring*

Departementet formulerer oppdrag, prioriterer sivile og militære etterretningsbehov og koordinerer etterretningsbehov fra berørte departementer. Den overordnede prioriteringen av oppdragene til Etterretningstjenesten fastsettes av departementet årlig i et prioriteringsdokument for nasjonale etterretningsbehov.

Departementet bestemmer prosedyrer for etterretningsbehov som ikke dekkes i prioriteringsdokumentet. Forsvarssjefen bestemmer prosedyrer for etterretningsbehov i Forsvaret som ikke dekkes i prioriteringsdokumentet.

6.3.4 Saker som krever særskilt vurdering og beslutning av departementet

Deler av Etterretningstjenestens virksomhet er av slik art at departementet bør ha en særlig direkte rolle i den operative styringen og få saken forelagt for vurdering og beslutning i ethvert tilfelle. Etter dagens lov og instruks[139] omfatter foreleggelsesplikten fire kategorier saker: etablering av nye samarbeid med utenlandske tjenester eller organisasjoner, organisering og status på okkupasjonsberedskapen, iverksettelse av etterretningsoperasjoner eller støtte som kan reise politiske problemstillinger og andre saker av særlig viktighet eller prinsipiell karakter.

Departementet vurderer at foreleggelsesplikten bør videreføres. Det følger av lovforslaget § 2-7 at etablering av samarbeid og avtaler med utenlandske tjenester eller internasjonale organisasjoner, særskilte etterretningsoperasjoner som kan reise politiske problemstillinger og andre saker av særlig viktighet eller prinsipiell karakter, fortsatt bør forelegges departementet for beslutning. I saker som omfattes av forslaget til § 2-7 vil departementet i tillegg kunne pålegge Etterretningstjenesten en særlig rapporteringsplikt og statusrapportering.

Departementet vurderer at plikten til å holde departementet orientert om okkupasjonsberedskapen innholdsmessig hører hjemme i bestemmelsen om okkupasjonsberedskap i lovforslaget § 3-3. Regulering av foreleggelsesplikten reflekterer gjeldende praksis og er ikke ment å utgjøre en realitetsendring i forhold til dagens situasjon. I enkelte tilfeller, slik som der en sak inngår i et større sakskompleks, herunder saker som har budsjettmessige konsekvenser, vil sakene som etter dagens regelverk er inntatt i bestemmelsen om særskilt foreleggelse, i praksis besluttes av departementet i K-utvalget. Dette ivaretar den overordnede politiske beslutningen som foreleggelsesplikten er ment å ivareta.

Departementet foreslår følgende regulering av foreleggelsesplikten i utkast til § 2-7:

§ 2-7 *Saker som skal forelegges for departementets beslutning*

Etterretningstjenesten skal forelegge for departementets beslutning

a. Etablering av samarbeid og avtaler med utenlandske tjenester eller internasjonale organisasjoner.
b. Iverksettelse av særskilte etterretningsoperasjoner som kan reise politiske problemstillinger.
c. Andre saker av særlig viktighet eller prinsipiell karakter.

[139] Instruks om Etterretningstjenesten av 31. august 2001 nr.1012 § 13

6.3.5 Løpende oppdragsstyring og kontroll

De formaliserte og overordnede særlige styringsfora, styringsdokumenter og særlige foreleggelsessakene som beskrevet over reflekterer de tilpassede styringsprosesser for Etterretningstjenesten. I tillegg er tjenesten gjenstand for kontinuerlig og løpende oppdragsstyring og kontroll på lik linje med Forsvaret og departementets øvrige underlagte virksomheter. Slike saker knyttet til den løpende og operative virksomheten vurderes og behandles i departementet på ordinær måte, tilpasset de særlige krav til skjerming. I departementets organisasjon vil det til enhver tid være dedikert saksbehandlerkompetanse for etterretningssaker med de nødvendige klareringer og autorisasjoner. De særskilte saksbehandlere vil blant annet ha ansvar for forberedelse og tilrettelegging av styringsfora som K-utvalget og utarbeidelsen av de overordnede styringsdokumenter.

6.4 Forsvarssjefens rolle

Forsvarssjefen er øverste militære foresatte for Etterretningstjenesten, og har både kommandomyndighet og instruksjonsmyndighet over tjenesten på lik linje med Forsvaret forøvrig. Forsvarssjefens ansvar må imidlertid forstås i sammenheng med Etterretningstjenestens helhetlige samfunnsoppdrag og den særlige styringsrollen som tillegges departementet. Der departementet er tiltenkt å utøve direkte styring ovenfor Etterretningstjenesten er dette i lovforslaget reflektert og tydeliggjort, se særlig §§ 2-4 om oppdragsstyring og 2-7 om saker som skal forelegges departementets beslutning. Et eksempel på hvordan forsvarssjefens ansvar som etatssjef og den særlige rollen til departementet gjennomføres i praksis, er K-utvalget som styringsfora, hvor forsvarssjefen er medlem og hvor det blant annet rapporteres på fastsatte mål og resultatkrav. Så langt dette lar seg gjøre, er prosessen tilpasset tilsvarende prosesser for Forsvaret forøvrig, slik at forsvarssjefen kan utøve sitt etatssjefsansvar på en koordinert og hensiktsmessig måte.

6.5 Varsling og rapportering

En av Etterretningstjenestens hovedoppgaver er å varsle og å rapportere tilbake til sivile og militære brukere om forhold som ligger under tjenestens oppdrag. Innhenting og bearbeiding av informasjon kan i den forbindelse ses på som det nødvendige middelet for å kunne utføre de lovpålagte oppgavene. I forslag til ny lov tydeliggjøres Etterretningstjenestens primærfunksjon ved at varslingsoppgaven foreslås lovfestet særskilt i utkast til § 2-6 første og annet ledd. I tillegg til plikten til å varsle om trusler, skal tjenesten også rapportere selvstendig om ethvert forhold av betydning for Norge og norske interesser som faller inn under tjenestens oppdrag. Dette må også ses i sammenheng med den oppgaven tjenesten er gitt i å bistå til å motvirke trusler. Det er viktig for norske myndigheter å ha en korrekt og oppdatert forståelse av den sikkerhetspolitiske situasjonen både nasjonalt og i sine internasjonale relasjoner.

En del av rapporteringen og varslingen følger i dag formaliserte prosedyrer og rutiner. Et eksempel på dette er rapportering av styringsmessige og økonomiske forhold til K-utvalget og daglige rapporteringer til forsvarsminister og forsvarsledelse. Etterretningstjenesten rapporterer videre til både sivile og militære myndigheter om konkrete og avgrensede forhold, blant annet som følge av oppdragsstyring på oppdukkende etterretningsmål som normalt følger de formaliserte prosedyrer for RFI. I enkelte saker vil Etterretningstjenesten også kunne bli pålagt en særskilt rapporteringsplikt etter departementets anvisninger.

Departementet vurderer at det i visse særlige kritiske situasjoner vil være nødvendig at Etterretningstjenesten kan varsle norske subjekter om en trussel direkte. Det typiske her vil være en nærstående trussel mot en norsk virksomhet, som krever umiddelbare tiltak. En slik adgang til direkte varsling foreligger også i dag under gjeldende instruks § 11, og departementet har fastsatt bestemmelser som angir nærmere rammer for varslingsadgangen. I forslag til lov videreføres bestemmelsen i noe endret ordlyd i utkast til § 2-6 tredje ledd. Varslingsadgangen er ikke tenkt utvidet med ny ordlyd, men det er ønskelig å klargjøre at det ved en varslingssituasjon vil kunne være nødvendig at det utgis gradert informasjon som det ikke er anledning til å utlevere i normalsituasjoner. Bestemmelsen forutsetter at departementet fastsetter det nærmere innholdet i utfyllende bestemmelser eller instruks.

Departementet foreslår følgende bestemmelse om varsling og rapportering i utkast til § 2-6:

§ 2-6 *Varsling og rapportering*

Innenfor rammen av oppgavene etter kapittel 3 skal Etterretningstjenesten:

1. Varsle norske myndigheter om trusler og andre forhold som Etterretningstjenesten blir kjent med og som krever umiddelbar handling eller av andre årsaker er av tidskritisk natur.
2. Rapportere til norske myndigheter om utenlandske forhold av betydning for Norge og norske interesser.

Etterretningstjenesten skal varsle og rapportere til militære myndigheter i samsvar med forsvarssjefens bestemmelser, og til sivile myndigheter i samsvar med departementets bestemmelser.

Etter departementets nærmere bestemmelser kan Etterretningstjenesten varsle og rådgi norske og utenlandske juridiske og fysiske personer om trusler som faller inn under Etterretningstjenestens oppgaver etter kapittel 3. Utlevering av sikkerhetsgradert informasjon kan bare skje i den grad dette er strengt nødvendig og anses sikkerhetsmessig forsvarlig.

6.6 Behovet for rettsregler som legger til rette for effektiv kontroll

Effektive kontrollsystemer er en sentral rettssikkerhetsgaranti.[140] Kontroll er et viktig premiss for å skape og opprettholde legitimitet for virksomheten, både for den ansvarlige kontrollerende myndighet, for samfunnet og for Etterretningstjenesten selv. Effektiv kontroll er ikke ensbetydende med at alle detaljer ved gjennomføringen av kontrollen er fastsatt i overordnede rettsregler. Men tatt i betraktning at det er begrenset mulighet til åpenhet og offentlig tilgang til alle deler av Etterretningstjenestens konkrete virksomhet, er det her særlig viktig at kontrollens rammer er klare. Med andre ord er det åpenheten og legitimiteten til kontrollvirksomheten som i stor grad vil bli identifisert med tillit til selve virksomheten. Det er viktig å klargjøre at dette ikke medfører at kontrollinstansen kan eller skal holdes ansvarlig for at virksomheten gjennomføres innenfor de lovgitte rammer. Uavhengig av kontrollen er det utelukkende forsvarsministeren som konstitusjonelt og parlamentarisk ansvarlig og Etterretningstjenesten som innehar dette ansvaret.

Tydelige rettslige rammer gjør kontrollen mer effektiv for alle parter. Gjennom EOS-utvalgets kontroll kan Stortinget ved den årlige behandlingen av utvalgets meldinger til Stortinget ivareta den nødvendige parlamentariske legalitetskontroll. Riksrevisjonen ivaretar sin revisjons- og kontrolloppgave for Stortinget blant annet gjennom sin representasjon i koordineringsutvalget for Etterretningstjenesten. Klare rammer bidrar til å minimere

[140] Se for eksempel NOU 2009:15 Skjult informasjon – åpen kontroll s. 130

potensiell uenighet og konflikt mellom den kontrollerende og kontrollerte virksomhet, og det sikrer en hensiktsmessig og praktisk tilrettelegging av kontrollen.

Etterretningstjenestens virksomhet kontrolleres av flere instanser. Disse ivaretar kontrollfunksjonen for ulike sider av virksomheten, og har separate kontrollmandater. Det er helheten i de ulike kontrollelementene som tilsammen sørger for at det sikres kontroll med at tjenesten holder seg innenfor sine fastsatte rammer. Departementet understreker derfor viktigheten av å se på de samlede kontrollmekanismene under ett når man skal vurdere hvorvidt Etterretningstjenesten er underlagt tilstrekkelig oversyn og kontroll. Flere internasjonale forum har i sine rapporter, resolusjoner og anbefalinger fremhevet betydningen av ulike kontrollmekanismer og deres bidrag til en tilfredsstillende kontroll sett under ett.[141]

Den forvaltningsmessige kontrollen av Etterretningstjenesten ivaretas av forsvarssjefen som etatsjef og departementet på vegne av forsvarsministeren. EOS-utvalget ivaretar den uavhengige kontrollen av samtlige etterretnings- og sikkerhetstjenester på vegne av Stortinget, og Riksrevisjonen ivaretar på vegne av Stortinget revisjon og kontroll av at statens midler og verdier forvaltes i tråd med Stortingets beslutninger. I tillegg til ekstern kontroll gjennomfører Etterretningstjenesten også en omfattende internkontroll. Det har de siste årene vært en utvikling i grad av åpenhet om rammene for styring og kontroll av Etterretningstjenesten. Dette har medført at flere instrukser og bestemmelser har blitt gjort ugraderte og tilgjengelige der dette etter dets innhold er mulig. Som eksempel kan nevnes instruks for Koordineringsutvalget av 3. mars 2017.

6.7 Nærmere om dagens kontroll og forslag til lovregulering

6.7.1 Innledning

Den eksterne kontrollen av Etterretningstjenesten har egne hjemmelsgrunnlag. EOS-utvalgets kontrolloppgave berøres i noen grad av forslaget til ny etterretningstjenestelov. Det vises i denne sammenheng til forslaget om styrket kontroll av Etterretningstjenestens bruk av tilrettelagt innhenting, jf. høringsnotatets punkt 11.12. Det vises dessuten til forslag om mulig endring i kontrollområde i punkt 4.3.4.1. Lovforslaget her har for øvrig ikke til hensikt å gjøre noen endringer i eksisterende rammer for den forvaltningsmessige kontrollen av Etterretningstjenesten, annet enn å tydeliggjøre og forankre disse på en hensiktsmessig måte. Det vil i det følgende gjøres rede for de ulike kontrollformer Etterretningstjenesten er underlagt.

6.7.2 Opprettelsen av EOS-utvalget

6.7.2.1 Generelt om bakgrunnen for opprettelsen

Stortingets kontrollutvalg for etterretnings- overvåkings- og sikkerhetstjenestene i Norge fører parlamentarisk kontroll over etterretnings- overvåkings- og sikkerhetstjeneste som utføres av offentlig forvaltning eller under styring av eller på oppdrag fra denne.[142] EOS-utvalget ble opprettet i 1996 som en følge av en lengre tids mistillit til de «hemmelige

[141] Se bl.a. Europarådets Commission for democracy through law (Veneziakommisjonen) «Report on the democratic oversight of the Security Services» fra juni 2007

[142] Lov av 3. februar 1995 nr.7 om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste § 1

tjenestene» og til hvilken kontroll som egentlig ble utøvet over disse. Flere saker nådde offentlighetens lys som resultat av journalistisk arbeid, og dannet et bakteppe for en omfattende offentlig og politisk debatt om overvåking og kontroll.[143] Debatten om behovet for tilstrekkelig kontroll av EOS-tjenestene var ikke entydig rettet inn mot et stortingsoppnevnt kontrollorgan, da særlig spørsmålet om forholdet til samarbeid med utenlandske tjenester og forholdet til statsrådenes konstitusjonelle ansvar talte for et kontrollorgan underlagt regjeringens instruksjonsmyndighet. Stortinget vedtok imidlertid enstemmig at det skulle opprettes et eksternt kontrollutvalg i 1993. Det ble opprettet et utvalg[144] for å utrede rammene for et slikt kontrollutvalg, som ga sin anbefaling i 1994.[145] Innstillingen lå til grunn for Stortingets vedtak om å opprette EOS-utvalget 3. februar 1995. Lov om kontroll med etterretnings-, overvåkings- og sikkerhetstjenestene («EOS-kontrolloven») trådte i kraft samme dag. Med hjemmel i lovens § 1 ble instruks om kontroll med etterretnings-, overvåkings- og sikkerhetstjenestene vedtatt 30. mai 1995.

6.7.2.2 Nærmere om EOS-kontrolloven med tilhørende instruks

Allerede da EOS-utvalget ble opprettet var det forutsatt at loven skulle være gjenstand for evaluering. EOS-kontrolloven var gjenstand for enkelte endringer i 2009 og 2013.[146] Endringer ble også gjort i EOS-kontrollinstruksen i 2013.[147] I 2013 initierte Stortingets kontroll- og konstitusjonskomite en gjennomgang av en rekke forhold knyttet til EOS-utvalgets virksomhet og rammer for kontrollen. Stortingets presidentskap fulgte dette opp i mars 2014 med å vedta oppnevnelsen av medlemmer til et utvalg til evaluering av EOS-utvalget (Evalueringsutvalget) med tilhørende mandat. Utvalget avla sin rapport til Stortinget 29.februar 2016.[148]

Evalueringsutvalget fant at EOS-utvalgets kontroll hadde fungert godt etter sin opprinnelige intensjon, men at det likevel var tid for enkelte endringer og justeringer i EOS-utvalgets arbeid og rammebetingelser. Evalueringsutvalgets rapport omfattet et konkret forslag til endringer i EOS-kontrolloven og opphevelse av gjeldende EOS-kontrollinstruks. I forbindelse med Stortingets behandling av Evalueringsutvalgets rapport fremmet flere av medlemmene i Stortingets kontroll- og konstitusjonskomite et representantforslag om endringer i EOS-kontrolloven. Forslaget ble behandlet av Stortinget våren 2016[149] og 21. juni 2016 trådte gjeldende lov om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste i kraft.[150]

---

[143] «Edderkoppsaken», «Mossad-saken» og «Løfsnes-saken» var alle saker i mediebildet i perioden 1989-92

[144] EOS-kommisjonen/Skauge utvalget

[145] NOU 1994:4 *Kontrollen med de hemmelige tjenester*, avgitt 7. februar 1994

[146] Se lov av 19. juni 2009 nr.87 og lov av 21. juni 2013 nr. 81

[147] Innst. S. nr. 228 (2008-2009)

[148] Dokument 16 (2015-2016) Rapport til Stortinget fra Evalueringsutvalget for Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjenestene (EOS-utvalget)

[149] Innst.431 L (2016-2017) Innstilling fra kontroll- og konstitusjonskomiteen om Representantforslag fra stortingsrepresentantene Jette F. Christensen, Martin Kolberg, Gunvor Eldegard, Michael Tetzschner, Erik Skutle, Helge Thorheim, Gjermund Hagesæter, Per Olaf Lundteigen og Bård Vegar Solhjell om endringer i EOS-kontrolloven

[150] Lovvedtak 130 (2016-2017) Lov om endringer i lov 3. februar 1995 nr. 7 om kontroll med etterretnings-overvåkings- og sikkerhetstjeneste (EOS-kontrolloven)

6.7.2.3 Unntaket i innsyn for særlig sensitiv informasjon

EOS-utvalgets legitimitet som kontrollorgan forutsetter uinnskrenket tilgang til og innsyn i alt av opplysninger i alle arkiver og registre i Etterretningstjenesten som er nødvendig for at utvalget skal kunne utføre sin kontrolloppgave.[151] Formålet for utvalgets kontroll utgjør således en ytre ramme for utvalgets innsynsrett. Loven gir anvisning på disse rammene i § 8, tredje ledd:

> 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.

EOS-kontrollovens § 8 tredje ledd er en videreføring av lovens tidligere bestemmelse. Bestemmelsens rekkevidde har imidlertid vært gjenstand for noe ulik fortolkning av EOS-utvalget på den ene side, og Etterretningstjenesten og departementet på den annen side. En meget liten del av Etterretningstjenestens saker er av særlig sensitiv karakter og med et særdeles stort skadepotensiale. Behovet for særlig skjerming av denne informasjonen var bakgrunnen for at daværende forsvarsminister Jørgen Kosmo i 1997 ga retningslinjer om at denne type informasjon var unntatt EOS-utvalgets innsyn. Etter en påfølgende kommunikasjon mellom forsvarsministere, EOS-utvalget og Stortingets presidentskap, fastslo Stortinget i 1999 at slik informasjon var unntatt innsyn, med en tilhørende prosessuell ordning for håndtering av eventuell uenighet. Ved uenighet om hvorvidt informasjonen kan unntas, skulle saken forelegges forsvarsministeren med en påfølgende rett for EOS-utvalget til å bringe saken inn for Stortinget dersom enighet ikke kunne oppnås. Stortingets flertall fastsatte det samme i 2009.

Informasjonen som betegnes som «særlig sensitiv informasjon» og kan unntas EOS-utvalgets innsyn er informasjon vedrørende kildeidentifisering, okkupasjonsberedskapen og særlig sensitive utenlandsoperasjoner. I 2014 fastsatte departementet en ugradert definisjon av særlig sensitiv informasjon.[152] I forbindelse med revisjon av EOS-kontrolloven i 2017 var innsynsretten gjenstand for særlige merknader fra både EOS-utvalget, Forsvarsdepartementet og Justis- og beredskapsdepartementet. I kontroll- og konstitusjonskomiteens innstilling[153] ble det vist til definisjonen som fastsatt av departementet i 2014, og den ordningen som ble fastsatt av Stortinget og er beskrevet over. I komiteens merknader heter det:

> «Komiteen er av den oppfatning at dagens innsynsrett, sammen med forsiktighetsregelen, fungerer etter hensikten med å ivareta kildevernet og kontrollbehovet for metodebruk og ønsker å opprettholde denne.»[154]

---

[151] Lov av 3. februar 1995 nr.7 om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste § 8

[152] Særlig sensitiv informasjon er «informasjon som røper opplysninger om: 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.»

[153] Innst.431 L (2016-2017) Innstilling fra kontroll- og konstitusjonskomiteen om Representantforslag fra stortingsrepresentantene Jette F. Christensen, Martin Kolberg, Gunvor Eldegard, Michael Tetzschner, Erik Skutle, Helge Thorheim, Gjermund Hagesæter, Per Olaf Lundteigen og Bård Vegar Solhjell om endringer i EOS-kontrolloven.

[154] Ibid. s. 9

Unntaket i innsynsretten for særlig sensitiv informasjon anses med dette å ha fått en endelig avklaring.

6.7.3 Riksrevisjonen

Riksrevisjonen er et av Stortingets kontrollorganer. Riksrevisjonen skal gjennom revisjon, kontroll og veiledning bidra til at statens inntekter blir innbetalt som forutsatt, og at statens midler og verdier blir brukt og forvaltet på en økonomisk forsvarlig måte og i samsvar med Stortingets vedtak og forutsetninger. Riksrevisjonen reviderer Etterretningstjenesten, og de aktuelle representantene fra Riksrevisjonen har alle påkrevde klareringer og autorisasjoner for å ivareta de særskilte skjermingsbehov som knytter seg til Etterretningstjenestens virksomhet. Det vises til notatets punkt 6.3.2 for beskrivelse av representasjon fra Riksrevisjonen i Koordineringsutvalget for Etterretningstjenesten. De overordnede rammene framgår av lov og instruks om Riksrevisjonen.

6.7.4 Stortingets ombudsmann for forvaltningen – sivilombudsmannen

Sivilombudsmannen fører kontroll med hele den offentlige forvaltningen, både på grunnlag av konkrete klager fra enkeltpersoner og saker som tas opp av eget initiativ. Sivilombudsmannen skal ikke behandle klager på etterretnings-, overvåkings- og sikkerhetstjenestene som EOS-utvalget har behandlet.[155]

6.7.5 Domstolene

Domstolenes kompetanse til å behandle søksmål med påstand om ulovlig etterretningsvirksomhet følger de alminnelige reglene for sivile saker etter tvisteloven.[156] Dette er nærmere behandlet i punkt 4.3.4.2 og 4.3.6.

Departementet foreslår at domstolen skal utøve forutgående domstolskontroll i saker vedrørende Etterretningstjenestens bruk av tilrettelagt innhenting, hvor enkeltindividets interesser ivaretas av en særskilt oppnevnt advokat. Det foreslås at Etterretningstjenesten og den særskilte advokaten bør kunne anke kjennelser de er uenige i, og at straffeprosesslovens regler får anvendelse så langt de passer i slike saker. Se nærmere om departementets forslag om særregler for domstolskontroll av tilrettelagt innhenting i punkt 11.11.

6.7.6 Forsvarsdepartementets kontroll

Forsvarsdepartementet gjennomfører forvaltningsmessig kontroll av Etterretningstjenesten. Det vises her til notatet punkt 6.3.2 om K-utvalget. I tillegg kontrollerer departementet Etterretningstjenesten på konkrete forhold som tas opp av eksterne instanser og myndigheter og i eksterne prosesser, herunder alle forhold som tas opp i EOS-utvalgets rapporter og i Stortingets behandling av disse. Kontrollens format er tilpasset sakenes omfang og karakter, og kan omfatte krav om jevnlig eller enkeltstående rapportering, besøk til tjenestens ulike lokasjoner, krav om departementets særlige godkjenning og instruksregulering av særlige saker eller virksomhet.

[155] Instruks av 1. mars 1980 for Stortingets ombudsmann for forvaltningen § 2, første ledd

[156] Lov av 17. juni 2005 nr. 90 om mekling og rettergang i sivile tvister

6.7.7 Etterretningstjenestens internkontroll og interne rutiner

I tillegg til øvrig ekstern kontroll har Etterretningstjenesten etablert internkontrollregimer for å sikre at tjenestens virksomhet utøves i henhold til lov og forskrift og andre overordnede føringer og rammer, herunder i det årlige prioriteringsdokument. De ulike internkontrollregimene er tilpasset tjenestens ulike fagområder og etterretningsdisipliner og er nedfelt i interne instrukser, bestemmelser og retningslinjer. Enkelte av internkontrollregimene – og/eller deler av disse – har vært mulig å fastsette på ugradert nivå, og er gjort offentlig tilgjengelig. Tilgjengelighet til kontrollrammer er en styrke for tilliten til at tjenesten er underlagt et tilfredsstillende kontrollregime.

Internkontrollregimene i Etterretningstjenesten er av ulik karakter, og omfatter både system- og enkeltsakskontroll. Det er etablert både manuelle og automatiske mekanismer og kontrollen berører alle faser av informasjonsbehandlingen. Dette omfatter alt fra krav om forhåndsgodkjenning til rapportering og gjennomgang underveis i en prosess for å sikre overholdelse av regelverk og rammer, og videre til etterfølgende avviksrapportering der det er avdekket avvik i en eller annen form. En slik etterfølgende evaluering tar sikte på å blant annet avdekke hvorvidt det er snakk om systemsvikt og/eller enkeltsaker, manglende rutiner eller menneskelige feil. Et eksempel på en slik mekanisme er at innhenting av informasjon om norske rettssubjekter i utlandet eller deling av personopplysninger om norske personer med samarbeidende tjenester i andre land forelegges ledelsesnivået i Etterretningstjenesten i hvert enkelt tilfelle. Et annet eksempel er at det er etablert et eget element i tjenesten som har til oppgave å sørge for intern legalitetskontroll knyttet til tjenestens tekniske innhentingsvirksomhet.[157]

I tillegg til internkontroll for konkrete prosesser og enkeltsaker, gjennomfører Etterretningstjenesten grundig opplæring av egne ansatte.

Etterretningstjenesten fikk i 2014 en egen personvernrådgiver med særskilt ansvar for å sikre at tjenestens virksomhet utføres innenfor rammene av lov og underliggende instruks- og regelverk av relevans for ivaretakelse av enkeltpersoners personvern. Dette er nærmere omtalt under punkt 12.11.

6.7.8 Forslag til regulering

Departementet foreslår at EOS-utvalgets og Riksrevisjonenes kontroll fremgår av loven i § 2-8:

§ 2-8 *EOS-utvalgets og Riksrevisjonens kontroll*

Etterretningstjenesten er underlagt kontroll som fastsatt i EOS-kontrolloven. EOS-utvalget fører styrket kontroll med etterlevelse av særreglene i kapittel 7 om tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon.

Etterretningstjenesten er underlagt revisjon og kontroll av Riksrevisjonen etter riksrevisjonsloven. Riksrevisjonen utpeker bestemte tjenestepersoner for å ivareta revisjon og kontroll av Etterretningstjenesten. Utpekte tjenestepersoner skal være norske statsborgere og sikkerhetsklarert for STRENGT HEMMELIG.

Riksrevisjonen skal være representert i K-utvalget.

[157] Eksemplene er hentet fra Lysne II-utvalgets rapport om digitalt grenseforsvar

6.8 Årlig orientering for Stortinget

Stortinget mottar årlig en orientering om Etterretningstjenestens virksomhet. Ordningen ble omtalt allerede i Lund-rapporten:[158]

> «Ut fra hensynet til Etterretningstjenestens spesielle oppgaver er det i etterkrigstiden utviklet en praksis hvor forsvarsministeren har orientert og konsultert lederen i militærkomiteen, senere forsvarskomiteen i Stortinget, om spørsmål som angår etterretningstjenestens virksomhet. Nestformannen i komiteen har som regel også vært tilstede. Ordningen ble formalisert fra og med 1973, da Stortingets president begynte å delta i orienteringene, som etter hvert utviklet seg til å bli årlige. Forsvarsministeren informerte den utvidete utenriks- og konstitusjonskomite om kontaktordningen i 1978. Komiteen sa seg tilfreds med ordningen, og det er fra Stortingets side ikke senere reist spørsmål ved denne.»

Bakgrunnen for at denne særskilte ordningen ble etablert er behovet for skjerming som setter hinder for en åpen stortingsorientering. Orientering gis derfor til et begrenset utvalg stortingsmedlemmer. Det er i dag praksis at stortingspresidenten mottar orienteringen på vegne av Stortinget, med ledelsen i Stortingets utenriks- og forsvarskomite tilstede. I tillegg deltar Riksrevisor som ansvarlig for revisjonen av Etterretningstjenestens regnskap, og forsvarsministeren som parlamentarisk og konstitusjonelt ansvarlig for Etterretningstjenesten. Departementet foreslår at denne særskilte orienteringsordningen tas i inn i lovforslaget i § 2-9:

§ 2-9 *Orientering til stortingspresidenten*

Statsråden som er ansvarlig for Etterretningstjenesten orienterer stortingspresidenten årlig om Etterretningstjenestens virksomhet.

Sjefen for Etterretningstjenesten skal delta ved orienteringen. Stortingspresidenten bestemmer øvrig deltakelse.

7 Etterretningstjenestens oppgaver

7.1 Innledning

Den sikkerhetspolitiske situasjonen har de siste årene blitt stadig mer uforutsigbar, og fravær av konflikt i vår del av verden kan ikke tas for gitt. Norge og norske interesser kan i økende grad komme under sikkerhetspolitisk press. For at norske myndigheter skal kunne treffe veloverveide beslutninger for å sikre Norges suverenitet, territorielle integritet og politiske handlefrihet, kreves det relevant, rettidig og pålitelig informasjon om utenlandske aktører og deres aktiviteter, kapasiteter og intensjoner, samt om andre relevante utenlandske forhold som kan besvare norske myndigheters prioriterte informasjonsbehov. Etterretningstjenestens primæroppgave er å bidra med unik informasjon og analyse til kunnskapsbildet om slike forhold.

Ved en lovrevisjon er det naturlig å stille spørsmålet om det eksisterende rettsgrunnlaget i tilstrekkelig grad hjemler det oppdraget Etterretningstjenesten er forventet å utføre i dag og i overskuelig fremtid, eller om endringer er påkrevet. Det bør også undersøkes om Etterretningstjenestens samfunnsoppdrag bør justeres av andre årsaker.

[158] Dokument nr. 15 (1995-1996) punkt 13.2.4 side 853

Samfunnsoppdraget oppsummerer hva norske myndigheter og det norske folk forventer at Etterretningstjenesten skal bidra med i ivaretakelsen av Norges suverenitet og samfunnssikkerhet.

Etterretningstjenestens visjon er V*iten om verden til vern av Norge*. Operasjonalisert blir spørsmålet *hva* slags viten som er nødvendig, *hvilke* interesser og verdier som skal vernes, og mot *hvem* eller *hva* interessene og verdiene skal vernes. Formålet med kapittelet her er å vurdere hvilke oppgaver Norges utenlandsetterretningstjeneste bør ha, og hvordan dette bør lovreguleres. Oppgavene må fastlegges i lys av det sikkerhetspolitiske landskapet og andre forhold som på kortere og lengre sikt kan true eller på annen måte influere Norge og norsk sikkerhet. Dette landskapet danner rammen for hvorfor vi har en utenlandsetterretningstjeneste, hvilke oppgaver den bør ha og i noen grad hvilke ambisjonsnivåer som bør tilstrebes.

Fremstillingen i kapittelet her må sees i sammenheng med fremstillingen i kapittel 3 om utenlandsetterretningens plass i det internasjonale system av nasjonalstater og normer, og kapittel 4 om forholdet til Grunnloven og menneskerettighetene. Særlig vil menneskerettighetenes krav til tilstrekkelig klare og forutberegnelige lovhjemler for myndighetsinngrep overfor den enkelte ha betydning for den lovmessige utformingen av oppgavene.

Kapittelet her må også forstås i lys av forslaget om å lovfeste enkelte konkrete forbud, se kapittel 8 om at Etterretningstjenesten ikke skal utføre oppgaver med industrispionasjeformål eller politiformål. Endelig må Etterretningstjenestens oppgaver sees i sammenheng med den geografiske begrensningen for tjenestens virksomhet, som det redegjøres for i samme kapittel.

Departementet vil i det følgende kort gjøre rede for hvordan oppgavesettet er regulert i dagens etterretningstjenestelov. Deretter vil endringene i trusselbildet og dimensjonerende faktorer for norske myndigheters etterretningsbehov belyses. Videre vil det redegjøres for enkelte overordnede forhold som gjør seg gjeldende for alle innhentingshjemlene, før de enkelte hjemmelsforslagene beskrives nærmere.

Når det gjelder utfyllende informasjon innenfor de enkelte tematiske områder som beskrives er dette å finne i Etterretningstjenestens årlige ugraderte etterretningsvurderinger (publikasjonen «Fokus»), sist fremlagt 5. mars 2018.

7.2 Gjeldende lovregulering av Etterretningstjenestens oppgaver

7.2.1 Gjeldende regulering

Formålet med Etterretningstjenestens virksomhet er å bidra til å kartlegge og motvirke ytre trusler mot rikets selvstendighet og sikkerhet og andre viktige nasjonale interesser, jf. etterretningstjenesteloven § 1.[159] Etterretningstjenestens lovpålagte oppgaver følger i dag nærmere av § 3, som grovt sett kan kategoriseres i tre undergrupper:

1. Varsle om ytre trusler mot Norge og norske interesser
2. Gi etterretningsstøtte til Forsvarets operasjoner hjemme og ute i verden

[159] Lov av 20. mars 1998 nr. 11 om Etterretningstjenesten

3. Understøtte viktige politiske beslutningsprosesser med relevant informasjon vedrørende fokusområder for norsk utenriks-, sikkerhets- og forsvarspolitikk

Etterretningstjenesten pålegges i § 3 å innhente, bearbeide og analysere informasjon i den utstrekning det kan bidra til å sikre *viktige nasjonale interesser*. Paragrafen oppregner deretter en ikke-uttømmende liste over ti saksfelt som vil utgjøre slike viktige nasjonale interesser. Saksfeltene er fastsatt slik i etterretningstjenesteloven § 3 første ledd:

> Etterretningstjenesten skal innhente, bearbeide og analysere informasjon som angår norske interesser sett i forhold til fremmede stater, organisasjoner eller individer, og på denne bakgrunn utarbeide trusselanalyser og etterretningsvurderinger i den utstrekning det kan bidra til å sikre viktige nasjonale interesser, herunder
> a. utformingen av norsk utenriks-, forsvars- og sikkerhetspolitikk,
> b. beredskapsplanlegging og korrekt episode- og krisehåndtering,
> c. langtidsplanlegging og strukturutvikling i Forsvaret,
> d. effektiviteten i Forsvarets operative avdelinger,
> e. støtte til forsvarsallianser som Norge deltar i,
> f. norske styrker som deltar i internasjonale militære operasjoner,
> g. tilveiebringelse av informasjon om internasjonal terrorisme,
> h. tilveiebringelse av informasjon om overnasjonale miljøproblemer,
> i. tilveiebringelse av informasjon om ulike former for spredning av masseødeleggelsesvåpen og utstyr og materiale for fremstilling av slike våpen, og
> j. grunnlaget for norsk deltakelse i og oppfølging av internasjonale avtaler om nedrustnings- og rustningskontrolltiltak.

7.2.2 Nærmere om «viktige nasjonale interesser»

Vilkåret «viktige nasjonale interesser» er et fleksibelt begrep som sammenfatter det som til enhver tid vil være norske myndigheters informasjonsbehov. Samtidig er begrepet skjønnsmessig og gir i seg selv forholdsvis liten veiledning. Kombinert med en ikke-uttømmende opplisting har begrepet derfor blitt kritisert for å inneha en lav grad av forutberegnelighet. At opplistingen i § 3 ikke skal være uttømmende kan både leses ut av paragrafen selv, jf. begrepet «herunder» og er dessuten uttrykkelig uttalt i E-instruksen § 7 annet ledd.[160] Her fremgår det også at hva som utgjør viktige nasjonale interesser vil avhenge av hvilke sikkerhetsutfordringer Norge til enhver tid stilles ovenfor. Manglende formell avgrensning i overordnet regelverk kompenseres imidlertid gjennom at oppgavene til enhver tid vil være ytterligere detaljert og prioritert fra oppdragsgivernes side, i det årlige prioriteringsdokumentet som er nevnt i E-instruksen § 12 og som utgis av Forsvarsdepartementet. For oppdukkende prioriteter benyttes RFI-systemet (Request For Information) fra oppdragsgiver.[161] Dette innebærer at all innhenting og behandling av informasjon som Etterretningstjenesten gjennomfører, skal kunne knyttes direkte til et oppdrag nedfelt i prioriteringsdokumentet eller i en RFI fra overordnet myndighet. Innsamlingsoppdraget er derfor til enhver tid formålsavgrenset. Etterretningstjenesten innhenter aldri etterretninger for egen skyld eller for andre formål enn de som loven fastsetter og myndighetene til enhver tid prioriterer.

[160] Instruks av 31. august 2001 nr. 1012 om Etterretningstjenesten

[161] Se mer om dette oppdragsstyringssystemet i punkt 6.3.3

7.2.3 Fokus og samarbeid

At Etterretningstjenestens fokus kun skal være rettet mot utenlandske forhold sies ikke uttrykkelig i lovteksten, men fremgår klart forutsetningsvis av innledningen til § 3 («…i forhold til fremmede…»). At Etterretningstjenestens oppdrag skal være rettet mot utenlandske forhold støttes ytterligere av formålsbestemmelsen i § 1, som angir at formålet med loven er å legge forholdene til rette for at Etterretningstjenesten effektivt kan bidra til å kartlegge og motvirke *ytre* trusler. Dette innebærer at tjenesten utelukkende skal ha sitt fokus mot forhold som har sin tilknytning til, eller opprinnelse i, utlandet. Begrepet utelukker likevel ikke at ulike trusler og forhold som det har utenlandsetterretningsmessig verdi å innhente informasjon om, kan være grenseoverskridende, og dermed også ha en forbindelse til norske forhold. Dette fremkommer forutsetningsvis ved at gjeldende lov § 4 annet ledd hjemler Etterretningstjenestens behandlingsgrunnlag for informasjon om norske personer og virksomheter dersom informasjonen har direkte tilknytning til ivaretakelsen av Etterretningstjenestens oppgaver etter § 3.[162]

Det følger av etterretningstjenesteloven § 3 annet ledd at Etterretningstjenesten kan etablere og opprettholde etterretningssamarbeid med andre land. Utveksling av informasjon med samarbeidende tjenester i utlandet er en forutsetning for og en viktig del av slikt samarbeid. Det følger av forarbeidene til dagens lov, referert i punkt 7.8 nedenfor, at tjenesten kan innhente informasjon som er i samarbeidende tjenesters interesse. Bakgrunnen for dette er at slik innhenting indirekte også vil ha betydning for norske interesser i lys av at tjenesten ofte får viktig informasjon tilbake ut fra et gjensidighets- og informasjonsbytteperspektiv.

Etter gjeldende lov § 3 tredje ledd er det også en oppgave for Etterretningstjenesten å sikre en nasjonal okkupasjonsberedskap.

7.3 Overordnede utviklingstrekk og dimensjonerende faktorer

7.3.1 Det sikkerhetspolitiske landskapet

Tiden før vedtakelsen av dagens lov fra 1998 var preget av at den kalde krigen var slutt, og de endringer i Etterretningstjenestens rolle og norske myndigheters informasjonsbehov som dette medførte. Lund-kommisjonens rapport, som gransket hvorvidt de såkalte hemmelige tjenestene hadde vært engasjert i ulovlig eller irregulær overvåkning av norske borgere, hadde skapt debatt. Dessuten diskuterte man på prinsipielt grunnlag om ledende tjenestemenn burde avstå fra partipolitisk virksomhet så lenge de var ansatt i tjenesten. Etterretningstjenestens virke hadde på dette tidspunkt ikke tidligere vært regulert i lov. Man vurderte i forarbeidene at det objektivt sett ikke var behov for å lovregulere tjenestens virksomhet:[163]

> «Hensikten med en slik lovregulering [vil] først og fremst være å etterkomme ønske om at Stortinget i lovs form trekker opp grensene for tjenestens oppdrag og beføyelser og innretter bestemmelsene slik at de underbygger det forhold at tjenesten er underlagt nasjonal politisk styring og kontroll.»

Det ble videre fremhevet at:

[162] Det redegjøres nærmere for behandlingen av personopplysninger i høringsnotatet kapittel 12.

[163] Se Ot.prp. nr. 50 (1996-1997) s. 3

> «En lovregulering av Etterretningstjenestens oppgaver signaliserer dessuten i seg selv en mer åpen holdning, og vil derigjennom søke å trygge allmennhetens tillit til tjenesten.»

Behovet for allmennhetens tillit til Etterretningstjenesten er det samme i dag som da gjeldende lov ble til. Men de samfunnsmessige og rettslige rammene for etterretningsvirksomheten ser annerledes ut. Det er god grunn til å hevde at det sikkerhetspolitiske landskapet ikke fremstår som mer stabilt og forutsigbart i dag, snarere tvert om. Betydningen av Norges geografiske plassering nær russiske strategiske baseområder har forsterket seg de senere år gjennom den russiske militære moderniseringen, samt NATOs fornyede fokus på alliansens nordlige område. Den sikkerhetspolitiske utviklingen, utviklingen i internasjonale maktstrukturer, fremvekst av nye trusler og måter trusselaktivitet utøves på, utviklingen innen digitalisering og den dertil tilhørende avhengigheten av og sårbarheten forbundet med digitale tjenester, samt rettsutviklingen særlig på menneskerettighetenes område, har vært stor. Departementet vil belyse dette i det følgende ved å trekke frem enkelte dimensjonerende faktorer for norske etterretningsbehov.

7.3.2 Dimensjonerende faktorer for utvikling av trusselbildet og politikkutformingen

7.3.2.1 Generelt

Sentrale globale utviklingstrekk som har alvorlige implikasjoner for Norges sikkerhet er tilbakekomsten av statlige baserte trusler der alle statens virkemidler tas i bruk for å påvirke andre nasjoner. Særlig har hendelsene på Krim og i Øst-Ukraina vært en alvorlig påminnelse om at statlig maktbruk og mellomstatlige konflikter er en faktor som aldri kan utelukkes. Videre er vi vitne til en økende trussel fra terrorisme og ekstremisme, en teknologisk utvikling og økende trusler i det digitale rom, samt utfordringer mot en lov- og regelbasert internasjonal orden som gjør det vanskeligere å håndtere globale utfordringer. Disse utviklingstrekkene danner grunnleggende premisser for utformingen av norsk sikkerhets-, utenriks- og forsvarspolitikk i årene fremover, og vil være drivende for norske sikkerhetspolitiske prioriteringer.

7.3.2.2 Våre nærområder

Russland vurderes å forbli en dimensjonerende faktor for norsk sikkerhets- og forsvarspolitikk, herunder som følge av Norges geografiske beliggenhet. Russlands folkerettsbrudd i Ukraina og strategiske rivalisering med Vesten har fundamentalt endret den sikkerhetspolitiske situasjonen i Europa. Det nåværende russiske regimets viktigste målsettinger er å holde på makten, samt gjenetablere Russland som en stormakt. Et mer offensivt Russland, med et forverret forhold til NATO og Vesten, har i de senere år fremstått stadig mer selvhevdende på den utenrikspolitiske arenaen. Et militært styrket Russland har demonstrert økt vilje til å bruke makt for å hevde sine interesser og understøtte sine stormaktsambisjoner. Russland har i takt med dette demonstrert målrettet evne til å benytte alle statens virkemidler for å sikre nasjonale interesser i sine nærområder, inkludert i strid med folkeretten. Russland utgjør ingen militær trussel mot Norge i dag, men Norges geografiske plassering og russiske kapasiteter medfører at utviklingen i Russland og nordområdene har vedvarende stor betydning for norsk og alliert sikkerhet. Solid og tidsriktig situasjonsforståelse, herunder inngående kunnskap om utviklingen i russisk utenriks- og innenrikspolitikk og om moderniseringen av den russiske militærmakt i Norges nærområder, er således avgjørende forutsetninger for å kunne utforme norsk utenriks-, forsvars- og sikkerhetspolitikk.

Hovedoppgaven til den russiske militærmakten i nordområdet er å ivareta den russiske evnen til kjernefysisk avskrekking og gjengjeldelse. Baseområdet for den russiske Nordflåtens baser på Kolahalvøya innebærer at norske nærområder er patruljeringsområde for ubåter som bærer interkontinentale ballistiske missiler med atomstridshoder, og det er et av de viktigste testområder for nye våpensystemer i Russland. Gjennom militærreformen som ble igangsatt i 2008 har Russland gjennomført en storstilt modernisering av militærmakten. Russland har styrket sin kjernevåpenkapasitet, og fortsetter å modernisere plattformene for levering av disse våpnene, herunder nye ubåter. Utviklingen i den russiske militærmakten tilsier dermed at nordområdets relative militærstrategiske betydning vil øke heller enn å avta i årene som kommer. Det russiske bastionsforsvarskonseptet innebærer at Russland vil kunne nekte eller kontrollere tilgang til hav- og landområder som også inkluderer deler av norsk territorium. Konseptet kan aktiveres i en situasjon med økt militær spenning mellom Russland og NATO i Europa, eller i en situasjon der verken NATO eller Norge er direkte part i en konflikt med Russland. Dette er en strategisk utfordring for NATO.

Gjennom militærreformen har Russland ervervet seg økt evne til presisjonsangrep over store avstander, strategisk styrkeoverføring og projisering av militærmakt. Russlands økte militære evne medfører at mulighetene for å oppdage og varsle forestående militære operasjoner i nordområdene har gått betydelig ned, og varslingstiden er tilnærmet ingen. Dette har store konsekvenser for norsk og alliert sikkerhet.

Russiske myndigheter har sterke økonomiske og militære interesser i Arktis og nordområdene. Det økonomiske potensialet i Arktis ligger for Russland primært i potensialet for ressursutvinning og utviklingen av Nordøstpassasjen som en internasjonal handelsrute. Styrket russisk kontroll i området har til formål å hindre andre aktører i å utfordre russiske økonomiske og militærstrategiske interesser i regionen når iskappen smelter og tilgangen blir enklere. Som en følge av issmelting er det økt aktivitet i nordområdene og Arktis. En rekke aktører, inkludert de arktiske kyststater og asiatiske land som Kina, Japan, Singapore, India og Sør-Korea, posisjonerer seg nå for fremtidige utviklingsmuligheter.

Norge har et spesielt ansvar overfor NATO i nordområdene. Dette innebærer at Norges bidrag til situasjonsforståelse av utviklingen i nordområdene og Russland er viktig for både norsk og alliert sikkerhet. I lys av den sikkerhetspolitiske og militærstrategiske utvikling må Norge ha en etterretningstjeneste som er rettet mot både sivile og militære intensjoner og kapasiteter, herunder forhold som kan påvirke Norges bilaterale forhold til Russland og/eller alliert sikkerhet. Tjenesten må evne å opprettholde situasjonsforståelse, kartlegge og varsle om trusler både i fredstid og i sikkerhetspolitiske krisesituasjoner. I lys av de senere års sikkerhets- og militærstrategiske utvikling har også NATO i økende grad fokusert på medlemslandenes territorier og nærområder. Dette har medført økt synlighet gjennom mer øving og trening, bedret beredskap knyttet til kollektivt forsvar av medlemslandene og fokus på en bred og tidsriktig situasjonsforståelse. Det er helt avgjørende at de respektive allierte bidrar med etterretninger fra sine nærområder. Norge må ha en etterretningstjeneste som, i likhet med tidligere, gir et vesentlig bidrag til alliert situasjonsforståelse i nordområdene. Norges etterretningsinnsats mot Russland og andre statlige aktører som har interesser i nordområdene gir i dag verdifull informasjon til allierte og partnere. Dette har igjen medført at Norge mottar støtte og tilgang på avansert teknologi, hvilket bidrar til å skape et best mulig etterretningsbilde på andre områder som er av betydning for Norge og norske interesser.

7.3.2.3 Digitalisering

Digitaliseringen av samfunnet er kanskje den største og mest målbare samfunnsendringen i moderne tid. I en stadig mer globalisert verden har vi også vært vitne til en økning i *grenseoverskridende* trusler. Norge er et av verdens mest digitaliserte samfunn. Det digitale rom er blitt et domene for alle aspekter ved samfunnsaktivitet. Dette domenet benyttes både sivilt og militært, som kommunikasjons- og møteplattform, viral virkelighet, krigføringsdomene og styringsplattform for tekniske innretninger og kritisk infrastruktur. Adgangen til å påvirke uten fysisk tilstedeværelse er fremtredende. Operasjoner kan i sin helhet styres fra andre land via tastaturet.

Selv om prinsippene om nasjonalstatens jurisdiksjon, det vil si statlig myndighetsutøvelse, gjelder på samme måte i det digitale som i det fysiske rom, er det en rekke faktiske forhold som kompliserer bildet. Kommunikasjonsstrømmene beveger seg over landegrensene og er gjerne innom flere land før de når sin mottaker. Internettet oppfattes som grenseløst, og myndighetskontrollen er i varierende grad effektiv. Bruken av stråmenn og muligheten til å rute aktivitet gjennom nettverket gjør at man kan utøve ondsinnede handlinger på nett med svært lav risiko for å bli oppdaget.

Digitale plattformer brukes også som kommunikasjonsmåte mellom terrorister. Terroranslag koordineres, planlegges og styres online. Radikalisering, rekruttering og støttevirksomhet, herunder pengeinnsamling, gjøres også i stor grad på nett. Her spiller sosiale medier en fremtredende rolle.

Fravær av myndighetskontroll øker anvendbarheten av digitale verktøy for etterretningsorganisasjoner og terrororganisasjoner. Etterretningsoperasjoner mot Norge øker i omfang og kompleksitet, særlig i det digitale rom. Statlig etterretningsvirksomhet utgjør den største trusselen. Det bedrives en omfattende kartlegging av sårbarheter, og fremmede stater har evne til å gjennomføre sabotasje ved hjelp av digitale verktøy.

7.3.2.4 Internasjonal terrorisme og sammensatte trusler

Trusselen fra *internasjonal terrorisme* vurderes å være vedvarende. Terrorplaner og angrep utføres av medlemmer av terroristgrupper, fremmedkrigere, radikaliserte kriminelle og andre som lar seg inspirere av ønske om å angripe statsmakter, symboler på vestlige demokratier og sivile for å spre sitt budskap og spre frykt. At norske fremmedkrigere i betydelig omfang skulle ta del i internasjonal terrorvirksomhet i Syria, Irak og andre områder, var ikke et forventet utviklingstrekk ved vedtakelsen av dagens lov i 1998.

Faren for spredning av *masseødeleggelsesvåpen*, samt spredning av utstyr og materiale til bruk i fremstillingen av slike våpen, har vært en kilde til uro så lenge disse våpnene har eksistert. Spredningsfaren vil kunne øke ytterligere dersom stadig flere land skulle klare å erverve en slik kapasitet.

Hybrid krigføring og *hybride trusler* er i dag et velkjent fenomen. Det finnes ulike definisjoner på hva som utgjør en hybrid trussel, og ulike synspunkter på om begrepet er særlig dekkende eller innebærer noe nytt. Felles er imidlertid en økende erfaring med at enkelte aktører bruker sammensatte handlemåter og mer eller mindre skjult trusselaktivitet, i den hensikt å påvirke et forhold, et objekt eller en adferd eller hendelsesutvikling. Aktiviteten kan utfordre nasjonalstaters suverenitet og internasjonale rettsnormer. Hybride trusler under terskelen for synlig militær maktbruk er ikke noe nytt. En ny faktor er imidlertid at digitaliseringen av samfunnet har ført med seg nye virkemidler og nye sårbarheter. Vi ser dessuten at bruken av alle statens virkemidler i de senere år har blitt mer fremtredende.

Denne utviklingen kan også til dels utfordre tersklene i folkeretten mellom fred, suverenitetskrenkelse, aggresjon og væpnet angrep. Behovet for god etterretning står helt sentralt for å finne frem til fakta for å kunne gjøre riktige vurderinger, som igjen gir grunnlag for riktig reaksjon.

Den mangefasetterte og omskiftelige sikkerhetspolitiske og teknologiske utviklingen, og signifikante endringer i trusselbildet, stiller store krav til en strategisk etterretningstjeneste, dens virksomhet og oppdrag. Behovet for pålitelig utenlandsetterretning har økt.

7.4 Etterretningstjenestens oppgaver i ny lov - hovedinnretning og begrepsbruk

7.4.1 Generelt

Etterretningstjenesten er Norges eneste utenlandsetterretningstjeneste, og den har ansvar for både sivil og militær utenlandsetterretning. Dette foreslås videreført. I Norge skiller vi mellom utenlandsetterretning og innenlandsetterretning, hvorav sistnevnte utøves av PST (og det ordinære politi på enkelte områder). PST og politiet har dessuten et påtaleansvar og dermed en straffeforfølgelsesoppgave. Etterretningstjenesten har ikke noe pønalt formål med sin virksomhet. Etter departementets syn er det ikke grunnlag for å endre på gjeldende ansvars- og oppgavedeling mellom PST og Etterretningstjenesten, se punkt 8.10 og 13.2.

Innenfor *utenlandsetterretningsdomenet* har departementet vurdert om oppgavene slik de er formulert i dagens lov skal beholdes eller om de bør justeres. Til dette kommer også spørsmålet om Etterretningstjenestens oppgavesett er formulert på en tilstrekkelig klar måte. Videre er det behov for å vurdere om hjemmelsgrunnlaget i tilstrekkelig grad dekker de aktiviteter det er ønskelig at tjenesten utfører. Departementet mener at det ikke er behov for større substansielle utvidelser eller innskrenkninger av Etterretningstjenestens samfunnsoppdrag, men mener likevel det er grunn til å gjøre visse justeringer av oppgaveformuleringene samt avgrense samfunnsoppdraget på en mer uttømmende og presis måte enn i gjeldende lov.

Departementet vil i det følgende gjøre rede for noen grunnleggende forutsetninger for reguleringen av Etterretningstjenestens oppgavesett som er felles for alle innhentingshjemlene som foreslås. Deretter vil den nærmere utformingen av innhentingshjemlene drøftes.

7.4.2 Uttømmende regulering av oppgavesettet

Gjeldende rett vurderes å dekke samfunnsoppdraget i tilstrekkelig grad, men departementet mener lovkravets kvalitative side tilsier at oppgavene bør fremgå på en mer presis og avgrenset måte i den nye lovteksten, sett i forhold til dagens regulering. Saksfeltene som oppgis i loven bør etter departementets syn gjøres *uttømmende*. Oppgaveformuleringen har betydning både for formålsbestemthetsprinsippet og forholdsmessighetsprinsippet for innhenting og behandling av informasjon, se nærmere om disse prinsippene i punktene 9.5.2, 9.5.3 og kapittel 12.

Ulempen med en slik regulering er at man mister noe av fleksibiliteten som følger av gjeldende lovverk, som i dag enkelt kan tilpasses og tolkes i lys av et dynamisk og skiftende trusselbilde. Samtidig vurderer departementet at en mer konkret beskrivelse av

oppgavefeltene vil skape høyere grad av tydelighet og forutberegnelighet, og dermed bidra til å øke tilliten til tjenestens samfunnsrolle. Forslaget til ny lovtekst innebærer i prinsippet et mer begrenset oppdrag for Etterretningstjenesten sammenlignet med det skjønnsmessige handlingsrommet som følger av dagens lov. Trusselbildet vil kunne endres betydelig over tid, og nye trusler utvikles raskt. Departementet har derfor i tråd med norsk lovgivningstradisjon søkt å utforme ny lovtekst på en slik måte at det ikke vil være behov for stadige lovendringer i takt med endringer i trusselbildet og fremvekst av andre utfordringer. En klarere og mindre skjønnsmessig oppgavebeskrivelse er derfor søkt kombinert med en tilstrekkelig fleksibel lovtekst, slik at den står seg over tid. Herunder er det brukt begreper som «trusler mot Norges selvstendighet og sikkerhet» for å ta høyde for fremtidige statssikkerhetstrusler som i dag ikke kan overskues.

Departementet vurderer at det verken er hensiktsmessig eller mulig å gi en detaljert beskrivelse i loven av *hvilke handlinger* som kan lede til at enkeltpersoner blir berørt av Etterretningstjenestens innhentingsvirksomhet eller at de havner i tjenestens søkelys. Det vises i denne forbindelse til fremstillingen i punkt 8.9 og til de klare forskjellene mellom kriminalitetsbekjempelse og etterretningsvirksomhet. Etterretningstjenestens oppgave er å innhente informasjon som er av betydning for politiske og militære myndigheter, ikke å fremskaffe bevis til bruk for straffeforfølgelse. Innhenting kan også skje mot personer som ikke utgjør noen trussel eller som ikke er involvert i noe klanderverdig, men som følge av at personene besitter, kommuniserer eller vil kunne motta informasjon som er relevant for formål som ligger innenfor oppgavebeskrivelsen.

Departementet mener at loven bør utformes slik at den beskriver hvilke *kategorier av saksfelt* Etterretningstjenesten skal innhente informasjon om. Dette må være saksfelt som sivile og militære myndigheter har et klart behov for kunnskap om i ivaretakelsen av nasjonal sikkerhet eller andre grunnleggende nasjonale sikkerhetsinteresser. For *trusler* gjelder dette innhenting av informasjon for å avdekke og motvirke nærmere angitte trusselkategorier. For innhenting av informasjon om *andre utenlandske forhold* gjelder det informasjon om militære og sivile forhold og utviklingstrekk i andre stater og regioner som kan være relevant for ivaretakelse av prioriterte norske utenriks-, forsvars- og sikkerhetspolitiske interesser, nasjonal beredskapsplanlegging, episode- og krisehåndtering, og planlegging og gjennomføring av nasjonale eller internasjonale militære operasjoner. Departementet viser i denne forbindelse til høringsnotatet kapittel 4 der det gjøres nærmere rede for de kvalitative kravene til lovteksters utforming i punkt 4.2.5.2, med henvisning til relevant rettspraksis. En avgrensning til kategorier av saksfelt oppfyller etter departementets syn menneskerettighetenes krav.

Oppregningen og rekkefølgen av saksfeltene i selve lovteksten skal ikke anses som en prioritering av Etterretningstjenestens innsats. Som i dag, ligger det heller ikke i ordet «skal innhente» at tjenesten plikter å utøve samtlige oppgaver samtidig. Etterretningstjenesten må evne å omstille innsamlingskapasiteter innenfor rammen av loven og de prioriteringer som til enhver tid fastsettes av overordnede myndigheter. Det vises til omtalen i punkt 6.3.3 om oppdragsstyring og det overordnede prioriteringsdokumentet som fastsettes årlig.

7.4.3 Sentrale innhentingsformål

Etterretningstjenestens tre hovedkategorier av oppgaver ble listet opp i punkt 7.2.1, nemlig strategisk varsling, etterretningsstøtte til Forsvaret og beslutningstøtte til norske myndigheter innenfor prioriterte saksfelt. Departementet mener at disse bør videreføres, om enn med noe

endret innretning; Oppgaven om å kartlegge og motvirke utenlandske trusler og yte beslutningsstøtte til norske sivile og militære og myndigheter videreføres i forslaget til lovtekst, men formuleres på en tydeligere og mer formålsavgrenset måte enn etter gjeldende lov. Oppdraget om å støtte norske styrker deployert i utlandet bør også etter departementets syn ligge fast.

Når det gjelder *strategisk varsling* om forhold som berører norsk statssikkerhet og samfunnssikkerhet blir dette ofte omtalt som en av Etterretningstjenestens viktigste oppgaver. Også det å *rapportere* til overordnede nasjonale myndigheter om viktige forhold som avdekkes gjennom informasjonsinnhenting og analyse står sentralt fordi Etterretningstjenesten jo ikke innhenter informasjon for sin egen del. Varslings- og rapporteringspliktene er imidlertid ingen selvstendige hjemler for informasjonsinnhenting, og hører derfor etter departementets syn strukturmessig sammen med oppdragsstyring og rapporteringsrutiner. Varslings- og rapporteringsplikten foreslås derfor regulert i lovutkastets kapittel 2 og ikke i kapittelet om Etterretningstjenestens oppgaver.

7.4.4 Hvem informasjonen er myntet på

Departementet har vurdert hvorvidt det er behov for å presisere i lovteksten hvem som er mottaker av informasjonen som Etterretningstjenesten henter inn. Gjeldende etterretningstjenestelov inneholder ingen slik presisering, men det følger av E-instruksen § 8 annet ledd at Etterretningstjenesten i fredstid skal produsere etterretninger som gir *nasjonale myndigheter* grunnlag for å treffe avgjørelser vedrørende, samt forebygge og håndtere, episoder, kriser og krig.

I lovforslaget følger regler om oppdragsstyring av kapittel 2. De formelle oppdragslinjer ligger dermed fast. Samtidig kan det anføres at en angivelse av *hvem* som er mottaker av informasjonen som hentes inn vil kunne gi en merverdi for hvordan informasjonsinnhentingen og etterretningsproduksjonen innrettes, fordi det kan indikere hvilket etterretningsbehov mottakeren har.

Mottakere av etterretningsinformasjonen er norske sivile og militære myndigheter. Etterretningsbehovet vil variere avhengig av hvilket organisatorisk nivå mottakeren sitter. På sivilt og militært strategisk nivå har etterretning som hovedoppgave å støtte nasjonale beslutningstakere med etterretninger innen et spekter av problemstillinger knyttet til ivaretakelsen av sentrale nasjonale sikkerhetsinteresser. På militært operasjonelt nivå er etterretning primært knyttet til operasjoner, og vil ofte omhandle forhold innenfor et avgrenset operasjonsområde i henhold til et operasjonsmandat. På militært taktisk nivå spiller etterretning en viktig rolle for å gi den taktiske sjefen mulighet til å vurdere hvordan han eller hun bør disponere sine enheter for å løse et oppdrag. På taktisk nivå i Forsvaret vil man imidlertid normalt også ha en egen innhentingsevne for å ivareta styrkebeskyttelse og komplettere det etterretningsbildet som gis av høyere nivå.

Etter en vurdering har departementet kommet til at det ikke er hensiktsmessig å presisere hvem som er mottaker av informasjonen i lovteksten. Etterretningsbehovet vil allerede fremgå av prioriteringsdokumentet og RFI. Dette fremgår av lovutkastet § 2-4 og er nærmere beskrevet i høringsnotatet punkt 6.3.3. Lovteksten vil bli unødvendig detaljert dersom alle oppdragsgivere skal spesifiseres særskilt, og et sekkebegrep som «for norske myndigheter» er etter departementets syn så overordnet at det gir lite veiledning. Selv om det ikke

presiseres i oppgavekapittelet er det imidlertid ikke tvil om at Etterretningstjenesten er et redskap for det øverste myndighetsapparatet og at den strategiske oppgaven står sentralt.

Departementet vil dessuten understreke at Etterretningstjenesten er en del av det norske Forsvaret og skal yte løpende støtte til Forsvaret og forsvarssektoren. Denne støtten utøves på daglig basis, og er særlig viktig for strategisk situasjonsforståelse, i forbindelse med episode- og krisehåndtering og som etterretningsstøtte for militære styrker som deltar i nasjonale og internasjonale operasjoner. Hvilken aktivitet i Forsvaret og forsvarssektoren Etterretningstjenesten skal støtte, blir i dagens lov listet opp i flere av underpunktene i § 3 første ledd. Departementet mener det ikke er behov for å videreføre opplistingen av alle former for etterretningsstøtte til Forsvaret som følger av dagens lov. Til illustrasjon vil det ikke være nødvendig å nevne støtte til langtidsplanlegging og strukturutvikling i Forsvaret særskilt. Slik støtte vil inngå som en naturlig tolking av at tjenesten skal innhente informasjon som kan ha relevans for ivaretakelse av prioriterte forsvarspolitiske interesser.

7.4.5 Relevansvurdering

Innhenting av informasjon, både om trusler og om andre utenlandske forhold, skal bare skje når informasjonen antas å ha relevans for en eller flere av de angitte oppgavene i lovutkastet kapittel 3. Formuleringen «som kan bidra til» i utkast til §§ 3-1 og 3-2 indikerer at terskelen for informasjonsinnhenting ikke må være for høy sett opp mot sannsynligheten for at innhentingen vil frembringe relevant informasjon for Etterretningstjenestens oppgaveløsing. Begrepet er ikke ment å tilføre noen selvstendig eller ytterligere terskel sett opp mot grunnvilkårene for innhenting. De foreslåtte nærmere terskler for henholdsvis målsøking og målrettet innhenting er derfor behandlet i høringsnotatet kapittel 9. Videre vises det til reglene for behandling av informasjon som allerede er innhentet, herunder bestemmelser om sletting. Reglene om dette er beskrevet i høringsnotatet kapittel 12 og 11.13.2. Formuleringen «for å avdekke og motvirke» i utkast til § 3-1 om utenlandske trusler er en formålsbeskrivelse som indikerer viktigheten av å hindre slike handlinger, og at avdekking sjelden er et poeng i seg selv dersom avdekkingen ikke kan bidra til å forebygge eller på annen måte motvirke den uønskede handlingen.

7.5 Nærmere om informasjonsinnhenting om utenlandske trusler (lovutkastet § 3-1)

7.5.1 Utfordringer mot stats- og samfunnssikkerheten (lovutkastet § 3-1 bokstavene a-c)

7.5.1.1 Generelt

Statssikkerhet vil si å ivareta statens eksistens, suverenitet, suverene rettigheter og territorielle integritet. Statssikkerheten kan utfordres gjennom væpnet angrep, politisk og militært press mot politiske myndigheter, og alvorlige anslag mot norske interesser fra statlige eller ikke-statlige aktører. Trusler mot Norges økonomiske handlefrihet kan også utfordre statssikkerheten.

Samfunnssikkerhet handler om å ivareta befolkingens liv, helse og trygghet, og sikre sentrale samfunnsfunksjoner og viktig infrastruktur mot skade. Man kan hevde at skillet mellom statssikkerhet og samfunnssikkerhet i blant kan fremstå mindre klart som følge av den teknologiske utvikling og gjensidige avhengigheter mellom offentlig og privat, og mellom

sivil og militær virksomhet. Samfunnssikkerheten kan også være utfordret i en situasjon hvor statssikkerheten er truet, men samfunnssikkerheten kan være truet uten at statens eksistens er truet.

7.5.1.2 Statssikkerheten – en grunnleggende oppgave

Norge befinner seg i et sikkerhetspolitisk landskap som er preget både av kontinuitet så vel som omfattende og raske endringer i stormaktsrelasjoner, militære utviklingstrekk i våre nærområder, grenseoverskridende trusler i det fysiske og digitale rom, samt en rekke regionale konflikter som kan få globale konsekvenser.

Det er en grunnleggende oppgave for Etterretningstjenesten å rette fokus mot statlige baserte trusler, intensivert statlig rivalisering og mulig bruk av alle statens virkemidler som kan true Norges territorielle integritet, politiske handlefrihet eller samfunnssikkerhet. I tillegg vil mulige krenkelser av norsk suverenitet eller norske suverene rettigheter alltid være en primæroppgave for Etterretningstjenesten, uavhengig av krenkelsens omfang og uavhengig av hvem som står bak. Denne oppgaven er formulert i lovutkastet § 3-1 første ledd bokstav a.

Med begrepet «økonomisk handlefrihet» i utkast til § 3-1 første ledd bokstav a forstår departementet sikkerhet for politisk handlefrihet på det økonomiske området, og begrepet vil inkludere informasjonsinnhenting som kan ha relevans for å avdekke og motvirke anslag mot virksomheter som har en helt sentral rolle knyttet til landets økonomiske trygghet og stabilitet, for eksempel i finanssektoren, energisektoren eller petroleumssektoren.

7.5.1.3 Samfunnssikkerheten

Etterretningstjenestens oppgave om å innhente informasjon som kan ha relevans for å avdekke og motvirke *alvorlige trusler mot samfunnssikkerheten* i Norge (bokstav b) bør etter departementets syn også fremgå direkte av lovteksten. Dette selv om enkelte forhold som alvorlig kan utfordre samfunnssikkerheten – blant annet grenseoverskridende terrorisme – er eksplisitt angitt som en oppgave for Etterretningstjenesten i lovforslaget § 3-1 første ledd bokstav f. Bakgrunnen for at samfunnssikkerheten bør angis som en egen kategori er at samfunnsutviklingen kan medføre fremvekst av nye alvorlige trusler som i dag ikke er kjent.

Begrepet «alvorlig» gjør det klart at Etterretningstjenesten ikke skal innhente informasjon om enhver trussel som kan utfordre samfunnssikkerheten, kun de truslene som utfordrer samfunnets grunnleggende funksjonalitet, stabilitet eller handlefrihet eller befolkningens grunnleggende sikkerhet.

I utgangspunktet legger departementet til grunn at kjernen i Etterretningstjenestens samfunnsoppdrag er å innhente informasjon om trusler fra statlige og ikke-statlige aktører, og ikke om ikke-villede trusler som naturkatastrofer og lignende. Dette utelukker ikke at Etterretningstjenesten kan innhente informasjon om naturgitte eller menneskeskapte fenomener som f. eks. tørke, epidemier, vann- og matmangel eller migrasjon i den utstrekning slike fenomener kan utfordre norsk samfunnssikkerhet på kortere eller lenger sikt eller utnyttes av aktører med ondsinnede hensikter.

7.5.1.4 Norske interesser i utlandet

I tråd med dagens praksis mener departementet at også alvorlige trusler mot *norske interesser i utlandet* (bokstav c) bør angis direkte i lovteksten. Dette alternativet kan omfatte trusler mot norske borgere i utlandet, for eksempel gisselsituasjoner, av en karakter som faller utenfor trusselen fra internasjonal terrorisme.

7.5.2 Fremmed etterretningsvirksomhet, sabotasje og annen påvirkning (lovutkastet § 3-1 bokstavene d og e)

7.5.2.1 Generelt

Departementet mener Etterretningstjenesten fortsatt skal ha som oppgave å innhente informasjon som kan bidra til å avdekke og motvirke fremmed etterretningsvirksomhet, sabotasje og annen påvirkning. Denne oppgaven er formulert i lovutkastet § 3-1 første ledd bokstavene d og e, og vil beskrives nærmere i det følgende.

7.5.2.2 Etterretningstrusselen fra statlige eller statsstøttede aktører

Statlig etterretning er et sentralt virkemiddel for å støtte et lands politiske, økonomiske og sikkerhetsmessige interesser. Etterretningsvirksomhet mot Norge og norske interesser skjer i stor utstrekning fra statlige aktører. Fremmede staters etterretningsvirksomhet representerer en vedvarende og økende trussel mot nasjonale myndigheter, norsk økonomi og samfunnssikkerhet. Økt digitalisering har medført at trusselen har blitt vesentlig mer alvorlig og omfattende. Aktørenes mål er å få tilgang til sensitiv og skjermingsverdig informasjon, påvirke politiske, økonomiske og forvaltningsmessige avgjørelser og undersøke muligheter for å kunne sabotere viktig infrastruktur ved en eventuell fremtidig konflikt. Industrispionasje er også fortsatt en utfordring, til tross for økende internasjonal enighet om at slik etterretningsvirksomhet er uakseptabel.

Hovedmålsettingene for trusselaktørenes etterretningsvirksomhet i Norge er å avdekke norske og allierte sikkerhets-, forsvars- og utenrikspolitiske posisjoner, og å sikre tilgang til høyverdig teknologi innen sivil og offentlig sektor. Etterretningsaktivitet mot Norge har også som mål å avdekke sårbarheter og muligheter for bruk av disse i mulige krise og krigssituasjoner. De siste 10-15 årene har vi sett en ny trussel vokse frem – trusselen mot samfunnskritiske IKT-systemer. Trusler vi tidligere så i det fysiske domenet, slik som fremmed etterretningsvirksomhet, subversjon og sabotasje, har nå tatt skrittet inn i det digitale rom. Man finner igjen de samme truslene og sårbarhetene og de samme trusselaktørene. Forskjellen er at de i dag opererer mot oss med et helt annet omfang og hastighet. Det er ikke Etterretningstjenestens oppgave å etablere forsvarsmurene mot de digitale truslene. Tjenestens oppgave er å støtte forsvarstiltakene, gjennom å avdekke hvem som er aktørene, hvilke motiver de har og hvordan og med hvilke våpen de opererer mot oss. Til det kreves en omfattende situasjonsforståelse av aktivitet i det digitale rom som kan true Norge og norske interesser.

7.5.2.3 Påvirkningsoperasjoner ved bruk av «alle statens virkemidler»

Gjennom sammensatte virkemidler ser vi at stater benytter et bredt sett av konvensjonelle og ukonvensjonelle tiltak i det fysiske og digitale domenet, slik som desinformasjon, nettverksangrep, subversjon eller forsøk på å påvirke nasjonale demokratiske prosesser, økonomisk press og spionasje, som del av målrettede kampanjer for å ramme motstanderens interesser og sikre egne målsettinger. Målsettingene med slike angrep varierer; fra å innta territorier uten åpenbar bruk av konvensjonell militærmakt, slik tilfelle var med den russiske annekteringen av Krim i 2014, til å konstruere et påskudd for å bruke konvensjonell militær makt, og til forsøk på å influere en annen stats politiske prosesser for å oppnå det ønskede resultat. Påvirkning av politiske prosesser kan blant annet skje gjennom påvirkning av samfunnsopinionen, forsøk på å skape intern konflikt mellom befolkningsgrupper, og påvirkning av valgoppslutning eller valgresultater. Det kan etter omstendighetene være vanskelig å spore og dokumentere hvem som står bak en slik kampanje eller et angrep. Og selv om attribusjon i enkelte tilfeller kan skje med stor grad av

sannsynlighet, vil vurderinger av mottiltak kunne vanskeliggjøres ved at trusselaktørens intensjoner og handlinger ikke nødvendigvis er åpenbare.

Ved en tilspisset sikkerhetspolitisk situasjon må det forventes at Norge vil bli utsatt for et spekter av virkemidler, inkludert etterretningstjenesters involvering i påvirkningskampanjer og spredning av desinformasjon. Departementet finner det naturlig at det i Etterretningstjenestens oppgaveangivelse fremheves at tjenesten skal bidra med informasjon som kan avdekke og motvirke fremmede påvirkningsoperasjoner.

7.5.2.4 Avdekking, avskrekking og motvirkning

Norske myndigheter og underliggende etater må i fellesskap arbeide for å kunne dekke hele bredden i trusselbildet og avdekke hvorvidt fremmede aktører har intensjoner om, eller har iverksatt tiltak for, å utfordre norske eller alliertes interesser. For å beskytte norske interesser har Norge behov for at Etterretningstjenesten, i samarbeid med andre, identifiserer, kartlegger og vurderer hvorvidt Norge er mål for trusler iverksatt av statlige aktører, samt hvorvidt militære, paramilitære eller sivile virkemidler benyttes i det fysiske og digitale domenet som del av en sammensatt kampanje for å ramme norske interesser.

Avdekking og motvirkning av denne type virksomhet har også en militær side ved seg. Kombinasjonen av regulær og irregulær krigføring har lange tradisjoner i store deler av verden. Det er essensielt at Norge har en effektiv etterretningstjeneste som kan fremskaffe informasjon i en tidlig fase og avdekke hvorvidt Norge er utsatt for et sammensatt angrep der for eksempel fremmede elitetropper under dekke benyttes i kombinasjon med en informasjonskampanje som søker å påvirke det norske folk og norske styresmakters situasjonsforståelse. I en slik situasjon må Etterretningstjenesten også evne å etablere løpende situasjonsforståelse av utviklingen i sjø-, luft- og landdomenet i våre nærområder, samt i det digitale domenet og i romdomenet. Solid situasjonsforståelse og evne til å produsere rettidige og relevante etterretninger vil i en slik situasjon være en forutsetning for et velfungerende forsvar og for at norske myndigheter kan treffe informerte beslutninger for å håndtere krisesituasjoner. En adekvat etterretningsevne vil også ha en avskrekkende effekt.

7.5.2.5 Særlig om digitale trusler

Det digitale domenet blir en stadig viktigere arena for statlig, samfunnsmessig og individuell virksomhet og for ivaretakelse av sikkerhet. Utviklingen er ikke avgrenset til infrastruktur, industrielle prosesser og tjenesteproduksjon, men omfatter også opinionsdannelse og sosial interaksjon. Norge er et av verdens mest digitaliserte land og i økende grad avhengig av nettverksteknologi på alle samfunnsområder. Forsvarets, andre myndigheters og samfunnets avhengighet av moderne informasjons- og kommunikasjonsteknologi har medført nye og økende sårbarheter. Det har de senere årene vært en kraftig eskalering av digitale trusler rettet mot Norge og norske interesser. Aktørene som står bak trusler i det digitale rom spenner fra statlige etterretnings- og sikkerhetstjenester, via tradisjonelle militære motstandere, globale næringsbedrifter, terrorist- og ekstremistgrupper til organiserte hackergrupper.

Det digitale rom benyttes blant annet til spionasje mot norske og alliertes interesser, samt til kommunikasjon mellom terrorgrupperinger. De tre viktigste kategorier av digitale trusler mot norsk samfunns- og statssikkerhet er etterretningsvirksomhet, (forberedelser til) sabotasje og påvirkningsoperasjoner. Angrep i det digitale rom kan utføres av både statlige og ikke-statlige aktører og kan være rettet mot privatpersoner, næringsliv, offentlige instanser og Forsvaret.

Per i dag er det utenlandsk etterretningsvirksomhet utført i statlig regi og rettet mot norske interesser som utgjør den mest alvorlige trusselen i det digitale domenet. Det har i de senere årene vært en kraftig økning i volum og kompleksitet i alvorlige digitale hendelser iverksatt av statlige aktører. Aktiviteten er både teknisk avansert og målrettet mot norske politiske, militære, teknologiske og økonomiske interesser. Fremmed etterretningsvirksomhet kan ha betydelige negative økonomiske, sikkerhetsmessige og samfunnsmessige konsekvenser. De mest avanserte etterretningsoperasjonene kan pågå i flere år uten å bli oppdaget, og skadevare kan være implementert for senere anvendelse. Utvikling av skadevare og leveringsmetoder på den ene siden og mekanismer for deteksjon og beskyttelse på den andre, foregår i form av et kappløp. Utbredelsen av teknologi gjør det mulig for stadig flere stater, grupper og personer å utvikle nye metoder og teknikker. Utviklingen vil bidra til at flere virksomheter og nye typer mål angripes. I fremtiden vil stadig flere fysiske gjenstander og systemer kobles til Internett, og de vil til dels handle autonomt basert på informasjon, sensorer og kunstig intelligens.

Utviklingen har medført at grensen mellom politisk påvirkning og konvensjonell og ukonvensjonell krigføring ikke er så skarp og entydig som tidligere. Det digitale rom er i dag et krigføringsdomene, og informasjonskrigføring og digitale angrep er en integrert del av militære operasjoner. Angrep i det digitale domenet kan ramme nasjonale beslutningsprosesser og utfordre både samfunns- og statssikkerheten. Angrep i det digitale domenet omfattes derfor av NATO-traktatens artikkel 5. De samlede tiltak for etterretning og beskyttelse er til syvende og sist et spørsmål om å hevde digital suverenitet, beskytte statens sikkerhet og samfunnssikkerheten, samt opprettholde demokratisk legitimitet, autonomi og handlefrihet. Norge har også en folkerettslig plikt til å sørge for at digital infrastruktur i Norge ikke blir brukt som fristed og transittland for rettsstridige handlinger mot mål utenfor Norge.

Etterretningstrusselen er vedvarende høy og stadig mer avansert. Norge har hittil vært forskånet for digitale angrep, i betydningen digitale trusler som har materialisert seg i betydelig fysisk skade for personell eller ødeleggelser eller lammelser av kritisk infrastruktur eller viktige samfunnstjenester. Etterretningstjenesten uttaler at den vurderer det som sannsynlig at Norge vil oppleve digitale angrep i årene fremover, enten alene eller som ledd i en større sammenheng. Digital sabotasje kan inngå som et virkemiddel i et overordnet konsept som ellers omfatter desinformasjon, manipulasjon, aggressiv propaganda og stimulans av sosial uro. Forstyrrelser eller ødeleggelse av utvalgte mål med høy økonomisk eller symbolsk verdi er egnet til å demonstrere makt. I en konflikt vil målet være å diskreditere motstanderens myndigheter, forvirre befolkningen og demoralisere militært personell. Hensikten med eventuell sabotasje er ikke ødeleggelsene i seg selv, men å avskrekke og tvinge igjennom en løsning på egne premisser. Digital sabotasje kan også omfatte evne til å forstyrre og undertrykke telekommunikasjon, kringkasting og Internett-medier med formål om å manipulere opinionsdannelse og nasjonale beslutningsprosesser. Degradering og forstyrrelser av infrastruktur og kritiske systemer i regi av stedfortreder-grupper gir mulighet til å fremstå aggressivt samtidig som knytningen til den ansvarlige aktøren kan benektes.

Å forhindre fremmed virksomhet i det digitale rom rettet mot Norge og norske interesser er en vedvarende prioritert oppgave for Etterretningstjenesten. Oppgaven inkluderer å forhindre industrispionasje av særlig alvorlig karakter. Det gjelder åpenbart dersom stater eller statsstøttede aktører står bak, men vil også dekke ikke-statlige aktører dersom

industrispionasjen har et betydelig omfang eller på annen måte må anses som fremmed etterretningsvirksomhet eller en trussel mot Norges økonomiske handlefrihet. Det går imidlertid en nedre grense for hva som naturlig vil tilligge Etterretningstjenesten å innhente og analysere informasjon om. Industrispionasje mellom kommersielle aktører som primært er å anse som kriminalitet som det tilligger politiet å forebygge, motvirke og etterforske skal ikke anses å falle inn under § 3-1 i lovutkastet.

Det er av avgjørende betydning for Etterretningstjenestens evne til å løse de høyest prioriterte oppdragene at den har tilgang og evne til å operere i det digitale domenet. Dette gjelder i fred, krise og væpnet konflikt. For å opprettholde evne til situasjonsforståelse og strategisk varsling må Etterretningstjenesten evne å følge trusselutviklingen og trusselaktørenes samlede aktivitet i det fysiske og digitale domenet. Norge har i dag få muligheter til å avdekke og motvirke alvorlige cyberhendelser. Dette er nærmere omtalt og begrunnet i kapittel 11.

7.5.2.6 Departementets vurdering

Drøftelsen over understreker behovet for å innhente informasjon om utøvelsen av fremmed etterretningsvirksomhet og fremmede sabotasje- og påvirkningsoperasjoner mot Norge og norske interesser. Departementet mener derfor dette bør fremgå eksplisitt av Etterretningstjenestens lovpålagte oppgaver, jf. lovutkastet § 3-1 første ledd bokstav d og e.

7.5.3 Grenseoverskridende terrorisme (lovutkastet § 3-1 bokstav f)

7.5.3.1 Trusselen fra internasjonal terrorisme

Terrorismens mest effektive virkemiddel er å skape frykt gjennom uforutsette anslag. Terrorhandlinger vil ikke nødvendigvis forårsake krigslignende tilstander. Terrorisme, ekstremisme og manglende statlig stabilitet ulike steder i verden utgjør likevel en alvorlig og direkte trussel mot Norge og norske interesser i utlandet. En rekke gjennomførte og avvergede angrep de siste årene viser hvor alvorlig, overhengende og kompleks terrortrusselen er.

At de fleste vestlige og mange andre land, inkludert Norge, anser trusselen fra internasjonal terrorisme som overhengende, tydeliggjøres ved at man har valgt å ta i bruk militær makt for å motvirke trusselen. Selv om risikoen for å bli rammet av en terrorhandling er meget liten for den enkelte borger, har slike handlinger politiske og samfunnsmessige konsekvenser langt utover personer og materiell som direkte blir rammet. Det dreier seg om angrep på verdier, trygghet og strukturer i samfunnet, som har implikasjoner ut over det kriminelle aspektet ved handlingene og som endog medfører at stater er villig til å gå til krig for å få bukt med handlingene og gruppene som står bak.

Det kan skilles mellom ulike kategorier av trusler; *styrte trusler*, hvor planlegging og gjennomføring styres sentralt i en terrororganisasjon, *oppmuntrede trusler,* hvor terrororganisasjonen gir generelle ordre og anmodninger, men hvor detaljplanlegging og gjennomføring overlates til utførende personer, og *inspirerte trusler*, hvor terrororganisasjonen ikke har medvirket annet enn indirekte gjennom propaganda og liknende, selv om utførende person(er) kan ha hatt kontakt med organisasjonen eller støttespillere til organisasjonen på nett eller på annet vis.

Terrororganisasjoner kan også potensielt utgjøre en direkte fare for statssikkerheten. Det er avdekket at terrororganisasjoner, blant dem Den islamske staten i Irak og Levanten (ISIL) og al Qaida, arbeider aktivt for å tilegne seg masseødeleggelsesvåpen. Bruk av kjemisk,

biologisk eller radioaktivt materiale vil kunne føre til omfattende skader og lidelse, og dessuten skape sterk frykt i befolkningen. Når slike våpen dessuten blir enklere å fremstille eller anskaffe, må man være forberedt på at også terrororganisasjoner kan tilegne seg og benytte dem.

7.5.3.2 Situasjonen i dag

Svake stater og manglende statlig stabilitet har medført at regjeringsfiendtlige grupper og militante islamistiske grupper har økt sin innflytelse i flere regioner i Midtøsten, Nord- og Øst-Afrika. Dette er en utfordring for statene i regionen og for vestlige interesser i flere av områdene. Økt kontakt og kapasitetsoverføring mellom militante islamister på tvers av landegrensene og til internasjonale nettverk har ikke bare regionale konsekvenser, men øker også terrortrusselen mot Vesten signifikant. Det er per i dag terrororganisasjonene ISIL og al-Qaida, samt deres støttespillere, som representerer den største trusselen. Disse aktørenes handlinger har resultert i enorme humanitære lidelser, og representerer en alvorlig og overhengende trussel for regional og internasjonal sikkerhet. FNs sikkerhetsråd har i flere resolusjoner slått dette fast. Som et resultat av massivt militært press har ISIL tapt territorium, inntekter og personell. Dette har redusert evnen til å finansiere angrep, trene og instruere angripere og til å reise til Europa. ISILs kapasitet til å gjennomføre godt planlagte og sentralstyrte angrep er når dette skrives dermed redusert. Svekkelsen av ISIL reduserer imidlertid ikke terrortrusselen mot Vesten og vestlige interesser på kort sikt. Flertallet av forsøk på og gjennomføring av direkte angrep i Europa har vært utført at støttespillere i Europa, enten på bakgrunn av direkte oppfordringer eller generell propaganda. ISILs evne til å bruke sosiale medier og propaganda til å delegere og inspirere enkeltpersoner og grupper til å gjennomføre terroranslag er mer eller mindre intakt.

ISIL og andre militante islamistgrupper ser per nå Norge og norske interesser i utlandet som et legitimt, men ikke prioritert angrepsmål. Trusselbildet kan raskt endres dersom Norge innlemmes i konkrete erklæringer eller oppfordringer til angrep. Det generelle trusselbildet, kombinert med at angrepsmål velges opportunistisk ut fra symboleffekt og sårbarhet, medfører vedvarende risiko for angrep mot Norge og norske interesser i utlandet.

22. juli 2011 er et eksempel på at det også eksisterer en reell trussel fra høyreekstreme, islamfiendtlige og anti-statlige miljøer. Slike miljøer finnes både i Norge og resten av verden. Høyreekstremister, islamfiendtlige grupperinger og anti-statlig ekstremisme er på fremmarsj i Europa, Russland og USA, og har økende aktivitet og voldsutøvelse. Disse grupperingene har internasjonale forgreninger og samarbeider politisk og ideologisk. Reell utøvelse av vold og terror fra disse grupperingene har så langt vært gjennomført av nasjonale aktører innenfor nasjonale grenser. Dette kan imidlertid raskt endre seg.

Trusselbildet knyttet til internasjonal terrorisme er i stadig endring, og nye grupper og fenomener vokser frem. Grenseoverskridende terrorisme vil forbli en alvorlig og dynamisk trussel mot nasjonal og internasjonal fred og sikkerhet i overskuelig fremtid. Så lenge de grunnleggende forutsetningene i form av ideologiske og religiøse motsetninger, svake stater, interne voldelige konflikter og sosial ulikhet er til stede, vil det finnes vedvarende motivasjon for å utøve terror.

7.5.3.3 Departementets vurdering

Departementet anser at internasjonal terrorisme og trusselen mot Norge og norske interesser i utlandet fra terrororganisasjoner og tilhørende støttespillere vil være et høyt

prioritert saksfelt for Etterretningstjenesten i årene som kommer. Departementet mener dette bør fremgå direkte av lovteksten i utkast til § 3-1 første ledd bokstav f.

Trusselen består av et komplekst, transnasjonalt aktørbilde i stadig endring. Avdekking og motvirkning krever en etterretningstjeneste som evner å gjennomføre raske endringer i fokus og kontinuerlig utvikling av innsamling som gir mulighet til å avdekke aktører og utvikling i *modus operandi*. Terrorisme er videre et grenseoverskridende fenomen som opphever ethvert forsøk på et klart skille mellom eksterne og interne trusler. Håndtering av utviklingen forutsetter nært internasjonalt kontraterrorarbeid, utstrakt informasjonsdeling, og forutsetter et tett integrert samarbeid mellom de nasjonale etterretnings- og sikkerhetstjenestene for å skape et helhetlig bilde. Informasjonen Etterretningstjenesten fremskaffer på dette feltet har relevans både for den innenlandske etterretnings- og sikkerhetstjenesten PST og den forebyggende sikkerhetstjeneste innenfor deres respektive ansvarsområder.

Vestlige etterretnings- og sikkerhetstjenester har avverget en rekke planlagte terrorhandlinger. Samtidig viser utviklingen at det ikke vil være mulig å forhindre ethvert angrep. Håndtering av terrorangrep er særdeles krevende, og Etterretningstjenesten vil spille en sentral rolle til støtte for en nasjonal krisehåndtering som følge av et eventuelt terroranslag i Norge. Ved trusler om terror eller ved reelle terroranslag vil det være kritisk viktig at Etterretningstjenesten evner å avdekke eventuelle internasjonale forgreininger eller kommandolinjer.

Etterretningstjenesten vil også ha en sentral rolle å spille ved trusler og anslag som rammer norske interesser i utlandet, slik tilfellet var ved det omfattende anslaget mot gasskraftverket ved *In Amenas* i Algerie i januar 2013. Etterretningstjenesten vil dessuten være en sentral støtte for norske myndigheter i saker der norske borgere blir kidnappet i utlandet. Departementet vurderer at Etterretningstjenesten innenfor realistiske rammer bør ha egenevne til å gi bidrag ved terroranslag mot norske interesser i utlandet, og samtidig ha et bredt nettverk av etablerte partnere for å kunne kompensere for egne begrensninger og raskt fremskaffe informasjon i oppdukkende kriser.

7.5.4 Spredning av masseødeleggelsesvåpen og internasjonal våpenhandel mv. (lovutkastet § 3-1 bokstavene g - i)

7.5.4.1 Generelt

Spredning av masseødeleggelsesvåpen (MØV) og utstyr og materiale for fremstilling av slike våpen, samt internasjonal våpenhandel, er alvorlige sikkerhetstrusler som kan fortsette å øke dersom den internasjonale rettsorden ytterligere svekkes. Departementet vurderer at Etterretningstjenesten fortsatt bør ha som oppgave å innhente informasjon om spredning av MØV. I tillegg foreslår departementet at Etterretningstjenesten skal innhente informasjon om internasjonal våpenhandel som kan utgjøre en alvorlig sikkerhetstrussel.

7.5.4.2 Masseødeleggelsesvåpen

Kjernevåpen er fortsatt en vesentlig del av stormaktspolitikken, og står i en klasse for seg som følge av det enorme skadepotensialet. Det er ikke mulig å skaffe seg en total beskyttelse mot kjernevåpen, ei heller ved et territorielt missilforsvar i Europa. Det kan ikke utelukkes at kjernevåpen kan bli brukt dersom statlige myndigheter i en ustabil kjernevåpenstat mister faktisk kontroll med våpen og produksjonsanlegg. Det kan også være en bekymring for at isolerte statsledere i totalitære stater kan tenkes å opptre irrasjonelt. De etablerte kjernevåpenmaktene har til en viss grad dempet sin kjernefysiske rivalisering, og er

enige om å begrense spredning til nye stater. Samtidig ser vi at flere kjernevåpenstater fortsetter videreutvikling av egen kapasitet. Det er i skrivende stund knyttet ny usikkerhet til atomavtalen med Iran. Det kan ikke utelukkes at landet vil ta opp igjen sine ambisjoner om å bli en kjernevåpenstat, i tillegg til å videreføre en omfattende satsing på å gi egne missiler bedre kapasitet til å bære ikke-konvensjonelle våpen. Kina, India og Pakistan moderniserer og videreutvikler kjernevåpen og leveringsmiddel. Det er en vedvarende fare for at regional utvikling i Midtøsten, Sør- eller Øst-Asia vil kunne få en kjernefysisk dimensjon. Til tross for sterkt og økende press internasjonalt er det usikkerhet knyttet til Nord-Koreas ambisiøse kjernevåpenprogram. Et Nord-Korea med kjernevåpen som faktisk kan true mål i Øst-Asia og vestover vil forsterke de regionale sikkerhetspolitiske spenningene og være en trussel mot internasjonal sikkerhet og stabilitet.

Spredning av MØV-relatert teknologi (rakett- og våpenteknologi) kan ha konsekvenser for hvorvidt nye kjernevåpenstater direkte vil kunne true Norge eller våre allierte, og er dermed en sentral utfordring for norske beslutningstagere, norsk sikkerhet og beredskap. Det forekommer en rask teknologi- og kompetanseutvikling innen en rekke MØV-relaterte fagområder. Denne utviklingen, kombinert med høy og økende internasjonal samhandel, multinasjonale selskaper, komplekse selskapsstrukturer og bruk av underleverandører, øker tilgjengeligheten av avanserte teknologier, utstyr og materialer og er dermed en betydelig og alvorlig sikkerhetsutfordring for det internasjonale samfunn, Norge og norske allierte.

Andre typer masseødeleggelsesvåpen finnes i ulikt omfang i flere land, til tross for forbudet mot slike våpen i internasjonale konvensjoner. I de senere år har kjemiske våpen blitt brukt av både statlige og ikke-statlige aktører, blant annet i Syria og Irak. Forskning og utvikling av nye typer kjemiske stridsmidler som kan omgå statlige kontrollregimer, kombinert med ikke-statlige aktørers økende ekspertise, gjør at kjemiske stridsmidler vil fortsette å utgjøre en reell trussel i overskuelig fremtid.

Utfordringer knyttet til spredning av MØV, med tilhørende teknologi, utstyr og kompetanse, vil vedvare i overskuelig fremtid. Hensynet til nasjonale interesser, beredskap, evne til krisehåndtering, behov for politikkutforming på nedrustnings- og ikke-spredningsområdet, samt internasjonale forpliktelser, forutsetter at Norge har en etterretningstjeneste med relevant informasjonstilgang og tilstrekkelig kompetanse og evne til å produsere tidsriktige etterretninger på dette området.

7.5.4.3 Internasjonal våpenhandel

Ikke bare atomvåpen, men også internasjonal våpenhandel kan utgjøre en alvorlig sikkerhetstrussel, spesielt der det innføres nye kapasiteter som kan påvirke maktbalansen i en region. I tillegg kan våpensystemer utgjøre en direkte militær trussel mot Norge og norske interesser. Våpenhandel mellom stater gir også en indikasjon på oppbygging av kapasiteter og allianser mellom parter. Våpenhandel kan videre ha en sammenheng med internasjonal terrorisme gjennom terrorfinansiering og på annen måte.

7.5.4.4 Sanksjonerte, listeførte eller sensitive varer og tjenester

Utkast til § 3-1 første ledd bokstavene g og h vil dekke en del av Etterretningstjenestens nåværende virksomhet for å avdekke og motvirke eksport av sanksjonerte, listeførte eller sensitive varer og tjenester. For å unngå at deler av denne virksomheten vil falle utenfor tjenestens oppgaver når oppgavelisten gjøres uttømmende, hvilket kan være tilfelle dersom varen eller tjenesten ikke har sammenheng med masseødeleggelsesvåpen eller internasjonal våpenhandel, foreslås at loven i utkast til § 3-1 første ledd bokstav i uttrykkelig

fastsetter at Etterretningstjenesten skal innhente informasjon om utenlandske forhold som kan bidra til å avdekke og motvirke eksport av sanksjonerte, listeførte eller sensitive varer og tjenester. Oppgavene vil dekke eksport av varer og tjenester i strid med norsk lov, jf. eksportkontrolloven, sanksjonsforskrifter eller bestemmelser i eller i medhold av annen norsk lovgivning.

7.5.4.5 Departementets vurdering

Departementet vurderer at Etterretningstjenesten fortsatt skal ha som oppgave å innhente informasjon om spredning av masseødeleggelsesvåpen og utstyr og materiale for fremstilling av slike våpen, og foreslår at dette presiseres i lovforslaget § 3-1 første ledd bokstav g.

Departementet mener også Etterretningstjenesten bør kunne innhente og analysere informasjon som kan ha relevans for å avdekke og motvirke internasjonal våpenhandel som kan utgjøre en alvorlig sikkerhetstrussel, og at dette fremgår av lovforslaget § 3-1 første ledd bokstav h. Med *alvorlig sikkerhetstrussel* menes at våpenhandelen må ha direkte eller indirekte relevans for norsk stats- eller samfunnssikkerhet, og terskelen ligger dermed forholdsvis høyt. Det vil ikke tilligge Etterretningstjenesten å innhente informasjon om enhver form for internasjonal våpenhandel. Eksempelvis vil ren kriminell grenseoverskridende omsetning av håndvåpen etter forslaget ligge utenfor tjenestens oppgavesett.

Departementet finner grunn til å presisere særskilt at Etterretningstjenesten skal innhente og analysere informasjon knyttet til eksport av sanksjonerte, listeførte eller sensitive varer og tjenester. Dette er en videreføring av dagens praksis.

7.5.5 Forslag til lovregulering

Departementet foreslår at hjemmel for å innhente informasjon om utenlandske trusler formuleres slik i lovens § 3-1:

§ 3-1 *Informasjonsinnhenting om utenlandske trusler*

Etterretningstjenesten skal innhente og analysere informasjon om utenlandske militære og sivile forhold som kan bidra til å avdekke og motvirke

a. trusler mot Norges selvstendighet og sikkerhet, territorielle integritet og politiske og økonomiske handlefrihet,
b. alvorlige trusler mot samfunnssikkerheten i Norge,
c. alvorlige trusler mot norske interesser i utlandet,
d. fremmed etterretningsvirksomhet,
e. fremmede sabotasje- og påvirkningsoperasjoner,
f. grenseoverskridende terrorisme,
g. spredning av masseødeleggelsesvåpen og utstyr og materiale for fremstilling av slike våpen,
h. internasjonal våpenhandel som kan utgjøre en alvorlig sikkerhetstrussel, og
i. eksport av sanksjonerte, listeførte eller sensitive varer og tjenester.

7.6 Nærmere om informasjonsinnhenting om andre utenlandske militære og sivile forhold (lovutkastet § 3-2)

7.6.1 Utenriks-, sikkerhets- og forsvarspolitiske interesser

7.6.1.1 Etterretningsbehovet

Norges utenriks-, sikkerhets- og forsvarspolitiske interesser har et bredt geografisk nedslagsfelt. Som en følge av dette etterspør norske myndigheter i økende grad etterretningsvurderinger om omverdenen basert på informasjon som ikke er allment tilgjengelig. Norge fører en aktiv utenrikspolitikk, norske interesser er spredd over mange land, og norsk sikkerhet og nasjonale interesser påvirkes i stadig økende grad av begivenheter andre steder i verden. Globalisering og digitalisering medfører at koblingen mellom lokale hendelser og internasjonal sikkerhet, og mellom taktisk og strategisk nivå, blir stadig tettere. Som følge av dette har norske myndigheter i dag stor spennvidde i informasjons- og etterretningsbehov knyttet til globale og regionale prosesser en rekke steder i verden. Informasjonsbehovene kan være av både militær og sivil karakter. Interessene kan også være knyttet til norske politiske interesser som følge av Norges virksomhet i utlandet eller andre forhold som gjør Norge mer synlig globalt. Norsk næringslivs rolle innenfor blant annet sjøfart, telekommunikasjon, romvirksomhet, fiskeri og energi har medført at norske interesser ikke bare favner bredt og globalt, men også innen sektorer som av mange land defineres som sensitive og strategiske. Norge er gjennom Statens pensjonsfond utland blitt en betydelig aktør på det globale finansmarkedet, noe som også retter oppmerksomhet mot Norge. Norges samlede etterretningsbehov er som følge av dette tettere knyttet til globale og regionale prosesser enn vår størrelse og beliggenhet skulle tilsi. I tillegg kommer det forhold at Norge tradisjonelt har ført en mer ekspansiv utenrikspolitikk enn småstater flest, noe som bidrar til å forsterke spennvidden i etterretningsbehovene.

Kunnskap om fenomener og forhold i ulike deler av verden har i dag relevans for de fleste samfunnsområder, enten det dreier seg om støtte til Utenriksdepartementets tilrettelegging for og deltakelse i freds- og forsoningsprosesser, globale utviklingstrekk av betydning for politikkutforming relatert til næringsutvikling og infrastrukturutbygging, migrasjonsspørsmål, områdevurderinger knyttet til norske myndighetspersoners reiser i utlandet, eller konflikter og utviklingstrekk i andre verdensdeler som på sikt kan influere på norsk utenriks-, forsvars- og sikkerhetspolitikk eller skape separatist- eller opprørsbevegelser av betydning for norske interesser i utlandet.

Norges behov for etterretningsinformasjon strekker seg i dag altså langt bortenfor nordområdene. Norges viktigste strategiske ansvarsområde er likevel fortsatt i nord. Norges interesser må sikres og beskyttes. Asymmetrien i forholdet mellom Norge og Russland blir tydeligere, og den russiske styrkeoppbyggingen skaper utfordringer. Utviklingen er blitt både kompleks og uoversiktlig. Mange av utfordringene kan utspille seg i gråsonen mellom fred og væpnet konflikt, og varslingstiden vil mest sannsynlig være særdeles kort.

Forhold og utviklingstrekk i andre deler av verden kan ha stor etterretningsmessig verdi selv om disse ikke direkte kan relateres til konkrete trusler. En av Etterretningstjenestens sentrale oppgaver foreslås derfor fortsatt å være å innhente og analysere informasjon om utenlandske militære og sivile forhold som kan bidra til ivaretakelsen av prioriterte utenriks-, forsvars- eller sikkerhetspolitiske interesser. Disse prioriterte interessene kan spenne over et

bredt og mangeartet felt. Informasjonsinnhenting knyttet til disse forholdene innebærer intet nytt i forhold til gjeldende oppgavesett etter dagens lov § 3 første ledd.

7.6.1.2 Skjæringspunkter

Utkast til § 3-2 første ledd bokstav a vil ha skjæringspunkter mot utkast til § 3-1 ved at interessene kan være knyttet til forhold som kan eskalere til trusler.

Den internasjonale rettsorden og mellomstatlige institusjoner er generelt under økende press. Enkelte mektige stater og ikke-statlige aktører ser bort fra internasjonale normer de anser for å være i motsetning til deres interesser. Russlands annektering av Krim, det syriske regimets bruk av kjemiske våpen og Nord-Koreas kjernefysiske testing er eksempler på dette. Dette har alvorlige implikasjoner også for norsk sikkerhet og norske interesser. Nedgangen i væpnede konflikter som preget årene etter den kalde krigen har nå snudd, og verden er nå i økende grad preget av væpnede konflikter. Afghanistan, Kongo, Irak, Nigeria, Pakistan, Sør-Sudan, Libya, Jemen og Syria er noen av de viktigste konfliktområdene i dag. Samtidig har det vært en sterk økning i antall drepte i krig, hovedsakelig som følge av krigen i Syria. Til tross for flere tiår med relativ fred og stabilitet i Europa samt i Asia- og Stillehavsregionen kan en heller ikke her utelukke væpnede konflikter i årene som kommer.

Skillet mellom hva som er et regionalt utviklingstrekk etter lovutkastet § 3-2 første ledd bokstav a, og hva som vil være å anse som en trussel etter lovutkastet § 3-1, vil derfor ikke alltid være like enkelt å trekke.

7.6.1.3 Departementets vurdering

Departementet vurderer at Etterretningstjenesten fortsatt bør ha som oppgave å bidra til utformingen av norsk utenriks-, forsvars- og sikkerhetspolitikk både på kort og lang sikt. Som anført i forarbeidende til någjeldende lov, kan det i mange tilfeller være vanskelig å skille klart mellom hva som er utenrikspolitikk, forsvarspolitikk og sikkerhetspolitikk.[164] Som den gang, ser departementet heller ikke nå et behov for å sondre skarpt mellom disse begrepene i loven.

Departementet foreslår at det tas inn som et vilkår i loven at innhentingen om andre utenlandske forhold enn trusler skal begrenses til «prioriterte» norske utenriks-, forsvars- eller sikkerhetspolitiske interesser. Styring av Etterretningstjenesten og prioriteringen av tjenestens oppgaver er nærmere beskrevet i kapittel 6. I denne sammenheng er det mest sentralt at innhentingen skal begrenses til de utenriks-, forsvars- og sikkerhetspolitiske interesser som til enhver tid er prioritert av oppdragsgiveren, nemlig norske myndigheter.

Ordlyden er samtidig ikke til hinder for at Etterretningstjenesten selv, med bakgrunn i sin innsikt i tematikkene, selv kan foreslå at bestemte temaer prioriteres innenfor nevnte saksfelt. Det vil imidlertid være opp til myndighetene å foreta den faktiske prioriteringen. Hvor mange stater/regioner eller geografiuavhengige temaer tjenesten skal innhente informasjon om, det vil si hvor mange prioriterte områder norske myndigheter kan fokusere på til enhver tid, vil etter departementets skjønn begrense seg selv i henhold til de økonomiske budsjettrammer tjenesten er satt til å operere innenfor, samt hvilket ambisjonsnivå som er ønskelig for de enkelte prioriterte områdene. Departementet mener derfor at begrepet *prioriterte* utenriks-, forsvars- eller sikkerhetspolitiske interesser vil fungere som et tilstrekkelig kvalifiserende vilkår.

[164] Se Ot. prp. nr. 50 (1996-97) s. 15

7.6.2 Beredskap, krisehåndtering og operasjoner

7.6.2.1 Generelt

Under informasjonsinnhenting om andre utenlandske forhold faller også oppgaver relatert til beredskap, krisehåndtering nasjonalt og internasjonalt, og støtte til militære operasjoner nasjonalt og internasjonalt. Disse fremkommer i lovutkastet § 3-2 første ledd punkt b - d.

Forsvaret skal kunne håndtere sikkerhetspolitiske kriser og anslag av et visst omfang. Episoder og kriser som håndteres nasjonalt skal kunne bringes under kontroll, eventuelt parallelt med at norske myndigheter involverer alliansen. Etterretningstjenesten må innrettes på en slik måte at den kan understøtte hele spekteret av Forsvarets oppgaver.

Norge har lang tradisjon som støttespiller for FN- og NATO- operasjoner. Norske bidrag til operasjonene i Afghanistan har vært det største militære norske utenlandsoppdraget den senere tid. Etterretningstjenestens bidrag var viktig for at Norge kunne nå særlig én av sine målsettinger med engasjementet i Afghanistan; nemlig å bidra til å styrke forholdet til USA, andre allierte og NATO, noe som er og var politisk viktig. Innenfor rammen av operasjon Enduring Freedom (OEF) ga også norsk etterretningspersonell direkte støtte i terrorbekjempelse, og var en del av Norges bestrebelser på å bidra til statsbyggingen i Kabul.

Det er en grunnleggende forutsetning at norske styrker har støtte fra Etterretningstjenesten ved deltagelse i nasjonale og internasjonale operasjoner. Militære operasjoner på alle nivå, fra det strategiske til det taktiske, er etterretningsdrevne og forutsetter et oppdatert etterretningsbilde og relevante etterretningsvurderinger om de faktiske forhold. Etterretningstjenestens direkte støtte til Forsvarets militære operasjoner og oppfyllelsen av deres mandat gis blant annet gjennom produksjon av grunnleggende etterretninger, ved løpende oppdatering av etterretningsbildet på strategisk og operasjonelt nivå og ved å støtte militære sjefer på taktisk nivå med konkrete etterretningskapasiteter og produkter. Etterretningstjenestens innsats i internasjonale operasjoner utgjør en vesentlig del av den støtten Norge yter allierte i disse operasjonene, og er et viktig bidrag til sikkerhet og beskyttelse av norsk og alliert personell i internasjonale operasjoner. Norges deltagelse i internasjonale operasjoner forutsetter at Norge har en etterretningstjeneste som innehar evnen til å støtte de militære styrkene, og er i stand til å utvikle seg i takt med tiden med henblikk på kapasiteter og metoder som er nødvendig for å opprettholde en slik støtte.

Etterretningstjenesten er forsvarssjefens etterretningsapparat til støtte for Forsvarets virksomhet både hjemme og ute. For å optimalisere bruken av militære kapasiteter, fly, fartøy og soldater, må man forstå det bildet og den situasjonen styrkene skal virke i. Militære operasjoner uten avansert etterretningsstøtte på alle nivåer er ikke lenger tenkelig. Derfor har Etterretningstjenesten i dag ikke bare et ansvar for sin egen aktivitet til støtte for Forsvaret, men også for den samlede etterretningsvirksomhet som drives i hele Forsvaret, ned i og på tvers av forsvarsgrenene.

7.6.2.2 Departementets vurdering

Departementet vurderer at Etterretningstjenesten fortsatt bør støtte Forsvaret med etterretninger av relevans for planlegging og gjennomføring av nasjonale eller internasjonale militære operasjoner.

Etterretningstjenesten bør også fortsatt ha som oppgave å kunne gi den informasjon som skal til for at landets beredskapsnivå til enhver tid kan tilpasses trussel- og risikobildet, slik at

riktige beslutninger kan treffes i tide på bakgrunn av et adekvat informasjonsgrunnlag. Dette inkluderer informasjon som er av betydning for beredskapsplanleggingen innenfor den sivile del av totalforsvaret. Nasjonal beredskapsplanlegging omfatter informasjon av relevans for å fastsette hensiktsmessige systemer for sentral krisehåndtering og beredskap – herunder Styrkeoppbyggingssystemet (SOS) og Nasjonalt beredskapssystem (NBS) – og utforming av nasjonalt og alliert operativt planverk på ulike nivåer.

Rettidige etterretninger er en viktig forutsetning for korrekt episode- og hendelseshåndtering. Informasjonsinnhenting for dette formål foreslås videreført som en sentral oppgave for Etterretningstjenesten. Oppgaven inkluderer informasjon som kan være av relevans for lavskala krisehåndtering, for eksempel grensekrenkelser og lignende hendelser som krever operativ og diplomatisk håndtering. For å kunne detektere potensielt eskalerende aktivitet kreves innhenting av grunnleggende etterretninger for å bygge et normalbilde. Dette innebærer blant annet å rutinemessig følge militær og sivil aktivitet i norsk interesseområde.

Selv om Etterretningstjenesten ikke skal utføre oppgaver med politiformål, er særlig PSTs oppgavesett av en slik karakter at informasjon som Etterretningstjenesten innhenter om utenlandske forhold innenfor rammen av tjenestens oppgaver, etter omstendighetene også kan være av stor betydning for PSTs lovpålagte oppdrag. Informasjonen vil også kunne ha relevans for andre aktører i justissektoren, særlig dersom informasjon peker mot forhold av kriminell karakter rettet mot norsk territorium eller norske interesser i utlandet.

7.6.3 Forslag til lovregulering

Departementet foreslår at informasjonsinnhenting om andre utenlandske forhold formuleres slik i utkast til § 3-2:

§ 3-2 *Informasjonsinnhenting om andre utenlandske forhold*

Etterretningstjenesten skal innhente og analysere informasjon om utenlandske militære og sivile forhold som kan bidra til

a. ivaretakelse av prioriterte utenriks-, forsvars- eller sikkerhetspolitiske interesser knyttet til forhold og utviklingstrekk i andre stater og regioner,
b. nasjonal beredskapsplanlegging,
c. episode- og krisehåndtering, og
d. planlegging og gjennomføring av nasjonale eller internasjonale militære operasjoner.

7.7 Okkupasjonsberedskap (lovutkastet § 3-3)

Okkupasjonsberedskap, med historisk referanse også tidvis benevnt *Stay Behind*, er i dagens lov angitt som en egen oppgave for Etterretningstjenesten. Departementet legger opp til en videreføring av denne oppgaven for Etterretningstjenesten, og foreslår å lovfeste oppgaven med i essens samme ordlyd som i gjeldende lov. Det foreslås også videreført en egen bestemmelse om at departementet skal holdes orientert på dette området. Sistnevnte fremgår i dag av E-instruksen § 13 bokstav b.

Etter direktiv fra forsvarsministeren har Etterretningstjenesten planlagt og øvd på dette oppdraget siden 1948. I fredstid innebærer virksomheten ingen fordekt innhenting av informasjon for etterretningsformål. Okkupasjonsberedskapen skal i fredstid drive styrkeproduksjon i form av rekruttering av beredskapspersonell, utarbeidelse og vedlikehold av nødvendig og relevant beredskapsplanverk, og gjennomføring av trening og øving. Det ligger i dagen at ytterligere informasjon om okkupasjonsberedskapens organisasjon, ledelse,

aktivitet og forberedelser er å anse som særlig sensitiv informasjon som krever ekstrem beskyttelse og kompartmentering, også internt i Etterretningstjenesten.

Departementet foreslår at innhentingshjemmel knyttet til ivaretakelsen av okkupasjonsberedskapen formuleres slik i lovutkastet § 3-3:

§ 3-3 *Okkupasjonsberedskap*

Etterretningstjenesten skal ivareta nasjonal evne til å innhente og formidle etterretninger til norske myndigheter fra et helt eller delvis okkupert Norge.

Departementet skal holdes generelt orientert om organisering og planlegging av okkupasjonsberedskapen.

7.8 Internasjonalt etterretningssamarbeid (lovutkastet § 3-4)

Grenseoverskridende trusler og andre sammenfallende interesser medfører behov for å dele informasjon og samarbeide over landegrensene. Norsk etterretning har alltid samarbeidet nært med viktige allierte, og oppbyggingen av Etterretningstjenesten under den kalde krigen hadde ikke vært mulig uten amerikansk støtte. Spesielt samarbeidet med USA har vært og er fortsatt avgjørende for Norges evne til å drive etterretning effektivt i våre nærområder. I dag samarbeider Etterretningstjenesten med en rekke partnere over hele verden. Etterretningstjenesten er ansvarlig for norsk samarbeid utad i etterretningsspørsmål, både bilateralt og i NATO og i annet multilateralt samarbeid.

En effektiv norsk etterretningstjeneste som evner å ha etterretningsmessig situasjonsforståelse i våre nærområder tjener både norske og allierte interesser, og bidrar til at andre land ikke dominerer våre nærområder med etterretningsmessig tilstedeværelse og aktivitet. Norsk kontroll med etterretningsvirksomhet i våre nærområder kan bidra til lavere spenning og derigjennom å minske risiko for utilsiktede hendelser og konflikter.

Etablering og opprettholdelse av etterretningssamarbeid ble i gjeldende lov understreket som en hovedoppgave for Etterretningstjenesten. I forarbeidene til nåværende lov, forutsettes det også at etterretningssamarbeid kan være et selvstendig grunnlag for informasjonsinnhenting:

> «Etablering og opprettholdelse av etterretningssamarbeid med andre land [...] er en av tjenestens hovedoppgaver. Det ligger også i denne bestemmelsen at Etterretningstjenesten kan innhente informasjon som er av betydning for samarbeidende lands tjeneste, selv om forholdene ikke er direkte relatert til Norges selvstendighet, sikkerhet eller viktige nasjonale interesser. Indirekte vil slik informasjonsinnhenting likevel ha en slik relasjon, fordi samarbeidet medfører at norsk etterretningstjeneste får tilsvarende opplysninger fra andre land som vil bidra til å oppfylle lovens formål [...].»[165]

Departementet tar sikte på å videreføre denne rettstilstanden, og foreslår en egen lovbestemmelse i oppgavekapitlet om internasjonalt etterretningssamarbeid. Det foreslås presisert i lovbestemmelsen at dette kan gjelde både bilateralt og multilateralt samarbeid. For å sikre at det ikke unødvendig innhentes informasjon etter denne bestemmelsen, foreslås presisert uttrykkelig at innhenting kun kan skje når det er i norsk interesse. For øvrig må denne oppgavebestemmelsen og informasjonsinnhentingshjemmelen sees i sammenheng med vilkårene for å dele opplysninger med andre lands samarbeidende tjenester. Dette er behandlet i høringsnotatet kapittel 13, hvor det også redegjøres for

[165] Se Ot prp. nr. 50 (1996-97) s. 15

prinsippet om, og reguleringen av, at det ikke er anledning til å omgå hverandres regelverk ved at stater innhenter informasjon for hverandre.

Departementet foreslår følgende regulering:

§ 3-4 *Internasjonalt etterretningssamarbeid*

Når det er i norsk interesse kan Etterretningstjenesten innhente og analysere informasjon om utenlandske trusler og andre forhold som nevnt i kapittelet her som antas å være av vesentlig betydning i bi- eller multilateralt etterretningssamarbeid som Etterretningstjenesten deltar i.

7.9 Nærmere om evneinformasjon

Informasjonsinnhenting som utgjør en nødvendig forutsetning for i det hele tatt å kunne gjennomføre etterretningsinnhenting så målrettet og risikofritt som mulig, har etter gjeldende rett vært antatt som en implisitt del av informasjonsinnhentingsbegrepet. Man må treffe en rekke faktiske tiltak, og innhente informasjon forut for de faktiske tiltakene, for å kunne komme i posisjon til å få tilgang til informasjon av etterretningsverdi. Etterretningstjenesten har for eksempel behov for å kunne innhente informasjon, også fordekt, om kriminalitetsbildet i et område hvor tjenestens personell skal gjennomføre operasjoner, for å kunne ivareta sikkerheten til tjenestens personell og aktivitet. Slik innhenting relaterer seg kun *indirekte* til det egentlige målet for informasjonsinnhentingen, men er nødvendig for at tjenesten skal kunne evne å innhente informasjon på en trygg, målrettet og klandestin måte. Et annet eksempel kan være å innhente informasjon om hvorledes et informasjonssystem er bygget opp eller om signalmiljøet i et område, for å forstå hvordan man kan tilegne seg tilstrekkelig aksess til den relevante informasjonen. Det kan videre dreie seg om å innhente informasjon om hvilke personer i en organisasjon eller på et sted som tjenesten *ikke* skal innhente informasjon om, slik at innhentingen kan skje så målrettet som mulig. Innhentingen må imidlertid ikke forveksles med målsøking, altså Etterretningstjenestens systematiske arbeid for å identifisere nye etterretningsmål etter lovforslaget § 5-1.

Hjemmelen for å innhente informasjon som utgjør et nødvendig grunnlag for å kunne innhente relevant informasjon, betegnes i lovforslaget som «innhenting av evneinformasjon», da det dreier seg om forhold som er nødvendig for at Etterretningstjenesten i det hele tatt skal *evne* å utføre sine lovpålagte oppgaver. Innhenting av evneinformasjon foreslås nå eksplisitt lovhjemlet, fordi all informasjonsinnhenting etter departementets syn bør synliggjøres og uttrykkelig hjemles i en helhetlig lovregulering. Hjemmelen foreslås inntatt i lovutkastet kapittel 3 for å knytte denne til innhentingshjemlene i §§ 3-1 til 3-4.

Departementet foreslår følgende bestemmelse i utkast til § 3-5:

§ 3-5 *Innhenting av evneinformasjon*

Etterretningstjenesten kan innhente og analysere informasjon om forhold som utgjør nødvendige forutsetninger for å kunne gjennomføre innhenting etter kapittelet her, herunder for å kunne

a. sørge for at innhenting ikke skjer i større utstrekning enn nødvendig,
b. ivareta sikkerheten til Etterretningstjenestens personell og operasjoner,
c. gjennomføre testing av teknisk utstyr og annen trenings- og øvingsaktivitet, og
d. opprettholde og videreutvikle Etterretningstjenestens aksesser og metodiske, teknologiske og øvrige evne til å utføre pålagte oppgaver.

7.10 Avgrensning mot etterretningsoperasjoner med annet formål enn informasjonsinnhenting

Foruten forventningen om at Etterretningstjenesten skal bidra med informasjon, kan det være grunn til å anta at norske myndigheter vil kunne ha en forventning om at Etterretningstjenesten i enkelte tilfeller handler på bakgrunn av informasjonen den har tilegnet seg, dersom dette er nødvendig for å avverge alvorlige trusler eller utfordringer. Dette omtales i dag som fordekte operasjoner med annet formål enn innhenting, eller såkalte effektoperasjoner. Slike operasjoner ligger utenfor kjernen av den tradisjonelle etterretningsvirksomhet, som er å innhente og analysere informasjon.

Effektoperasjoner kan gjennomføres både i det fysiske og digitale rom, ved bruk av menneskebaserte eller tekniske kapasiteter. Operasjonen må ha et selvstendig rettslig grunnlag, i og med at virksomheten ikke hjemles i lov om Etterretningstjenesten. Etter omstendighetene kan effektoperasjoner gjennomføres direkte med hjemmel i folkeretten eller med samtykke fra den stat hvor effekten manifesterer seg. Gjennomføring av slike operasjoner må skje med et klart folkerettslig grunnlag og innenfor rammene av FN-pakten, humanitærretten og annen relevant internasjonal rett. Det rettslige grunnlaget vil variere etter omstendighetene, blant annet om effektoperasjoner gjennomføres i eller utenfor rammen av væpnet konflikt, om vilkårene for statlig selvforsvar er tilstede eller om tiltaket er en respons på en i fredstid folkerettsstridig handling («international wrongful act») fra en utenlandsk statlig aktør. Rettsgrunnlaget og øvrige aspekter må vurderes konkret i det enkelte tilfelle.

Etterretningstjenesten har det nasjonale ansvaret for å planlegge og gjennomføre offensive cyberoperasjoner, herunder cyberangrep (Computer Network Attack), samt koordinere mellom offensive og defensive cybertiltak i Forsvaret. Etterretningstjenesten har også ansvaret for å forestå etterretningsmessig attribusjon av utenlandske trusselaktører ved alvorlige cyberoperasjoner rettet mot Norge eller norske interesser. Rettslig sett faller disse oppgavene utenfor rammen av en lov som dreier seg om innhenting og behandling av informasjon, og legaliteten av handlingene må derfor vurderes konkret ut fra omstendighetene.

8 Territoriell begrensning og andre særskilte forbud

8.1 Innledning

Etterretningstjenesten oppgavesett og innhentingshjemler er beskrevet i foregående kapittel i høringsnotatet her. At et forhold objektivt sett faller innenfor oppgavesettet innebærer imidlertid ikke at Etterretningstjenesten i alle tilfeller kan innhente informasjon om det. Lovforslaget inneholder flere konkrete innhentingsforbud som danner rammen for innhentingsvirksomheten. Forbudene foreslås regulert i lovens kapittel 4 og er henholdsvis en territoriell begrensning for innhentingsvirksomheten, forbud mot industrispionasje og forbud mot å utføre oppgaver med politiformål. Det vil redegjøres for disse i det følgende.

8.2 Etterretningstjenestens forhold til norske fysiske og juridiske personer

8.2.1 Historiske årsaker og ansvarsdelingen mellom Etterretningstjenesten og PST

Gjeldende etterretningstjenestelov § 4 første ledd oppstiller et forbud mot at Etterretningstjenesten på *norsk* territorium overvåker eller på annen fordekt måte innhenter informasjon om *norske* fysiske eller juridiske personer. Bestemmelsen ble opprinnelig inntatt for å motvirke eventuelle uklarheter knyttet til legalitetsprinsippets relevans for Etterretningstjenestens informasjonsinnhenting, ettersom dette på 1990-tallet fremdeles var uavklart. Den territorielle begrensningen ble videre begrunnet med viktigheten av å påse at tjenesten fokuserte sin virksomhet på forhold som lå utenfor norsk territorium, slik at det ble fastsatt et tydelig skille mellom innenlandsetterretningsrelevante forhold som PST (daværende Politiets overvåkingstjeneste) under Justisdepartementet var ansvarlig for, og utenlandsetterretningsrelevante forhold som det tillå Etterretningstjenesten, underlagt Forsvarsdepartementet, å fokusere på. Denne begrensningen i Etterretningstjenestens virksomhet ble ikke først introdusert gjennom etterretningstjenesteloven i 1998, men representerte en formalisering og synliggjøring av det som allerede da var langvarig praksis for overvåkingstjenestens og etterretningstjenestens virksomhetsutøvelse.

Det tydelige territorielle skillet gjenspeilet også datidens trusselbilde og teknologiske utvikling, som i langt mindre grad var grenseoverskridende i det omfang det er i dag. Bestemmelsen ble utformet i en historisk kontekst der Norges etterretningsbehov for å ivareta nasjonens sikkerhetsmessige interesser kunne utledes av de mål som var styrende for Forsvarets generelle virksomhet. Dette inkluderte forebygging av krig, vern av norsk handlefrihet overfor politisk og militært press, samt å sikre norsk medinnflytelse i internasjonale samarbeidsprosesser og forsvare norsk territorium mot krenkelser og angrep.[166] Dette fremgår også av Lund-rapporten fra 1995, der det presiseres at Etterretningstjenestens virksomhet var rettet mot den ytre trussel, i form av fremmede makter som kunne utgjøre en militær trussel mot Norge.[167] Betydningen av de teknologiske og trusselbaserte utviklingstrekkene for den territorielle begrensningen siden vedtakelsen av dagens etterretningstjenestelov beskrives nærmere under punkt 8.3.

8.2.2 Forholdet til norske fysiske og juridiske personer etter dagens regelverk

8.2.2.1 Saklig og geografisk avgrensning

Etterretningstjenesteloven § 4 oppstiller en saklig og geografisk avgrensning for Etterretningstjenestens målrettede innhentingsaktivitet. Bestemmelsen lyder som følger:

> Etterretningstjenesten skal ikke på norsk territorium overvåke eller på annen fordekt måte innhente informasjon om norske fysiske eller juridiske personer.
>
> Etterretningstjenesten kan bare oppbevare informasjon som gjelder norske fysiske eller juridiske personer dersom informasjonen har direkte tilknytning til ivaretakelsen av Etterretningstjenestens oppgaver etter § 3 eller er direkte knyttet til en slik persons arbeid eller oppdrag for Etterretningstjenesten.

[166] Ot. prp. nr. 50 (1996-1997) s. 8

[167] Dokument 16 (1995-1996) punkt 13.2.6 s. 845

Det er sikker rett at ordlyden ikke kan tolkes motsetningsvis slik at den *fritt* hjemler Etterretningstjenestens adgang til å innhente informasjon om norske personer såfremt disse befinner seg *utenfor* norsk territorium. Dette fremkommer både direkte i forarbeidene til etterretningstjenesteloven av 1998, og følger dessuten av fast og langvarig praksis forut for lovens vedtakelse.[168]

8.2.2.2 Fremmed etterretningsvirksomhet i Norge

Forbudet i § 4 er begrenset til «norske» fysiske og juridiske personer. En ren ordlydsfortolkning vil derfor kunne tilsi at alle ikke-norske subjekter faller utenfor innhentingsforbudet. Dette er ikke tilfellet. Etterretningstjenestens ansvarsområde er knyttet til utenlandske forhold, men tjenesten kan ikke av den grunn fritt innhente informasjon om ikke-norske fysiske og juridiske personer med opphold i Norge. E-instruksen[169] § 5 tredje ledd utdyper begrensningen nærmere. Tredje ledd lyder:

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

Som det fremgår av siste punktum skal innhentingen skje gjennom eller med samtykke fra PST.

8.2.2.3 Overskuddsinformasjon

Av E-instruksen § 5 første ledd, forarbeidene[170] samt langvarig praksis følger det også at dersom Etterretningstjenesten i utførelsen av sine lovpålagte oppgaver mottar overskuddsinformasjon om norske personer som er av interesse for andre norske myndigheter, skal slik informasjon kunne overbringes rette myndigheter. Overskuddsinformasjon er informasjon om forhold som ligger utenfor tjenestens ansvarsområde, og som således er uten etterretningsverdi, men som tjenesten likevel kommer i besittelse av som følge av sin lovlige innhentingsaktivitet. I etterretningstjenesteloven § 4 annet ledd er det inntatt et vilkår om at Etterretningstjenesten bare kan *oppbevare* informasjon som gjelder norske fysiske og juridiske personer dersom informasjonen har direkte tilknytning til ivaretakelsen av tjenestens oppgaver, eller er direkte knyttet til en slik persons arbeid eller oppdrag for tjenesten. Slik informasjon kan oppbevares så lenge formålet med oppbevaringen ikke er å drive fordekt innhenting rettet mot de norske personene. Sistnevnte forhold gjelder også frivillig samkvem mellom tjenesten og norske borgere, hvilket ikke omfattes av forbudet i etterretningstjenesteloven § 4, ettersom bestemmelsen bare rammer *fordekt* innhenting av informasjon. Forarbeidene og E-instruksen § 5 annet ledd fastslår at tjenesten uten hinder av etterretningstjenesteloven § 4 kan utføre troverdighetskontroll med slike kilder.[171]

8.2.2.4 Utenfor norsk territorium

Rettsstillingen til norske fysiske og juridiske personer *utenfor norsk territorium* reguleres ikke i dagens lov. Dette følger naturlig av datidens trusselbilde, som ikke tilsa at slik innhenting

---

[168] Ot. prp. nr. 50 (1996-1997) s. 10

[169] Instruks av 31. august 2001 nr. 1012 om Etterretningstjenesten

[170] Ot. prp. nr. 50 (1996-1997) s. 11

[171] Ibid. s. 11

var av stor relevans for Etterretningstjenestens oppdrag. I følge forarbeidene, kan slik innhenting gjennomføres «i den grad det er nødvendig for at tjenesten skal oppfylle lovens formål og utføre de oppgaver den i denne sammenheng er pålagt».[172] Avgjørende blir dermed om innhentingen ligger innenfor Etterretningstjenestens oppgaver i § 3. Dette må sammenholdes med forarbeidenes presisering av at etterretningsloven § 4 første ledd ikke skal tolkes motsetningsvis, dithen at Etterretningstjenesten overfor norske personer i utlandet *fritt* kunne innhente informasjon.

I lys av økningen av grenseoverskridende trusler, særlig terrortrusselen, har slik innhenting imidlertid blitt mer aktualisert for Etterretningstjenesten. I 2013 fastsatte følgelig Forsvarsdepartementet utfyllende bestemmelser for Etterretningstjenestens innsamling mot norske personer i utlandet samt for utlevering av personopplysninger om norske personer til utenlandske samarbeidende tjenester.[173] Bestemmelsene kodifiserer tjenestens tidligere interne retningslinjer og praksis for fordekt innhenting rettet mot slike personer, og fastslår hvilke vilkår som må være oppfylt for at tjenesten kan utføre denne type virksomhet, samt hvilke krav som gjelder ved utlevering av slike opplysninger til utenlandske samarbeidende tjenester. De utfyllende bestemmelsene er publisert og tilgjengeliggjort på Lovdata, og fastslår prosessuelle krav, i tillegg til å reflektere de menneskerettslige prinsippene om nødvendighet og forholdsmessighet.

8.2.2.5 Grenseoverskridende aktivitet og overvåkingshensikt

Departementet vil understreke at til tross for at Etterretningstjenesten skal fokusere sin virksomhet på forhold som ligger utenfor norsk territorium, vil det viktigste landet for vår nasjonale utenlandsetterretningstjeneste være Norge, både generelt og i et trusselperspektiv. For å kunne varsle om ytre trusler mot Norge, *er utenlandske trusselaktørers aktivitet i og mot Norge* av åpenbar utenlandsetterretningsinteresse. Dette vil eksempelvis inkludere kommunikasjon mellom etterretningsrelevante utenlandske aktører og norske personer. I enkelte tilfeller vil det være nødvendig at tjenesten i sin målsøking etter utenlandske etterretningsmål benytter informasjon som tjenesten allerede besitter om norske personer som utgangspunkt for målsøkingen. Da vil utenlandske personer av etterretningsmessig interesse som kommuniserer med norske personer kartlegges, men det er kun de utenlandske forbindelsene som har etterretningsverdi og som det potensielt vil bli iverksatt fordekt innhenting mot. Etterretningstjenesten kan ikke iverksette fordekt innhenting rettet mot den norske enden av kommunikasjonen. Slike tiltak ligger klart under PST sitt mandat.

Etterretningstjenesteloven § 3 og 4 hviler på dette premisset, ved at førstnevnte bestemmelse konstaterer at tjenesten skal innhente informasjon «som angår norske interesser» sett i forhold til fremmede stater, organisasjoner og individer. Følgelig vil forbindelsen mellom norske interesser og det utenlandske etterretningsmålet være høyst relevant for Etterretningstjenestens oppdragsløsning. Etterretningstjenesteloven § 4 annet ledd forutsetter videre at tjenesten må kunne behandle opplysninger om norske personer for å kunne løse sine lovbestemte oppgaver.

---

[172] Ibid. s. 10

[173] Utfyllende bestemmelser for Etterretningstjenestens innsamling mot norske personer i utlandet samt for utlevering av personopplysninger til utenlandske samarbeidende tjenester, fastsatt av Forsvarsdepartementet 24. juni 2013 med hjemmel i E-instruksen § 17. Bestemmelsene er kunngjort i Lovdata.

Det 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. I dette ligger det en forutsetning om *overvåkningshensikt* fra Etterretningstjenestens side. Den territorielle begrensning omfatter dermed aktiv og fordekt innhenting *rettet mot* norske personer i Norge. Fordekt-begrepet relaterer seg til selve innsamlingsmetoden og fokuset for innsamlingen, og ikke til den etterfølgende analysen og sammenstillingen av allerede innsamlet informasjon. Disse forholdene drøftes nærmere under punkt 8.4 og 8.5.

8.2.2.6 Videre fremstilling

Drøftelsene i det følgende vil redegjøre for utviklingstrekk som har hatt betydning for Etterretningstjenestens forhold til norske personer siden etterretningstjenestelovens vedtakelse. Deretter vil forslag til ny regulering av innhentingsforbudet behandles i punkt 8.4 og 8.5. Punkt 8.6 og 8.7 tar for seg to problemstillinger som er særskilt reist av EOS-utvalget, nemlig innhenting av rådata i bulk, og spørsmålet om adgangen til å foreta metadatasøk med utgangspunkt i en selektor tilhørende personer i Norge. Punkt 8.8 redegjør for innhenting gjennom åpne kilder, mens punkt 8.9 og 8.10 tar for seg forslag til lovregulering av enkelte særskilte forbud.

8.3 Fremtredende utviklingstrekk siden etterretningstjenestelovens vedtakelse av betydning for den territorielle begrensningen

8.3.1 Betydningen av trusselbildet

8.3.1.1 Generelt

Utviklingstrekkene innen trusselbilde og teknologi er av grenseoverskridende karakter, og har hatt en særlig betydning for Etterretningstjenestens forhold til norske fysiske og juridiske personer. Endringen i trusselbildet er utførlig beskrevet i kapittel 7 og 11. Av særlig relevans for Etterretningstjenestens befatning med norske personer er utviklingstrekkene relatert til internasjonal terrorisme. I dag er det særlig dette fenomenet som har gjort norske personer i utlandet til relevante etterretningsmål for tjenesten, men departementet understreker at også andre deler av tjenestens oppgaver kan kreve innhenting mot norske personer i utlandet.

8.3.1.2 Grenseoverskridende aktivitet

Ved lovens vedtakelse i 1998 var det ikke forventet at norske fremmedkrigere i betydelig omfang skulle ta del i internasjonal terrorvirksomhet. Dagens terrorisme preges av å være et grenseoverskridende fenomen som umuliggjør et klart skille mellom eksterne og interne trusler. Trusselen kommer fra enkeltpersoner og ikke-statlige organisasjoner som forflytter seg og er forgreinet over landegrensene, og som benytter teknologi som muliggjør forberedelser til og styring av terroranslag på tvers av ulike jurisdiksjoner. Selv om terrortrusselen de senere år i stor grad har vært knyttet til ekstreme islamistiske grupperinger, er internasjonal terrorisme i kontinuerlig endring. Nye grupper og fenomener vokser frem, som illustrert ved høyreekstremisme, islamfiendtlige og anti-statlige miljøer. Departementet anser at internasjonal terrorisme og trusselen mot Norge og norske interesser i utlandet fra terrorgrupperinger og deres støttespillere, vil være høyt prioritert av Etterretningstjenesten i overskuelig fremtid. Dette betyr at norske personer i utlandet med tilknytning til slike miljøer, vil fortsette å være relevante utenlandsetterretningsmål, og at

forbindelsen mellom personer i Norge og personer i utlandet som er involvert i internasjonal terrorisme vil være av åpenbar interesse for tjenesten i årene som kommer.

Denne grenseoverskridende utviklingen, som også kjennetegner digitale trusler, har utfordret den tradisjonelle distinksjonen mellom utenlandsetterretning og innenlandsetterretning. Etterretningstjenesten og PST har i økende grad sammenfallende oppgaver og arbeider svært ofte mot de samme truslene, men for noe ulike formål. Den grenseoverskridende terrortrusselen kan illustreres med norske fremmedkrigere som oppholder seg i utlandet, men som også kan vende tilbake til norsk territorium for kortere eller lengre perioder. Terrorgrupperinger i utlandet kan ha forgreininger til norske personer i Norge, eksempelvis støttespillere, hvilket betyr at trusselen både er ekstern og intern. Trusselen anses å både utfordre statssikkerheten, samtidig som den innbefatter kriminelle handlinger etter straffeloven. Dette fordrer håndtering både fra Etterretningstjenesten og PST, og i noen tilfeller også politiet. Det er en særlig forventning fra samfunnet om at terroranslag i størst mulig grad avverges av statlige myndigheter før de får utspille seg. Dette betyr at fremskaffelse av etterretninger er avgjørende, slik at det kan etableres et rettidig og helhetlig bilde, noe som igjen betinger et nært og godt samarbeid mellom Etterretningstjenesten, PST og politiet. Det har vært et politisk ønske om å tilrettelegge for samarbeid på dette området, som vist gjennom vedtakelsen av Instruks om samarbeid mellom Etterretningstjenesten og PST av 2006,[174] samt gjennom opprettelsen av Felles kontraterrorsenter i 2014.

I sin særskilte melding til Stortinget av 17. juni 2016 fremhevet EOS-utvalget fremveksten av grenseoverskridende terrorisme som en viktig årsak til å gjennomgå Etterretningstjenestens lovgrunnlag. Dette utviklingstrekket ble også vektlagt under Stortingets debatt om utvalgets særskilte melding i februar 2017.

8.3.2 Betydningen av kommunikasjonsteknologi

8.3.2.1 Ny teknologi – nye forutsetninger

Samtidig som trusselbildet har endret seg og internasjonal terrorisme har ført til at Etterretningstjenesten må følge med på norske personer i utlandet, har den teknologiske utviklingen akselerert. Kommunikasjonsstrukturen ser annerledes ut i dag enn i 1998, ettersom majoriteten av datatrafikk i dag går via fiberoptiske kabler og ikke i luftgrensesnittet, det er opprettet nye kommunikasjonsplattformer, og det har funnet sted en gjennomgripende digitalisering av vårt samfunn. Dette har medført at det genereres, lagres og prosesseres enorme mengder data. Informasjonssamlinger og datasett der en vesentlig del av informasjonen ikke er relevant for etterretningsformål kalles gjerne bulk-innsamling, se definisjon i lovutkastet § 1-4 nr. 2. Dette er nærmere problematisert i høringsnotatet punkt 9.5.6.

I punkt 9.5.6 redegjøres det nærmere for at det i moderne kommunikasjonsetterretning er teknisk umulig å tolke og sammenstille rådata, herunder utføre analyse, utvalg og filtrering, mens de er i transitt. Rådataen, som er ubearbeidet eller automatisk bearbeidet informasjon i enhver form hvis etterretningsverdi ikke er vurdert, må derfor lastes ned og lagres, for at det i det hele tatt skal være mulig å finne de informasjonsbitene om utenlandske forhold som er interessante. Dette kan eksemplifiseres med det mye omtalte nålen i høystakken-

[174] Instruks av 13.10.2006 nr. 1151 om samarbeidet mellom Etterretningstjenesten og Politiets sikkerhetstjeneste («Samarbeidsinstruksen»)

eksempelet, som tilsier at man må ha tilgang til relevante deler av høystakken for å kunne finne nålen. I bulk-innsamling vil de kommunikasjonsstrømmer som har størst etterretningsmessig verdi selekteres ut. I denne prosessen følger det, teknisk uunngåelig, med trafikkdata som ikke er av interesse. Ved senere evaluering av dataene vil slike data klassifiseres som overskuddsinformasjon. Overskuddsinformasjonen vil kunne inneholde trafikkdata relatert til norske personers kommunikasjon, selv om dette ikke er intendert.

Dette faktum, som er en konsekvens av den teknologiske utviklingen, bør derfor reflekteres i en oppdatert etterretningstjenestelov.

8.4 Den territorielle begrensningen i ny lov – hovedregel

8.4.1 Innledning

8.4.1.1 Ulike land – ulik organisering

Som redegjort for innledningsvis har den territorielle begrensningen for Etterretningstjenestens innhentingsadgang først og fremst sin begrunnelse i ansvarsfordelingen mellom Etterretningstjenesten som landets utenlandsetterretningstjeneste, og PST som landets innenlands sikkerhets- og etterretningstjeneste.

Andre sammenlignbare land har organisert og fordelt disse oppdragene på andre måter, eksempelvis i Nederland, Sverige og Storbritannia. I Nederland er *Algemene Inlichting-en Veiligheidsdienst*, underlagt Innenriksdepartementet, ansvarlig for ikke-militær innenlands- *og* utenlands- samt signaletterretning i den hensikt å beskytte nasjonal sikkerhet, mens *Militaire Inlichtingen-en Veiligheidsdienst*, underlagt forsvarsdepartementet, er ansvarlig for internasjonale trusler, herunder særlig militære og statsbaserte trusler som spionasje. I Sverige er *Försvarets radioanstalt*, underlagt forsvarsdepartementet, ansvarlig for signaletterretning og cybersikkerhet og opererer på oppdrag fra både regjeringen, departementene, forsvaret, rikspolitiet og den svenske sikkerhetstjenesten SÄPO. Sistnevnte, underlagt justisdepartementet, er ansvarlig for å forebygge og etterforske trusler mot rikets sikkerhet, som terror og spionasje. *Militära underrättelse- och säkerhetstjänsten*, en avdeling i det svenske forsvaret, er utelukkende ansvarlig for den militære etterretning i utlandet. I Storbritannia fungerer *Government Communication Headquarte*rs, underlagt utenriksdepartementet, som den nasjonale signaletterretningstjenesten. Den utfører signaletterretningsoppdrag på vegne av blant annet regjeringen, departementer, forsvaret, *National Crime Agency*, *Secret Intelligence Service* og *the British Security Service*. De to sistnevnte, er henholdsvis underlagt utenriksdepartementet og innenriksdepartementet og er ansvarlige for utenlandsetterretning og innenlandssikkerhet- og etterretning.

Det er ingenting i Grunnloven eller våre folkerettslige forpliktelser som forutsetter at den gjeldende norske modellen for innretning av etterretningsvirksomheten er den eneste tillatte måten å innrette seg på. Stortinget som lovgiver står dermed fritt til å vedta ny lovgivning som endrer denne.

Når det er sagt finner departementet ikke grunn til å foreslå noen endringer i den etablerte arbeidsfordeling mellom Etterretningstjenesten og PST, som etter departementets syn fungerer godt. Departementet understreker imidlertid at denne arbeidsfordelingen forutsetter

at tjenestene på en hensiktsmessig måte kan utveksle informasjon og samarbeide i generelle og konkrete saker der det er behov.

8.4.1.2 Er dagens lovtekst hensiktsmessig utformet?

Det kan reises spørsmål ved om utformingen av den territorielle begrensningen i dagens lov på egnet måte hjemler den aktivitet Etterretningstjenesten må utøve for å kunne produsere de etterretningsvurderinger som det er forventet av tjenesten.

Bestemmelsen i etterretningstjenesteloven § 4 og E-instruksen § 5 har blitt karakterisert som utydelige i EOS-utvalgets særskilte melding til Stortinget av 17. juni 2016, som problematiserer enkelte sider ved Etterretningstjenestens rettsgrunnlag. Problemstillingene som EOS-utvalget trekker frem er hva som ligger i fordektbegrepet, tolkingen av begrepet «norsk», problemstillinger knyttet til hvem innhenting er rettet mot, samt oppbevaring av overskuddsinformasjon.

I sin behandling av den særskilte meldingen fra EOS-utvalget uttaler Stortingets kontroll- og konstitusjonskomité at regelverket for Etterretningstjenestens virksomhet må legge til rette for tjenestens mulighet til effektiv oppgaveløsning og ivaretakelse av sikkerhetshensyn.[175] Komiteen uttaler videre at det er viktig at tjenestens hjemler for inngrep er tilstrekkelig klare til å kunne fastslå om tjenesten utfører virksomheten i tråd med lovgivers vilje. Videre fremhever komiteen at det er viktig både for tilliten til tjenesten og for faktisk og opplevd trygghet for landet og borgerne, at virkemidler som er forholdsmessige og nødvendige for å utføre tjenestens oppdrag beskrives gjennom et lovverk som stemmer overens med de utfordringer vi står overfor.

Under Stortingets debatt 21. februar 2017 om EOS-utvalgets særskilte melding, ble det anført at de virkemidlene som skulle til for å overvåke noen i 1998 var helt annerledes enn i dag, og at det nå var behov for å tilpasse disse. Herunder ble det vist til at dagens trusselaktører er oppdaterte med tanke på den tekniske utviklingen, hvilket betyr at Etterretningstjenesten også er nødt til å være utrustet med de virkemidlene de behøver for å utføre oppdraget som man er forventet å utføre. Det ble vektlagt at de siste års teknologiske utvikling innen kommunikasjonsteknologi er uten sidestykke, og at det eksisterende lovgrunnlaget for Etterretningstjenesten følgelig behøver revidering.

8.4.1.3 Departementets vurdering

Departementet deler oppfatningen om at den territorielle begrensningen kan formuleres på en tydeligere måte i lovteksten. Departementet vurderer at den rettslige uklarhet som EOS-utvalget peker på først og fremst beror på bestemmelsens ordlyd og begrepsbruk. Det er derfor hensiktsmessig å klargjøre hjemmelsgrunnlaget bedre, men det prinsipielle utgangspunktet om at det fortsatt bør oppstilles et territorielt innhentingsforbud ligger fast. Departementet har bestrebet seg på å reflektere og balansere de ulike hensyn som det er redegjort for over i forslaget til ny normering.

Departementet vil tilføye at det er en prioritert oppgave for EOS-utvalgets kontroll med Etterretningstjenesten å kontrollere at det territorielle innhentingsforbudet overholdes. Et oppdatert og klarere regelverk på dette området vil dermed etter departementets syn bidra til å styrke forutsetningene for en god kontroll.

[175] Innst. 164 S, 2016-2017 side 2

Departementet mener på denne bakgrunn at det er behov for å drøfte nærmere hva som bør ligge i et forbud mot innhenting mot personer og virksomheter i Norge, og hvordan dette bør formuleres i loven.

8.4.2 Personer og virksomheter som befinner seg i Norge – hvem som omfattes (lovutkastet § 4-1)

8.4.2.1 Gjeldende rett

Som redegjort for over har etterretningstjenesteloven § 4 første ledd blitt oppfattet som uklar med tanke på hva som ligger i begrepet «norsk». For det første brukes betegnelsen «*norsk* territorium» for å avgrense Etterretningstjenestens oppdrag. Hva dette omfatter er ikke nærmere utdypet i forarbeidene til någjeldende lov, men en naturlig forståelse av ordlyden sammenholdt med tjenestens etablerte praksis, tilsier at det korresponderer med det som utgjør Norges geografiske territorium. Dette inkluderer både det norske land-, sjø, og luftterritoriet, Svalbard, Jan Mayen, samt bilandene som er underlagt norsk statshøyhet etter bilandsloven av 1930. Etterretningstjenestelovens etablerte territorialbegrep er dermed sammenfallende med de alminnelige regler for hva som anses å være norsk geografisk territorium. Områder som kun er underlagt norsk jurisdiksjon, slik som norskregistrerte fartøyer på åpent hav og i utlandet eller norske utenriksstasjoner, faller følgelig utenfor den territorielle begrensningen.

Videre bruker etterretningstjenesteloven betegnelsen «*norske* fysiske eller juridiske personer» i § 4 første ledd. Lysne II-utvalgets rapport, som utreder et digitalt grenseforsvar, foretar innledningsvis en grundig gjennomgang av Etterretningstjenestens samfunnsoppdrag og informasjonstilgang. I rapporten side 16 er det nærmere utdypet hva som legges i dette begrepet:

> «Med «norske personer» menes
>
> norske og utenlandske statsborgere som har fast eller midlertidig lovlig opphold i Norge og som ikke opptrer på vegne av fremmed makt, eller
>
> norske og utenlandske juridiske personer som har hovedkontor i Norge eller på annen måte lovlig opererer på norsk territorium eller har annen særlig primærtilknytning til riket og som ikke opptrer på vegne av fremmed makt, uavhengig av hvilke(n) ikke-statlig(e) fysisk(e) eller juridisk(e) person(er) som eier eller kontrollerer virksomheten.»

I tråd med gjeldende praktisering av regelverket tolkes innhentingsforbudet i § 4 første ledd utvidende til også å omfatte fysiske personer som har fast eller midlertidig lovlig opphold i Norge, det være seg gjennom norsk statsborgerskap, asylsøknad eller som turist. Dette til tross for at det i forarbeidene til någjeldende lov er påpekt at «Bestemmelsen vil derfor ikke ramme innhenting av informasjon om utenlandske statsborgere som oppholder seg i Norge og annen fremmed aktivitet i Norge, såfremt dette er nødvendig for å gjennomføre Etterretningstjenestens oppgaver [...]».[176] Praksisen begrunnes i reelle hensyn. Oppfatningen er at utenlandske statsborgere som har lovlig opphold i Norge, midlertidig eller permanent, i dette henseende ikke burde tilkjennes dårligere rettsstilling enn norske statsborgere. Det er derfor en etablert praksis at Etterretningstjenesten ikke fordekt innhenter informasjon om utenlandske statsborgere i Norge, med mindre disse opptrer på

[176] Ot. prp. nr. 50 (1996-1997) s. 11

vegne av fremmed makt. Hva som ligger i begrepet «fremmed makt» drøftes nærmere under punkt 8.5.1.

For juridiske personer i Norge er det krav om at de enten har hovedkontor i riket, på annen måte lovlig opererer her, eller har annen særlig primærtilknytning til Norge, for at de skal omfattes av innhentingsforbudet. Sistnevnte kan eksempelvis gjelde dersom den juridiske personen skatter til Norge.

8.4.2.2 Tvilstilfeller

I tvilstilfeller må man vurdere hvordan en person skal kategoriseres. Praksis fra Etterretningstjenesten viser at en person som befinner seg i Norge behandles som en «norsk» person med mindre det foreligger eller fremkommer klare holdepunkter for at vedkommende ikke er det. Det er således etablert en relativt høy terskel for å konkludere med at innhentingsforbudet ikke gjelder. Tilsvarende behandler Etterretningstjenesten en person som befinner seg i utlandet som ikke-norsk, med mindre det foreligger eller fremkommer klare holdepunkter for at vedkommende er norsk. Ved tvil om en person befinner seg i Norge eller i utlandet, legges det til grunn som fremstår mest sannsynlig basert på den informasjon som er tilgjengelig eller som kan skaffes til veie fra PST, andre partnere, åpne kilder eller annen lovlig innhenting.

Gitt dagens grenseoverskridende trusler, både hva gjelder internasjonal terrorisme og digitale trusler, som tilsier at etterretningsmål beveger seg og kommuniserer over landegrensene, antas det nettopp å være en del tilfeller der tjenesten vil være i tvil om *hvor* en trusselaktør eller annen etterretningsrelevant person oppholder seg. I dag praktiseres i disse sakene prinsippet om alminnelig sannsynlighetsovervekt. Det betyr at det er tilstrekkelig at informasjonen som Etterretningstjenesten besitter eller klarer å fremskaffe gir minimum 51 prosent sannsynlighet for at det anførte faktum er riktig for at faktumet kan legges til grunn. Et strengere krav, eksempelvis kvalifisert sannsynlighetsovervekt, antas i slike saker å vesentlig vanskeliggjøre tjenestens oppdragsløsning. Dette fordi det vil kunne være utfordrende å fremskaffe slik avgjørende informasjon i en tidlig fase av Etterretningstjenestens kartleggingsaktivitet.

8.4.2.3 Departementets vurdering

Som presisert over mener departementet det er grunn for å videreføre innhentingsforbudet i ny lov, men i en noe annen utforming. Bestemmelsen som departementet foreslår er i tråd med gjeldende praksis og viderefører hovedregelen om at det er forbudt for Etterretningstjenesten å rette innhenting mot personer og virksomheter med tilhold i Norge. Likeledes bør det fortsatt være tillatt for Etterretningstjenesten å innhente informasjon om nordmenn i utlandet, forutsatt at det ligger innenfor de lovpålagte oppgavene i lovforslaget kapittel 3 og oppfyller grunnvilkårene i lovforslaget kapittel 5.

I forslaget til ny regulering ser departementet ingen grunn til å fravike tolkningen av hva som utgjør norsk territorium som redegjort for innledningsvis. Departementet tilrår å videreføre gjeldende rett, men foreslår for enkelhets skyld å benytte betegnelsen «Norge» i stedet for «norsk territorium» i ny § 4-1.

Når det gjelder begrepet «norsk» mener departementet at dette ikke er et dekkende begrep, og foreslår å endre ordlyden i ny regulering. Dette har sammenheng med at det springende punktet i bestemmelsen er *hvor* en person oppholder seg, altså på norsk territorium, og ikke den formelle tilknytningen i form av statsborgerskap. I forslaget til ny bestemmelse foreslår derfor departementet at § 4-1 første ledd presiseres til å gjelde «en fysisk person som

oppholder seg i Norge», og at annet ledd presiseres til å gjelde «virksomhet i Norge som utøves av en juridisk person». En slik formulering vil være i overensstemmelse med slik regelverket praktiseres i dag, og vil sørge for at ordlyd og praksis er bedre kalibrert. Departementet har vurdert om første og andre ledd skulle formuleres under ett, men har av språklige hensyn kommet til at det er mest hensiktsmessig å dele opp disse.

Gode grunner taler etter departementets syn for å videreføre den etablerte praksisen om at Etterretningstjenesten ikke fordekt skal innhente informasjon om utenlandske statsborgere i Norge, med mindre disse opptrer på vegne av fremmed makt. PST vil i stor grad vil ha som oppgave å foreta slik fordekt innhenting, riktignok for andre formål enn de som er styrende for Etterretningstjenestens virksomhet. Likelydende oppdrag vil kunne føre til at de to tjenestene går i beina på hverandre, og for stor grad av overlapping i oppgavesettene vil også være uhensiktsmessig ut fra effektivitetshensyn. Unntaket knyttet til fremmed makt følger av unntaksbestemmelsen i lovutkastet § 4-2.

Departementet foreslår at det inntas et tredje ledd i § 4-1 som spesifiserer at Etterretningstjenesten, der det er tvil om en person oppholder seg eller driver virksomhet i Norge, skal søke å avklare forholdet basert på tilgjengelig informasjon fra PST, andre partnere, åpne kilder eller egen innhenting. At dette nå foreslås spesifisert i lovteksten er nytt, men det innebærer ingen materiell endring i forhold til gjeldende rettstilstand.

8.4.3 Overvåkningshensikt (lovutkastet § 4-1)

8.4.3.1 Gjeldende rett

Andre tolkingsspørsmål som springer ut av etterretningstjenesteloven § 4 første ledd er hva som ligger i begrepet «overvåkning eller annen fordekt innhenting» og hva som menes med å innhente informasjon «om» norske fysiske eller juridiske personer. En nærmere fastleggelse av innholdet i disse begrepene har både betydning for å forklare dagens rettstilstand, men danner også et viktig bakteppe for forslaget til ny formulering i loven.

En ren ordlydsfortolkning av begrepet «overvåkning eller annen fordekt innhenting» tilsier at innhentingen finner sted på en slik måte at den det gjelder ikke er kjent med den. Dette er også i overensstemmelse med uttalelser i forarbeidene til gjeldende lov, som henviser til en kvalifisert form for overvåkning sett opp mot det generelle innhentingsbegrepet i etterretningstjenesteloven § 3.[177] Disse uttalelsene i forarbeidene taler for at begrepet «overvåkning eller annen fordekt innhenting» må forstås snevrere enn det alminnelige innhentingsbegrepet etter § 3. Etter en naturlig ordlydstolkning er en person ikke «overvåket» med mindre personen er blitt utsatt for systematisk, eller i det minste en form for bevisst eller tilsiktet, informasjonsinnhenting.

8.4.3.2 EOS-utvalgets særskilte melding

EOS-utvalget drøfter forholdet mellom begrepene «innhenting» etter lovens § 3 og «overvåkning og annen fordekt innhenting» etter § 4 i sin særskilte melding avgitt til Stortinget i juni 2016.[178] Etter EOS-utvalgets syn foreligger det to mulige tolkingsalternativer. Begrepet «overvåkning eller annen fordekt innhenting» i etterretningstjenesteloven § 4 kan etter utvalgets syn tolkes som en generell henvisning til bruk av skulte metoder for å tilegne

[177] Ot.prp. nr. 50 (1996-1997), punkt 12 s. 15 i merknader til de enkelte paragrafer

[178] Se EOS-utvalgets særskilte melding til Stortinget om rettsgrunnlaget for Etterretningstjenestens overvåkingsvirksomhet punkt 5.2 s. 19 flg.

seg opplysninger som ikke er allment tilgjengelig. Utfordringen med en slik fortolkning er etter utvalgets oppfatning at den ikke bærer i seg hensynet til etterretningstjenestelovens formål og Etterretningstjenestens mulighet til effektivt å kunne løse sine oppgaver i etterretningstjenesteloven §§ 1 og 3, som taler for en snever forståelse av innhentingsbegrepet i forbudet. Det andre tolkingsalternativet utvalget fremhever er at forbudet i § 4 må forstås slik at det rammer den fordekte innhenting som er *rettet mot* norske personer og at det dermed må innfortolkes en overvåkingshensikt overfor disse. Det kan etter utvalgets syn argumenteres for at uttalelsene i forarbeidene om en kvalifisert form for overvåkning taler for at begrepet «overvåkning eller annen fordekt innhenting» må forstås snevrere enn en generell henvisning til alle fordekte metoder, for å sikre Etterretningstjenestens mulighet til effektiv å løse sine oppgaver, jf. etterretningstjenesteloven §§ 1 og 3. EOS-utvalget fremhever at en utfordring med en slik forståelse er at lovgivningen ikke gir anvisning på hvor grensen i slike tilfeller må gå. Dette reiser etter utvalgets syn spørsmål om når overvåkingshensikt inntrer og hvor inngripende tiltaket er i personvernet.

8.4.3.3 Dagens praktisering - kvalifisert form for innhenting

Etterretningstjenestens praksis på området gjenspeiler en forståelse av bestemmelsen som korresponderer med at det kreves en kvalifisert form for innhenting for at innhentingsforbudet skal få anvendelse. I dette ligger at fordekt-begrepet relaterer seg til innsamlings*metoden* samt *fokuset* for innsamlingen. Hva som er fokus for innhentingen reflekteres i begrepet «om» i § 4 første ledd. Fordekt innhenting «om» norske personer må da forstås som fordekt innhenting *rettet mot* slike personer. Det betyr at det fra Etterretningstjenestens side må foreligge en overvåkningshensikt overfor disse personene for at aktiviteten rammes av forbudet i etterretningstjenesteloven § 4 første ledd. I Lysne II-utvalgets rapport ble tilsvarende rettsforståelse lagt til grunn da utvalget beskrev dagens grunnvilkår for Etterretningstjenestens innsamlingsvirksomhet: *"*Innhentingen kan ikke innebære fordekt innhenting på norsk territorium rettet mot norske fysiske eller juridiske personer.*"*[179] [vår understrekning].

En tolkning av § 4 første ledd som forbyr all bruk av skjulte metoder for å tilegne seg opplysninger som ikke er allment tilgjengelige og som kan innbefatte informasjon om nordmenn i Norge harmonerer dårlig med § 4 annet ledd som på nærmere vilkår tillater Etterretningstjenesten å oppbevare informasjon om norske fysiske eller juridiske personer. Vilkårene i annet ledd spesifiserer ikke *hvordan* Etterretningstjenesten har fått opplysningene i hende. Man kan lese forholdet mellom første og andre ledd slik at første ledd gir en anvisning på *mot hvem* og *hvor* Etterretningstjenesten kan rette sin *aktive* innhentingsvirksomhet, mens andre ledd fastsetter vilkår for selve oppbevaringen av opplysninger knyttet til personer og virksomheter i Norge. Dette taler for at det er den målrettede innhentingsvirksomheten som reguleres i første ledd, og tilsier at det må foreligge en overvåkningshensikt. En slik forståelse forhindrer Etterretningstjenesten fra å iverksette målrettet innhenting i etterretningsøyemed mot en person eller virksomhet i Norge. På den annen side vil Etterretningstjenestens generelle målsøkingsaktivitet falle utenfor forbudet, selv om norsk informasjon uintendert kan følge med på lasset ved slik innsamling, fordi slik aktivitet ikke kan sies å være direkte *rettet mot* en person eller virksomhet i den hensikt å innhente for etterretningsformål. Oppbevaring av rådata, herunder overskuddsinformasjon,

[179] Lysne II-utvalget rapport om digitalt grenseforsvar av 26. august 2016, s. 60

og de personvernmessige implikasjonene dette har, drøftes nærmere under punkt 8.6.3 og punkt 9.5.6.

Avslutningsvis vil departementet bemerke at henvisningen til «fordekte» metoder i dagens lovtekst synes å antyde at innhenting fra åpne kilder ikke omfattes av forbudet. All innhentingsaktivitet som Etterretningstjenesten utfører, det være seg gjennom åpne kilder eller fordekte metoder, skal imidlertid ha et utenlandsetterretningsfokus i tråd med vilkårene etter etterretningstjenesteloven §§ 1 og 3. Dette drøftes nærmere under punkt 8.7.

8.4.3.4 Behov for presisering av forbudet i ny §§ 4-1 og 4-2

I forslaget til oppdatert regulering av innhentingsforbudet er det et grunnleggende poeng å søke å formulere forbudet på en så presis og dekkende måte som mulig, akkompagnert av en redegjørelse i lovens forarbeider. Departementet opplever at mye av årsaken til debatten knyttet til innhentingsforbudets rekkevidde beror på at ordlyden i dagens lov kan tolkes på ulike måter, og at dagens lov ble til i lys av et annet trusselbilde og i en annen teknologisk tidsalder enn det vi lever i dag.

Departementer mener det er hensiktsmessig at innhentingsforbudet deles i to bestemmelser i loven. Den første bestemmelsen, § 4-1, bør etter departementets syn oppstille et forbud mot innhenting mot personer som befinner seg i Norge, mens unntakene fra hovedregelen angis i den påfølgende bestemmelsen, § 4-2. Departementet ønsker ikke å videreføre begrepet «overvåkning eller annen fordekt innhenting» i ny § 4-1, ettersom også innsamling fra åpne kilder må være rettet mot utenlandsetterretningsrelevante forhold. Felles for begge de nye bestemmelsene er dermed at innhentingsforbudet gjelder all innhenting, herunder gjennom åpne kilder og fordekte innhentingsdisipliner, av informasjon rettet mot personer eller virksomheter i Norge.

Det forutsettes videre at forbudet bare gjelder der det foreligger *overvåkningshensikt* fra Etterretningstjenestens side. Dette reflekteres gjennom begrepet «rettet mot» i overskriften i utkast til § 4-1. Formuleringen «rette innhenting av informasjon mot», brukes også i nevnte paragrafer og er ment å reflektere det samme. Departementet mener at det er nødvendig å operere med et krav om overvåkningshensikt for at Etterretningstjenesten skal kunne løse sine lovpålagte oppgaver på en hensiktsmessig og effektiv måte, og anser dette for å være i tråd med gjeldende praksis.

Departementets forslag til en oppdatert regulering av den territorielle begrensningen bygger på dagens prinsipielle utgangspunkt og hovedregel om at Etterretningstjenesten ikke skal drive rettet innhentingsvirksomhet mot personer og virksomheter som befinner seg i Norge. Samtidig søker forslaget å tydeliggjøre hva som ligger i begrepet «rette innhenting mot» både for å unngå tolkningstvil knyttet til hjemmelsgrunnlaget for Etterretningstjenestens virksomhet, og for å sikre at tjenesten er i stand til å drive effektiv utenlandsetterretning. Det vises til redegjørelsene for dette i overstående punkt. Med forslag til ny formulering i loven mener departementet at hjemmelsgrunnlaget er bedre tilpasset de utfordringer vi står overfor, og at lovregelen er utformet tilstrekkelig klart til at man på en god måte vil kunne kontrollere at Etterretningstjenesten utfører virksomhet i tråd med lovgivers vilje.

Det foreslås derfor følgende lovtekst til ny § 4-1:

§ 4-1 *Forbud mot innhenting rettet mot personer som befinner seg i Norge*

Det er forbudt for Etterretningstjenesten å rette innhenting av informasjon mot en fysisk person som oppholder seg i Norge.

Det er forbudt for Etterretningstjenesten å rette innhenting av informasjon mot virksomhet i Norge som utøves av en juridisk person.

Hvis Etterretningstjenesten er i tvil om en person oppholder seg eller driver virksomhet i Norge, skal den søke å avklare forholdet basert på den informasjon som er tilgjengelig eller for dette formål kan skaffes til veie fra Politiets sikkerhetstjeneste, andre partnere, åpne kilder eller egen innhenting.

8.5 Den territorielle begrensingen i ny lov - unntak og presiseringer

8.5.1 Innhenting mot person eller virksomhet som opptrer på vegne av fremmed makt i Norge (lovutkastet § 4-2 første ledd)

8.5.1.1 Gjeldende rett

Dagens territorielle innhentingsforbud gjelder ikke absolutt. Dette fremgår av forarbeidene til dagens etterretningstjenestelov samt av tilhørende E-instruks § 5 tredje ledd. Unntak gjelder overfor personer eller virksomheter som opptrer i Norge på vegne av fremmed makt, og favner etter gjeldende rett både utlendinger og nordmenn. Bakgrunn og hensyn bak reguleringen knyttet til disse to kategoriene er i noen grad ulik.

Når det gjelder Etterretningstjenestens adgang til å rette informasjonsinnhenting mot *utlendinger* i Norge, så var tjenestens praksis knyttet til fordekt innhenting mot representanter for fremmed makt i Norge etablert lenge før vedtagelsen av etterretningstjenesteloven i 1998. Praksisen omtales i Lund-rapporten, som viser til Etterretningstjenestens veletablerte avlytting av såkalte «utenlandske kontorer» i Norge.[180] I forarbeidene til gjeldende lov, fremgår det at forbudet i § 4 første ledd derfor ikke vil ramme innhenting av informasjon om utenlandske statsborgere som oppholder seg i Norge og annen fremmed aktivitet i Norge, såfremt dette er nødvendig for å gjennomføre tjenestens oppgaver.[181] Uttalelsen åpner i prinsippet for innhenting mot enhver utlending i Norge dersom dette antas å bidra til løsningen av Etterretningstjenestens oppgaver. I praksis har man imidlertid lagt seg på en forsiktig tolkning, og kun innhentet mot personer som anses å opptre på vegne av fremmed makt.

Begrensningen av forbudet i etterretningstjenesteloven § 4 første ledd er omtalt og utdypet i Lysne II-utvalgets rapport, hvor hensynene bak en slik begrensning ble redegjort for slik:[182]

> «Tilknytning til fremmed stat kan imidlertid tilsi at enkelte utenlandske personer ikke har samme krav på beskyttelse mot etterretning på samme måte som andre utenlandske statsborgere som lovlig oppholder seg i Norge.»

Det ble i den forbindelse vist til etterretningstjenestelovens forarbeider, der det presiseres at det vil være tilfeller hvor forbudet etter § 4 første ledd ikke kommer til anvendelse. Særlig nevnes «fremmed aktivitet» på norsk territorium. Lysne-utvalget bemerker at dette må forstås som «utenlandsk aktivitet som utføres på vegne av fremmed stat eller internasjonal organisasjon».

---

[180] Dokument nr. 15 (1995-1996), vedlegg 5 av Ketil Lund

[181] Ot. prp. nr. 50 (1996-1997) s. 11

[182] Rapport fra Lysne II-utvalget om digitalt grenseforsvar av 26. august 2016, s. 15-16

Det er følgelig sikker rett at Etterretningstjenesten i tråd med gjeldende lovgivning og praksis kan rette informasjonsinnhenting mot utlendinger som opptrer på vegne av fremmed makt i Norge. I dette ligger det ingen begrensning med tanke på innhentingens formål, hvilket betyr at Etterretningstjenesten kan rette innhenting mot vedkommende for alle formål som fremgår av Etterretningstjenestens oppgavesett etter lovens § 3.

E-instruksen § 5 tredje ledd presiserer innhentingsforbudet i etterretningstjenesteloven § 4 første ledd nærmere med tanke på norske personer og virksomheter. I følge instruksen er lovens § 4 ikke til hinder for at Etterretningstjenesten kan innhente opplysninger om fremmed etterretningsvirksomhet i Norge, herunder om norske fysiske og juridiske personer som driver slik virksomhet, i den utstrekning tjenesten har behov for slik informasjon. I den kongelige resolusjonen som lå til grunn for instruksen heter det om § 5 at denne paragrafen «klargjør spørsmål som hittil har fremgått som forutsetninger i proposisjonen som lå til grunn for loven». Unntaket fra det territorielle innhentingsforbudet lå følgelig til grunn som en forutsetning i forarbeidene til dagens etterretningstjenestelov, som blant annet illustrert ved følgende presisering i forarbeidene:[183]

> «E-tjenesten må ha full innsikt i fremmed etterretningsvirksomhet i Norge rettet mot den norske etterretningstjenesten, for – i samarbeid med overvåkningstjenesten – å kunne treffe adekvate mottiltak.»

E-instruksen § 5 tredje ledd gjelder kun innhenting av opplysninger om fremmed *etterretningsvirksomhet* i Norge. Av bestemmelsens overskrift fremgår det at bestemmelsen bare omfatter Etterretningstjenestens forhold til *norske* fysiske og juridiske personer. Presiseringen er dermed uten betydning for Etterretningstjenestens forhold til ikke-norske personer som oppholder seg i Norge. Denne formen for informasjonsinnhenting for kontraetterretningsformål er etter E-instruksen § 5 tredje ledd annet punktum betinget av at det skjer gjennom eller etter samtykke fra PST, av hensyn til PSTs primæransvar for å forebygge og motvirke ulovlig etterretningsvirksomhet på norsk territorium, og forutsetter at «tjenesten har behov for slik informasjon».

Innhenting på norsk territorium for andre formål enn kontraetterretningsformål kan etter gjeldende rett ikke utøves overfor norske personer, med unntak av kildeverifikasjon etter instruksens § 5 annet ledd, se nærmere om kildeverifikasjon i punkt 8.5.2. Videre kan det legges til grunn at innhenting rettet mot norske personer med dobbelt statsborgerskap som ikke lenger har lovlig opphold i Norge og som opptrer på vegne av annen stat, er tillatt etter gjeldende rett. I disse tilfellene er det mer nærliggende å anse personen som utenlandsk borger enn norsk borger, fordi vedkommende vil ha en sterkere tilknytning til en fremmed stat enn til Norge også ut over å inneha utenlandsk statsborgerskap.

8.5.1.2 Behov for oppdatert regulering

Departementet mener at det fortsatt er behov for å opprettholde et unntak fra hovedregelen om territoriell begrensning for Etterretningstjenestens virksomhet, knyttet til personer eller virksomheter som opptrer på vegne av fremmed makt i Norge. Departementet ser imidlertid behov for å tydeliggjøre unntaket i større grad enn det som er tilfellet i dagens regulering. Særlig er det nødvendig å vurdere hvilke personer i Norge som kan bli gjenstand for Etterretningstjenestens innhenting, og hvilke formål som kan begrunne innhenting. Dette gjelder særlig med tanke på å belyse hvilke personer i Norge som ikke har krav på samme

[183] Ot.prp. nr. 50 (1996-1997) side 11

beskyttelse mot etterretning som andre, samt for å påse at det videreføres en hensiktsmessig fordeling av oppgaver mellom Etterretningstjenesten og PST. Departementet vil bemerke at det ikke tas sikte på å endre dagens ansvars- og oppgavefordeling mellom de to tjenestene. Det anses videre formålstjenlig å utdype hva som innbefattes i begrepet «fremmed makt», samt redegjøre for hvilken terskel som legges til grunn for å kunne fastslå om en person opptrer på vegne av en fremmed makt.

8.5.1.3 Personkretsen – generelt om forslag til ny regulering

Departementet mener at den rettslige og faktiske utviklingen som har funnet sted siden vedtakelsen av etterretningstjenesteloven og tilhørende instruks tilsier en revurdering av hvilke personer som bør kunne bli gjenstand for Etterretningstjenestens innhenting i Norge. Herunder er departementet av den oppfatning at innhenting mot norske statsborgere som driver med fremmed etterretningsvirksomhet i Norge, ikke lenger behøver å tilligge Etterretningstjenestens oppgavesett. Departementet begrunner dette primært med at slik aktivitet i all hovedsak vil utgjøre ulovlig etterretningsvirksomhet, noe det tilligger PST etter politiloven § 17 b å forebygge og etterforske. Sekundært var begrunnelsen for unntaket i forbudet etter etterretningstjenesteloven § 4 første ledd at Etterretningstjenesten måtte kunne treffe adekvate mottiltak mot fremmed etterretningsvirksomhet som var rettet mot tjenesten i Norge. Ettersom Etterretningstjenesten er underlagt bestemmelsene i lov om nasjonal sikkerhet, vil tjenesten kunne utøve adekvate forebyggende beskyttelsestiltak innenfor denne rammen, eksempelvis etter sikkerhetslovens § 4-3 samt tilhørende forskrift om plikt til å gjennomføre sikkerhetstiltak for å redusere risikoen for sikkerhetstruende virksomhet.[184] Departementet kan vanskelig se at det skulle være et reelt behov for å iverksette innhentingstiltak med kontraetterretningsformål rettet mot norske statsborgere i Norge, gitt PST sitt ansvar på området og muligheten til å treffe forebyggende tiltak etter sikkerhetsloven.

Etterretningstjenestens kontraetterretningsinnsats i Norge i fred, krise og væpnet konflikt vil med en slik regulering utelukkende være rettet mot fremmed aktivitet på norsk jord, og vil utenfor rammen av væpnet konflikt alltid skje gjennom eller med samtykke fra PST. Departementet understreker også at det fortsatt vil være en sentral oppgave for Etterretningstjenesten å innhente informasjon om fremmed etterretningsvirksomhet rettet mot Norge og norske interesser, og at norske personer som driver ulovlig etterretningsvirksomhet vil være relevant for tjenesten å kjenne til, samt motta og behandle informasjon om. Det samme gjelder hvilke mål i Norge utenlandsk etterretning prioriterer. Men det *aktive* innhentingsfokuset for Etterretningstjenesten vil og bør etter departementets syn være rettet mot den *utenlandske* etterretningsvirksomheten og eventuelt deres styring av og kommunikasjon med norske borgere som er vervet av den fremmede aktøren. Videre oppfølging og innhenting mot norske personer i Norge vil være PSTs ansvar.

8.5.1.4 Virksomheter

Departementet vurderer at dersom det foreligger konkrete holdepunkter for at en virksomhet i Norge opptrer på vegne av fremmed makt, stiller situasjonen seg noe annerledes. Det kan dreie seg om et multinasjonalt selskap, en organisasjon eller et selskap som har hovedsete i Norge og som har en vesentlig andel norske ansatte. I slike tilfeller er innhentingen rettet mot virksomheten som sådan, og ikke mot fysiske personer. Dette tilsier at de personvernhensyn som gjør seg gjeldende for fysiske personer i Norge, ikke kommer til

[184] Lov av 1. juni 2018 om nasjonal sikkerhet (i skrivende stund ikke trådt i kraft)

anvendelse i samme grad overfor en virksomhet. Dette understøttes av at de beskyttelsesverdige personverninteressene hovedsakelig er knyttet til fysiske personer, hvilket også gjenspeiles i personopplysningsloven som ikke gjelder for juridiske personer. Departementet vektlegger dette, samt at virksomheter, eksempelvis selskaper og organisasjoner, i dag ofte kan ha en sammensatt eierskaps- eller styreform og at de opererer i flere jurisdiksjoner. Dette tilsier at Etterretningstjenesten vil kunne ha et etterretningsmessig behov for å innhente mot slike virksomheter i Norge, forutsatt at disse opptrer på vegne av fremmed makt og anses å utøve fremmed etterretning eller annen fremmed aktivitet på norsk territorium. Det tilrådes derfor at Etterretningstjenesten kan rette innhenting mot virksomheter i Norge dersom virksomheten utøves på vegne av fremmed makt.

8.5.1.5 Utenlandske personer

Departementet legger videre til grunn at Etterretningstjenesten har langvarig og etablert praksis knyttet til informasjonsinnsamling rettet mot *utenlandske* personer i Norge som opptrer på vegne av fremmed makt. Dagens rettstilstand legger til rette for at Etterretningstjenesten kan iverksette innsamling rettet mot slike personer i Norge, både når de er involvert i «fremmed etterretningsvirksomhet» og når de utøver annen «fremmed aktivitet» i Norge. I dette ligger at tjenesten kan innhente informasjon for samtlige formål som fremgår av Etterretningstjenestens oppgavesett. Dersom det innhentes mot fremmed etterretningsvirksomhet, skal dette imidlertid skje gjennom eller med samtykke fra PST. Utenlandske eller statsløse personer som har en tilknytning til fremmed stat, og som anses å opptre på vegne av en fremmed stat, kan ikke sies å ha samme krav på beskyttelse mot strategisk etterretning som andre utenlandske statsborgere som lovlig oppholder seg i Norge. Departementet ser ingen grunn til å endre denne rettstilstanden, og legger til grunn at slik innhenting åpenbart vil ha utenlandsetterretningsrelevans.

8.5.1.6 Forslag til unntaksbestemmelse

På denne bakgrunn tilrår departementet at ny § 4-2 første ledd fastsetter et unntak fra forbudet i § 4-1. Det foreslås at Etterretningstjenesten kan rette innhenting av informasjon mot en utenlandsk statsborger eller en statsløs person, eller mot en norsk eller utenlandsk virksomhet i Norge, dersom det foreligger konkrete holdepunkter for at disse opptrer på vegne av fremmed makt eller virksomheten utøves av fremmed makt, og naturligvis forutsatt at de øvrige vilkår for innhenting foreligger.

Departementet foreslår at unntaket fra innhentingsforbudet ikke skal gjelde for personer med norsk statsborgerskap. For personer som både har norsk og utenlandsk statsborgerskap må det foretas en vurdering av om vedkommende skal anses som «norsk» eller «utenlandsk», hvor det blant annet må legges vesentlig vekt på om vedkommende har lovlig opphold i Norge. Departementet anser det ikke hensiktsmessig å fastsette vurderingskriteriene nærmere i lov.

Departementet vurderer at forslaget her vil medføre at unntaket fra innhentingsforbudet fremkommer klarere og mer presist av lovteksten. Etter departementets syn vil det også klargjøre den faktiske oppgavefordeling mellom Etterretningstjenesten og PST. Det anbefales at innhenting av informasjon om fremmed etterretningsvirksomhet fremdeles skal skje etter samtykke fra PST, slik at denne aktiviteten koordineres på hensiktsmessig måte.

8.5.1.7 Nærmere om begrepet «fremmed makt»

Departementet foreslår å benytte begrepet «fremmed makt» i lovforslaget. Dette vil i hovedsak omfatte det som defineres som en fremmed stat, i tillegg til enkelte andre fremmede aktører med en særlig status i folkeretten. For å fastslå hva som er en fremmed stat, vil det være naturlig å legge til grunn den alminnelige folkerettslige definisjonen av begrepet stat, som innbefatter fire vilkår. Disse er et krav til territorium, befolkning, et styresett og kapasitet til å inngå forbindelser med andre stater. Ettersom anerkjennelse av en stat er en politisk markering og ikke et juridisk krav, vil statsbegrepet også kunne omfatte stater som ikke er anerkjent som en stat av Norge eller det internasjonale samfunn for øvrig.

For at en person eller en virksomhet skal anses å opptre eller utøve virksomhet *på vegne av* en fremmed stat, forutsetter det at staten utøver en viss instruksjon eller kontroll med personens eller virksomhetens aktivitet i Norge. Departementet mener det her er riktig å legge prinsippene om statsansvar, som nedfelt i International Law Commission (ILC) sitt *Draft articles on Responsibility of States for Internationally Wrongful Acts* av 2001, til grunn. Disse anses i hovedsak å utgjøre folkerettslig sedvanerett. Artikkel 8 fastslår når handlinger begått av en person eller persongruppe skal attribueres til en stat. Det legges til grunn at en handling skal betraktes som en statshandling når personen(e) faktisk handlet på bakgrunn av instruksjoner fra, under ledelse eller kontroll av staten i utførelsen av handlingen. Eksempelvis vil informasjonsinnhenting rettet mot væpnet personell som opptrer på vegne av fremmed stat i Norge være omfattet av unntaket i forslag til § 4-2 første ledd bokstav a. Dette kan være i form av fremmede elitetropper under dekke, som opptrer på vegne av fremmed stat på norsk territorium i en tidlig fase av en sikkerhetspolitisk konflikt eller i form av hybrid krigføring. Dette er nærmere beskrevet under punkt 7.3 og 7.5. Det vil i slike tilfeller være essensielt at Etterretningstjenesten kan fremskaffe informasjon og avdekke hvorvidt Norge er utsatt for et sammensatt angrep. Departementet mener at personer med slik opptreden ikke er beskyttet av de hensyn som ligger til grunn for hovedregelen i utkast til § 4-1.

Utover representanter for fremmede stater, vil det også være av utenlandsetterretningsmessig relevans å rette innhenting mot personer eller virksomheter som opptrer eller utøver virksomhet på vegne av andre fremmede aktører. Dette er bakgrunnen for at departementet foreslår å benytte begrepet fremmed *makt*. Lysne II-utvalget la i sin rapport til grunn at «internasjonale organisasjoner» også vil kunne inngå i «fremmed makt» begrepet.[185] Departementet anser at begrepet er skjønnsmessig og må kunne tolkes dynamisk i tråd med endringer i trusselbildet. Begrepet vil kunne innbefatte andre internasjonale aktører eller organisasjoner som eksempelvis er anerkjent av norske myndigheter som en politisk aktør eller som aksepteres av det internasjonale samfunn å opptre på den internasjonale arena med en viss folkerettslig handleevne uten å være en stat i formell forstand.

For å kunne iverksette innhenting mot personer som opptrer på vegne av fremmed makt, mener departementet at det må oppstilles krav om at Etterretningstjenesten frembringer *konkrete holdepunkter* for at personen eller virksomheten opptrer på vegne av slik makt. Dette tilsvarer den terskelen som er lagt til grunn som et grunnvilkår for målrettet innhenting mot etterretningsmål i utlandet etter ny § 5-2 første ledd. Det kreves således ikke sannsynlighetsovervekt, men det må foreligge ett eller flere objektive holdepunkter for at

[185] Rapport fra Lysne II-utvalget om digitalt grenseforsvar av 26. august 2016, s. 16

personen eller virksomheten opptrer på vegne av slik makt. De øvrige vilkår for innhenting må i tillegg være oppfylt. Innhenting mot personer eller virksomheter som opptrer på vegne av fremmed makt forutsetter derfor blant annet at innhentingen er *formålsstyrt*, dvs. at det foreligger konkrete holdepunkter for at innhentingen vil være relevant for løsning av tjenestens oppgaver etter lovforslagets kapittel 3, og *forholdsmessig* etter lovforslaget § 5-4.

Oppsummert anbefaler departementet at rettstilstanden i hovedsak videreføres i ny lov, med unntak av den nye begrensningen som gjelder innhenting rettet mot norske statsborgere i Norge. Herunder foreslås at Etterretningstjenesten, for alle formål etter ny §§ 3-1 og 3-2, skal kunne rette innhenting mot utenlandske statsborgere eller statsløse personer, eller mot norsk eller utenlandsk virksomhet i Norge som antas å opptre på vegne av fremmed makt. Departementet foreslår følgende ordlyd i § 4-2 første ledd:

> Etterretningstjenesten kan rette innhenting av informasjon mot en utenlandsk statsborger eller statsløs person, eller mot en norsk eller utenlandsk virksomhet i Norge, dersom det foreligger konkrete holdepunkter for at personen opptrer på vegne av fremmed makt eller virksomheten utøves av fremmed makt. Innhenting av informasjon om fremmed etterretningsvirksomhet i Norge skal skje etter samtykke fra Politiets sikkerhetstjeneste.

8.5.2 Kildeverifikasjon av Etterretningstjenestens menneskelige kilder (lovutkastet § 4-2 annet og tredje ledd)

8.5.2.1 Innledning

En kilde vil si en person som kultiveres, rekrutteres og føres av Etterretningstjenesten for å gjennomføre menneskebasert innhenting, eller en person som utfører oppdrag for tjenesten ved å tilrettelegge for menneskebasert innhenting. En organisasjon eller et miljø kan også fungere som kilde inntil relevante enkeltpersoner innenfor organisasjonen eller miljøet er identifisert. Kilder kan være norske eller utenlandske statsborgere, som kan oppholde seg på norsk eller utenlandsk territorium.

8.5.2.2 Gjeldende rett

Da etterretningstjenesteloven ble vedtatt i 1998 var Stortinget kjent med og forutså behovet for at Etterretningstjenesten også måtte kunne oppbevare opplysninger om norske borgere. Tjenesten ble gitt hjemmel i § 4 annet ledd til å «oppbevare informasjon som gjelder norske fysiske eller juridiske personer dersom informasjonen har direkte tilknytning til ivaretakelsen av etterretningstjenestens oppgaver etter § 3 eller er direkte knyttet til en slik persons arbeid eller oppdrag for Etterretningstjenesten.» Av forarbeidene fremgår det at man tok høyde for at tjenesten ville ha behov for frivillige norske kilder:[186]

> «Frivillig samkvem mellom tjenesten og norske borgere vil heller ikke være forbudt, fordi bestemmelsen bare rammer fordekt innhenting av informasjon. Bestemmelsen tar i denne forbindelse ikke sikte på å forby at det gjennomføres en troverdighetskontroll av slike kilder.»

Stortingets forutsetninger ble nedfelt i dagens E-instruks § 5 annet ledd, som fastslår at «Tjenesten kan gjennomføre tiltak for å verifisere sine kilders troverdighet». Etterretningstjenesteloven § 4 annet ledd oppstiller i den forbindelse et relevansvilkår om at nedtegning av slike opplysninger må være «direkte knyttet til» tjenestens oppgaveløsning, herunder direkte knyttet til tjenestens samarbeid med frivillige norske kilder. Evalueringsutvalget, som vurderte EOS-utvalgets kontroll med de hemmelige tjenestene i

[186] Ot.prp. nr. 50 (1996-1997), s. 11

Norge, viste til dette unntaket fra forbudet i etterretningstjenesteloven § 4 første ledd i sin rapport, og understreket at tjenesten kan innhente informasjon på norsk territorium for å kontrollere kilders troverdighet.[187] Det ligger i sakens natur at dette inkluderer fordekte innhentingstiltak rettet mot potensielle og rekrutterte kilder, både for å kunne vurdere om en person bør tilnærmes for rekruttering, og for å vurdere om en rekruttert person kan utgjøre en trussel eller risiko for Etterretningstjenesten, eksempelvis ved at vedkommende også er rekruttert av fremmed lands etterretningstjeneste.

8.5.2.3 Behov, egnethet og troverdighet

For en moderne utenlandsetterretningstjeneste vil det åpenbart være behov for å kunne innhente informasjon via mennesker, både norske og utenlandske, for å besvare norske myndigheters prioriterte informasjonsbehov. Departementet legger til grunn at det vil være avgjørende at menneskelige kilder, både potensielle og eksisterende, vurderes med tanke på egnethet og troverdighet, gitt de konsekvenser det kan ha dersom kildene kompromitterer tjenestens informasjonsbehov, personell, eller i verste fall opererer på vegne av fremmed stats etterretningstjeneste.

I tråd med det som er sagt over er det antatt å følge forutsetningsvis av gjeldende lov at Etterretningstjenesten uten hinder av innhentingsforbudet kan gjennomføre visse fordekte og ikke-fordekte tiltak for å verifisere sine potensielle og eksisterende kilders egnethet og troverdighet. Instruksen § 5 annet ledd forutsetter at det foreligger slik adgang. Tiltakene kan innbefatte aktive og passive tiltak. Et eksempel på sistnevnte er forespørsler til andre norske myndigheter om utlevering av relevant informasjon som belyser hvorvidt personen er egnet som kilde. Det er sikker rett at slike forespørsler om informasjon, som ikke innebærer noen form for operativ aktiv innhenting fra Etterretningstjenestens side, ikke er å anse som fordekt innhenting etter etterretningstjenesteloven § 4 første ledd. Dette er også omtalt i punkt 8.2.2.3.

Aktive tiltak vil kunne omfatte innhenting av strengt nødvendig informasjon om en person som er tilgjengelig i åpne kilder. Kun opplysninger som er nødvendige for å kunne foreta en formålstjenlig kildeverifikasjon kan innhentes og nedtegnes. Det saklige formålet med innhentingen kan være todelt. Formålet med innhentingen kan på den ene siden være å fastslå hvorvidt en potensiell eller eksisterende kilde besitter eller kan skaffe tilgang til relevant informasjon for utenlandsetterretningsformål. Innhentingen foretas da i forkant av at disse kontaktes av tjenesten. Hensikten vil aldri være å innhente etterretningsrelevant informasjon *om* norske miljøer eller innenlandske forhold, som det ligger utenfor tjenestens mandat å innhente informasjon om. På den annen side kan formålet være å fastslå vedkommendes motivasjon, troverdighet og egnethet. Opplysninger som innhentes vil i så fall være direkte relevante for denne vurderingen av kilden, for vurdering av sikkerheten til kilden selv og for Etterretningstjenestens virksomhet. Slik innhenting inngår i tjenestens målsøkingsaktivitet, og vil normalt være mindre inngripende i personvernet enn en ordinær sikkerhetsklareringsprosess. Videre kan aktive innhentingstiltak, i enkelte avgrensede tilfeller der det foreligger tungtveiende sikkerhetsmessige grunner, omfatte fordekt tilnærming til og fordekt innhenting rettet mot potensielle og eksisterende kilder. I slike saker må det foretas en forholdsmessighetsvurdering mellom viktigheten av å etablere eller videreføre et frivillig

[187] Dokument 16 (2015–2016) Rapport til Stortinget fra Evalueringsutvalget for Stortingets kontrollutvalg for etterretnings-, overvåkings og sikkerhetstjeneste (EOS-utvalget), s. 68

samarbeid med en kilde, opp mot inngrepet et slikt fordekt innhentingstiltak vil ha overfor vedkommende. Selv om hovedregelen er åpen tilnærming til potensielle kilder, kan Etterretningstjenesten i slike tilfeller velge ikke å tilkjennegi tilhørighet til tjenesten, i en innledende fase. Formålet med å opptre slik er å skaffe tilstrekkelig informasjon til å vurdere påfølgende åpen tilnærming til personen i den hensikt å rekruttere vedkommende som kilde. Fordekte innhentingstiltak er i dag begrenset til menneskebasert innhenting samt systematisk observasjon, og gjennomføres utelukkende dersom det foreligger tungtveiende sikkerhetsmessige grunner til det.

8.5.2.4 Tydeliggjøring av lovgrunnlaget for kildeverifikasjon

Sikkerhetsmessige årsaker som redegjort for ovenfor, samt behovet for tilstrekkelig informasjon til å vurdere hvorvidt en person er egnet som kilde, tilsier at Etterretningstjenesten må ha mulighet til å iverksette visse passive og aktive innhentingstiltak. Departementet vektlegger her de betydelige konsekvensene det kan ha dersom kildene kompromitterer tjenestens informasjonsbehov, personell eller opererer på vegne av fremmed stats etterretningstjeneste. Dette tilsier også at tjenesten i visse avgrensede tilfeller vil kunne ha behov for å tilnærme seg en kilde fordekt, eller iverksette visse fordekte innhentingstiltak mot vedkommende. Slik fordekt innhenting mener departementet at bør avgrenses til menneskebasert innhenting etter forslag til § 6-3 og systematisk observasjon som beskrevet i forslag til § 6-4, hvilket er i tråd med Etterretningstjenestens etablerte praksis. Dermed er det ikke hjemmel for å foreta øvrige fordekte innhentingstiltak med mindre det foreligger samtykke fra kilden.

Selv om innhentingen av informasjon er rettet mot en person eller virksomhet i Norge, vil ikke Etterretningstjenestens hensikt være å innhente informasjon ut fra etterretningsformål. Formålet er utelukkende å belyse eventuelle sikkerhetsmessige forhold rundt personen eller virksomheten, samt belyse hvorvidt vedkommende er egnet som kilde. Det foreligger dermed ingen overvåkningshensikt i § 4-1 sin forstand. Tiltakene vil likevel kunne utgjøre inngrep i en persons rett til privatliv, og departementet anser at hjemmelsgrunnlaget for slike tiltak klart bør fremkomme i ny lov. Det vektlegges herunder at innhentingen må være forholdsmessig i lys av viktigheten av en adekvat kildeverifikasjon, opp mot det inngrepet som innhentingen av strengt nødvendige opplysninger om vedkommende utgjør. Her må det vektlegges hvorvidt mindre inngripende tiltak i tilstrekkelig grad kan ivareta formålet, inngrepets virkning for den som rammes og sakens betydning. Dette følger av lovutkastet § 5-4.

Det må antas at opplysninger som Etterretningstjenesten behøver for å belyse en persons eller virksomhets egnethet eller troverdighet, vil kunne være av en viss personlig karakter. Departementet henviser her til Etterretningstjenestens etablerte praksis som viser at passive og aktive innhentingstiltak i kildeverifikasjonsøyemed, kun benyttes i avgrensede tidsperioder for å innhente strengt nødvendig informasjon. Fordekte innhentingstiltak iverksettes utelukkende i situasjoner der tungtveiende sikkerhetsmessige årsaker tilsier det. Det foreslås at disse kvalifiserende vilkårene fremgår i ny § 4-2 tredje ledd.

I tråd med etablert praksis foreslås det at hovedregelen skal være at Etterretningstjenesten tilnærmer seg potensielle kilder i Norge åpent, det vil si at tilknytningen til norske myndigheter eller Etterretningstjenesten oppgis til vedkommende i den innledende fasen hvor det søkes kontakt med vedkommende. Tjenestens frivillige samarbeid med menneskelige kilder skal være basert på et informert samtykke fra kildene.

Departementet tilrår at gjeldende praksis og rettstilstand videreføres, og at formålet med innhentingen klart fremgår i § 4-2 annet ledd. Det anses videre formålstjenlig å innta kvalifiserende vilkår i ny § 4-2 tredje ledd, herunder at det ikke skal innhentes mer informasjon enn det som er strengt nødvendig. Hovedregelen vil være at informasjon innhentes gjennom åpne kilder, utlevering av opplysninger fra andre norske myndigheter, eller med samtykke fra den det gjelder. Unntaket som omfatter fordekt tilnærming til eller innhenting etter ny §§ 6-2 og 6-3, forutsetter at det foreligger tungtveiende sikkerhetsmessige grunner og at det kun innhentes strengt nødvendig informasjon i en avgrenset tidsperiode. Unntaket vil følgelig være strengt formåls- og tidsavgrenset.

Departementet foreslår følgende lovtekst i ny § 4-2 annet og tredje ledd:

Etterretningstjenesten kan rette innhenting av informasjon mot personer eller virksomheter i Norge dersom formålet med innhentingen er å frembringe relevant informasjon for å finne potensielle kilder eller gjennomføre kildeverifikasjon.

Ved innhenting etter annet ledd skal det ikke innhentes mer informasjon enn det som fremstår som strengt nødvendig. Informasjon skal innhentes gjennom åpne kilder, utlevering av opplysninger fra andre norske myndigheter, eller med samtykke fra den det gjelder. Dersom det foreligger tungtveiende sikkerhetsmessige grunner kan strengt nødvendig informasjon likevel innhentes i en avgrenset tidsperiode uten å oppgi tilknytning til Etterretningstjenesten eller norske offentlige myndigheter, samt ved bruk av metoder som nevnt i §§ 6-3 og 6-4 i loven her. Øvrige metoder kan kun benyttes med samtykke fra den som innhentingen rettes mot.

Departementet foreslår følgende definisjon av begrepet kildeverifikasjon i lovutkastet § 1-4 nr 6:

Kildeverifikasjon; innhenting og vurdering av informasjon for å fastslå hvorvidt en potensiell eller eksisterende kilde besitter eller kan skaffe tilgang til relevant informasjon for etterretningsformål, samt fastslå motivasjon, troverdighet og egnethet.

8.5.3 Mottak av informasjon om personer og virksomheter i Norge (lovutkastet § 4-2 fjerde ledd)

8.5.3.1 Gjeldende rett

Det er etablert rettsforståelse at Etterretningstjenesten både kan motta og anmode om å få utlevert informasjon om fysiske og juridiske personer i Norge, forutsatt at opplysningene har direkte tilknytning til ivaretakelsen av Etterretningstjenestens oppgaver etter etterretningstjenesteloven § 3. Etterretningstjenesteloven § 4 annet ledd forutsetter at tjenesten må kunne behandle opplysninger om norske personer for å kunne løse sine lovbestemte oppgaver, og legger til grunn et relevansvilkår ved at informasjonen må ha *direkte tilknytning* til ivaretakelsen av tjenestens oppgaver. Slik mottatt informasjon kan oppbevares så lenge opplysningene anses relevante for løsningen av tjenestens oppgaver. Etter dette skal opplysningene slettes fra tjenestens operative systemer. Forarbeidene til dagens etterretningstjenestelov understøtter denne rettsoppfatningen, ved at det der presiseres at det i forbindelse med tjenestens kontraetterretningstiltak på norsk territorium, kunne utleveres slike opplysninger til Etterretningstjenesten fra overvåkningspolitiet, forutsatt at tjenesten hadde behov for det, og at Etterretningstjenesten kunne anmode overvåkningspolitiet om slik informasjon.[188]

[188] Ot. prp. nr. 50 (1996-97) s. 11

Et illustrerende eksempel kan i dag være Etterretningstjenestens mottak av opplysninger fra PST om norske fremmedkrigere, selv om disse på utleveringstidspunktet skulle befinne seg på norsk territorium. Slike trusselaktører har en klar relevans for Etterretningstjenestens oppdragsløsning, og opplysningene vil kunne brukes i den hensikt å avdekke utenlandsetterretningsrelevante forhold. Det er behov for å få tidlig informasjon om disse, for å kunne være forberedt på å kunne rette innhenting mot personene dersom de reiser til utlandet og således faller inn under Etterretningstjenestens primæransvar.

Det samme gjelder forespørsler fra Etterretningstjenesten til andre norske myndigheter om utlevering av relevant informasjon som belyser hvorvidt en norsk person er egnet som kilde. Dette utgjør heller ikke fordekt innhenting fra tjenesten sin side.

8.5.3.2 Departementets vurdering

Departementet vektlegger at Etterretningstjenestens virksomhet er rettet mot forhold som ligger utenfor norsk territorium, men at koblingen som forutsettes i dagens etterretningstjenestelov § 3 om tjenestens innhenting av informasjon som angår «norske interesser sett i forhold til fremmede stater, organisasjoner eller individer», betinger at Etterretningstjenesten også kan anmode om, motta og behandle opplysninger om personer og virksomheter i Norge, når dette er direkte relevant for ivaretakelsen av tjenestens oppdrag etter loven. Slike opplysninger kan eksempelvis benyttes som utgangspunkt for videre målutvikling knyttet til utenlandske trusselaktører, og er ikke innhentet på en måte som omfattes av forslag til formulering av forbudet i § 4-1.

Departementet understreker at denne adgangen ikke skal brukes for å omgå Etterretningstjenestens eget regelverk og begrensninger. Eksempelvis skal ikke forespørsler fra Etterretningstjenesten til andre om slik informasjon undergrave den territorielle begrensningen i tjenestens lovgrunnlag. Dette er nærmere omtalt i punkt 13.4 om utlevering av informasjon. Det vil tilligge EOS-utvalget å undersøke og kontrollere at slike omgåelser ikke finner sted.

Departementet mener det er behov for å videreføre dagens praksis og at denne materialiseres i form av et eget ledd i unntaksbestemmelsen i § 4-2 fjerde ledd:

> Forbudet i § 4-1 er ikke til hinder for at Etterretningstjenesten mottar eller for etterretningsformål ber om å få utlevert informasjon som andre besitter om personer eller virksomhet i Norge.

8.5.4 Utstyrstesting, trening og øving (lovutkastet § 4-2 femte ledd)

I lovforslaget § 3-5 om innhenting av evneinformasjon fremkommer det at Etterretningstjenesten kan innhente informasjon blant annet for å gjennomføre strengt nødvendig testing av teknisk utstyr og etterretningsfaglig trening og øving. I § 9-10 i utkastet er innhentede personopplysninger nærmere regulert, blant annet i form av plikt til å slette alle opplysninger når testingen/øvingen/treningen er gjennomført. Det er i punkt 12.9 redegjort nærmere for hvorfor denne aktiviteten må foregå i Norge. Det er ikke til å komme forbi at man vil måtte behandle personopplysninger som ledd i denne virksomheten, uten at personene som opplysningene kan knyttes til er kjent med dette. Selv om innhentingen åpenbart ikke har overvåkingshensikt og at opplysningene ikke innhentes for å inngå i produksjon av etterretninger, bør det ryddes av vei eventuell tvil om at innhentingen kan komme i konflikt med hovedregelen om forbudet mot å rette innhenting mot personer og virksomheter i Norge.

Departementet foreslår derfor følgende bestemmelse i § 4-2 femte ledd:

Forbudet i § 4-1 er ikke til hinder for at det innhentes informasjon som er strengt nødvendig for å kunne gjennomføre testing av utstyr eller trening og øving i Norge.

8.6 Innhenting av rådata i bulk som inneholder informasjon om personer og virksomheter som befinner seg i Norge (lovutkastet § 4-2 sjette ledd)

8.6.1 Generelt

Som redegjort for i punkt 8.3.2, er det i moderne kommunikasjonsetterretning teknisk umulig å vurdere og sammenstille rådata mens de er i transitt. Dette innebærer at Etterretningstjenesten først må laste ned dataene og lagre dem for en bestemt periode, for at det deretter skal være mulig å detektere de dataene om utenlandske forhold som er av interesse. Prinsipper knyttet til bulk-innsamling ble offentlig belyst i Lysne II-utvalgets rapport om Digitalt grenseforsvar, der det ble understreket at Etterretningstjenesten er avhengig av å kunne innhente og lagre slike rådata for å løse sitt oppdrag.[189] Etterretningstjenesten har tilsvarende understreket at det for en moderne etterretningstjeneste i dag er avgjørende å ha tilgang til et relevant rådatagrunnlag for å kunne utøve etterretningsvirksomhet i form av målsøking og målrettet innhenting.

Rådata utgjør ubearbeidet eller automatisk bearbeidet informasjon i enhver form hvis etterretningsverdi ikke er vurdert. Når slike data innhentes i *bulk*, betyr det at Etterretningstjenesten innhenter informasjonssamlinger og datasett hvorav en vesentlig andel av informasjonen antas irrelevant for etterretningsformål. Departementet foreslår at det lovfestes egne grunnvilkår som regulerer innhentingen av og søk i rådata i bulk i utkast til § 5-3. Dette er nærmere behandlet i punkt 9.5.6. En særskilt problemstilling som reiser seg i forbindelse med innhenting av rådata i bulk er at disse datasamlingene kan inneholde informasjon om personer som oppholder seg, eller virksomhet som utøves, i Norge.

Slik Etterretningstjenesten praktiserer dette i dag, for eksempel fra nedlesing av satellittsignaler, selekterer tjenesten ut de datastrømmer og datasamlinger som vurderes å ha størst etterretningsmessig verdi for oppdraget. I denne prosessen følger det, teknisk uunngåelig, med trafikkdata som ikke er av interesse. Dette anses som overskuddsinformasjon, som også i noen tilfeller kan inneholde trafikkdata relatert til personer eller virksomheter i Norge. Det er langvarig praksis for at Etterretningstjenesten lagrer slike data, og av tekniske, praktiske og økonomiske årsaker er det ikke mulig å foreta rutinemessig manuell gjennomgang av alle rådata for å vurdere deres etterretningsrelevans. I motsetning til forslaget om tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon, der en ikke ubetydelig andel vil være metadata relatert til personer eller virksomheter i Norge, vil ordinær innsamling av rådata i bulk inneholde en svært liten andel av slik informasjon. Dette fordi innsamlingen ikke er knyttet til den *grenseoverskridende* kommunikasjonen mellom Norge og utlandet, men tar utgangspunkt i generelle datastrømmer og datasamlinger, som inneholder både metadata og innholdsdata, og som vurderes å ha størst andel data relatert til personer og virksomheter i utlandet.

[189] Se Lysne II-utvalgets rapport om digitalt grenseforsvar av 26. august 2016, punkt 3.3.2 s. 16

8.6.2 Innhenting av rådata i bulk

I EOS-utvalgets særskilte melding til Stortinget i juni 2016 ble det stilt spørsmål ved Etterretningstjenestens nåværende hjemmelsgrunnlag for å *innhente* metadata som kan inneholde opplysninger om norske personer i Norge. Gitt de tekniske premissene for innhenting av rådata, blir spørsmålet i tillegg om Etterretningstjenesten kan *oppbevare* overskuddsinformasjon når dette er strengt nødvendig for å løse sitt oppdrag.

Gjeldende etterretningstjenestelov § 4 første ledd forbyr fordekt informasjonsinnhenting om norske fysiske og juridiske personer i Norge. Departementet mener at en forutsetning for at forbudet skal komme til anvendelse er at det foreligger overvåkningshensikt fra Etterretningstjenestens side, og foreslår at dette skal komme tydeligere frem i forslag til ny normering. Den territorielle begrensningen er følgelig ment å ramme den aktive og fordekte innhentingen *rettet mot* norske fysiske og juridiske personer i Norge. Dette er nærmere beskrevet under punkt 8.4.3 over.

Departementet viser til at innhenting av rådata i bulk ikke har til hensikt å samle inn informasjon om personer og virksomheter i Norge. Dette er snarere informasjon som teknisk uunngåelig og uintendert «følger med på lasset», og som for de fleste former for bulk-innsamling utgjør en svært liten andel av den samlede datamengden. Innhentingen som sådan vil uansett ikke være *rettet mot* personer eller virksomheter i Norge, fordi dette vil stride mot forbudet i gjeldende lov § 4, som foreslås videreført i lovutkastet § 4-1. Det kan dermed vanskelig legges til grunn at Etterretningstjenesten i denne sammenheng utviser noen form for overvåkningshensikt overfor personer eller virksomheter i Norge.

8.6.3 Lagring og oppbevaring av rådata

Hva gjelder Etterretningstjenestens oppbevaring av uevaluerte data som kan være overskuddsinformasjon, vektlegger departementet at det ikke finnes realistiske alternativer for å filtrere ut ikke-relevant informasjon fra datasettene. Departementet vil videre fremheve at mengden overskuddsinformasjon relatert til norske rettssubjekter fra alminnelig bulkinnsamling relativt sett vil være meget liten. Videre vil informasjonen ligge forsvarlig sikret og lagret i tjenestens dataservere, som trolig er Norges best beskyttede datalagre. Opplysningene, som vil kunne inkludere metadata og innholdsdata, vil ligge der ubehandlet, med mindre en analytiker aktivt søker etter informasjonen og henter den ut av rådatamaterialet. Inngrepets virkning for den enkelte som rammes av tiltaket, vurderes følgelig å være marginal. Eventuelle søk vil være sporbare, vil måtte tilfredsstille grunnvilkårene for innhenting, og være underlagt EOS-utvalgets kontroll. Det legges følgelig til grunn at risikoen for misbruk av opplysninger relatert til personer og virksomheter i Norge, eller uautorisert tilgang til slik informasjon, vil være minimal gitt den svært begrensede mengden av slik innsamlet overskuddsinformasjon. Sporbarheten i datasystemene, samt EOS-utvalgets kontroll med tjenestens søk inn i rådatamaterialet vil videre redusere risikoen for eventuelt misbruk. På bakgrunn av disse momentene mener departementet at dette inngrepet i retten til privatliv i en forholdsmessighetsvurdering veiet opp mot formålet med tiltaket, nemlig ivaretakelsen av rikets sikkerhet, ikke kan tillegges avgjørende vekt. Departementet vektlegger herunder Etterretningstjenesten sitt grunnleggende behov for innhenting av rådata i bulk for å kunne løse sitt lovpålagte oppdrag, og viser til punkt 8.3.2 som nærmere redegjør for hvorfor det ikke foreligger andre tekniske alternativer som er mindre inngripende.

8.6.4 Forslag til presisering i lovteksten

På bakgrunn av forestående redegjørelse anbefaler departementet at dagens rettstilstand videreføres, men at det inntas en tydelig presisering i lovteksten av at innhenting av rådata i bulk ikke anses som rettet mot personer eller virksomhet omfattet av det territorielle innhentingsforbudet, selv om rådataene kan inneholde slik informasjon. Følgende lovbestemmelse foreslås i ny § 4-2 sjette ledd:

> Innhenting av rådata i bulk er ikke å anse som rettet mot personer eller virksomhet omfattet av § 4-1, selv om rådata kan inneholde informasjon om personer som oppholder seg eller virksomhet som utøves i Norge.

8.7 Nærmere om metadatasøk med utgangspunkt i selektor tilhørende person i Norge (lovutkastet § 4-2 syvende ledd)

8.7.1 Loggsøk i metadata for målsøkingsformål

8.7.1.1 Nærmere om problemstillingen

Under punkt 8.3.2 om betydningen av kommunikasjonsteknologi, ble det vist til viktigheten av målsøking i Etterretningstjenestens arbeid. Under målsøking benyttes blant annet såkalte metadatasøk, som innebærer søk i store rådatagrunnlag som tjenesten lovlig har innhentet ved hjelp av tekniske kapasiteter. Slike søk er i sin natur kartleggende og avgjørende for å avdekke nye og ukjente trusselaktører. Aktiviteten finner sted før et etterretningsmål er identifisert som relevant og målrettet fordekt innsamling mot vedkommende iverksettes. Betydningen av slike metadata, det vil si data som beskriver typen eller formatet av innholdet, hvem som er avsender og mottaker, størrelse, tidspunkt og varighet av kommunikasjon, har blitt stadig viktigere i etterretningsarbeidet de senere år. Dette er utførlig omtalt i høringsnotatets punkt 9.3 og 11.7.2.

I den særskilte meldingen til Stortinget av juni 2016 stilte EOS-utvalget spørsmål ved Etterretningstjenestens rettsgrunnlag for å foreta loggsøk i lagrede metadata med utgangspunkt i en selektor tilhørende norsk person i Norge, i den hensikt å identifisere selektorer i utlandet for utenlandsetterretningsformål. Utvalget la til grunn at dagens § 4 første ledd kan begrense tjenestens mulighet til å innhente informasjon av slik utenlandsetterretningsmessig relevans.

8.7.1.2 Målsøking

Målsøking er en av Etterretningstjenestens viktigste aktiviteter. Denne type søk kan være nødvendig for blant annet å avdekke etterretningsmål i utlandet som kommuniserer med personer i Norge, eller for å avdekke personer eller virksomheter i Norge som er utsatt for angrep eller påvirkning fra en fremmed trusselaktør. I slike tilfeller vil søket eksempelvis ta utgangspunkt i et telefonnummer, e-postadresse, eller brukernavn på en gitt adresse som tilhører den norske personen, for å avdekke hvilke selektorer i utlandet som har vært i forbindelse med denne. Metadatasøk i målsøkingsøyemed gir dermed Etterretningstjenesten mulighet til å avdekke nye trusselaktører i utlandet som kommuniserer med norske personer, slik at tjenesten kan fremskaffe kritisk informasjon om grenseoverskridende trusler for å kunne verne Norge og norske interesser. Aktiviteten er således også en forutsetning for å kunne gjennomføre påfølgende målrettet fordekt innsamling, og kan på den måten redusere eventuelle unødvendige inngrep i individers privatliv. Dette er fordi man gjennom målsøkingsaktivitet kan selektere ut de etterretningsmål som vurderes å ha størst

etterretningsverdi, og dermed unngå å gå unødvendig bredt ut i en tidlig innsamlingsfase. Denne type målutvikling har ikke bare verdi innenfor kontraterrorarbeidet, men har også betydning for avverging og oppfølging av alvorlige cyberhendelser. Dette kan illustreres med et eksempel der en norsk IP-adresse som har vært utsatt for en alvorlig cyberhendelse kan brukes som inngangsverdi for å forsøke å finne kommunikasjon til og fra denne IP-adressen, noe som igjen kan bidra til å identifisere en fremmed aktørs spionasje og denne aktørens *modus operandi*.

Departementet viser til at andre land har vurdert behovet tilsvarende, og understreket at slike søk ikke medfører innhenting av *ny* informasjon. Metadatasøk med utgangspunkt i nasjonale selektorer ble forklart slik av den daværende amerikanske etterretningssjefen for noen år siden:[190]

> "To 'query' means to take a term, such as a name, phone number or email address, and use it to isolate communications with that term from a larger pool of data an agency has already lawfully collected. Queries do not result in the additional collection of any information. Rather, they allow an agency to rapidly and efficiently locate foreign intelligence information, such as information potentially related to a terrorism plot against the United States, without having to sift through each and every communication that has been collected."

I dette ligger det at søket i seg selv ikke fører til at det fordekt innhentes ny informasjon; søket selekterer kun ut relevante metadata fra en stor samling av allerede innhentede rådata. Fordekt-begrepet i etterretningstjenesteloven § 4 første ledd er som tidligere påpekt blitt tolket som å relatere seg til innsamlingsmetoden, ikke til etterfølgende analyse og sammenstilling av informasjon. Departementet vektlegger derfor at slike loggsøk i allerede innsamlet kommunikasjonsdata skjer uten at innhentingen *rettes mot* personen eller virksomheten i Norge, hvilket for øvrig må kunne dokumenteres før og etter gjennomføringen av søket, og at det dermed ikke foreligger en overvåkningshensikt overfor disse i § 4 første ledds forstand. Videre utføres loggsøkene i etterkant av innsamlingen, slik at søkene de facto kun utgjør seleksjon og sammenstilling av allerede innsamlet informasjon. Fordelen med fremgangsmåten er at istedenfor å måtte rette utallige spørringer mot datamaterialet med utgangspunkt i utenlandske selektorer for å undersøke treff mot Norge vil man langt mer tidseffektivt kunne ta utgangspunkt i den norske selektoren og undersøke om denne har kommunisert med for eksempel en selektor i et særskilt konfliktområde, for å identifisere mulige selektorer i dette området som bør gjøres til gjenstand for nærmere undersøkelser av Etterretningstjenesten.

Departementet anser ikke at aktiviteten er i strid med någjeldende etterretningstjenestelov § 4 første ledd, men ser at bestemmelsens ordlyd åpner for tolkningsspørsmål.

---

[190] Brev av 27. juni 2014 fra Office of the Director of National Intelligence (ODNI) til senator Ron Wyden. Det fremgår av samme brev at NSA i 2013 foretok slike søk med utgangspunkt i "U.S. person identifiers" 198 ganger for søk i *innholdsdata* og ca. 9500 ganger for søk i *metadata*. Det amerikanske "Privacy and Civil Liberties Board" (PCLOB) har i en rapport av 2. juli 2014 ("Report on the Surveilleance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act") konkludert med at slike søk ikke strider mot den amerikanske grunnloven eller amerikansk lovgivning. PCLOB anbefaler at muligheten til å foreta slike søk opprettholdes, men at det i internt regelverk bør klargjøres at dette kun kan skje "based upon a statement of facts showing that it is reasonable likely to return foreign intelligence information", og at NSA og CIA bør utvikle skriftlige retningslinjer, med eksempler, som tydeliggjør hvilken informasjon/dokumentasjon som er påkrevet for å møte denne standarden.

8.7.2 Presisering inntatt i lovteksten

Departementet har vurdert behovet og begrunnelsen for å kunne gjennomføre søk som beskrevet over, samt behov for en tydeligere lovhjemmel. Departementet har i denne forbindelse lagt avgjørende vekt på at loggsøkene er rettet mot utenlandske forhold og at det ikke foreligger overvåkningshensikt mot personen eller virksomheten i Norge. Slik søkene innrettes – og selv om de tar utgangspunkt i en selektor tilknyttet en person eller virksomhet i Norge, er de ikke rettet mot å fremskaffe informasjon om disse, eller om innenlandske forhold knyttet til deres kontakter eller aktiviteter. Formålet er å finne frem til nye eller hittil ukjente trusselaktører i utlandet som er i kontakt med den norske selektoren, altså ikke å fremskaffe opplysninger om den norske personens eller virksomhetens aktivitet i Norge. Søkene må vurderes som en forberedende aktivitet hvis formål er å frembringe nødvendig grunnlagsmateriale slik at tjenesten på et senere tidspunkt kan iverksette innsamling mot et aktuelt mål i utlandet.

Departementet har som et alternativ vurdert hvorvidt innsamlingen kan foretas av PST i medhold av deres rettsgrunnlag. PST er ingen utenlandsetterretningstjeneste, og har ikke noen rettslig mulighet til å innhente metadata som antas å kunne frembringe utenlandsetterretningsrelevant informasjon. Etterretningstjenestens målsøking gjennom denne type loggsøk innebærer således etter departementets syn ingen omgåelse, ettersom PST verken kan eller skal besvare slike informasjonsbehov. Videre må metoden ses i en kontekst der Etterretningstjenesten og PST er lovpålagt å samarbeide tett for å avverge og forebygge trusler mot Norge. Gjennom loggsøkene kan Etterretningstjenesten bidra til å dekke en viktig brikke i etterretningsbildet, nemlig ved å avdekke eventuelle forbindelser mellom utenlandske trusselaktører og norske personer eller virksomheter i Norge. Dersom Etterretningstjenesten ikke skal kunne utføre denne form for loggsøk, er det ingen andre norske myndigheter som har mandat eller kapasitet til å gjøre det. Det vil kunne medføre at norske myndigheter ikke besitter et godt nok situasjons- og etterretningsbilde hva gjelder grenseoverskridende cyber- og terrortrusler. Under Stortingets debatt om EOS-utvalgets særskilte melding 21. februar 2017, ble det anført at det var behov for å tilpasse Etterretningstjenestens virkemidler for overvåkning. De beskrevne loggsøkene i innsamlet rådata, er etter departementets syn et illustrerende eksempel på et virkemiddel som i dag tas i bruk på bakgrunn av den tekniske utviklingen og som en direkte følge av det nye grenseoverskridende trusselbildet. Under stortingsdebatten ble det særlig fremhevet at Etterretningstjenesten må være utrustet med de virkemidlene og det lovgrunnlaget som de behøver for å utføre oppdraget som de er forventet å utføre. Departementet slutter seg til dette, og vektlegger Etterretningstjenestens behov for denne type målsøkingsaktivitet for å kunne løse sitt lovpålagte oppdrag.

Departementet ser behov for at Etterretningstjenesten gis en tydeligere og klarere lovhjemmel for å kunne utføre søk i rådata med utgangspunkt i en personselektor som kan knyttes til en person som omfattes av ny § 4-1. Herunder vektlegges at selv om søket i seg selv ikke er *rettet mot* personen i Norge, vil det likevel kunne utgjøre et inngrep i vedkommendes personvern. Dette fordrer at det foreligger en klar lovhjemmel for inngrepet. Av denne grunn, og fordi tiltaket vil berøre personer og virksomheter i Norge, foreslås det også å innta et forhøyet terskelvilkår for å gjennomføre loggsøket, ved å innta et krav om at søket må vurderes å ha eller kunne få *vesentlig* betydning for ivaretakelsen av Etterretningstjenestens oppgaver. Hva som er av vesentlig betydning må vurderes fra sak til sak, men det må vektlegges særskilt om det finnes alternative metoder å fremskaffe

informasjonen på, hva saken gjelder, eksempelvis kontraterror, cybertrusler eller kontraproliferasjon, og tidshensynet.

Departementet foreslår følgende lovtekst til § 4-2 syvende ledd:

> Søk i rådata med utgangspunkt i en personselektor som kan knyttes til en person som omfattes av § 4-1, kan gjennomføres dersom søket ikke er rettet mot denne personen og søket anses å ha eller kunne få vesentlig betydning for ivaretakelsen av Etterretningstjenestens oppgaver etter kapittel 3.

8.8 Nærmere om innhenting gjennom åpne kilder (lovutkastet § 4-2 åttende ledd)

8.8.1 Generelt

Ettersom etterretningstjenesteloven § 4 første ledd kun gjelder *fordekt* innhenting om norske personer og virksomheter i Norge, vil ikke innhenting av åpent tilgjengelig informasjon være omfattet av forbudet. 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.

Departementet vil presisere at, på samme måte som for all annen informasjonsinnhenting, må innhenting av åpent tilgjengelig informasjon alltid være begrunnet i Etterretningstjenestens oppdrag, altså rettet mot utenlandsetterretningsrelevante forhold. Åpne kilder, eller såkalt *Open Source Intelligence (OSINT)*, beskriver innsamling og bearbeiding av fritt tilgjengelig informasjon i etterretningsøyemed. Denne innhentingsmetoden foreslås nå hjemlet i lovens § 6-2.

8.8.2 Innhenting gjennom åpne kilder etter gjeldende rett – forholdet til den territorielle begrensningen

Ettersom innhenting fra åpne kilder ikke er å anse som overvåkning eller fordekt innhenting etter gjeldende etterretningstjenestelov, må metoden i dag ikke underlegges samme vurdering av territoriell tilhørighet som fordekte innhentingsdisipliner. Innhentingen må likevel være rettet mot utenlandske forhold, i tråd med etterretningstjenestelovens føringer i §§ 1 og 3. Når det gjelder informasjon som ligger åpent tilgjengelig på Internett vil det fremstå som tilfeldig om legaliteten knyttet til åpen innsamling om utenlandske etterretningsmål via norske personers sosiale nettsteder, skal avhenge av om den norske personen rent faktisk befinner seg i utlandet eller i Norge, eller hvorvidt det angjeldende nettstedet har norsk domenenavn eller lignende. Det er heller ikke gitt at Etterretningstjenesten gjennom åpent tilgjengelig informasjon kan fastslå hvorvidt den norske personen oppholder seg i Norge eller i utlandet. Ettersom nettbasert informasjon vanskelig kan sies å «befinne seg» på norsk territorium eller i utlandet, og det ikke anses hensiktsmessig å knytte slike vurderinger til domenenavn, serverlokasjon eller til lokasjonen av personen som opprinnelig publiserte informasjonen, må

den bestemmende forutsetningen for Etterretningstjenestens innhenting fra åpne kilder være at det innhentes mot utenlandske forhold eller personer.

Dette innebærer at man i dag vurderer at Etterretningstjenesten kan benytte åpent tilgjengelig informasjon som den besitter, herunder opplysninger om norske personer eller virksomheter, som grunnlag for å rette innhenting mot utenlandske forhold eller personer. Eksempelvis vil søk kunne foregå på sosiale medier til norske personer, for eksempel fordi disse har hatt kontakt med terroristnettverk i utlandet. Ved slike søk kan det ikke legges til grunn at Etterretningstjenesten utviser noen overvåkningshensikt i relasjon til personen eller virksomheten i Norge, all den tid formålet er å innhente informasjon om relevante utenlandske kontakter, i den utstrekning disse kontaktene faller innenfor innsamlingsformålet. Innsamlingsaktiviteten er da følgelig ikke *rettet mot* en personen i Norge, men mot utenlandsetterretningsrelevante forhold. Dersom det innhentes informasjon som er publisert av eller berører personer i Norge, eller som befinner seg på sosiale profiler, hjemmesider eller lignende som er knyttet til personer eller virksomheter i Norge, og formålet med innhentingen er å belyse vedkommendes innenlandske forhold, kontaktnettverk eller aktivitet, vil imidlertid innhentingen være i strid med dagens etterretningstjenestelov §§ 1 og 3.

8.8.3 Presisering inntatt i lovteksten

Ettersom åpent tilgjengelig informasjon på Internett vanskelig kan sies å «befinne seg» på norsk territorium eller i utlandet, og Etterretningstjenesten tidvis vil ha behov for å ta utgangspunkt i informasjon knyttet til personer eller virksomheter i Norge for å belyse relevante utenlandske forhold eller trusler, anser departementet det som formålstjenlig å lovfeste et vilkår om at slik innhenting skal ha et utenlandsetterretningsfokus. Departementet finner samtidig behov for å innta en presisering i utkast til § 4-2 åttende ledd at slik innhenting ikke er å anse som rettet mot person eller virksomhet i Norge. Presiseringen foreslås for å unngå tolkningstvil.

På samme måte som etter gjeldende rett bør innhentingsaktivitet som knytter seg til personer eller virksomheter i Norge, der formålet med innhentingen er å belyse innenlandske forhold, etter departementets syn være i strid med innhentingsforbudet i ny § 4-1, ettersom denne bestemmelsen også omfatter innhenting gjennom åpne kilder. Departementet understreker at alle opplysninger som Etterretningstjenesten kommer over om rene innenlandske forhold og innenlandsk aktivitet i forbindelse med innhenting som er rettet mot utenlandske forhold, er å anse som overskuddsinformasjon som tjenesten skal slette, eventuelt oversende relevant norsk myndighet i tråd med reglene om deling av informasjon i lovforslaget kapittel 10.

Departementet tilrår følgende lovtekst til ny § 4-2 åttende ledd:

> Dersom formålet med innhentingen er rettet mot forhold eller personer i utlandet, er innhenting av informasjon gjennom åpne kilder ikke å anse som rettet mot personer eller virksomhet i Norge, selv om det innhentes informasjon som er publisert av eller berører personer i Norge eller som befinner seg på sosiale profiler, hjemmesider eller lignende media som er knyttet til personer i Norge.

8.9 Forbud mot industrispionasje – begrepsbruk og presiseringer (lovutkastet § 4-3)

De senere år har man sett en gryende sedvanerettsutvikling knyttet til et folkerettslig forbud mot såkalt industrispionasje mellom stater. Forbudet omfatter primært cyberbasert tyveri av åndsverk, handelshemmeligheter eller annen konfidensiell forretningsinformasjon, med det formål å gi et konkurransemessig fortrinn til kommersielle virksomheter eller sektorer. Det er inngått bilaterale avtaler mellom Kina og henholdsvis USA i 2015 og Canada og Australia i 2017, som forbyr denne type spionasje mellom statene. Tilsvarende ble avtalt mellom Storbritannia og Kina i 2015, da de avga en felles uttalelse om at de ikke ville utføre slik spionasje overfor hverandre. Sedvanerettsdannelsen viser seg også gjennom felles uttalelser, eksempelvis fra G20-landenes ledere, som i 2015 avga en erklæring der det i avsnitt 26 fremgår følgende:

> "In the Information Communication Technology (ICT) environment, just as elsewhere, states have a special responsibility to promote security, stability, and economic ties with other nations. In support of that objective, we affirm that no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[191]

Norge har tilsluttet seg samme norm, blant annet gjennom fellesuttalelse av 14. september 2016 fra de tredje nordisk-baltisk-amerikanske cyberkonsultasjoner.

De bilaterale avtalene som de senere år er inngått, samt felleserklæringene som er avgitt, kan sies å reflektere en mellomstatlig regel som har oppstått som følge av en felles forståelse blant et økende antall sentrale stater. Forbudet omfatter bevisst ikke tradisjonell etterretning og andre aktiviteter knyttet til nasjonal sikkerhet, men skiller disse aktivitetene fra den rene industrispionasjen som omfattes av forbudet. Denne folkerettsutviklingen samsvarer med de rettslige rammene som i dag er gitt for Etterretningstjenesten, ettersom nåværende § 3 ikke hjemler slik innhenting. Det er departementets syn at en ny lov for Etterretningstjenesten bør reflektere denne utviklingen. Forbudet vil ikke innskrenke eller hindre tjenestens mulighet til å innhente økonomiske og finansielle opplysninger som kan belyse de nærmere definerte oppdragene som fremgår av Etterretningstjenestens oppgavesett etter lovutkastet kapittel 3.

Forbudet vil ikke bare gjelde innhenting av slik informasjon, men også bearbeiding eller utlevering av slik informasjon.

Departementet tilrår at følgende forbud mot industrispionasje inntas i ny § 4-3:

§ 4-3 *Forbud mot industrispionasje*

Etterretningstjenesten skal ikke innhente eller medvirke til å innhente, bearbeide eller utlevere informasjon med formål å gi selskaper eller andre kommersielle virksomheter eller sektorer konkurransemessige fortrinn.

[191] G20 Leader´s Communique Antalya Summit, 15-16 November 2015.

8.10 Forbud mot å utføre oppgaver med politiformål – begrepsbruk og presiseringer (lovutkastet § 4-4)

8.10.1 Gjeldende rett

Etterretningstjenesten kan i dag, på lik linje med resten av Forsvaret, bli anmodet om å bistå politiet etter politiloven[192] § 27 a. Anmodningsoppdraget utføres i henhold til politiets mandat og rettsgrunnlag. Dette er i overensstemmelse med det etablerte skillet mellom Etterretningstjenesten og PST og politiet. Etterretningstjenesten innhenter informasjon for å avdekke og motvirke utenlandske trusler, og innsamler informasjon om andre utenlandske forhold for å gi norske myndigheter et best mulig beslutningsgrunnlag. Formålet med denne virksomheten er ikke å forebygge eller bekjempe kriminalitet, da dette er oppgaver som tilligger PST og politiet for øvrig. Formålsavgrensningen har betydning med tanke på mulig omgåelsesproblematikk. Det betyr at EOS-tjenestene ikke skal utføre oppgaver for hverandre på en måte som innebærer en omgåelse av lovgivningen. EOS-utvalget har særlig fokus på dette i forbindelse med sine inspeksjoner av Etterretningstjenesten og PST, og kontrollerer at de to tjenestene opererer ut fra eget rettsgrunnlag og ikke løser oppdrag på vegne av hverandre, eksempelvis fordi deres eget rettsgrunnlag kanskje ikke åpner for en gitt metode eller oppdrag.

8.10.2 Departementets vurdering

Departementet mener det er formålstjenlig å lovfeste et forbud mot at Etterretningstjenesten utfører oppgaver med politiformål i loven. En slik avgrensning av Etterretningstjenestens mandat viser tydelig at tjenesten ikke skal kunne samarbeide med PST eller politiet på en slik måte at tjenestens metoder eller kapasiteter brukes *for det formål* å oppfylle PSTs eller politiets mandat.

Departementet vektlegger samtidig at Etterretningstjenesten og PST er pålagt å samarbeide nært på en rekke prioriterte områder, herunder innen kontraterror, kontraproliferasjon og kontraetterretning, gjennom instruks om samarbeid mellom Etterretningstjenesten og Politiets sikkerhetstjeneste av 2006.[193] Økt samarbeid har politisk vært en ønsket utvikling, og nevnte instruks pålegger tjenestene å effektivt møte aktuelle trusler og sikkerhetsutfordringer gjennom informasjonsutveksling, samhandling og arbeidsdeling. De to tjenestene samarbeider også i økende grad i egne samarbeidssentre, slik som Felles kontraterrorsenter (FKTS) som ble opprettet i 2014 og Felles cyberkoordineringssenter (FCKS) som ble opprettet i 2017. Tettere samhandling og samarbeid mellom utenlandsetterretning, innenlandsetterretning og politi er en klar trend i de fleste vestlige demokratier, og er en direkte konsekvens av grenseoverskridende trusler og kommunikasjonsteknologi. Utveksling av informasjon og samarbeid i generelle og konkrete saker er derfor avgjørende for å lykkes i arbeidet med å avdekke og motvirke trusler mot Norge. Både Etterretningstjenesten, PST og politiet må ut fra sine respektive rettsgrunnlag bidra til å dekke etterretnings- og situasjonsbildet på en slik måte at arbeidsdelingen er formålstjenlig og resultatet er en adekvat statlig innsats mot prioriterte trusler og

[192] Lov av 4. august 1995 nr. 53 om politiet

[193] Instruks av 13. oktober 2006 nr. 1151 om samarbeidet mellom Etterretningstjenesten og Politiets sikkerhetstjeneste («Samarbeidsinstruksen»)

sikkerhetsutfordringer. Departementet vektlegger derfor at Etterretningstjenesten må kunne dele informasjon som den har innhentet for etterretningsformål, med politiet eller andre norske myndigheter.

Departementet ser ingen grunn til å foreslå endringer i nåværende oppgavefordeling mellom Etterretningstjenesten og PST, men ser behov for å understreke nødvendigheten av et nært og tillitsfullt samarbeid mellom Etterretningstjenesten, PST og andre rettshåndhevende myndigheter. Departementet vektlegger at denne form for samarbeid, både etter samarbeidsinstruksen, og innenfor rammen av FKTS og FCKS, kan utføres uten at Etterretningstjenesten skal utføre oppgaver for politiformål. Etterretningstjenesten skal samarbeide og utføre sine oppgaver innenfor eget rettsgrunnlag, med mindre politiet anmoder tjenesten om bistand etter politiloven § 27 a. Sistnevnte er også nevnt under punkt 5.2.2.

Departementet anbefaler at gjeldende rettstilstand videreføres, men at denne nå lovfestes i utkast til ny § 4-4:

§ 4-4 *Forbud mot å utføre oppgaver med politiformål*

Etterretningstjenestens virksomhet skal ikke ha som formål å løse kriminalitetsforebyggende eller kriminalitetsbekjempende oppgaver som tilligger politiet eller andre norske rettshåndhevende myndigheter.

At informasjon innhentet for etterretningsformål også kan være relevant for politiet eller andre norske rettshåndhevende myndigheter, er ikke i strid med forbudet etter første ledd. Det samme gjelder at Etterretningstjenesten kan bistå politiet innenfor politiets rettsgrunnlag i medhold av politiloven § 27 a og § 10-3 i loven her.

9 Grunnvilkår for informasjonsinnhenting

9.1 Innledning

Mens hensikten med kapittel 7 om Etterretningstjenestens oppgaver er å definere og avgrense for hvilke *formål* tjenesten kan innhente informasjon, er hensikten med kapittelet her å definere hvilke *andre grunnleggende vilkår* som må være oppfylt før Etterretningstjenesten kan igangsette informasjonsinnhenting.

Det understrekes innledningsvis at Etterretningstjenestens informasjonsinnhenting ikke skjer for straffeavvergings- eller straffeforfølgingsformål, men for å redusere usikkerhet hos beslutningstakere og svare på norske myndigheters informasjonsbehov. Norske myndigheter har behov for informasjon om utenlandske trusler og forhold av betydning for norske grunnleggende interesser på et tidligst mulig tidspunkt. Det må videre tas i betraktning at *før* informasjon er innhentet, kan det ofte være svært vanskelig eller tilnærmet umulig å vite om informasjonen er relevant for Etterretningstjenestens oppgaveløsning. I tillegg kommer at etterretningstjenester ofte må gå bredt ut og snevre inn informasjonssøkingen etter hvert. Det følger av at den relevante informasjonen og de relevante etterretningsmålene ofte ikke er kjent på forhånd. Nettopp det å finne de ukjente etterretningsmålene, skjer i en prosess som kalles *målsøking*.[194] Det er først når man har funnet relevante etterretningsmål at man kan spisse innsamlingen målrettet mot disse.

[194] Se også punkt 8.7.1.2.

Denne prosessen kalles *målrettet innhenting*. Terskelen for å innhente informasjon som ledd i målsøking må derfor være noe lavere enn terskelen for målrettet innhenting.

Det er krevende å lovgi presist om de generelle grunnvilkår for innhenting. Det skyldes blant annet at hvilke grunnleggende vilkår som må være oppfylt før informasjonsinnhenting kan skje for etterretningsformål, både må ta hensyn til de ulike oppgavene Etterretningstjenesten er pålagt og til ulikt fokus og informasjonsbehov innenfor hver av disse oppgavene. Grunnvilkårene må også ta høyde for den kontekst som innhentingen skjer i. Innhentingsfokus kan spenne fra det taktiske, f.eks. om og hvor det er utplassert eksplosiver (IEDer) på en veiakse i et avgrenset geografisk område, til det storstrategiske, f.eks. om en stat har langsiktige planer om å etablere et spesielt våpenprogram. Aksen strategisk-operasjonelt-taktisk glir likevel over i hverandre; taktisk informasjon kan informere strategiske vurderinger, og strategisk etterretning kan være med på å spisse de taktiske informasjonsbehov.

For all informasjonsinnhenting vil det være et viktig prinsipp at innhenting og videre bruk av informasjon bare kan skje dersom dette anses *forholdsmessig*, etter en avveining mellom formålet og viktigheten av handlingen på den ene siden, og karakteren og omfanget av handlingens inngrep overfor enkeltpersoner på den andre siden. Hvorvidt det foreligger alternative og mindre inngripende måter å frembringe informasjonen på er et viktig moment i denne vurderingen. En generell forholdsmessighetsbestemmelse foreslås lovfestet. Bestemmelsen 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.

9.2 Grunnleggende karaktertrekk ved informasjonsinnhenting for etterretningsformål

9.2.1 Generelt

De grunnleggende karaktertrekkene ved informasjonsinnhenting for etterretningsformål legger premissene for hvordan grunnvilkårene kan og bør formuleres i loven. Gjeldende lov har ingen slike lovfastsatte grunnvilkår, og departementet mener derfor det er grunn til å utdype forutsetningene i noe mer detalj før man går over til den konkrete utformingen av forslag til lovbestemmelser.

9.2.2 Hva kjennetegner utenlandsetterretning?

9.2.2.1 Generelt

Etterretningstjenester er av natur og fag «samlere» av informasjon. Etterretningsvirksomhet er i mange tilfeller et møysommelig puslespill som krever behandling og sammenstilling av informasjon fremkommet gjennom mange kilder og ved ulike metoder over lang tid. Det er kun på denne måten den nødvendige, helhetlige og forsvarlige kunnskapen en etterretningstjeneste trenger etableres, og informasjonsgrunnlaget er en forutsetning for å kunne utarbeide korrekte og oppdaterte trusselanalyser og etterretningsvurderinger.

Innhenting av informasjon skjer ofte gjennom sammenstilling av fragmentariske informasjonsbiter gjennom år og tiår. Dette langsiktige perspektivet, sammenholdt med fokuset på utenlandske forhold, er noe av det som kjennetegner Etterretningstjenestens

virke. Virksomheten er tid- og ressurskrevende, og fordrer at opplysninger oppbevares og analyseres med en langsiktig horisont selv om relevansen av informasjonen på lagringstidspunktet isolert sett kan synes meget lav. Ofte kreves en langsiktig oppbygging av og forståelse for et normalsituasjonsbilde, for å kunne detektere avvik fra det normale.

9.2.2.2 Utenlandsetterretning er ikke kriminalitetsbekjempelse

Det hender ikke sjelden at noen trekker den grunnleggende feilslutningen at innhenting for etterretningsformål må være basert på mistanke eller lignende individualbaserte terskler for innhenting og behandling av informasjon, etter analogi fra justissektoren og straffeprosessen. Departementet understreker at en slik analogi ikke kan trekkes. Bakgrunnen for dette er at utenlandsetterretningstjenester skiller seg grunnleggende fra politiorganer, både hva gjelder formål og virksomhet, selv om informasjonsbehovet i visse tilfeller tilsynelatende kan være sammenfallende. Mens tradisjonelle politiorganer og rettshåndhevende myndigheter (law enforcement) fokuserer på å bygge opp en juridisk sak relatert til en kriminell handling som er begått eller forberedes begått (historisk perspektiv med stor vekt på beviskjede), er etterretningstjenesters fokus å redusere usikkerhet hos viktige beslutningstakere, med et særlig fokus på å predikere fremtiden – å vurdere fremmede trender og handlinger hos stater, organisasjoner og personer, uavhengig av om disse har gjort eller vil gjøre noe straffbart, og uten å være styrt av å måtte beskytte informasjonens integritet på en slik måte at den kan benyttes i en rettslig prosess. Etterretningstjenestens innhentingstiltak er ikke tvangsmidler, selv om metodene på enkelte områder kan sammenlignes med politiets metoder. For å finne de ukjente aktørene og antatt relevant informasjon som man ikke vet hvor befinner seg, vil man måtte gå bredt ut og snevre inn etter hvert. Det ligger også i sakens natur at målrettet innhenting vil måtte rettes mot personer og organisasjoner som ikke er involvert i noen aktivitet som norske myndigheter ønsker å motvirke. Om vedkommende har begått, vil begå eller aldri har begått et straffbart forhold er uten betydning for vurderingstemaet om en utenlandsetterretningstjeneste kan iverksette innhentingstiltak mot en person, organisasjon eller aktivitet. Det avgjørende er om vedkommende besitter, kommuniserer eller vil motta, eller om innhenting på annen måte kan frembringe, informasjon som er relevant for løsningen av Etterretningstjenestens lovpålagte oppdrag.

9.2.2.3 Man må lete etter informasjonen der den befinner seg

Mengden tilgjengelig informasjon har økt betydelig de senere år, og øker fortsatt eksponentielt. Bulkinnsamling av informasjon, se punkt 9.5.6 nedenfor om dette, har blitt en nødvendig og daglig del av alt etterretningsarbeid som retter seg mot å finne elektronisk informasjon. Papirdokumenter og papirarkiver er i en moderne digital tidsalder mindre viktige. Den relevante elektroniske informasjonen lagres og transporteres i dag i lokale, regionale og globale nett sammen med all annen ikke-relevant elektronisk informasjon. Å trekke ut den relevante informasjonen fra den ikke-relevante mengden og strømmen av data er meget krevende, og fordrer ikke sjelden at man av teknologisk nødvendighet først må ha tilgang til, og bearbeide, hele datasett for i det hele tatt å forstå hva som er relevant og hva som ikke er relevant. Analyse og prosessering av tilgjengelig informasjon er dessuten krevende, og fordrer i dag støtte i form av maskinell behandling og moderne analyse- og prosesseringsverktøy. Dataminimalisering (å redusere mengden data til kun det som er relevant) av selve mengden data som Etterretningstjenesten trenger tilgang til forut for å gjennomføre målrettede søk og målrettet innhenting, vil sjelden være teknisk og praktisk mulig, selv om dette både av personvernhensyn og effektivitetshensyn er ønskelig. Ettersom

det forut for en bulkinnsamling vanskelig eller umulig kan positivt anslås hvilke opplysninger i mengden som er relevant for tjenestens oppdrag, vil dataminimalisering på dette tidspunktet være ødeleggende for formålet med etterretning.

Det er et grunnleggende poeng at man må lete etter informasjon der hvor den relevante informasjonen mest sannsynlig finnes. I dag er den informasjonen som Etterretningstjenesten trenger for å løse sitt oppdrag som oftest sammenblandet med og i datasamlinger og datastrømmer hvor det aller meste ikke er relevant for etterretningsformål. Forutgående dataminimalisering kan kanskje være ønskelig fra et personvernperspektiv, og Etterretningstjenesten søker så langt mulig å gjøre et utvalg så tidlig som mulig. Blant annet vil tjenesten velge ut de kommunikasjonsstrømmer som antas å inneholde mest mulig relevant informasjon. Men et slikt utvalg vil likevel ikke kunne hindre at det må innhentes datasamlinger som også inneholder ikke-relevant informasjon. Fra et etterretningsperspektiv er det ingen alternativer til dette. Før omfattende mengder data er lagret og analysert, kan man ikke vite hvilke data som det er nødvendig å behandle for oppgaveløsningen. Etterretning er kunsten å finne og tolke de relevante data, men da må man først kunne lete der disse finnes. Det er ikke mulig å gjøre et utvalg forut for tolkningen av rådata og analysen av hva som har etterretningsverdi fordi man på dette tidspunktet ikke har de riktige utvalgsparametere som kan snevre inn utvalget. I dette perspektivet er datamaksimalisering viktigere enn dataminimalisering. Det er først når potensielt relevante data trekkes ut av en større mengde grunndata, at dataminimalisering blir både mulig og ønskelig – både av hensyn til personopplysningsvernet og av hensynet til å få mest mulig effektiv etterretningsinnsats ut av begrensede analyseressurser.

Etterretningsvirksomhet er i vesentlig grad informasjonsorientert snarere enn personorientert. Dette gjelder innenfor hele oppgavesettet, også på kontraterrorfeltet. Tjenesten innhenter relevant informasjon der den finnes og der det er lettest å frembringe denne. For en etterretningstjeneste er det irrelevant om personer som tjenesten innhenter informasjon om, gjennom eller ved hjelp av, er mistenkt for å planlegge eller ha begått straffbare handlinger. Etterretningstjenestens oppdrag er ikke og skal heller ikke være styrt av å innhente opplysninger om handlinger som etter norsk rett faller inn under en straffebestemmelse. Det er politiets oppgave. Det avgjørende er om innhenting kan fremskaffe utenlandsetterretningsrelevant informasjon for å tilfredsstille norske myndigheters kritiske informasjonsbehov. Det er derfor mindre stigmatiserende å havne i søkelyset til en etterretningstjeneste sammenlignet med å havne i søkelyset til politiet.

9.2.2.4 Sikkerhetsbevissthet

Mange relevante etterretningsmål er svært sikkerhetsbevisste, noe som medfører at Etterretningstjenesten må tilnærme seg målene indirekte ved å innhente informasjon om personer og forhold som relaterer seg til målene, men som ikke er relevante etterretningsmål i seg selv. Etterretningstjenesten vil således kunne hente inn informasjon ad omveier og rette innhentingen mot personer som i seg selv ikke er involvert i aktivitet som er av etterretningsmessig interesse, men som likevel besitter eller har eller kan få tilgang til etterretningsrelevant informasjon, for eksempel fordi de befinner seg i personkretsen rundt etterretningsmålet. I enkelte tilfeller innebærer dette at det kan være svært vanskelig eller umulig å innrette seg på en måte som hindrer at man blir gjenstand for informasjonsinnhenting, med unntak for norske borgere i Norge eller virksomheter i Norge som tjenesten etter lovforslaget § 4-1 ikke kan rette informasjonsinnhentingen mot.

9.3 Målsøking og målrettet innhenting – forslag til definisjoner i lovutkastet § 1-4

9.3.1 To hovedkategorier innhenting

Etterretningstjenesten innhenter informasjon med to ulike utgangspunkter; Informasjon innhentes for å kartlegge målmiljøer og identifisere nye etterretningsmål, dette kalles *målsøking*. Når man har identifisert legitime etterretningsmål pågår innhentingen over tid for å finne mest mulig informasjon om etterretningsmålene og deres intensjoner, aktiviteter og nettverk. Dette kalles *målrettet innhenting*.

Målsøking er i lovutkastet § 1-4 nr. 9 definert som «systematisk arbeid for å identifisere nye etterretningsmål». Målrettet innhenting er i lovutkastet § 1-4 nr. 8 definert som «systematisk arbeid for å finne informasjon knyttet til identifiserte etterretningsmål». Begge formene for innhenting gjennomføres som søk i metadata eller innholdsdata, eller begge deler.

De to utgangspunktene for innsamling glir imidlertid av og til over i hverandre. Målrettet innhenting kan ha elementer av målsøking, særlig når man forsøker å identifisere nye etterretningsmål i kretsen rundt et allerede etablert etterretningsmål. Målsøking på sin side leder frem til nye etterretningsmål som det vurderes å gjennomføre målrettet innhenting mot. For eksempel vil man i det digitale rom ha et kontinuerlig fokus på å knytte ulike digitale identiteter til ett og samme etterretningsmål for å oppnå et mest mulig dekkende bilde av etterretningsmålet. Det kan være en smakssak om denne prosessen for å finne mer informasjon rundt allerede kjente mål skal karakteriseres som målsøking eller målrettet innhenting. Etterretningstjenesten benytter begrepet mål*utvikling* om dette, som i denne sammenheng er en underkategori av målrettet innhenting. Departementet ser ikke grunn til å benytte begrepet målutvikling i lovutkastet, men holder seg til de to hovedkategoriene.

9.3.2 Nærmere om målsøking

Målsøking er altså prosessen for å finne *nye* trusselaktører eller andre legitime etterretningsmål som hittil ikke er kjent. Målsøking er grunnstammen i og forutsetningen for all etterretningsvirksomhet fordi nettopp det å identifisere og vurdere *ikke-kjente* trusler og andre utenlandske forhold som er av betydning for landets sikkerhet og nasjonale myndigheter er en helt sentralt oppgave for Etterretningstjenesten.

Normalt gjøres målsøking basert på historiske data supplert med sanntids- og andre data, i den utstrekning man har tilgang til slike, og disse dataene vurderes relevante. Målsøking forutsetter at det foreligger et inngangsparameter; en form for ledetråd. En ledetråd kan for eksempel være et telefonnummer til en nylig avslørt terrorist som Etterretningstjenesten har fått av en samarbeidende tjeneste. Tjenesten vil da umiddelbart prøve å finne ut forhold slik som følgende:

- Har aktøren være i kontakt med andre trusselaktører man ikke kjenner til?
- Har aktøren andre identifikatorer (e-postadresser osv.)?

For å kunne gjøre disse analysene er historiske data avgjørende, også fordi telefonnummeret i mange tilfeller ikke lenger er i bruk. Ved å nøste i den historiske aktiviteten kan andre ledetråder komme frem, som er avgjørende for å gi etterretningsinformasjon som kan bidra til at ansvarlige myndigheter kan rette inn sine

virkemidler, rulle opp nettverket og forhindre en trussel. Mange målsøkingprosesser er mer komplekse enn eksemplet ovenfor, da både teknologien og trusselaktørene blir stadig mer avanserte, men det gir likevel et bilde av de viktigste aspektene innen målsøking.

Målsøkingsprosessen begynner der et oppdrag skal operasjonaliseres og innsamlingsmål blir utledet. Formålet med prosessen er å oppnå tilgang til informasjon fra organisasjoner, miljøer og individer som antas å besitte eller kunne få tilgang til relevant informasjon for løsning av tjenestens lovpålagte oppdrag. Individer eller organisasjoner kan identifiseres ved at de opptrer på en bestemt måte eller innehar visse karakteristika. Ofte vil tjenesten benytte seg av avanserte kombinasjoner av utvalgskriterier, herunder mønstre og andre avgrensninger som sannsynliggjør at man får frem den relevante informasjonen. Slik sett gjennomføres også målsøkingsprosessen så målrettet som mulig, men naturligvis sjelden like målrettet som når man innhenter mot allerede kjente etterretningsmål. Målsøking skjer likevel aldri på måfå, men baserer seg alltid på en retning som kan begrunnes rasjonelt.

De utvalgskriterier som angis for å avgrense informasjonsinnhenting for målsøkingsformål, og som ikke er tilknyttet en bestemt person eller virksomhet, kalles *modusselektorer*. Med selektor menes en identifikator, for eksempel et telefonnummer, epostadresse eller brukernavn på en gitt tjeneste, eller en søkealgoritme som er egnet til å frembringe informasjon for etterretningsformål. En modusselektor er i lovutkastet § 1-4 nr. 7 definert som «et søkebegrep eller søkestreng som beskriver et bestemt mønster eller avgrensning, herunder handlingsmønster eller geografisk område». Målsøking kan også baseres på en personselektor, se nedenfor om dette. Typisk vil dette skje gjennom å avdekke nye potensielle etterretningsmål basert på en persons nettverk.

9.3.3 Målrettet innhenting

Også for *målrettet innhenting* benyttes inngangsverdier i form av modusselektorer eller personselektorer. En personselektor er i lovutkastet § 1-4 nr. 12 definert som «en identifikator tilknyttet en bestemt person eller virksomhet, for eksempel et telefonnummer, en epostadresse eller et brukernavn på en gitt tjeneste». En og samme person har oftest en rekke selektorer av ulik karakter. Vedkommende kan også ha flere selektorer av samme karakter, eksempelvis ha ulike twitterkonti med tilhørende brukeridentiteter. Målrettet innhenting kan skje både mot identifiserte eller uidentifiserte mål, men det må foreligge konkrete holdepunkter for at målet er et etterretningsmål. Målrettet innhenting basert på modusselektor kan for eksempel gjelde innhenting av trafikk knyttet til et målspesifikt digitalt verktøy.

Målsøkingsprosessen er sluttført når Etterretningstjenesten besitter tilstrekkelig informasjon til å vurdere om målet faktisk er relevant for oppdragsløsningen og at det ligger innenfor Etterretningstjenestens mandat å iverksette målrettet innhenting mot målet. Målsøking har altså som formål å avklare *om* noe eller noen er et relevant etterretningsmål eller ikke. Som ledd i denne prosessen må man også søke å identifisere målets juridiske status, dvs. om Etterretningstjenesten lovlig kan rette innhenting mot målet innenfor rammen av tjenestens rettsgrunnlag. I enkelte tilfeller vil målsøkingsprosessen indikere at målet besitter relevant informasjon, men at informasjonen likevel ikke lovlig kan innhentes, for eksempel fordi målet viser seg å befinne seg i Norge. Ved tvil skal Etterretningstjenesten søke å avklare forholdet nærmere på ulike måter, se lovforslaget § 4-1 tredje ledd.

9.4 Gjeldende rett om grunnvilkår for innhenting

9.4.1 Generelt

Av de grunner som det er redegjort for ovenfor, har det alltid vært en lav terskel for at Etterretningstjenesten kan innhente informasjon, herunder ikke-verifiserte opplysninger. Nærmere bestemmelser om tjenestens etterfølgende behandling av personopplysninger og utlevering av informasjon drøftes i høringsnotatet kapittel 12 og 13.

Det er viktig å understreke at innhenting for etterretningsformål *aldri* vil være basert på *mistanke* eller lignende individualbaserte terskler for innhenting og behandling av informasjon etter analogi fra justissektoren og straffeprosessen. En slik analogi kan ikke trekkes. Etterretningstjenestens oppgave er å vurdere trender og fremtidige handlinger hos fremmede stater, organisasjoner og personer, uavhengig av om disse har gjort eller vil gjøre noe straffbart. Det vises til fremstillingen i punkt 9.2 ovenfor.

9.4.2 Legitimt formål og forholdsmessighet

Etter dagens regelverk er vilkåret for å iverksette målsøking, ved siden av kravet om at innhentingstiltaket må være forholdsmessig, kun at letingen må basere seg på et legitimt formål; dvs. at letingen må knyttes til et legitimt etterretningsbehov slik dette er fastsatt i lov og av overordnede myndigheter. Etter at et mål av interesse er identifisert gjennom målsøking, vil terskelen for å iverksette målrettet innhenting være noe høyere enn for å iverksette målsøking. Det er imidlertid aldri krav om at det må godtgjøres sannsynlighetsovervekt for at innhenting av informasjon vil frembringe etterretningsinformasjon som kan behandles videre. Ut over dette gjelder ingen «beviskrav» eller andre høyere terskler, rett og slett fordi slike krav i praksis vil gjøre det umulig å frembringe etterretninger. Dette står naturligvis ikke i motsats til at informasjon så langt mulig må kvalitetssikres, for å øke verdien av etterretningsanalysen og vurderingene. Som beskrevet over vil dessuten målsøking alltid være knyttet til bestemte ledetråder og aldri skje på måfå. Men til syvende og sist er det et faktum at stater ofte må basere seg og handle på basis av usikker informasjon.

Det som skisseres ovenfor om grunnvilkår for målsøking og målrettet innhenting, er i dag basert på doktrine, god etterretningsskikk og etablert praksis. Grunnvilkårene er etter dagens rettsgrunnlag verken nedfelt i lov eller annet offentlig tilgjengelig regelverk. På diverse saksavgrensede områder har Etterretningstjenesten imidlertid internt regelverk som reflekterer forannevnte prinsipper.

9.5 Forslag til grunnvilkår i utkast til ny lov

9.5.1 Innledning

Departementet foreslår å lovfeste grunnvilkår for målsøking og målrettet innhenting, som i all hovedsak vil kodifisere gjeldende praksis. På enkelte områder vil lovforslaget likevel innebære en viss materiell skjerpelse sammenlignet med dagens rettstilstand. Forslaget vil bidra til å sikre at de menneskerettslige krav til forholdsmessighet og nødvendighet blir reflektert i loven.

9.5.2 Formålsbestemthet (lovutkastet kapittel 5, jf. kapittel 3)

All informasjonsinnhenting, enten det er for målsøkingsformål eller er målrettet innhenting, skal bare kunne skje med det formål å frembringe informasjon som er relevant for å ivareta en eller flere av Etterretningstjenestens oppgaver. Dette kan også formuleres som et krav om at innhentingen skal være saklig begrunnet i tjenestens samfunnsoppdrag. Dette formålsbestemthetskravet følger etter gjeldende lov forutsetningsvis av lovens § 3 om tjenestens oppgaver, som fastsetter at tjenesten skal innhente informasjon «som kan bidra til» de oppgaver som er angitt i bestemmelsen.

Departementet foreslår i reguleringen av grunnvilkårene for målsøking og målrettet innhenting at det presiseres uttrykkelig at innhenting bare kan skje med det formål å frembringe informasjon «som er relevant for etterretningsformål». Etterretningsformål er i lovutkastet § 1-4 nr. 3 definert som «formål å ivareta en eller flere av Etterretningstjenestens oppgaver etter kapittel 3».

9.5.3 Forholdsmessighetskrav (lovutkastet § 5-4)

9.5.3.1 Nærmere om vurderingen

Informasjonsinnhenting rettet mot en person vil utgjøre et inngrep i dennes private sfære. Slike inngrep må være nødvendige og forholdsmessige. Se mer om dette i høringsnotatet kapittel 4 om forholdet til Grunnloven og menneskerettighetene.

Departementet foreslår å lovfeste et alminnelig forholdsmessighetsprinsipp som skal gjelde for ethvert inngrep som Etterretningstjenesten gjør overfor den enkelte. En slik forholdsmessighetsvurdering praktiseres også i dag, selv om dette ikke er særskilt nedfelt i gjeldende lov. Departementet mener likevel at forholdsmessighetsprinsippet er så sentralt at det er nødvendig å lovfeste det. Bestemmelsen vil etter sin ordlyd bare komme til anvendelse der informasjonsinnhentingen utgjør et inngrep overfor subjekter som er vernet etter menneskerettighetene, det vil si fysiske og juridiske subjekter. Aktivitet der dette ikke gjør seg gjeldene, for eksempel ved akustisk innhenting, omfattes således ikke.

Forholdsmessighetskravet pålegger Etterretningstjenesten å foreta en konkret vurdering i det enkelte tilfellet. Dersom man etter en helhetsvurdering kommer til at innhentingen vil utgjøre et uforholdsmessig inngrep, vil tiltaket ikke være lovmessig. Følgelig kan man se for seg tilfeller der innhentingen vil kunne oppfylle de øvrige grunnvilkårene, men at den etter omstendighetene likevel ikke vil kunne gjennomføres. Forholdsmessighetsprinsippet krever at skaden eller uleiligheten forbundet med inngrepet ikke må stå i misforhold til det som søkes oppnådd. I dette ligger for det første at det må foreligge et klart *behov* for det aktuelle tiltaket, altså at tiltaket er *nødvendig*. En forutsetning for at tiltaket skal være nødvendig er at det er *egnet* til å oppnå formålet. Hva som er nødvendig, avhenger dessuten av hvilke alternative tiltak som står til rådighet. En side av nødvendighetskravet er derfor et minsteinngrepsprinsipp (subsidiaritetsprinsipp). I dette ligger at man alltid skal benytte det minst inngripende tiltaket som er tilgjengelig. Samtidig kan ikke vurderingen av tilgjengelige alternativer skje på rent teoretisk grunnlag. I vurderingen må det også tas i betraktning ressursmessige og etterretningsfaglige hensyn, samt risikovurderinger og andre relevante omstendigheter. Det kan blant annet være at alternativene må anses utilstrekkelige eller uhensiktsmessige, eller at saken har så stor betydning eller tidsnød at mer inngripende tiltak etter omstendighetene anses forholdsmessige. Forholdsmessighetsbestemmelsen kan derfor ikke oppfattes som et påbud om at alle mindre inngripende tiltak først forgjeves må ha

vært forsøkt. Til syvende og sist må alvorligheten i inngrepet for den enkelte også måtte avveies mot viktigheten av å frembringe informasjon som er av betydning for de samfunnsmessige verdier som norske myndigheter ved hjelp av Etterretningstjenesten har til oppgave å beskytte, i lovforslaget omtalt som «sakens betydning». I en konkret helhetsvurdering vil det også være tillatt å ta i betraktning nødvendigheten av at Etterretningstjenesten i en målsøkingsfase må gå bredt ut. I disse tilfellene kan det ikke oppstilles en for høy terskel knyttet til sannsynligheten for at formålet med informasjonsinnhenting vil bli oppnådd.

Den avveining som må gjøres mellom hva som søkes oppnådd og hvilke implikasjoner dette antas å ha overfor den enkelte må gjøres i lys av sakens karakter og betydning. Tidsaspektet kommer også inn her. Desto viktigere formålet er og jo mer det haster, jo mer inngripende tiltak vil normalt kunne tillates. Motsatt vil oppdrag der man har god tid til å innrette seg og velge mellom fremgangsmåter, stille større krav til skånsomhet i metodevalg og utførelse. For eksempel vil aktivitet forbundet med en overhengende internasjonal terrortrussel mot norske interesser åpne for mer inngripende tiltak enn et oppdrag om å vurdere generelle politiske utviklingstrekk i et land.

Tilgjengelige ressurser, tekniske muligheter og krav til effektivitet er også faktorer som spiller inn i vurderingen. Ikke sjelden vil den mest optimale løsningen fra et personvernperspektiv også være den mest kostnads- og ressurskrevende. Dette vil igjen gå ut over tjenestens øvrige evne til å løse sitt samfunnsoppdrag. Som ellers i forvaltningen må man derfor prioritere på en måte som sikrer en forsvarlig balanse mellom god virksomhetsutøvelse og effektiv ressursbruk.

I forholdsmessighetsregelen ligger det implisitt et krav om objektivitet, likebehandling av like tilfeller, saklighet og plikt til ikke å legge vekt på utenforliggende hensyn. Det ligger også i regelen et generelt utgangspunkt om at alle personer har grunnleggende krav på personvern og kommunikasjonsfrihet, selv om personene befinner seg utenfor norsk jurisdiksjon og myndighetsområde.

9.5.3.2 Betydning for både metodevalg og utførelse

Forholdsmessighetsprinsippet får både betydning for valg av *innhentingsmetode* og for *hvordan* informasjonsinnhentingen skal gjennomføres, det vil si selve utførelsen. Krav til og grad av skånsomhet vil måtte vurderes her. For spørsmålet om metodebruk vil bestemmelsen både ha betydning for spørsmålet om en bestemt metode for informasjonsinnhenting kan benyttes, og for hvor lenge innhenting ved bruk av metoden kan pågå. For enkelte metoder gjelder et høyere terskelkrav, jf. pkt. 9.5.5 og kapittel 10. Et særskilt spørsmål for enkelte innhentingsmetoder er hvorvidt det må foretas enkeltstående forholdsmessighetsvurderinger for hvert individuelle inngrep, eller om det er tilstrekkelig å foreta én samlet vurdering for innsamlingen som sådan. Dette kommer særlig på spissen for enkelte tekniske innsamlingsmetoder. Eksempelvis kan det ut fra omstendighetene anses forholdsmessig å avlese mobiltelefoner som befinner seg i en bestemt bydel i et krigsområde, fordi man har grunn til å anta at det i denne sonen oppholder seg mange etterretningsmål. Her vil forholdsmessighetsvurderingen måtte ta opp i seg det akkumulerte inngrepet mot de som oppholder seg i den avgrensede sonen. Det vil i en slik situasjon ikke være krav om å foreta en individuell forholdsmessighetsvurdering knyttet til hver enkelt innhenting. Den konkrete forholdsmessighetsvurderingen vil her først foretas som ledd i vurderingen av om den innhentede informasjon er nødvendig å behandle videre for

etterretningsformål i tråd med bestemmelsene om personvern i lovforslaget kapittel 9. Dette er nærmere omtalt i høringsnotatet kapittel 12.

9.5.3.3 Når skal vurderingen foretas

Etterretningstjenesten må etter lovforslaget foreta en forholdsmessighetsvurderingen *før* informasjonsinnhenting igangsettes. Varigheten av tiltaket vil dessuten være en faktor i forholdsmessighetsvurderingen som sådan. Et spørsmål som reiser seg er hvorvidt det er nødvendig å foreta en ny forholdsmessighetsvurdering underveis i innhentingen, eller om man kan forholde seg til den tidsangivelsen som er satt. Det samme gjelder hvilken vurdering som må gjøres for å fortsette innhentingen etter at tidsperioden er avsluttet. Departementet foreslår ikke å lovregulere dette spesifikt, men mener det vil påligge Etterretningstjenesten å foreta en ny forholdsmessighetsvurdering knyttet til en pågående innhenting dersom forholdene som ligger til grunn for innhentingen endrer seg på en slik måte at det må anses påkrevd å vurdere hvorvidt fortsatt innhenting fremdeles vil være forholdsmessig og dermed lovmessig. Dersom en tidsavgrenset innhenting utløper må Etterretningstjenesten vurdere forholdsmessigheten på nytt. Det ligger imidlertid i dette at dersom ingen forhold av betydning har endret seg, og behovet for innsamling er vedvarende, vil man kunne lene seg på tidligere betraktninger knyttet til forholdsmessigheten av tiltaket.

Utlevering av informasjon utgjør i seg selv et menneskerettslig inngrep overfor den enkelte, og krav om å vurdere forholdsmessighet bør derfor etter departementets syn også gjelde for utlevering av informasjon. Når det gjelder behandling av personopplysninger etter at de er innhentet vil også dette være et inngrep. De nærmere vilkår for behandling av personopplysninger utover innhenting og utlevering er gjenstand for en særskilt forholdsmessighetsvurdering. Dette er omtalt nærmere i høringsnotatet kapittel 12.

1.5.3.4 Forslag til bestemmelse

Departementet foreslår at kravet til forholdsmessighet formuleres slik i loven:

§ 5-4 *Forholdsmessighet*

Innhenting og utlevering av informasjon skal ikke gjennomføres dersom det vil være et uforholdsmessig inngrep overfor den enkelte. Ved vurderingen skal det tas hensyn til om mindre inngripende tiltak i tilstrekkelig grad kan ivareta formålet, inngrepets virkning for den som rammes, sakens betydning og forholdene ellers.

9.5.4 «Grunn til å undersøke» (lovutkastet §§ 5-1 og 5-2)

9.5.4.1 Innledning

I tillegg til grunnvilkårene om formålsbestemthet (punkt 9.5.2) og forholdsmessighet (punkt 9.5.3), foreslår departementet at informasjonsinnhenting gjennom målsøking og målrettet innhenting bare kan gjennomføres dersom det foreligger *grunn til å undersøke* om innhentingen kan bidra til å frembringe informasjon som er relevant for etterretningsformål. Dette begrunnes med at selv om informasjonsinnhentingen har et legitimt etterretningsformål og ikke anses uforholdsmessig, bør den likevel ikke tillates med mindre det foreligger *etterprøvbare* forhold for hvorfor innhentingen ble gjennomført.

9.5.4.2 Nærmere om hva som ligger i begrepet «grunn til å undersøke»

Etterretningstjenesten skal ikke innhente informasjon basert på ren vilkårlighet eller «mageføelse». En eller annen ledetråd vil alltid måtte ligge til grunn. Dette er begrunnet både i personvernhensyn og av hensyn til forsvarlig ressursbruk. Det skal ikke søkes vilkårlig etter informasjon gjennom simpel gjetting. For Etterretningstjenesten gjelder et

saklighetskrav, og et krav til forholdsmessighet mellom det som skal undersøkes for etterretningsverdi og de virkemidler som tas i bruk, hvilket krever et visst grunnlag som kan bidra til nominasjon av søk. En lovbestemt generell terskel for målsøking og målrettet innhenting er ment å sikre at Etterretningstjenesten ikke innhenter informasjon som tjenesten i ettertid ikke konkret kan underbygge hvorfor ble innhentet. En slik terskel vil sikre mot vilkårlig innhenting og bidra til at tjenesten så langt mulig retter informasjonsinnhentingen mot mest mulig relevante forhold. Et eksempel på vilkårlighet vil være å rette innhenting mot alle ansatte i sentralforvaltningen i en stat, ut fra en tanke om at man før eller siden vil treffe på informasjon som har etterretningsverdi. Selv om man kognitivt kan argumentere for at ansatte i sentralforvaltningen før eller siden vil besitte informasjon som kan knyttes til informasjonsbehov innenfor Etterretningstjenestens lovpålagte oppgaver, er holdepunktene for en slik bred innhenting, uten nærmere begrunnelse, for vag og avledet til at den kan aksepteres.

Departementet mener i tråd med gjeldende praksis at terskelen bør ligge noe lavere for målsøking enn for målrettet innhenting. Årsaken til at terskelen er ulik er at grunnlaget for å iverksette målrettet innhenting gjennomgående vil være noe klarere enn når informasjonsinnhenting skjer for målsøkingsformål. Man vil kun iverksette målrettet innhenting mot identifiserte mål, og det vil derfor som oftest foreligge mer opplysninger knyttet til dette målet enn ved søking etter ukjente mål. I tillegg kommer at målrettet innhenting – hvor man følger et mål over tid – gjennomgående vil være mer inngripende enn ved målsøking. Også dette tilsier at terskelen for målrettet innhenting bør være høyere.

For begge kategorier innhenting foreslår departementet at det første elementet i terskelkravet bør være at Etterretningstjenesten må ha «grunn til å undersøke» om innhentingen kan frembringe «informasjon som er relevant for etterretningsformål». Departementet foreslår at det for målrettet innhenting oppstilles et ytterlig element i terskelkravet.

Begrepet «grunn til å undersøke» i lovutkastet § 5-1 sikter til at *målsøkingen* må bygge på enkelte ledetråder. Dette vil kunne være erfaringsbaserte hypoteser eller et holdepunkt. Eksempelvis vil kontaktlisten til en person som deltar i spredning av masseødeleggelsesvåpen være et holdepunkt for å igangsette målsøking. Med erfaringsbaserte hypoteser menes at hypotesen må kunne begrunnes med holdepunkter basert på ervervet kunnskap. At premisset for å igangsette innhenting vil kunne være basert på en hypotese ligger innbakt i selve konseptet målsøking. Målsøking handler, som beskrevet i punkt 9.3, om å forsøke å finne frem til hittil ukjent kunnskap og trusler for å kunne gi en prediktiv vurdering av betydning for nasjonens sikkerhet og interesser. Når innhentingen baserer seg på en hypotese er det fordi man på dette tidspunktet i oppdragsløsningen ikke nødvendigvis har konkrete holdepunkter for å igangsette innhenting, men der erfaring tilsier at det foreligger tilstrekkelig grunnlag for å undersøke et forhold nærmere. Men også på et så tidlig stadium i prosessen *kan* det foreligge mer konkrete ledetråder som tilsier at målsøking bør igangsettes.

For *målrettet innhenting* har man gjennomgående mer konkret informasjon som grunnlag for å undersøke om innhentingen kan frembringe etterretningsrelevant informasjon. I § 5-2 foreslår departementet derfor at for denne kategorien innhenting må «grunn til å undersøke» bygge på «konkrete holdepunkter» for at «etterretningsmålet besitter, kommuniserer eller vil motta, eller om innhenting på annen måte kan frembringe, informasjon som er relevant for etterretningsformål». Sannsynlighetskravet er dermed noe strengere for målrettet innhenting

enn for målsøking. Alternativet om «på annen måte kan frembringe» vil særlig være aktuelt som terskel for innhenting innenfor det tradisjonelle militære domenet, hvor innhentingen er rettet mot objekter i form av fartøyer, fly, øvingsmønster, våpensystemer, styrkeforflyttinger, kommando- og kontrollsystemer, militære operasjoner mv.

Hvorvidt grunnkravene er oppfylt må vurderes konkret. Grunnlaget må kunne artikuleres substansielt. For kontrollformål må Etterretningstjenesten i ettertid kunne vise til et kvalifiserende faktum eller en begrunnet hypotese eller assosiering som holdepunkt for innhenting. Departementet vil understreke at et slikt faktum eller en slik hypotese imidlertid ikke vil måtte kreve dokumentasjon med en spesiell bevisgrad. Det vil heller ikke kunne kreves at holdepunktet må bygge på objektive eller kvalitetssikrede opplysninger. På dette stadiet i innhentingsprosessen mener departementet i tråd med fast og langvarig praksis, at inngangsparametret for å iverksette innhenting kan være basert på etterretningsfaglig begrunnede antagelser.

9.5.4.3 Grad av sannsynlighet

Det er vanskelig å angi konkret hvilken sannsynlighetsterskel som bør kreves, men selve ordlyden «*undersøke* om innhenting *kan* bidra» tilsier at innhenting også kan skje dersom sannsynligheten for å frembringe relevant informasjon er relativt lav, herunder i området 10-40 prosents sannsynlighet. Sannsynlighetsovervekt (mer enn 50 prosent) eller enda høyere sikkerhet for at innhentingen vil gi etterretningsverdi vil under enhver omstendighet ikke kunne kreves. Eksempelvis fremstår det som klart at det vil foreligge grunn til å undersøke kontaktlistene til en kjent terrorist – altså søke å avklare hvem disse kontaktene er og om de kan knyttes til internasjonal terrorisme – selv om det er lite sannsynlig at et stort antall av kontaktene også er terrorister. Etter omstendighetene kan det faktum at en aktør innehar en viss kapasitet være tilstrekkelig for å tilfredsstille vilkårene. Dette gjelder selv om det ikke foreligger kjente indikasjoner på trusselvilje. Man må kunne innhente informasjon om etterretningsmål som man med grunn ikke kan utelukke vil kunne utgjøre en trussel i fremtiden, selv om det ikke foreligger et underbyggbart grunnlag på innhentingstidspunktet som sannsynliggjør at målet vil utgjøre en slik trussel på et bestemt senere tidspunkt. Standarden må derfor ikke forstås som et forbud mot å undersøke forhold som med liten grad av sannsynlighet vil frembringe relevante etterretninger, eller som et forbud mot å undersøke forhold som i tid og rom har en relativt sett fjern sammenheng med dagsaktuelle utfordringer. Det må tas i betraktning at innhenting også kan skje i den hensikt å «sjekke personer ut» av et saksforhold, eller avklare at en stat eller organisasjon *ikke* antas å ville utfordre norske interesser i nær fremtid. I denne kontekst kan slik innhenting bidra til å spisse innhentingsvirksomheten mot de mer relevante aktørene.
Forholdsmessighetsvurderingen spiller imidlertid også inn i slike tilfeller, og kan etter omstendighetene utelukke innhenting eller bruk av bestemte innhentingsmetoder.

9.5.4.4 Presisering – vilkåret må forstås i en utenlandsetterretningskontekst

Det presiseres at standarden «grunn til å undersøke» ikke har eller skal ha noen sammenheng med tilsvarende begreper som brukes i politiloven og straffeprosessloven i forbindelse med etterforskning eller i tilknytning til PSTs forebyggende saker («med grunn», «grunn til å undersøke», «rimelig grunn til å undersøke» og lignende formuleringer). Standarden er, og er ment som, en isolert etterretningsterskel for utenlandsetterretningsformål. Tolkningspraksis knyttet til kriminaletterretning, etterforskning og tvangsmiddelbruk i politiet har overhodet ingen bæring eller relevans for forståelsen av terskelbegrepet i en utenlandsetterretningskontekst. Gjennomgående vil terskelen for

innhenting også være vesentlig annerledes for Etterretningstjenesten enn for politiet. Dette er begrunnet i flere forhold: Standarden for en utenlandsetterretningstjeneste må vurderes i lys av at ukjente trusler knyttet til fremmede stater, organisasjoner og personer ikke er mulig å avdekke uten å innhente, sammenstille og analyse små informasjonsbiter over lang tid som hver og en ikke i seg selv sannsynliggjør trusselen. Dernest kommer at undersøkelsesstandarden for politiet forholder seg til sannsynligheten for at noen har foretatt eller vil foreta en bestemt straffbar handling, mens Etterretningstjenesten forholder seg til om innhenting vil besvare norske myndigheters informasjonsbehov uavhengig av om noen i sakskomplekset har gjort eller vil gjøre noe straffbart eller på annet vis opptre klanderverdig. Det at begrepene har lignende språkdrakt i de ulike regelsettene innebærer derfor ikke at de skal tolkes og anvendes likt.

9.5.4.5 Forslag til bestemmelse

Departementet foreslår at grunnvilkår for henholdsvis målsøking og målrettet innhenting formuleres på følgende måte i loven:

§ 5-1 *Grunnvilkår for målsøking*

Etterretningstjenesten kan iverksette målsøking når det foreligger grunn til å undersøke om innhenting kan bidra til å frembringe informasjon som er relevant for etterretningsformål.

§ 5-2 *Grunnvilkår for målrettet innhenting*

Etterretningstjenesten kan iverksette målrettet innhenting når konkrete holdepunkter tilsier at det foreligger grunn til å undersøke om etterretningsmålet besitter, kommuniserer eller vil motta, eller om innhenting på annen måte kan frembringe, informasjon som er relevant for etterretningsformål.

9.5.5 Særskilte innhentingskrav for bestemte metoder for informasjonsinnhenting – vesentlig betydning for oppgaveløsningen

All informasjonsinnhenting vil være underlagt grunnvilkårene i lovforslaget kapittel 5. For bruk av de mest inngripende metodene i lovforslaget kapittel 6 foreslår departementet at det oppstilles et ytterligere skjerpende krav om at innhentingen *anses strengt nødvendig* for *ivaretakelsen av Etterretningstjenestens oppgaver*. Dette vil særlig gjelde gjennomsøking og avlytting på ikke offentlig sted, samt endepunktinnhenting. Nevnte forslag til skjerpet innhentingskrav innebærer en strengere forholdsmessighetsvurdering, og er nærmere omtalt i kapittel 10 om Etterretningstjenestens metodebruk som foreslått i lovutkastet kapittel 6.

9.5.6 Innhenting av rådata i bulk (lovutkastet § 5-3)

9.5.6.1 Innledning og definisjon

Bulk-innsamling omtales flere steder i høringsnotatet her. Departementet vurderer at gode grunner taler for at det bør oppstilles et eget grunnvilkår for innhenting av og søk i rådata i bulk i lovutkastet kapittel 5.

Med «bulk» menes informasjonssamlinger og datasett hvorav en vesentlig andel av informasjonen antas å være irrelevant for etterretningsformål, se definisjon i lovutkastet § 1-4 nr. 2. Hva som menes med en «vesentlig del» vil i utgangspunktet bero på skjønn. Departementet legger til grunn som en rettesnor at det normalt vil kreves at minimum 40% av datamengden må antas irrelevant for etterretningsformål før det er tale om innhenting i bulk.

Lysne II-utvalget har i sin rapport[195] omtalt bulkbegrepet nærmere i relasjon til innhenting av elektronisk kommunikasjon for etterretningsformål. Her henvises det videre til vurderinger gjort av andre stater. Bulk kan defineres slik:[196]

> "References to signals intelligence in 'bulk' mean the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.)."

Denne definisjonen er på enkelte områder uklar. Særlig gjelder det dersom man bruker vide selektorer, f.eks. «Syria» som seleksjonsterm. I det tilfellet vil separasjonen av all trafikk til og fra Syria etter definisjonen fremstå som målrettet, og ikke som bulkinnhenting. Motsatt ville en innhenting av all trafikk som går over en spesiell kommunikasjonskanal som kun brukes av to personer, være å anse som bulkinnhenting, fordi man ikke benytter selektorer («discriminants») som grunnlag for innhentingen. I en rapport fra 2015 utarbeidet av det amerikanske National Research Council (NRC) tas det heller til orde for at:[197]

> «if a significant portion of the data collected is not associated with current targets, it is bulk collection; otherwise, it is targeted".

Rapporten uttaler også at:

> "there is no precise definition of bulk collection, but rather a continuum with no bright line separating bulk from targeted".

I rapporten erkjennes det at begrepet "significant" i seg selv er et upresist begrep. Departementet legger NCRs tilnærming til grunn for hva som må anses som innhenting i bulk.

9.5.6.2 Nærmere presisering - volum

Bulkbegrepet sier etter sin ordlyd og definisjon ikke noe om omfanget (volumet) av innhentet informasjon, kun om ratio mellom relevant og ikke-relevant informasjon i data som innhentes samlet eller løpende fra en bestemt aksess/tilgang. I prinsippet vil derfor etter denne definisjonen en intern telefonliste over alle ansatte i et selskap som er involvert i våpenhandel mest sannsynlig være å anse som bulkinnhenting, fordi mesteparten av selskapets ansatte og deres telefonnumre ikke vil være relevant for etterretningsformål. Departementet mener på sin side at datamengden er et viktig element for at noe skal kunne defineres som bulkinnsamling, og ikke bare forholdstallet mellom relevant og ikke-relevant informasjon. For å vise til at det må være tale om datamengder av et større omfang, foreslår departementet å bruke begrepet «informasjonssamlinger og datasett» i legaldefinisjonen. Departementet antar på den annen side at det ikke er formålstjenlig å forsøke å definere presist hvor stort omfang som må til for at noe skal kvalifisere som bulk, men legger til grunn som retningsgivende at volumet i hvert fall må være så omfattende at det ikke vil være mulig med Etterretningstjenestens menneskelige ressurser å gjennomgå alle datamengdene manuelt med sikte på å vurdere etterretningsmessig relevans.

---

[195] Rapport fra Lysne II-utvalget om digitalt grenseforsvar av 26. august 2016 s. 10 note 3

[196] U.S. Presidential Policy Directive/PPD-28 on Signals Intelligence Acitivities, datert 17. januar 2014

[197] Rapport NCR 2015 «Bulk Collection of Signals Intelligence: Technical Options»

9.5.6.3 Teknologiske forutsetninger

Det er i mange tilfeller helt nødvendig å innhente data i bulk, slik at man etterpå kan søke målrettet i mengden av data. Med en slik metode går man bredt ut, og snevrer inn etter hvert. Ofte illustreres dette med at dersom Etterretningstjenesten skal kunne finne nålen, må den ha tilgang til høystakken. Årsaken til at man må innhente informasjon på denne måten er at det på kommunikasjonsetterretningsområdet som oftest er teknisk umulig å gjøre analyse, utvalg og filtrering i sanntid, altså mens dataene er i transitt. Følgelig må data lastes ned og lagres, for at det i det hele tatt skal være mulig å finne de informasjonsbitene om utenlandske forhold som er av interesse. Et illustrerende eksempel på dette er innsamling av metadata fra satellittkommunikasjon. Ved denne formen for signaletterretning velger Etterretningstjenesten ut de satellittlinker som har størst relevans for utenlandsetterretningsoppdraget. I denne prosessen følger det uunngåelig med trafikkdata som ikke er av interesse. Dette er såkalt overskuddsinformasjon. Overskuddsinformasjonen kan inkludere noe trafikkdata relatert til norske borgeres kommunikasjon. Men over 99% av alle lagrede metadata fra satellittkommunikasjon er *ikke* knyttet til norske personer, og det vil av tekniske grunner aldri være slik at begge endene i kommunikasjonen stammer fra Norge. På dette punkt skiller satellittinnhenting seg grunnleggende fra forslaget om tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon, se høringsnotatet kapittel 11. Etter at metadata fra utvalgt satellittkommunikasjon er lagret, er det på grunn av mengden data praktisk umulig for Etterretningstjenestens ansatte å gå gjennom alle disse for å evaluere hver enkelt datahendelse for etterretningsverdi. Dersom slik gjennomgang og analyse hadde vært praktisk mulig, ville det ha medført at tjenestens analytikere ville fått innsyn i en mengde data uten etterretningsverdi. Det paradoksale blir dermed at et slikt innsyn ville ha fått større negative personvernkonsekvenser sammenlignet med dagens ordning, hvor alle data som trekkes ut og sees på skjer etter spesifikke søkekriterier som tilfredsstiller grunnvilkårene for innhenting. Dagens ordning innebærer at de fleste irrelevante data aldri vil bli sett på av ansatte i Etterretningstjenesten. Søkekriteriene som anvendes i dag er underlagt et internt regelverk som sikrer at alle søk er formålsbegrensede, nødvendige og forholdsmessige. Datasettene slettes når det ikke lenger er behov for dem. Det skjer snarest mulig basert på en etterretningsfaglig vurdering, og senest etter 15 år regnet fra innhentingen. Denne rettstilstanden bør etter departementets syn videreføres, se lovutkastet § 9-9 annet ledd som er nærmere omtalt i høringsnotatet punkt 12.6.5.

Begrunnelsen for dette og en redegjørelse for de øvrige hensyn som gjør seg gjeldende for bulkinnsamling, er også omtalt i kapittel 11 om tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon. Bulkinnhenting er særlig aktuelt for midtpunktinnhenting, det vil si innhenting av elektronisk kommunikasjon mens kommunikasjonen transporteres, men kan i prinsippet skje ved bruk av enhver innhentingsmetode. Eksempelvis kan også innhenting i åpne kilder innebære innhenting i bulk.

Kommunikasjonsetterretning i form av bulkinnsamling er først og fremst et resultat av den teknologiske utvikling som har funnet sted de seneste tiår. Mengden kommunikasjon har økt eksponentielt, og muligheten for å spore opp det som er etterretningsrelevant kommunikasjon er dermed mer krevende. I tillegg er kommunikasjonsstrukturen og kommunikasjonsmulighetene i dag helt andre enn hva som gjaldt tidligere, med et vell av plattformer og kanaler å interagere på. Uten mulighet for å drive bulkinnsamling som basis for målsøking eller målrettet innhenting i de tilfeller der dette anses nødvendig, vil det i praksis være lite igjen av kommunikasjonsetterretningen på sikt. Gitt

kommunikasjonsetterretningens betydning for Etterretningstjenestens leveranser, vil dette sette tjenesten i langt dårligere i stand til å levere etterretningsprodukter fremover.

9.5.6.4 Andre land

Andre land vurderer verdien av bulkinnhenting på samme måte. I forbindelse med forslaget til ny etterretnings- og sikkerhetslovgivning i Storbritannia ga den britiske regjeringen den 1. mars 2016 ut dokumentet «Operational Case for Bulk Powers». Verdien av innhenting av etterretningsinformasjon i bulk oppsummeres slik i dokumentet på s. 4:

> «1.7. Bulk powers have been essential to the security and intelligence agencies over the last decade and will be increasingly important in the future. The acquisition and use of bulk data – information acquired in large volumes and used subject to special restrictions – provides vital and unique intelligence that the security and intelligence agencies cannot obtain by any other means. The security and intelligence agencies use the same techniques that modern businesses increasingly rely on to analyse data in order to overcome the most significant national security challenges. They do so subject to strict safeguards and robust oversight.
>
> Bulk capabilities are among the most important tools that the agencies can use to:
>
> - obtain intelligence on overseas subjects of interest, including threats to UK citizens and our Armed Forces;
> - identify threats here in the UK, sometimes from fragments if intelligence;
> - establish and investigate links between known subjects of interest, at pace, in complex investigations;
> - understand known suspects' behaviour and communications methods to identify potential attack planning;
> - verify information obtained about subjects of interest through other sources (e.g. agents); and
> - resolve sometimes anonymous online personae to real world identities.
>
> 1.8. There is clear evidence that these capabilities have helped to protect the UK. The analysis of bulk data, for example, has:
>
> played a significant part in every major counter terrorist investigation of the last decade, including in each of the seven terrorist attack plots disrupted since November 2014;
>
> enabled over 90% of the UK's targeted military operations during the campaign in the south of Afghanistan;
>
> been essential to identifying 95% of the cyber-attacks on people and businesses in the UK discovered by the security and intelligence agencies over the last six months; and
>
> been used to identify serious criminals seeking to evade detection online, and who cannot be pursued by conventional means, supporting the disruption of over 50 paedophiles in the UK in the last three years."

Bulkinnsamling er for øvrig i tråd med slik andre vestlige utenlandsetterretningstjenester utøver etterretningstjeneste, og det støttes også av flere uavhengige internasjonale utredninger, som eksemplifisert gjennom Royal United Services Institute sin utredning som la til grunn at innsamling av rådata i bulk er en forutsetning for å drive moderne

etterretning.[198] Utredningene har vektlagt at andre tekniske alternativer i sum vil være mer inngripende i individers sivile rettigheter, herunder kommunikasjonsvern og rett til privatliv.

9.5.6.5 Betydningen av et tilstrekkelig datagrunnlag

Målsøkingsprosessen fordrer at Etterretningstjenesten har behov for tilgang til relevante datasett for å kunne gjennomføre søk. I målsøkingsarbeidet må datagrunnlaget som ligger til grunn være så stort som mulig og datasettene bør inneholde nødvendige verdier for at de kan svare ut spørsmål og hypoteser som stilles. Jo større datagrunnlag å søke mot, desto mer uttømmende svar. Det er avgjørende for en effektiv prosess at spørsmålene som stilles og hypotesene som skal prøves er så spissede som mulig. Resultatet fra målrettede spørringer og hypoteser vil gi Etterretningstjenesten et godt beslutningsgrunnlag når det skal tas stilling til om målet er av en slik verdi at det skal etableres kontinuerlig innsamling og etterretningsproduksjon ved bruk av mer inngripende metoder.

Alternativene til bulkinnsamling er etter omstendighetene små, se kapittel 11 om mangel på teknologisk tilgjengelige alternativer til metadatalagring ved midtpunktinnhenting. Manglende mulighet til å foreta komplekse analyser og søk i bulkinnhentet informasjon ville derfor i prinsippet tvinge Etterretningstjenesten til å gjøre bruk av andre metoder, som vurderes som langt mer inngripende overfor en langt større gruppe av mennesker, for å kunne evaluere om de er involvert i aktivitet som det tilligger tjenesten å avdekke og motvirke. Dersom man for eksempel skulle gjennomført en nettverksanalyse basert utelukkende på menneskebasert innhenting, ville det medført massiv overvåking over tid fra Etterretningstjenestens operatører og kilder overfor en stor mengde personer. Til sammenligning ville det tatt et tiendedels sekund å eliminere majoriteten av disse fra videre behandling ved bruk av nettverksanalyse basert på metadata. Bulkinnhenting muliggjør i stedet å fokusere begrensede ressurser mot de mest aktuelle personer og raskt utelukke assosierte personer (for eksempel familiemedlemmer) som ikke er av interesse for Etterretningstjenesten. Analysene basert på et tilstrekkelig informasjonsgrunnlag kan også raskere utelukke falske positiver. For en etterretningstjeneste med begrensede ressurser er det også et poeng i seg selv at bulkinnsamling vil være eneste praktiske mulighet til å finne frem til et større antall relevante etterretningsmål med relativt små midler. Bulkinnhenting kan i enkelte sammenhenger også være nødvendig for å unngå å avsløre overfor fremmede lands etterretningstjenester hvem Etterretningstjenesten innhenter mot.

9.5.6.6 Departementets vurdering

Fordi alternativene er få eller ikke-eksisterende og fordi det muliggjør en effektiv måte å innhente etterretninger på, vurderer departementet at innhenting av informasjon i bulk i mange tilfeller er helt nødvendig for å kunne oppdage og velge ut potensielle etterretningsmål og derigjennom ivareta Etterretningstjenestens samfunnsoppdrag. Et bredt tilfang av data som inneholder relevante parametere er ikke bare hensiktsmessig for et ressurseffektivt målsøkingsarbeid. Det sørger også for at mer inngripende metoder kan nyttes selektivt og målrettet. Tilgang til relevante datasett i både bredde og dybde gjør Etterretningstjenesten i stand til å finne de viktige etterretningsmålene.

Det må samtidig erkjennes at innhenting av data i bulk i enkelte henseender etter en samlet vurdering kan innebære et større inngrep enn målrettet innhenting, fordi

[198] Royal United Services Institute, «A Democratic Licence to Operate: Report by the Independent Surveillance Review», 2016

Etterretningstjenesten faktisk vil lagre en mengde rådata knyttet til personer og forhold som ikke er relevante for tjenestens oppgaveløsning. I et menneskerettsperspektiv utgjør lagringen et inngrep selv om ikke-relevante rådata verken vil bli sett på eller benyttet til etterretningsproduksjon. Departementet mener derfor at terskelen for å kunne innhente datasamlinger og datasett i bulk må være høyere enn det grunnvilkårene ellers oppstiller for tjenestens informasjonsinnhenting. Departementet foreslår at innhenting av rådata i bulk kun kan skje dersom dette er nødvendig for å få tilgang til et relevant og tilstrekkelig informasjonsgrunnlag i den hensikt å gjennomføre målsøking eller målrettet innhenting i dette informasjonsgrunnlaget. I kravet om at innhentingen i seg selv må være nødvendig ligger at det i praksis ikke foreligger mindre inngripende alternativer som gir tilsvarende tilgang til et adekvat informasjonsgrunnlag som muliggjør målsøking og målrettet innhenting innenfor den metodikk og tematikk som nødvendiggjør innhenting. Et nødvendighetskrav ligger også innbakt i det alminnelige forholdsmessighetsprinsippet som foreslås i lovutkastet § 5-4, men departementet mener likevel at det vil skape større klarhet og forutberegnelighet at kravet inntas generelt for all bulkinnhenting.

Når først rådata er innhentet i bulk, gjelder de alminnelige grunnvilkår for *søk* i rådataene. For å unngå tvil om dette vil departementet foreslå at dette fremgår uttrykkelig av lovforslaget.

Departementet foreslår følgende bestemmelse om innhenting av og søk i rådata i bulk:

§ 5-3 *Grunnvilkår for innhenting av og søk i rådata i bulk*

Rådata kan innhentes i bulk når det er nødvendig for å få tilgang til et relevant og tilstrekkelig informasjonsgrunnlag i den hensikt å gjennomføre målsøking eller målrettet innhenting i dette informasjonsgrunnlaget.

Alle søk i bulkinnhentede rådata skal tilfredsstille grunnvilkårene for målsøking eller målrettet innhenting og logges for kontrollformål.

10 Innhentingsmetoder

10.1 Innledning

Hittil i høringsnotatet har det vært redegjort for hjemmelsgrunnlaget for Etterretningstjenestens informasjonsinnhenting, hvilke formål som kan begrunne innhentingen, hvilke grunnvilkår som bør gjelde, samt territorielle og andre begrensninger for tjenestens informasjonsinnhenting. Fokus i kapittelet her er *hvordan* informasjon kan innhentes av Etterretningstjenesten, forutsatt at de øvrige vilkårene for innhenting er oppfylt. Med andre ord er det spørsmål om hvilke *innhentingsmetoder* som tjenesten kan benytte.

Departementet ønsker å være så åpen som mulig om Etterretningstjenestens virksomhet. I erkjennelsen av at det er helt nødvendig for demokratisk tillit og troverdighet at offentligheten på generelt grunnlag er kjent med Etterretningstjenestens virksomhet og formål, har også tjenesten de senere årene vist stadig mer åpenhet. Lovkravet etter Grunnloven og internasjonale menneskerettskonvensjoner tilsier dessuten en så presis lovregulering som mulig av tjenestens metodebruk.

Det ligger samtidig i dagen at det går en grense for hvor detaljert metodene og kapasitetene til en hemmelig tjeneste kan beskrives i et offentlig dokument. En for stor grad av åpenhet vil undergrave tjenestens evne til å løse sine oppdrag. Dette skyldes at aktørene som Etterretningstjenesten retter sin informasjonsinnhenting mot ofte er høyst profesjonelle, og

de vil kunne innrette seg slik at de omgår tjenestens metoder og kapasiteter. Reguleringen av tjenestens metodebruk og fremstillingen i høringsnotatet må derfor holdes på et overordnet nivå. Det er ikke mulig å gå inn på forhold som i detalj røper hvordan en metode anvendes i praksis, og hvilke praktiske og andre begrensninger som gjelder for en bestemt metode.

10.2 Begrepsbruk og oversikt

10.2.1 Sentrale begreper

I etterretningsterminologi brukes begrepene *etterretningsdisiplin*, *innhentingsmetode* og *etterretningskilde* med noe ulikt innhold. For å tydeliggjøre hva som er hva, og hvilket begrep som foreslås benyttet i lovforslaget, er det nødvendig med en kort redegjørelse for begrepsbruken.

Begrepene *etterretningsdisiplin* og *innhentingsmetode* benyttes i en viss utstrekning om hverandre, men er ikke fullt ut sammenfallende. Disiplinbegrepet er videre enn metodebegrepet, og inkluderer etterretninger og produkter som er *fremkommet* gjennom bruk av innhentingsmetoder. Det er innsamlingen av informasjon, analysen, bearbeidingen og videreformidlingen av resultatet som til sammen kalles for *etterretning*.

Uansett hvilken disiplin eller metode som benyttes, vil informasjonen alltid ha sin opprinnelse i en *kilde*. Etterretningstjenestens egne kilder er de kilder som tjenesten selv kan skaffe seg tilgang til og benytte. Kildene er de stedene hvor man finner informasjon. Disipliner og metoder er utviklet og innrettet for å kunne innhente informasjon fra disse kildene slik at tjenesten kan løse konkrete oppdrag. Begrepet *kilde* benyttes både for menneskebaserte og tekniske innhentingsdisipliner. For menneskebasert innhenting har imidlertid begrepet kilde også en spesifikk mening som betegnelse på den *person* som kultiveres, rekrutteres og føres av Etterretningstjenesten for å gjennomføre menneskebasert innhenting. Kildebegrepet slik dette er definert i § 1-4 i lovutkastet henviser til denne personen, og ikke til den mer generelle betydningen.

10.2.2 Menneskebasert og teknisk innhenting

Et hovedskille for tjenestens innhentingsdisipliner og -metoder går mellom *menneskebasert* innhenting på den ene siden og ulike former for *teknisk* innhenting på den andre. Det karakteristiske ved menneskebasert innhenting er at innhentingen i hovedsak skjer ved hjelp av mellommenneskelig kontakt, i motsetning til teknisk innhenting som skjer ved passiv eller aktiv innsamling av signaler og lignende fenomener som blant annet opptrer under vann, gjennom luften/rommet eller i fysiske ledere.

Teknisk etterretning er en samlebetegnelse for etterretning utledet av informasjon og data fra tekniske objekter; det være seg radar, kommunikasjonsbærere i det elektromagnetiske spektrum, akustikk eller andre former for signaler og utstråling. Teknisk innhenting inkluderer etterretningsdisipliner som signaletterretning – som igjen deles inn i kommunikasjonsetterretning og elektronisk etterretning – nettverksetterretning, bildeetterretning, akustisk etterretning, radaretterretning, etterretning ved bruk av åpne kilder, måle- og signaturetterretning og geografisk etterretning.

Anvendbarheten av den ene fremfor den annen metode vil ofte være situasjonsavhengig, blant annet med hensyn til etterretningsbehovet som foreligger og hvilket miljø en opererer i. Etterretningsbehovet vil ofte være overordnet styrende for valg av innhentingsmetode. Menneskebasert innhenting vil gjennom et godt etablert kildenettverk eller en godt plassert enkeltkilde f.eks. kunne skaffe verdifull informasjon om aktørers tankesett, verdensbilde og intensjoner. Ved behov for en detaljert oversikt over fysiske installasjoner og deres geografiske plassering, kan bildeetterretning være en bedre egnet metode.

Ved tekniske innhentingsmetoder søkes gjerne et meget bredt datatilfang, for deretter gjennom analyse å kunne trekke ut det som er viktig for etterretningsformål.

Informasjon som kommer fra én kilde vil i en del tilfeller kunne besvare et konkret etterretningsbehov, mens innhenting fra flere uavhengige kilder og ved bruk av ulike metoder vil kunne ha en gjensidig forsterkende effekt i besvarelsen av et annet etterretningsbehov. Som regel gir kombinasjonen av flere innhentingsmetoder bedre forutsetninger for å besvare et etterretningsbehov, særlig når det gjelder påliteligheten av analysen for å forstå situasjonen helhetlig og korrekt. En forutsetning for det hele er at det er der kommunikasjon og annen informasjon finnes, at Etterretningstjenesten må lete.

10.2.3 Egen innhenting og samarbeid

Hvilke informasjonsbehov Etterretningstjenesten kan besvare, samt ressursbruk og metodebruk for å få besvart informasjonsbehovet, avhenger i all hovedsak av den løpende trussel- og risikovurdering samt bestillingene og føringene fra oppdragsgiverne. I utgangspunktet bør Etterretningstjenesten ved den informasjon tjenesten får fra sine egne kilder, langt på vei kunne løse de viktigste informasjonsinnhentingsoppdrag som norske politiske myndigheter prioriterer. Det er begrunnet i to forhold: For det første har en suveren stat behov for et eget informasjonsgrunnlag for egne handlinger og beslutninger, slik at man ikke blir prisgitt informasjon fra andre stater. For det annet er Etterretningstjenestens viktigste oppdrag knyttet til utenlandske trusler mot Norge og norske interesser, og man kan ikke legge til grunn at andre stater vil prioritere norske interesser foran, eller likestilt med, egne interesser. Informasjonstilgang fra egne kilder er for et relativt lite land og en relativt liten etterretningstjeneste imidlertid ikke tilstrekkelig for å dekke etterretningsbehovet, sett opp mot globale utfordringer og informasjonsbehov. Etterretningstjenesten er derfor avhengig av samarbeid med og informasjon fra andre nasjonale og utenlandske tjenester. Nasjonalt og internasjonalt samarbeid er nærmere behandlet i kapittel 13.

10.3 Gjeldende rett

10.3.1 Dagens regulering er teknologi- og metodenøytral

Dagens lov er i stor grad en fullmaktslov som overlater til regjeringen å regulere Etterretningstjenestens virksomhet. Det gjelder særlig tjenestens metoder for informasjonsinnhenting. Innhentingshjemmelen i etterretningstjenesteloven § 3 er teknologi- og metodenøytral, og nevner ikke hvilke metoder for innhenting som Etterretningstjenesten kan ta i bruk for å tilegne seg informasjon. Stortinget var likevel ikke ukjent med metodebruk for utenlandsetterretningsvirksomhet ved lovens vedtakelse, og i lovens forarbeider ble det redegjort for at tjenesten benytter både menneskebaserte og tekniske innhentingsmetoder. Forarbeidene henviser til at Etterretningstjenestens to hovedmetoder for egeninnhenting av

informasjon er (i) teknisk innhenting gjennom egne lyttestasjoner, av elektroniske data fra radio-, radar- og akustiske kilder, og (ii) menneskebasert innhenting.[199] I tillegg fremgår det at innsamling skjer gjennom samarbeid og informasjonsutveksling med andre lands etterretningstjenester.[200] Utover dette uttrykkes det i forarbeidene ikke annet om Etterretningstjenestens innsamlingskapasitet enn at tjenesten må ha «nødvendig innsamlingskapasitet for prioriterte behov».

10.3.2 Åpen og fordekt innhenting

Å drive etterretning innebærer både åpen og fordekt innhenting av informasjon ved bruk av forskjellige metoder. Informasjon innhentes normalt fordekt av Etterretningstjenesten. Dette skyldes at mesteparten av den informasjonen Etterretningstjenesten må innhente, ikke er offentlig tilgjengelig for enhver. Fordekt innhenting er også nødvendig for at fremmede aktører ikke kan tilpasse sin handlemåte på bakgrunn av kunnskap om hva norske beslutningstakere vet eller har mulighet til å tilegne seg av informasjon.

Formålet med Etterretningstjenestens virksomhet er å verne norsk sikkerhet og suverenitet og å sikre grunnleggende nasjonale sikkerhetsinteresser. Metodene for å oppnå dette vil for enhver etterretningstjeneste kunne reise etiske problemstillinger. I Etterretningstjenestens etiske retningslinjer, som er publisert på www.forsvaret.no, heter det om dette:

> «Paradokset er at tjenesten i denne virksomheten er nødt til å bruke metoder som bryter andre lands lover, som tidvis utfordrer personvernet, og som også fra tid til annen kan bryte med grunnleggende norske kulturelle normer for hvordan vi bør behandle hverandre som mennesker.
>
> Eksempelvis vil signal-, kommunikasjons- og nettverksetterretning tidvis trenge inn i enkeltpersoners privatsfære for å innhente informasjon. Menneskebasert innhenting innebærer en instrumentell utnyttelse av enkeltpersoner for å tilfredsstille informasjonsbehov. I konfliktområder kan den informasjonen E-tjenesten frembringer, bidra direkte og indirekte til å ta menneskeliv. Som en relativt liten etterretningstjeneste er den norske E-tjenesten også nødt til å samarbeide med utenlandske partnere med arbeidsmetoder som kan avvike fra våre egne.
>
> Det å arbeide i E-tjenesten innebærer en grunnleggende aksept for at vi lever i en verden der inngripende arbeidsmetoder tidvis er nødvendige for å trygge norsk suverenitet og demokrati, samt andre viktige nasjonale interesser. Alle tjenestens medarbeidere, både ledere og ansatte, har et ansvar for å bidra til at midlene vi bruker står i forhold til dette formålet, og at tjenestens ressurser kun benyttes med dette for øye.
>
> I praksis kan det være snakk om vanskelige avveininger, og viktige beslutninger om vår virksomhet vil alltid måtte bli tatt av tjenestens ledelse. Gjennom etiske retningslinjer som er forankret hos alle våre ansatte og som derved inngår som en naturlig del av de ansattes daglige virke, ønsker E-tjenesten ytterligere å sikre at våre metoder alltid vil kunne forsvares i henhold til de overordnede målene for vår virksomhet.»

Sitatet illustrerer at det verken er eller bør være fritt frem for å bruke enhver tilgjengelig metode for å løse oppgavene. Nødvendigheten av inngripende metodebruk må avveies mot rettssikkerhets- og personvernhensyn for de som berøres av innhentingen, jf. fremstillingen av forholdsmessighetsprinsippet i punkt 9.5.3. Det er heller ikke normalt opp til

[199] Ot. prp. nr. 50 (1996–1997) s. 8

[200] Ibid s. 9 og 15

saksbehandlere og operatører på lavere nivå å treffe beslutninger om inngripende metodebruk. Metodebruk er en ledelsesstyrt prosess.

10.4 Vurdering av gjeldende rett sett opp mot lovkravet i menneskerettighetene

10.4.1 Bakgrunn og vurderinger

Dagens etterretningstjenestelov, sett på bakgrunn av forarbeidene, tjenestens forhistorie og vedvarende statspraksis, er ansett å gi et alminnelig hjemmelsgrunnlag for bruk av inngripende metoder så lenge det dreier seg om bruk som ligger innenfor lovens formål. Det foreligger klare regler og rutiner for hvordan tjenestens metoder og operasjoner skal behandles, både i E-instruksen[201] § 13 og internt regelverk. Et spørsmål har imidlertid vært om Etterretningstjenestens metodebruk må fremgå klarere av loven.

Lovkravet etter Grunnloven og menneskerettighetene ble berørt i en utredning av professor Erling Johannes Husabø.[202] Fra utredningen hitsettes:

> «Hvilke metoder E-tjenesten kan bruke for å overvåke utlendinger, samt norske borgere i utlandet, sier verken loven eller instruksen noe nærmere om. Det gjør heller ikke de utfyllende bestemmelsene til instruksen som Forsvarsdepartementet vedtok i 2013 (også tilgjengelig på Lovdata). Disse inneholder imidlertid enkelte nærmere regler om informasjonsinnsamling rettet mot norske personer i utlandet og utlevering av personopplysninger til utenlandske samarbeidende tjenester. Blant annet stilles det et uttrykkelig krav om formålsbestemthet og forholdsmessighet både for innsamling og videreformidling av personopplysninger. Det gis også noen nærmere regler om saksbehandlingsregler og beslutningskompetanse.
>
> Samlet sett har E-tjenestens overvåking av utenlandske og (i utlandet) norske borgere et klart svakere hjemmelsgrunnlag enn det som gjelder for PST. At E-tjenesten de senere årene har dreid oppmerksomheten mer mot grupper og individer, som en følge av terrorfaren ute og hjemme, og at tjenesten samarbeider tett med PST om slike saker, gjør dette mer problematisk enn før. Det samme gjør den raske teknologiske utviklingen som gir stadig nye muligheter for overvåking over landegrensene. Generelt har EMD blitt mer skeptisk til statenes argument om at hensynet til nasjonal sikkerhet krever vagere regler på dette området. Å flytte noen av de reglene som nå finnes i instruksen og de utfyllende bestemmelsene opp i loven selv, vil gi bedre tilgjengelighet og større demokratisk legitimitet. Dessuten bør det gis en noe nærmere beskrivelse av hvilke metoder tjenesten kan bruke, særlig i den grad tjenesten skal kunne benytte metoder som ligner eller går ut over de som PST har adgang til. At dette blir gjort i tilsvarende regelverk i enkelte europeiske land, tyder på at det er mulig uten å underminere de hensynene som tjenesten skal ivareta. Det er derfor tvilsomt om dagens hjemmelsgrunnlag for E-tjenesten tilfredsstiller de kravene som nå stilles etter EMK.»

Tjenestens metodebruk i et lovreguleringsperspektiv ble tatt opp av EOS-utvalget i en særskilt melding til Stortinget om rettsgrunnlaget for Etterretningstjenestens

[201] Instruks om Etterretningstjenesten av 31. august 2001 nr. 1012

[202] Se rapport av 11. desember 2015, inntatt som vedlegg 4 i Rapport til Stortinget fra Evalueringsutvalget for Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget), se Dokument 16 (2015–2016).

overvåkingsvirksomhet, som ble fremmet 17. juni 2016.[203] I meldingen pekte utvalget på at lovkravet etter EMK artikkel 8 innebærer at metoder som innebærer et inngrep i artikkelens rettigheter må være tilgjengelige og forutsigbare, og at lovkravet også retter seg mot lovens kvalitet, idet den må oppfylle grunnleggende rettsstatsprinsipper. Utvalget konkluderte med at «(d)et kan være grunn til å utrede nærmere om en lov som ikke regulerer metoder for innhenting av opplysninger om individer tilfredsstiller det lovkravet som er nedfelt i EMK».

Fra kontroll- og konstitusjonskomiteens innstilling til Stortinget om EOS-utvalgets særskilte melding, gjengis:[204]

> «K o m i t e e n mener det er av avgjørende betydning for tilliten til E-tjenesten og faktisk og opplevd trygghet for landet og borgerne, at virkemidler som er forholdsmessige og nødvendige for å utføre tjenestens oppdrag, beskrives gjennom et lovverk som stemmer overens med de utfordringer vi står overfor. Samtidig er det også viktig for å ivareta en demokratisk kontroll av at lovverket blir fulgt, at EOS-utvalget blir gitt tilsvarende justert mulighet for kontroll av virkemiddelbruk.»

På basis av innstillingen ble det truffet vedtak om at:

> «Stortinget ber regjeringen legge frem forslag til revidert lov om Etterretningstjenesten.»

10.4.2 Balanse mellom skjerming og åpenhet

De vurderinger som er referert ovenfor, tilsier at Etterretningstjenestens metoder lovreguleres i en ny lov. Etterretningstjenesten er riktignok fortsatt avhengig av å verne strengt om konkrete opplysninger om tjenestens kilder, metoder og kapasiteter. Den nærmere utforming av bestemmelsene må ta hensyn til at EMD i flere saker har slått fast at statene har en viss skjønnsmargin med hensyn til den konkrete utformingen av reglene, særlig ved inngrep som begrunnes i hensynet til rikets sikkerhet.

Det er verken mulig eller ønskelig å gå i detalj i beskrivelsen av hvordan metoder for informasjonsinnhenting anvendes, da dette vil medføre at fremmede aktører vil tilpasse sin handlemåte til Etterretningstjenestens metoder. Dette vil få alvorlige konsekvenser for informasjonstilfanget for norske offentlige myndigheter og dermed deres evne til å verne norsk suverenitet og grunnleggende nasjonale sikkerhetsinteresser. Det samme gjelder hvordan ulike metoder benyttes i samspill med hverandre, blant annet slik at bruk av én metode kan gi viktige inngangsverdier for bruk av en annen metode, for å løse et konkret innhentingsbehov.

Behovet for hemmelighold må imidlertid balanseres mot kravet om at inngripende virkemidler må ha en åpen regulering og avgrensning i lovs form.

Lovkravet etter menneskerettighetene, særlig etter EMDs domspraksis, er redegjort for generelt i kapittel 4, og dessuten omtalt ovenfor spesielt når det gjelder regulering av metodebruk. Lovkravet taler for en konkret angivelse av tjenestens *metoder* for innhenting av informasjon, regler om *når* metodene kan tas i bruk, regler om *hvem* som kan beslutte anvendelse av metoder i konkrete saker, og regler om *formkrav* til beslutningene.

Departementet legger således til grunn at lovkravet etter EMK innebærer at metoder som utgjør et inngrep i enkeltpersoners privatliv eller kommunikasjonsfrihet krever en konkret og

[203] Dok 7:2 (2015–2016) s. 15

[204] Innst. 164 S (2016–2017) s. 9

tilstrekkelig presis forankring i lov. Hvor detaljert de ulike metodene må reguleres, beror i en viss grad på skjønn og summen av de rettssikkerhetsgarantier og kontrollmekanismer som lovgivningen samlet oppstiller.

10.5 Forslag til lovregulering av Etterretningstjenestens innhentingsmetoder

10.5.1 Generelt

Etterretningstjenesten har siden etableringen i 1942 benyttet ulike metoder for informasjonsinnhenting. Departementet understreker at forslaget til lovregulering av metodebruken i lovutkastet kapittel 6 ikke har til hensikt å utvide verktøykassen av metoder for Etterretningstjenesten. Snarere er hensikten å kodifisere og mer presist avgrense og regulere de enkelte innhentingsmetodene, for å tilfredsstille dagens lovkrav etter menneskerettighetene.

Dagens lov er metode- og teknologinøytral. Dette har blant annet sin årsak i at Etterretningstjenesten arbeider under rammebetingelser som andre land og fremmede aktører ofte kan endre totalt, uten forvarsel og med stor betydning for nasjonale sikkerhetsinteresser. Departementet har derfor søkt å finne en regulering av metodene som på den ene siden sikrer klarere lovgivning, samtidig som reguleringen søker å sikre at tjenesten har den nødvendige evne og mulighet til omstilling og fleksibilitet i målprioriteringer innenfor rammen av loven.

Samtlige metoder som foreslås lovfestet i lovens kapittel 6 kan tas i bruk både for *målsøking* og for *målrettet innhenting*. Det vises til høringsnotatet kapittel 9 om terskelvilkårene for disse to innhentingsformene. Anvendelsen av metodene må imidlertid vurderes konkret, blant annet hvorvidt inngrepet er forholdsmessig sett i lys av formålet med inngrepet, inngrepets art og varighet, inngrepets virkning for den som rammes og omstendighetene for øvrig. Dette følger av forslaget til bestemmelsen om forholdsmessighet i § 5-4.

Et særtrekk ved innhentingsmetodene for en etterretningstjeneste er at de kan og må anvendes uten at de personer som er gjenstand for, eller som på annen måte berøres av, metodebruken er klar over det. Metodene etter kapittelet her kan således anvendes fordekt. Innhentingen skjer fordekt både for å skjerme hvem som står bak innhentingen og det faktum i seg selv at innhentingen skjer. Formålet med innhentingen vil bli vesentlig forfeilet dersom anvendelsen skulle bli kjent. For de personer som berøres, utgjør metodebruken like fullt et inngrep i deres rettssfære, selv om de ikke er kjent med den. Metodene skal derfor kun anvendes når det er nødvendig, forholdsmessig og ellers ikke strider mot øvrige rettsregler som gjelder for tjenesten.

Det er flere måter å inndele metodene på. For å være så konkret som mulig, finner departementet det ønskelig å dele metodene inn på en mer finmasket måte enn å sondre mellom menneskebasert og teknisk innhenting. Videre må det gjøres noen grunnleggende inndelinger avhengig av om metoden er aktiv eller passiv, krever fysisk nærhet til målet eller kan gjennomføres ved fjerntilgang, hvor inngripende metoden er, og hvorvidt informasjon i form av kommunikasjon innhentes mens den er i transitt eller når den er lagret på et endepunkt før og/eller etter informasjonen er sendt/mottatt/produsert. Metodene foreslås inndelt som følger:

1. Åpne kilder
2. Menneskebasert innhenting
3. Systematisk observasjon
4. Teknisk sporing
5. Gjennomsøking, avlytting, skjult bildeovervåking og annen teknisk innhenting
6. Midtpunktinnhenting
7. Endepunktinnhenting

10.5.2 Avgrensning og presiseringer

Etterretningstjenesten retter sin innhenting mot både personer, objekter og fenomener. Departementet anser at det ikke er grunn til å lovhjemle metoder som ikke medfører inngrep overfor enkeltpersoner. Verken menneskerettslige eller andre grunner taler for det. Det ligger i dagen at innhenting av akustiske signaler under vann eller innhenting av satellittbilder av et større område ikke reiser rettssikkerhetsspørsmål eller personvernspørsmål som krever lovregulering. Høyoppløselige satellittbilder som klarer å identifisere enkeltpersoner vil på den annen side kunne ha slike aspekter, og vil etter omstendighetene omfattes av reguleringen vedrørende skjult bildeovervåking. Det foreslås derfor at det i loven fastsettes at kapittel 6 om metodebruk kun gjelder for inngripende metoder i menneskerettslig forstand.

Avgrensningen mot metoder som ikke utgjør inngrep overfor enkeltpersoner, innebærer ikke at bruk av slike metoder ikke er underlagt regler. Lovens øvrige bestemmelser gjelder også for slike metoder. Det gjelder blant annet at innhenting kun kan skje for de formål som fremgår av Etterretningstjenestens oppgaver etter lovforslagets kapittel 3, og at grunnvilkårene for informasjonsinnhenting etter lovforslagets kapittel 5 kommer til anvendelse. Det samme gjelder bestemmelsene i lovforslagets kapittel 2 om styring og kontroll, herunder bestemmelsen om nasjonal kontroll.

Innhenting av grenseoverskridende elektronisk kommunikasjon som transporteres over den norske landegrensen faller i utgangspunktet inn under metoden «midtpunktinnhenting». Denne tilgangen bør etter departementets syn underlegges særskilte lovreguleringer og autorisasjons- og kontrollmekanismer. Departementet viser til høringsnotatet kapittel 11 om dette, og foreslår at det for å unngå enhver tvil fremgår av lovutkastet at kapittel 6 ikke skal gjelde for denne tilgangen. Det presiseres at særreguleringen i lovens kapittel 7 og 8 kun gjelder midtpunktinnhenting der det er nødvendig å oppnå tilgang i medhold av tilretteleggingsplikten etter lovforslagets § 7-2, jf. § 7-1 annet ledd. Denne innhentingsformen kalles i høringsnotatet her for enkelthets skyld «tilrettelagt innhenting».

10.5.3 Forberedende tiltak

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.

10.5.4 Mottak av opplysninger

Metodebruk forutsetter at det finner sted en *utøvende* innsamlingsaktivitet fra Etterretningstjenestens side. Det er derfor ikke å anse som en metode som krever hjemmel etter kapittelet her dersom Etterretningstjenesten *passivt mottar* opplysninger, eller gjenstander som kan inneholde informasjon (f.eks. en mobiltelefon), fra andre som etter eget rettsgrunnlag har innhentet eller på annen måte besitter informasjon. Det gjelder uavhengig av om opplysningene gis uoppfordret eller etter anmodning fra Etterretningstjenesten. Dette prinsippet er blant annet reflektert i lovutkastet § 4-2 fjerde ledd. Forutsetningen er at informasjonen antas å ha relevans for løsningen av Etterretningstjenestens oppgaver slik disse er angitt i lovforslagets kapittel 3. Videre evaluering og behandling av mottatte opplysninger skal da skje etter reglene om behandling av personopplysninger, se høringsnotatet kapittel 12.

Det ligger i dagen at Etterretningstjenesten ikke kan be andre om å innhente informasjon på Etterretningstjenestens vegne, dersom Etterretningstjenesten selv ikke kunne ha innhentet informasjonen etter sitt rettslige grunnlag. Andre norske myndigheter, eksempelvis PST, vil heller ikke ha rettslig grunnlag for å gjennomføre slik innhenting på vegne av Etterretningstjenesten. Etterretningstjenesten kan derimot anmode andre myndigheter om å vurdere innhenting etter eget rettsgrunnlag og for sitt eget formål, men dette blir helt og holdent opp til den innhentende myndighet å beslutte. Ettertids deling i et slikt tilfelle med Etterretningstjenesten, forutsatt at utleverende instans vurderer delingen nødvendig og forholdsmessig, vil ikke være å anse som en omgåelse av Etterretningstjenestens rettsgrunnlag.

10.5.5 Særlige forhold

Det er vesentlig å ha in mente for forståelsen av de ulike metoder beskrevet i det følgende, at Etterretningstjenestens innhentingsvirksomhet er rettet mot svært avanserte og sikkerhetsbevisste aktører i utlandet, og gjerne under risikofylte og fiendtlige omstendigheter. Samtykke fra den som metodebruken rammer er ikke et alternativ. Tidsaspektet, særlig ved trusselaktivitet som er pågående eller nært forestående, må også tas i betraktning. Beslutninger om metodebruk må ofte treffes raskt og ut fra en «føre var»-tilnærming i disse sakene. Det vises for øvrig til kapittel 9 om at det ligger i etterretningsvirksomhetens natur at innhenting ofte må gjennomføres basert på et mangelfullt beslutningsgrunnlag, og at terskelen for metodebruk derfor ikke kan være for høy.

10.5.6 Forslag til regulering

I tråd med overstående drøftelser foreslår departementet følgende lovbestemmelser:

§ 6-1 *Saklig virkeområde og generelle vilkår*

Etterretningstjenesten kan for etterretningsformål benytte metoder etter bestemmelsene i kapittelet her, når grunnvilkårene etter kapittel 5 er oppfylt og innhentingen ikke strider mot øvrige bestemmelser i denne loven. Metodebruk etter kapittelet her kan skje fordekt overfor personer som er

gjenstand for eller som på annen måte berøres av metodebruken. Metodebruk skal avsluttes dersom det blir klart at vilkårene etter loven her ikke lenger er til stede.

Bestemmelsene i kapittelet her kommer bare til anvendelse for innhenting som medfører inngrep overfor den enkelte.

Bestemmelsene i kapittelet her kommer ikke til anvendelse for tilrettelagt innhenting av elektronisk kommunikasjon som transporteres over den norske landegrensen og som reguleres av kapitlene 7 og 8.

§ 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.

10.5.7 Åpne kilder

10.5.7.1 Nærmere om åpne kilder

Informasjonsinnhenting i åpne kilder er innhenting av offentlig/åpent tilgjengelig informasjon fra for eksempel Internett, radiosendinger, foredrag, papiraviser, sosiale medier eller andre kilder. I *åpent* tilgjengelig ligger det at informasjon ikke er skjermet fra allmenheten, og at informasjonen kan innhentes uten at noen form for sikkerhetsbarrierer må brytes. Søk på det mørke nettet (*dark web*) anses i denne sammenheng ikke som prinsipielt skjermet fra allmennheten selv om informasjonen ikke indekseres og er tilgjengelig gjennom vanlige søkemotorer o.l., med mindre spesielle beskyttelsesmekanismer er etablert for å få tilgang til innholdet.

Fiktiv/oppdiktet identitet, slik som fiktive brukeridentiteter-/kontoer, kan benyttes for å skjerme hvem som står bak innhentingen og for å få generell tilgang til den aktuelle tjenesten, uten at dette endrer på at det er informasjonsinnhenting i åpne kilder. Eventuell påfølgende dekryptering anses i denne sammenheng ikke som et ledd i det å oppnå tilgang. Kryptert informasjon kan være åpent tilgjengelig for enhver å laste ned.

Åpne kilder er i dagens informasjonssamfunn en svært relevant metode for å samle inn etterretningsinformasjon, enten på selvstendig grunnlag eller som understøttelse av annen metodebruk. Et eksempel på dette er omfanget av informasjon som deles digitalt av personer i umiddelbar nærhet av viktige hendelser. Departementet mener at Etterretningstjenesten må kunne innhente informasjon fra åpne kilder. Lovforslaget i § 6-2 kodifiserer og presiserer gjeldende metodebruk.

10.5.7.2 Passiv opptreden

Innhentingen forutsetter passiv opptreden, og skjer i mange tilfeller ved fjernavstand til etterretningsmålet. Informasjon fra åpne kilder hentes inn uten å ta fysisk eller logisk kontakt med andre i den hensikt å oppnå tilgang til informasjon som ellers ikke ville ha vært allment tilgjengelig. Aktiv opptreden ved interaksjon mellom mennesker vil være å anse som menneskebasert innhenting. Dersom det benyttes metoder for logisk forsering av sikkerhetsbarrierer for å oppnå tilgang til elektronisk informasjon, vil aktiviteten falle inn under endepunktinnhenting. Dersom det betales vederlag for åpent tilgjengelig informasjon, for eksempel kjøp av informasjon som tilbys enhver på nett eller abonnementsutgifter som enhver kan betale for å få tilgang til informasjon, innebærer dette ikke i seg selv en aktiv opptreden som gjør at man faller utenfor kategorien åpne kilder. Men dersom det f.eks. er nødvendig å manipulere noen eller noe for å få den ønskede tilgang, vil man som oftest være utenfor åpne kilder som innhentingsmetode. Det vil på den annen side fortsatt være

innhenting i åpne kilder hvis Etterretningstjenesten, for å opprettholde troverdighet eller eksistens som fiktiv bruker på nett, må opptre med en viss aktivitet slik andre brukere normalt gjør, når dette ikke er begrunnet med å oppnå tilgang til spesifikk informasjon.

Påfølgende bearbeidelse av informasjonen som er egnet til å besvare et konkret informasjonsbehov betegnes på engelsk som *open source intelligence*, forkortet OSINT. Innhenting av informasjon i åpne kilder danner grunnlaget for OSINT-produksjon.

10.5.7.3 Inngrepets karakter

Både kommersielle og offentlige aktører innhenter opplysninger som er åpent tilgjengelige, herunder opplysninger som er personopplysninger. Opplysningene er i stor grad offentliggjort av personene selv, typisk gjennom sosiale medier. Normalt vil derfor innhenting av åpne kilder ikke være av særlig inngripende karakter for den enkelte. I tillegg vil personvernbegrunnede krav om rettslig behandlingsgrunnlag for å behandle opplysninger fra åpne kilder ivareta viktige rettssikkerhetsaspekter, jf. kapittel 12 nedenfor. Departementet foreslår likevel å regulere metoden særskilt fordi innhentingen ikke skjer med samtykke fra den eller de personer som berøres av innhentingen, og fordi summen av informasjon som innhentes om en og samme person, og sammenstillingen av slik informasjon over tid, etter omstendighetene kan utgjøre et inngrep overfor den enkelte, selv om den enkelte selv har valgt å dele informasjonen åpent.

10.5.7.4 Forslag til regulering

Departementet foreslår følgende lovbestemmelse:

§ 6-2 *Åpne kilder*

Etterretningstjenesten kan innhente informasjon fra åpne kilder.

Etterretningstjenesten kan bruke fiktive brukeridentiteter og -kontoer for å skjerme hvem som står bak innhentingen.

Med åpne kilder menes informasjon som er åpent tilgjengelig. Informasjon er ikke åpent tilgjengelig dersom tilgang krever forsering av passord eller lignende beskyttelsesmekanismer, eller dersom tilgang krever aktivt fordekt opptreden.

10.5.8 Menneskebasert innhenting

10.5.8.1 Nærmere om menneskebasert innhenting

Med menneskebasert innhenting menes systematisk innhenting av informasjon gjennom samhandling mellom mennesker. Samhandlingen kan skje både i det fysiske og det digitale rom. Forslaget kodifiserer og presiserer gjeldende rammer for bruk av menneskebasert innhenting og gjeldende praksis.

Menneskebasert innhenting inkluderer kildeverifikasjon. Med kildeverifikasjon menes innhenting og vurdering av informasjon for å fastslå hvorvidt en potensiell eller eksisterende kilde besitter eller kan skaffe tilgang til relevant informasjon for etterretningsformål, samt fastslå vedkommendes identitet, motivasjon, troverdighet og egnethet. *Kilde* defineres i denne sammenheng som en person som kultiveres, rekrutteres eller føres av Etterretningstjenesten for å gjennomføre innhenting, eller person som utfører oppdrag for Etterretningstjenesten ved å tilrettelegge for innhenting. En organisasjon eller et miljø kan fungere som kilde inntil relevante enkeltpersoner innenfor organisasjonen eller miljøet er identifisert. Det vises til legaldefinisjonene i § 1-4 nr. 5 og 6.

Menneskebasert innhenting innebærer i kjernen å finne, rekruttere, trene og føre individer i den hensikt å innhente informasjon som ikke er offentlig tilgjengelig, eller tilrettelegge for slik informasjonsinnhenting. Kildens sikkerhet og aktivitetens sensitive natur er dimensjonerende

for skjermingsbehovet til operasjonene. Menneskebasert innhenting må underlegges stor grad av hemmelighold.

Menneskebasert innhenting er den eldste etterretningsmetoden, og den mellommenneskelige relasjonen er en grunnleggende og varig faktor. Så lenge det finnes mennesker vil menneskebasert innhenting forbli relevant for Etterretningstjenestens oppdragsløsning – også i et høyteknologisk samfunn. Menneskebasert innhenting er av en særskilt karakter som ikke kan erstattes av andre metoder, uavhengig av teknologisk utvikling. For eksempel vil en aktørs intensjoner ikke nødvendigvis være registrert i en form som direkte kan samles inn teknisk. Menneskebasert innhenting er videre godt egnet som et supplement til, eller til å bli supplert av, andre innhentingsmetoder for effektiv løsning av Etterretningstjenestens oppdrag.

10.5.8.2 Aktiv opptreden

Menneskebasert etterretning er en aktiv metode. I dette ligger det at mennesker anspores til å gjøre noe. Når hensikten er etterretningsproduksjon, innhentes opplysninger fra en menneskelig kilde. Dersom formålet er tilrettelegging av etterretningsoperasjoner, utfører kilden tjenester og/eller stiller fasiliteter til rådighet. Kilder kan innhente opplysninger eller utføre andre etterretningsrelaterte oppgaver som Etterretningstjenesten i sin natur ikke kan utføre selv.

Relasjonen mellom Etterretningstjenesten og en kilde kan enten være deklarert, og dermed kjent for kilden, eller ikke. For å skjerme en menneskebasert innhentingsoperasjon kan det nyttes dekke med virkemidler som blant annet dekkstrukturer samt uriktige, falske eller villedende identiteter, dokumenter og opplysninger. Det vises til lovforslagets § 11-5 annet ledd.

10.5.8.3 Infiltrasjon og provokasjon

Menneskebasert innhenting kan skje ved at kilden selv enten tar kontakt eller blir kontaktet, og ønsker å bistå ved å tilby informasjon. Menneskebasert innhenting kan imidlertid også inkludere infiltrasjon og provokasjon, noe som ofte vil være nødvendig for å oppnå formålet med innhentingen og ivareta sikkerheten for operasjonen og personellet involvert. Det finnes ikke allmenngyldige definisjoner av infiltrasjon og provokasjon, og man kan ikke uten videre legge til grunn det samme meningsinnhold som i politietterforskning. Med *infiltrasjon* i lovforslaget menes å utgi seg for å være noen andre for å få innpass eller tilgang til et forum, organisasjon, miljø eller lignende. Det ligger i den menneskebaserte innhentingens natur at Etterretningstjenestens personell og kilder må gjennomføre infiltrasjon for å oppnå den ønskede interaksjon med de personer som besitter eller har eller vil få tilgang til informasjon av etterretningsverdi. Med *provokasjon* menes i lovforslaget initierende handlinger fra etterretningsoffiseren eller kilden for å påvirke handlingsmønsteret til den som utsettes for provokasjonen. Det kan for eksempel være å etterspørre informasjon som det for en annen person er ulovlig å selge eller på annen måte gi fra seg.

Etterretningstjenestens personell og kilder vil i utgangspunktet ikke ha et rettslig grunnlag for å fremprovosere straffbare handlinger etter norsk rett som ellers ikke ville ha blitt begått. Etterretningstjenestens personell og kilder må imidlertid kunne måtte overvære og til dels medvirke til mindre alvorlige straffbare forhold etter norsk rett, og i nødretts- og nødvergesituasjoner til mer alvorlige straffbare forhold, for å opprettholde troverdighet som infiltratør eller ivareta eget liv og egen helse. Den alminnelige rettsstridsreservasjonen, doktrinen om lovlige myndighetshandlinger, bestemmelsene etter lovforslaget her og i

unntakssituasjoner nødrett eller nødverge kan medføre at handlinger som ellers ville ha vært straffbare likevel er lovlige og straffrie etter en forholdsmessighetsvurdering. Medvirkning til virksomhet som innebærer en reell risiko for at ufravikelige og andre grunnleggende menneskerettigheter krenkes vil på den annen side ikke være akseptabelt, jf. forslaget til § 1-3 annet ledd.

10.5.8.4 Forslag til regulering

Departementet foreslår følgende lovbestemmelse:

§ 6-3 *Menneskebasert innhenting*

Etterretningstjenesten kan ved aktiv opptreden i det fysiske eller digitale rom gjennomføre menneskebasert innhenting og kildeverifikasjon.

Menneskebasert innhenting kan inkludere infiltrasjon og provokasjon.

Med menneskebasert innhenting menes systematisk innhenting av informasjon gjennom samhandling mellom mennesker.

10.5.9 Systematisk observasjon

10.5.9.1 Nærmere om systematisk observasjon

Med systematisk observasjon menes planlagte visuelle iakttakelser i det fysiske rom av en person eller gruppe av personer, eiendom, virksomhet, område eller andre relevante etterretningsmål. Det foreslås lovfestet at Etterretningstjenesten kan foreta systematisk observasjon på offentlig sted hvor etterretningsmål med sannsynlighet antas å befinne seg eller oppsøke. Det samme gjelder mot privat lukket sted dersom den som observerer befinner seg utenfor. Det kan tas i bruk hjelpemidler for observasjon, opptak og annen dokumentasjon.

Ikke alle spaningslignende tiltak krever hjemmel i lov. Den nedre grensen for hva som utgjør et inngrep i privatlivet er drøftet i høringsnotatet punkt 4.2.3.3. Departementet mener likevel gode grunner taler for å lovhjemle grensene for systematisk observasjon for slik å angi klare rammer for denne metoden. Forslaget kodifiserer og presiserer gjeldende praksis.

10.5.9.2 Aktiv opptreden

Systematisk observasjon er en aktiv metode og innebærer fysisk tilstedeværelse for personellet som gjennomfører metodebruken innenfor siktlinje til målet, med den risiko dette innebærer. Det er hovedsakelig en ikke-teknisk innsamlingsmetode, men kan støttes av tekniske hjelpemidler, f.eks. kikkerter. Metodebruken er ressurskrevende og derfor normalt avgrenset i tid og sted, men kan i særlig viktige saker innebære mer langvarig systematisk innhenting.

Etterretningsformålet med systematisk observasjon omfatter blant annet beskyttelse av egne operasjoner, målsøking, målverifikasjon og støtte for annen metodebruk, herunder:

- Å avklare normalsituasjonen på et sted og følge med på eventuelle endringer
- Å avklare om individer utgjør en sikkerhetstrussel mot pågående operasjoner og aktiviteter
- Å samle inn informasjon om individer som er etterretningsmål.

Behovet for systematisk observasjon og hvem og hva som observeres er situasjonsavhengig og må nødvendigvis baseres på en etterretningsfaglig vurdering. Behovet kan endres underveis i et oppdrag.

10.5.9.3 Forslag til regulering

Departementet foreslår følgende lovbestemmelse:

§ 6-4 *Systematisk observasjon*

Etterretningstjenesten kan foreta systematisk observasjon på offentlig sted hvor etterretningsmål med sannsynlighet antas å befinne seg eller oppsøke. Det samme gjelder mot privat lukket sted dersom den som observerer befinner seg utenfor.

Det kan tas i bruk hjelpemidler for observasjon, opptak og annen dokumentasjon.

Med systematisk observasjon menes planlagte visuelle iakttakelser i det fysiske rom av en person eller gruppe av personer, eiendom, virksomhet, område eller andre relevante etterretningsmål.

10.5.10 Teknisk sporing

10.5.10.1 Nærmere om teknisk sporing

Med teknisk sporing menes plassering av tekniske peilemekanismer på eller ved en person eller et objekt, i den hensikt å kartlegge posisjon og bevegelser.

Det foreslås at Etterretningstjenesten kan ta i bruk teknisk sporing dersom det for etterretningsformål anses å ha eller kunne få betydning å lokalisere en person eller gjenstand. Forslaget kodifiserer og presiserer gjeldende metodebruk.

Teknisk sporing innebærer at peileutstyr festes på et etterretningsmål eller på en gjenstand eller transportmiddel som benyttes av etterretningsmålet, i den hensikt å kartlegge målets posisjon og bevegelser. Dersom sporingen gjennomføres ved å avlese posisjon fra etterretningsmålets elektroniske utstyr, som for eksempel en mobiltelefon eller datamaskin, vil dette være endepunktinnhenting eller midtpunktinnhenting, avhengig av hvor informasjonen kan observeres, og ikke teknisk sporing.

Sporingsinnretningen skal kun være aktiv så lenge det anses å ha eller kunne få betydning for aktuelle prioriterte etterretningsbehov. Dette vil som oftest være begrenset til varigheten av en etterretningsoperasjon som har en definert sluttilstand og sluttidspunkt.

10.5.10.2 Forslag til regulering

Departementet foreslår følgende lovbestemmelse:

§ 6-5 *Teknisk sporing*

Etterretningstjenesten kan ta i bruk teknisk sporing for å lokalisere en person eller gjenstand.

Med teknisk sporing menes plassering av tekniske peilemekanismer i det fysiske rom på eller ved et etterretningsmål, i den hensikt å kartlegge målets posisjon og bevegelser.

10.5.11 Gjennomsøking, avlytting, skjult bildeovervåking og annen innhenting med tekniske midler

10.5.11.1 Nærmere om annen innhenting med tekniske virkemidler

Med gjennomsøking menes undersøkelse av bolig, rom, oppbevaringssted eller person for å søke etter informasjon eller gjenstander.

Med avlytting og skjult bildeovervåking menes utplassering av kamera, mikrofon eller andre tekniske sensorer på eller i nærheten av et sted hvor det er rimelig å anta at et etterretningsmål vil oppholde seg.

Med annen innhenting med tekniske midler menes enhver innhenting ved bruk av tekniske sensorer eller tilgangsmetoder som ikke reguleres av §§ 6-7 eller 6-8, herunder bildeovervåking av enkeltpersoner fra sensorer i det ytre rom eller fra luftbårne plattformer. Dette vil typisk være innhenting med andre typer sensorer enn kamera og mikrofon, som

krever at sensor plasseres i fysisk nærhet til målet og som er egnet til å kartlegge aktiviteten til et aktuelt etterretningsmål. Slik innhenting kan imidlertid også dreie seg om fjerninnhenting og ikke-fysisk nærhet, eksempelvis bildeovervåking av enkeltpersoner fra rombaserte sensorer (typisk satellitter) eller fra andre luftbårne plattformer (typisk droner).

Disse metodene er – når de benyttes utenfor offentlig sted – til dels meget inngripende og ofte ressurskrevende, og vil normalt benyttes i en meget begrenset tidsperiode. Metoden vil være spisset inn mot det aktuelle etterretningsmålet og skal ikke innrettes slik at tilfeldige personer som befinner seg i nærheten av det aktuelle området blir unødvendig omfattet av innhentingen. Eventuell overskuddsinformasjon vil uansett bli slettet så tidlig som mulig i den påfølgende prosessen.

Gjennomsøking, avlytting, skjult bildeovervåking og annen teknisk innhenting vil kunne kombineres med endepunktinnhenting mot datautstyr som måtte befinne seg på det aktuelle stedet, ofte omtalt som *computer forensics*.

Departementet foreslår en lovhjemmel for gjennomsøking, avlytting, skjult bildeovervåkning og annen teknisk innhenting som kodifiserer og presiserer gjeldende rammer og praksis.

10.5.11.2 Forhøyet terskelkrav

Der aktiviteten gjennomføres på eller mot sted som etter sin art ikke er tilgjengelig for alle, mener departementet at terskelen for når tiltaket kan benyttes må ligge høyere enn dersom det er snakk om offentlig sted. Departementet mener at tiltaket i disse tilfeller bare bør kunne gjennomføres dersom det anses *strengt nødvendig* for ivaretakelsen av Etterretningstjenestens oppgaver etter kapittel 3.

Departementet mener det er hensiktsmessig at forståelsen av hva som menes med «sted som etter sin art ikke er tilgjengelig for alle», tar utgangspunkt i tilsvarende grensedragning i straffeprosessloven § 193.[205] Det høyere terskelkravet for bruk av denne metoden på slike steder («strengt nødvendig» for oppgaveløsningen) innebærer at metoden kun skal anvendes dersom de øvrige vilkår for innhenting foreligger, og det i tillegg vurderes i den konkrete saken at bruken av metoden vil kunne frembringe etterretningsinformasjon som vil kunne stå sentralt eller på annen måte være viktig for å besvare et prioritert etterretningsbehov. Normalt vil denne vurderingen dekkes av den alminnelige bestemmelsen om forholdsmessighet i lovutkastet § 5-4, men departementet finner likevel grunn til å synliggjøre at det kan tenkes tilfeller hvor inngrepet vil være forholdsmessig, for eksempel fordi man ikke har noen andre relevante metoder tilgjengelig, men hvor metoden likevel ikke kan tas i bruk fordi innhentingen ikke kan sies å være strengt nødvendig for tjenestens samfunnsoppdrag.

Avlytting og skjult bildeovervåking innebærer at kamera, mikrofon eller andre tekniske sensorer plasseres på et sted hvor det er rimelig å anta at et etterretningsmål vil oppholde seg. Avlytting eller skjult kameraovervåking vil også kunne gjennomføres ved hjelp av innhenting fra endepunktsensorer, f.eks. fra kamera eller mikrofon på mobiltelefon. Dette vil i så tilfelle være å anse som endepunktinnhenting, da dette krever logisk forsering av sikkerhetsmekanismer på endepunktet, i motsetning til utplassering av egne sensorer.

10.5.11.3 Forslag til regulering

Departementet foreslår følgende lovbestemmelse:

[205] Lov om rettergangsmåten i straffesaker av 22. mai 1981 nr. 25

§ 6-6 *Gjennomsøking, avlytting, skjult bildeovervåkning og annen innhenting med tekniske midler*

Etterretningstjenesten kan gjennomføre gjennomsøking, avlytting, skjult bildeovervåkning og annen innhenting med tekniske midler. Dersom tiltaket gjennomføres på eller mot sted som etter sin art ikke er tilgjengelig for alle, kan tiltaket bare gjennomføres dersom tiltaket anses strengt nødvendig for ivaretakelsen av Etterretningstjenestens oppgaver etter kapittel 3.

Med gjennomsøking menes undersøkelse av bolig, rom, oppbevaringssted eller person for å søke etter informasjon eller gjenstander.

Med avlytting og skjult bildeovervåking menes utplassering av kamera, mikrofon eller andre tekniske sensorer på eller i nærheten av et sted hvor det er rimelig å anta at et etterretningsmål vil oppholde seg.

Med annen innhenting med tekniske midler menes enhver innhenting ved bruk av tekniske sensorer eller tilgangsmetoder som ikke reguleres av §§ 6-7 eller 6-8, herunder bildeovervåking av enkeltpersoner fra rombaserte sensorer eller luftbårne plattformer.

10.5.12 Midtpunktinnhenting

10.5.12.1 Nærmere om midtpunktinnhenting

Med midtpunktinnhenting menes innhenting av elektronisk kommunikasjon og kartlegging av kommunikasjonsinfrastruktur. Med elektronisk kommunikasjon menes kommunikasjon ved bruk av et system for signaltransport som muliggjør overføring av lyd, tekst, bilder eller andre data.

Departementet foreslår en lovhjemmel for at Etterretningstjenesten kan gjennomføre midtpunktinnhenting av kommunikasjon, som kodifiserer og presiserer gjeldende rammer og praksis.

Midtpunktinnhenting innebærer å fange opp kommunikasjonssignaler under transport mellom en avsender og en mottaker. Eksempler på aktuelle kommunikasjonsbærere i denne sammenheng kan være radiokommunikasjon, kommunikasjon over telenettet/internett eller satellittkommunikasjon.

10.5.12.2 Passiv opptreden

Midtpunktstilgang er en passiv metode. I dette ligger det at innhentingen skjer ved å avlese/avlytte passivt og uten at sikkerhetsmekanismer brytes for å få tak i informasjonen. Eventuell dekryptering av informasjonen endrer ikke dette, da det skjer etter at tilgang er etablert og data er innhentet. Elektronisk kommunikasjon er i dag i økende grad kryptert under transport. Metoden er likevel av avgjørende betydning, da tilgangen gir viktige inngangsverdier til målsøkingsprosessen og til tjenestens øvrige metoder. Som det vises til i punkt 8.3.2, vil verdien av midtpunktinnhenting som metode ofte kreve bulkinnhenting i metadata knyttet til kommunikasjonen.

Communications intelligence, forkortet COMINT, benyttes gjerne som et samlebegrep både for å beskrive tilgang, analyse og produkt innen kommunikasjonsetterretning. I en slik sammenheng er ofte midtpunktinnhenting underforstått. Etter hvert som endepunktstilgang har blitt mer og mer relevant når det gjelder å produsere kommunikasjonsetterretning, er det imidlertid behov for å skille mellom de ulike tilgangsmetodene. Det blir dermed mer nøyaktig å avgrense COMINT-begrepet til bearbeidelse og analyse av kommunikasjonsdata, samt selve produktet som svarer på informasjonsbehovet.

10.5.12.3 Forslag til regulering

Departementet foreslår følgende lovbestemmelse:

§ 6-7 *Midtpunktinnhenting*

Etterretningstjenesten kan gjennomføre midtpunktinnhenting.

Med midtpunktinnhenting menes innhenting av elektronisk kommunikasjon og kartlegging av kommunikasjonsinfrastruktur. Med elektronisk kommunikasjon menes kommunikasjon ved bruk av et transport- eller overføringssystem som muliggjør overføring av lyd, tekst, bilder eller andre data.

10.5.13 Endepunktinnhenting

10.5.13.1 Nærmere om endepunktinnhenting

Med endepunktinnhenting menes teknisk observasjon av og innhenting av ikke åpent tilgjengelig elektronisk lagrede data i datasystem eller lignende system eller tjeneste, når innhentingen ikke er å anse som midtpunktinnhenting.

Endepunktinnhenting innebærer å avlytte eller avlese informasjon direkte fra en elektronisk kommunikasjonsenhet eller datamaskin som tilhører et etterretningsmål eller annet system hvor relevante etterretningsdata ligger lagret eller blir behandlet. Dette til forskjell fra midtpunktinnhenting, hvor informasjonen hentes inn under transport. Med lagrede data forstås både informasjon i dataminne og på lagringsmedier.

Det foreslås en lovbestemmelse som hjemler at Etterretningstjenesten kan gjennomføre endepunktinnhenting av informasjon i systemer og tjenester som etterretningsmål besitter eller antas å ville benytte. Forslaget kodifiserer og presiserer gjeldende metodebruk.

10.5.13.2 Aktiv opptreden

Endepunktinnhenting er en aktiv metode som normalt innebærer forsering av sikkerhetsmekanismer for å få tilgang til enheten. Så langt mulig vil innhentingen gjennomføres slik at det ikke unødig voldes fare for driftshindring eller for skade på utrustning eller data, samt at utenforstående ikke som følge av gjennomføringen av innhentingen får uberettiget tilgang til datasystemet eller lignende system/tjeneste.

Innhentingen kan blant annet skje over internettet, telenettet eller ved fysisk varig eller midlertidig tilgang til endepunktet.

Endepunktinnhenting vil i tillegg til å kunne hente ut lagret informasjon som ikke er ment for kommunikasjon, slik som kontaktlister, også kunne benyttes til å hente ut kommunikasjonsdata, for eksempel eposter. Den samme informasjonen vil dermed potensielt kunne hentes ut både ved hjelp av midtpunktinnhenting og ved endepunktinnhenting. Forskjellen er at midtpunktinnhenting innebærer en passiv tilgang (avlesing/avlytting) til informasjon under transport, mens endepunktinnhenting gjøres aktivt (forsering av sikkerhetsmekanismer) mot endepunktene.

10.5.13.3 Forhøyet terskelkrav

Endepunktinnhenting kan i grove trekk sammenlignes med politiets dataavlesing,[206] selv om formålet med innhentingen etter lovforslaget her er rettet mot mål i utlandet og skjer for etterretningsformål knyttet til rikets sikkerhet og ikke for å forebygge eller motvirke straffbare handlinger av kvalifisert art. Endepunktinnhenting kan likevel innebære et stort inngrep i enkeltpersoners personvern i utlandet.

Innhenting av informasjon som lagres på et endepunkt uten å være kommunisert til andre, kan anses å utgjøre et større inngrep enn innhenting av innholdet i brukerens kommunikasjon. Departementet finner derfor grunn til å skille mellom data som det er grunn til å tro at er ment for kommunikasjon og ikke. For førstnevnte bør terskelen være identisk for

[206] Se kapittel 14 i Prop. 68 L (2015–2016).

både midtpunktinnhenting og endepunktinnhenting. For sistnevnte kategori bør det etter departementets syn gjelde et høyere terskelkrav, ved at innhentingen i disse tilfellene må anses *strengt nødvendig* for ivaretakelsen av Etterretningstjenestens oppgaver etter lovutkastet kapittel 3 – i tillegg til de øvrige alminnelige vilkår for å kunne ta i bruk metoden. I vurderingen av kravet om streng nødvendighet må det tas i betraktning at metoden har stor og økende verdi overfor meget viktige etterretningsmål. Kravet betinger at det foretas en konkret forholdsmessighetsvurdering av tiltakets inngripende karakter, informasjonens relevans for tjenestens oppdragsløsning, og om mindre inngripende metoder kan brukes for å oppnå samme resultat. Dersom sistnevnte besvares bekreftende, vil det strenge nødvendighetskravet vanskelig være oppfylt.

10.5.13.4 Forslag til bestemmelse

Departementet foreslår følgende lovbestemmelse:

§ 6-8 *Endepunktinnhenting*

Etterretningstjenesten kan gjennomføre endepunktinnhenting av informasjon i systemer og tjenester som etterretningsmål besitter eller antas å ville benytte. Dersom det er grunn til å tro at innhentingen vil inneholde data som ikke er ment for kommunikasjon, skal tiltaket bare iverksettes dersom det anses strengt nødvendig for ivaretakelsen av Etterretningstjenestens oppgaver etter kapittel 3.

Med endepunktinnhenting menes teknisk observasjon av og innhenting av ikke åpent tilgjengelig elektronisk informasjon i datasystem eller lignende system eller tjeneste, når innhentingen ikke er å anse som midtpunktinnhenting.

10.6 Rettssikkerhetsgarantier og beslutningsprosedyrer

10.6.1 Generelt

Ikke bare lovreguleringen som sådan, men også de aktuelle metodene og anvendelsen av dem, må være formålsavgrenset og tjene til oppfyllelse av et legitimt formål. Hvor tungtveiende samfunnshensyn det dreier seg om, vil ha mye å si for om inngrepet er lovlig etter Grunnloven og EMK.

Departementet legger opp til at enhver bruk av inngripende metoder bare kan besluttes iverksatt dersom metoden er nødvendig for, formålsavgrenset til, og egnet til å bidra til å løse, Etterretningstjenestens oppgaver slik disse er uttømmende foreslått i lovutkastet kapittel 3, og forholdsmessig etter en avveining mellom viktige stats- og samfunnssikkerhetshensyn på den ene siden og konsekvensene for den enkelte på den andre siden. Dersom den samme informasjonen kan fremskaffes ved å bruke en tilgjengelig metode som er mindre inngripende, vil bruk av den mer inngripende metoden ikke være forholdsmessig.[207] I en totalvurdering av om inngripende metoder kan tas i bruk, må det også sees hen til lovforslagets øvrige rettssikkerhetsgarantier, regler for å hindre myndighetsmisbruk og regler som sikrer innsyn og kontroll av uavhengige kontrollinstanser.

[207] Se mer om forslaget til konkret forholdsmessighetsvurdering etter en lovfestet standard i lovutkastet § 5-4 som omtalt i punkt 9.5.3

10.6.2 Forhåndsautorisasjon

Departementet 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. En slik ordning vil innebære en dramatisk endring av gjeldende praksis som vil svekke tjenestens effektivitet og som vil innebære et avvik fra hva som gjelder for sammenlignbare etterretningstjenester i andre land. Det er avgjørende at den som beslutter metodebruk har oversikt over alle tilgjengelige kapasiteter, har kunnskap om etterretningsfaglige, risikomessige og ressursmessige aspekter ved bruk av ulike metoder, forstår hvordan ulike metoder kan spille sammen og kjenner saksfeltenes viktighet i en nasjonal og internasjonal kontekst. Også antallet metodebeslutninger (normalt flere hver dag) og sikkerhetsmessige hensyn knyttet til de mest skjermingsverdige operasjonene, som også kan berøre samarbeid med andre lands etterretningstjenester, innebærer at det ikke vil være praktisk mulig å legge beslutningsmyndigheten i enkeltsaker utenfor tjenesten.

Etterretningstjenestens innhentingsaktivitet er rettet mot forhold i utlandet, ofte i kaotiske områder og innenfor ikke-vennligsinnede staters jurisdiksjon. Dette gjør det tilnærmet umulig for en norsk domstol eller annen uavhengig instans å skulle ta selvstendig stilling til faktum i sakene, særlig med tanke på det tidspress som normalt foreligger. Departementet frykter at man med en slik løsning i praksis vil ende opp med en forhåndsautorisasjonsinstans som ikke vil være i stand til å fatte rettidige avgjørelser, som avslår alle begjæringer og dermed setter tjenesten ute av stand til å utføre sitt samfunnsoppdrag – eller som bidrar til en form for falsk legitimitet for tjenestens metodebruk, men som i realiteten ikke har god innsikt i egne avgjørelser. Verken alminnelig sivilprosess eller straffeprosess er egnet til å regulere saksgangen i denne type saker. Dette ville derfor kreve utarbeidelse av en tilpasset prosessordning, og det ville kreve omfattende ressursbruk hos domstolene eller tilsvarende instans å ta stilling til så mange saker på så kort tid med så store krav til saksinnsikt i forhold som ligger utenfor norsk territorium.

Departementet vil understreke at man ikke uten videre kan trekke noen analogi fra forutgående rettslig prøving av straffeforfølgende myndigheters tvangsmiddelbruk, da formålet og den rettslige begrunnelsen for slike myndigheters virksomhet er vesensforskjellig fra strategisk utenlandsetterretning.

Departementet viser også til fast og langvarig praksis for at Etterretningstjenesten, og på visse vilkår departementet, beslutter metodebruk uten ekstern og uavhengig forhåndsautorisasjon. Denne praksisen har siden 1998 blitt kontrollert av EOS-utvalget, som har anledning til å kontrollere all metodebruk i tjenesten, uten at det har foreligget grunnlag for kritikk.

Man kan alternativt se for seg en løsning der den uavhengige instansen på overordnet nivå skulle forhåndsautorisere metodebruk for hele saksområder. Dette ville være praktisk mulig, men en slik ordning vil i realiteten innebære at denne instansen overtar styringen av Etterretningstjenestens virksomhet og resultatmål til fortrengsel for de alminnelige styringsmekanismer. Lignende synspunkter sto sentralt ved opprettelsen av EOS-utvalget i 1996, hvor prinsippet om etterfølgende kontroll ble ilagt avgjørende vekt.[208] Bakgrunnen for prinsippet om etterfølgende kontroll var blant annet oppfatningen om at EOS-utvalget ikke

[208] Se Evalueringsutvalgets rapport i Dokument 16 (2015–2016) s. 122 med videre henvisninger.

skulle ha noen styringsfunksjoner, altså at kontrollen ikke skulle bli så inngripende eller innrettes på en slik måte at regjeringens og fagdepartementets styringsmulighet og -ansvar ble vesentlig svekket. Et annet vesentlig poeng var at kontrollorganet ikke måtte utvikle seg til å bli et styre som legitimerte tjenestens disposisjoner. De samme argumenter for innretningen av kontrollen med tjenestens metodebruk gjør seg etter departementets syn gjeldende også i dag.

En uavhengig forhåndsgodkjenningsordning vil dessuten ikke ivareta behovet for konkrete forholdsmessighetsvurderinger av metodebruk knyttet til spesifikke etterretningsmål eller -operasjoner, hvor omstendighetene kan være i konstant endring.

På bakgrunn av ovennevnte momenter fremstår en ordning med uavhengig forhåndsautorisering av Etterretningstjenestens metodebruk som lite hensiktsmessig, kostbar og ineffektiv. Departementet kan heller ikke se at en slik ordning vil medføre noen vesentlig rettssikkerhetsmessig gevinst. Det vil dessuten avvike fra det som gjelder for nær sagt alle andre sammenlignbare lands etterretningstjenester.

Departementet mener imidlertid at det er behov for særlige forhåndsautorisasjonsregler og styrket kontroll knyttet til tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon etter lovforslagets kapittel 7 og 8. Årsaken til at det foreslås særregler for denne spesielle tilgangen innenfor rammen av midtpunktinnhenting som metode, er ikke metoden som sådan, men at tilgangen krever metadatalagring som i ikke ubetydelig grad vil inneholde trafikkdata knyttet til personer som oppholder seg i Norge. Se nærmere om den territorielle begrensningen i lovutkastet kapittel 4 og høringsnotatet kapittel 8. Dette er årsaken til at det er nødvendig med særskilt autorisasjon og kontroll med alle søk som gjøres i dette datagrunnlaget. For de metodene som foreslås regulert av lovutkastet kapittel 6, gjør det seg ikke gjeldende tilsvarende hensyn.

10.6.3 Menneskerettslige rammer for metodebruken

Inngripende metoder må holde seg innenfor rammene som oppstilles blant annet i Grunnloven og EMK. Det vises til fremstillingen i kapittel 4. Det vil være lovkravet og kravet om forholdsmessighet som i første rekke setter grenser. Det må legges til grunn at statene har en skjønnsmargin på dette punkt, men rettspraksis indikerer at det går en grense for hva som kan begrunne et inngrep. På grunn av faren for å bruke innhentingsmetoder i et større omfang enn det som er forholdsmessig, har EMD i sin praksis også stilt krav om prosessuelle garantier mot misbruk, jf. blant annet *Malone mot Storbritannia* av 2. august 1984. Saken gjaldt kommunikasjonskontroll, men det må av dommen kunne utledes et krav om prosessuelle garantier som hindrer misbruk ved særlig inngripende tiltak fra offentlige myndigheter i den private sfære. EMD uttaler at slike garantier blant annet kan være domstolskontroll eller annen uavhengig kontroll med myndighetens bruk av slike inngripende tiltak.[209]

Departementet legger til grunn at EOS-utvalgets uavhengige kontroll av tjenestens metodebruk oppfyller EMDs prosessuelle krav, og gir de nødvendige garantier for at metoder ikke misbrukes. Alternativet til EOS-utvalgets etterhåndskontroll av metodebruk er forhåndskontroll av domstol eller domstolslignende organer. Imidlertid vil denne kontrollen være lite anvendelig av flere årsaker, som angitt ovenfor, samt at den gir begrensede

[209] Se *Malone mot Storbritannia* av 2. august 1984, avsnitt 81

ytterligere garantier ut over det som EOS-utvalget kan ivareta. En generell forhåndsautorisasjonsordning vil også skape uklarheter i forhold til departementets styring og kontroll, herunder departementets godkjenning av nye metoder eller bruk av metoder som reiser nye politiske, viktige eller prinsipielle problemstillinger. Det vises for øvrig til omtalen av styring og forvaltningskontroll i kapittel 6.

10.6.4 Materielle og prosessuelle garantier mot vilkårlighet og misbruk

Det at Etterretningstjenestens metoder nå foreslås lovregulert kan i seg selv sies å bidra til større forutsigbarhet og dermed også større rettssikkerhet. Lovforslaget oppstiller dessuten følgende bestemmelser som skal sikre at metodebruk ikke skjer vilkårlig eller benyttes i større grad enn nødvendig:

- Metodene må benyttes formålsbestemt og være knyttet til et oppgavesett som er mer presist angitt og dessuten uttømmende regulert i lovforslaget.
- Grunnvilkår for innhenting og dermed også metodebruk for innhenting foreslås lovfestet.
- Forholdsmessigheten av metodebruk skal vurderes i hvert enkelt tilfelle, jf. forslag om et lovfestet generelt proporsjonalitetsprinsipp i § 5-4.
- For enkelte metoder foreslås lovfestet en høyere terskel for bruk (strengt nødvendig).
- Beslutning om metodebruk skal alltid forankres på sjefsnivå i Etterretningstjenesten, og i særlige saker på departementsnivå.
- Det stilles lovmessige krav til dokumentasjon av vurderinger knyttet til metodebruk, og plikt til regelmessig revurdering og ellers når grunnlaget for beslutningene endres.
- Et styrket EOS-utvalg vil føre effektiv kontroll med tjenestens metodebruk.

Under henvisning til foranstående foreslår departementet at sjefen for Etterretningstjenesten eller den han eller hun bemyndiger skal treffe beslutning om bruk av metoder regulert i kapittelet her, med mindre beslutning tilligger departementet etter lovutkastet § 2-7.

Videre foreslås at beslutninger om metodebruk skal dokumenteres skriftlig gjennom innhentingsplan, operasjonsordre eller lignende skriftlig dokumentasjon. Dokumentasjonen skal angi det eller de etterretningsoppdrag som ligger til grunn for metodebruken, og det eller de etterretningsmål eller kategorier av etterretningsmål som metoden retter seg mot. Etterretningstjenesten har et internt system med et dokumenthierarki som medfører aktiv ledelseskontroll med metodebruk. Av sikkerhetsmessige grunner kan det i et åpent dokument ikke redegjøres nærmere for dette systemet, hvem som er involvert i beslutningsprosessen og hva slags informasjonsgrunnlag som inntas i de ulike godkjenningsskjemaer, operasjons- og plandokumenter. På overordnet nivå utarbeidet Etterretningstjenesten en ugradert skriftlig beskrivelse av sine internkontrollsystemer til utvalget som evaluerte EOS-utvalgets kontroll. Fra rapporten hitsettes:[210]

> «Etterretningstjenesten har etablert internkontrollfunksjoner for å sikre en lovlig og hensiktsmessig utøvelse av tjenestens virksomhet. Disse er av ulik karakter og i nødvendig utstrekning tilpasset disiplin og fagområde. Funksjonene er nedfelt i interne

[210] Dok. 16 (2015–2016) s. 82

bestemmelser, instrukser og retningslinjer. Internkontrollfunksjonene er samlet sett ment å utgjøre et system som både er systematisk og helhetlig.

Tjenesten har bl.a. gjennom regelverk og prosedyrer pålagt seg selv en rekke interngodkjennings-, kontroll- og notoritetsmekanismer. Mekanismene er delvis automatiserte og delvis manuelle. Internkontrollen kan særlig ta form av at godkjenning fra flere instanser i tjenesten er påkrevd før iverksettelse, eller ved særskilt periodisk rapportering og/eller gjennomgang av enkeltsaker for å sikre regelverksetterlevelse.

Et eksempel på en slik mekanisme er at innhenting av informasjon om norske rettssubjekter i utlandet eller deling av personopplysninger om norske personer med samarbeidende tjenester i andre land forelegges ledelsesnivået i tjenesten i hvert enkelt tilfelle.

Et annet eksempel er at det er etablert et eget element i tjenesten som utelukkende har til oppgave å sørge for intern legalitetskontroll i forhold til tjenestens tekniske innhentingsvirksomhet.

I tillegg kommer andre typer ordninger, blant annet opplæringstiltak samt særskilt rådgivning fra – og rapportering til – tjenestens personvernrådgiver og tjenestens juridiske enhet. Tjenesten legger stor vekt på preventive tiltak som opplæring av ansatte i gjeldende regelverk og prosedyrer innen de ulike etterretningsdisipliner. Dette gjøres rutinemessig for alle nytilsatte, samt på seksjons- og/eller avdelingsbasis blant annet når det er gjort endringer i internt regelverk mv.

Det er i tjenesten etablert et system for avviksrapportering. Når et brudd avdekkes, foretas det rutinemessig en etterfølgende vurdering av hvorvidt det dreier seg om systemsvikt eller et enkeltstående avvik. Dette er avgjørende for tjenestens håndtering av bruddet og for hvilke prosesser som iverksettes i etterkant. Avviksrapporter forelegges rutinemessig for EOS-utvalget. Det er ikke avdekket regelverksbrudd de senere år som tjenesten ikke selv har oppdaget og rapportert til EOS-utvalget. Det nevnes for øvrig at tjenesten har implementert en varslingsmekanisme (varslingskanal) som tjenestens ansatte blant annet kan benytte til å innrapportere brudd på regelverk eller tjenestens etiske regler. Rapporteringen kan skje anonymt.

Det interne regelverket og dertil knyttede internkontrollmekanismer vurderes jevnlig med tanke på nødvendighet, tilstrekkelighet og effektivitet. For tjenesten er det vesentlig å ha en dynamisk tilnærming til internt regelverk mv, slik at rutiner og systemer på en forsvarlig måte kan tilpasses den kontinuerlige utviklingen innen bl.a. teknologi og andre operative forhold. Internkontrollordningene drøftes rutinemessig med EOS-utvalget, og tilpasses så langt mulig også EOS-utvalgets kontrollbehov.»

Departementet foreslår videre at vurdering av forholdsmessighet etter § 5-4 skal fremgå av dokumentasjonen. I hastetilfeller kan beslutning treffes muntlig, men skal snarest mulig formaliseres skriftlig. Særlig kan bruk av hastekompetanse være aktuelt ved alvorlige hendelser, for eksempel et terroranslag i utlandet som kan berøre norske interesser. At beslutningene skal formaliseres snarest mulig reduserer risiko for udokumenterte beslutninger som i ettertid kan være vanskeligere å etterprøve og kontrollere.

10.6.5 Varighet

Varighet av metodebruk innenfor ulike oppgavesett og overfor ulike etterretningsmål kan variere betydelig, fra noen sekunders metodebruk til innhenting over mange år. Det er derfor vanskelig å lovregulere spesifikke tidskrav. Beslutningene bør etter departementets vurdering likevel revurderes *minst* en gang i året. Også dersom omstendighetene som lå til grunn for en beslutning vesentlig endres, bør beslutningen snarest mulig revurderes. Det

ligger for øvrig i sakens natur at Etterretningstjenesten ikke vil bruke ressurser på metodebruk som ikke gir den ønskede etterretningsmessige verdi. Metodebruk vil derfor bli avviklet så snart det fremstår som klart at metoden ikke er egnet til å fremskaffe de ønskede opplysninger. At metodebruken skal avsluttes dersom det blir klart at vilkårene etter loven ikke lenger er tilstede følger implisitt av lovens system, men foreslås av pedagogiske grunner presisert i lovutkastet § 6-1 første ledd siste punktum.

Departementet foreslår etter dette følgende lovbestemmelse om beslutningsprosess for metodebruk:

§ 6-10 *Beslutningsprosess for metodebruk*

Sjefen for Etterretningstjenesten eller den han eller hun bemyndiger treffer beslutning om bruk av metoder regulert i kapittelet her, med mindre beslutning tilligger departementet etter § 2-7.

Beslutninger om metodebruk skal dokumenteres skriftlig gjennom innhentingsplan, operasjonsordre eller lignende skriftlig dokumentasjon. Dokumentasjonen skal angi det eller de etterretningsoppdrag som ligger til grunn for metodebruken, og det eller de etterretningsmål eller kategorier av etterretningsmål som metoden retter seg mot. Vurdering av forholdsmessighet etter § 5-4 skal fremgå av dokumentasjonen.

I hastetilfeller kan beslutning treffes muntlig, men skal snarest mulig formaliseres skriftlig.

Dokumentasjonen som nevnt i annet ledd skal revurderes minst en gang i året. Dersom omstendighetene som lå til grunn for en beslutning vesentlig endres, skal beslutningen snarest mulig revurderes.

11 Særregler om innhenting av grenseoverskridende elektronisk kommunikasjon

11.1 Innledning

I den politiske plattformen for en regjering utgått av Høyre, Fremskrittspartiet og Venstre (Jeløya-plattformen) heter det i punkt 16 på side 78:

> «Regjeringen vil på selvstendig grunnlag utrede og etablere en form for digitalt forsvar av landets grenser utelukkende for utenlandsetterretningsformål, som både øker vår beskyttelsesevne mot trusler mot rikets sikkerhet og som ivaretar sentrale menneskerettigheter og personvernforpliktelser. Venstre tar forbehold om mulig dissens i regjering når denne saken kommer til behandling.»

Hensikten med dette kapittelet i høringsnotatet er å følge opp denne målsettingen i regjeringserklæringen.

11.2 Bakgrunn

11.2.1 Ekspertgruppen for forsvaret av Norge

Daværende forsvarsminister Ine Eriksen Søreide oppnevnte 15. desember 2014 en ekspertgruppe for forsvaret av Norge. Ekspertgruppen ble bedt om å drøfte Forsvarets forutsetninger for å kunne løse sine mest krevende utfordringer knyttet til sikkerhetspolitisk krise og krig. Gruppen avga 28. april 2015 sin rapport Et felles løft. I rapportens kapittel 8 drøfter ekspertgruppen kritiske funksjoner for forsvarsevnen. En av disse funksjonene er etterretning og overvåkning. På side 75 uttaler ekspertgruppen:

> «Den nyeste utfordringen gjelder trusler i det digitale rom. Trusselen gjenspeiler paradigmeskiftet innenfor kommunikasjon og det enkle faktum at innsamling av etterretning må skje der kommunikasjonen foregår, i dette tilfellet på Internett. Alvorlige digitale angrep mot Norge og norske interesser kommer over den samme digitale landegrensen. Kabler er hovedforbindelsen for elektronisk kommunikasjon mellom Norge og utlandet. For å kunne oppdage, varsle og håndtere utenlandske trusler som terror, spionasje og digitale angrep, trengs det å kunne følge med på relevant internettrafikk som går via kabler. Dette vil kunne utgjøre et slags digitalt grenseforsvar. I motsetning til de fleste land vi gjerne sammenligner oss med, som Sverige og USA, har Etterretningstjenesten ikke mulighet til å følge med på slik trafikk. Virksomheten vil ikke være prinsipielt annerledes enn andre former for utenlandsetterretning, men den vil omfatte store datamengder. Tjenesten trenger betydelige investeringer i den tekniske kapasiteten til å prosessere, behandle og analysere informasjon. Samtidig må et digitalt grenseforsvar kombineres med gode kontrollordninger som ivaretar hensynet til personvernet.»

Ekspertgruppen anbefaler på side 85 i rapporten at etableringen av et digitalt grenseforsvar prioriteres.

11.2.2 Lysne I-utvalgets utredning Digital sårbarhet – sikkert samfunn

Utvalget om digitale sårbarheter (Lysne I-utvalget) ble nedsatt av regjeringen 20. juni 2014 for å kartlegge samfunnets digitale sårbarheter. Utvalget ble bedt om å foreslå konkrete tiltak for å styrke beredskapen og redusere den digitale sårbarheten i samfunnet. Utvalget avga sin rapport «Digital sårbarhet – sikkert samfunn» i november 2015. [211]

Utredningen redegjorde for de nye digitale truslene som samfunnet står overfor, og hvordan disse kan møtes. Utvalget uttrykte forståelse for det etterretningsfaglige behovet for digital grenseovervåking, men mente at slik overvåkning ikke burde innføres uten en forutgående offentlig debatt. Utvalget foreslo derfor at det skulle settes ned et eget utvalg for å utrede spørsmålet i større bredde enn det utvalget hadde hatt anledning til å gjøre.[212] Forslaget ble fulgt opp gjennom oppnevningen av Lysne II-utvalget.

11.2.3 Lysne II-utvalgets rapport om digitalt grenseforsvar

Forsvarsdepartementet oppnevnte 24. februar 2016 et uavhengig ekspertutvalg bestående av professor Olav Lysne (utvalgsleder), pensjonert kontreadmiral Trond Grytting, advokat Eva Jarbekk, avdelingsdirektør Einar Lunde og advokat Christian Reusch (Lysne II-utvalget).

Utvalgsmedlemmene ble oppnevnt med hensyn til deres teknologiske, juridiske og etterretningsfaglige kompetanse. Sekretariatsfunksjonen for utvalget ble ivaretatt av Etterretningstjenesten, og de fleste av utvalgets møter ble av praktiske og sikkerhetsmessige årsaker avholdt i Etterretningstjenestens lokaler. Forsvarsministeren ga utvalget i oppdrag å vurdere sentrale problemstillinger knyttet til å gi Etterretningstjenesten tilgang til elektronisk informasjon som kommuniseres gjennom fiberoptiske kabler inn og ut av Norge, omtalt som digitalt grenseforsvar (DGF). Det sentrale formålet med utredningen var å vurdere det faktiske behovet, det rettslige rammeverket, de teknologiske mulighetene

[211] NOU 2015: 13 *Digital sårbarhet – sikkert samfunn*, avgitt 30. november 2015

[212] Ibid. punkt 21.11.8 s. 279

og begrensningene samt de sentrale hensynene for og imot et digitalt grenseforsvar. Det var også et viktig formål at rapporten skulle gi grunnlag for en bred offentlig debatt om temaet.

Utvalget avga sin rapport 26. august 2016. I rapporten anbefaler utvalget å etablere et digitalt grenseforsvar som gir Etterretningstjenesten tilgang til digitale datastrømmer som krysser landegrensen i fiberoptiske kabler. Forutsetningen for anbefalingen var at det etableres et strengt kontrollregime bestående av både teknologiske og menneskelige kontrollmekanismer. Kontrollregimet som foreslått av utvalget består av tekniske filtre for siling av informasjon og domstolens forhåndsgodkjennelse av hvilke søk Etterretningstjenesten kan foreta i informasjonslagrene. Rapporten foreslo videre en uavhengig kontroll utført av et eget tilsyn i tilnærmet sanntid, samt en etterhåndskontroll utført av EOS-utvalget. Utvalget uttalte at et digitalt grenseforsvar utelukkende bør benyttes til utenlandsetterretning, og at informasjon derfra ikke under noen omstendighet bør kunne benyttes som bevis mot tiltalte i straffesaker.

Forsvarsdepartementet sendte 5. oktober 2016 utvalgets rapport på offentlig høring med tre måneders høringsfrist. Departementet mottok nærmere 120 høringssvar. I grove trekk mente høringsinstansene som støtter et digitalt grenseforsvar at et slikt tiltak er nødvendig for at Etterretningstjenesten skal kunne løse samfunnsoppdraget sitt, mens høringsinstansene som var kritiske til forslaget, fremholdt at tiltaket er for inngripende, at det vil ha en nedkjølende effekt på ytringsfriheten, og at det er en fare for formålsglidning. Dertil mente flere at bruken av krypteringsløsninger vil hindre eller begrense effekten av tiltaket. Enkelte instanser mente at forslaget ikke tilfredsstilte rettslige krav som følger av Grunnloven og Den europeiske menneskerettskonvensjon (EMK). Noen problematiserte også hvorvidt forslaget var i tråd med Norges forpliktelser etter EØS-avtalen.

Synspunkter fremmet under høringen vil bli drøftet fortløpende i høringsnotatet her. Utvalgets rapport og høringsuttalelsene ligger offentlig tilgjengelig på regjeringens hjemmesider.

11.2.4 Offentlig debatt i etterkant av høringen

I etterkant av høringen av Lysne II-utvalgets rapport har ulike aktører deltatt i offentlig debatt om forslaget. Utvalgets forslag har vært diskutert i aviser, tidsskrifter, kringkastingsmedier og på Internett. Datatilsynet og Norges nasjonale institusjon for menneskerettigheter arrangerte et debattmøte om forslaget 25. september 2017. Forslaget var tema for Advokatforeningens årstale 23. november 2017 og et debattprogram på NRK 1. februar 2018, og det har også vært diskutert på en rekke offentlige seminarer og konferanser i regi av forskjellige aktører.

Samlet er det departementets inntrykk at det har vært en bred offentlig debatt om Lysne II-utvalgets rapport, noe som også var et av formålene med utredningen. Departementet mener at bred offentlig debatt om temaet bidrar til å belyse viktige hensyn knyttet til hvilke sårbarheter vi som samfunn står overfor og hvordan disse bør håndteres. En åpen debatt bidrar dessuten til større innsikt i en tematikk som normalt skjermes, noe som kan bidra til å motvirke misoppfatninger om karakteren og omfanget av Etterretningstjenestens virksomhet. Dette vil etter departementets syn bidra til å avhjelpe en potensiell nedkjølingseffekt, som er nærmere beskrevet i punkt 11.13.8. Departementet oppfordrer på denne bakgrunn til offentlig debatt også om forslaget som fremgår av dette høringsnotatet.

11.3Terminologi – hva bør denne formen for innhenting kalles?

Det har blitt brukt ulike betegnelser for å beskrive forslaget om å gi Etterretningstjenesten tilgang til kommunikasjon som transporteres i fiberkabler over den norske landegrensen. Både Ekspertgruppen for forsvaret av Norge og Lysne II-utvalget bruker betegnelsen «digitalt grenseforsvar» i sine rapporter. «Digital grensekontroll», «digital grenseovervåking» og «kabelaksess» har også vært brukt. Betegnelsene kan gi ulike assosiasjoner, men kjernen i tiltaket de beskriver har hele tiden vært det samme: Etterretningstjenesten skal på nærmere bestemte vilkår kunne innhente utvalgt kommunikasjon som passerer Norges grenser i fiberoptiske kabler. Innhentingen gjelder altså kommunikasjon som passerer landegrensen – kommunikasjon som er i transitt – og ikke lagrede data. Kommunikasjonsbegrepet innebærer derimot ikke at det må være to eller flere parter som kommuniserer med hverandre. Også ensidig overføring av lyd, tekst, bilder eller andre data omfattes.

Betegnelsen «digitalt grenseforsvar» er treffende i den forstand at tiltaket vil styrke vår evne til forsvar mot angrep fra en motstander som benytter det digitale rom til krigføring. På den andre siden kan forsvarsbegrepet gi en urealistisk forventning til den umiddelbare virkningen tiltaket kan ha mot et angrep – tiltaket kan ikke sammenlignes med et kinetisk våpensystem, som for eksempel en fregatt, et kampfly eller en stridsvogn. Betegnelsen er heller ikke spesielt beskrivende for hva tiltaket nærmere bestemt går ut på. Departementet mener derfor at det bør velges en annen betegnelse, selv om «digitalt grenseforsvar» og forkortelsen «DGF» nå langt på vei er innarbeidet. De samme innvendingene kan gjøres gjeldende mot betegnelsene «digital grenseovervåking» og «digital grensekontroll».

Betegnelsen «kabelaksess» eller «kabeltilgang» er mer beskrivende for tiltaket, men i lys av den raske teknologiske utviklingen bør reguleringen av Etterretningstjenestens metoder og tilganger så langt som mulig gjøres teknologinøytral. Dessuten gir betegnelsene assosiasjoner til at Etterretningstjenesten skal ha tilgang til selve kablene, i stedet for at det er tjenesteleverandører som bidrar til å gi tjenesten tilgang til relevante kommunikasjonsstrømmer. Det er for øvrig ikke i dag tegn på at ny teknologi vil erstatte fiberkablene i overskuelig fremtid, men det kan ikke helt utelukkes. Departementet mener derfor at det bør brukes en teknologinøytral betegnelse, og ikke en som spesifikt knyttes til kabelnettet. Betegnelsen «bulkaksess» eller «bulktilgang» er teknologinøytral, men får ikke frem hva som skiller denne formen for innhenting fra andre former for innhenting i bulk, nemlig at de kommersielle tilbyderne må tilrettelegge for den. Departementet mener at dette særtrekket bør fremgå av betegnelsen. Betegnelsen bør også få frem at tilgangen gjelder kommunikasjon som passerer den norske landegrensen, altså at den er grenseoverskridende. Departementet foreslår på denne bakgrunn betegnelsen «tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon». I høringsnotatet vil en av språklige grunner også benytte kortformen «tilrettelagt innhenting».

11.4 Rettstilstanden i andre land

11.4.1 Innledning

I takt med den teknologiske utviklingen de siste tiårene har det blitt stadig mer vanlig at statenes etterretningstjenester i større eller mindre grad får aksess til grenseoverskridende elektronisk kommunikasjon. På grunn av statenes skjermingsbehov på etterretningsfeltet

kan det ikke gis en uttømmende liste over hvilke land som har slik aksess. Imidlertid er det enkelte stater som har valgt å regulere slik innhenting i åpent tilgjengelige regelverk. Dette gjelder blant annet en rekke sammenlignbare land. Departementet har foretatt et utvalg av de landene det gjelder for å gi en oversikt over hvordan statene organiserer innhentingen, mekanismene som fører kontroll med slik innhenting og, i de tilfellene dette er åpent regulert, innretningen av teletilbyderes tilretteleggingsplikt.

Departementet finner grunn til å understreke at fremstillingen under er basert på åpne kilder. Det er sannsynlig at instrukser og retningslinjer som er underordnet lovgivningen vil være graderte. Departementet tar således forbehold om at det kan forekomme feil i fremstillingen som følge av at nyanser og praksis basert på lovtolkninger ikke synliggjøres i kildene som er åpent tilgjengelig.

11.4.2 Sverige

11.4.2.1 Generelt

I Sverige har Försvarets radioanstalt (FRA) som oppgave å innhente elektronisk kommunikasjon som går i kabelnettet. Innhentingen skjer innenfor rammen av formålsangivelsen i FRA-loven og på bakgrunn av oppdrag fra svenske myndigheter.

Innhentingen skjer etter filtrering basert på nærmere angitte søkebegrep. Søkebegrepene skal utformes og anvendes på en måte som medfører minst mulig inngrep i den personlige integriteten. Dette innebærer blant annet at opplysninger som knyttes til en konkret person ikke kan brukes som søkebegrep med mindre det er av betydelig viktighet for etterretningen.

FRAs virksomhet er underlagt en rekke begrensninger. Et sentralt eksempel er at FRA ikke kan innhente kommunikasjon dersom både avsender og mottaker befinner seg i Sverige, med mindre både avsender og mottaker befinner seg på utenlandske statsfartøy, statsluftfartøy eller militære kjøretøy. En annen begrensning er at FRA bare kan behandle personopplysninger dersom disse er nødvendige for utførelsen av lovpålagte oppgaver, personen opplysningene gjelder har tilknytning til et spesifikt oppdrag og opplysningene om vedkommende må være nødvendig for å fullføre dette oppdraget.

11.4.2.2 Kontrollmekanismer

FRAs virksomhet er underlagt både forutgående og etterfølgende kontrollmekanismer. Kontrollregimet består for det første av forutgående domstolskontroll, som det redegjøres nærmere for i punkt 11.11.3. Videre utfører de øvrige kontrollorganene kontroll med ulike aspekter av etterretningsvirkomheten. Statens inspektion för försvarsunderrättelseverksamheten (SIUN) utfører kontroll av lovmessigheten av FRAs virksomhet, med særlig fokus på FRAs anvendelse av søkebegreper og hvordan plikter knyttet til rapportering og sletting av informasjon overholdes. I tillegg utøves forvaltningskontroll av Datainspektionen, som ser til at FRA behandler personopplysninger i samsvar med lag (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet. Den svenske Riksdagen fører parlamentarisk kontroll av FRA gjennom Signalspaningskommitén.

11.4.2.3 Særlig om tilretteleggingsplikten etter svensk rett

I Sverige er operatører av kabler som frakter signaler over Sveriges grense pålagt å tilrettelegge for FRAs innhenting av grenseoverskridende elektronisk kommunikasjon. Tilretteleggingsplikten følger av lag (2003:389) om elektronisk kommunikation 19 a §, og innebærer at berørte operatører må overføre signalene til innmeldte «samverkanspunkter».

Tilretteleggingsplikten skal utføres slik at beslutning om signalspaning kan iverksettes uten å bli avslørt. Post- og telestyrelsen, som er underlagt Näringsdepartementet, utfører tilsyn med at operatørene overholder sine forpliktelser.

11.4.3 Danmark

11.4.3.1 Generelt

I Danmark har Forsvarets Efterretningstjeneste (FE) som oppgave å innhente utenlandsetterretning. Lovgivningen om etterretningstjenestens innhentingsmetoder er teknologinøytral, og gjelder tilsvarende uavhengig hvordan opplysningene har blitt fremskaffet. FE kan benytte alle lovlige metoder for innhenting av informasjon som er nødvendig for å utføre sine oppgaver, herunder signaletterretning og innsamling i bulk.

11.4.3.2 Kontrollmekanismer

I Danmark er det forutgående domstolskontroll ved innhenting som medfører et inngrep i kommunikasjonsvernet til en person som er hjemmehørende i Danmark men som oppholder seg i utlandet. Innhenting av slike opplysninger tillates bare dersom det foreligger konkrete holdepunkter for at vedkommende deltar i aktiviteter som kan innebære eller forøke en terrortrussel mot Danmark og danske interesser. Rettighetene til den som innhentingen retter seg mot ivaretas av en advokat som har rett til å være til stede og til å uttale seg på rettsmøter, samt å gjøre seg bekjent med det materialet som FE har fremskaffet.

Tilsynet med Efterretningstjenesterne (TET) er et særlig uavhengig kontrollorgan som fører legalitetskontroll med FEs behandling av opplysninger om danske borgere og fysiske og juridiske personer som er bosatt eller har tilhold i Danmark. TET har også som oppgave å behandle klager fra enkeltpersoner som frykter at FE uberettiget behandler opplysninger om vedkommende. Tilsynet har tilgang på all informasjon som er nødvendig for utøvelsen av kontrolloppgavene. Tilsynet kan pålegge FE å slette opplysninger i enkelte saker, men har ikke instruksjonsmyndighet for øvrig. TET gir rådgivende uttalelse til FE dersom det mener at tjenesten bryter loven. Dersom FE velger å ikke følge TETs henstilling skal FE rapportere dette til TET og forsvarsministeren til avgjørelse. Tilsynet rapporterer årlig til forsvarsministeren om utøvelsen av tilsynet med FEs virksomhet.

I Danmark fører «Udvalget vedrørende Efterretningstjenesternes arbejde» parlamentarisk kontroll av FEs virksomhet. Regjeringen skal orientere utvalget før det utstedes retningslinjer om FE og om vesentlige omstendigheter av sikkerhetsmessig karakter eller utenrikspolitiske spørsmål av betydning for FEs virksomhet.

For øvrig kan Folketingets ombudsmand håndtere klager vedrørende FEs etterretningsvirksomhet. Det same gjelder den danske forsvarsministeren.

11.4.4 Finland

11.4.4.1 Generelt

Den finske militære etterretningstjenesten, Försvarsmaktens underrättelsetjänst, har ikke i skrivende stund tilgang på grenseoverskridende elektronisk kommunikasjon. Det samme gjelder skyddspolisen, som utøver sivil etterretningsvirksomhet. Den finske regjeringen overleverte i januar 2018 lovforslag om henholdsvis den militære og den sivile etterretningstjenestens virksomhet til riksdagen. Lovforslaget om den militære etterretningstjenesten inneholder bestemmelser som avgrenser formålet for innhenting av

elektronisk kommunikasjon, hvem innhenting kan rettes mot, prinsippene som bør gjelde og styring og kontroll med etterretningstjenestens virksomhet. Videre er det fremmet forslag om en egen lov om innhenting av datatrafikk for sivile etterretningsformål, som inneholder materielle, prosessuelle og personelle bestemmelser for innhenting. Her foreslås også et forbud mot innhenting av kommunikasjon hvor både avsender og mottaker befinner seg i Finland. Den tekniske gjennomføringen av innhenting av datatrafikk for både sivile og militære formål følger av lovforslaget om militær etterretningsvirksomhet. Det er Försvarets underrättelsetjänst som utfører selve innhentingen, også på vegne av sikkerhetspolitiet.

11.4.4.2 Kontrollmekanismer

I det finske lovforslaget foreslås forutgående domstolskontroll på nærmere bestemte vilkår, se om dette i høringsnotatet punkt 11.11.3. Den finske regjeringen har videre lagt frem lovforslag om kontroll av tjenestens innhenting i förslag till lag om övervakning av underrättelseverksamheten. I loven foreslås innretningen av henholdsvis legalitets- og parlamentarisk kontroll. I likhet med den svenske ordningen foreslås at det opprettes et eget utvalg i riksdagen – riksdagens underrättelsetillsynsutskott – med omfattende rett til informasjon og redegjørelser. Videre foreslås at det opprettes en ny, uavhengig myndighet underlagt dataombudsmannens byrå som skal forestå legalitetskontrollen. Underrättelseombudsmannen foreslås å ha som oppgave å overvåke lovligheten av etterretningstjenestens metodebruk og hvordan tjenesten overholder menneskerettighetene og andre grunnleggende rettigheter, samt å gi årlige redegjørelser til riksdagen, riksdagens justitieombudsmann og statsrådet. Ombudsmannen foreskrives myndighet til å beslutte stans av innhenting og sletting av innhentede opplysninger. Videre foreslås ombudsmannen som klageinstans. Ombudsmannen skal samarbeide med og redegjøre for sine observasjoner til riksdagens underrättelsetillsynsutskott.

11.4.4.3 Særlig om tilretteleggingsplikten etter lovforslagene

Alle som eier eller innehar hele eller deler av et grenseoverskridene kommunikasjonsnett plikter å tilrettelegge for innhenting av datatrafikk. Plikten omfatter at den som faller inn under betegnelsen dataöverförare skal gi informasjon til Försvarets underrättelsetjänst om relevante aksesspunkt, samt gi tjenesten tilgang slik at innhentingen kan gjennomføres. Videre plikter dataoverføreren å gi både de sivile og militære etterretningstjenestene informasjon om tekniske data som er nødvendig for å vurdere om et kommunikasjonsnett er relevant for etterretningsformål.

11.4.5 Frankrike

11.4.5.1 Generelt

I Frankrike har Direction Générale de la Sécurité Extérieure (DSGE) som oppgave å innhente utenlandsetterretning. DGSE har hatt aksess til grenseoverskridende elektronisk kommunikasjon i hvert fall siden 2008. DSGE kan innhente kommunikasjon i bulk og dele denne med de øvrige etterretningstjenestene.

11.4.5.2 Kontrollmekanismer

Det er ingen forutgående domstolskontroll av DGSEs innhenting, men innsamling av kabelbåren kommunikasjon krever statsministerens godkjennelse. Statsministeren skal forut for sin beslutning som hovedregel få rådgivende uttalelse fra Commission nationale de contrôle des techniques de renseignement (CNCTR), som er et uavhengig forvaltningsorgan. Statsministeren kan fatte beslutning uten CNCTRs uttalelse dersom det

foreligger en nødssituasjon og innhentingen har som formål å fremme nasjonens uavhengighet, territoriets integritet eller det nasjonale forsvar, eller forebygge terror eller andre anslag med tilstrekkelig grad av alvorlighet. Dersom statsministeren treffer beslutning i en hastesak skal CNCTR få umiddelbar beskjed om dette. CNCTR rapporterer til Conceil d'État, som er Frankrikes øverste domstol i administrative tvistespørsmål.

11.4.5.3 Særlig om tilretteleggingsplikten etter fransk rett

Etter loven av 2015 plikter ekomtilbyderne å samarbeide med DGSE. Loven gir DGSE mulighet til å pålegge ekomtilbydere å gjennomføre nødvendige endringer i nettverket, herunder automatisering av databehandlingen, for å gi mulighet for bl.a. sanntids innsamling for å forebygge terrorisme.

11.4.6 Storbritannia

11.4.6.1 Generelt

I Storbritannia har UK Government Communications Headquarters som oppgave å innhente elektronisk kommunikasjon. Innhenting av kommunikasjon er særskilt og utførlig regulert i Investigatory Powers Act (IPA) fra 2016 og en rekke underordnede reguleringer fra 2018. IPA er omfattende og består av over 270 bestemmelser. I korte trekk inneholder loven materielle, prosessuelle og personelle vilkår for innhenting og behandling av informasjon, med særlige regler for lagring av kommunikasjonsdata og innhenting av informasjon i bulk. Videre inneholder IPA en rekke regler som har til formål å forhindre misbruk og sikre hensynet til privatlivet, herunder bestemmelser om tilsyn og kontroll av virksomheten, samt bestemmelser om hvilke overtredelser som gir grunnlag for straffereaksjon.

11.4.6.2 Kontrollmekanismer

I Storbritannia prøves ikke GCHQs innhenting av en domstol, men begjæringer om å foreta innhenting må godkjennes av en judicial commissioner før utenriksministeren gir endelig tillatelse. Det føres også etterfølgende juridisk kontroll med ministerens avgjørelser.

Videre føres parlamentarisk kontroll av the Intelligence and Security Committee of Parliament, som undersøker de britiske etterretningstjenestenes policy, administrasjon og pengebruk. Komiteen publiserer årlige rapporter og utreder spesifikke tema knyttet til etterretningsvirksomhet.

The Investigatory Powers Commissioner foretar legalitetskontroll av myndighetenes inngripende metodebruk og har blant annet som oppgave å vurdere anmodninger og foreta inspeksjoner hos tjenestene.

The Investigatory Powers Tribunal (IPT) undersøker anklager om ulovlig metodebruk som kan ha krenket noens privatliv. Tribunalet kan også undersøke anklager om brudd på en rekke andre menneskerettigheter. Tribunalet oppfyller således den menneskerettslige forpliktelsen som påligger statene etter EMK om å ha effektive rettsmidler tilgjengelig for privatpersoner hvis rettigheter kan ha blitt krenket.

For innhenting av opplysninger som kan knyttes til medlemmer av parlamentet eller som nyter særlig rettslig vern gjelder ytterligere rettssikkerhetsgarantier. For eksempel må innhenting rettet mot et parlamentsmedlem besluttes av statsministeren. For privilegert kommunikasjon gjelder en særlig høy terskel for innhenting.

11.4.6.3 Særlig om tilretteleggingsplikten etter britisk rett

Teletilbydere i Storbritannia er pålagt å tilrettelegge for innhenting av elektronisk kommunikasjon i tråd med utenriksministerens instruksjoner. Utenriksministerens myndighet og rekkevidden av tilbydernes plikter fremkommer detaljert i IPA kapittel 1 additional powers del 9.

11.5 Åpenhet og skjerming

Etterretningstjenestens innhenting av informasjon vil ofte foregå fordekt. Fordekt innhenting gir Etterretningstjenesten særlige forutsetninger for å produsere gode etterretningsvurderinger til støtte for Norges nasjonale sikkerhet. Samtidig forutsetter dette at metoder, kapasiteter og kilder skjermes.

Departementet bestreber seg i dette høringsnotatet på å beskrive så åpent som mulig hvilke metoder og tilganger Etterretningstjenesten bør kunne benytte seg av. Denne åpenheten kan sies å være resultatet av en tendens de senere år i retning av større grad av innsyn i et område som tradisjonelt, både nasjonalt og internasjonalt, har vært gjenstand for mye hemmelighold. Samtidig går det en grense for hva som kan beskrives åpent. Full åpenhet ville undergrave tjenestens virksomhet, med de alvorlige konsekvenser det ville få for norsk sikkerhet. Manglende innsyn og transparens må for etterretningsvirksomhet derfor avbøtes med andre kontrolltiltak på fellesskapets vegne. Dette er nærmere behandlet under punkt 11.10 til 11.13 under. Det kan hevdes at spørsmålet om tillit og kontroll kommer særlig på spissen når det gjelder spørsmål om søk i kommunikasjon som transporteres i fiberkabler over den norske landegrensen, fordi dette tiltaket angår kommunikasjonen til potensielt svært mange mennesker. Dette er en av årsakene til at spørsmålet om søk i slik kommunikasjon behandles særskilt både i høringsnotatet og i lovutkastet, og at de tilhørende kontrolltiltakene som foreslås er meget strenge.

Departementet har merket seg at flere instanser i høringen av Lysne II-rapporten mener at effekten av et digitalt grenseforsvar, særlig på grunn av kryptering, vil være liten, og at man heller bør gå inn for mer spissede og mindre inngripende innhentingsmetoder. Departementet har vurdert nøye hvilke alternative metoder som kan løse det overhengende problemet, som er Etterretningstjenestens manglende tilgang til internettbasert kommunikasjon. Null-alternativet er også vurdert. En gjennomgående utfordring i drøftelsene er at man ikke kan utvise full åpenhet om hvilke muligheter Etterretningstjenesten har til å nyttiggjøre seg av den informasjonen som hentes inn, blant annet fordi dette vil gi trusselaktører mulighet til å endre sin atferd for å unngå innhentingen. En for stor grad av åpenhet rundt tiltakene vil derfor kunne gjøre tiltaket mindre treffsikkert og effektivt.

Som det vil fremgå av drøftelsene i det følgende, mener departementet at innhenting av kommunikasjon som transporteres i fiberoptiske kabler vil være et effektivt og strengt nødvendig virkemiddel for Etterretningstjenesten.

Departementet vil fremheve at kryptering av norsk data er viktig både for personvernet og samfunnet, og at høringsforslaget ikke på noen måte vil svekke sikkerheten som kryptering gir. Høringsnotatet vil ikke beskrive nærmere hvordan Etterretningstjenesten håndterer kryptert informasjon, men nøyer seg med å konstatere at problemstillingen ikke er ukjent for tjenesten. Det er dessuten slik at metadata, som er helt avgjørende for tjenestens oppgaveløsning, ikke i like stor grad krypteres og til dels heller ikke kan krypteres.

11.6 Behovet for tilgang til grenseoverskridende elektronisk kommunikasjon

11.6.1 Innledning

Den teknologiske utviklingen har ført til et paradigmeskift med tanke på hvordan vi kommuniserer. Utviklingen har også ført til forenkling av norske borgeres hverdag, mer innovasjon, produktivitet, økonomisk vekst og sosial utvikling. Norge har etter hvert blitt et av verdens mest digitaliserte land, og regjeringen har høye ambisjoner og en uttalt målsetting om å digitalisere flere av de offentlige tjenestene.[213] Det digitale rom integreres i stadig større grad i både hverdagsliv og virke.

Som et utgangspunkt mener departementet at det er både naturlig og nødvendig at Etterretningstjenesten, slik som øvrige myndighetsorganer, tilpasser og moderniserer sin virksomhet i takt med den teknologiske utviklingen. Det er godt kjent at i tillegg til alle gevinstene ved teknologiutviklingen, bringer denne også med seg sårbarheter og utfordringer som kan få store konsekvenser for rikets sikkerhet og borgernes trygghet. Modernisering av Etterretningstjenestens kapasiteter og aksesser er dermed en forutsetning for at den skal kunne innhente informasjon *der denne befinner seg* og produsere gode etterretningsanalyser til støtte for Norges nasjonale sikkerhet.

I det følgende skal departementet redegjøre for Etterretningstjenestens behov for grenseoverskridende elektronisk kommunikasjon, herunder trusselbildet som manifesterer seg i og ved bruk av det digitale rom, og hvordan tilgang på elektronisk kommunikasjon kan bidra til håndteringen av dette.

11.6.2 Trusselbildet i det digitale rom

Trusselbildet i det digitale rom er generelt behandlet i punkt 7.5.2.5. Her skal kun trekkes frem enkelte hovedmomenter som er spesielt relevante og som underbygger behovet for tilrettelagt innhenting.

De teknologiske fremskrittene vi opplever i dag, er en sterk driver for samfunnsutvikling nasjonalt og internasjonalt og for den økende globaliseringen som vever verdens land tettere sammen. Den teknologiske utviklingen er imidlertid ikke utelukkende positiv. Digitaliseringen nasjonalt og globalt skaper nye sårbarheter og utfordringer som kan få alvorlige konsekvenser som norske myndigheter må være i stand til å håndtere. For det første gjennomfører både statlige og private aktører sikkerhetstruende handlinger i det digitale rom i form av angrep, sabotasje, påvirkningsoperasjoner og spionasje. Aktørene utvikler stadig nye, sofistikerte metoder for slike nettverksoperasjoner.[214] For det andre bruker trusselaktører de digitale kommunikasjonsplattformene til å planlegge og koordinere blant annet terrorhandlinger. For det tredje kommuniserer de fleste etterretningsmål over nettbaserte tjenester, slik at tilgang til elektronisk kommunikasjon blir nødvendig for produksjon av etterretning generelt.

[213] Meld. St. 27 (2015–2016) Digital agenda for Norge

[214] Etterretningstjenesten og PST har begge understreket fiendtlige aktørers bruk av det digitale rom i sine åpne trusselvurderinger fra 2018.

Norske myndigheter må være rustet med nødvendige og effektive verktøy for å håndtere utfordringene på en god måte. I første instans er det nødvendig å ha *kunnskap* som er egnet til å gi god *forståelse* av en trussel eller et annet forhold med opprinnelse i utlandet. Det er Etterretningstjenesten som har ansvaret for å skaffe slik kunnskap, noe som gjenspeiles i mottoet *Viten om verden for vern av Norge.* Kunnskap om *hva* sikkerhetstruende handlinger eller hendelser innebærer, *omfanget* av dem og *hvem* som står bak er essensielt for at norske beslutningstakere skal kunne gjøre presise og gode vurderinger som verner rikets sikkerhet. Det samme gjelder den generelle forståelsen av situasjoner i prioriterte områder i utlandet, hvor tjenestens daglige oppdrag er å kartlegge normalsituasjonen for å være i stand til å oppdage eventuelle avvik som kan ha betydning for norske interesser.

Etterretningstjenesten skal etterstrebe å avdekke sikkerhetstruende forhold før disse manifesterer seg i virkeligheten. Et viktig poeng er derfor at kunnskapen erverves rettidig. Tjenesten og myndighetene for øvrig kan ha et svært begrenset tidsvindu fra et relevant forhold oppdages til riktige myndighet eller samfunnsaktør må agere for å motvirke eller håndtere en trussel, for eksempel der noen planlegger eller har iverksatt et terrorangrep eller en nettverksoperasjon rettet mot Norge. Dersom Etterretningstjenesten er avhengig av å spørre om informasjon fra andre fordi den mangler egen tilgang til relevante informasjonskilder, kan ventetiden være skjebnesvanger. Det er heller ikke gitt, og i mange tilfeller svært lite sannsynlig, at andre besitter den nødvendige informasjonen. Departementet vurderer det som svært viktig at tjenesten har tilgang til relevant informasjon uten unødig opphold. Behovet for rettidig informasjon henger også sammen med informasjonens relevans, ettersom utdatert informasjon har liten eller ingen etterretningsmessig verdi.

Betydningen av Norges evne til å drive selvstendig etterretning må ikke underkjennes. All den tid Etterretningstjenesten ikke har adekvat tilgang på elektronisk kommunikasjon, vil tjenesten være avhengig av å fylle informasjonsgapet gjennom å motta informasjon fra samarbeidende tjenester og allierte. Disse vil ikke ha norske interesser som topprioritet. Ved manglende egen aksess vil Etterretningstjenesten dessuten mangle anledning til å kvalitetssikre og verifisere opplysningene den mottar, og er dermed sårbar for at informasjonen har dårlig kvalitet, er ufullstendig, forfalsket eller på annen måte villedende. Majoriteten av de land som Etterretningstjenesten samarbeider med, har ordninger som gir deres etterretningstjenester tilgang på elektronisk kommunikasjon. Med andre ord kan det informasjonsgrunnlaget som Etterretningstjenesten bygger analysene sine på, stamme fra lignende ordninger som den som foreslås her, men uten noen garanti for at opplysningene ble innhentet på en måte som ville ha vært i samsvar med norsk lov. Dette taler for at Etterretningstjenesten gis egen, adekvat tilgang.

11.6.3 Departementets vurdering

Departementet vurderer at tilgang på grenseoverskridende elektronisk kommunikasjon vil gi Etterretningstjenesten anledning til å selvstendig og formålsrettet innhente kritisk informasjon fra en helt sentral informasjonskilde som tjenesten i dag ikke har tilgang til. Departementet vurderer det som alvorlig at norske myndigheter i dag ikke er rustet til å avdekke og avverge de mest avanserte truslene mot Norge i det digitale rom. Det gjelder særlig statlig spionasje, forberedelser til cyberangrep og grenseoverskridende terrorplanlegging. Departementet vurderer også at tilgang på grenseoverskridende elektronisk kommunikasjon i årene fremover vil gi nødvendig informasjon innen andre

prioriterte områder, herunder cyberterrorisme i form av cyberangrep som utføres av terrororganisasjoner og lignende ikke-statlige aktører.

11.7 Alternative løsninger

11.7.1 Innledning

11.7.1.1 Bakgrunn

Som redegjort for over transporteres kommunikasjon på en annen måte enn før. I tillegg er trusselbildet i det digitale rom av en helt annen karakter enn det vi forbinder med tidligere kommunikasjonsformer. Utviklingen stiller Norge overfor en todelt utfordring: For det første har vi mistet en viktig kilde til kommunikasjonsetterretning, og for det andre er vi dårlig rustet til å oppdage og avverge trusler og fiendtlig aktivitet i det digitale rommet.

Lysne II-utvalget utredet og anbefalte et konsept som vil kunne avhjelpe begge disse utfordringene. Spørsmålet i det følgende er om det finnes alternative løsninger som både er egnet til å møte utfordringene, og som samtidig er mindre personverninngripende enn Lysne II-utvalgets modell.

11.7.1.2 Hva er alternativene?

Enkelte har kritisert at Lysne II-utvalget fikk som mandat å utrede et digitalt grenseforsvar, snarere enn å få i oppgave å skissere og analysere hvilke alternative løsninger som kunne besvare sårbarheten og behovet som er beskrevet over. Departementet deler synspunktet om at det er nødvendig å vurdere alternative løsninger til Lysne II-utvalgets konsept. Departementet finner at det i denne sammenheng har lite for seg å utrede en modell som i større grad enn Lysne II-utvalget fokuserer på etterretningsfaglige hensyn, og som dermed vil kunne medføre et større personverninngrep. Samtidig er det grunn til å understreke at dersom etterretningsfaglige hensyn alene skulle være førende, ville tilgangen til kabelbasert informasjon vært innrettet ganske annerledes enn etter Lysne II-utvalgets modell. En slik løsning ville tillatt mer lagring av innholdsdata, lengre lagringstid og hatt færre rettssikkerhetsgarantier og kontrollordninger.

Basert på at forutsetningen er å vurdere mindre personverninngripende alternativer, er det to måter man kan begrense innsamling av data. Man kan begrense *hvilke* data man tillater at plukkes ut, behandles og lagres. Alternativt kan man begrense dekningen (hvilke kommunikasjonsstrømmer man kan innhente fra) – altså den generelle *tilgangen* til data. Som beskrevet i punkt 8.3.2 og 9.5.6 kan elektronisk informasjon ikke analyseres mens den er i transitt. For at tilgang til informasjonen skal kunne ha etterretningsmessig verdi må den dermed samles inn og lagres før den kan analyseres. Dette gjør at det er begrenset hvor mange alternative løsninger som finnes.

Departementet vurderer i det følgende både muligheten for å innsnevre hvilke data som kan innsamles fra kommunikasjonsstrømmene («lettversjonen»), og muligheten for å begrense tilgangen til å samle inn data («sensorer hos utvalgte virksomheter»). Alternativet om ikke å gi tilgang til kabelbåren kommunikasjon, det såkalte «nullalternativet» vurderes også. Først redegjør departementet for en del premisser som ligger til grunn for vurderingen av de ulike løsningsalternativene.

11.7.1.3 Premisser for utredningen av alternativer

Lysne II-utvalget oppstilte fire absolutte kriterier som premisser for sin modell. For det første måtte løsningen gi nødvendig etterretningsmessig verdi. Dernest måtte systemet implementeres på en måte som både var juridisk gangbar og teknologisk gjennomførbar. Dessuten måtte systemet ikke svekke befolkningens tillit til de hemmelige tjenestene. Departementet mener at dette på en god måte illustrerer hvilke hensyn som må tas i valg av modell. I tillegg kommer en vurdering av kostnadene. En kostnadskrevende modell som gir lav eller ingen etterretningsmessig verdi kan ikke anbefales.

I vurderingen av alternativer har departementet lagt stor vekt på at løsningen må gi tilstrekkelig *etterretningsmessig verdi*. Med «etterretningsmessig verdi» menes at alternativet må være egnet til å oppfylle lovens formål gjennom å besørge Etterretningstjenesten med informasjon som er nødvendig for utførelsen av oppdrag innenfor rammen av kapittel 3 i lovforslaget her. Etterretningsmessig verdi vil i denne sammenhengen være synonymt med nytteverdien.

Faren for at etterretningsmål kan *omgå* systemet har også vært viktig for departementets vurdering. Etterretningsmål bør i minst mulig grad kunne omgå de kommunikasjonsbærerne som Etterretningstjenesten har tilgang til. Dette er viktig fordi omgåelse kan føre til at andelen etterretningsrelevant informasjon blir lav sammenlignet med overskuddsinformasjonen som samles inn og lagres. Fare for omfattende omgåelse vil dermed forringe den etterretningsmessige verdien av et alternativ, noe som kan ha stor betydning for vurderingen av om løsningen anses nødvendig og forholdsmessig.

Kontrollmekanismer og innretningen av disse er en annen faktor som potensielt kan begrense den etterretningsmessige verdien. Det er imidlertid utelukket å foreslå en løsning som ikke tar innover seg faren for myndighetsoverskridelser og misbruk av tilgangen på grenseoverskridende elektronisk kommunikasjon. Departementet har derfor sett det som helt sentralt at løsningen må innrammes av robuste, reelle og troverdige kontrolltiltak.

Det avgjørende for departementet har vært hvilket alternativ som etter en *helhetsvurdering* gir størst etterretningsmessig verdi samtidig som det ivaretar personvernhensyn og andre grunnleggende verdier i vår demokratiske rettsstat. Det har vært en grunnleggende forutsetning for departementet at løsningen skal være i overensstemmelse med Norges menneskerettslige forpliktelser og andre overordnede rettslige rammer. Lovgivningen må herunder møte de menneskerettslige krav til klare og presise hjemler, se nærmere punkt 4.2.5.2.

En vurdering av etterretningsmessig verdi må ta inn over seg hvilken *bruksnytte* modellen gir. En løsning kan legge så mange begrensninger på innsamling og bruk av informasjon at systemet til slutt ikke lenger er et egnet verktøy. For eksempel vil en ordning som ikke vil kunne nyttiggjøres til målsøking og retrospektiv analyse, gi lav etterretningsverdi.

Spørsmålet om mengden lagret informasjon henger nært sammen med spørsmålet om hvordan *utvalg* av kommunikasjonsbærere og *filtrering* av informasjon bør reguleres. Departementet ser det av personvernhensyn som sentralt at mest mulig overskuddsinformasjon filtreres vekk. Utvalg av kommunikasjonsbærere og automatisk filtrering av datatrafikken bør imidlertid ikke skje på en måte som sterkt reduserer den etterretningsmessige verdien av tiltaket, og således underminerer formålet med det.

Sterk *kryptering* har blitt stadig mer tilgjengelig og tatt i bruk, først og fremst for å verne innholdet i kommunikasjonen. Metadata krypteres ikke i samme grad. *Datatilsynet* peker i sitt høringssvar til Lysne II-utvalget på at:

> «løsninger for både innholdskryptering og metadatakryptering er lett tilgjengelig og også vanlig i bruk. Dette betyr at DGF i hovedsak vil ramme den vanlige mann og kvinne som ikke gjør spesielle tiltak for å beskytte sin kommunikasjon – bevisste og kompetente trusselaktører kan i stor grad unngå å bli fanget opp av DGF».

Utfordringene som relaterer seg til kryptering må være overkommelige for Etterretningstjenesten for at en løsning skal ha etterretningsmessig verdi. Blant annet av hensyn til å unngå at etterretningsmål innretter seg kan det ikke gås nærmere inn på hvordan krypteringsutfordringer løses, men departementet vil understreke at dersom slike utfordringer medfører at en ordning har lav etterretningsverdi, vil ikke denne bli foreslått.

I det følgende redegjøres for de alternativene departementet har vurdert som mulige løsninger på sårbarhetene som Norge står overfor, derunder Lysne II-utvalgets modell.

11.7.2 Tilrettelagt innhenting utelukkende av innholdsdata og metadata knyttet til kjente mål – «lettversjon»

11.7.2.1 Nærmere om hva alternativet går ut på

I etterkant av publiseringen av Lysne II-utvalgets rapport har det vært reist spørsmål om det er mulig å utforme en mer spisset og mindre inngripende variant av utvalgets forslag, det som kan kalles en «lettversjon». En slik løsning vil vurderes i det følgende.

En «lettversjon» baserer seg på et premiss om mindre omfattende lagring av overskuddsinformasjon. Det er to kategorier informasjon som kan samles inn fra elektronisk kommunikasjon – innholdsdata og metadata. Lysne II-utvalget foreslo at Etterretningstjenesten først skal kunne få tilgang til *innholdsdata* knyttet til en selektor *etter* at en domstol har godkjent det, og bare *fremover* i tid. Utvalgets forslag er derfor etter departementets syn allerede behørig spisset når det gjelder innhentingen av innholdsdata.

Spørsmålet er dermed om innsamlingen av *metadata* kan snevres inn. Lysne II-utvalget beskriver seleksjon og filtrering av metadata i rapporten på side 50 og 53–54. Som det fremheves der er det tekniske og maskinelle forhold som setter begrensninger for hvilken informasjon man evner å filtrere vekk, og departementet kan dermed ikke se at det er mulig å gjøre metadatalagringen mer spisset enn foreslått av utvalget. En «lettversjon» vil derfor måtte bero på en løsning der man utelukkende lagrer data basert på en positiv filtrering. Positiv filtrering fungerer slik at man på forhånd spesifiserer hva som skal tillates lagret, knyttet til kjente selektorer. Alle datastrømmer som ikke maskinelt gjenkjennes vil filtreres vekk og blir ikke lagret. Lysne II-utvalget omtaler dette kort på side 50 i sin rapport.

Forslaget til en «lettversjon» åpner ikke for at Etterretningstjenesten skal kunne søke i et datagrunnlag for målsøkingsformål, for å foreta retrospektiv analyse eller for å finne nye identiteter tilknyttet allerede kjente etterretningsmål.

11.7.2.2 Departementets vurdering

Den mest fremtredende fordelen med «lettversjonen» er at det i teorien vil samles inn og lagres vesentlig mindre overskuddsinformasjon. Et system som bare lagrer etterretningsrelevant informasjon vil minke overvåkningstrykket, og potensialet for en eventuelt nedkjølende effekt og faren for myndighetsmisbruk reduseres. Det vil med en slik

løsning fortsatt lagres personopplysninger, noe som utgjør et menneskerettslig inngrep overfor den enkelte. Lagringens omfang vil imidlertid bli langt mindre og dermed ramme færre personer.

For departementet er det imidlertid et avgjørende moment i vurderingen at «lettversjonen» baserer seg på en forutsetning om at Etterretningstjenesten allerede sitter på tilstrekkelig informasjon for å kunne *igangsette* målrettet innhenting, og at man i praksis også klarer å finne og følge det kjente målets kommunikasjon. Med andre ord forutsetter løsningen at tjenesten allerede har de utvelgelseskriterier som ligger til grunn for den positive filtreringen. Denne forutsetningen gjenspeiler ikke virkeligheten. Premisset om at det er mulig å følge ett kjent mål over tid basert på en eller kun få selektorer som inngangsverdi for innhentingen, som er tilegnet fra andre kilder, lar seg ikke realisere i praksis. Det skyldes at etterretningsmål benytter mange ulike identiteter og kommunikasjonsplattformer digitalt. Hvilke identiteter som kan knyttes til et kjent etterretningsmål er derfor ikke en konstant størrelse og vil raskt kunne endre seg. I tillegg kommer at kjente, sikkerhetsbevisste etterretningsmål vil benytte seg av alle tilgjengelige virkemidler for å unndra seg tjenestens søkelys.

For at Etterretningstjenesten skal kunne følge kjente aktører over tid, herunder for å kunne identifisere målets utallige digitale identiteter, vil det være behov for å lagre metadata knyttet til all kommunikasjon som velges ut. Dette er nødvendig for å finne målet, følge målet, identifisere målets nye identiteter og filtrere ut trafikk som ikke skal registreres. Å utelukkende innhente og lagre innholdsdata og metadata spisset mot kjente mål lar seg ikke teknisk gjennomføre uten samtidig å lagre betydelige mengder metadata fra den kommunikasjonsstrømmen som innholdsdata planlegges innhentet fra. Dette skyldes, litt forenklet forklart, at for å kunne gjennomføre *koblingen* mellom en kjent selektor og en kommunikasjon i kommunikasjonsstrømmen må det først gjennomføres maskinell analyse av all metadata i kommunikasjonsstrømmen. Uten slik forutgående maskinell metadataanalyse vil selektoren for alle praktiske formål være ubrukelig.

Uavhengig av utfordringene med å følge kjente mål uten et bredt metadatagrunnlag vurderer departementet at manglende mulighet til å gjøre søk i et metadatalager i betydelig grad forringer verdien av en slik løsning. Det er på det rene at innsamling, lagring og bruk av metadata spiller en viktig rolle for løsningen av Etterretningstjenestens oppgaver. Tilgang på store mengder data er for det første avgjørende for at Etterretningstjenesten skal kunne gjennomføre effektiv målsøking.[215] Et hovedoppdrag for Etterretningstjenesten er nettopp å identifisere hittil ukjente trusler. Målsøking er en iboende del av etterretningsvirksomhet slik den gjennomføres i de fleste land i dag. For det andre er metadata nødvendig for at tjenesten skal kunne foreta retrospektiv analyse der dette er nødvendig. Retrospektiv analyse av metadata brukes for eksempel til å danne et bilde av størrelsen til et terrornettverk eller omfanget av en nettverksoperasjon basert på trafikkanalyse av kommunikasjonsmønster og IP-adresser. Her er et viktig poeng at identifikasjon og

[215] Med *målsøking* menes systematisk arbeid for å identifisere nye etterretningsmål, jf. lovforslaget § 1-4 nr. 9. Motsetningen til målsøking er *målrettet innhenting*, definert som systematisk arbeid for å finne informasjon knyttet til identifiserte etterretningsmål, jf. lovforslaget § 1-4 nr. 8. Målsøking og målrettet innhenting er med andre ord to vidt forskjellige tilnærminger som brukes til å utføre forskjellige sider av etterretningsvirksomheten. Det er et vesentlig poeng i denne sammenheng at den ene tilnærmingen ikke kan erstatte den andre. Uten målsøkingsvirksomheten vil Etterretningstjenesten ikke ha de nødvendige inngangsverdier for å igangsette målrettet innhenting.

kartlegging av trusler ofte fordrer evne til å sammenstille ny og gammel informasjon. Målsøking og retrospektiv analyse henger dermed sammen. Uten evne til å avdekke trusler gjennom trafikkanalyse basert på både målsøking og retrospektiv analyse mener departementet at man gjør seg sårbar for hendelser og angrep som kunne ha vært avverget.

Nytten av metadata og trafikkanalyse kan illustreres med et eksempel fra kampen mot terrorisme. Terroraktører er svært vanskelige å identifisere og følge, da de – for å unngå å bli oppdaget – konstant endrer kommunikasjonsmidler og -tjenester. Én terrorist kan operere med en rekke ulike brukernavn eller identifikatorer på mange ulike nettsteder og meldingstjenester, som brukes til å kommunisere med andre aktører i terrornettverket, som igjen vil ha en mengde ulike identifikatorer på flere forskjellige internettbaserte tjenester. Løpende identifikasjon og kartlegging av etterretningsmål som utgjør en terrortrussel fordrer at Etterretningstjenesten har verktøy som kan benyttes til å sammenstille de ulike identifikatorene som tilhører terroraktørene. Dette skjer gjennom trafikkanalyse, som baserer seg på metadata. Et bredt metadatagrunnlag er derfor avgjørende både for å følge kjente mål og for at tjenesten skal kunne finne tilknytninger mellom kjente mål og nye mål gjennom målutvikling.

Metadata kan avsløre mye informasjon, særlig hvis man sammenstiller ulike metadata og plasserer det i en kontekst av tid og rom. Departementet mener imidlertid at innholdsdata på generelt grunnlag må anses som mer sensitive data enn metadata, ettersom *hva* noen har kommunisert normalt er mer avslørende enn *at* noen har kommunisert. Til illustrasjon legger Lysne II-utvalgets forslag opp til å benytte seg av metadatagrunnlaget som et utgangspunkt for å finne frem til de etterretningsrelevante innholdsdata. Uten et bredt metadatagrunnlag, som i seg selv representerer mindre sensitiv informasjon, vil ikke tjenesten kunne spisse innsamlingen av innholdsdata på samme måte.

Departementet har på bakgrunn av drøftelsene over vurdert den etterretningsmessige verdien av «lettversjonen» som svært lav. Departementet har vurdert hvorvidt det kan benyttes kompenserende tiltak som alternativ til søk i og analyse av et metadatalager. Selv om man i teorien kunne fått tilgang til relevante selektorer fra andre som kunne benyttes som utvalgskriterium for den positive filtreringen, vil man som beskrevet over likevel ikke ha teknisk mulighet til å gjenkjenne og følge disse selektorene uten et metadatagrunnlag. Departementet har vanskelig for å se at en løsning uten tilgang til et større metadatagrunnlag, som kan gi grunnlag for å analysere seg frem til disse identitetene, vil gi den nødvendige etterretningsverdi. Å utelukkende tillate målrettet innhenting og lagring av data kan fremstå ønskelig i et personvernperspektiv, men departementet anser at dette i realiteten ikke er et egnet alternativ for å løse de utfordringer vi står overfor.

Etter en helhetlig vurdering mener departementet at «lettversjonen» vil gi en meget lav etterretningsmessig verdi. Som følge av at alternativet ikke vurderes som egnet finner departementet ikke grunn til å vurdere alternativet opp mot personvernmessige og økonomiske konsekvenser. Departementet mener at løsningen ikke kan anbefales.

Departementets vurdering kan sammenfattes som følger:

EFFEKT	«LETTVERSJONEN»
Kontraterror	Dette er etterretningsmål som det i utgangspunktet er svært vanskelig å følge. Løsningen vil ikke evne å finne og følge kjente mål, da et bredt metadatagrunnlag er nødvendig for å gjenkjenne tekniske parametere knyttet til selektorene og følge målenes konstante endring av kommunikasjonsmidler og tjenester. **Svært lav etterretningsmessig verdi mot terrortrusler.**
Digitale trusler	Løsningen vil gjøre det svært vanskelig eller umulig å oppdage de mest avanserte trusselaktørene. Den vil heller ikke oppdage nye ukjente trusler, avdekke omfanget av fremmed spionasje og sabotasjeforberedelser, avdekke trusler som benytter norsk infrastruktur som transittledd mot mål utenfor Norge, samt muliggjøre attribusjon av nye trusler. Man vil i vesentlig grad være avhengig av tips fra andre land. **Svært lav etterretningsmessig verdi mot digitale trusler.**
Øvrige oppdrag	Alternativet vil ikke kunne gi tilgang til transittrafikk mv. som er egnet til å løse tjenestens øvrige oppdrag, som f.eks. å bidra til ivaretakelse av prioriterte norske utenriks-, forsvars- og sikkerhetspolitiske interesser. På grunn av mangel på metadata vil løsningen ikke kunne gi tilstrekkelige inngangsverdier. **Svært lav etterretningsmessig verdi for tjenestens øvrige oppdrag.**

11.7.3 Sensorer hos utvalgte virksomheter

11.7.3.1 Nærmere om hva alternativet går ut på

Departementet har vurdert om utplassering av sensorer i utvalgte norske virksomheter kan være et alternativ til tilrettelagt innhenting av data i transitt.

I motsetning til «lettversjonen», som vil begrense *hvilken* informasjon som hentes inn og lagres, vil dette alternativet innskrenke *dekningen* og *oppgaverelevansen*, det vil si hvilke kommunikasjonsstrømmer som det kan hentes inn fra, og for hvilke formål informasjonen kan hentes inn. I stedet for å plassere sensorer på sentrale lokasjoner som gir tilgang til utenlandstrafikken, som foreslått av Lysne II-utvalget, vil man her plassere ut sensorer i utvalgte norske offentlige og private virksomheter som man antar vil kunne være relevante for å avdekke trusler mot Norge i form av kjente cybersignaturer. Det vil av naturlige årsaker ikke være aktuelt å plassere ut sensorer i private hjem eller lignende.

Det er i denne sammenheng viktig å skille mellom en sikkerhetssensor og en etterretningssensor. Alternativet gir kun mening dersom det er tale om å utplassere etterretningssensorer. En sikkerhetssensor som for eksempel NorCERT sine VDI sensorer, har til hensikt å øke sikkerheten i et spesifikt nettverk i Norge, mens en etterretningssensor vil ha til hensikt å belyse en utenlandsk trusselaktør, slik at man kan detektere og dermed ha mulighet til å stanse trusselaktivitet før trusselaktøren opererer i det spesifikke nettverket. Fra et etterretningsmessig perspektiv er det ikke bare aktørens sluttmål som det er relevant å observere. En trusselaktør vil ofte kompromittere en hel rekke små og mellomstore

virksomheter for å skjule sine spor og benytte disse som utgangspunkt for videre angrep. Det å kunne observere en aktør i denne fasen før aktiviteten rettes mot kritisk infrastruktur i Norge eller hos våre allierte er meget relevant ut i fra et etterretningsståsted.

Dette alternativet er utvilsomt mindre generisk enn Lysne II-utvalgets forslag, blant annet fordi Etterretningstjenesten må velge ut hvilke virksomheter som antas å være særlig utsatt for digitale trusler, og rette fokus mot disse. Trafikk til og fra private PC-er og mobiltelefoner vil ikke kunne samles inn og lagres.

11.7.3.2 Departementets vurdering

Til sikkerhetsovervåking av nettverk viser erfaring fra VDI-nettverket at utplassering i utvalgte virksomheter kan ha stor verdi for den aktuelle virksomheten, og departementet mener at dette nettverket bør videreutvikles og utplasseres i flere virksomheter enn i dag. Dette er imidlertid ikke overførbart til nasjonal etterretningsverdi. I det følgende omtales derfor ikke sikkerhetssensorer i dette alternativet. Alternativet baserer seg på at Etterretningstjenesten utplasserer etterretningssensorer i utvalgte virksomheter.

Fordelen med denne løsningen er at de personvernmessige konsekvensene vil være betraktelig mindre sammenlignet med de øvrige alternativene. Ulempen er at løsningen vil ha lav etterretningsmessig verdi. Det skyldes flere forhold.

For det første vil det ønskelige metadataperpektivet ikke oppnås, med mindre virksomheten har lagret relevante data og utleverer dem til Etterretningstjenesten

For det andre vil utplassering av etterretningssensorer kun bidra til å avdekke sikkerhetstruende hendelser rettet mot de virksomhetene hvor sensorene er utplassert. Aktivitet rettet mot andre steder vil ikke kunne oppdages, og vil dermed gi et dårlig bilde av trusselaktørens totale aktivitet i og mot Norge. Det er kun kjente og oppdaterte digitale signaturer som vil kunne bidra til å avdekke hendelsene. Selv ved «treff» vil ikke denne løsningen kunne besvare de sentrale spørsmålene som oppstår ved et digitalt angrep, dvs. *når* aktøren først ble observert, *hvilken* aktør som står båk, *hvilke* (øvrige) mål i Norge aktøren går etter, og *hva* som er intensjonen med aktiviteten. Manglende helhetsoversikt vil gi et dårligere utgangspunkt for trusselvurderinger, som igjen vil gi redusert evne til effektiv innretting av forebyggende sikkerhetstiltak.

For det tredje vil operasjoner rettet mot virksomheter uten sensorer fortsatt kunne iverksettes og gjennomføres uten at Etterretningstjenesten oppdager det. Et kompliserende moment er at det vil være utfordrende å vite *hvor* sensorene bør plasseres. En av årsakene til dette er at det ofte ikke er den kompromitterte virksomheten som er trusselaktørens endelige mål. Utenlandske trusselaktører kan benytte norske virksomheter som en del av sin infrastruktur ved å opprette såkalte kommando- og kontrollnoder i servere til små og mellomstore bedrifter som ikke regnes som kritiske for Norge. Slik aktivitet vil kunne skjule trusselaktørens identitet og bidra til gjennomføring av nettverksoperasjoner rettet mot andre mål i Norge eller mot utenlandske mål. Det vil være mulig å se trafikk til og fra en kjent trusselaktør der hvor det finnes en sensor, men det vil ikke være mulig å avdekke hvilke andre virksomheter som er berørt og når trusselen først forekom i Norge. Departementet vurderer at en løsning basert på sensorer i liten grad vil bidra til å gi et helhetlig bilde av trusselaktørenes aktivitet i det digitale rom. Riktignok vil de data som innhentes gjennom sensorene kunne lagres og analyseres i ettertid, men i motsetning til data innsamlet gjennom bred dekning av kommunikasjonsstrømmene, vil ikke denne løsningen kunne gi det nødvendige helhetsbildet. Mangelen på et helhetlig bilde vil redusere evnen til å bygge

situasjonsforståelse, og således muligheten til å tolke hendelser på en korrekt måte. For eksempel kan en virksomhet med sensorer utsettes for noe som i realiteten er et digitalt angrep på flere virksomheter, men hvor kun den ene hendelsen detekteres. Det vil dermed vanskeliggjøre kartlegging av omfanget av et digitalt angrep og iverksettelse av effektive, rettidige og adekvate mottiltak. Videre må det legges til grunn at avanserte trusselaktører har kapasitet til å kartlegge svakheter i systemet uten å bli oppdaget, herunder hvilke virksomheter som har og ikke har sensorer. Departementet mener dermed at dette alternativet er egnet for omgåelse, samtidig som det kan skape en falsk følelse av trygghet.

En sensorløsning som vil gi et noenlunde tilstrekkelig bredt bilde av cyberetterretning og digitale forberedelser til cybersabotasje og lignende, vil derfor kreve utplassering av sensorer i tusentalls. Disse sensorene må være høyt graderte objekter etter sikkerhetsloven fordi de må kunne håndtere høyt gradert informasjon. Løsningen forventes derfor å bli svært kostbar og krevende å håndtere med tanke på sikring av de mange lokasjonene.

Departementet har også vurdert i hvilken grad sensorer i utvalgte virksomheter kan bidra til Etterretningstjenestens øvrige oppgaveløsning. Løsningen er ikke egnet til å gi tjenesten tilgang på informasjon som kan brukes til å avdekke og kartlegge terrornettverk og således bidra til å forebygge og avverge terroranslag mot Norge eller norske interesser i utlandet. Årsaken til dette er at Etterretningstjenesten har behov for å kunne søke etter relevant informasjon som stammer fra kommunikasjon i transitt mellom trusselaktørene. Slik kommunikasjon stammer fra private kommunikasjonsplattformer, og vil ikke fanges opp av sensorer utplassert i utvalgte virksomheter. Løsningen er heller ikke egnet til å løse tjenestens øvrige oppgaver.

Det følger av det ovennevnte at utrulling av etterretningssensorer i en lang rekke virksomheter vil kunne bli svært kostbart, samtidig som den etterretningsmessige verdien vil være svært lav. Departementet kan på denne bakgrunn ikke anbefale løsningen. Løsningen kan oppsummeres som følger:

EFFEKT	**Sensorer hos utvalgte virksomheter**
Kontraterror	Kontraterrormål kan ikke følges ved sensorer hos utvalgte virksomheter. Aktørene benytter seg av private kommunikasjonsmidler (PC og mobiltelefon). **Ingen etterretningsmessig verdi mot terrortrusler.**
Digitale trusler	Svært mange sensorer vil måtte plasseres ut for å oppnå selv en lav dekning. Avanserte aktører oppretter kommando- og kontrollnoder hos små og mellomstore virksomheter som ikke vil kunne dekkes. Det vil ikke være mulig å se det totale omfanget av et angrep/en trussel. Private PC-er og mobiltelefoner benyttes ofte som inngangsport til virksomhetens interne nettverk. Disse vil ikke være dekket. **Lav etterretningsmessig verdi mot digitale trusler.**
Øvrige oppdrag	Sensorene vil ikke gi tilgang til trafikk som er egnet til å løse tjenestens øvrige oppdrag, som f.eks. å bidra til ivaretakelse av prioriterte norske utenriks-, forsvars- og sikkerhetspolitiske interesser.

	Ingen etterretningsmessig verdi for tjenestens øvrige oppdrag.

11.7.4 «Nullalternativet»

11.7.4.1 Nærmere om hva alternativet går ut på

«Nullalternativet» innebærer at status quo fastholdes og at Etterretningstjenesten ikke får tilgang til grenseoverskridende elektronisk kommunikasjon gjennom pliktig tilrettelegging fra hjemlige tjenestetilbydere. Spørsmålet er hvordan dette vil påvirke tjenestens oppgaveløsning og hvilke konsekvenser manglende tilgang kan få for norske myndigheters ansvar for ivaretakelsen av rikets sikkerhet.

Etterretningstjenestens fremste oppgave er å produsere etterretningsanalyser til bruk for norske myndigheter. Etterretningsanalysene brukes som grunnlag for myndighetenes beslutninger knyttet til norske interesser innenfor forsvars-, sikkerhets- og utenriksdomenet. For å lage gode analyser har tjenesten behov for informasjon fra forskjellige kilder og fra ulike tidsrom. Når relevante informasjonsbiter settes sammen til et hele, kan tjenesten trekke slutninger om hvorvidt informasjonen danner grunnlag for rapportering eller varsling til myndighetene. Dersom tjenesten mangler tilgang på sentrale informasjonskilder, vil dette nødvendigvis ha betydning for etterretningsanalysenes kvalitet. Informasjonsgapet må derfor fylles, enten ved at man mottar informasjon fra andre, eller øker egen innsamling ved bruk av andre metoder.

11.7.4.2 Departementets vurdering

Gjennom internasjonalt etterretningssamarbeid får Etterretningstjenesten utlevert relevant informasjon, herunder elektronisk kommunikasjon. Samarbeidet er av vesentlig betydning for å dekke Etterretningstjenestens informasjonsbehov og for at tjenesten skal kunne løse sitt samfunnsoppdrag. Departementet anser etterretningssamarbeidet som viktig for Norge, og mener at det er i norsk interesse å ivareta forholdet til våre samarbeidspartnere. Likevel er det grunn til å problematisere en for sterk avhengighet til andre lands etterretningstjenester. Det er særlig to forhold som bør trekkes frem i lys av «nullalternativet».

Det første er hensynet til nasjonal selvstendighet og suverenitet. Norske myndigheter er i dag avhengig av etterretningssamarbeid med andre land. Informasjonen som blir utlevert er innhentet på bakgrunn av vedkommende etterretningstjenestes løsning av *egne* oppgaver. Følgelig er ofte den informasjonen som Norge får utlevert et biprodukt av partnernes egne prioriteringer. I tillegg kommer varsler ofte for sent. For Norge er denne avhengigheten en sårbarhet som i verste fall kan føre til en svekkelse av evnen til å treffe riktige beslutninger angående nasjonal sikkerhet. Et annet aspekt ved dette er at vi blir sårbare for ufullstendig eller villedende informasjon. De fleste stater anser etterretning som et nasjonalt anliggende, hvor egne interesser – naturlig nok – kommer foran andre lands behov og interesser. En samarbeidspartner kan dermed velge å holde noe informasjon tilbake og bare dele de informasjonsbitene som tjener egne interesser. Dette kan tenkes både for å skjerme egne kapasiteter og metoder, eller fordi de ønsker at Norge skal treffe en bestemt beslutning og dermed velge å gi den informasjonen som er best egnet til å dytte norske myndigheter i «riktig» retning. All informasjon vil i utgangspunktet være nyttig, men departementet anser det som en vesentlig svakhet dersom Etterretningstjenesten ikke har anledning til selv å verifisere informasjonen den får utlevert. For sterk avhengighet av andre lands tjenester kan svekke den nasjonale evnen til å treffe rettidige og presise beslutninger. Egen tilgang vil

gjøre Norge mindre prisgitt andre lands informasjonsdeling, og bidra til å styrke Etterretningstjenestens evne til å lage etterretningsanalyser og trusselvurderinger av best mulig kvalitet til norske myndigheter.

Det andre forholdet som bør trekkes frem er Norges evne til å bidra i internasjonalt etterretningssamarbeid. Operativt samarbeid er en stadig viktigere forutsetning for at Etterretningstjenesten skal kunne ivareta sitt samfunnsoppdrag, og det er i Norges interesse å opprettholde sin status som en relevant og kompetent samarbeidspartner. Å opprettholde et nært etterretningssamarbeid krever imidlertid at tjenesten bevarer evnen til å bidra med både sivile og militære etterretninger som er relevante for våre samarbeidspartnere. Ettersom elektronisk kommunikasjon er, og vil fortsette å være, en stadig mer sentral kilde til etterretningsrelevant informasjon, er det nærliggende å anta at manglende tilgang vil redusere Etterretningstjenestens evne til å bidra i etterretningssamarbeidet. En bekymring knyttet til «nullalternativet» er dermed at andre lands etterretningstjenester ikke vil dele informasjon med Norge i like stor grad i fremtiden som nå. Dette vil i så fall innebære en svekkelse av tjenestens evne til å bidra til ivaretakelse av nasjonal sikkerhet.

En annen følge av «nullalternativet» er at informasjonsgapet som vil oppstå må fylles gjennom utvidet bruk av andre midler, eksempelvis menneskebasert innhenting. Slik kompensering kan medføre økt risiko for Etterretningstjenestens personell der disse må operere nærmere trusselaktører eller i områder der de kan finne etterretningsrelevant informasjon. I Norge kan manglende utenlandsetterretning paradoksalt nok medføre økt bruk av innenlandsetterretning. PST kan bli nødt til å øke overvåkingstrykket mot norske rettssubjekter for å være i stand til å avdekke og kartlegge mistenksom utenlandsk aktivitet i Norge og vurdere hvorvidt vedkommende aktører utgjør en trussel for rikets sikkerhet. I så måte kan mangel på tilgang til elektronisk kommunikasjon bli mer inngripende for norske borgere enn hvis Etterretningstjenesten gis tilgang, fordi PST kun fokuserer på den norske enden av kommunikasjonen.

Til tross for økt innenlandsetterretning, vil «nullalternativet» medføre at ingen myndigheter vil kunne detektere utenlandske forhold og trusler som ikke er knyttet til mulige pågående eller fremtidige straffbare handlinger, også fordi dette vil falle utenfor PSTs lovbestemte oppgaver. Løsningen kan dermed tenkes å fremtvinge en diskusjon om ansvarsgrensene mellom PST og Etterretningstjenesten. Departementet legger likevel til grunn at et utvidet ansvar for PST når det gjelder strategisk etterretning neppe vil være ønskelig, blant annet fordi det vil kreve oppbygging av dublerende kompetanse og kapasiteter som etter departementets vurdering ikke er samfunnsøkonomisk regningssvarende. Løsningen vil også være suboptimal når man tar i betraktning nødvendigheten av å sammenstille informasjon fra tilrettelagt innhenting med informasjon innhentet basert på andre tilganger og metoder for å danne det helhetlige bildet av utenlandske trusler og andre utenlandsetterretningsrelevante forhold.

Aktiviteten som utspiller seg i og ved bruk av det digitale rom kan på en alvorlig måte utfordre stats- og samfunnssikkerheten. Departementet ser med bekymring på omfanget av informasjon som trusselaktører kan tilegne seg fra norske digitale systemer og hvilken skade som kan gjøres, sist sett ved det omfattende angrepet mot Helse Sør-Øst i januar 2018. Systemer kan dessuten manipuleres eller ødelegges, og det kan plantes skadevare for senere bruk. Utenlandske aktører benytter også det digitale rom for å rekognosere og planlegge annen aktivitet som kan true Norges grunnleggende sikkerhetsinteresser og evne til å beskytte befolkningen mot utenlandske trusler. Departementet mener at man gitt dagens

trusselsituasjon ikke kan forholde seg passiv til de sårbarheter vi står overfor som nasjon. Følgelig vil et valg av status quo medføre at man må belage seg på andre og kompenserende tiltak for å søke å avbøte informasjonsgapet. Departementet kan på denne bakgrunn ikke anbefale «nullalternativet».

11.7.5 Lysne II-utvalgets modell

Lysne II-utvalget anbefalte innretningen «digitalt grenseforsvar» (DGF).[216] Utvalget definerer DGF slik:

> «E-tjenestens målrettede innhenting og analyse av utenlandsetterretningsrelevant informasjon, basert på aksess til elektronisk kommunikasjon som går inn og ut av Norge, i den hensikt å kartlegge og motvirke mulige ytre trusler mot rikets sikkerhet og selvstendighet og andre viktige nasjonale interesser.»

Lysne II-utvalgets anbefaling innebærer at Etterretningstjenesten gis anledning til å samle inn og lagre elektronisk kommunikasjon i bulk,[217] og på nærmere bestemte kriterier søke i og bruke den lagrede informasjonen til utenlandsetterretningsformål.

Utvalgets anbefaling er dels betinget av et bestemt teknologisk oppsett, og dels av omfattende tilgangsregler, formålsskranker og kontrollregimer. Den tekniske installasjonen består av lagrede data, filtre som filtrerer ut hvilke data som skal kunne lagres, og maskinell kontroll med hvilke søk som tillates utført i disse datalagrene. Kontrollmekanismene som foreslås består av en domstol som står for forhåndsgodkjenninger, et tilsyn som overvåker bruken av DGF i nær sanntid, samt at EOS-utvalget styrkes for å etterhåndskontrollere Etterretningstjenestens bruk av DGF.

Systemet som foreslås av Lysne II-utvalget består av tre forskjellige datasett som det kan gjøres søk i. Disse tre datasettene kaller utvalget for korttidslageret, metadatalageret og lageret med spesifiserte innholdsdata.

11.7.5.1 Korttidslageret

Korttidslageret inneholder et uttrekk av ufiltrert kommunikasjon som har gått over den fiberoptiske kabelen i løpet av den siste 14-dagers perioden. Dette er ikke et kontinuerlig bilde av all datatrafikk, men svært korte tidsintervaller som vil inneholde både metadata og innholdsdata. Lysne II-utvalget foreslår at intervallene normalt ikke bør være lengre enn ett minutt, og at det bør legges restriksjoner på hvor hyppig innsamlingsintervallene kommer. Korttidsdatalageret vil bare benyttes til teknisk vedlikeholdsarbeid av de filterfunksjonene som Lysne II-utvalget foreslår, og aldri til søk for etterretningsformål. Lysne II-utvalget vurderer at mellomlagring av data er nødvendig for å kunne gjøre et fornuftig utvalg av kommunikasjonsbærere, herunder forstå hva slags kommunikasjon som går på bæreren, samt for å videreutvikle filtrerings- og seleksjonsmekanismene i systemet og etterfølgende re-prosessering. På denne bakgrunn vurderer Lysne II-utvalget at korttidslageret er helt nødvendig for å drive kontinuerlig teknologisk oppdatering av filtrene i systemet.

---

[216] Punktet her refererer til Lysne II utvalgets rapport og bruker følgelig begrepene «digitalt grenseforsvar» og DGF.

[217] Med bulkinnhenting/bulkaksess mener Lysne II-utvalget at Etterretningstjenesten må samle inn eller på annen måte ha tilgang til store mengder data *før* tjenesten målrettet og med bruk av utvalgte søkekriterier kan trekke ut relevant informasjon fra den større datamengden. Datamengdene det søkes i vil da inneholde en betydelig mengde informasjon som ikke er relevant for utenlandsetterretningsformål.

På grunn av at korttidsdatalageret vil inneholde ufiltrert kommunikasjon, anbefaler Lysne II-utvalget at det legges svært sterke begrensninger på hvordan dette lageret kan benyttes. Utvalget foreslår at korttidslageret skal behandles av mennesker, og at gruppen mennesker som har tilgang må være liten. Det må utvikles tydelige retningslinjer for hvordan datasettene kan samles inn og brukes. Som det vises til nedenfor foreslår utvalget at Etterretningstjenestens bruk av korttidslageret og informasjonen som stammer herfra bør underlegges kontroll av det såkalte DGF-tilsynet. Det foreslås at DGF-tilsynet skal ha som oppdrag å ettergå retningslinjene og praktiseringen av disse, samt all utvikling og alle oppdateringer av DGF-systemet som sådan og dets ulike funksjoner. Utvalget anbefaler videre at tilsynet bør rapportere periodisk til EOS-utvalget om hvordan korttidslageret er benyttet, og hvilke filteroppdateringer det har ført til.

11.7.5.2 Metadatalageret

Metadatalageret inneholder metadata fra utvalgte protokoller knyttet til utvalgte kommunikasjonstjenester. Utvalget foreslår at metadata skal lagres i så lang tid som anses nødvendig for å løse etterretningsoppdrag, og maksimalt 18 måneder. Dette antallet måneder vurderes som nødvendig og tilstrekkelig for å kunne gjennomføre en tilfredsstillende retrospektiv analyse av trafikkdata. Så langt det er teknisk og praktisk mulig vil metadata som ikke er relevant for Etterretningstjenestens samfunnsoppdrag filtreres bort, men utvalget legger til grunn at ikke alle irrelevante data lar seg filtrere bort.

Etterretningstjenestens søk i metadatalageret vil kun baseres på personselektorer knyttet til personer som DGF-domstolen har godkjent eller modusselektorer knyttet til parametere som DGF-domstolen har godkjent.

Lysne II-utvalget slår fast at effektiv kontroll med bruken av metadata må bygge på strenge begrensninger på søk i metadatalageret. Utvalget anbefaler at hvert søk i metadatalageret må gjennomføres av en særskilt DGF-operatør og at alle søk skal logges for kontrollformål.

Utvalget anbefaler at hvert søk bør være hjemlet i en rettsavgjørelse. Utvalget anbefaler at rettsavgjørelsen må inneholde minst ett av følgende elementer:

1. den bør identifisere konkrete individer eller kategorier av individer som det er lov å søke på, hvorpå avgjørelsen åpner for søk på alle personselektorer tilknyttet disse, eller
2. den bør identifisere et handlingsmønster eller lignende modus som det er lov å gjøre søk på.

Utvalget vurderer at søk i metadatalageret bør ta utgangspunkt i enten en kjent aktør eller et kjent modus, og at det ikke bør tillates søk hvor både aktør og modus er ukjent.

11.7.5.3 Innholdsdatalageret

Lageret med spesifiserte innholdsdata vil inneholde fullstendige datastrømmer med kommunikasjon tilknyttet personselektorer. Selektorene skal etter forslaget være forhåndsgodkjent av DGF-domstolen. Lysne II-utvalget anbefaler at DGF-tilsynet har innsyn i DGF-domstolens avgjørelser, i utformingen av filtermekanismen tilknyttet lageret og i alle søk som gjøres her. Formålet med tilsynets innsyn vil være å kontrollere i hvilken grad lageret kun inneholder data innenfor rammen av domstolens kjennelse. Tilsynet anbefales å rapportere jevnlig til EOS-utvalget om hvordan innholdsdatalageret benyttes, og om hvordan beslutningene i domstolen omsettes i filtreringsmekanismer.

11.7.5.4 Utvalg og filtrering

Filtreringssystemet som Lysne II-utvalget foreslår innebærer tre filtre med forskjellige oppgaver. Filter 1 har som hovedoppgave å redusere mengden data som flyter inn i systemet. Dette gjøres for det første gjennom å dynamisk velge ut hvilke kommunikasjonsbærere som til enhver tid er i Etterretningstjenestens søkelys. Lysne II-utvalget foreslår at valg av kommunikasjonsbærere skjer etter dialog med tjenestetilbyderne og basert på forutgående teknisk profilering av datatrafikk. For det andre skal mengden data reduseres ved å foreta filtrering av trafikk som enkelt lar seg identifisere som utenfor Etterretningstjenestens oppgavesett. Dette vil i stor grad skje gjennom negativ filtrering. Nye kommunikasjonsformer som ikke tidligere er identifisert vil derfor slippe gjennom.

Filter 2 har som oppgave å filtrere bort alle innholdsdata. Videre skal det i størst mulig grad filtrere ut overskuddsinformasjon i form av metadata. Filtrering av innholdsdata er teknisk overkommelig, i motsetning til fullstendig filtrering av metadata. Metadatalageret vil derfor inneholde store mengder overskuddsinformasjon.

Filter 3 har som oppgave å slippe gjennom kun innholdsdata og tilhørende metadata fra datatrafikk knyttet til personselektorer som er godkjent av DGF-domstolen.

11.7.5.5 Kontrollmekanismer

Lysne II-utvalgets anbefaling om å innføre et digitalt grenseforsvar er betinget av at det innføres strenge kontrollmekanismer som vil tilføre systemet troverdighet og en forsikring mot at søk og innsyn i data skjer i større utstrekning enn strengt nødvendig. Kontrollmekanismene består av tre hovedelementer: DGF-domstol, DGF-tilsyn og EOS-utvalgets kontroll.

DGF-domstolen foreslås å skulle forhåndsgodkjenne hvilke objekter det skal samles inn innholdsdata fra, og hvilke objekter og handlingsmønstre man kan gjøre søk på i metadatalageret. DGF-tilsynet foreslås å skulle, i nær sanntid, motta all informasjon om alle søk som gjøres i alle datasamlinger i DGF-systemet, motta alle avgjørelser fra DGF-domstolen, ha tilgang til all informasjon om hvordan filtrene er implementert og konfigurert, og ha tilgang til all informasjon om hvordan interne retningslinjer og avgjørelser fra domstolen er oversatt til søkeprivilegier. Utvalget anbefaler videre at DGF-tilsynet skal rapportere avvik til EOS-utvalget og for øvrig rapportere regelmessig til EOS-utvalget, Forsvarsdepartementet og Samferdselsdepartementet, samt føre tilsyn med at datasikkerheten i DGF-systemet er så høy som teknologisk og praktisk mulig. EOS-utvalget foreslås å føre etterhåndskontroll på samme måte som den gjør for Etterretningstjenestens virksomhet i dag. I tillegg anbefaler Lysne II-utvalget at EOS-utvalget skal motta rapporter fra DGF-tilsynet, ha ubegrenset innsynsrett i DGF-systemet og ha rapporteringsplikt til Stortinget om Etterretningstjenestens bruk av systemet, og om Forsvarsdepartementets håndtering av tjenestens bruk.

For nærmere redegjørelse av Lysne II-utvalgets anbefaling vedrørende kontrollmekanismene vises til Lysne II-rapporten punkt 9.2.2, 9.3.2 til 9.3.4 og 9.5.2.

11.7.6 Departementets vurdering

Statens mest grunnleggende oppgave er å sikre landets suverenitet og innbyggernes sikkerhet. Truslene i det digitale rom er sterkt økende. Digitale angrep rettet mot både private og offentlige aktører finner sted daglig. Fremmede aktørers etterretningsoperasjoner i det digitale rom representerer en alvorlig trussel mot norske myndigheter og virksomheter.

Aktørene som står bak slik aktivitet er kapable, pågående og effektive. Manglende evne til å avdekke ondsinnet aktivitet gjør at Norge kan benyttes som en «frihavn» til å rute nettverksoperasjoner og angrep via Norge mot andre land. Terrorisme og voldelig ekstremisme forblir en alvorlig trussel mot vår sikkerhet, og en rekke terrorangrep og avdekte planer om terror de siste årene viser hvor grenseløs og kompleks terrortrusselen er. Fysiske avstander og landegrenser elimineres ved at terrorister i stor grad rekrutterer, kommuniserer og koordinerer seg imellom ved bruk av sosiale medier, applikasjoner og samtaletjenester. Vektige hensyn tilsier at Etterretningstjenesten må settes i stand til å kunne oppdage og avverge fremmed aktivitet som truer norsk stats- og samfunnssikkerhet.

Departementet har vurdert ulike alternativer som kan være egnet til å fylle informasjonsgapet som følger av at Etterretningstjenesten i dag ikke har tilgang til elektronisk kommunikasjon som transporteres i fiberkabler, altså via Internett. Et grunnleggende utgangspunkt i vurderingen har vært at løsningen må gi etterretningsmessig verdi. Som det fremgår av drøftelsene over mener departementet at det er knyttet svakheter til alle de alternativene løsningene til Lysne II-utvalgets forslag. Sammenstilt kan dette fremstilles slik:

	Alt 1 **Lettversjonen**	**Alt 2** **Sensorer i utvalgte virksomheter**	**Alt 3** **Null-alternativet**	**Alt 4** **Lysne II**
Kontraterror	Svært lav verdi	Ingen verdi	Ingen verdi	God verdi
Cybertrusler	Svært lav verdi	Lav verdi	Ingen verdi	God verdi
Øvrige oppdrag	Svært lav verdi	Ingen verdi	Ingen verdi	God verdi

Alternativ 1 innebærer en løsning uten et bredt metadatagrunnlag, som er viktig både for tjenestens målsøking og evnen til å finne og følge kjente etterretningsmål. Som omtalt over er målsøking grunnstammen i og forutsetningen for etterretningsvirksomhet. Normalt gjøres målsøking basert på historiske data så snart en eller annen form for inngangsparameter foreligger. Et inngangsparameter kan for eksempel være et telefonnummer til en mulig smugler av kjemiske våpen. Etterretningstjenesten vil da umiddelbart prøve å finne ut hvilken aktør som kan knyttes til telefonnummeret, om aktøren har vært i kontakt med andre medsammensvorne man ikke kjenner til, og om aktøren har andre identifikatorer (e-postadresser osv.). For å kunne gjøre disse analysene, er historiske data avgjørende, også fordi telefonnummeret trolig ikke lenger er i bruk. Ved å nøste i den historiske aktiviteten kan andre ledetråder komme frem, som er avgjørende for å gi etterretningsinformasjon som kan bidra til at ansvarlige myndigheter kan rette inn sine virkemidler, rulle opp nettverket og forhindre spredning av kjemiske våpen.

Etter departementets vurdering er alternativ 1 likevel konseptuelt å foretrekke fremfor alternativ 2. Alternativ 2 medfører tilgang til informasjon fra bare utvalgte virksomheter. Sensorsystemet gir i likhet med alternativ 1 ikke noe relevant metadatagrunnlag som kan benyttes i målsøking. I tillegg vil alternativ 2 ikke være et relevant verktøy for å forebygge terrortrusler, fordi forberedelse, planlegging og rekruttering til terrorisme erfaringsmessig ikke skjer ved hjelp av en virksomhets IKT-utstyr, men med private PC-er og mobiltelefoner.

Alternativ 3 tilsvarer dagens situasjon og medfører at Norge ikke vil ha noen systemer for å kontrollere den digitale landegrensen og innhente elektronisk kommunikasjon i norskkontrollerte ekomnett og -tjenester om fremmede aktører og forhold som kan representere en trussel mot Norge eller norske interesser. Dette vil i så fall måtte søkes kompensert med økt innenlandsovervåking, økt bruk av inngripende metodebruk og stor avhengighet av partnere, med de konsekvenser dette vil innebære.

I dag har norske myndigheter en svært begrenset evne til å oppdage, følge, varsle og motvirke alvorlige trusler mot Norge. Etter departementets syn bør dagens situasjon avhjelpes ved at Etterretningstjenesten får tilgang til etterretningsrelevant elektronisk kommunikasjon fra fremmede aktører når denne krysser grensen til norsk territorium ved hjelp av elektroniske kommunikasjonstjenester og -nett som er underlagt norsk jurisdiksjon og lovgivning, innenfor de strenge begrensninger og kontrollmekanismer som vil gjelde for Etterretningstjenestens informasjonsinnhenting, og innenfor de prioriterte informasjonsbehov som overordnede politiske myndigheter fastsetter. På bakgrunn av drøftelsene over mener departementet at Etterretningstjenesten bør få anledning til å innhente både metadata i bulk, samt målrettet innholdsdata. Dette anses nødvendig for å kunne utføre tjenestens samfunnsoppdrag på best mulig måte. Utredede alternativer er ikke egnet til å ivareta dette.

Departementets konklusjon på dette punkt underbygges av EMDs uttalelse i saken *Big Brother Watch mot Storbritannia*,[218] hvor domstolen sluttet seg til konklusjonene i to spesifikke utredninger foretatt av henholdsvis den britiske *Independent Reviewer of Terrorism Legislation* og Den europeiske kommisjonen for demokrati gjennom lovgiving (Veneziakommisjonen).[219] Utredningene konkluderte i korte trekk med at bulkinnsamling av data var en essensiell kapabilitet hvis nytteverdi ikke kunne oppnås med alternative midler, og ble omtalt som følger: [220]

> "384. With regard to the proportionality of the bulk interception regime, the Court notes that the Independent Reviewer of Terrorism Legislation, examined a great deal of closed material and concluded that bulk interception was an essential capability: first, because terrorists, criminals and hostile foreign intelligence services had become increasingly sophisticated at evading detection by traditional means; and secondly, because the nature of the global Internet meant that the route a particular communication would travel had become hugely unpredictable. Although he and his team (including a person with the necessary technical background to understand the systems and techniques used by GCHQ, and the uses to which they could be put, an investigator with experience as a user of secret intelligence, including intelligence generated by GCHQ, and senior independent counsel with the skills and experience to challenge forensically the evidence and the case studies presented by the security and intelligence services) looked at alternatives to bulk interception (including targeted interception, the use of human sources and commercial cyber-defence products), they concluded that no alternative or combination of alternatives would be sufficient to substitute for the bulk interception power (see paragraph 176 above).
>
> 385. Similarly, while acknowledging the risks that bulk interception can pose for individual rights, the Venice Commission nevertheless recognised its intrinsic value for security operations, since it enabled the security services to adopt a proactive approach, looking

[218] Dommen ble avsagt 13. september 2018 og er i skrivende stund ikke rettskraftig.
[219] The 2015 *Report of the European Commission for Democracy through Law ("the Venice Commission") on the Democratic Oversight of Signals Intelligence Agencies* og *Report of the bulk powers review* av David Anderson Q.C. (august 2016)
[220] *Big Brother Watch m.fl. mot Storbritannia* av 13. september 2018, avsnitt 384-386

for hitherto unknown dangers rather than investigating known ones (see paragraph 211 above).

386. The Court sees no reason to disagree with the thorough examinations carried out by these bodies and the conclusions subsequently reached. It is clear that bulk interception is a valuable means to achieve the legitimate aims pursued, particularly given the current threat level from both global terrorism and serious crime."

En vurdering av etterretningsmessig verdi har vært avgjørende for at departementet har valgt å foreslå en løsning som i kjernen er lik Lysne II-utvalgets anbefaling. Departementet foreslår imidlertid en rekke endringer som særlig knytter seg til innretningen og organiseringen av kontrollmekanismene. Departementet vurderer at disse endringene styrker ordningen.

Innsamling, lagring og bruk av meta- og innholdsdata vil ha menneskerettslige og personvernrettslige implikasjoner. Departementet vil understreke at all innhenting og videre bruk av lagrede data må være underlagt strenge restriksjoner som sikrer at all bruk er innenfor gjeldende rettslige rammer, herunder borgernes rett til respekt for sitt privatliv. I det følgende vil det redegjøres for departementets forslag til nærmere innretning og lovregulering av Etterretningstjenestens tilgang til elektronisk kommunikasjon gjennom tilrettelagt innhenting.

11.8 Rettslige rammer for tilrettelagt innhenting

11.8.1 Innledning

Departementet skal i det følgende vurdere hvorvidt tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon kan gjennomføres innenfor gjeldende konstitusjonelle og folkerettslige rammer.

11.8.2 Menneskerettslige rammer

11.8.2.1 Innledning

De menneskerettslige rammene for tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon følger i hovedsak av Grunnloven, Den europeiske menneskerettskonvensjon (EMK) og FNs konvensjon om sivile og politiske rettigheter (SP). Enkelte av Norges EØS-rettslige forpliktelser kan også sies å ha en side til menneskerettighetene. EØS-retten behandles nedenfor i punkt 11.8.3.

Det følger av Grunnloven § 102 første ledd første punktum at enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Bestemmelsen har paralleller i EMK artikkel 8 og SP artikkel 17. Det følger av menneskerettsloven §§ 2 og 3 at disse bestemmelsene gjelder som norsk lov og ved motstrid går foran bestemmelser i annen lovgivning. Det er særlig retten til respekt for privatliv og retten til respekt for kommunikasjon som er den sentrale rammen for tilrettelagt innhenting, og som departementet vil fokusere på i det følgende. Tilrettelagt innhenting kan imidlertid også berøre andre menneskerettigheter, herunder særlig ytrings- og informasjonsfriheten, jf. Grunnloven § 100, EMK artikkel 10 og SP artikkel 19.

Departementet legger til grunn at tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon utgjør et inngrep i retten til respekt for privatliv og kommunikasjon. Det er

ikke tvilsomt at de formene for kommunikasjon som vil hentes inn etter forslaget, både innholdsdata og metadata, omfattes av rettighetsvernet. Innsamlingen, lagringen og bruken vil normalt regnes som selvstendige inngrep, og det kan heller ikke utelukkes at lovgivningen i seg selv kan regnes som et inngrep. Departementet viser til Lysne I-utvalgets utredning Digital sårbarhet – sikkert samfunn[221] s. 78 med videre henvisninger og Lysne II-utvalgets rapport s. 39.

Grunnlovsvernet av privatliv og kommunikasjon gjelder ikke absolutt. Formuleringen «rett til respekt for» ble valgt for å synliggjøre at bestemmelsen ikke står i veien for lovlig etterretning.[222] Det følger av Høyesteretts praksis at inngrep i Grunnloven § 102 første ledd første punktum kan finne sted når inngrepet har hjemmel i lov, forfølger et legitimt formål og er forholdsmessig, se for eksempel Rt. 2015 s. 93 avsnitt 60. Departementet vil i det følgende drøfte hvorvidt disse tre vilkårene er oppfylt.

11.8.2.2 Tilfredsstiller tilrettelagt innhenting kravet til hjemmel i lov?

Det første vilkåret som må være oppfylt for at inngrepet skal kunne aksepteres, er kravet til *hjemmel i lov*. Kravet kan sees i sammenheng med det generelle legalitetsprinsippet som følger av Grunnloven § 113. Prinsippet skal legge til rette for forutberegnelighet for borgerne og sikre at forvaltningen holder seg innenfor rammen av fullmaktene de er gitt av folkets representanter i Stortinget.

Hjemmelskravets *formelle side* vil utvilsomt være oppfylt gjennom at inngrepet vil ha grunnlag i lov vedtatt av Stortinget i tråd med Grunnloven § 75 bokstav a. Kravet til hjemmel i lov har imidlertid også en *kvalitativ side*. Det stilles for det første visse krav til lovgivningens *klarhet* og *presisjon*. På denne bakgrunn har departementet i lovutkastet kapittel 7 og 8 tilstrebet å regulere tiltaket så klart og presist som mulig. Både av hensyn til at regelverket ikke må bli så omfattende at det blir vanskelig tilgjengelig og av hensyn til å unngå at etterretningsmål kan innrette seg slik at de omgår systemet, foreslås ikke alle detaljer lovregulert. Etter departementets syn oppfyller lovforslaget her de krav til klarhet og presisjon som følger av hjemmelskravet.

Hjemmelskravet tilsier at lovgivningen ikke må være for fragmentarisk. Departementet har på denne bakgrunn tilstrebet å samle bestemmelsene om tilrettelagt innhenting i lovutkastet kapittel 7 og 8. Det er samtidig ikke til å komme ifra at lovgivning av et visst omfang vil ha en viss fragmentarisk karakter. I lovforslaget her vil for eksempel bestemmelsene i lovutkastet kapittel 7 og 8 måtte leses i sammenheng blant annet med reglene om Etterretningstjenestens oppgaver i lovutkastet kapittel 3, innhentingsforbudene i kapittel 4 og grunnvilkårene i kapittel 5. Dette er etter departementets vurdering ikke i strid med hjemmelskravet.

Kravet til hjemmel kan også sies å innebære et krav til rimelige garantier mot vilkårlighet og misbruk, se for eksempel Høyesteretts flertall i Rt. 2014 s. 1105 avsnitt 30 med videre henvisninger til praksis fra EMD. Departementet har lagt stor vekt på at lovgivningen om tilrettelagt innhenting skal inneholde solide og betryggende garantier for borgerne. Det vises særlig til punkt 11.10 til 11.13 om kontrolltiltak som foreslås for bruk av tilrettelagt innhenting.

[221] NOU 2015: 13

[222] Se Innst. 186 S (2013–2014) s. 27

Eksistensen av garantier mot vilkårlighet og misbruk har stor betydning også for tiltakets forholdsmessighet, og departementet viser i den forbindelse til vurderingen i punkt 11.8.2.4.

På bakgrunn av drøftelsen konkluderer departementet med at forslaget i høringsnotatet tilfredsstiller kravet til hjemmel i lov.

11.8.2.3 Forfølger tilrettelagt innhenting et legitimt formål?

Det andre vilkåret som må være oppfylt for at inngrepet skal kunne aksepteres, er kravet til *legitimt formål*.

Departementet finner det ikke tvilsomt at tilrettelagt innhenting forfølger et legitimt formål. Det vises til at et overordnet formål med lovforslaget er å bidra til å trygge Norges suverenitet, territorielle integritet, demokratiske styreform og andre nasjonale sikkerhetsinteresser, herunder forebygge, avdekke og motvirke utenlandske trusler mot Norge og norske interesser, se lovutkastet § 1-1 bokstav a. Tilrettelagt innhenting vil være et verktøy for Etterretningstjenesten når den løser sine lovbestemte oppgaver i tråd med lovutkastet kapittel 3. Alle disse oppgavene bidrar til å ivareta nasjonale sikkerhetsinteresser. I den spesifikke forholdsmessighetsvurderingen som må gjøres i hver enkelt sak etter lovutkastet § 5-4, vil det kunne ha betydning hvilken av oppgavene innhentingen begrunnes i.

Departementet konkluderer etter dette med at kravet til legitimt formål er oppfylt.

11.8.2.4 Er tilrettelagt innhenting forholdsmessig?

Det tredje vilkåret som må være oppfylt for at inngrepet skal kunne aksepteres, er kravet til *forholdsmessighet*. Det må foretas en *sammensatt proporsjonalitetsvurdering*, se HR-2016-2554-P avsnitt 82 for så vidt gjelder den tilsvarende vurderingen etter Grunnloven § 101 første ledd. Det overordnede vurderingstemaet kan formuleres som et spørsmål om tiltaket er nødvendig i et demokratisk samfunn, jf. EMK artikkel 8 nr. 2. Dette vurderingstemaet kan igjen konkretiseres til spørsmål om tiltaket er egnet, nødvendig og forholdsmessig, se for eksempel Høyesteretts dom HR-2018-104-A avsnitt 23. Departementet legger til grunn at de ulike spørsmålene i noen grad overlapper med hverandre. Det understrekes at forholdsmessighetsvurderingen bygger på de beskrivelser, drøftelser og vurderinger som fremgår av høringsnotatet for øvrig, og må leses i sammenheng med disse.

Departementet finner det ikke tvilsomt at tiltaket er *egnet*. Det vises til beskrivelsen i punkt 11.7.6, hvor det fremgår at tilrettelagt innhenting vil gi stor etterretningsmessig verdi. Utfordringene knyttet til økt bruk av kryptering, som flere høringsinstanser til Lysne II-utvalgets rapport har trukket fram, er omtalt samme sted. Det fremgår der at tiltaket vil ha god effekt til tross for økt bruk av kryptering.

Det neste spørsmålet er hvorvidt tiltaket er *nødvendig*.

Departementet foreslår å gi Etterretningstjenesten tilrettelagt tilgang til grenseoverskridende elektronisk kommunikasjon fordi det er et *presserende behov* for slik tilgang. Tjenesten mangler i dag tilgang på en vesentlig kilde til informasjon som er nødvendig for løsningen av tjenestens lovpålagte oppgaver. Uten slik tilgang vil det være vanskelig å oppdage og varsle om trusler som stammer fra utlandet, og manglende tilgang kan føre til at visse trusler ikke avdekkes i det hele tatt. På grunn av mangelen på tilgang er Etterretningstjenesten i dag avhengig av å fylle informasjonsgapet gjennom samarbeid med andre lands tjenester. En slik avhengighet har en rekke uheldige konsekvenser.

Det ligger i nødvendighetskravet at det ikke må finnes *mindre inngripende tiltak* som vil ha samme effekt. Departementet har vurdert ulike alternativer til tilrettelagt innhenting. Analysen tilsier at tilrettelagt innhenting basert på, men ikke identisk med, Lysne II-utvalgets forslag, vil gi best effekt, det vil si etterretningsmessig verdi som imøtekommer kravet til egnethet. Etter departementets vurdering vil de alternativene løsningene gi så lav etterretningsmessig verdi, både i seg selv og sett i forhold til de økonomiske og administrative konsekvenser forbundet med investering og drift, at de ikke kan anbefales. Det følger av analysen at også en videreføring av status quo («nullalternativet») ventes å ha en rekke negative konsekvenser, gitt sårbarhetene som Norge står overfor og behovet for kompenserende tiltak som vil oppstå. Etter departementets syn finnes det ikke mindre inngripende tiltak som vil ha samme effekt som tilrettelagt innhenting.

På bakgrunn av denne drøftelsen mener departementet at tiltaket er *nødvendig*.

Det avgjørende spørsmålet blir etter dette hvorvidt tiltaket er *forholdsmessig*. Det skal her foretas en *bredere interesseavveining*, se for eksempel Rt. 2015 s. 93 avsnitt 60, hvor Høyesterett uttaler at forholdsmessighetsvurderingen «må ha for øye balansen mellom de beskyttede individuelle interessene på den ene siden og de legitime samfunnsbehovene som begrunner tiltaket på den andre».

Departementet tar utgangspunkt i at det legitime samfunnsbehovet som begrunner tiltaket, er sterkt. Det er et overordnet formål med lovforslaget å bidra til å trygge Norges suverenitet, territorielle integritet, demokratiske styreform og andre nasjonale sikkerhetsinteresser, herunder forebygge, avdekke og motvirke utenlandske trusler mot Norge og norske interesser. Tilrettelagt innhenting skal sikre at Etterretningstjenesten får tilgang på den informasjonen som er strengt nødvendig for å kunne utføre sine oppgaver, og således bidra til å oppfylle lovens formål. Tiltakets kjerne er altså vern av vår demokratiske rettsstat og de grunnleggende verdiene, rettighetene og frihetene som denne bygger på. Det er etter departementets vurdering vanskelig å se for seg en mer tungtveiende og beskyttelsesverdig interesse enn denne.

Det er samtidig ingen tvil om at tilrettelagt innhenting utgjør et sterkt inngrep i retten til respekt for privatliv og kommunikasjon. *Metadatalageret*, hvor Etterretningstjenesten skal få lagre metadata fra grensekryssende elektronisk kommunikasjon i 18 måneder, fremstår som mest problematisk fra et personvernperspektiv. Mengden av rådata som lagres i metadatalageret vil være stor, og det må legges til grunn at en betydelig del vil være overskuddsinformasjon. Dette avhjelpes imidlertid i en viss grad gjennom at det foreslås en plikt til gjennom utvalg og filtrering å sørge for at så lite overskuddsinformasjon som praktisk mulig lagres.

Korttidslageret fremstår også som en problematisk del av systemet fordi det innebærer innhenting og lagring av *ufiltrert informasjon* for testformål. Slik testvirksomhet er avgjørende for at systemet skal kunne drives på best mulig og minst inngripende måte, blant annet med hensyn til oppdatering av filtrene som skal hindre lagring av overskuddsinformasjon. Departementet foreslår *strenge og ufravikelige tidsbegrensninger* for de ufiltrerte uttrekkene som lagres i korttidslageret, noe som begrenser misbrukspotensialet. Det foreslås også lovfestet et *uttrykkelig forbud* mot å bruke korttidslageret til etterretningsproduksjon og *personelle krav* til dem som skal gjøre uttrekkene.

Innhenting og lagring av innholdsdata gir etter departementets vurdering ikke opphav til de samme betenkeligheter med hensyn til personvernet som innhenting og lagring av metadata og testdata. Dette har sammenheng med at slik innhenting i sin natur er mer spisset.

På grunn av inngrepets karakter og omfang har departementet foreslått en rekke materielle og prosessuelle vilkår og garantier mot misbruk og vilkårlighet. Departementet viser for det første til at innhentingen er *formålsbegrenset* i tråd med Etterretningstjenestens oppgaver etter lovutkastet kapittel 3. Videre er det oppstilt *innhentingsforbud* i lovutkastet kapittel 4 og *grunnvilkår for innhenting* i lovutkastet kapittel 5. Alt personell skal være *skikket* og gjennomgå *særskilt opplæring*. Det foreslås lovfestet en *maksimal lagringstid* og regler om *behandling av personopplysninger* og *sletteplikt*. Behandling av fortrolig kommunikasjon med særlige yrkesutøvere, for eksempel advokater, helsepersonell og journalister, gis et *særlig vern*.

Departementet legger i forholdsmessighetsvurderingen stor vekt på at forslaget inneholder en rekke *kontrollmekanismer* som både hver for seg og samlet utgjør solide og betryggende garantier mot vilkårlighet og misbruk.

For det første stilles det krav om *forhåndsgodkjennelse av en domstol*. Denne oppgaven foreslås lagt til de alminnelige domstolene, som utvilsomt oppfyller de kravene som må stilles til uavhengighet fra forvaltningen. Ved at sakene behandles av alminnelige dommere unngår man risikoen for at de over tid vil identifisere seg med tjenestens virksomhet, samtidig som man ved å samle sakene i Oslo tingrett legger til rette for at de vil kunne opparbeide seg en erfaring med sakstypen som gir grunnlag for en god og reell kontroll.

Domstolen skal foreta en *fullstendig legalitetskontroll* på bakgrunn av vilkår fastsatt i loven, herunder at innhentingen er forholdsmessig og ikke strider mot noen av innhentingsforbudene. Domstolen vil normalt oppnevne en *særskilt advokat*, som avhengig av sakens karakter vil ha som oppgave å ivareta interessene til den personen som innhentingen retter seg mot eller mer alminnelige personverninteresser. Dette innebærer at domstolsprosessen så langt som mulig er *kontradiktorisk*. Det kan avholdes *muntlige forhandlinger* dersom retten ser behov for det. Kjennelsen skal *begrunnes*, noe som i seg selv utgjør en rettssikkerhetsgaranti. Den særskilte advokaten vil også kunne anke kjennelser til en overordnet domstol. Det foreslås altså en *rett til overprøving*, noe som også er en viktig rettssikkerhetsgaranti.

Den forutgående domstolskontrollen må for det andre sees i sammenheng med kontrollen som skal foretas av EOS-utvalget. EOS-utvalget foretar etter gjeldende ordning etterfølgende kontroll med Etterretningstjenestens virksomhet innenfor rammen av EOS-kontrolloven. Etter forslaget tillegges utvalget en ny kontrolloppgave som innebærer en styrket og mer løpende kontroll med Etterretningstjenestens bruk av tilrettelagt innhenting. Utvalget skal kontrollere at søk gjennomføres i tråd med rettens kjennelse, at testdata ikke benyttes til etterretningsformål og at de øvrige bestemmelsene i loven etterleves. En slik *styrket kontroll* av Etterretningstjenestens bruk av tilrettelagt innhenting kommer i tillegg til den alminnelige kontrollen som utvalget utfører etter gjeldende regelverk.

Departementet legger dessuten vekt på at det i tillegg til den uavhengige forutgående, løpende og etterfølgende kontrollen som vil utføres av domstolene og EOS-utvalget, også vil gjelde andre kontrollmekanismer, herunder tjenestens internkontroll og departementets forvaltningskontroll.

Samlet er det departementets syn at kontrollmekanismene som foreslås må karakteriseres som betryggende og solide. Et så omfattende kontrollregime som foreslås i høringsnotatet her antas å gå lenger enn de menneskerettslige krav som kan oppstilles. Departementet er ikke kjent med noe land med et system for tilrettelagt innhenting med en mer omfattende kontrollordning enn den som foreslås her.

Departementet har tatt i betraktning risikoen for *formålsglidning*, herunder særlig risikoen for at det kan oppstå et press i retning av å bruke informasjonen til utenforliggende formål, for eksempel for å skaffe bevis mot tiltalte i en straffesak. Etter departementets vurdering foreligger det en risiko for formålsglidning. Det legges i den forbindelse vekt på at det for å motvirke slik risiko foreslås et *forbud mot deling av overskuddsinformasjon* og et *forbud mot bruk av informasjon fra tilrettelagt innhenting som bevis mot tiltalte i straffesaker.* I denne sammenhengen har også det generelle *forbudet mot å utføre oppgaver med politiformål* betydning. Til syvende og sist er det Stortinget som lovgiver sin egen risikobevissthet som vil redusere faren for formålsglidning.

Risikoen for at tiltaket vil ha en *nedkjølende effekt på ytrings- og informasjonsfriheten* har også vært en del av departementets vurdering. Departementet ser det som lite sannsynlig at tiltaket vil ha en slik effekt. Det vises til at tilrettelagt innhenting er et verktøy for utenlandsetterretning, samt til de strenge reglene som foreslås vedrørende formålsavgrensning, innhentings- og delingsforbud, behandling av overskuddsinformasjon og behandling av personopplysninger. I tillegg kommer det omfattende kontrollregimet som skal sikre etterlevelse av de nevnte begrensningene. På denne bakgrunn vurderer departementet at risikoen for nedkjølingseffekt er såpass liten at det ikke kan legges stor vekt på den.

Departementet har sett hen til at tiltaket vil innebære en viss byrde for tilbydere som omfattes av tilretteleggingsplikten. Byrden vurderes som lav, særlig siden det foreslås lovfestet at merutgifter knyttet til tilretteleggingsplikten skal dekkes av staten. Tilretteleggingsplikten vil heller ikke kreve at tilbyder setter av omfattende tekniske og andre ressurser. Departementet mener derfor at tilretteleggingsplikten ikke har vesentlig innvirkning på forholdsmessighetsvurderingen.

Etter denne brede interesseavveiningen har departementet kommet til at vilkåret om forholdsmessighet er oppfylt. Departementet har lagt avgjørende vekt på det sterke samfunnsmessige behovet som begrunner inngrepet, sammenholdt med summen av garantier mot misbruk og vilkårlighet.

Departementet har merket seg at EMD i enkelte saker som gjelder kriminalitetsbekjempelse og innenlandsetterretning har oppstilt et krav om *streng nødvendighet*, se for eksempel *Kennedy mot Storbritannia*.[223] Departementet vil ikke utelukke at det må oppstilles en høyere terskel også for et tiltak som foreslås i høringsnotatet her. For departementet er det imidlertid ikke nødvendig å ta endelig stilling til dette, idet tilrettelagt innhenting etter departementets syn uansett oppfyller et slikt strengere krav.

[223] *Kennedy mot Storbritannia* avsagt 18. mai 2019, avsnitt 153

11.8.2.5 Særlig om EMDs avgjørelse i Centrum for rättvisa mot Sverige 19. juni 2018

Sentrale momenter i avgjørelsen

EMD traff 19. juni 2018 en kammeravgjørelse i sak mot Sverige innklaget av organisasjonen *Centrum för Rättvisa*. Avgjørelsen er når dette skrives anket og således ikke rettskraftig, men den belyser mange sentrale spørsmål knyttet til bulkinnsamling av grenseoverskridende elektronisk kommunikasjon for utenlandsetterretningsformål. Departementet vil derfor redegjøre for avgjørelsen i det følgende.

Saken gjaldt spørsmålet om den svenske signaletterretningstjenesten (FRA) sin bulkinnsamling av data fra grenseoverskridende kommunikasjon i fiberoptiske kabler (såkalt *signalspaning*) for strategiske etterretningsformål innebar brudd på EMK artikkel 8. Det ble også anført brudd på retten til effektive rettsmidler i EMK artikkel 13.[224] EMD traff enstemmig avgjørelse om at den svenske ordningen verken innebærer brudd på EMK artikkel 8 eller artikkel 13.

Domstolen vurderer signalspaningen opp mot EMK og domstolens tidligere rettspraksis knyttet til særlig forståelsen av EMK artikkel 8. Avgjørelsen går ikke nærmere inn på EU-retten som ramme for bulkinnhenting for utenlandsetterretningsformål, og henviser til at EUs forordninger og direktiver ikke kommer til anvendelse for «State activities concerning public safety, defence and State security». Dette er nærmere drøftet under høringsnotatet punkt 11.8.3.

Domstolen tar utgangspunkt i det faktum at den vesentlige del av global kommunikasjon transporteres i fiberoptiske kabler («A great majority of the traffic relevant for signals intelligence is cable-based»), og anerkjenner at strategisk etterretning og bulkinnhenting er nødvendig i et demokratisk samfunn. Bulkinnsamling kan *potensielt* berøre alle brukere av telekomtjenester («potentially affects all users of, for example, mobile telephone services and the internet»). Domstolen knytter dette til statens rett (skjønnsmargin) til å treffe adekvate tiltak for å møte dagens trusselbilde, den teknologiske realitet, behovet for bulkinnsamling og nødvendigheten av å evne å finne de ukjente trusselaktørene (målsøking). Domstolen uttaler i avsnitt 112:

> «In *Weber and Saravia* and *Liberty and Others* the Court accepted that bulk interception regimes did not *per se* fall outside this margin. Given the reasoning of the Court in these judgments and in view of the current threats facing many Contracting States (including the scourge of global terrorism and other serious crime, such as drug trafficking, human trafficking, sexual exploitation of children and cybercrime), advancements in technology which have made it easier for terrorists and criminals to evade detection on the internet, and the unpredictability of the routes via which electronic communications are transmitted, the Court considers that the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security is one which continues to fall within States' margin of appreciation."

Domstolen anerkjenner behovet for å gjennomføre testanalyser og testinnhenting, herunder for utviklingsformål, og uttaler at disse aktivitetene «are essential for the proper functioning of the foreign intelligence».

[224] Den norske avdelingen av ICJ (*International Commission of Jurists*) intervenerte til støtte for klageren, basert på at norske borgeres kommunikasjon, også innenriks kommunikasjon, i stor grad krysser grensen til Sverige og dermed blir berørt av signalspaningen.

Domstolen anerkjenner videre behovet for lagring av rådata som omfatter betydelige mengder overskuddsinformasjon i avsnitt 146:

> «Although the FRA may maintain databases for raw material containing personal data for up to one year, it has to be kept in mind that raw material is unprocessed information. That is, it has yet to be subjected to manual treatment. The Court accepts that it is necessary for the FRA to store raw material before it can be manually processed. At the same time, the Court stresses the importance of deleting such data as soon as it is evident that it lacks pertinence for a signals intelligence mission."

Når det gjelder de generelle vilkår for å gjøre inngrep i borgernes rettigheter, henviser domstolen til de generelle prinsippene om lovkravet samt kravene om legitimt formål, forholdsmessighet og effektive rettsmidler, slik de blant annet er uttrykt i *Zakharov*, *Weber og Saravia,* samt *Liberty*, se nærmere i kapittel 4 om disse prinsippene. EMD viser også til at tidligere EMD-avgjørelser demonstrerer at statene har en relativt vid skjønnsmargin i å velge de virkemidler som anses best tilpasset det legitime formålet å beskytte sentrale nasjonale sikkerhetsinteresser. Domstolen peker samtidig på misbrukspotensialet ved myndighetenes tilgang til store datamengder. Avgjørelsen understreker derfor at statenes skjønnsmargin ikke kan sette til side viktige rettssikkerhetsprinsipper for å minimere risiko for misbruk (*minimum safeguards*) knyttet til implementeringen av slike systemer.[225]

Domstolen uttaler at den finner det «klart» at signalspaningslovgivningen i Sverige forfølger et legitimt formål, nærmere bestemt «in the interest of national security by supporting Swedish foreign, defence and security policy and identifying external threats to the country".

Domstolen vurderer den svenske lovgivning opp mot lovkravet etter menneskerettighetene, og bygger her på etablerte prinsipper om bl.a. tilgjengelighet og forutsigbarhet for borgerne og de kvalitative kravene til lovgivningen.[226] Den fremhever også som et viktig poeng at FRAs oppgavesett i loven er ytterligere utdypet i lovens forarbeider, som er en viktig rettskilde i svensk rett. Domstolen finner at den svenske lovgivningen tilfredsstiller lovkravet, selv om det på enkelte punkter foreligger et forbedringspotensial.

Domstolen er kritisk til at det i den svenske lovgivningen ikke fremgår uttrykkelig at innhenting må avsluttes dersom vilkårene for innhenting ikke lenger foreligger. Domstolen finner likevel ikke dette avgjørende fordi den særskilte utenlandsetterretningsdomstolen i Sverige avsier kjennelser som autoriserer søk og innhenting, og disse kjennelsene må fornyes etter en begrenset tid (6 måneder). Det anføres også at behovet for en klar regel om kansellering er større på straffebekjempelsesområdet enn for trusler rettet mot rikets sikkerhet. Domstolen vektlegger for øvrig at de personer i FRA som behandler personopplysninger som ledd i signalspaning, er sikkerhetsklarert og underlagt lovbestemt taushetsplikt, og at det er lovbestemmelser som angir når data skal slettes.

EMD erkjenner behovet for at forhåndsautorisasjon fra den svenske særdomstolen må behandles i hemmelighet og ikke for åpne dører. Dette kompenseres i noen grad av oppnevning av særskilt personvernombud for å ivareta interessene til de som berøres av

[225] Domstolen vektlegger i tråd med tidligere praksis seks minimumsvilkår som skal bidra til å forhindre myndighetsmisbruk. Minimumsvilkårene stiller krav om 1) en tilstrekkelig klar beskrivelse av hvilke forhold som kan begrunne innhenting, 2) en definering av hvilke personer eller grupper som kan bli gjenstand for innhenting, 3) at inngrepet er tidsbegrenset, 4) at det er gode prosedyrer og kontrollmekanismer for når data kan lagres, undersøkes eller brukes, 5) at det er klare regler for når data kan utleveres til andre, og 6) at det er regler for når data må slettes. Minimumsvilkårene er nærmere redegjort for i høringsnotatet punkt 4.2.5.

[226] Se note 232 og høringsnotatet punkt 4.2.5.2 for en nærmere beskrivelse av disse kravene.

inngrepet, og at anmodningene til særdomstolen i det minste må angi de kategorier av søketermer som skal ligge til grunn for søk i data. EMK anser domstolsgodkjenning for å være svært viktig («of crucial importance»). Samtidig er systemet med hurtigkompetanse tillagt FRA akseptabelt, kombinert med regelen om at bruken av slik kompetanse snarest mulig skal forelegges for særdomstolen.

Etter at data er innhentet av FRA, vurderer EMD at det ligger i selve formålet med kommunikasjonsetterretning at resultatet av innhentingen kan rapporteres til relevante nasjonale myndigheter, og at dette ikke strider mot relevante menneskerettighetsprinsipper. EMD uttaler videre at det samme gjelder overfor internasjonale partnere (domstolen uttaler i avsnitt 150 «it is evident that there must be a possibility of exchanging intelligence collected with international parters"). Domstolen mener imidlertid at svensk lovgivning ikke oppstiller tilstrekkelig spesifikke vilkår for *når* informasjon kan utleveres til tredjepart, og at dette ga grunn for noe bekymring («gives some cause for concern»). Samlet sett finner man imidlertid at de øvrige rettssikkerhetsgarantiene etter svensk rett balanserer denne svakheten.

Domstolen mener at signalspaningslovgivningens utgangspunkt om i ettertid å underrette personer om å ha blitt gjenstand for innhenting, ikke har noen praktisk betydning, fordi FRA i praksis alltid benytter seg av retten til å gjøre unntak fra utgangspunktet når sikkerhetsmessige hensyn tilsier det. Fordi *enhver* som mener seg uberettiget utsatt for innhenting kan klage til en kontrollmyndighet *uten* å måtte sannsynliggjøre at vedkommende *faktisk* har blitt utsatt for innhenting, finner domstolen likevel at systemet sett under ett tilfredsstiller kravet til effektive rettsmidler. Domstolen legger vekt på at selv om klagemyndighetens avgjørelser ikke er bindende for FRA, nyter klagemyndighetens syn i praksis stor respekt i Sverige og derfor som regel etterleves.

Samlet sett konkluderer EMD med at det svenske systemet ikke inneholder vesentlige rettslige mangler når det gjelder de rettslige rammene for signalspaning og hvorledes dette implementeres i praksis. Ordningen inkluderer adekvate og tilstrekkelige rettssikkerhetsgarantier mot misbruk. Lovgivningen møter kvalitetskravet i lovkravet, og inngrepet som signalspaning representerer er etter domstolens helhetsvurdering nødvendig og forholdsmessig i et demokratisk samfunn. Domstolen uttaler følgende i avsnitt 179:

> «The Court is mindful of the potential harmful effects that the operation of a signals intelligence scheme may have on the protection of privacy. Nevertheless, the Court acknowledges the importance for national security operations of a system such as the one examined in the present case. It notes, in this respect, the similar conclusions drawn by the Venice Commission [..]. Having regard to the present-day threats being posed by global terrorism and serious cross-border crime as well as the increased sophistication of communications technology, the decision to set up a bulk interception regime in order to identify such threats was one which fell within the respondent State's margin of appreciation. As noted above [..], in deciding on the type of regime neccessary, the margin afforded was a wide one."

Departementets vurdering av avgjørelsens betydning for tilrettelagt innhenting

Departementet vurderer at EMDs avgjørelse ytterligere styrker argumentasjonen om at departementets lovforslag tilfredsstiller de rettssikkerhetsgarantier som EMD vektlegger ved bulkinnhenting for utenlandsetterretningsformål, og at tilrettelagt innhenting ikke er i strid med sentrale menneskerettighetsprinsipper.

Likhetene mellom tilrettelagt innhenting og signalspaning er større enn forskjellene. Utenlandsetterretning, både i Sverige og Norge, kan ikke gjennomføres med det formål å

løse politiets eller andre rettshåndhevende myndigheters oppgaver. FRAs utenlandsrettede oppgaver går imidlertid i ett henseende noe lenger enn i Norge fordi lovgivningen også gir FRA i oppgave å innhente opplysninger om «other serious cross-border crimes that may threaten essential national interests». Dette kan etter omstendighetene gjelde narkotikatrafikk og menneskesmugling. Systemet i Sverige skiller seg også fra forslaget i lovutkastet her ved at det svenske sikkerhetspolitiet og enkelte andre deler av svensk politi kan gi detaljerte oppdrag («tasking directives») til FRA om innsamling. Risikoen for fremtidig formålsglidning vurderes derfor som enda mindre ved tilrettelagt innhenting.

Departementet viser videre til at domstolens kritiske merknader til den svenske lovgivningens mangel på lovregulering av vilkårene for utlevering av personopplysninger til nasjonale myndigheter og internasjonale partnere ikke vil gjelde lovforslaget her, jf. forslaget til spesifikke lovbestemmelser om dette i lovutkastets kapittel 10.

Departementet finner ellers at forslaget om tilrettelagt innhenting samlet sett ligger godt innenfor de krav som EMD har oppstilt i sin avgjørelse. Forslaget om tilrettelagt innhenting skiller seg på enkelte punkter fra ordningen i Sverige. Det gjelder for eksempel at domstolsgodkjenning etter forslaget om tilrettelagt innhenting foreslås lagt til de ordinære domstoler (med oppnevning av særskilt advokat for å ivareta interessene til den innhentingen retter seg mot), mens man i Sverige har valgt en særdomstolsløsning (med oppnevning av et personvernombud for å ivareta interessene til den innhentingen retter seg mot). I lovforslaget om tilrettelagt innhenting foreslås også, i motsats til svensk lovgivning, en uttrykkelig lovregel om at Etterretningstjenesten skal avslutte søk og innhenting dersom lovens vilkår ikke lenger foreligger.

Til tross for at kontrollordningene er noe ulike er det videre departementets vurdering at det norske samlede kontrollsystemet vil være vel så effektivt og inngående som det svenske. Det vises blant annet til at funksjonen om kontroll i tilnærmet sanntid, som foreslås implementert gjennom å styrke EOS-utvalgets kontroll, synes å gå lenger enn det svenske. Selv om det etter svensk lovgivning er flere myndigheter som har et delansvar for tilsyn og kontroll med FRA, står kontrollsystemet som foreslås for tilrettelagt innhenting – gjennom kombinasjonen av domstolens forhåndsgodkjenning, forvaltningstilsyn i linjen, Nkoms tilsyn med ekomindustriens tilrettelegging og en vesentlig styrket kontroll fra EOS-utvalget – på ingen måte i sin effekt tilbake for det svenske systemet. Departementet mener derfor at en eventuell fremtidig EMD-vurdering av EOS-utvalget vil tilfredsstille de formelle og reelle krav til uavhengighet, kontrollmetodikk, kompetanse og effektivitet. Departementet viser også til forslaget om å endre EOS-kontrolloven på enkelte punkter for å styrke EOS-utvalgets funksjoner som ledd i det samlede system av effektive rettsmidler i Norge.

11.8.2.6 Konklusjon

Departementet konkluderer på bakgrunn av drøftelsen med at tilrettelagt innhenting tilfredsstiller kravet til hjemmel i lov, forfølger et legitimt formål og er forholdsmessig. Departementet legger etter dette til grunn at forslaget i høringsnotatet ligger innenfor de menneskerettslige rammene som følger av Grunnloven § 102 første ledd første punktum, EMK artikkel 8 og SP artikkel 17 Heller ingen andre menneskerettslige krav vurderes å stå i veien for forslaget.

11.8.2.7 Sikringsplikten – i hvilken grad foreligger det en positivt forpliktelse til å ivareta sikkerheten i det digitale rom og sikre borgernes rettigheter mot ytre trusler?

Statens plikt til å respektere menneskerettighetene kan også implisere en forpliktelse til å tilrettelegge for at befolkningen får realisert sine rettigheter og friheter, eller til å beskytte borgere mot at tredjepersoner griper inn i disse.[227] Departementet har på denne bakgrunn vurdert om norske myndigheter kan være positivt forpliktet til å ivareta sikkerheten i det digitale rom og sikre borgernes rettigheter mot ytre trusler på adekvat måte.

Handlingsplikten følger ikke direkte av EMK eller EMKs forarbeider, men er basert på EMDs rettspraksis. Det kan imidlertid argumenteres for at sikringsplikten følger implisitt av EMK artikkel 1, hvor det fremkommer at statene «skal sikre enhver innen sitt myndighetsområde de rettigheter og friheter» som følger av rettighetskapittelet i konvensjonen. EMD har begrunnet mangel på oppfyllelse av positive forpliktelser som et grunnlag for konvensjonsbrudd med at dette er nødvendig for å gjøre konvensjonen effektiv.[228] Departementet vurderer at det ikke er en absolutt motsetning mellom Etterretningstjenestens behov for aksess til grenseoverskridende elektronisk kommunikasjon og ivaretakelsen av personverninteresser. Etter departementets syn kan det argumenteres for at den teknologiske utviklingen og økt fremmed aktivitet i det digitale rom utsetter både folks privatliv og vernet om kommunikasjon i transitt for risiko.

I punkt 4.2.2 vises det til at menneskerettighetskrenkelser mellom private i like stor grad kan skje over landegrenser. Nettverksoperasjoner og grenseoverskridende terrorisme utgjør potensielle trusler mot menneskers liv og helse, privatliv og kommunikasjonsvern. Departementet anser denne faren også som egnet til å skape en nedkjølende effekt på befolkningens vilje til å ytre seg både offentlig og privat og til å ta i bruk digitaliserte løsninger som tilbys av det offentlige.

I tråd med Høyesteretts avgjørelse i Rt. 2013 s. 588 mener departementet at det avgjørende i vurderingen av om tilrettelagt innhenting omfattes av sikringsplikten, er om truslene som materialiserer seg i eller gjennom det digitale rom utgjør en reell og umiddelbar risiko som myndighetene er kjent med eller burde vært kjent med, og om tilrettelagt innhenting kan bidra til reell beskyttelse mot slike trusler.

Etterretningstjenesten har i flere utgaver av den årlige åpne trusselvurderingen *Fokus* lagt frem at tjenesten har sikker kunnskap om at nettverksoperasjoner og terrorisme er reelle trusler som kan materialisere seg i Norge og mot norske borgere. Når sjefen for Etterretningstjenesten uttaler at vi ikke er i stand til å fange opp de mest avanserte digitale truslene mot Norge fordi Etterretningstjenesten ikke har de nødvendige tilganger og lovhjemler dette krever, er det et alvorlig budskap. Det digitale rom er en arena for spionasje, sabotasje og påvirkningsoperasjoner, og det er flere eksempler på at Norge har blitt utsatt for denne typen operasjoner. Datainnbruddet rettet mot Helse Sør-Øst er et nærliggende eksempel her. I andre land har det digitale rom blitt brukt til å utføre handlinger med vesentlig skadepotensiale, slik som for eksempel strømbruddet i Ukraina vinteren 2015 og innsettingen av skadevaren Stuxnet mot det iranske atomprogrammet i 2010. Det digitale

[227] Se for eksempel *Marckx mot Belgia* avsagt 13. juni 1979, *Osman mot UK* avsagt 28. oktober 1998 og *Von Hannover mot Tyskland* avsagt 24. juni 2004. Se generelt om statens plikt til å ivareta statens suverenitet og borgernes sikkerhet i punkt 4.2.2.

[228] Harris, O'Boyle & Warbrick, *Law of the European Convention on Human Rights*, Oxford University Press, tredje utgave s. 22.

rom er også en arena for fri kommunikasjon mellom aktører som opererer i eller for utenlandske terrorceller. Kunnskap om disse cellene og evne til å følge dem og iverksette tiltak ved eventuell terrorplanlegging, er naturlig nok avgjørende for å forhindre anslag. Departementet kan ikke utelukke at truslene som kan materialisere seg i eller gjennom det digitale rom vil kunne utgjøre en reell og umiddelbar risiko for borgernes liv og helse dersom de ikke avverges rettidig. Spørsmålet er hvorvidt kunnskap om disse truslene pålegger myndighetene en plikt til å innføre adekvate tiltak for å beskytte borgerne mot dem.

I tillegg mener departementet at manglende evne til å kontrollere mistenkelig aktivitet i det digitale rom kan gjøre nettverksinfrastruktur i Norge sårbare for fremmede aktørers virksomhet. Det kan ikke utelukkes at slike aktører evner å spionere på eller innhente informasjon om personer eller virksomheter i Norge og således trenge inn i deres personlige sfære. Det kan heller ikke utelukkes at slike aktører kan innhente, manipulere eller på annen måte forfalske kommunikasjon mellom private eller mellom det offentlige og private. Dette kan tenkes å få utilsiktede konsekvenser for konfidensialiteten til kommunikasjon som krysser norske landegrenser, herunder en uvilje mot å benytte nettverksinfrastruktur i Norge.

Det neste spørsmålet er om tilrettelagt innhenting kan forventes å bidra til å beskytte befolkningen mot truslene som nevnt over. Det vises her til punkt 11.6, hvor det redegjøres for behovet. I Norge er Etterretningstjenesten, PST og NSM sentrale aktører med oppgaver knyttet til ivaretakelsen av rikets sikkerhet. Av disse er det Etterretningstjenesten som har som sitt samfunnsoppdrag å kartlegge trusler med utenlandsk opprinnelse og bistå rette myndigheter med etterretninger om slike trusler. Uten tilgang på grenseoverskridende elektronisk kommunikasjon vil Etterretningstjenesten ikke være i stand til å avdekke nettverksoperasjoner eller å bidra til arbeidet mot grenseoverskridende terrorisme der aktørene kommuniserer over nettet. I denne sammenheng er det illustrerende at mer enn 50 % av britisk etterretning knyttet til kontraterror[229] og 95 % knyttet til avdekking av nettverksoperasjoner[230] er basert på analyse av data innsamlet i bulk.

Omfanget og rekkevidden av sikringspliktens innhold baserer seg i stor grad på skjønn, og departementet tar ikke direkte stilling til om det kan utledes en konkret positiv plikt her. Departementet har merket seg at Henning Harborg og Hans Petter Graver, i en utredning om datalagring for kriminalitetsbekjempelsesformål, konkluderer med at en plikt til slik datalagring ikke kan utledes av sikringsplikten.[231] Departementet mener uansett at det er problematisk dersom myndighetene er kjent med sårbarheter som gjør landets borgere, virksomheter og demokratiske institusjoner utsatt for ondsinnede handlinger fra fremmede aktører, uten at man innfører tiltak for å motvirke dette. Som det fremkommer av drøftelsene over, mener departementet at tilgang til grenseoverskridende elektronisk informasjon er egnet til å bidra til reell beskyttelse mot trusler som kan materialisere seg i eller gjennom det digitale rom. Departementet mener at dette kan tale for at tilrettelagt innhenting ikke bare bør innføres for å dekke myndighetenes behov for informasjon, men også for å sikre effektiv beskyttelse av den norske befolkningens menneskerettigheter.

---

[229] David Anderson Q.C: *A Question of Trust – Report of the Investigatory Powers* Review (juni 2015), s. 122. Se også Siri Strand, *The Power of Bulk Interception: an analysis of digital communications interception and its strategic aspects*, King's College London 2017, s. 23.

[230] David Anderson Q.C: *A Question of Trust – Report of the Investigatory Powers* Review (juni 2015), side 81 og 154.

[231] Se utredningen Datalagring og menneskerettighetene (2015) punkt 7.5 s. 68 til 71.

11.8.2.8 Øvrige folkerettsforpliktelser

Norge har en folkerettslig plikt til å unngå at norsk territorium brukes som transittland for fremmede aktørers operasjoner i det digitale rom. Dette kalles gjerne det sedvanerettslige *due diligence* prinsippet. Manglende tilgang til grenseoverskridende elektronisk kommunikasjon gjør at norske dataservere er sårbare for slik aktivitet.

Norge er videre forpliktet, gjennom en rekke konvensjoner og bindende resolusjoner fra FNs sikkerhetsråd til å bekjempe internasjonal terrorisme. Det foreligger også internasjonale normer og sanksjonsregimer som Norge er forpliktet til å etterleve når det gjelder å hindre spredning av masseødeleggelsesmidler og komponenter til bruk for slike.

11.8.3 Norges EØS-rettslige forpliktelser

11.8.3.1 Rettslige utgangspunkter

Tiltak innen nasjonal sikkerhet, slik som utenlandsetterretning, omfattes ikke av EØS-avtalens saklige virkeområde. EØS-relevant EU-regelverk kan etter omstendighetene ha betydning for slike tiltak, men det klare utgangspunktet er at tiltak innen nasjonal sikkerhet ikke omfattes av EU-retten. Dette følger av traktaten om den europeiske union (TEU) artikkel 4 nr. 1, som fastslår at nasjonal sikkerhet forblir den enkelte medlemsstats eneansvar.

EUs pakt (charter) om grunnleggende rettigheter beskytter blant annet retten til respekt for privatlivet, retten til beskyttelse av personopplysninger og ytringsfriheten. Pakten er etter TEU artikkel 6 nr. 1 bindende for EUs medlemsland. Den er derimot ikke gjort til en del av EØS-avtalen, og dermed ikke bindende for Norge. Pakten kan likevel ha betydning for tolkningen av EU-regelverk som er innlemmet i EØS-avtalen, og som i tråd med homogenitetsmålsettingen skal tolkes og anvendes likt i Norge og i EU. Pakten kan også indirekte få betydning ved at den påvirker tolkningen av menneskerettighetene i Grunnloven og EMK. Flere av bestemmelsene i pakten har paralleller i Grunnloven og EMK, slik som retten til respekt for privatlivet og ytringsfriheten. Pakten har også bestemmelser uten paralleller i Grunnloven og EMK, slik som retten til beskyttelse av personopplysninger.

Kommunikasjonsverndirektivet[232] er EØS-relevant og gjennomført i norsk rett i ekomloven.[233] Det følger av direktivet artikkel 5 nr. 1 at medlemsstatene plikter å sikre konfidensialitet for kommunikasjon og tilhørende trafikkdata. Medlemsstatene skal særlig forby avlytting, lagring og andre former for overvåkning uten brukernes samtykke, med mindre det er tillatt etter lov i samsvar med artikkel 15 nr. 1. Etter artikkel 15 nr. 1 kan medlemsstatene på nærmere vilkår treffe tiltak som griper inn i rettigheter og plikter etter direktivet, blant annet ut fra hensyn til nasjonal sikkerhet. Samtidig følger det av artikkel 1 nr. 3 at direktivet ikke kommer til anvendelse for tiltak innen nasjonal sikkerhet.

[232] Europaparlaments- og rådsdirektiv 2002/58/EF om behandling av personopplysninger og beskyttelse av privatlivets fred innen området for elektronisk kommunikasjon

[233] EU-kommisjonen har foreslått en ny kommunikasjonsvernforordning til erstatning for direktivet. Forslaget har som mål å harmonisere personvernbeskyttelsen på ekom-området med personvernforordningens regler. Det følger av personvernforordningen artikkel 2 nr. 2 bokstav a at forordningen ikke får anvendelse på behandling av opplysninger som utføres i forbindelse med utøvelse av en aktivitet som ikke omfattes av unionsretten.

Personvernforordningen trådte i kraft i EU 25. mai 2018.[234] Den ble folkerettslig bindende for Norge ved EØS-komiteens beslutning.[235] Forordningen er gjennomført i norsk rett ved personopplysningsloven. Det følger av personopplysningsloven § 1 at forordningen, slik den er inntatt i EØS-avtalen og med de tilpasninger som følger av EØS-komiteens beslutning om innlemmelse og EØS-avtalen for øvrig, gjelder som norsk lov. Loven og forordningen gjelder i utgangspunktet både innenfor og utenfor EØS-avtalens virkeområde, jf. personopplysningsloven § 2 første ledd første punktum, som går foran unntakene i forordningen artikkel 2 nr. 2. Det følger imidlertid av personopplysningsloven § 2 første ledd annet punktum at loven og forordningen ikke gjelder når annet er bestemt i eller med hjemmel i lov. Det åpnes dermed for at det kan gjøres unntak i særlovgivningen innenfor rammen av unntakene i forordningen artikkel 2 nr. 2. I tråd med dette foreslås det i høringsnotatet her at personopplysningsloven ikke skal gjelde for behandling av personopplysninger for etterretningsformål, se lovutkastet § 9-1 første ledd og punkt 12.3. Dette unntaket er i tråd med unntaket i forordningen artikkel 2 nr. 2 bokstav a. og i tråd med omtalen i forarbeidene til personopplysningsloven, knyttet til personopplysningslovens overgangsbestemmelser.[236]

Ved lov 15. april 2011 nr. 11 vedtok Stortinget lovendringer for å gjennomføre EUs datalagringsdirektiv[237] i norsk rett. Hensikten med datalagringsdirektivet var å gi justismyndighetene et verktøy for å avdekke, etterforske og straffeforfølge alvorlig kriminalitet. Direktivet regulerte ikke datalagring i forbindelse med utenlandsetterretningsvirksomhet. Blant annet som følge av at direktivet ble kjent ugyldig av EU-domstolen i Digital Rights-dommen, har loven aldri trådt i kraft.[238] Justis- og beredskapsdepartementet har på bakgrunn av et anmodningsvedtak fra Stortinget igangsatt et arbeid med å utrede generell lagringsplikt for IP-adresser som et virkemiddel i kampen mot kriminalitet.[239]

11.8.3.2 Særlig om EU-domstolens dom i de forente sakene C-203/15 og C-698/15 (Tele2-dommen)

EU-domstolens storkammer avsa 21. desember 2016 – mens Lysne II-utvalgets rapport var på høring – dom i de forente sakene C-203/15 Tele2 Sverige AB mot Post- och telestyrelsen og C-698/15 Secretary of State for the Home Department mot Tom Watson, Peter Brice og Geoffrey Lewis. Flere høringsinstanser har i sine høringssvar tatt til orde for at dommen står i veien for Lysne II-utvalgets forslag, eller i det minste at forslaget må vurderes nærmere i lys av dommen. Departementet har derfor funnet grunn til å vurdere betydningen av dommen særskilt.

---

[234] Regulation (EU) 2016/679

[235] EØS-komiteens beslutning nr. 154/2018 av 6. juli 2018 om endring av EØS-avtalens vedlegg XI (Elektronisk kommunikasjon, audiovisuelle tjenester og informasjonssamfunnstjenester) og protokoll 37 om listen omhandlet i artikkel 101.

[236] Prop. 56 LS (2017–2018) s. 222

[237] Europaparlaments og rådsdirektiv 2006/24/EF av 15. mars 2006 om lagring av data fremkommet ved bruk av elektronisk kommunikasjon med endring av direktiv 2002/58/EF

[238] Se EU-domstolens storkammers dom 8. april 2014 i de forente sakene C-293/12 og C-594/12.

[239] Se Prop. 1 S (2017–2018) for Justis- og beredskapsdepartementet punkt 10 s. 359

Bakgrunnen for sak C-203/15 (Tele2) var EU-domstolens dom i sakene C-293/12 og C-594/12 (Digital Rights), hvor EU-domstolen fastslo at datalagringsdirektivet var ugyldig. Dagen etter at Digital Rights-dommen var avsagt, informerte Tele2 den svenske Post och-telestyrelsen om at Tele2 ikke lenger ville lagre trafikkdata i tråd med den svenske lovgivningen som gjennomførte direktivet. Etter at en utreder oppnevnt for å vurdere lovgivningen i lys av avgjørelsen i Digital Rights-dommen konkluderte med at den ikke var i strid med EU-retten eller EMK, fattet Post och- telestyrelsen vedtak som påla Tele2 å gjenoppta datalagringen. Tele2 anla på denne bakgrunn sak for domstolene. Det ble besluttet å forelegge for EU-domstolen spørsmål om hvorvidt en generell og unntaksløs plikt til å lagre trafikkdata med sikte på kriminalitetsbekjempelse var i tråd med EU-retten. Hvis spørsmålet ble besvart negativt, ble det stilt spørsmål om hvorvidt lagring under visse forutsetninger likevel kunne være lovlig.

Sak C-698/15 (Watson), som ble forent til behandling med Tele2-saken, hadde bakgrunn i tre søksmål om lovligheten av britisk datalagringslovgivning i kjølvannet av Digital Rights-dommen. Det ble besluttet å forelegge for EU-domstolen spørsmål om hvorvidt Digital Rights-dommen oppstilte tvingende EU-rettslige krav til en medlemsstats nasjonale bestemmelser om tilgang til opplysninger lagret i samsvar med nasjonal lovgivning. Det ble også stilt spørsmål om hvorvidt Digital Rights-dommen ga EU-pakten artiklene 7 og/eller 8 et videre anvendelsesområde enn anvendelsesområdet til EMK artikkel 8 slik det følger av praksis fra EMD.

EU-domstolen drøftet først hvorvidt nasjonal lovgivning som den svenske var omfattet av kommunikasjonsverndirektivet. Spørsmålet oppsto fordi det følger av artikkel 1 nr. 3 at direktivet ikke gjelder statens aktiviteter på det strafferettslige området. Domstolen kom likevel til at direktivet kom til anvendelse, under henvisning til at artikkel 15 nr. 1 ellers ville bli fratatt sin virkning.[240]

Domstolen kom videre til at artikkel 15 nr. 1 måtte tolkes strengt[241] og i lys av de fundamentale rettighetene i EU-pakten.[242] Det fulgte av pakten, direktivet og rettspraksis at et inngrep i rettighetene måtte være forholdsmessig.[243]

I forholdsmessighetsvurderingen tok EU-domstolen utgangspunkt i at den svenske lovgivningen åpnet for generell og udifferensiert lagring av samtlige trafikk- og lokaliseringsdata om alle abonnenter og registrerte brukere i forbindelse med alle elektroniske kommunikasjonsmidler, og at den uten unntak påla tilbydere av elektroniske kommunikasjonstjenester å lagre disse dataene systematisk og uavbrutt.[244] Dette måtte regnes som et meget vidtrekkende og særlig alvorlig inngrep i rettighetene etter EU-pakten artiklene 7 og 8.[245] Generell og udifferensiert lagring av samtlige trafikk- og lokaliseringsdata kunne ikke rettferdiggjøres av formålet om bekjempelse av alvorlig kriminalitet.[246]

---

[240] Se EU-domstolens storkammers dom 8. april 2014 C-293/12 og C-698/15, avsnitt 73

[241] Ibid avsnitt 89

[242] Ibid avsnitt 91

[243] Ibid avsnitt 94 til 96

[244] Ibid avsnitt 97

[245] Ibid avsnitt 100

[246] Ibid avsnitt 103

Domstolen konkluderte med at den svenske lovgivningen gikk utenfor rammen av hva som var strengt nødvendig, og ikke kunne rettferdiggjøres i et demokratisk samfunn, slik direktivet artikkel 15 nr. 1, lest i lys av EU-pakten artiklene 7, 8 og 11 samt 52 nr. 1, krever.[247] Direktivet var derfor til hinder for slik nasjonal lovgivning.[248]

Domstolen drøftet deretter det andre spørsmålet i sak C-203/15 og det første spørsmålet i sak C-698/15, som etter domstolens syn i sin essens dreide seg om hvorvidt direktivet artikkel 15 nr. 1, lest i lys av EU-pakten artiklene 7, 8 og 52 nr. 1, måtte tolkes som å være til hinder for nasjonal lovgivning som regulerer beskyttelsen av og sikkerheten til trafikkdata og lokaliseringsdata, og spesielt kompetente nasjonale myndigheters adgang til lagrede data, uten at lovgivningen begrenser adgangen til formålet om bekjempelse av grov kriminalitet, uten å undergi adgangen forutgående kontroll av en domstol eller uavhengig forvaltningsmyndighet og uten å stille krav om at dataene lagres innen EU. Dette spørsmålet ble besvart bekreftende.[249]

Avslutningsvis drøftet domstolen hvorvidt den i Digital Rights-dommen oppstilte et vern som går lenger enn det som følger av EMK. Domstolen tok ikke stilling til spørsmålet, men pekte på at EU-pakten artikkel 52 ikke er til hinder for å oppstille et vern som går lenger enn EMK, samt at EU-pakten artikkel 8 er distinkt fra EU-pakten artikkel 7 og ikke har noe motsvar i EMK.[250]

Departementet tar som utgangspunkt at aktiviteter som gjelder offentlig sikkerhet, forsvar og statssikkerhet ifølge kommunikasjonsverndirektivet artikkel 1 nr. 3 faller utenfor direktivets anvendelsesområde. For så vidt gjelder aktiviteter innenfor strafferetten er det bare statens aktiviteter som faller utenfor virkeområdet, det vil si at ikke-anvendelsen av direktivet kan sies å være mindre absolutt på strafferettens område. At kommunikasjonsverndirektivet ikke kommer til anvendelse for tiltak innen nasjonal sikkerhet, har støtte i direktivets forhistorie, forarbeider og fortale. Departementet viser for så vidt til Norges innlegg til EU-domstolen i sak C-623/17 (Privacy International), som gjennomgår rettskilder knyttet til dette spørsmålet.

Den svenske lovgivningen som var tema i Tele2-dommen åpnet for at politiet kunne hente inn opplysninger i saker som gjaldt lovbrudd som kunne straffes med fengsel i mer enn to år. Loven åpnet også for slik tilgang i saker om enkelte lovbrudd med enda lavere strafferamme. Den britiske lovgivningen åpnet for å pålegge lagringsplikt blant annet av hensyn til nasjonal sikkerhet, men også for å forebygge eller avdekke kriminalitet, og uten noen begrensning til alvorlig kriminalitet. Selv om domstolen nevner nasjonale sikkerhetsinteresser med hensyn til terrorisme i dommens avsnitt 119, er det etter departementets syn klart at temaet for dommen var nasjonal lovgivning om datalagring med sikte på å bekjempe kriminalitet, ikke med sikte på å beskytte nasjonal sikkerhet.

Etterretningstjenesten har ikke kriminalitetsbekjempelse som formål. Tjenesten kan riktig nok sies å bidra til kriminalitetsbekjempelse i den forstand at den skal bidra til å motvirke enkelte handlinger som retter seg mot Norges sikkerhet og som dessuten er straffbare, slik som terrorhandlinger som stammer fra utlandet. Det er likevel en prinsipiell forskjell at *formålet*

[247] Ibid avsnitt 107

[248] Ibid avsnitt 112

[249] EU-domstolens storkammers dom 8. april 2014 C-293/12 og C-698/15 avsnitt 113 til 125

[250] Ibid avsnitt 126 til 133

med virksomheten er å verne rikets sikkerhet mot utenlandske trusler, ikke å oppklare, etterforske og straffeforfølge kriminalitet.

Det er heller ingen tvil om at forslaget om tilrettelagt innhenting i høringsnotatet her har beskyttelse av nasjonal sikkerhet som formål, ikke kriminalitetsbekjempelse. At forslaget også kan ha som virkning å bidra til å motvirke bestemte former for kriminalitet, rokker ikke ved dette. Departementet viser i den sammenheng dessuten til at det foreslås å oppstille et forbud mot å bruke informasjon som stammer fra tilrettelagt innhenting som grunnlag for ileggelse av straff eller andre strafferettslige reaksjoner, se punkt 11.13.3. Dette forslaget understreker tiltakets karakter av beskyttelse av nasjonal sikkerhet, i motsetning til kriminalitetsbekjempelse.

Departementet mener på denne bakgrunn at Tele2-dommen ikke står i veien for nasjonal lovgivning som åpner for tilrettelagt innhenting av grensekryssende elektronisk kommunikasjon for utenlandsetterretningsformål. Departementet finner det derfor ikke nødvendig å drøfte lovforslaget opp mot kriteriene som EU-domstolen oppstilte for at et tiltak skulle være i samsvar med kommunikasjonsverndirektivet. Departementet presiserer at kriteriene ble utviklet med hensyn til tiltak med kriminalitetsbekjempelse som formål, og slik kriteriene er utformet er de på ingen måte egnet for å regulere utenlandsetterretning.

Det er viktig å understreke at departementets syn ikke innebærer at individet står uten rettslig beskyttelse mot tiltak som faller utenfor direktivets virkeområde. For Norges del er det særlig Grunnloven og EMK som setter skranker og oppstiller rettssikkerhetsgarantier med hensyn til slike tiltak.

Departementet tilføyer at en ikke er kjent med at noe land med lovgivning som tillater innhenting av grenseoverskridende elektronisk kommunikasjon for utenlandsetterretningsformål, har gitt uttrykk for at Tele2-dommen står i veien for dette.

Det bemerkes til slutt at EU-domstolen for tiden har til behandling den nevnte sak C-623/17 (Privacy International), som synes å være mer relevant for forslaget i høringsnotatet her enn Tele2-dommen. Departementet vil følge utviklingen i denne saken nøye, på samme måte som sakene er til behandling i EMD.

11.8.4 Europarådets personvernkonvensjon

Norge har ratifisert Europarådets konvensjon om personvern i forbindelse med elektronisk databehandling av personopplysninger.[251] Formålet med konvensjonen er å sikre respekten for individets rettigheter og grunnleggende friheter, særlig retten til privatliv, med hensyn til elektronisk databehandling av personopplysninger.

Konvensjonen stiller i artikkel 5 krav til datakvalitet:

> «Personopplysninger som bearbeides ved elektronisk saksbehandling skal:
>
> a) innsamles og bearbeides på rettferdig og lovlig vis;
>
> b) lagres for bestemte og lovlige formål og ikke nyttes på en måte som er uforenlig med disse formål;
>
> c) være adekvate, relevante og ikke for omfattende i relasjon til de formål de lagres til;

[251] Europarådets konvensjon nr. 108 av 28. januar 1981 om personvern i forbindelse med elektronisk databehandling av personopplysninger

d) være nøyaktige og, der det er nødvendig, holdt a jour;

e) oppbevares på en måte som ikke gir anledning til å identifisere datasubjektene lenger enn nødvendig for det formål som disse opplysningene lagres til.»

Konvensjonens artikkel 6 oppstiller et særskilt vern for særlig sensitive personopplysninger:

«Personopplysninger som åpenbarer rasemessig opprinnelse, politiske oppfatninger samt religiøs eller annen tro, så vel som personopplysninger vedrørende helse eller seksualliv, kan ikke behandles elektronisk med mindre intern lovgivning gir tilstrekkelig vern. Det samme skal gjelde for personopplysninger som gjelder domfellelser for straffbare handlinger.»

Konvensjonens artikkel 8 oppstiller regler om tilleggsvern for datasubjektene:

«Enhver person skal ha rett til:

a) å bringe på det rene om det eksisterer et elektronisk persondataregister, dets hovedformål, så vel som den ansvarlige registerførers identitet og faste bopel eller hovedkontor.

b) med rimelige mellomrom og uten ugrunnet opphold eller urimelige utgifter å få bekreftet hvorvidt personopplysninger vedrørende ham selv er lagret i det elektroniske persondataregister og å få seg meddelt disse opplysninger i en forståelig form;

c) å få korrigert eller slettet, alt etter omstendighetene, slike opplysninger dersom disse er blitt behandlet i strid med de bestemmelser i intern lovgivning som gjennomfører hovedprinsippene fastsatt i denne konvensjons artikler 5 og 6;

d) å klage eller på annen måte bringe saken videre dersom en anmodning om bekreftelse eller, alt etter omstendighetene, meddelelse, korrigering eller sletting som nevnt i denne artikkels punkter b) og c), ikke etterkommes.»

Det følger av artikkel 9 nr. 2 at avvik fra artiklene 5, 6 og 8 skal være tillatt når slikt avvik følger av lov og er et nødvendig tiltak i et demokratisk samfunn av hensyn til blant annet beskyttelse av statens sikkerhet og offentlig sikkerhet. Vurderingstemaet er i hovedtrekk sammenfallende med vurderingstemaene som gjelder lovligheten av inngrep i rettighetene etter Grunnloven § 102 første ledd første punktum og EMK artikkel 8. Departementet legger på denne bakgrunn til grunn at tiltak som tilfredsstiller kravene som følger av Grunnloven og EMK, heller ikke vil være i strid med konvensjonen. Forslagets forhold til konvensjonen vurderes derfor ikke særskilt i høringsnotatet.

11.8.5 Konklusjon

Departementet konkluderer på bakgrunn av drøftelsene ovenfor med at det ikke vil være i strid med menneskerettighetene, Norges EØS-rettslige forpliktelser eller andre folkerettslige forpliktelser å vedta lovgivning som gir Etterretningstjenesten tilgang til tilrettelagt grenseoverskridende elektronisk kommunikasjon for utenlandsetterretningsformål.

11.9 Hvilke vilkår stilles til innhentingen?

11.9.1 Krav til utformingen av regelverket. Skjønnsmargin og rettssikkerhetsgarantier

Statens skjønnsmargin for regulering av inngrep i borgernes rettigheter av hensyn til rikets sikkerhet diskuteres i punkt 4.2.5. I sin praksis har EMD lagt til grunn at statene har en nokså vid skjønnsmargin når de skal foreta interesseavveiningen mellom retten til et privatliv

og hensynet til å beskytte nasjonal sikkerhet mot ytre trusler.[252] Samtidig understreker domstolen at dette ikke betyr at statene har en ubegrenset diskresjonær myndighet til å gjøre personer innenfor sin jurisdiksjon til gjenstand for skjulte metoder, og at interesseavveiningen vil avhenge av en konkret vurdering av alle sakens omstendigheter.

Det følger av legalitetsprinsippet i Grunnloven § 113 og lovkravet i EMK artikkel 8 nr. 2 at Etterretningstjenestens innhenting av opplysninger som kan innebære inngrep i noens privatliv må ha forankring i lov. Det redegjøres for det generelle innholdet i lovkravet i punkt 4.2.5.2. EMDs praksis viser at det stilles strengere krav til lovens klarhet og presisjon der det er tale om større inngrep. Hovedelementene i regelverket må komme til uttrykk i formell lov, som eventuelt suppleres av bestemmelser gitt i medhold av lov. Departementet mener at prosessuelle så vel som personelle og materielle regler knyttet til tilrettelagt innhenting bør lovfestes. Gitt innhentingens særskilte karakter har departementet funnet det hensiktsmessig å samle reguleringen av denne formen for midtpunktinnhenting i et eget kapittel i loven.

Det må fastsettes bestemmelser som regulerer hvordan Etterretningstjenesten skal behandle, oppbevare og slette informasjon som den får tilgang til. Departementet vurderer at de samme hensyn gjør seg gjeldende for behandling av informasjon innhentet etter reglene for tilrettelagt innhenting som for annen informasjonsinnhenting. Følgelig mener departementet at det ikke er påkrevd med egne regler for behandling av personopplysninger innhentet etter særreglene om tilrettelagt innhenting, men legger til grunn at bestemmelsene i lovforslaget kapittel 9 kommer til anvendelse. Kapittelet oppstiller skjerpede krav til behandling av bestemte kategorier informasjon, se forslag til diskrimineringsforbud i § 9-4 og krav om streng nødvendighet for behandling av opplysninger som er betrodd særlige yrkesutøvere i deres stilling i utkast til § 9-6. De øvrige alminnelige forbudene i lovforslaget vil også gjelde tilrettelagt innhenting, slik som § 1-3, og kapittel 4.

Departementet mener at tilgang til tilrettelagt elektronisk kommunikasjon som passerer den norske landegrensen forutsetter at det fastsettes strenge rettssikkerhetsgarantier som skal sikre at tilgangen til informasjon blir så spisset som mulig, at lovens krav følges og at potensialet for myndighetsmisbruk reduseres i det ytterste. For å sikre dette må systemets omfang reduseres til det strengt nødvendige, kontrollregimet må være strengt og kun personer som er nøye autorisert og klarert kan settes til å operere systemet. Departementet vil i det følgende gjøre rede for de rettssikkerhetsgarantier i form av begrensninger og kontrolltiltak som anses nødvendig.

11.10 Kontroll av Etterretningstjenestens bruk av tilrettelagt innhenting

11.10.1 Innledning

En forutsetning for Lysne II-utvalgets anbefaling om å gi Etterretningstjenesten tilgang til grenseoverskridende elektronisk kommunikasjon var at tjenestens bruk av systemet ble

[252] NOU 2015: 13 *Digital sårbarhet – sikkert samfunn* s. 79; *Weber og Saravia mot Tyskland* avsagt 29. juni 2006, avsnitt 106. I *Centrum for rättvisa mot Sverige* avsagt 19. juni 2018 (ikke rettskraftig) og *Big Brother Watch mfl. mot Storbritannia* avsagt 13. september 2018 (ikke rettskraftig) uttaler EMD at det faller innenfor statenes skjønnsmargin å avgjøre om man ønsker å innføre et slikt bulkinnsamlingsregime, se blant annet punkt 11.8.2.5.

underlagt uavhengig og effektiv kontroll. Utvalget skisserte et mulig kontrollregime bestående av tre hovedelementer: forhåndsgodkjenning utført av en DGF-domstol, løpende kontroll utført av et DGF-tilsyn og etterhåndskontroll utført av EOS-utvalget.[253]

Departementet foreslår en ordning som i sin kjerne er lik Lysne II-utvalgets anbefaling. De samme hensyn som Lysne II-utvalget la til grunn for sin anbefaling gjør seg gjeldende for tilrettelagt innhenting, herunder hensynet til Etterretningstjenestens tillit og legitimitet, kontrollmekanismenes uavhengighet til Etterretningstjenesten og rettssikkerhet og effektivt personvern for den enkelte. Departementet er langt på vei enig i de vurderinger utvalget har gjort om hvordan disse hensynene bør ivaretas.

Et overordnet formål er å ivareta hensynet til personvernet. Personvernet sikres i stor grad av de menneskerettslige krav i Grunnloven og EMK. Imidlertid er det grunn til å vurdere om tilrettelagt innhenting bør underlegges kontrollmekanismer utover de som staten er forpliktet til å innføre, særlig av hensyn til befolkningens tillit til at systemet ikke misbrukes. Departementet støtter seg her til Lysne II-utvalgets uttalelse på side 52 i rapporten, hvor det står:

> «Utvalget har gjennom sitt arbeid fått forståelse for at DGF vil være nødvendig for at E-tjenesten fortsatt skal ivareta sitt samfunnsoppdrag. DGF kan utformes på mange måter, både teknisk og juridisk. Utvalget anser samtidig at DGF i sin natur vil være sterkt personverninngripende og at et demokratisk samfunn som Norge må vektlegge en eventuell innføring på en måte som gjør at grunnleggende hensyn som at befolkningens tillit til myndighetene ikke svekkes, og at det i minst mulig grad oppstår noen nedkjølingseffekt på den offentlige debatt og informasjonssøken. […]
>
> Utvalget vurderer altså at en rekke tiltak og vilkår bør være på plass, dersom DGF skal iverksettes. Det er avgjørende at tiltakene samlet sett er troverdige, og at ordningene på en betryggende måte ivaretar både hensynet til E-tjenestens oppgaveløsning og hensynet til personvern og kommunikasjonsvern. Det er kun på den måten at folk flest kan ha tillit til at DGF ikke vil innebære at E-tjenesten, verken lovlig eller ulovlig (ved misbruk), vil lese SMS 'ene, e-postene eller facebookmeldingene deres eller hvilke nettsider de surfer på. Risiko for misbruk må innen rimelighetens grenser reduseres til det usannsynlige.
>
> Fire sentrale prinsipper som utvalget legger til grunn i denne sammenheng, er formålsavgrensning, minimalisering, autorisasjon og kontroll. *Formsålsavgrensning* innebærer at data samlet inn for ett formål skal ikke kunne anvendes for et helt annet formål. *Minimalisering* innebærer å samle inn tilstrekkelige og nødvendige data for det formål eller den oppgave som foreligger, og samtidig unnta, begrense tilgang til eller sortere bort eventuell ikke-relevant eller overskytende informasjon. *Autorisasjon* innebærer i denne sammenheng at bruk av inngripende metoder krever prøving og forhåndsgodkjenning fra (uavhengig) kompetent myndighet. *Kontroll* innebærer uavhengige og effektive mekanismer som etterprøver om de begrensninger som følger av de øvrige tre prinsippene etterleves i praksis. Kontroll kan skje samtidig eller etterfølgende, eller begge deler.»

Departementet er langt på vei enig i at de grunnleggende prinsippene om formålsavgrensning, minimalisering, autorisasjon og kontroll bør være retningsgivende for hvilke begrensende tiltak som bør integreres. Videre vil departementet understreke at de ulike kontrollelementene som foreslås spesielt for tilrettelagt innhenting må ses i

[253] Se Lysne II-utvalgets rapport om digitalt grenseforsvar av 26. august 2016, s. 52 og 57-60

sammenheng med Etterretningstjenestens internkontroll, forvaltningskontrollen i regi av departementet og den uavhengige etterfølgende kontrollen i regi av EOS-utvalget.

Lysne II-utvalget trekker også frem i sin rapport på side 57 det forhold at kontrollmekanismene

> «i noen grad vil redusere overordnede myndigheters mulighet til å styre og innrette E-tjenestens innhentingsvirksomhet for denne metoden/aksessens vedkommende. Etter utvalgets vurdering oppveies imidlertid eventuelle ulemper forbundet med dette av de fordeler som kontrollmekanismene vil tilføre DGF-systemet i form av en troverdig og uavhengig forsikring mot at søk og innsyn i data skjer i større grad enn strengt nødvendig.»

Departementet støtter dette resonnementet.

Selv om departementet er enig i Lysne II-utvalgets anbefaling om at Etterretningstjenestens tilgang til grenseoverskridende elektronisk kommunikasjon bør underlegges et uavhengig autorisasjon- og kontrollregime, foreslås en innretning som skiller seg i noen grad fra utvalgets forslag. Etter departementets syn er det mekanismene som foreslås både hver for seg og samlet best i stand til å ivareta behovet for en uavhengig og helhetlig kontroll. Departementet vil redegjøre for dette i det følgende.

11.11 Forutgående domstolskontroll

11.11.1 Innledning

Departementet skal i det følgende drøfte hvorvidt det bør oppstilles et krav om forutgående domstolskontroll av Etterretningstjenestens bruk av tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon, og i tilfelle hvordan en slik ordning bør utformes. Lysne II-utvalget går i sin rapport inn for domstolskontroll gjennom en ordning med forhåndsgodkjennelser av søk i metadatalageret og innsamling av innholdsdata.

11.11.2 Lysne II-utvalgets rapport

Lysne II-utvalget drøfter forhåndsgodkjennelse i rapportens punkt 9.3.2. Utvalget fremholder at prøvingen for en domstol i det enkelte tilfelle vil bero på avveininger som ikke utelukkende er av rettslig karakter, og uttaler på side 58:

> «Det vil derfor være viktig at domstolen har grunnleggende forståelse for etterretningsfaget og innsikt i etterretningsvurderinger og trusselbildet som ligger til grunn for anmodninger om søk. Av sikkerhetsmessige hensyn vil antallet dommere måtte være begrenset. De vil måtte inneha etterretningsfaglig kompetanse, teknisk og operativ innsikt i tjenestens virksomhet samt i overordnede myndigheters styrings- og prioriteringsvirksomhet. Videre vil godkjenningsmyndigheten måtte ta hensyn til at utenlandsetterretning ofte innebærer at man søker etter ukjente aktører basert på kjent modus, hvilket kan tilsi bred målutvikling før man gjennom analyse og videre tiltak kan skille ut den relevante informasjon for videre målrettet og presis innsamling. En forhåndsprøving som søker å «hoppe over» målutviklingsfasen, blir meningsløs.
>
> Det vil alltid være en viss risiko for at dommerne etter hvert kan identifisere seg med tjenestens virke og oppgaver, grunnet deres operative medvirkning til tjenestens løpende oppdragsløsning. Det må derfor sikres mekanismer som også sørger for tilstrekkelig «avstand» mellom dommerne og tjenesten, for å unngå for tette bånd og at det utvikles en slik kultur.»

Utvalget har ikke utredet i detalj hvordan domstolsbehandlingen skal legges opp, men har pekt på enkelte sentrale forhold:

Reglene om domstolskontroll bør etter utvalgets syn fremgå av etterretningstjenesteloven selv. Det bør gjelde grunnleggende vilkår for å tillate søk, herunder terskelkrav («beviskrav»), varighet av søketillatelsen og kontroll med at tillatelse ikke vil være uforholdsmessig inngripende. Loven bør fastslå at domstolen ikke kan tillate søk når det vil fremstå som uforholdsmessig. Utfyllende regler om for eksempel utforming av begjæringer til domstolen bør kunne fastsettes i forskrift.

Utvalget antar at det et stykke på vei vil kunne søkes veiledning i utformingen av regelverket i politiloven kapittel III a, som blant annet gjelder PSTs forebyggende bruk av tvangsmidler. Regelverket bør så langt som mulig være åpent og offentlig tilgjengelig. Enkelte mer detaljerte spørsmål bør kunne overlates til regulering i forskrift eller interne retningslinjer i Etterretningstjenesten. Det kan gjelde personell kompetanse til å be om rettens tillatelse, utforming av begjæringer mv.

Utvalget går inn for at rettens avgjørelser bør treffes ved kjennelse. Kjennelsen kan ikke meddeles de personer den gjelder, men den skal foruten til tjenesten selv, meddeles DGF-tilsynet og også være tilgjengelig for EOS-utvalget.

Etter utvalgets syn må hovedvilkåret for å tillate søk knyttes opp mot Etterretningstjenestens formål, jf. etterretningstjenesteloven § 3. Tillatelse til søk i registrene bør bare kunne gis dersom det er grunn til å tro at inngrepet vil gi opplysninger av betydning for dette formålet. Loven bør anvise – så langt det lar seg gjøre – hvor vide søketillatelser som kan gis. For søk basert på personselektorer knyttet til personer som domstolen har godkjent innhenting mot, antar utvalget at domstolens kjennelser i alle fall bør kunne inkludere to ledd ut i kommunikasjonskjeden. Dette vil for det første fasilitere bedre treff ved søk, og det vil i tillegg bidra til at antall rettsavgjørelser kan holdes på et håndterlig nivå.

I alle fall for modusselektorer mener utvalget at varigheten ikke bør være for kort, for å ivareta muligheten til å detektere enkelte mer sjeldne signaturer. Politiloven kapittel III a gir en lengste varighet på seks måneder, jf. § 17 e. For DGF kan dette i enkelte tilfeller synes for knapt, og utvalget antar derfor at lengstetiden bør kunne settes opp til ett år, i enkelte tilfeller muligens også lenger. Det innebærer ikke at dette nødvendigvis skal være den normale varigheten av en søketillatelse.

Etter utvalgets oppfatning er det sentralt at DGF-domstolen har kapasitet til å håndtere antall saker og at behandlingen kan skje raskt. Utvalget tar for sin del ikke stilling til om dette skal være en spesialdomstol eller om det for eksempel bør inngå som en del av porteføljen til Oslo tingrett. Av hensyn til gradering og sikkerhet mener utvalget at det antagelig ikke vil være mulig å behandle sakene i Oslo tingretts vanlige lokaler. Skal sakene legges til Oslo tingrett, mener utvalget derfor at det nok er mest nærliggende å se for seg en ordning der dommere med nødvendig sikkerhetsklarering kan rullere på å behandle denne sakstypen i godkjente lokaler hos Etterretningstjenesten.

Utvalget skriver at det i enkelte tilfeller kan oppstå behov for å iverksette søk uten å avvente domstolens avgjørelse, og at regelverket, etter mønster av politiloven § 17 d tredje ledd, antagelig bør åpne for det. Etter utvalgets syn må det da stilles krav om etterfølgende foreleggelse for domstolen og sletting av søk dersom domstolen avslår godkjennelse.

11.11.3 Nordisk rett

Sverige har opprettet en spesialdomstol, Försvarsunderrättelsedomstolen, ved lov.[254] Domstolen prøver spørsmål om tillatelse til *signalspaning* i henhold til egen lovgivning.[255] Etter lov om signalspaning § 5 skal det oppnevnes et *integritetsskyddsombud* som skal beskytte den enkeltes integritetsinteresse i saker ved domstolen. Ombudet har rett til å ta del i det som forekommer i saken og til å ytre seg. Det følger av § 8 at ombudet ikke uberettiget skal røpe hva han eller hun har fått kjennskap til i saken. I kvalifiserte hastetilfeller kan domstolen møtes og fatte beslutning uten at ombudet har vært til stede eller på annen måte hatt mulighet til å ytre seg, jf. § 12. Det følger av lov om signalspaning § 13, jf. FRA-loven § 16, at domstolens beslutninger i spørsmål om signalspaning ikke kan ankes. Det følger videre av sistnevnte paragraf at heller ingen andre beslutninger av domstolen etter loven, kan ankes.

Regjeringen i *Finland* fremmet 25. januar 2018 en proposisjon med forslag til Lag om militär underrättelseverksamhet.[256] Etter forslaget skal loven blant annet regulere innhenting av grenseoverskridende datatrafikk. Slik innhenting skal besluttes av en domstol, jf. lovforslaget § 66 (innhenting rettet mot statlige aktører) og § 68 (innhenting rettet mot ikke-statlige aktører). Tillatelse kan gis for inntil seks måneder av gangen. Etter lovforslaget § 113 skal sakene behandles ved tingretten i Helsingfors. Det er ikke foreslått regler om oppnevnelse av særskilt advokat for den som innhentingen retter seg mot. Slik departementet forstår forslaget, er ankeretten begrenset til anke over saksbehandlingsfeil. I hastetilfeller kan hovedstabens etterretningssjef fatte beslutning om innhenting, som skal legges frem for domstolen så snart som mulig og senest 24 timer etter at innhentingen ble iverksatt.

11.11.4 Departementets vurdering

11.11.4.1 Bør tilrettelagt innhenting kreve domstolens forhåndsgodkjennelse?

Departementet har i punkt 10.6.2 drøftet hvorvidt det bør oppstilles et krav om domstolens forhåndsgodkjennelse av Etterretningstjenestens metodebruk. Dette spørsmålet ble besvart benektende. I likhet med Lysne II-utvalget mener departementet imidlertid at det er behov for særlige forhåndsautorisasjonsregler og styrket kontroll knyttet til tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon. Dette har sammenheng med det særpreg tilgangen har som følge av at det er nødvendig med lagring av store mengder metadata om norsk kommunikasjon.

Domstolskontroll av tilrettelagt innhenting kan ta form av at retten på forhånd må gi tillatelse til bruk av metoden. Slik forutgående domstolskontroll kjennes særlig fra politiets bruk av tvangsmidler. Justisdepartementet påpekte i forarbeidene i forbindelse med endringer i straffeprosessloven og politiloven[257]at det er en grunnleggende rettssikkerhetsgaranti at bruk av tvangsmidler som hovedregel må tillates av domstolene ved kjennelse, og uttalte deretter:

---

[254] Lag (2009:966) om Försvarsunderrättelsedomstol (her omtalt som FRA-loven)

[255] Lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet.(her omtalt som lov om signalspaning)

[256] RP 203/2017 rd

[257] Ot.prp. nr. 60 (2004–2005) Om lov om endringer i straffeprosessloven og politiloven (romavlytting og bruk av tvangsmidler for å forhindre alvorlig kriminalitet) punkt 9.4.3.2

> «Kravet om forhåndstillatelse fra domstolene vil virke disiplinerende, og gi bedre rettssikkerhet og personvern enn om det ikke skulle kreves tillatelse fra retten. Det er dessuten vanskelig å finne frem til bedre former for forhåndsgodkjenning. For eksempel ville det være lite naturlig å legge en slik oppgave til EOS-utvalget eller til den høyere påtalemyndighet.»

Justisdepartementet påpekte deretter at domstolene i relasjon til enkelte av vilkårene reelt sett ville ha begrensede muligheter til å etterprøve det faktiske grunnlaget for begjæringen, og at den viktigste funksjonen til domstolene trolig ville være å utelukke bruken av tvangsmidler fordi de ville være for inngripende, eller fordi kravet til særlige grunner for bruk av enkelte av tvangsmidlene ikke var oppfylt. Justisdepartementet uttalte videre:

> «Departementet vil sammen med Domstoladministrasjonen vurdere om det er behov for særskilte tiltak for å heve domstolenes kompetanse i saker om rikets sikkerhet, slik at kontrollen blir mest mulig effektiv og reell. Det må likevel advares mot urealistiske forestillinger om hvor høy rettssikkerhet og hvor godt personvern som kan oppnås ved å kreve at domstolene på forhånd må gi tillatelse til å bruke tvangsmidler i forebyggende øyemed. Andre former for supplerende kontroll, i regi av departementet og i ettertid ved EOS-utvalget, blir desto viktigere.»

Departementet mener at disse hensynene langt på vei gjør seg gjeldende også for spørsmålet om domstolskontroll av tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon. Rettssikkerhets- og legitimitetshensyn tilsier et krav om forhåndsgodkjennelse fra domstolene. Det ville virke mindre betryggende om Etterretningstjenesten som hovedregel selv skulle kunne beslutte bruk av metoden, eller om slik myndighet ble lagt til departementet eller en annen del av den utøvende makt. En kunne sett for seg å legge forhåndsgodkjennelsen til EOS-utvalget, som er et uavhengig organ, men dette er lite ønskelig. På denne bakgrunn mener departementet at forhåndskontrollen bør legges til domstolene.

Et krav om forhåndstillatelse fra domstolene vil etter departementets syn utgjøre en reell og viktig rettssikkerhetsgaranti – for det første i form av den disiplinerende virkning et slikt krav må antas å ha for Etterretningstjenesten, og for det andre i form av den legalitetskontroll domstolene vil utføre, særlig med hensyn til inngrepets forholdsmessighet. Departementet vil samtidig påpeke at det reelt sett kan være vanskelig for domstolene å etterprøve enkelte andre vilkår etter loven og på samme måte som i Ot.prp. nr. 60 (2004–2005) kan det derfor være grunn til å advare mot urealistiske forestillinger om hvor høy rettssikkerhet og hvor godt personvern som kan oppnås ved å kreve at domstolene på forhånd må gi tillatelse til metodebruken. Den forutgående domstolskontrollen kan imidlertid ikke sees isolert fra øvrige mekanismer for tilsyn og kontroll. Dette poenget understrekes av EUs byrå for fundamentale rettigheter i en rapport fra 2017:[258]

> «[Addressing] any issue relating to prior oversight in isolation of the oversight system as a whole will not offer a complete picture of its effectiveness. Inevitably, national systems will strike different balances when designing their respective architecture of checks and balances. Consequently, apparent strengths or weaknesses of ex ante review may be undermined or remedied, respectively, in ongoing and ex post oversight.»

Departementet vil på denne bakgrunn understreke at den forutgående domstolskontrollen må sees i sammenheng med tilsyns- og kontrollsystemet for øvrig. Etterretningstjenestens internkontroll, forvaltningskontrollen i regi av departementet og den uavhengige løpende og

[258] Surveillance by intelligence services – Volume II: field perspectives and legal update (2017) s. 97

etterfølgende kontrollen i regi av EOS-utvalget er viktige elementer i det samlede systemet, som etter departementets syn må karakteriseres som betryggende og solid.

11.11.4.2 Bør domstolskontrollen ivaretas av de alminnelige domstoler eller av en særdomstol?

Lysne II-utvalget tok i sin rapport ikke stilling til om domstolskontrollen burde legges til en særdomstol (spesialdomstol) eller til de alminnelige domstolene.

De høringsinstansene som har uttalt seg om spørsmålet, mener at domstolskontrollen bør legges til de alminnelige domstoler. *Advokatforeningen* mener at en særdomstol på dette området er grunnleggende betenkelig, og ser ingen grunn til at legalitetskontrollen ikke kan utøves av de ordinære domstoler. *Borgarting lagmannsrett* og *Dommerforeningen* mener at kontrollen må legges til de alminnelige domstoler på samme måte som kontrollen med hemmelige tvangsmidler under etterforskning, for å avverge alvorlig kriminalitet eller i forebyggende øyemed. *Norges nasjonale institusjon for menneskerettigheter* slutter seg til dette, og peker på at hensynet til allmennhetens tillit til en reell og uavhengig kontroll bedre ivaretas ved at kontrollen legges til de alminnelige domstolene. *Juristforbundet* har generelt sluttet seg til Dommerforeningens høringsuttalelse. *Justis- og beredskapsdepartementet* peker på at en i Norge tradisjonelt har benyttet spesialdomstoler i liten grad, og mener at behovet for kunnskap om etterretningsfaget og trusselbildet kan ivaretas ved at avgjørelsene legges til én bestemt tingrett eller enkelte dommere eller en avdeling i en tingrett. Høringsinstansen stiller spørsmål om det er ressursmessig forsvarlig å opprette en spesialdomstol, og peker dessuten på at risikoen for at dommerne over tid vil identifisere seg med Etterretningstjenestens virke og oppgaver, trolig vil være mindre hvis de befatter seg med ulike oppgaver og fagfelt, slik det i dag er ved de alminnelige domstoler.

Særdomstolsutvalget har vurdert nye domstolsordninger for foreldretvister, barnevernssaker og utlendingssaker.[259] I punkt 5.4 drøfter utvalget noen generelle hensyn som taler for og imot dommerspesialisering. Noen av synspunktene som trekkes frem, kan etter departementets syn være relevante også for spørsmålet om domstolskontrollen med tilrettelagt innhenting bør legges til de alminnelige domstolene eller til en særdomstol.

Særdomstolsutvalget tar utgangspunkt i at utviklingen i de siste tiårene har gått i retning av at det bør vises tilbakeholdenhet med å etablere særdomstoler, og at slike bare bør opprettes når det er særskilte forhold ved det aktuelle saksområdet som tilsier det. Utvalget fremholder videre:

> «Sentrale elementer i begrunnelsen for ikke å gå inn for særdomstoler, er at dommere med en bred fagkrets gir det beste utgangspunktet for god saksbehandling og kvalitativt gode avgjørelser, for en helhetlig utvikling av rettssystemet, og for rekruttering av de beste kandidatene til dommerstillingene. Videre har det vært antatt at det er generalistdommere som har de beste forutsetningene for å vurdere bevis.»

Om hensynet til realkompetanse og effektiv ressursutnyttelse uttaler Særdomstolsutvalget:

> «Blant de argumenter som gjerne trekkes frem i favør av spesialisering, er at dommerne, gjennom konsentrasjon om noen typer av saker, opparbeider større realkompetanse innenfor det aktuelle området, og at de gjerne også vil ha en særskilt interesse for det området som de har søkt seg til. Med mye erfaring innenfor ett eller noen få områder, er det dessuten nærliggende å anta at dommerne kan behandle de aktuelle sakene mer

[259] NOU 2017: 8 *Særdomstoler på nye områder? - Vurdering av nye domstolsordninger for foreldretvister, barnevernsaker og utlendingssaker*

effektivt enn det som oppnås gjennom en bredere praksis. På den annen side vil særdomstoler kunne gi mindre fleksibilitet ved variasjoner i saksinngangen. En ordning med spesialiserte dommere innenfor enkelte saksområder, men som også behandler andre typer saker, ivaretar i noen grad både behov for spesialkunnskap og for effektiv ressursutnyttelse.»

Særdomstolsutvalget trekker også frem risikoen for at spesialisering kan føre til at dommeren i for stor grad identifiserer seg med saksområdet:

> «Et annet argument som ofte anføres imot spesialisering, er at spesialiseringen innebærer en risiko for at de som arbeider med sakene kan bli for opptatt av sitt eget område, og i for stor grad identifisere seg med dette. I sin tur kan dette medføre at mer generelle holdninger og verdier ikke trekkes inn, og at avgjørelsene dermed kan komme i utakt med samfunnet for øvrig. Dette kan ses som uttrykk for mer generelle holdninger om skadevirkningene av «ekspertvelde». En innvending mot denne betraktningsmåten er at samfunnsutviklingen på mange områder går i retning av mer spesialisering. Denne utviklingen kan bety at det er nødvendig med mer spesialisert kunnskap også for bedømmelsen av de rettslige sider ved forskjellige virksomheter. På den annen side er den generaliserte juridiske tilnærmingen til samfunnets forskjellige motsetninger og konflikter et gode fordi den bidrar til å binde samfunnet sammen.»

Deretter drøfter Særdomstolsutvalget hensynet til dommerrekrutteringen:

> «Det har også vært innvendt at det kan være vanskeligere å rekruttere gode jurister til spesialdomstoler enn til de alminnelige domstolene. Mens det tidligere periodevis har vært et problem å rekruttere gode dommere, er det god søkning til dommerembeter mange steder i dag. Utenfor de store stedene kan imidlertid rekrutteringsgrunnlaget fortsatt være lite. Tradisjonelt oppfatter mange det som attraktivt å arbeide over et bredt spekter av rettsområder. I et høyt spesialisert samfunn vil imidlertid også konsentrasjon om utvalgte fagområder kunne ses som et gode. Det er vanskelig å si noe bestemt om hvordan søkningen til dommerstillinger med et begrenset fagfelt vil være.»

Særdomstolsutvalget konkluderer drøftelsen med at Norge generelt har et godt domstolsapparat, og støtter innretningen med hovedsakelig generelle domstoler og dommere som behandler saker over et bredt fagfelt. På enkelte områder mener utvalget at det likevel kan være behov for tiltak for å sikre et tilstrekkelig høyt faglig nivå og engasjement for de sakene som skal behandles. I punkt 5.4.2 peker utvalget på at behov for spesialkompetanse innenfor et område i praksis kan tenkes dekket på to måter; enten gjennom etablering av en særdomstol som bemannes med dommere med den aktuelle kompetansen, eller ved å sørge for at tilstrekkelig mange av dommerne i de alminnelige domstolene har den aktuelle kompetansen, og tilordne sakene til dem. Utvalget drøfter deretter en del fordeler og ulemper ved hvert av disse alternativene:

> «Ved å etablere en særdomstol, får den dømmende virksomheten der en tydelig egen identitet, adskilt fra de alminnelige domstolene. Domstolens navn kan gi allmennheten og samarbeidspartnere informasjon om hvilke saker som behandles der, og understreke at domstolen representerer særskilt kompetanse innenfor det aktuelle området. Ved rekruttering av dommere og andre medarbeidere til domstolen vil det være klart hvilke fagområder den som ansettes skal arbeide med, og både arbeidsgiver og søker vil naturlig reflektere over søkerens forutsetninger for å behandle den eller de sakstypene som hører under særdomstolen. De ansatte vil ha et felles fagområde, og dermed gode forutsetninger for å skape et godt faglig miljø.»

Som en potensielt vesentlig innvending mot særdomstoler, trekker Særdomstolsutvalget frem at virksomheten må konsentreres på ett eller noen få steder i landet for å kunne bli det faglige tyngdepunktet som vil være formålet med etableringen. Utvalget peker også på at

etablering av særdomstoler innebærer et mer komplekst, mindre «strømlinjeformet» domstolsapparat, og at det dessuten kan kreve betydelige organisatoriske endringer, blant annet ved overføring av personell fra de alminnelige domstolene til særdomstolen.

Særdomstolsutvalget påpeker avslutningsvis at undersøkelser viser at innbyggerne generelt har stor tillit til domstolene. Hvis en ny særdomstol behandler saker etter de samme prosessreglene som dagens domstol, er det ifølge utvalget mulig at tilliten raskt vil omfatte også denne. Hvis den nye domstolen derimot skal behandle saker på en enklere måte, med færre rettssikkerhetsgarantier, mener utvalget at det vil være mer usikkert om den generelle tilliten til domstolene «følger med».

Lysne II-utvalget peker i sin rapport på at det er viktig at domstolen har grunnleggende forståelse for etterretningsfaget og innsikt i etterretningsvurderinger og trusselbildet som ligger til grunn for anmodninger om søk. Lysne II-utvalget mener at antallet dommere av sikkerhetsmessige hensyn vil måtte være begrenset, og at de vil måtte inneha etterretningsfaglig kompetanse, teknisk og operativ innsikt i tjenestens virksomhet samt i overordnede myndigheters styrings- og prioriteringsvirksomhet.

Departementet mener at hensynene som Lysne II-utvalget har trukket frem, kan tale for en form for dommerspesialisering. Den europeiske kommisjonen for demokrati gjennom lovgivning (Veneziakommisjonen) har også fremholdt at verdien av domstolskontroll avhenger av ekspertisen de aktuelle dommerne har i å vurdere trusler mot nasjonal sikkerhet og balansere disse mot inngrep i menneskerettighetene. Etter kommisjonens syn taler svært sterke argumenter for en grad av spesialisering og spesialistopplæring for dommere som behandler godkjennelser.[260]

Ett alternativ er å opprette en særdomstol, slik som for eksempel i Sverige. Dette vil gi virksomheten en tydelig egen identitet og vil kunne legge til rette for utviklingen av et godt faglig miljø med den rettslige og faktiske kunnskapen som er nødvendig for å kunne ta stilling til begjæringene på en effektiv måte og med høy kvalitet. En innvending mot dette kan være at saksmengden ikke nødvendigvis vil være av en størrelse som tilsier et behov for et stort antall dommere og andre ansatte. Departementet viser for så vidt til årsberetningen for den svenske Försvarsunderrättelsedomstolen for 2016, hvor det fremgår at bare én dommer var ansatt på heltid, i tillegg til en kontorsjef og to administrativt ansatte.

Etter departementets syn er det sentralt for legitimiteten til Etterretningstjenestens virksomhet at befolkningen har tillit til at domstolene foretar en reell og uavhengig kontroll av tilrettelagt innhenting. Departementet mener dette hensynet ivaretas bedre hvis legalitetskontrollen legges til de alminnelige domstolene, heller enn til en særdomstol. Risikoen for at dommerne i en særdomstol over tid kan komme til å identifisere seg med Etterretningstjenestens virksomhet, må antas å være større enn i de alminnelige domstolene, hvor dommerne er generalister som behandler alle sakstyper.[261] Det er i det minste en risiko for at det i allmennheten, eller deler av denne, kan danne seg et slikt inntrykk. Hensynet til Etterretningstjenestens tillit og legitimitet i befolkningen tilsier derfor at domstolskontrollen legges til de alminnelige domstolene.

[260] Se *Report on the democratic oversight of the security services* (revidert utgave 2015) avsnitt 216–221. Uttalelsene gjelder straffesaker, men har i denne sammenhengen overføringsverdi.

[261] Se *Report on the democratic oversight of the security services* (revidert utgave 2015) avsnitt 223.

Domstolskontroll ved de alminnelige domstolene er etter departementets syn ikke til hinder for en viss form for dommerspesialisering i saker om tilrettelagt innhenting, i det minste i den forstand at det på grunn av krav til sikkerhetsklarering vil være et begrenset antall dommere som behandler de aktuelle sakene, og at disse dommerne derfor vil opparbeide seg erfaring med sakstypen. Domstolene bør også sørge for at de aktuelle dommerne – på en måte som tar tilbørlig hensyn til domstolenes uavhengighet – kan skaffe seg nødvendig faglig kompetanse gjennom kursdeltakelse, studiepermisjoner eller lignende.

Etter departementets syn kan det legges til rette for en viss dommerspesialisering ved å samle sakene i én tingrett. Oslo tingrett fremstår i så måte som et naturlig alternativ. Det er særlig to grunner til dette. For det første har Etterretningstjenesten, som er den eneste myndigheten som skal kunne fremme begjæring om søk, sete i Oslo. For det andre vil sakene medføre at domstolen må være i stand til å behandle høyt gradert informasjon i tråd med kravene i sikkerhetsloven. Disse kravene vil mest hensiktsmessig kunne oppfylles hvis sakene samles i Oslo tingrett, særlig på bakgrunn av denne domstolens erfaring med behandling av PSTs begjæringer om bruk av skjulte tvangsmidler, som regelmessig inneholder sikkerhetsgraderte opplysninger.

Departementet foreslår etter dette at den forutgående domstolskontrollen med tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon legges til Oslo tingrett.

11.11.4.3 Hva skal domstolen prøve?

Departementet går inn for at retten skal foreta en forutgående legalitetskontroll av bruken av tilrettelagt innhenting. Dette innebærer at retten, når den behandler Etterretningstjenestens begjæring, skal prøve om lovens vilkår er oppfylt. Retten skal herunder prøve at innhentingen ligger innenfor Etterretningstjenestens oppgaver, tilfredsstiller grunnvilkårene for målsøking og målrettet innhenting, og ikke er uforholdsmessig.

Det er grunn til å tro at retten ikke så ofte vil fravike Etterretningstjenestens vurdering av hvorvidt innhentingen ligger innenfor tjenestens oppgaver, jf. lovutkastet kapittel 3, og tilfredsstiller grunnvilkårene for målsøking og målrettet innhenting, jf. lovutkastet §§ 5-1 og 5-2. Dette har sammenheng med at tersklene for innhenting ikke kan settes for høyt, spesielt når det gjelder målsøking, se nærmere punkt 9.3. I tillegg antar departementet at den forutgående domstolskontrollen i seg selv vil virke disiplinerende på tjenesten. Det er for eksempel lite trolig at Etterretningstjenesten vil fremme en begjæring om å gjennomføre et søk som ligger utenfor tjenestens oppgaver når tjenesten vet at den vil bli «sett i kortene» av en uavhengig domstol og eventuelt også en særskilt oppnevnt advokat. Departementet understreker at domstolen skal foreta en reell legalitetskontroll i den enkelte sak. På bakgrunn av de nevnte forhold kan det likevel være grunn til å understreke at det ikke uten videre kan sluttes fra en høy andel av godkjennelser til at kontrollen ikke er reell.

En sentral del av rettens forhåndskontroll blir å påse at inngrepet ikke er uforholdsmessig, jf. forslag til § 5-4. Kravet til forholdsmessighet er godt egnet for rettslig prøving, og domstolene har lang og bred erfaring med forholdsmessighetsvurderinger fra andre rettsområder. Retten skal videre prøve at innhentingen ikke strider mot noen av de særskilte forbudene som er fastsatt i loven, herunder forbudet i § 1-3 andre ledd mot virksomhet som innebærer en reell risiko for at ufravikelige og andre grunnleggende menneskerettigheter krenkes, forbudet i § 4-1 mot innhenting rettet mot personer som befinner seg i Norge, forbudet i § 4-3 mot industrispionasje, forbudet i § 4-4 mot å utføre oppgaver med politiformål og forbudet i § 9-4 mot vilkårlig behandling av personopplysninger.

Departementet foreslår følgende regulering av hva domstolen skal prøve:

§ 8-4 *Hva retten skal prøve*
Retten skal prøve om vilkårene etter loven her er oppfylt, herunder at innhentingen ligger innenfor Etterretningstjenestens oppgaver etter kapittel 3, ikke innebærer brudd på forbudene i §§ 1-3 annet ledd, 4-1, 4-3, 4-4 eller 9-4, og tilfredsstiller grunnvilkårene etter kapittel 5.

11.11.4.4 Saksbehandlingen i domstolen

Behandling av begjæringer om søk
Saksbehandlingen ved domstolen bør innledes gjennom at Etterretningstjenesten fremmer en begjæring om søk i lagrede metadata etter lovutkastet § 7-8 eller innhenting og lagring av innholdsdata etter lovutkastet § 7-9. Domstolene skal med andre ord ikke kunne beslutte bruk av tilrettelagt innhenting på eget initiativ. Dette følger av rollefordelingen mellom Etterretningstjenesten og domstolene, hvor sistnevnte utelukkende skal ha en kontrollfunksjon. Departementet har i lovforslaget ikke lagt opp til noe krav om at begjæringene må individualiseres. Etterretningstjenesten vil derfor etter forslaget kunne fremme begjæringer som består av et sakskompleks.

Kompetansen til å fremsette begjæring om tilrettelagt innhenting bør i utgangspunktet ligge til sjefen for Etterretningstjenesten. Kompetansen bør imidlertid kunne delegeres, for eksempel til jurister i tjenesten. Hensyn til notoritet og forsvarlig saksbehandling tilsier at begjæringen må være skriftlig.

Begjæringen må inneholde den informasjonen som er nødvendig for at domstolen skal kunne prøve om lovens vilkår er oppfylt. Omfanget vil nødvendigvis kunne variere fra sak til sak, men Etterretningstjenesten må påvise at innhentingen er relevant for å løse en av tjenestens oppgaver og at den oppfyller grunnvilkårene, herunder at den ikke utgjør et uforholdsmessig inngrep. Mer konkret kreves at begjæringen skal angi hva eller hvem søkene retter seg mot, samt opplysninger om det rettslige og faktiske grunnlaget for innhentingen. Dette innebærer ikke at Etterretningstjenesten må angi konkret hvilke søkebegreper som skal benyttes; det sentrale er at domstolen settes i stand til å foreta en reell prøving av nødvendigheten og forholdsmessigheten av søkene.[262] Hvis retten mener at begjæringen ikke gir tilstrekkelig grunnlag for avgjørelsen, kan den kreve ytterligere opplysninger. Retten kan også beslutte muntlige forhandlinger for å opplyse saken ytterligere, og Etterretningstjenesten kan i så fall stille med fagkyndige i den grad det anses nødvendig. Hvis retten oppnevner en særskilt advokat vil også denne kunne bidra til sakens

[262] I *Big Brother Watch m. fl. mot Storbritannia* avsagt 13. september 2018 (ikke rettskraftig) uttalte domstolen at angivelse av selektorer og søkekriterier ikke var påkrevd ved begjæring om innhenting, men at de selektorer og søkebegrepet som *de facto* ble anvendt ved innhenting måtte være underlagt uavhengig kontroll. Domstolen uttaler i avsnitt 340:

«This does not mean that selectors and search criteria need to be made public; nor does it mean that they necessarily need to be listed in the warrant ordering interception. In fact, in the *Liberty* proceedings the IPT found that the inclusion of the selectors in the warrant or accompanying certificate would "unnecessarily undermine and limit the operation of the warrant and be in any event entirely unrealistic" (see paragraph 44 above). The Court has no reason to call this conclusion into question. Nevertheless, the search criteria and selectors used to filter intercepted communications should be subject to independent oversight; a safeguard which appears to be absent in the section 8(4) regime. Indeed, the ISC report criticised the absence of any meaningful oversight of both the selectors and search criteria (see paragraph 157 above).»

opplysning, jf. nedenfor, men etter departementets syn må det holdes fast ved at det primært er Etterretningstjenesten som skal sørge for å gi retten et forsvarlig grunnlag for den forutgående legalitetskontrollen.

Retten avgjør saken i form av en skriftlig kjennelse som skal begrunnes. Krav til begrunnelse skal sikre en reell og samvittighetsfull vurdering og motvirke muligheten for urettmessige og vilkårlige avgjørelser, og utgjør dermed i seg selv en rettssikkerhetsgaranti. Begrunnelsen skal også gi Etterretningstjenesten og den særskilt oppnevnte advokaten grunnlag for å vurdere om kjennelsen bør ankes, og, hvis den ankes, gi grunnlag for ankedomstolens behandling av anken. Begrunnelsespliktens utstrekning vil kunne variere fra sak til sak, både hva gjelder de faktiske forhold og rettsanvendelsen, men begrunnelsen må være så utfyllende at de nevnte hensynene ivaretas.

Departementet foreslår følgende regulering av rettens kjennelser:

§ 8-1 *Kjennelse om tillatelse til tilrettelagt innhenting*

Retten kan ved kjennelse gi Etterretningstjenesten tillatelse til søk etter § 7-8 og innhenting og lagring etter § 7-9.

Retten kan oppstille vilkår i kjennelsen. Kjennelsen skal begrunnes. Retten kan omgjøre kjennelsen.

Rettens avgjørelse skal treffes så raskt som mulig.

Avgjørelsen treffes uten at den som avgjørelsen retter seg mot eller ellers rammer gis adgang til å uttale seg. Kjennelsen blir ikke meddelt dem.

Kjennelsen skal meddeles Etterretningstjenesten. Tjenesten skal gjøre kjennelsen tilgjengelig for EOS-utvalget.

Departementet foreslår følgende regulering av krav til begjæringen:

§ 8-2 *Krav til begjæringen*

Etterretningstjenestens begjæringer skal være skriftlige og angi hva eller hvem innhentingen retter seg mot og opplysninger om det rettslige og faktiske grunnlaget for innhentingen.

Begjæringen fremmes for Oslo tingrett av sjefen for Etterretningstjenesten eller den som sjefen bemyndiger.

Departementet foreslår følgende regulering om rettsmøte:

§ 8-3 *Rettsmøte*

Retten kan beslutte muntlige forhandlinger. Etterretningstjenesten møter ved sjefen for tjenesten eller den som sjefen bemyndiger. Tjenesten kan medbringe fagkyndige dersom dette anses nødvendig for å opplyse saken.

Rettsmøtene holdes for lukkede dører.

Særskilt oppnevnt advokat

Lysne II-utvalget drøfter i sin rapport ikke hvorvidt det bør innføres en ordning med særskilt advokat for den som berøres av en begjæring om tilrettelagt innhenting. *Advokatforeningen*, *Borgarting lagmannsrett* og *Dommerforeningen* har i sine høringsuttalelser tatt til orde for en slik ordning. *Juristforbundet* har generelt sluttet seg til Dommerforeningens høringsuttalelse.

Kontradiksjonsprinsippet er et grunnleggende prinsipp i norsk domstolsprosess. Prinsippet skal ivareta hensynet til sannhetssøken, rettssikkerheten og partenes og allmennhetens tillit til rettsapparatet. Det har blant annet forankring i retten til rettferdig rettergang etter Grunnloven § 95 første ledd andre punktum. En sentral side ved kontradiksjonsprinsippet er partenes rett til kjennskap til og mulighet til å imøtegå det rettslige og faktiske grunnlaget for motpartens anførsler.

Det ligger i sakens natur at tilrettelagt innhenting må kunne skje i det skjulte overfor personer som den berører. Noe annet ville undergrave formålet med innhentingen. Det følger av dette at de berørte ikke vil kunne underrettes om eller ta del i en sak om forhåndsgodkjennelse av inngrepet. En kontradiktorisk domstolsbehandling lar seg derfor ikke gjennomføre på vanlig måte. Når dette er situasjonen, mener departementet at det er viktig å legge til rette for en saksbehandling som kan ivareta rettssikkerhetshensyn så langt det er mulig. Departementet viser for så vidt til EMDs dom *Roman Zakharov mot Russland*,[263] hvor domstolen uttaler:

> «Review and supervision of secret surveillance measures may come into play at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights.»

Kontradiksjonsprinsippet kan i en viss utstrekning ivaretas gjennom at retten oppnevner en særskilt advokat for den som berøres av innhentingen. En ordning med særskilt advokat ble for første gang innført i 1999 gjennom vedtakelsen av straffeprosessloven § 100 a, som kommer til anvendelse når politiet bruker skjulte tvangsmidler i saker hvor det er skjellig grunn til å tro at det begås eller er begått et lovbrudd av en viss alvorlighetsgrad. Bestemmelsen gjelder dessuten når politiet bruker skjulte tvangsmidler for å avverge bestemte former for organisert og annen alvorlig kriminalitet med hjemmel i straffeprosessloven § 222 d samt når PST med hjemmel i politiloven § 17 d bruker skjulte tvangsmidler for å forebygge de mest alvorlige forbrytelsene innenfor PSTs arbeidsområde, slik som terrorhandlinger.

Særskilt advokat kan etter utlendingsloven[264] § 133 oppnevnes i enkelte utlendingssaker som berører grunnleggende nasjonale interesser eller utenrikspolitiske hensyn. Det samme gjelder i enkelte statsborgersaker som berører slike interesser eller hensyn, jf. statsborgerloven[265] § 31 c, som ikke ennå har trådt i kraft.

Straffeprosessloven § 100 a ble vedtatt etter forslag fra Metodeutvalget. Den særskilte advokatens rolle ble av utvalget omtalt slik:[266]

> «En slik oppnevnt advokat vil ha en tosidig oppgave. Den ene er å sørge for kontradiksjon ved å stille kritiske spørsmål og belyse saken fra andre innfallsvinkler forut for domstolens avgjørelser. Det andre er at man skal være en rettssikkerhetsgaranti for at loven blir etterlevd. Et hovedpoeng må her være at den oppnevnte advokat ikke primært er der for å ivareta den siktedes sak, men derimot representere allmennheten og påse at det tas tilstrekkelig hensyn til personvernet i den avveining som i den konkrete sak skal skje mellom hensynet til den enkeltes integritet, og felleskapets behov for oppklaring og avverging av alvorlig kriminalitet.

[263] *Roman Zakharov mot Russland* avsagt 5. desember 2015, avsnitt 233

[264] Lov av 15. mai 2008 nr. 53 om utlendingers adgang til riket og deres opphold her

[265] Lov av 10. juni 2005 nr. 51 om norsk statsborgerskap

[266] NOU 1997: 15 *Etterforskningsmetoder for bekjempelse av kriminalitet*, Delinnstilling II punkt 6.2.10 s. 8

> Det viktigste argument for å innføre en slik ordning vil være at man da vil få et topartsforhold som er det normale ved rettergang. Et viktig utslag av dette er at det blir praktisk mulig å påkjære også de kjennelser hvor politiet gis adgang til å anvende telefonkontroll.»

Selv om drøftelsen knytter seg til politiets tvangsmidler for kriminalitetsbekjempelse, har den relevans også for domstolskontrollen av tilrettelagt innhenting. Det er etter departements syn viktig for balansen i domstolsprosessen at en av aktørene har som oppgave å stille kritiske spørsmål til Etterretningstjenestens begjæring og sørge for å belyse personvernhensyn som grunnlag for rettens forholdsmessighetsvurdering i den enkelte sak.

Departementet foreslår at den særskilte advokaten skal ivareta interessene både til den eller de innhentingen retter seg mot og interessene til eventuelle tredjepersoner. Departementet viser for så vidt til Justis- og beredskapsdepartementets vurdering i forbindelse med endringer i straffeprosessloven, av en lovfesting av at særskilt advokat oppnevnt etter straffeprosessloven § 100 a også skal ivareta interessene til tredjepersoner, som i hovedsak er dekkende også for så vidt gjelder forslaget her:[267]

> «Ettersom flere av de skjulte metodene i stor grad er inngripende også for tredjepersoner, ser departementet viktigheten av at også deres interesser varetas. Det kan argumenteres med at tredjepersons interesser blir tilstrekkelig varetatt gjennom forholdsmessighetsvurderingen og kravet til særlige grunner hvor en kommunikasjonskontroll eller romavlytting kan berøre et større antall personer, se ovenfor. I tillegg vil den offentlig oppnevnte advokaten i praksis fremsette innsigelser basert på tredjepersoners forhold, for å kunne vareta mistenktes interesser. Departementet har likevel tro på at en lovfesting av at den offentlige advokaten skal trekke inn tredjepersoners interesser kan ha en viss betydning for å gi domstolene et bredest mulig overblikk. En slik lovfesting vil ikke innebære noen formell rolle overfor eventuelle berørte tredjepersoner, og vil i praksis antakelig skille seg lite fra hvordan § 100 a-oppdraget allerede utføres i dag.»

Det bør være opp til retten å beslutte oppnevning. Hvis innhentingen retter seg mot en eller flere bestemte personer, bør særskilt advokat som hovedregel oppnevnes. I noen saker vil ikke innhentingen rette seg mot bestemte personer eller grupper (modusselektorsøk). Retten kan likevel beslutte å oppnevne en særskilt advokat, for eksempel for å belyse mer allmenne personverninteresser som gjør seg gjeldende. På dette punktet går forslaget lenger enn straffeprosessloven § 100 a, som ikke synes å åpne for at retten kan oppnevne særskilt advokat bare for tredjepersoner.[268] En annen løsning på dette punktet er etter departementets syn en naturlig konsekvens av at tilrettelagt innhenting ikke alltid vil rette seg mot bestemte personer.

Etter forslaget skal den særskilte advokaten varsles om rettsmøtet og ha rett til å være til stede og til å uttale seg før retten treffer avgjørelse. Advokaten skal gjøres kjent med begjæringen og annen informasjon som legges frem i retten, men skal utover dette ikke ha noen rett til innsyn i saken. Advokaten skal ikke sette seg i forbindelse med den saken gjelder.

Advokaten skal etter forslaget oppnevnes fra en gruppe av advokater med den høyeste sikkerhetsklareringen (strengt hemmelig), og kan ikke møte ved eller la seg representere av

---

[267] Prop. 68 L (2015–2016) Endringer i straffeprosessloven mv. (skjulte tvangsmidler) punkt 6.6.5 s. 58

[268] Ibid.

en annen advokat eller ved en fullmektig. Departementet skal etter forslaget ha kompetanse til å gi nærmere regler i forskrift om oppnevning av særskilt advokat.

Det er viktig at det legges til rette for at gruppen av advokater opparbeider seg tilstrekkelig faglig kompetanse til å kunne oppfylle rollen på en god måte.

§ 8-5 *Oppnevning av særskilt advokat*

Retten kan beslutte at det skal oppnevnes en særskilt advokat for å ivareta rettighetene til den eller de som innhentingen retter seg mot og eventuelle tredjepersoner. Advokaten beskikkes fra den særlige krets av sikkerhetsklarerte advokater, og kan ikke la seg representere eller møte ved annen advokat eller fullmektig.

Advokaten skal gjøres kjent med Etterretningstjenestens begjæring og annen informasjon som legges frem i retten, men har utover dette ingen innsynsrett. Advokaten skal varsles om rettsmøter i saken og har rett til å delta i dem. Advokaten har rett til å uttale seg før retten treffer avgjørelse.

Advokaten må ikke sette seg i forbindelse med den som saken gjelder.

Departementet kan gi forskrift om oppnevning av særskilt advokat.

Offentlighet

Offentlighetsprinsippet er et grunnleggende prinsipp i norsk domstolsprosess. Det skal legge til rette for offentlig kontroll med og mulighet for kritikk av rettergangen. Prinsippet har blant annet kommet til uttrykk i Grunnloven § 100 femte ledd første punktum, som fastsetter at enhver har rett til å følge forhandlingene i rettsmøter. Etter bestemmelsens andre punktum kan det likevel i lov fastsettes begrensninger i denne retten ut fra hensyn til personvern og av andre tungtveiende grunner. I samme retning følger det av domstolloven[269] § 124 første ledd at rettsmøtene er offentlige og rettsavgjørelsene kan gjengis offentlig, hvis ikke annet er bestemt i lov eller av retten i medhold av lov.

Det ligger i sakens natur at tilrettelagt innhenting må kunne skje i det skjulte overfor personer som den berører og offentligheten for øvrig. Noe annet ville undergrave formålet med innhentingen. Departementet finner det derfor klart at det er nødvendig å gjøre unntak fra hovedregelen om offentlighet, og foreslår at rettsmøtene skal holdes for lukkede dører og at rettens avgjørelser ikke kan gjengis offentlig.

Anke

Departementet mener at Etterretningstjenesten og den særskilte advokaten bør kunne anke kjennelser de er uenige i. Ankemuligheten må antas å virke skjerpende for underinstansens avgjørelse, og utgjør dermed i seg selv en rettssikkerhetsgaranti.

Departementet foreslår at reglene i straffeprosessloven kapittel 26 om anke over kjennelser og beslutninger gis anvendelse så langt de passer. Departementet legger til grunn at dette gjelder reglene om ankefrist (§ 379 første ledd), den innledende saksbehandlingen ved tingretten (§ 381 første og andre ledd), at anken som hovedregel ikke har oppsettende virkning (§ 382 første ledd), at ankedomstolen kan innhente ytterligere opplysninger (§ 384), ankedomstolens avgjørelse (§ 385), muntlige forhandlinger når særlige grunner taler for det (§ 387 første ledd) og anke til Høyesterett (§§ 387 a og 388).

Departementet ber om høringsinstansenes syn på hvorvidt det bør presiseres nærmere hvilke regler som passer, eventuelt ikke passer, og i så fall hvilke regler dette gjelder.

Departementet foreslår følgende regulering av ankeadgangen:

[269] Lov av 13. august 1915 nr. 5 om domstolene

§ 8-9 *Anke*

Etterretningstjenesten og den særskilte advokaten kan anke rettens kjennelse. Anke fra den særskilte advokaten har ikke oppsettende virkning.

Straffeprosessloven kapittel 26 gjelder så langt reglene passer.

§ 8-7 gjelder tilsvarende for ankedomstolen.

Hastekompetanse

Et særskilt spørsmål er hvorvidt Etterretningstjenesten bør gis kompetanse til å beslutte søk i lagrede metadata eller innhenting og lagring av innholdsdata i situasjoner hvor rettens kjennelse ikke kan avventes.

Departementet tar utgangspunkt i at kravet til forhåndsgodkjennelse fra domstolene er en grunnleggende rettssikkerhetsgaranti som en bør være varsom med å gjøre unntak fra, særlig av hensyn til allmennhetens tillit til Etterretningstjenestens virksomhet. Selv om en oppstiller som vilkår for hastekompetansen at retten skal kontrollere beslutningen snarest mulig etter at den ble fattet, vil ikke en slik etterfølgende kontroll kunne forhindre inngrep som det ikke var grunnlag for.

På den andre siden er det etter departementets syn ikke til å komme ifra at det i tidskritiske situasjoner kan være strengt nødvendig for Etterretningstjenesten å gjennomføre søk uten at det er mulig å avvente rettens kjennelse. Et eksempel kan være et cyberangrep som finner sted på en helligdag, hvor tjenesten har behov for søk i metadata for å kunne bidra til å motvirke angrepet. Departementet mener dessuten at faren for misbruk av hastekompetansen vil være begrenset, all den tid beslutningen vil være gjenstand for etterfølgende domstolskontroll kort tid etter at den ble fattet, samt løpende og etterfølgende kontroll av EOS-utvalget.

Departementet mener på denne bakgrunn at loven, på visse, strenge vilkår, bør åpne for at Etterretningstjenesten kan beslutte søk eller innhenting i kvalifiserte hastetilfeller. Departementet viser i den forbindelse til politiloven § 17 d, som gir sjefen og den assisterende sjefen for PST hastekompetanse til å tillate bruk av tvangsmidler blant annet for å forebygge terrorhandlinger. Vilkårene for bruk av hastekompetanse etter politiloven § 17 d er vesentlig strengere enn de tilsvarende reglene i straffeprosessloven, og bestemmelsen er ment å være en «meget snever unntaksregel».[270] Departementet tar samme utgangspunkt for bestemmelsen om hastekompetanse som foreslås her. Etter forslaget skal hastekompetansen bare kunne brukes når det ved opphold er «stor fare» for at etterretningsinformasjon «av vesentlig betydning» for Etterretningstjenestens oppgaver kan gå tapt. Etter mønster av politiloven § 17 d foreslår departementet å legge hastekompetansen til sjefen for Etterretningstjenesten. Departementet går inn for at hastekompetansen ikke skal kunne delegeres, det vil si at det bare er sjefen eller eventuelt den som fungerer som sjef i dennes fravær, som kan fatte slik beslutning.

Departementet foreslår følgende regulering av hastekompetansen:

§ 8-10 *Hastekompetanse*

Dersom det ved opphold er stor fare for at etterretningsinformasjon av vesentlig betydning for utførelsen av Etterretningstjenestens oppgaver etter kapittel 3 kan gå tapt, kan ordre fra sjefen for Etterretningstjenesten tre i stedet for rettens kjennelse. I slike tilfeller skal Etterretningstjenesten straks og senest innen 24 timer etter at innhentingen ble påbegynt forelegge saken for retten.

[270] Ot.prp. nr. 60 (2004–2005) punkt 9.4.3.2 s. 134 og Prop. 68 L (2015–2016) punkt 13.5.4 s. 209

Retten avgjør ved kjennelse om innhentingen kan tillates, jf. § 8-1. Kommer retten til at innhentingen var urettmessig, skal retten meddele dette til EOS-utvalget og pålegge Etterretningstjenesten å slette innhentet informasjon.

11.11.4.5 Tillatelsens varighet

Etter departementets syn bør retten i den enkelte sak vurdere og ta stilling til varigheten av tillatelsen. Hovedregelen bør være at tillatelsen ikke skal vare lenger enn nødvendig. Dessuten tilsier personvernhensyn at det oppstilles en yttergrense for tillatelsens varighet, som retten ikke kan gå utover. Departementet foreslår at den maksimale varigheten settes til ett år når søket gjelder målsøking og seks måneder når søket gjelder målrettet innhenting. Når en tillatelse har løpt ut eller er i ferd med å løpe ut, må Etterretningstjenesten fremme en ny begjæring hvis den ønsker å gjenoppta eller fortsette søket.

Selv om det for så vidt allerede må sies å følge av lovens system, foreslår departementet av pedagogiske grunner å lovfeste at Etterretningstjenesten skal avslutte pågående søk av eget tiltak dersom vilkårene ikke lenger er til stede. Det kan for eksempel være tilfelle hvis nye faktiske omstendigheter gjør at inngrepet ikke lenger kan regnes som forholdsmessig.

Departementet foreslår følgende regulering av tillatelsens varighet:

§ 8-6 *Varighet*

Rettens tillatelse etter § 8-1 skal ikke gis for lengre tid enn nødvendig. Tillatelsen kan ikke overstige ett år når innhentingen gjelder målsøking og seks måneder når innhentingen gjelder målrettet innhenting.

Etterretningstjenesten skal avslutte pågående innhenting dersom vilkårene etter loven her ikke lenger er til stede.

11.12 Styrket kontroll av Etterretningstjenestens bruk av tilrettelagt innhenting

11.12.1 Innledning

Lysne II-utvalget understreket i sin rapport behovet for effektiv og uavhengig kontroll av Etterretningstjenestens innsamling, lagring og bruk av grenseoverskridende elektronisk kommunikasjon. Utvalgets anbefaling om å innføre et digitalt grenseforsvar ble blant annet gitt under forutsetning av en løpende og uavhengig kontroll i nær sanntid. Lysne-utvalget foreslo at denne skulle utføres av et eget forvaltningsorgan – DGF-tilsynet.[271]

Departementet har vurdert alle sider av Lysne II-utvalgets rapport på nytt, derunder også anbefalingen om at det etableres en løpende kontroll av systemet for tilrettelagt innhenting. Departementet har kommet til at det er behov for en styrket kontroll. Et spørsmål for departementet har vært om Lysne II-utvalgets forslag er den beste kontrollmodellen, eller om man bør anbefale en annen løsning. Departementet mener også det er nødvendig å analysere innholdet i kontrolloppgaven nærmere. Dette vil drøftes nærmere i det følgende.

11.12.2 Lysne II-utvalgets forslag og innspill fra høringsrunden

Lysne II-utvalget understreket behovet for god kontroll. Det avgjørende er at tiltakene samlet sett er troverdige, og at ordningene på en betryggende måte ivaretar både hensynet til

[271] Lysne II-utvalgets rapport om digitalt grenseforsvar av 26. august 2016 punkt 9.3.3 s. 59

Etterretningstjenestens oppgaveløsning og hensynet til personvern og kommunikasjonsvern. Lysne II-utvalget foreslo at DGF-tilsynets oppgaver burde være som følger:

> «DGF-tilsynet skal:
>
> I nær sanntid motta all informasjon om alle søk som gjøres i alle datasamlinger i DGF-systemet, motta alle avgjørelser fra DGF-domstolen, ha tilgang til all informasjon om hvordan filtrene er implementert og konfigurert, og ha tilgang til all informasjon om hvordan interne retningslinjer og avgjørelser fra domstolen er oversatt til søkeprivilegier.
>
> Rapportere avvik til EOS-utvalget og for øvrig rapportere regelmessig til EOS-utvalget, Forsvarsdepartementet og Samferdselsdepartementet. Avvik vil i denne sammenheng være bruk av DGF-systemet som ikke er hjemlet i E-loven, domstolens avgjørelser, eventuelle forskrifter og interne retningslinjer.
>
> Føre tilsyn med at datasikkerheten i DGF-systemet er så høy som teknologisk og praktisk mulig.»

Lysne II-utvalget vurderte at det *antakelig* vil være uhensiktsmessig å legge kontrollen av Etterretningstjenestens bruk av tilrettelagt innhenting til EOS-utvalget på grunn av dets parlamentariske oppheng og lovregulerte oppdrag om *etterfølgende* kontroll. Utvalget anbefalte derfor at et DGF-tilsyn burde opprettes som et eget forvaltningsorgan.

Lysne II-utvalget foreslo å organisere DGF-tilsynet under Samferdselsdepartementet på grunn av tilretteleggingsplikten for teletilbydere i Norge, og fordi innhenting av grenseoverskridende elektronisk kommunikasjon berører kommunikasjonsfriheten. Man foreslo videre at det administrative forvaltningsansvaret for tilsynets virksomhet kunne delegeres til Nasjonal kommunikasjonsmyndighet (Nkom). Etter Lysne II-utvalgets syn burde kontrollen underlegges et annet departement enn Forsvarsdepartementet for å sikre uavhengighet av statsråden med konstitusjonelt ansvar for Etterretningstjenestens virksomhet.

EOS-utvalgets høringsuttalelse til Lysne II-rapporten utfordrer flere sider ved rapportens anbefalinger. For det første peker EOS-utvalget på at opprettelsen av et DGF-tilsyn vil innebære at EOS-utvalgets kontroll av denne metoden blir indirekte. Videre påpeker EOS-utvalget at all rapportering fra DGF-tilsynet til EOS-utvalget til en viss grad vil måtte baseres på et skjønn, særlig med tanke på hva som vurderes å utgjøre et avvik. En konsekvens av dette vil kunne være at skjønnsutøvelsen av hva som er et avvik, og som dermed rapporteres videre til EOS-utvalget, vil være unntatt parlamentarisk kontroll, med mindre EOS-utvalgets kontrolloppgave utvides til også å gjelde DGF-tilsynet. Hva angår Lysne II-utvalgets begrunnelse for ikke å legge DGF-tilsynets oppgaver til EOS-utvalget, anser EOS-utvalget at det ikke «er klart at EOS-utvalgets parlamentariske forankring som uavhengig kontrollutvalg oppnevnt av Stortinget, samt etterfølgende kontroll, er omstendigheter som gjør EOS-utvalget uegnet til å utføre oppgavene som foreslås gitt til et eventuelt DGF-tilsyn.» EOS-utvalget mener også at opprettelsen av et DGF-tilsyn med oppgave å føre tilsyn med at virksomheten drives i henhold til lov, vil medføre dublering av teknisk og juridisk kompetanse.

Nasjonal sikkerhetsmyndighet (NSM) støtter Lysne II-utvalgets anbefaling om at systemet bør underlegges kontrollmekanismer, men foreslår at EOS-utvalget styrkes fremfor at det etableres et nytt organ i form av et DGF-tilsyn. Dette anses som mer hensiktsmessig for å forhindre spredning av sensitiv informasjon til flere enn strengt nødvendig.

Nasjonal kommunikasjonsmyndighet (Nkom) viser til Lysne II-utvalgets forslag om at de kan tillegges det administrative forvaltningsansvaret for virksomheten til et DGF-tilsyn. Nkom har i dag som oppgave å sikre kommunikasjonsvernet, både i form av krav overfor tilbyderne av elektronisk kommunikasjon når det gjelder sikkerhet og stabilitet i nett- og tjenester, og som tilsynsmyndighet overfor teletilbydernes etterlevelse av sletteplikt og taushetsplikt etter ekomregelverket. På denne bakgrunn anser Nkom at de har kompetanse til å påta seg en tilsynsoppgave for staten tilknyttet Etterretningstjenestens aksess til grenseoverskridende elektronisk kommunikasjon. Nkom påpeker at gjennomføringen av eventuelle tilsynsoppgaver vil forutsette tilføring av tilstrekkelige ressurser.

11.12.3 Menneskerettslige krav

Departementet har vurdert hvorvidt det kan utledes særskilte menneskerettslige krav til denne formen for kontroll med strategisk utenlandsetterretning. Den europeiske menneskerettsdomstolen (EMD) har den senere tid avsagt to kammerdommer der kontrollen med bulkinnsamling av grenseoverskridende elektronisk kommunikasjon behandles.[272] Dommene understreker viktigheten av tilstrekkelige og uavhengige kontrollmekanismer for å beskytte mot myndighetsmisbruk, og angir hvilke forutsetninger som gjelder for at et bulkinnsamlingssystem og dets kontrollmekanismer skal være i samsvar med EMK. Kravene kan i korte trekk oppsummeres som følger:

- Systemet må være utformet og opereres i henhold til seks konkrete minimumskrav utmeislet i EMDs praksis;
- Kontrollmekanismene må balansere hverandre; og
- Eksistensen eller fraværet av faktiske tilfeller av misbruk må tas i betraktning ved vurderingen av om tiltaket oppfyller menneskerettighetenes krav.

Dommene etterlater inntrykket av at EMD foretar en grundig og utpreget konkret vurdering av det enkelte etterretningsregimet, og det er tydelig at domstolen vektlegger helheten i systemet fremfor enkeltelementer. Departementet oppfatter at domstolen ikke stiller detaljerte krav til *organiseringen* av kontrollmekanismene, men til *kvaliteten* av den kontrollen som føres. Ulike land har innrettet sin utenlandsetterretningsvirksomhet med tilhørende kontrollsystemer på ulike måter. Det har derfor lite for seg å påberope at enkeltkomponenter i ett lands system skal være påkrevet i et annet lands system, fordi balanseringen av kontrollmekanismene kan ha vært gjort på en annen måte.

Videre vektlegger domstolen hensynet til *uavhengige* kontrollinstanser tungt. Uavhengighet kombinert med faglig integritet og kompetanse er viktige faktorer for å sikre en god kvalitativ kontroll og ikke minst tillit i befolkningen til at kontrollen utføres på en god måte.

Lovforslaget her tar utgangspunkt i de overnevnte vilkårene som er utviklet i EMDs praksis. Den løpende kontrollen vil utgjøre ett av flere kontrollelementer. Dette er nærmere beskrevet i høringsnotatet kapittel 4 og punkt 11.8.2.

[272] *Big Brother Watch m. fl. mot Storbritannia* avsagt 13. september 2018 og *Centrum för rättvisa mot Sverige* avsagt 19. juni 2018. Ingen av dommene er når dette skrives rettskraftige, men begge domsavsigelsene bygger på etablert praksis.

11.12.4 Hva består kontrolloppgaven i og hva er formålet med denne – enkelte presiseringer

11.12.4.1 Innledning

Departementet mener det er nødvendig å ha klart for seg hva *kontrolloppgaven* skal bestå i. Lysne II-rapporten beskriver dette nokså kortfattet. Det er dermed behov for å belyse nærmere hva som skal kontrolleres og kontrollens formål før man kan vurdere hvilket organ som vil være best egnet til å utføre kontrollen. Før en slik drøftelse er det nødvendig med enkelte presiseringer.

11.12.4.2 Presiseringer

Som det fremgår over mener departementet at det er behov for en mer intensivert kontroll med systemet for tilrettelagt innhenting enn kontrollen som føres med Etterretningstjenestens øvrige virksomhet, og støtter seg til Lysne II-utvalgets uttalelser om dette. Departementet mener imidlertid at Lysne II-rapporten i for liten grad drøfter fordeler og ulemper med den kontrollmodellen som anbefales, og savner en nærmere problematisering av hvordan en slik løsning vil slå ut i praksis. Flere viktige spørsmål er ikke berørt, slik også høringsinnspillene til rapporten viser. Grensesnittet mot andre aktører, slik som EOS-utvalget, er ikke utredet nærmere. Utvalget vurderte ikke konsekvensen av at både Nkom og Samferdselsdepartementet er potensielle brukere av etterretningsinformasjon og kan formulere oppdrag til Etterretningstjenesten.[273] De sikkerhetsmessige konsekvenser knyttet til kontrolloppgavens omfang, altså hvor mye av Etterretningstjenestens aktivitet kontrollmyndigheten må få innsyn i for å kunne føre en god kontroll, er heller ikke problematisert. Rapporten tar videre ikke stilling til mulige uheldige konsekvenser av at kontrollmyndigheten kan bli sittende for «tett på» Etterretningstjenesten, og dermed miste den nødvendige distansen til kontrollobjektet. Departementet mener alle disse faktorene må undersøkes nærmere. Det førende aspekt må i alle tilfeller være at den kontroll som utøves holder høy kvalitet og har en fornuftig innretning.

11.12.4.3 Kontrolloppgaven

Slik departementet leser Lysne II-rapporten mener utvalget at den løpende kontrollen skal begrenses til å etterse at Etterretningstjenestens speiling og filtrering av informasjon utføres i henhold til lovens krav og at tjenesten bare utfører de søk som er tillatt i henhold til rettens kjennelser. Dette inkluderer en kontroll av hvordan avgjørelsene fra domstolen er omsatt i søkekriterier. Mer konkret forstår departementet Lysne II-rapporten dithen at tilsynet skal kontrollere:

- Hva som *samles inn* i alle datalagre – dvs. hva som filtreres bort, hva som samles inn uselektert (i bulk) og hva som samles inn selektert (innholdsdata)
- Hva det *søkes etter* i datalagrene – dvs. hvilke type spørringer som gjennomføres, at det ikke gjennomføres spørringer i data som domstolen ikke har godkjent, mv.
- At det tekniske arbeidet med testinnhenting og testanalyser av trafikk og nett (korttidslageret) ikke brukes for etterretningsformål

Lysne II-rapporten omtaler i liten grad kontroll med selve speilingen og hvordan tilretteleggingsplikten utøves fra tjenestetilbydernes side. Departementet mener at også denne virksomheten må underlegges tilstrekkelig kontroll. Noen må kontrollere at tjenesteleverandørene tilrettelegger og speiler den kommunikasjonen de er pålagt å speile, verken mer eller mindre. Etter departementets syn bør det herunder sikres uavhengig

[273] RFI-prosessen er nærmere beskrevet under punkt 6.3.3.

kontroll med at de kommunikasjonslinker som omfattes av tilretteleggingsplikten ikke kun inneholder ren norsk til norsk kommunikasjon. Det samme gjelder kontroll med at tilretteleggingen ikke medfører «bakdører» som andre kan utnytte, men at tilretteleggingen gjennomføres på en måte som ivaretar forsvarlig sikkerhet.

11.12.4.4 Formål

Lysne II-rapporten legger stor vekt på at innhentingen er underlagt effektive og uavhengige kontrollmekanismer som utfyller hverandre. Departementet slutter seg til at en effektiv kontroll har en viktig tillitsskapende funksjon. Vissheten om at Etterretningstjenesten blir *tilnærmet løpende* kontrollert av et kompetent kontrollorgan vil bidra til å motvirke eventuelle mistanker om at tjenesten eller dennes ansatte ikke følger lovens krav eller domstolens kjennelser. Tidsaspektet står etter departementets syn frem som et sentralt moment i Lysne II-rapportens anbefaling. Alle aspekter knyttet til systemet for tilrettelagt innhenting faller jo innenfor EOS-utvalgets kontrolloppgave etter EOS-kontrolloven, og vil dermed være gjenstand for etterfølgende kontroll. Departementet mener derfor at en viktig funksjon ved kontrollen må være at eventuelle avvik kan avdekkes, følges opp og stanses relativt raskt.

En annen viktig forutsetning er at formålet med kontrollen må være en ren *etterlevelsesvurdering* basert på den tekniske anvendelsen av systemene, og ikke en godhetsvurdering knyttet til søkene som utføres. Godhetsvurderingen, altså en vurdering av om søket skal tillates, er ivaretatt av domstolene i rettens kjennelse. Det blir ikke riktig om kontrollmyndigheten skal overprøve rettens vurdering. Spørsmål knyttet til hvordan Etterretningstjenesten har tolket en kjennelse og beveggrunnene bak et konkret søk faller på sin side klart innenfor EOS-utvalgets kontrolloppgave etter EOS-kontrolloven. Informasjon fra tilrettelagt innhenting vil bare være én av mange informasjonskilder for Etterretningstjenesten. Begrunnelsen for hvorfor et søk gjennomføres på en særskilt måte vil derfor ofte måtte forklares med henblikk til annen informasjon som tjenesten besitter. Det er EOS-utvalget som på samfunnets vegne har fullt innsyn og tilgang til Etterretningstjenestens virksomhet og som dermed har kompetanse og innsikt til å vurdere slike vurderinger i sin fulle tyngde.

11.12.4.5 Særlig om avvikshåndtering

Lysne-II utvalget anbefalte at kontrollmyndigheten «ved mistanke om avvik, skal rapportere dette umiddelbart til EOS-utvalget, som vil vurdere oppfølgingstiltak i tråd med de fullmakter som EOS-utvalget besitter, og rapportere til Stortinget i tråd med etablert praksis.»[274] Organet var derfor ikke tiltenkt myndighet til å stanse virksomhet eller offentlig kritisere Etterretningstjenesten for brudd på regelverket. Departementet vil bemerke at heller ikke EOS-utvalget har myndighet til å beordre stans i innhenting. Dette har sammenheng med EOS-utvalgets organisatoriske oppheng, og er gjort nærmere rede for i høringsnotatet 4.3.6.3. Det er kun forsvarssjefen som etatssjef og Forsvarsdepartementet i kraft av å være ansvarlig departement, som kan gi pålegg til Etterretningstjenesten med bindende virkning.

11.12.4.6 Begrepet «tilsyn»

Departementet finner i forlengelsen av punktet over et behov for å kommentere Lysne II-utvalgets forslag til navn på kontrollmyndigheten, nemlig «DGF-tilsynet». Departementet foreslår å gå bort fra begrepet «DGF» og dette videreføres derfor ikke. Departementet mener dessuten at begrepet «tilsyn» er et mindre godt begrep fordi man ikke foreslår at

[274] Lysne II-utvalgets rapport om digitalt grenseforsvar av 26. august 2016, s. 59

kontrollmyndigheten skal kunne sanksjonere avvik. Et alminnelig forvaltningstilsyn vil litt forenklet ha to overordnede oppgaver; den ene er å følge med på tilsynsobjektets regelverksetterlevelse, den andre er å reagere der regelverket ikke følges. Dette innebærer at et forvaltningstilsyn normalt vil følge opp avvik med en nødvendig reaksjon, det være seg veiledning, pålegg om oppretting, stansing av virksomheten, bøter eller andre tiltak for å sikre at kravene overholdes. «DGF-tilsynet» er ikke tiltenkt slik sanksjonsmulighet, men skal rapportere avvik til EOS-utvalget og overordnet myndighet. Departementet mener derfor betegnelsen «kontrollmyndighet» er et mer dekkende begrep og benytter dette i drøftelsene her.

11.12.5 Sentrale hensyn i vurderingen

11.12.5.1 Innledning

Departementet mener det er grunn til å løfte frem noen grunnleggende hensyn som bør tillegges vekt i vurderingen av både hvordan kontrolloppgaven bør innrettes, og valget av kontrollmyndighet.

11.12.5.2 Den norske kontrollmodellen

Et sentralt spørsmål er hvordan opprettelsen av et forvaltningsorgan med oppgave å kontrollere deler av Etterretningstjenestens informasjonsinnhentingsvirksomhet passer inn i den kontrollmodellen som Stortinget har valgt i saker som gjelder rikets sikkerhet og kontroll med EOS-tjenestene. Den norske kontrollmodellen er nylig vurdert og enstemmig opprettholdt i forbindelse med Stortingets evaluering av EOS-utvalget.[275] Modellen er rendyrket. Dette kommer blant annet til syne ved at andre tilsynsorganer, som kanskje i prinsippet kunne ha tilført økt fagkontroll innenfor sine ansvarsområder, har fått sitt mandat avgrenset i forhold til EOS-utvalgets mandat. Dette gjelder blant annet for Kontrollutvalget for kommunikasjonskontroll og Datatilsynet. Konsekvensene ved å gjøre avvik fra den valgte kontrollmodellen er usikre, men departementet viser til at også PST og NSM behandler kommunikasjonsdata fra henholdsvis kommunikasjonskontroll og utplasserte sikkerhetssensorer. Dersom man velger en særskilt kontrollmyndighet for tilrettelagt innhenting, kan det argumenteres for at samtlige EOS-tjenester bør underlegges slik kontroll. Departementet utelukker heller ikke at en slik løsning kan generere påtrykk om kontroll fra andre fagområder, dersom man først åpner for avvik fra den kontrollmodellen som det hittil har vært bred enighet om.

11.12.5.3 Sikkerhetshensyn

Den norske kontrollmodellen er blant annet begrunnet i sikkerhetsmessige hensyn. EOS-tjenestene forvalter et særlig ansvar for rikets sikkerhet, og besitter store mengder svært sensitiv og høygradert informasjon. Etterretningstjenesten besitter også betydelige mengder sensitiv og høygradert informasjon fra etterretningstjenester i andre land. Av hensyn til rikets sikkerhet, og av hensyn til å redusere sårbarheten for at informasjonen kompromitteres, anses det som nødvendig at færrest mulig personer har tilgang til slik høygradert informasjon. At man har samlet kontrollen med EOS-tjenestene og lagt denne oppgaven til *ett* organ er dermed fornuftig i et sikkerhetsperspektiv. Sikkerhetsmessige hensyn er et særlig vektig argument i valg av kontrollaktør.

[275] Dokument 14 (2002–2003). Rapport til Stortinget fra utvalget til å utrede Stortingets kontrollfunksjon og Dokument 16 (2015–2016) Rapport til Stortinget fra Evalueringsutvalget for Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste, se særlig side 37–39.

11.12.5.4 Praktiske hensyn og distanse til kontrollobjektet

Kontrolloppgavens omfang har betydning for hvor mange årsverk myndigheten vil bestå av. Det er anslått at oppgaven vil sysselsette ca. 4 personer på årlig basis. Etterlevelseskontrollen må i stor utstrekning foretas i Etterretningstjenestens lokaler, i tillegg til hos ekomtilbyderne. Personene må være klarert for høyeste sikkerhetsgrad og kan av hensyn til sakenes gradering og sensitivitet ikke inngå i et større kompetansemiljø, med mindre det øvrige kompetansemiljøet har samme sikkerhetsklarering og autorisasjoner. Man kan av samme hensyn heller ikke basere seg på rotasjon av personell.

11.12.5.5 Klare ansvarslinjer

Flere kontrollmyndigheter kan utfylle og balansere hverandre og således skape en god kontrolldynamikk. Det kan også virke disiplinerende for kontrollobjektet å bli møtt med ulike vinklinger fra de kontrollerende myndigheter. Flere kontrollmyndigheter med ulike organisatoriske oppheng kan samtidig skape uklare ansvarsgrenser, rapporteringslinjer og risiko for forsinkelser i kontrollarbeidet. Dersom det foreligger uenighet mellom kontrollmyndighetene kan dette svekke effektiviteten og ikke minst tilliten til kontrollen som sådan. Særlig på et område som utenlandsetterretning, der kontrollmyndigheten får innsyn i Etterretningstjenestens virksomhet på samfunnets vegne, er denne tilliten helt nødvendig, fordi offentligheten som regel ikke kan gis innsyn i fakta. Det vil ikke være mulig å «spille med åpne kort» i en eventuell offentlig debatt om hvem som har «rett» i en eventuell disputt mellom kontrollmyndighetene, fordi tematikken vil være sikkerhetsgradert.

11.12.6 Hvilke alternativer foreligger?

11.12.6.1 Innledning

Uansett organisering må kontrollmyndigheten som en statlig virksomhet ha et organisatorisk oppheng for å sikre administrativ og økonomisk oppfølging, budsjettmessige tildelinger osv. Dette kan løses på ulike måter. Det vil også være mulig å justere kontrolloppgaven sett i forhold til Lysne II-utvalgets forslag, i innskrenkende eller utvidende retning. Dette kan ha betydning for hvilke alternativer som er aktuelle. Alternativene beskrevet nedenfor kan i prinsippet kombineres og ett alternativ utelukker ikke nødvendigvis et annet.

11.12.6.2 Forvaltningsorgan

Lysne II-utvalget mente kontrolloppgaven burde ligge til forvaltningsdelen av maktfordelingstrekanten, men under et annet departement enn Forsvarsdepartementet for å skape avstand til forsvarsministeren som har det konstitusjonelle ansvaret for Etterretningstjenesten. Lysne II-utvalget foreslo et forvaltningsorgan som kunne legges under Samferdselsdepartementet og der man kunne delegere det administrative forvaltningsansvaret for tilsynets virksomhet til Nkom. Det vises til beskrivelsen av Lysne II-utvalgets forslag i punkt 11.12.2.

Andre organisatorisk oppheng i forvaltningen kan også tenkes. I Norge har vi ministerstyre og dermed ingen tradisjon for å legge forvaltningsorganer direkte under regjeringen, slik man har i for eksempel Sverige.[276] En forvaltningsmessig organisering medfører derfor at kontrollmyndigheten må være administrativt underlagt et departement.

[276] I svensk rett foretas kontrollen av *Statens inspektion för försvarsunderrättelseverksamhet* (SIUN) som er direkte organisert under regjeringen. SIUN er ekvivalenten til det norske EOS-utvalget og foretar også den etterfølgende kontrollen av det svenske systemet for bulkinnhenting av elektronisk kommunikasjon.

11.12.6.3 Uavhengig kontrollorgan

Alternativt kan det tenkes et særskilt kontrollorgan utnevnt av Kongen bestående av spesielt utpekte og uavhengige personer, for eksempel ledet av en dommer.

På strafferettens område er det etablert et eget *Kontrollutvalg for kommunikasjonskontroll* med hjemmel i straffeprosessloven § 216 h.[277] Kontrollutvalget er sikret formell og reell uavhengighet i lov og organisatorisk oppheng, og kan tjene som modell for et mulig uavhengig kontrollorgan.

Kontrollutvalget utnevnes av Kongen og skal bestå av minst tre medlemmer. Lederen for utvalget skal oppfylle de krav som stilles til høyesterettsdommere. Utvalget skal kontrollere at de opplysningene som politiet har fått ved kommunikasjonskontroll, romavlytting eller dataavlesing bare blir brukt på lovlig måte, og at lovens regler om oppbevaring og tilintetgjøring av materiale blir fulgt. Utvalget skal også påse at bestemmelsene om taushetsplikt blir etterfulgt. Utvalget kan ikke bestemme at løpende kommunikasjonskontroll skal avbrytes, men kan gi pålegg om internkontroll og informasjonssikkerhet, jf. politiregisterloven § 15 og § 16. For andre forhold som er gjenstand for kontroll kan utvalget kun gi anmerkning.

Kontrollutvalget vurderer innberetninger og rapporter som politimestrene oversender til riksadvokaten i henhold til kommunikasjonskontrollforskriften § 10. I tillegg undersøker de enhver klage fra enkeltpersoner eller organisasjoner som mener seg urettmessig utsatt for kommunikasjonskontroll. Utvalget kan for øvrig av eget tiltak ta opp enhver sak eller ethvert forhold i tilknytning til politiets og påtalemyndighetens bruk av kommunikasjonskontroll, romavlytting og dataavlesing som det finner grunn til å behandle. Utvalget skal herunder særlig legge vekt på forhold som har vært gjenstand for offentlig omtale eller kritikk.

Kontrollutvalget utfører *ikke* kontroll med saker som omfattes av lov om kontroll med etterretnings-, overvåknings- og sikkerhetstjenesten (EOS-loven), jf. straffeprosessloven § 216 h første ledd annet punktum. Begrensningen i kontrolloppgaven begrunnes slik i straffeprosesslovens forarbeider:[278]

> «Behandlingen av saker om rikets sikkerhet er underlagt en generell kontroll av et eget kontrollutvalg etter lov om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste. Kontrollen gjelder også bruken av kommunikasjonskontroll. Det er dermed ikke behov for at kontrollutvalget for saker om kommunikasjonskontroll skal føre kontroll med sakene om rikets sikkerhet. Departementet foreslår derfor at saker som omfattes av lov om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste, unntas fra kontrollen etter § 216h, se *nytt annet punktum i første ledd.* Forslaget er i samsvar med Metodeutvalgets forslag.»

11.12.6.4 Kontrolloppgaven legges til EOS-utvalget

EOS-utvalget er et av Stortingets kontrollorganer. Utvalget utfører imidlertid sitt verv selvstendig og uavhengig av Stortinget, jf. EOS-kontrolloven § 1 femte ledd.[279] At Lysne II-utvalget ikke foreslo å legge den løpende kontrollfunksjonen til EOS-utvalget forklares med at dette *antakelig* ville være uhensiktsmessig, gitt EOS-utvalgets oppheng og lovregulerte oppdrag om etterfølgende kontroll. Spørsmålet er dermed om konstitusjonelle aspekter eller

[277] Nærmere bestemmelser er nedfelt i forskrift av 9. september 2016 om kommunikasjonskontroll, romavlytting og dataavlesing (kommunikasjonskontrollforskriften)

[278] Ot. prp. nr. 64 (1998-1999)

[279] EOS-utvalget er nærmere beskrevet i dette høringsnotatet punkt 6.7

prinsippet om etterfølgende kontroll er til hinder for at EOS-utvalget kan foreta den løpende kontrollen.

I vurderingen av de konstitusjonelle aspekter må man ta utgangspunkt i at den norske modellen for kontroll med EOS-tjenestene bygger på et system med kontrollelementer innenfor alle statsmaktene, der det parlamentarisk oppnevnte EOS-utvalget utøver en kjernefunksjon. Spørsmålet om Stortingets virksomhet på forvaltningens område, herunder EOS-utvalgets kontroll, har blitt problematisert og evaluert av ulike ekspertutvalg. Departementet nøyer seg med å vise til ekspertutvalgenes rapporter for mer inngående drøftelser av denne og relaterte problemstillinger.[280]

Prinsippet om etterfølgende kontroll, herunder at EOS-utvalget ikke skal ha en styringsfunksjon overfor forvaltningen eller brukes til konsultasjoner av tjenesten, var en sentral forutsetning ved etableringen av EOS-utvalget. Prinsippet kommer til uttrykk i EOS-kontrolloven § 2 tredje ledd, der det heter at formålet med kontrollen er «rent kontrollerende», at utvalget «skal følge prinsippet om etterfølgende kontroll» og at utvalget ikke kan «instruere de kontrollerte organer, eller nyttes av disse til konsultasjoner». Mangelen på instruksjonsmyndighet innebærer at det er Etterretningstjenesten, forsvarssjefen som etatssjef eller Forsvarsdepartementet som ansvarlig departement, som i første instans må avgjøre om EOS-utvalgets syn skal følges, og til syvende og sist ved behandlingen i Stortinget. Bestemmelsens formål er således å forhindre at EOS-utvalgets kontroll blir så inngripende at regjeringens og fagdepartementenes styringsmulighet- og ansvar blir vesentlig svekket.[281]

Prinsippet om etterfølgende kontroll innebærer imidlertid ikke at EOS-utvalget er forhindret fra å foreta løpende kontroll av forvaltningen. Dette følger uttrykkelig av EOS-kontrolloven § 2 tredje ledd siste punktum, hvor det heter at utvalget også kan kreve innsyn i og uttale seg om løpende saker. Evalueringsutvalget uttaler på side 123 i sin rapport at:

> «… prinsippet om etterfølgende kontroll ikke [bør] være til hinder for at EOS-utvalget kontrollerer og uttaler seg om løpende saker. […] Etter Evalueringsutvalgets syn bør prinsippet […] først og fremst få som konsekvens at kontrollen med de enkelte beslutninger og disposisjoner i pågående saker skal skje i etterkant, og at utvalget ikke skal forhåndskonsulteres eller gi råd om fremtidige beslutninger eller handlinger. Prinsippet medfører heller ingen begrensning i EOS-utvalgets rett til innsyn i pågående saker. Slikt innsyn er en forutsetning for at utvalget skal kunne avdekke pågående krenkende virksomhet. Ansvaret for eventuelle krenkelser som alt er begått vil imidlertid forbli hos statsråden.»[282]

I EOS-kontrollovens forarbeider er det forutsatt at:[283]

> «kontrollorganet skal utføre en rettssikkerhetskontroll som i prinsippet skal være etterfølgende og skilt fra styringsfunksjonen. Man er imidlertid enig med kommisjonen i at en viss samtidighet må aksepteres fordi enkelte saker løper over lang tid.»

[280] Se blant annet Evalueringsutvalgets rapport i Dokument 16 (2015–2016)

[281] Ibid s. 122

[282] Ibid s. 123

[283] Ot.prp. nr. 83 (1993–1994) s. 12

Det presiseres samme sted at kontrollen bør være både formell og materiell, men at kontroll av tjenestenes skjønnsutøvelse må utøves med forsiktighet. Kritikk av skjønnsutøvelse som ligger innenfor rimelighetens rammer, må unngås.

11.12.7 Departementets vurdering av alternative kontrollmyndigheter

11.12.7.1 Innledning

Som det fremgår er det flere måter å innrette den løpende kontrollen på. Å legge kontrolloppgaven til et forvaltningsorgan er ett alternativ. Departementet vil bemerke at et forvaltningsorgan underlagt Forsvarsdepartementet trolig ville sikre raskest oppfølging av eventuelle avvikssaker fordi Forsvarsdepartementet kan instruere Etterretningstjenesten og beordre stans i innhenting, og dermed sørge for at eventuelle regelbrudd opphører. Organet kan sikres faglig og faktisk uavhengighet i lov. Departementet ser imidlertid at en slik organisering *utad* kan fremstå som for lite uavhengig, noe som vil gå ut over tilliten til kontrollordningen. Dessuten vil man i sakene hvor det foreligger faktiske eller rettslige uklarheter uansett måtte gå i dialog med Etterretningstjenesten samt ønske å avvente EOS-utvalgets vurderinger og konklusjoner. Til tross for at departementet mener et forvaltningsorgan underlagt Forsvarsdepartementet kunne utført en materielt god kontroll og der man kunne sikre relativt rask avvikshåndtering, vil ikke departementet forfølge dette forslaget videre i høringsnotatet her.

Departementet utelukker ikke at man kan opprette et uavhengig kontrollorgan, gjerne ledet av representanter fra domstolen, som kan føre kontroll med at Etterretningstjenesten etterlever materielle, prosessuelle og personelle regler for tilrettelagt innhenting. En slik kontroll vil imidlertid måtte bygge på Etterretningstjenestens rapportering og dermed bære preg av å være en formell legalitetskontroll. Dersom man skulle opprette et uavhengig utvalg som skulle utføre kontroller i Etterretningstjenestens lokaler vil man raskt ende opp med å duplisere EOS-utvalgets oppgave og funksjon. Dette anses lite hensiktsmessig og departementet vil derfor ikke foreslå en slik løsning.

Departementet mener det er grunn til å understreke at den norske modellen for kontroll med etterretnings- overvåknings- og sikkerhetstjeneste bygger på grunnpilaren om at det er EOS-utvalget som på samfunnets vegne foretar kontrollen med sakene om rikets sikkerhet. Man fant ikke grunn til gjøre unntak fra denne hovedregelen i saker om kommunikasjonskontroll, som er et meget inngripende tiltak. En oppfatning av at EOS-utvalgets oppheng skulle tilsi at utvalget ikke kan foreta den løpende kontrollen med tilrettelagt innhenting bygger på forutsetningen om at tilrettelagt innhenting er noe *prinsipielt annet* enn den aktivitet EOS-tjenestene ellers bedriver. Departementet finner ingen slike prinsipielle grunner som taler for at kontrollen med tilrettelagt innhenting krever en annen organisatorisk forankring. At EOS-utvalget er et kontrollorgan under Stortinget er derfor etter departementets syn ikke til hinder for å legge kontrolloppgaven dit. Som det fremgår av redegjørelsen over utgjør heller ikke prinsippet om etterfølgende kontroll en slik hindring.

Departementet har vurdert spørsmålet nøye og anbefaler at den løpende kontrolloppgaven tillegges EOS-utvalget. Departementet har lagt særlig vekt på at EOS-utvalget har de beste forutsetningene for å drive legalitetskontroll av Etterretningstjenestens virksomhet. Kontrollen bør etter departementets syn ikke bare begrenses til rent tekniske forhold, men se på alle deler av Etterretningstjenestens innhentingsaktivitet. Anbefalingen utdypes nærmere i det følgende.

11.12.7.2 Nærmere om departementets anbefaling

Den norske kontrollmodellen

Det er departementets klare oppfatning at *den norske kontrollmodellen* bør opprettholdes. EOS-utvalget er parlamentarisk forankret, det kontrollerer alle EOS-tjenestene, har dyp innsikt i alle sidene av EOS-tjenestenes aktivitet og modellen er rendyrket. Det kan hevdes at tilrettelagt innhenting er en ordning som har et så spesielt kontrollbehov at EOS-utvalget ikke bør føre kontrollen alene, og at et unntak fra den norske kontrollmodellen derfor er nødvendig i dette tilfellet. Det kan også anføres at det er et gode å spre kontrollansvaret på flere aktører, og at Lysne II-utvalgets anbefaling om å legge kontrolloppgaven til ekommiljøet i samferdselssektoren kan tilføre særskilt teknisk innsikt. Departementet vurderer imidlertid at den nødvendige tekniske innsikten kan oppnås gjennom å knytte til seg teknisk kompetent personell og gjennom kompetanseutvikling.

Videre vil departementet ikke utelukke at et unntak fra kontrollmodellen vil kunne åpne for et senere press om at også andre forvaltningstilsyn bør kontrollere EOS-tjenestene på sine fagområder. En slik utvikling vil på sikt kunne utfordre den norske kontrollmodellen som sådan. Dette vil være problematisk i et sikkerhetsperspektiv og departementet er ikke overbevist om at kontrollen vil bli bedre med en fragmentert modell. Departementet antar derfor at dette er en problemstilling Stortinget som lovgiver vil måtte vurdere nøye.

Et annet aspekt i vurderingen er at det vil være uheldig dersom et forslag om å legge den løpende kontrollfunksjonen til EOS-utvalget gir inntrykk av en redusert *kontrollambisjon* basert på at antallet kontrollmyndigheter vil være færre enn i Lysne II-utvalgets forslag. Det er viktig for departementet å understreke at kontrollambisjonen er minst like sterk som Lysne II-utvalgets, men at man legger grunnleggende vekt på at kontrollen skal være god og hensiktsmessig innrettet.

Man kan hevde at *flere kontrollaktører* vil føre til mer kontroll og at det derfor i seg selv er en fordel å spre kontrollansvaret på flere aktører. Departementet bemerker imidlertid at dette argumentet ikke har fått gjennomslag når det gjelder den øvrige kontrollen med EOS-tjenestene, og at argumentet heller ikke kan ilegges avgjørende vekt her. Det viktigste må etter departementets syn være at den løpende kontrollfunksjonen ivaretas på beste måte, og da kan antall kontrollmyndigheter ikke i seg selv være avgjørende.

Legalitetskontroll

Kontrollmyndighetens *kompetanse* er en annen viktig faktor. Kontrollen av tilrettelagt innhenting bør etter departementets skjønn, så langt det lar seg gjøre, bygges på allerede eksisterende kompetanse og innretninger.

EOS-utvalget har lang erfaring med å kontrollere Etterretningstjenesten. Utvalget og dets sekretariat har den senere tid styrket sin teknologiske kompetanse, blant annet gjennom opprettelse en egen teknologisk enhet i sekretariatet, og vil med lovforslaget måtte tilføres økte ressurser. Utvalget har dessuten mulighet for å knytte til seg sakkyndig bistand dersom de finner det nødvendig, jf. EOS-kontrolloven § 19. EOS-utvalget kjenner Etterretningstjenestens systemer godt, og har direkte tilgang til disse. Den beste kvalitative kontrollen med tilrettelagt innhenting forutsetter etter departementets syn full innsikt i hvorledes tjenesten jobber, hvilke systemer som benyttes til hvilke formål og hvordan etterretningsproduksjon foregår, hvordan målutvikling gjennomføres, hvilke etterretningsmål tjenesten jobber med, hvordan ulike informasjonsgrunnlag og metodebruken spiller sammen

og hvorledes data behandles i hele tjenesten. Nettopp hensynet til helhetsoversikten tilsier at EOS-utvalget vil være bedre egnet og ha størst kompetanse til å gjennomføre kontrollen.

Nkom, som Lysne II-utvalget foreslo kunne utføre kontrolloppgaven, fører i dag i all hovedsak kun tilsyn med virksomheter underlagt ekomloven og postloven, ikke med offentlige myndigheters utøvelse av sitt samfunnsoppdrag eller med hvordan offentlige myndigheter, herunder politiet, behandler data som stammer fra elektronisk kommunikasjon.[284]

Uavhengighet

Hensynet til *uavhengig* kontroll er et annet moment. Selv om et kontrollorgan kan sikres uavhengighet ved lov vil kontrollorganer som tilhører *ulike* deler av maktfordelingstrekanten utad fremstå som mer uavhengig enn organer som er underlagt samme statsmakt. Formelt og reelt uavhengige kontrollorganer er viktig både i et menneskerettslig perspektiv og av hensyn til befolkningens tillit til troverdige kontrollordninger. Det faktum at både Nkom og Samferdselsdepartementet er potensielle oppdragsgivere for Etterretningstjenesten, og at Etterretningstjenesten og Nkom samarbeider på enkelte områder, blant annet i rammen av Ekom sikkerhetsforum, blir ikke problematisert av Lysne II-utvalget. En slik dobbeltrolle ville etter departementets syn bli krevende å håndtere, både reelt og av hensyn til den nødvendige tillit utad.

Avvikshåndteringen

Spørsmålet om *avvikshåndtering* er beskrevet over. Det kan anføres at en kontrollmyndighet som skal sikre overholdelse av regelverket uten å ha kompetanse til å gjennomføre avvikshåndtering bare vil medføre en unødvendig byråkratisering av kontrollen av Etterretningstjenestens virksomhet, uten at det er klart at kontrollmyndigheten bidrar til å styrke den samlede kontrollen med tjenesten. Et eget forvaltningsorgan kan dermed fremstå som overflødig all den tid EOS-utvalget har avvikshåndtering som oppgave, og utvalgets gjennomføring fungerer etter sin hensikt. Vurderingen kan dessuten kreve inngående avveininger av teknisk, rettslig, etterretningsfaglig og samfunnsmessig karakter. Det innebærer at selv om kontrollmyndigheten raskt rapporterer et avvik, vil EOS-utvalget på vanlig måte måtte gå inn i alle aspekter ved avviket, som ellers be om utfyllende informasjon og/eller selv forestå ytterligere kontrolltiltak overfor Etterretningstjenesten for å klargjøre faktum mv., samt vurdere om sakens karakter tilsier varsling til Forsvarsdepartementet samt rask informasjon til Stortinget i form av særskilt melding. I de fleste tilfeller vil Etterretningstjenesten, som i dag, stanse en virksomhet så snart det blir klart at EOS-utvalget mener dette bør gjøres (selv om tjenesten skulle være uenig i EOS-utvalgets syn). Det er på den annen side ikke like klart at dersom kontrollmyndigheten varsler et mulig avvik til EOS-utvalget så vil dette umiddelbart innebære stansing (med mindre avviket skulle være så åpenbart at Etterretningstjenesten uansett ville ha stanset virksomheten av eget tiltak). Dette er fordi, som påpekt over, handlingen kan være begrunnet i andre deler av Etterretningstjenestens aktivitet, som kontrollmyndigheten ikke har innsyn i.

Sikkerhet

Departementet vil understreke betydningen av *sikkerhetsmessige forhold* i valget av kontrollmyndighet. Hensynet til nasjonal sikkerhet taler etter departementets syn mot at et nytt organ gis innsikt i høygradert og ekstremt sensitiv informasjon om operasjoner,

[284] Nkom vil etter lovforslaget i alle tilfeller føre tilsyn med ekomtilbyderne, herunder hvorledes tilretteleggingsplikten etter lovforslaget gjennomføres.

etterretningsmål, kapasiteter og metoder hos Etterretningstjenesten. Dersom slik informasjon kommer på avveie vil det kunne få svært alvorlige skadefølger for landet. Jo flere personer som har tilgang til denne typen informasjon, jo større er sårbarheten for kompromittering og sannsynligheten for at noen utsettes for press fra ondsinnede aktører. Det er derfor et poeng i seg selv å forhindre slik eksponering i størst mulig grad. I høringsrunden til Lysne II-utvalgets rapport tok Nasjonal sikkerhetsmyndighet til orde for at den løpende kontrollen heller bør legges til EOS-utvalget. Også hensynet til internasjonale partneres tillit til samarbeid og utveksling av informasjon med Etterretningstjenesten tilsier at ytterligere organer ikke gis så omfattende innsyn i høygradert materiale som EOS-utvalget har.

Praktiske forhold

I forlengelsen av spørsmålet om sikkerhet mener departementet at også *praktiske* aspekter må tillegges vekt i vurderingen. Et organ med en begrenset kontrolloppgave som foreslått av Lysne II-utvalget vil måtte bestå av et lite antall personell klarert for høyeste sikkerhetsgrad, som vil måtte sitte tett på kontrollobjektet. Av skjermingshensyn vil personellet ikke kunne utveksle informasjon fra kontrollarbeidet i et kompetansemiljø, med mindre kompetansemiljøet har en lignende kontrolloppgave. Dette vil være tilfellet for EOS-utvalget, men ikke for et tilsyn som foreslått av Lysne II.

EOS-utvalget gjennomfører kontroll med alle sider av Etterretningstjenestens virksomhet, og planlegging og vurdering av resultatet av kontrollene kan drøftes i et større miljø med teknologisk, juridisk og samfunnsmessig kompetanse. Hvis en liten kontrollmyndighet får en tilnærmet fast plassering hos Etterretningstjenesten frykter departementet at kontrollmyndighetens personell kan risikere å assosiere seg med tjenestens virksomhet på en måte som vil svekke snarere enn styrke hensynet til uavhengig kontroll. Departementet antar at det vil være enklere for EOS-utvalget, gitt utvalgets størrelse, erfaring og geografiske plassering, å opprettholde den nødvendige distansen til kontrollobjektet.

Klare ansvarsforhold

Departementet vil understreke betydningen av *klare ansvarsforhold* og grensesnitt mellom aktørene. Dersom man velger et tosporet kontrollsystem er det grunn til å frykte uklare grensesnitt mellom disse. Det kan heller ikke utelukkes uklare ansvarsforhold mellom departementene og de konstitusjonelt ansvarlige statsråder. Forsvarsministeren er konstitusjonelt ansvarlig for Etterretningstjenesten og må ivareta sitt ansvar fullt ut – også i forbindelse med Etterretningstjenestens metode- og kildebruk. Gode grunner taler for at det er mest hensiktsmessig at ansvaret for forvaltningskontrollen med Etterretningstjenesten hører under én statsråd. Etablering av en kontrollmyndighet under en annen statsråd kan gjøre forsvarsministerens konstitusjonelle ansvar mer uklart.

11.12.7.3 Konklusjon

Dagens ordning med parlamentarisk forankret kontroll gjennom EOS-utvalget har gjentatte ganger blitt funnet å være den beste løsningen for den alminnelige kontrollen med Etterretningstjenestens virksomhet. Spørsmålet har vært om det i den løpende kontrollen med systemet for tilrettelagt innhenting, basert på Lysne II-utvalgets anbefaling, er grunn til å gjøre unntak fra den norske kontrollmodellen.

Som det fremgår over er flere viktige momenter ikke drøftet i Lysne II-utvalgets rapport. Disse er nærmere belyst over. Departementet vil trekke frem sikkerhetsaspektet som et særlig tungtveiende argument. Dessuten mener departementet gode grunner taler for at en

helthetlig kontroll som baserer seg på innsikt i all Etterretningstjenestens aktivitet gir de beste forutsetninger for å drive legalitetskontroll. Det styrker legitimiteten at EOS-utvalget ligger under Stortinget, og ikke til den utøvende makt. Departementet mener derfor kontrolloppgaven bør legges til EOS-utvalget og betegnes *styrket kontroll.*

11.12.8 Forslag til regulering – styrket kontroll

Departementet foreslår at EOS-utvalget får i oppgave å føre løpende kontroll med Etterretningstjenestens etterlevelse av bestemmelsene i lovforslaget kapittel 7 og 8. En slik *styrket kontroll* av tilrettelagt innhenting bør være en del av EOS-utvalgets oppgaveportefølje, og komme i tillegg til utvalgets alminnelige kontroll etter EOS-kontrolloven. Departementet mener at styrket kontroll i så tilfelle bør foretas relativt hyppig og på EOS-utvalgets eget initiativ. Selve kontrollen bør imidlertid gjennomføres på den måten som EOS-utvalget anser som best egnet for formålet. I praksis forventes mye av den utøvende rutinekontrollen å skje av EOS-utvalgets sekretariat, som bør forsterkes ytterligere i tillegg til den styrkingen som allerede er gjennomført ved at det bl.a. er opprettet en teknologisk enhet med flere personer i sekretariatet.

EOS-utvalget bør ha full innsikt i Etterretningstjenestens begjæringer til domstolen og rettens kjennelser. Om nødvendig kan gjennomføring av styrket kontroll utføres straks etter at EOS-utvalget mottar melding om at Etterretningstjenesten har fått rettens kjennelse til å gjennomføre søk i data som stammer fra tilrettelagt innhenting. Et sentralt formål med kontrollen er å kontrollere at tjenestens søk ikke strider med eller går lenger enn de betingelser som uttrykkelig fremgår av rettens kjennelse.

Departementet vurderer at EOS-utvalget ellers bør følge normale kontrollrutiner. Forsvarsdepartementets oppfølging av en sak kan innebære instruks om stans av innhenting og/eller sletting av opplysninger som har fremkommet gjennom søket. Departementet bør imidlertid ikke være forpliktet til å beordre stans og/eller sletting dersom det kommer frem til at det innmeldte forholdet er innenfor gjeldende regelverk og prioriteringer. Forsvarsministeren vil på denne måten ivareta sitt konstitusjonelle ansvar og utøve styring og kontroll av Etterretningstjenesten. EOS-utvalget vil på vanlig måte kunne bringe saken inn for Stortinget. På bakgrunn av varsler fra EOS-utvalget om avvik mener departementet at Etterretningstjenesten må vurdere å stanse innhenting og/eller slette opplysninger på eget initiativ. Dersom Etterretningstjenesten selv avdekker avvik i egne systemer som følge av teknisk eller menneskelig svikt bør tjenesten pålegges å melde fra om dette til EOS-utvalget. Det gjelder i dag strenge regler for internkontroll i tjenesten, og egen innmelding av avvik er allerede gjeldende praksis hos Etterretningstjenesten.[285]

I samsvar med gjeldende regler om alminnelig kontroll av Etterretningstjenestens virksomhet bør EOS-utvalget ha uhindret adgang til nødvendig informasjon.[286] Utvalget bør på forespørsel få innsyn i interne retningslinjer og prosedyrer, lokaler, utstyr, programvare,

[285] Se blant annet EOS-utvalgets årsmelding 2017 Dokument 7:1 (2017–2018) s. 9 og 43–44. Utvalget bemerket her at dets inntrykk er at «tjenesten tar slike feil og avvik alvorlig, og at tjenesten har oppmerksomhet rettet mot kvalitetssikring og rutiner for å minimere mulighetene for at slike feil skal oppstå igjen.»

[286] EOS-utvalgets tilgang til informasjon er nærmere behandlet i høringsnotatet punkt 6.7.2.3

filteroppdateringer, aktivitetslogger og annet som benyttes for gjennomføring av Etterretningstjenestens virksomhet etter lovforslaget kapittel 7 om tilrettelagt innhenting.

Departementet foreslår følgende lovtekst:

§ 7-11 *EOS-utvalgets styrkede kontroll av tilrettelagt innhenting*

EOS-utvalget skal føre styrket kontroll med at Etterretningstjenesten bare gjennomfører søk i henhold til rettens kjennelser, at korttidslageret og testdata ikke benyttes til etterretningsformål, og at de øvrige bestemmelsene i kapittelet her etterleves.

EOS-utvalget skal ha uhindret adgang til all informasjon, interne retningslinjer og prosedyrer, lokaler, utstyr, programvare, filteroppdateringer, aktivitetslogger og annet som benyttes for gjennomføring av virksomhet etter kapittelet her.

11.12.9 Forvaltningskontroll ved departementet

Tilrettelagt innhenting vil i tillegg være underlagt Forsvarsdepartementets alminnelige styring og kontroll. Dette er nærmere behandlet i kapittel 6.

11.13 Ytterligere tiltak for å forhindre misbruk eller utilsiktede konsekvenser av tilrettelagt innhenting

11.13.1 Innledning

Faren for misbruk har blitt trukket frem både av Lysne II-utvalget selv og i høringsrunden. Utvalget pekte i rapporten på at ved en eventuell opprettelse av et slikt informasjonsinnhentingsregime må det treffes tiltak som reduserer risiko for misbruk, og uttalte i denne sammenheng at: [287]

> «DGF-systemets omfang må reduseres til det strengt nødvendige. Sikrings- og kontrollregimet må være meget strengt, og personer som skal operere systemet må være nøye sjekket og klarert.»

Departementet er enig i utvalgets vurdering av misbruksfaren og har lagt stor vekt på å fremme et forslag som reduserer misbruksfaren til et minimum. Likevel må det erkjennes, som også utvalget peker på, at intet system er perfekt. Det vil alltid være en restrisiko. Målet er dermed å lage et system som ikke bare minimerer faren, men som også er egnet til å avdekke det dersom noen prøver eller faktisk klarer å tilegne seg informasjon eller bruker informasjon på en måte som er i strid med lov, forskrift eller andre bestemmelser som setter skranker for bruken av systemet.

Lysne II-utvalget viste til urettmessig deling av overskuddsinformasjon som en mulig misbrukssituasjon. Et annet eksempel som ble trukket frem av utvalget var faren for utilsiktet formålsglidning ved at lovgiver endrer kravene til bruk av systemet og dets kontroll- og sikkerhetsmekanismer for å lette opp i begrensninger som oppleves som uheldige. I det følgende vil departementet redegjøre for tiltak for å forhindre misbruk som kommer i tillegg til de kontrollmekanismer som er redegjort for i punkt 11.11 om domstolskontroll og punkt 11.12 om EOS-utvalgets styrkede og alminnelige kontroll.

[287] Lysne II-utvalgets rapport om digitalt grenseforsvar av 26. august 2016, s. 36

11.13.2 Forbud mot deling av overskuddsinformasjon

11.13.2.1 Problemstillingen

Overskuddsinformasjon er i lovutkastet § 1-4 nr. 10 definert som «informasjon som er uten selvstendig interesse for etterretningsformål». Hovedregelen om behandling av overskuddsinformasjon følger av lovutkastet § 10-8, som gir Etterretningstjenesten adgang til å dele overskuddsinformasjon med andre myndigheter hvis det er nødvendig for å bidra til mottakerens oppgaveløsning.[288] I tillegg må delingen anses forholdsmessig og sikkerhetsmessig forsvarlig. Dette innebærer i hovedsak en kodifisering av gjeldende rett.

Spørsmålet i det følgende er hvorvidt det bør oppstilles et helt eller delvis forbud mot deling av overskuddsinformasjon som stammer fra tilrettelagt innhenting.

For ordens skyld vil departementet understreke at det aldri vil være aktuelt å dele lagret informasjon som Etterretningstjenesten ikke har fått domstolens tillatelse til å innhente ved søk. Informasjon som ligger lagret og uevaluert vil alltid kategoriseres som *rådata* – altså «ubearbeidet eller automatisk bearbeidet informasjon i enhver form hvis etterretningsverdi ikke er vurdert», jf. lovutkastet § 1-4 nr. 13. Overskuddsinformasjon er informasjon hvis etterretningsverdi *alltid* vil være vurdert. I lys av dette vil departementet presisere at spørsmålet knytter seg til deling av informasjon som Etterretningstjenesten har innhentet basert på rettens kjennelse, og som Etterretningstjenesten har vurdert som ikke-relevant for utenlandsetterretningsformål.

11.13.2.2 Lysne II-rapporten og uttalelser fra høringsrunden

Lysne II-utvalget går i sin rapport inn for å lovfeste at Etterretningstjenesten skal slette all overskuddsinformasjon som stammer fra digitalt grenseforsvar:[289]

> «Overskuddsinformasjon som slettes i E-tjenesten, kan etter dagens regelverk overføres til andre offentlige myndigheter dersom opplysningene anses relevant for disse myndighetenes oppgaveløsning. Etter utvalgets syn bør dette ikke være mulig for informasjon fremkommet gjennom DGF. Utvalget vurderer at overskuddsinformasjon fra DGF bør slettes og ikke deles. Dette er viktig for å hindre formålsglidning. Utvalget anbefaler derfor at det for DGF lovfestes at all overskuddsinformasjon som ikke er relevant for E-tjenestens oppgaveløsning skal slettes. Klare instrukser og kontrollmekanismer må sikre at dette blir ivaretatt. Tiltaket vil sammen med øvrige tiltak bidra til at publikum vil ha tillit til at DGF ikke misbrukes for andre formål enn det informasjonstilgangen er ment for. I praksis vil dette si at dersom E-tjenesten – mot formodning og uten hensikt – skulle komme over informasjon om at en person har begått et drap, seksuelle overgrep mot barn eller deltatt i annen alvorlig kriminalitet som ikke er av relevans for E-tjenestens ansvarsområde, vil slik informasjon bli slettet uten videre oppfølging. Hensynet til rikets sikkerhet er viktigere enn å tillate bruk av denne overskuddsinformasjonen.»

Det har vært delte meninger blant høringsinstansene om Lysne II-utvalgets forslag. Flere høringsinstanser, herunder *Advokatforeningen*, synes å støtte et totalforbud mot deling av overskuddsinformasjon. Andre høringsinstanser derimot, herunder *Riksadvokaten*, stiller seg kritiske til et absolutt forbud. Flere høringsinstanser har påpekt at utvalget ikke har vurdert

[288] Det redegjøres for de generelle reglene om Etterretningstjenestens behandling av overskuddsinformasjon i høringsnotatet punkt 13.3.3.

[289] Lysne II-utvalgets rapport om digitalt grenseforsvar av 26. august 2016 punkt 9.4.2 s. 60

forholdet til ulike plikter som følger av annen lovgivning, herunder spesielt plikten etter straffeloven § 196 til å avverge nærmere bestemte alvorlige straffbare handlinger.

Det siterte avsnittet fra rapporten tyder på at Lysne II-utvalget mente at overskuddsinformasjon aldri skulle kunne deles, uansett alvorlighetsgrad. Det kan samtidig hevdes at deling av overskuddsinformasjon fra tilrettelagt innhenting for å *avverge* at et straffbart forhold realiserer seg, eller der noens liv er i fare, ikke er uttrykkelig drøftet av utvalget.

11.13.2.3 Departementets vurdering

Delingsforbud for informasjon som stammer fra tilrettelagt innhenting.
Departementet har vurdert problemstillingen på nytt og mener at det i utgangspunktet bør gjelde et strengt forbud mot deling av overskuddsinformasjon fra tilrettelagt innhenting. Et slikt forbud vil bidra til å motvirke et press i retning av å tillate at informasjonen brukes til annet enn etterretningsformål. Erfaring fra ulike sammenhenger viser at når informasjon først er innsamlet, vil det kunne komme spørsmål om bruk av opplysningene til andre formål enn det opprinnelige innsamlingsformålet. En slik konsekvens bør søkes motvirket på best mulig måte. Formålsglidning kan skje både bevisst og ubevisst. Den bevisste formålsglidning finner sted ved lovendringer og er dermed en villet handling. Det man kan kalle «ubevisst» formålsglidning karakteriseres ved at det etablerer seg en praktisering av ordningen som ikke nødvendigvis er i overensstemmelse med lovgivers intensjon. Den bevisste formålsglidningen er demokratisk sett mindre betenkelig enn den ubevisste, ettersom det da er lovgiver som har vurdert hvilke formål som kan åpne for informasjonsdeling, og veid disse mot ulempene ved deling. En tredje kategori er de bevisste misbrukstilfellene. De omtales ikke nærmere her. Misbruk må motvirkes og håndteres ved gode kontrollordninger. Forutsetningen for drøftelsen her er at informasjon innhentes for utenlandsetterretningsformål, og at ikke-relevant informasjon dukker opp som et resultatet av innhentingen.

Et system for tilrettelagt innhenting som er *rendyrket* for utenlandsetterretningsformål, uten å åpne for sekundærbruk, vil ha et «utoverrettet» fokus. En slik rendyrking vil kunne motvirke et eventuelt senere press på å bruke informasjonen til oppgaver med et «innoverrettet» fokus slik som straffeforfølgning mv. fordi sondringen mellom disse er så klar. Med dette som utgangspunkt kan man hevde at dersom man allerede ved innføringen av et system for tilrettelagt innhenting ved lov tillater at overskuddsinformasjonen brukes til for eksempel polisiære oppgaver, vil den videre formålsglidningen – slik som for eksempel deling av overskuddsinformasjon til andre myndigheter – gå enklere fordi det første «hinder» allerede er passert.

Samtidig har departementet identifisert enkelte rettslige forhold som kan utfordre et ubetinget forbud. På bakgrunn av dette, samt innspill i høringsrunden av Lysne II-utvalgets rapport, har departementet vurdert om forbudet kan eller bør gjelde absolutt, eller om det bør oppstilles unntak fra dette som vil åpne for en sekundærbruk av informasjonen. Disse vil drøftes i det følgende.

Hvilke hensyn og forpliktelser kan utfordre et absolutt forbud?
Etter en analyse av delingsforbudet opp mot andre bestemmelser i lov, menneskerettighetsforpliktelser og andre hensyn er det identifisert fire rettslige problemstillinger som må vurderes nærmere. Problemstillingen er om et absolutt forbud kan innføres uten å bryte med rettslige normer knyttet til den strafferettslige avvergingsplikten,

prinsippet om at uskyldige ikke skal bli dømt, statens sikringsplikt og nødrettslige betraktninger. Disse kan konkretiseres som følger:

Avvergingsplikten etter straffeloven § 196
Straffeloven § 196 første ledd bokstav a til c, sammenholdt med andre ledd, setter straff for den som unnlater gjennom anmeldelse eller på annen måte å forsøke å hindre visse alvorlige straffbare handlinger eller følgene av disse. De straffbare handlingene som omfattes av avvergingsplikten er uttømmende oppregnet i bestemmelsen. I korte trekk er det alvorlige forbrytelser mot rikets sikkerhet, grove seksuallovbrudd og grove voldslovbrudd som omfattes. Plikten gjelder for enhver og uten hensyn til taushetsplikt. Den inntrer når avverging «fortsatt er mulig og det fremstår som sikkert eller mest sannsynlig» at den aktuelle straffbare handlingen er eller vil bli begått. Bestemmelsen markerer en grunnleggende samfunnsplikt.[290] Avvergingsplikten er vedtatt ved lov og kan dermed fravikes i lov.

Plikt til å gi opplysninger som kan forhindre at uskyldige blir dømt etter straffeloven § 226
Straffeloven § 226 setter straff for den som unnlater å opplyse om omstendigheter som godtgjør at en som er tiltalt eller domfelt for en straffbar handling som kan medføre fengsel i mer enn ett år, er uskyldig. Prinsippet om at det er bedre at ti skyldige går fri enn at én uskyldig blir dømt er en grunnpilar i den norske strafferettspleien. Straffeloven § 226 skal bidra til å avverge justismord, og er forankret i rettssikkerhetsmessige hensyn og retten til en rettferdig rettergang – som for så vidt også følger av Grunnloven § 95 og EMK artikkel 6. Dette er tungtveiende hensyn, noe som gjenspeiles ved at bestemmelsen gjelder uten hensyn til taushetsplikt. Opplysningsplikten er vedtatt ved lov og kan dermed fravikes i lov, men det kan stilles spørsmål ved om staten har en menneskerettslig forpliktelse til å avverge potensielle justismord dersom den får kunnskap om at dette er i ferd med å skje, se nærmere om dette i avsnittet under.

Menneskerettslige sikrings- og beskyttelsesplikter
Grunnloven og den europeiske menneskerettskonvensjonen (EMK) pålegger statene positive forpliktelser, herunder en plikt til å treffe tiltak mot at noens menneskerettigheter krenkes.[291] For eksempel kan statsansatte ha en plikt til å agere dersom vedkommende gjennom sitt arbeid får kunnskap om at noens liv er i overhengende fare. En konsekvens av disse pliktene er at staten etter omstendighetene må treffe tiltak mot krenkelser av menneskerettighetene, også for så vidt gjelder privates krenkelser av andre private, se for eksempel Høyesteretts dom i Rt. 2013 s. 588. Den positive plikten til å sikre menneskerettighetene gjelder særlig retten til liv, vernet mot tortur og annen umenneskelig eller nedverdigende behandling eller straff, jf. for så vidt den spesielle beskyttelsesplikten i Grunnloven § 93 fjerde ledd. Plikten kan også gjelde krenkelser av retten til respekt for privatliv, familieliv og hjem. Det er krevende å angi den eksakte avgrensningen av de positive forpliktelsene en gang for alle.

Nødrettslige betraktninger
En handling som ellers er straffbar vil kunne være lovlig dersom den er foretatt for å f.eks. redde noens liv fra en fare for skade som ikke kan avverges på en annen rimelig måte. Det vil være opp til den enkelte rettsanvenderens skjønn i den konkrete situasjon å vurdere om

[290] Jf. Ot.prp. nr. 8 (2007–2008) punkt 10.14 side 261.

[291] Se mer om de positive forpliktelsene i punkt 4.2 i høringsnotatet.

det foreligger en nødrettssituasjon eller ikke. Spørsmålet om nødrett står i en særstilling fordi i tillegg til å være en straffrihetsgrunn regulert i straffeloven, kan det anføres at nødretten i sin kjerne er en alminnelig rettsgrunnsetning som vanskelig kan begrenses i lov. De klare nødrettstilfeller vil dermed ofte kunne påberopes på ulovfestet grunnlag.

Departementets nærmere vurdering av de rettslige hensynene som utfordrer et totalforbud mot deling av overskuddsinformasjon opp mot risikoen for formålsglidning
Hensynet til å unngå formålsglidning taler sterkt for at man holder fast ved at overskuddsinformasjon fra tilrettelagt innhenting ikke kan deles, og at man derved innskrenker omfanget av mulige unntakshjemler i den grad det er mulig uten å bryte med trinnhøyere rettsregler.

Begrunnelsen for en slik tilnærming er at det kan tenkes situasjoner der det politiske presset fra samfunnsaktører som knytter utvidet bruksadgang til gode formål blir så stort at lovgiver ikke vil klare å stå imot. Som vist over kom et slikt ønske om å bruke opplysningene til formål som i seg selv ikke kan begrunne denne type inngripende myndighetsutøvelse frem allerede under høringen av Lysne II-rapporten fra ulike instanser i justissektoren. En rendyrking av utenlandsetterretningsformålet i lovforslaget vil gi et tydelig signal om at denne informasjonen ikke skal gjenbrukes for andre formål. Dette kan gjøre det enklere å stå imot et eventuelt fremtidig press for å få tilgang til overskuddsinformasjon fra tilrettelagt innhenting ved lovendring.

Også av hensyn til den ubevisste formålsglidningen vil et ubetinget forbud mot deling være enklere å praktisere og kontrollere, enn dersom det oppstilles skjønnsmessige begrensninger til forbudet. Av samme grunn bør eventuelle unntak fra delingsforbudet gjøres så spesifikke som mulig.

Samtidig ser departementet at et absolutt delingsforbud kan få uønskede utfall i enkeltsaker. Dessuten utfordrer forpliktelsene som listet opp over, på ulike vis, en ubetinget regel.

For det første mener departementet at det bør ses hen til at lovgiver gjennom straffeloven § 196 har fastsatt regler om at *enhver* har plikt til «gjennom anmeldelse eller på annen måte å søke å avverge» en rekke alvorlige straffbare handlinger, og at denne plikten går foran lovbestemt taushetsplikt. Bestemmelsen gir til enhver tid en oppdatert oversikt over de handlinger som lovgiver mener er så alvorlige at *enhver* skal bidra til å avverge dem dersom det er mulig. At det er straffbart å ikke etterkomme avvergingsplikten oppfatter departementet som en indikasjon på hvor alvorlig Stortinget vurderer denne plikten. Det kan synes å ha formodningen mot seg at Etterretningstjenestens personell ikke skal være underlagt en tilsvarende samfunnsplikt som resten av befolkningen. I denne sammenheng finner departementet grunn til å understreke at det skilles mellom handlinger som enda kan avverges og handlinger som er begått, og at eventuelle unntak fra delingsforbudet kun vil omfatte avverging. Det er følgelig ikke *strafferettslige hensyn* som er avgjørende i vurderingen, men hensynet til den enkelte som potensielt kan utsettes for alvorlig kriminalitet *som fortsatt kan unngås.*

Departementet vil samtidig peke på at avvergingsplikten etter straffeloven § 196 er en generell regel. Den er ikke utformet med tanke på den spesielle situasjonen man her står overfor, hvor det også gjør seg gjeldende tungtveiende personvernhensyn. For å ivareta disse personvernhensynene kan det raskt tenkes at kretsen av straffbare forhold derfor bør gjøres snevrere enn det som er tilfellet etter straffeloven § 196.

Et alternativ til å hekte en unntaksbestemmelse på straffeloven § 196 kan derfor være å knytte unntakene til kun enkelte av bestemmelsene som omfattes av avvergingsplikten. For eksempel kan man knytte unntakene til straffbare forhold etter straffeloven kapittel 17 og 18, og som kan avverges.[292] Disse kapitlene omfatter straffbare forhold av en karakter som er nært beslektet med Etterretningstjenestens samfunnsoppdrag, noe som kan tale for at informasjon bør kunne deles selv om opplysningene viser seg ikke å ha tilknytning til utlandet. Til fordel for et unntak taler særlig at det vil kunne virke svært ødeleggende på tilliten til myndighetene dersom Etterretningstjenesten ikke skal kunne dele informasjon om planlagte terrorhandlinger med PST, tilsvarende angrepet 22. juli 2011, dersom Etterretningstjenesten hadde hatt indikasjoner om dette i forkant, kun fordi det ikke forelå noen tegn på tilknytning til utlandet.

For det andre kan rettssikkerhetsmessige hensyn tale for at opplysningsplikten etter straffeloven § 226 bør gå foran et delingsforbud. I norsk strafferett er det som nevnt et grunnleggende prinsipp at det er bedre at ti skyldige går fri enn at én uskyldig blir dømt. Departementet vurderer videre at dette prinsippet gis ytterligere vekt ved at det har menneskerettslig forankring. Departementet antar samtidig at det er forholdsvis urealistisk at Etterretningstjenesten vil komme over informasjon som vil kunne oppklare potensielle eller begåtte justismord. Først og fremst fordi Etterretningstjenesten ikke har noen oppgave innenfor strafferettspleien og dermed ikke vil være kjent med hva som kan være relevante fakta i en sak og hva som vil kunne bidra til at en uskyldig ikke blir dømt eller at justismord oppklares.

For det tredje antar departementet at informasjonsdeling kan være påkrevd etter Grunnloven og menneskerettighetene i en situasjon hvor Etterretningstjenestens ansatte – mot formodning og uten hensikt – kommer over informasjon om for eksempel et nært forestående drap. Departementet utelukker ikke at et absolutt forbud mot deling av overskuddsinformasjon kan komme på kant med statens positive menneskerettslige sikrings- og beskyttelsesplikter jf. Grunnloven § 92 og § 93 fjerde ledd samt EMK artikkel 1 og SP artikkel 2. Forpliktelser etter Grunnloven er av trinnhøyere rang enn alminnelig lov, og vil i et slikt tilfelle tilsidesette motstridende lovgivning. Tilsvarende går plikter etter EMK i tilfelle motstrid foran norsk lov, slik at et lovfestet forbud mot deling av overskuddsinformasjon vil måtte vike dersom det kommer i konflikt med slike positive forpliktelser.

I vurderingen av hvor langt statens sikringsplikt strekker seg må det foretas en avveining. Den praktiske konsekvensen av dette er at ikke enhver privat integritetskrenkelse vil utløse en sikringsplikt for staten; det må foretas en avveining av hvor alvorlig en menneskerettskrenkelse er eller vil kunne være, sett opp mot hvilke konsekvenser det vil ha for samfunnet dersom staten er positivt forpliktet til å agere. Ved bulk-innhenting til utenlandsetterretningsformål er også personvernhensyn relevant, og EMD har tatt til orde for at det ved slik innhenting bør oppstilles skranker for informasjonsbruken. Departementet legger da til grunn at statene vil ha en skjønnsmargin ved vurderingen av hvilke lovbrudd som kvalifiserer til informasjonsdeling. Departementet legger også til grunn at det ikke er noe til hinder for at det er lovgiver, og ikke den konkrete rettsanvenderen, som foretar denne avgrensningen. Det er som nevnt gode grunner som tilsier at unntak fra delingsforbudet

[292] Straffeloven kapittel 17 og 18 gir bestemmelser om henholdsvis *vern av Norges selvstendighet og andre grunnleggende nasjonale interesser* og *terrorhandlinger og relaterte handlinger.*

angis spesifikt i loven, heller enn ved en skjønnsmessig henvisning til Norges internasjonale forpliktelser, ettersom en spesifikk angivelse bidrar til å hindre ubevisst formålsglidning.

For det fjerde kan det anføres at det er uheldig å oppstille et forbud som ikke regulerer nødrettstilfellene, fordi alminnelige nødrettsbetraktninger uansett vil komme til anvendelse. Jo mer restriktivt delingsforbudet er, jo sterkere hensyn vil tale for å innfortolke en adgang til deling på nødrettsgrunnlag. Presisjonshensyn kan tas til inntekt for at en delingsadgang bør fremgå uttrykkelig av lovteksten, slik at all deling av overskuddsinformasjon innhentet gjennom tilrettelagt innhenting har forankring i lov, og slik at det ikke er opp til den enkelte rettsanvenderens skjønn å vurdere hvor grensen går for hva som er et nødrettstilfelle og ikke. En slik ordning ivaretas ved at loven uttømmende angir hvilke straffbare forhold som åpner for unntak fra delingsforbudet.

Departementet vil understreke at utlevering av overskuddsinformasjon vil være en problemstilling som etter all sannsynlighet sjelden eller aldri vil aktualiseres. Selv om store mengder informasjon vil *lagres*, har de materielle og prosessuelle vilkårene for *tilgang* til lagrede data, i kombinasjon med de strenge *kontrollordningene* som foreslås, til hensikt nettopp å sikre at Etterretningstjenesten får tilgang til informasjon som er utenlandsk etterretningsrelevant. Det er derfor grunn til å understreke at mengden av overskuddsinformasjon som Etterretningstjenesten vil få tilgang til ved tilrettelagt innhenting er svært begrenset. Departementet understreker også at det vil være misbruk av ordningen om den brukes for å omgå annet regelverk, for eksempel ved å innhente informasjon for politiet som politiet ikke selv kan innhente. Det tilføyes at verken nødrettslige eller andre betraktninger kan begrunne en omgåelse av lovens vilkår for søk i og innhenting av data.

Videre mener departementet at transparens knyttet til omfanget av den faktiske bruken av unntaksbestemmelsen kan ha en skjerpende effekt på Etterretningstjenestens personell, og dessuten styrke tilliten til den rettslige reguleringen av tilrettelagt innhenting. Det foreslås derfor at dersom det gjøres innskrenkning i delingsforbudet bør Etterretningstjenesten oppgi antallet utleveringer i medhold av en unntaksregel årlig. Et offentlig tilgjengelig tallgrunnlag vil også være et demokratisk gode i et så vanskelig spørsmål som det herværende, ettersom det vil gi anledning til å vurdere praktiseringen av en eventuell delingsadgang sett i lys av hensynet til å forhindre formålsglidning.

Forslag til bestemmelse

Oppsummert mener departementet at det bør gjelde et forbud mot deling av overskuddsinformasjon fra tilrettelagt innhenting. Departementet har vurdert hvorvidt dette forbudet skal gjelde ubetinget. Regelen må utformes på en måte som ivaretar Norges forpliktelser etter Grunnloven og EMK. Videre bør regelen utformes så vidt presist at den ikke gir rom for nødrettsbetraktninger på ulovfestet grunnlag, ettersom slike skjønnsmessige vurderinger kan føre til formålsglidning.

Selv om vurderingen er krevende og vektige hensyn står mot hverandre mener departementet etter dette at hensynet til å motvirke formålsglidning tilsier at forbudet formuleres så klart og uinnskrenket som mulig. Sett hen til de personvernhensyn som gjør seg gjeldende, mener departementet at det bør gjøres unntak fra pliktene som følger av straffeloven §§ 196 og 226. Samtidig har departementet kommet til at de straffbare handlingene som fremgår av straffelovens kapittel 17 og 18 (om anslag mot nasjonens selvstendighet og sikkerhet og grunnleggende nasjonale interesser, samt terrorhandlinger og terrorrelatert handlinger) ligger så nært opp mot Etterretningstjenestens formål og

oppdrag at overskuddsinformasjon fra tilrettelagt innhenting som faller innenfor disse straffebudene bør kunne deles. Forutsetningen er at handlingen fortsatt kan avverges. Departementet mener beslutningen bør fattes av Sjefen for Etterretningstjenesten eller den han eller hun bemyndiger.

Departementet oppfordrer høringsinstansene til å vurdere problemstillingen særskilt og til å inngi sitt syn.

Departementet foreslår følgende lovbestemmelse:

§ 7-12 *Forbud mot utlevering av overskuddsinformasjon*

Etterretningstjenesten skal ikke utlevere overskuddsinformasjon fremkommet gjennom innhenting etter kapittelet her. Straffeloven §§ 196 og 226 gjelder ikke for Etterretningstjenestens personell i den utstrekning de får kunnskap om det aktuelle forholdet gjennom innhenting etter kapittelet her.

Forbudet etter første ledd gjelder ikke overskuddsinformasjon om en straffbar handling som omfattes av straffeloven kapittel 17 eller 18 og som kan avverges. Sjefen for Etterretningstjenesten beslutter skriftlig om utlevering skal skje.

Informasjon som ikke er overskuddsinformasjon kan utleveres dersom vilkårene i kapittel 10 er oppfylt.

Departementet vurderer at det av pedagogiske grunner bør inntas en henvisning til lovutkastet § 7-12 i den generelle bestemmelsen om overskuddsinformasjon i kapittel 10. Her bør det også fremkomme hvilke prosessuelle krav som stilles ved eventuell utlevering av overskuddsinformasjon som fremkommer gjennom tilrettelagt innhenting. Henvisningen kan utformes slik og plasseres i lovutkastet § 10-8 annet ledd:

Overskuddsinformasjon som fremkommer gjennom innhenting etter kapittel 7, kan bare utleveres etter § 7-12.

Utlevering av overskuddsinformasjon fra tilrettelagt innhenting i det snevre unntakstilfellet som foreslås over vil innebære en adgang til å utlevere informasjon uten hinder av lovbestemt taushetsplikt. De alminnelige reglene for avveining av om utlevering kan skje etter § 10-5 bør dermed ikke komme til anvendelse. Dette er synliggjort gjennom at § 10-8 første ledd henviser til § 10-5, mens paragrafens annet ledd ikke har en tilsvarende henvisning.

11.13.3 Forbud mot bruk av bevis mot tiltalte i straffesaker

Departementet skal i det følgende vurdere hvorvidt det bør lovfestes et bevisforbud i straffesaker for informasjon som stammer fra tilrettelagt innhenting. Lysne II-utvalget gikk i sin rapport inn for et slikt forbud:[293]

> «Det bør fastsettes i lov at DGF-innhentet informasjon ikke under noen omstendighet kan bli brukt som bevis mot tiltalte i straffesaker. Utvalget er klar over at dette av noen kan oppfattes å være i strid med prinsippet om fri bevisbedømmelse i straffeprosessretten, men mener like fullt at en slik formålsbegrensning i vesentlig grad vil styrke tilliten til at DGFs formålsbegrensninger etterleves. Omfattende databasert analyse kan i enkelte tilfeller føre til at bevisbyrden for å være uskyldig snus i praksis. Dette underbygger ytterligere denne begrensningen.»

[293] Se Lysne II-utvalgets rapport om digitalt grenseforsvar av 26. august 2016 punkt 9.4.2 s. 61

Utvalget skriver videre:[294]

> «En slik formålsbegrensning vil i vesentlig grad styrke tilliten til at DGF ikke vil bli benyttet til andre formål enn forutsatt, og således hindre formålsglidning. Dette er imidlertid ikke til hinder for at informasjon innhentet gjennom DGF som ikke er å anse som overskuddsinformasjon, kan deles med PST – herunder gjennom Felles kontraterrorsenter (FKTS) – på vanlig måte, som kan bruke informasjonen som inngangsverdi for egen metodebruk/etterforskning basert på PSTs hjemmelsgrunnlag. Dersom en etterforskningssak leder til tiltale, vil imidlertid DGF-innhentet informasjon delt med PST ikke kunne benyttes som bevis.»

Høringsinstansene har gitt uttrykk for ulike syn på Lysne II-utvalgets forslag. Blant høringsinstansene som støtter et bevisforbud er *Advokatforeningen*, *Dommerforeningen* og *Justis- og beredskapsdepartementet*. Andre høringsinstanser stiller seg kritiske til et forbud, herunder *Det nasjonale statsadvokatembetet*, *Kripos*, *Politidirektoratet*, *Politiets sikkerhetstjeneste* og *Riksadvokaten*.

Departementet tar utgangspunkt i at norsk straffeprosess bygger på prinsippet om fri bevisføring. Prinsippet innebærer at partene i utgangspunktet har rett til å føre de bevisene de ønsker, jf. f.eks. Rt. 1990 s. 1008. Om begrunnelsen for prinsippet skriver Straffeprosessutvalget:[295]

> «Prinsippet finner først og fremst sin begrunnelse i en antakelse om at det vil bidra til sakens opplysning – og dermed til at straffesaken får en korrekt avgjørelse – dersom partene gis adgang til å føre de bevis de ønsker. Denne begrunnelsen krysses av de verdier som ligger til grunn for bevisforbudsreglene, herunder hensynet til en effektiv saksavvikling.»

Spørsmålet er om det finnes tilstrekkelig tungtveiende grunner til å gjøre unntak fra prinsippet om fri bevisføring i straffeprosessen gjennom å oppstille et bevisforbud for informasjon som stammer fra tilrettelagt innhenting.

Det er spesielt hensynet til å motvirke formålsutglidning som kan tilsi et bevisforbud i straffesaker. Faren for slik utglidning var begrunnelsen da Justisdepartementet foreslo et bevisforbud i straffesaker for opplysninger innhentet ved bruk av skjulte tvangsmidler i forebyggende øyemed:[296]

> «Departementet foreslår som hovedregel at opplysninger som blir innhentet ved bruk av tvangsmidler i forebyggende øyemed, ikke skal kunne benyttes som bevis under hovedforhandlingen i en straffesak. Dette legger strenge bånd på bruken av opplysningene. Dersom det for eksempel ikke lykkes å forebygge for eksempel ulovlig etterretningsvirksomhet, innebærer begrensningen at opplysningene som ble innhentet ved forebyggende bruk av tvangsmidler ikke kan brukes som bevis mot gjerningspersonen i en etterfølgende straffesak. Det kan ikke utelukkes at en slik begrensning vil kunne virke urimelig i enkeltsaker, men departementet har lagt større vekt på å unngå at rettssikkerhetsgarantier i strafforfølgningen blir undergravet ved at det oppstår et press i retning av å nytte forebyggende tvangsmidler i stedet for bruk av tvangsmidler som ledd i etterforsking. Det ville kunne oppstå fare for en slik utglidning dersom det skulle gjelde de

[294] Lysne II-utvalgets rapport om digitalt grenseforsvar av 26. august 2016 punkt 9.4.3 s. 61

[295] NOU 2016: 24 *Ny straffeprosesslov* punkt 13.2.3 s. 257

[296] Ot.prp. nr. 60 (2004–2005) punkt 9.4.4.1 s. 135

> samme reglene for bruk av opplysninger som er innhentet i forebyggende øyemed som for opplysninger som er innhentet ved bruk av tvangsmidler som ledd i etterforsking.»

På tilsvarende måte vil det for tilrettelagt innhenting kunne tenkes å oppstå et press i retning av å benytte tilgangen som ledd i etterforskningen av straffbare handlinger. De strenge og omfattende kontrollmekanismene som foreslås vil være den fremste garantisten mot slikt misbruk, men et bevisforbud vil ytterligere kunne bidra til å redusere risikoen. Departementet erkjenner at et bevisforbud vil kunne virke urimelig i enkeltsaker, men har kommet til at hensynet til å motvirke formålsglidning må få gjennomslag. Departementet foreslår derfor et slikt forbud.

Departementet har vurdert hvorvidt det bør gjøres et unntak fra bevisforbudet i saker som gjelder terrorhandlinger, slik Det nasjonale statsadvokatembetet og PST tar til orde for i sine høringsuttalelser til Lysne II-rapporten. Departementet viser for så vidt til politiloven § 17 f annet ledd bokstav c, hvor det for terrorhandlinger er gjort unntak fra bevisforbudet for opplysninger som er innhentet med forebyggende tvangsmidler etter politiloven § 17 d. Unntaket ble av Justisdepartementet begrunnet slik:[297]

> «Fra utgangspunktet om at opplysninger som er innhentet ved bruk av tvangsmidler ikke skal kunne brukes som bevis under hovedforhandlingen i en straffesak, foreslår departementet likevel at det skal gjøres unntak for terrorhandlinger, jf. straffeloven § 147 a. Dersom det ikke skulle lykkes å forebygge en terrorhandling som i verste fall kan lede til at en rekke mennesker mister livet, kan det støte an mot den alminnelige rettsbevissthet om det ikke skulle være mulig å føre opplysningene som bevis i en etterfølgende straffesak.»

Det samme hensynet kan gjøre seg gjeldende også når det gjelder tilrettelagt innhenting. På den andre siden vil et unntak kunne uthule formålet med bevisforbudet, som er å motvirke et press i retning av å benytte tilgangen som ledd i etterforskningen av straffbare handlinger. Departementet ber om høringsinstansenes syn på spørsmålet.

Departementet antar at det er tilstrekkelig at bestemmelsen om bevisforbud i straffesaker inntas i lov om Etterretningstjenesten, og at det ikke er nødvendig med en egen bestemmelse i straffeprosessloven. Bestemmelsen kan plasseres i lovutkastet § 7-13 og utformes slik:

§ 7-13 *Bevisforbud*

Informasjon fremkommet gjennom innhenting etter kapittelet her kan ikke brukes som grunnlag for ileggelse av straff eller andre strafferettslige reaksjoner.

Bevisforbudet innebærer at påtalemyndigheten ikke kan legge frem informasjon som stammer fra tilrettelagt innhenting som grunnlag for krav om straff eller andre strafferettslige reaksjoner, jf. straffeloven §§ 29 og 30. Retten plikter å avskjære slik bevisføring. Bevisforbudet innebærer også at påtalemyndigheten ikke kan bruke slik informasjon som grunnlag for egen ileggelse av straff eller andre strafferettslige reaksjoner, som for eksempel forelegg på bot etter straffeprosessloven § 255 eller påtaleunnlatelse etter straffeprosessloven § 69. Bevisforbudet innebærer derimot ikke et forbud for retten eller påtalemyndigheten mot å bruke informasjon som stammer fra tilrettelagt innhenting som grunnlag for bruk av tvangsmidler. Departementet mener det ikke foreligger grunn til å forby slik bruk av informasjonen, da de strenge begrensningene på adgangen til å dele

[297] Ot.prp. nr. 60 (2004–2005) punkt 9.4.4.1 s. 135

informasjon anses som tilstrekkelig for å forhindre at påtalemyndigheten innhenter informasjon via Etterretningstjenesten istedenfor å ta i bruk eget rettsgrunnlag.

11.13.4 Nærmere om formålsglidning

11.13.4.1 Lysne II-utvalgets rapport og høringsrunden

Sammenlignet med Etterretningstjenestens øvrige innhentingsmetoder er tilrettelagt innhenting i en særstilling fordi store mengder av overskuddsinformasjonen vil være kommunikasjon mellom personer som befinner seg i Norge eller der avsender eller mottaker av informasjonen er norsk.[298] Overskuddsinformasjonen er ikke av interesse for Etterretningstjenesten, men kan være relevant for andre myndigheters oppgaveløsning. Det kan stilles spørsmål ved om det faktum at slik informasjon lagres, og dermed er teoretisk tilgjengelig for øvrige myndigheter, vil medføre et press på tjenesten om å utlevere overskuddsinformasjon.

Lysne II-utvalget omtalte faren for formålsglidning i sin rapport, og viser til at den typiske utfordringen «er at så snart informasjonen er samlet inn eller kapasiteten etablert, så vil andre interessenter potensielt hevde at det ikke er hensiktsmessig ut fra et ressurs- eller kapasitetsperspektiv å avgrense bruken av systemet kun til det opprinnelige formål.»[299] Utvalget påpekte at dersom andre interessenter gis adgang til å benytte systemet, vil dette være problematisk av hensyn til den opprinnelige forholdsmessighetsvurderingen av systemet, da denne gjerne hviler på spesifikke premisser. Videre mener Lysne II-utvalget at det vil ligge et latent skadepotensiale i en kapasitet som digitalt grenseforsvar selv om det er foretatt grundige vurderinger i forkant.[300]

Enkelte høringsinstanser har uttrykt bekymring for formålsglidning, herunder at politiet i lang tid har ønsket seg ordinær datalagring fra elektronisk kommunikasjon, og at det derfor vil kunne oppstå press for å få tilgang til lagrede data. Dette kom for så vidt tydelig frem under høringen av Lysne II-rapporten, hvor både *Riksadvokaten*, *Politidirektoratet*, *PST* og *Kripos* argumenterte for at Etterretningstjenesten burde kunne dele overskuddsinformasjon om enkelte typer straffbare handlinger. Politi- og påtalemyndighetenes innspill er drøftet i kapitlene om forbud mot deling av overskuddsinformasjon som stammer fra bruk av tilrettelagt innhenting i punkt 11.13.2 og forbudet mot at slik informasjon skal kunne brukes som bevis i straffesaker i punkt 11.13.3.

11.13.4.2 Departementets vurdering

Departementet har vurdert faren for formålsglidning og hvordan utilsiktet utvidet bruk av tilrettelagt innhenting kan unngås. Departementet er enig i Lysne II-utvalgets konklusjon om at ikke enhver endring i formål med den løsningen som foreslås vil være «feil» eller uforholdsmessig. Imidlertid er det, som følge av det latente skadepotensialet for personvernet, viktig at enhver utvidelse er villet og har demokratisk forankring.

Departementet har vurdert hvordan lovforslaget kan utformes for å forhindre at det skjer en utilsiktet formålsglidning. Under utredningen har departementet identifisert enkelte forhold

[298] De materielle og prosessuelle vilkårene for tilgang til lagrede data, samt de strenge kontrollordningene som foreslås, vil imidlertid medføre at Etterretningstjenesten ikke vil få reell tilgang til de mengdene rådata som utgjør overskuddsinformasjon, se nærmere om dette i punkt 13.3.3.

[299] Lysne II-utvalgets rapport om digitalt grenseforsvar av 26. august 2016 punkt 6.2 s. 34

[300] Ibid.

som kan øke risikoen for at det vil kunne skje. I det følgende vil departementet redegjøre for disse forholdene og hvordan problemstillingen er søkt løst ved utformingen av lovforslaget.

For det første vurderer departementet at formålsglidning kan skje dersom reglene knyttet til behandling av *overskuddsinformasjon* ikke er tilstrekkelige robuste. Departementet foreslår en hovedregel som forbyr Etterretningstjenesten å utlevere overskuddsinformasjon som fremkommer gjennom innhenting etter lovforslagets kapittel 7. Unntaket fra hovedregelen er meget snevert og langt snevrere enn den alminnelige strafferettslige avvergingsplikten, se nærmere om dette i punkt 11.13.2.

For det andre vil *formålsangivelsen* ha betydning. *Den norske dommerforening* påpekte i sin høringsuttalelse til Lysne II-utvalgets rapport at formålsglidning kun kan forhindres dersom listen over formål som aksessen kan brukes til er klart avgrenset og uttømmende formulert i lovteksten. Departementet er enig i at en ikke-uttømmende liste over hvilke formål som kan begrunne innhenting er egnet til å føre til formålsglidning, og vil i denne sammenheng også bemerke at formålsangivelsen har betydning for om loven oppfyller lovkravet etter EMK. Videre anser departementet at en uttømmende opplisting vil skape et klarere skille mellom etterretningsrelevant informasjon og overskuddsinformasjon. Departementet vurderer at en slik avgrensning av oppgavesettet bidrar til å gjøre hjemmelsgrunnlaget for Etterretningstjenestens virksomhet klart og forutsigbart, og egnet for reell prøving av domstolen og kontroll av EOS-utvalget. Departementet foreslår derfor at de formål som kan begrunne innhenting generelt blir uttømmende regulert i lovforslaget.

Det kan anføres at opplistingen av Etterretningstjenestens oppgaver i kapittel 3 ikke gir tilstrekkelig veiledning hva angår de tilfeller som kan begrunne at tjenesten innhenter informasjon om potensielle eller identifiserte etterretningsmål. Departementet vurderer imidlertid at det er nødvendig med relativt vide formåls- og oppgavebestemmelser på grunn av Etterretningstjenestens særegne funksjon i samfunnet som Norges eneste utenlandsetterretningstjeneste med oppgave å finne ukjente utenlandske trusler eller andre utenlandske forhold av betydning for rikets sikkerhet. Dette innebærer imidlertid ikke at tjenesten kan hente inn all informasjon som kan tenkes etterretningsmessig relevant. Den faktiske innhentingen må være i tråd med de grunnvilkår som stilles til ethvert inngrep i noens menneskerettigheter, herunder at innhenting av informasjon ikke skal gjennomføres dersom det vil være et uforholdsmessig inngrep overfor den enkelte. Denne begrensningen følger av gjeldende rett og praktiseres av Etterretningstjenesten i dag. Kravet foreslås kodifisert i lovforslaget § 5-4. Departementet vil understreke at løsningen som foreslås her innebærer et mer begrenset samfunnsoppdrag for Etterretningstjenesten sammenlignet med dagens etterretningstjenestelov. Etter gjeldende rett har Etterretningstjenesten hjemmel til å innhente informasjon om utenlandske forhold i den utstrekning det kan bidra til å sikre «viktige nasjonale interesser», jf. lovens § 3. Hva som er «viktige nasjonale interesser» er ikke uttømmende opplistet, og vil avhenge av hvilke sikkerhetsutfordringer Norge til enhver tid stilles overfor, jf. instruks om Etterretningstjenesten § 7. Sammenlignet med dagens lov bidrar dermed lovforslaget til å tydeliggjøre hvilke forhold som kan begrunne innhenting av informasjon, herunder ved bruk av tilrettelagt innhenting.

Hva angår innhenting av grenseoverskridende elektronisk kommunikasjon foreslår departementet som nevnt i punkt 11.7.1.3 at denne informasjonen skal kunne innhentes og benyttes for løsningen av samtlige av Etterretningstjenestens oppgaver. Tjenesten kan imidlertid ikke innhente informasjon bare fordi innhentingen forfølger et lovfestet formål;

innhentingen må oppfylle en rekke vilkår som begrenser tjenestens bruk av tilgangen. Vilkårene for innhenting er inntatt i lovforslaget § 7-1 første ledd og lyder:

> «Etterretningstjenesten kan for etterretningsformål innhente elektronisk kommunikasjon som transporteres over den norske landegrensen når grunnvilkårene etter kapittel 5 er oppfylt, særreglene i kapittel 7 og 8 følges og innhenting ikke strider mot øvrige bestemmelser i loven her».

Departementet anser at kravet til domstolsprøving av skriftlige og begrunnede begjæringer om innhenting etter lovforslaget kapittel 8 er særlig viktig for å unngå formålsglidning. Det samme gjelder for så vidt også EOS-utvalgets styrkede og alminnelige kontroll, men det må antas at forhåndsprøving av en domstol er særlig egnet til å disiplinere Etterretningstjenestens bruk av tilrettelagt innhenting og sørge for at utglidningen ikke forekommer.

Videre er Etterretningstjenestens bruk av tilrettelagt innhenting både positivt og negativt avgrenset i lovforslaget. Den positive avgrensningen følger av bestemmelsene i kapittel 3, særlig med sikte på at tjenestens informasjonsinnhenting retter seg mot utenlandske trusler eller andre utenlandske forhold. Videre ligger det en negativ avgrensning i bestemmelsene som forbyr tjenesten å innhente informasjon for industrispionasjeformål og politiformål i henholdsvis lovforslagets §§ 4-3 og 4-4. Skillet mellom innenlands- og utenlandsetterretning tydeliggjøres i lovforslaget ved at tjenesten som nevnt ikke får dele overskuddsinformasjon innhentet gjennom tilrettelagt innhenting med en tredjepart, herunder politiet (lovforslaget § 7-12 første ledd andre punktum), og at politiet ikke kan anmode om bistand til å fremskaffe informasjon med hjemmel i lovforslaget kapittel 7 (lovforslaget § 10-3 annet punktum). Departementet vurderer at en slik negativ avgrensning av hvilke formål som kan berettige bruk av tilrettelagt innhenting, er godt egnet til å sikre mot utilsiktet formålsglidning. Til dette kommer at forsettlige brudd på lovforslaget §§ 4-3 og 4-4 vil kunne straffes som tjenestefeil eller misbruk av offentlig myndighet etter straffeloven §§ 171 til 173. For det tredje vurderer departementet at det er av betydning om tilrettelagt innhenting reguleres i lov eller forskrift. Forhold regulert i forskrift ikke vil ha den samme parlamentariske forankringen som forhold regulert i lov. Departementet har av den grunn valgt å forankre de vesentlige sider av Etterretningstjenestens virksomhet i lov.

11.13.5 To tekniske sakkyndige tilstede ved testanalyser

En integrert del av tilrettelagt innhenting vil være testinnhenting og testanalyse av ufiltrert kommunikasjon fra datastrømmene som omfattes av innhentingshjemmelen i lovforslaget § 7-1. Informasjonen som innhentes for dette formål vil lagres i et såkalt *korttidslager*, og bruken av dette vil være underlagt strenge begrensninger. Informasjonen som lagres i korttidslageret skal utelukkende benyttes for teknisk drift av systemet, og aldri for etterretningsformål. Selv om korttidslageret har et strengt avgrenset formål foreslår departementet at det bør lovfestes en regel om at uttrekk fra datastrømmen og analyse av kommunikasjonen som innhentes kun skal utføres av et begrenset antall tekniske spesialister som har mottatt særskilt opplæring og som ikke har etterretningsanalyse som oppgave. Videre foreslår departementet at det alltid skal være to tekniske spesialister til stede når uttrekkene settes opp og analyseres. Formålet med å lovfeste slike krav til personellet som håndterer korttidslageret er å styrke tilliten til at adgangen til testinnhenting ikke misbrukes. Det redegjøres for formålet med korttidslageret og hvordan dette foreslås driftet i punkt 11.14.4 under.

11.13.6 Informasjonssikkerhet

Tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon vil innebære lagring av store mengder data. Dette stiller strenge krav til informasjonssikkerhet. Lysne II-utvalget har omtalt problemstillingen i sin rapport:[301]

> «Hendelser har vist at det ikke er mulig å lage noen elektroniske systemer som er fullt ut sikre mot datainnbrudd. Reduksjon av risiko for at uvedkommende får tilgang til data og utstyr må derfor ha høy prioritet.
>
> E-tjenesten besitter det som kanskje er Norges fremste ekspertisemiljø innen cybertrusler. Deres lokaler er fysisk godt skjermet, og oppmerksomheten rundt elektronisk sikkerhet og datasikkerhet er svært høy. Få om noen institusjoner i Norge er kompetansemessig bedre i stand til å ivareta sikkerheten rundt sine systemer. Grunnet DGF-systemets sensitivitet anbefaler utvalget at DGF-tilsynet har som en tilleggsoppgave å føre tilsyn med at datasikkerheten er så høy som teknologisk og praktisk mulig.
>
> En særskilt problemstilling er knyttet til en potensiell fremtidig ikke-demokratisk maktovertakelse. Det bør utvikles mekanismer og rutiner for både sletting av all informasjon lagret i DGF, og for ødeleggelse av DGF-utstyret. Disse mekanismene og rutinene bør innrettes slik at det kan iverksettes ved ikke-demokratisk maktovertakelse.»

I lovutkastet § 7-14 første ledd foreslår departementet å lovfeste at Etterretningstjenesten plikter å hindre at uvedkommende får tilgang til informasjon som lagres og behandles etter kapittelet om tilrettelagt innhenting.

Departementet har foreslått generelle bestemmelser om informasjonssikkerhet i lovutkastet § 9-11 og § 11-4, se nærmere om dette i høringsnotatet kapittel 12 og 14. Pliktene som følger av disse bestemmelsene vil gjelde også for virksomheten knyttet til tilrettelagt innhenting. Det foreslås av pedagogiske grunner å presisere dette i lovutkastet § 7-14 annet punktum.

Enkelte høringsinstanser til Lysne II-utvalgets rapport har tatt utvalgets uttalelse om sletting og ødeleggelse ved ikke-demokratisk maktovertakelse til inntekt for et syn om at DGF-data og DGF-systemet er ekstraordinært inngripende. Departementet vil imidlertid bemerke at slike tiltak ikke er spesielle sammenlignet med andre registre og systemer i sentralforvaltningen og Forsvaret. Det følger blant annet av gjeldende beredskapssystem for sikkerhetspolitiske kriser og væpnet konflikt at dette er en standard tiltaksprosedyre.

11.13.7 Lagringstid

Lagring av opplysninger kan innebære et inngrep i noens privatliv. Personvernhensyn taler dermed for at opplysninger innhentet gjennom tilrettelagt innhenting lagres for så kort tid som mulig. Imidlertid taler hensynet til Etterretningstjenestens behov for tilgang på informasjon for en så lang lagringstid som mulig. Utfordringen for departementet har vært å balansere hensynet til personvernet med hensynet til Etterretningstjenestens behov for tilgang på lagret informasjon. På bakgrunn av departementets avveining mellom de kryssende hensyn, anbefales en lagringstid for metadata på 18 måneder, jf. lovforslaget § 7-7 tredje ledd. Det redegjøres nærmere for departementets vurdering av lagringstid av metadata i punkt 11.14.5.

[301] Lysne II-utvalgets rapport om digitalt grenseforsvar av 26. august 2016 punkt 9.5.5 s. 69

11.13.8 Nærmere om nedkjølingseffekten

11.13.8.1 Innledning

Etterretningstjenestens virksomhet vil ikke fysisk eller direkte hindre noen fra å ytre seg. Spørsmålet er imidlertid om Etterretningstjenestens adgang til å innhente grenseoverskridende elektronisk kommunikasjon vil føre til at folk avstår fra å ytre seg som de ellers ville ha gjort, eventuelt modifiserer eller sensurerer egne ytringer, som følge av frykt for at disse kan fanges opp av Etterretningstjenesten. Konsekvensen av slik selvsensur vil være mindre eller endret privat og offentlig meningsbryting, noe som vil innvirke negativt på den demokratiske debatten. Dette omtales ofte som nedkjølingseffekten. Dersom spørsmålet over besvares bekreftende vil tilrettelagt innhenting kunne innebære et inngrep i ytringsfriheten som går utover det som tillates etter Grunnloven § 100 og EMK artikkel 10.

Departementet skiller mellom det vi kan kalle en positiv og en negativ nedkjølingseffekt. Med positiv nedkjølingseffekt menes at personer unnlater å utføre ulovlige handlinger, herunder ytre seg rasistisk eller hatefullt på en måte som overskrider ytringsfrihetens rammer. Dette kalles også preventiv effekt. En slik virkning er ikke hensikten med forslaget, men hvis det har en slik konsekvens, vil det kunne regnes som samfunnsmessig positivt. Problemstillingen diskuteres ikke nærmere her. Departementet vil i det følgende drøfte hvorvidt forslaget er egnet til å skape en negativ nedkjølingseffekt, som vil si at personer avstår fra å utføre lovlige handlinger i frykt for å bli overvåket.

Departementet vil avslutningsvis vurdere en annen side av problemstillingen, nemlig hvorvidt personer og bedrifter avstår fra å utnytte det mulighetsrom som digitalisering åpner for på grunn av dårlig sikkerhet og mindre grad av tillit mellom aktører i det digitale rom. Hvis så er tilfelle, vil det kunne utfordre norske politiske ambisjoner om å oppmuntre til digitaliserte løsninger og tjenester i samfunnet.

11.13.8.2 Lysne II-utvalgets vurdering

Lysne II-utvalgets rapport vurderer hvorvidt innføringen av et digitalt grenseforsvar kan medføre en nedkjølende effekt. Problemstillingen er også løftet frem som viktig av ulike høringsinstanser og i den offentlige debatten i kjølvannet av rapporten. Lysne II-utvalget uttaler i sin rapport:[302]

> «Nedkjølingseffekten, også kjent som «chilling effect», har lenge vært omtalt som en etablert sannhet om at generell overvåkning i samfunnet gir lavere eller endret privat og offentlig meningsbrytning. Antakelsen er at dersom man vet at myndighetene overvåker kommunikasjon, så vil man endre atferd og unnlate å søke på eller skrive forhold som kan gi grunnlag for mistanke mot en selv.»

Videre vurderte Lysne II-utvalget at dersom antakelsen om atferdsendring som følge av visshet om statlig overvåking er riktig, så vil nedkjølingseffekten «innvirke på den demokratiske debatt på en negativ måte, og det vil særlig ramme dem som er i randsonen for hva som er gjengs oppfatning.» Etter en helhetlig vurdering konkluderte utvalget med at «befolkningen, med de begrensninger og kontrolltiltak som er foreslått, vil kunne ha tillit til at dataene kun anvendes for Etterretningstjenestens formål og at en eventuell nedkjølingseffekt derfor blir svært liten.»[303] Videre konkluderte utvalget med at deres forslag

[302] Lysne II-utvalgets rapport om digitalt grenseforsvar av 26. august 2016 punkt 6.3 s. 34

[303] Ibid. punkt 9.5.3 s. 67

til et digitalt grenseforsvar ikke vil innebære en innskrenking i ytringsfriheten som går utover det tillatte etter Grunnloven § 100 eller EMK artikkel 10.[304]

11.13.8.3 Er tilrettelagt innhenting egnet til å skape en negativ nedkjølingseffekt?

Departementet har funnet det nødvendig å foreta en selvstendig vurdering av spørsmålet om tilrettelagt innhenting kan føre til en nedkjølende effekt på samfunnsdebatten og privat meningsytring. Tilrettelagt innhenting etter lovforslaget her medfører at Etterretningstjenesten får en teoretisk tilgang til store mengder informasjon som ikke er relevant for å løse tjenestens oppgaver.[305] I vurderingen mener departementet at denne problemstillingen ikke kan behandles isolert, men må ses i sammenheng med de strenge kriterier og kontrollmekanismer som foreslås og som skal sikre at overskuddsinformasjon ikke misbrukes.[306]

En særlig utfordring når det gjelder en vurdering av nedkjølingseffekten er at det er lite forskning på fenomenet. Det finnes få studier, og flere av dem er basert på spørreundersøkelser. Hva angår spørreundersøkelser er det særlig to forhold som kan begrense verdien av de resultatene som utledes. For det første kan respondentene svare mer eller mindre hypotetisk, uten at den faktiske handlemåten kan verifiseres. Slike spørreundersøkelser kan dermed ikke legges til grunn som empiriske fakta knyttet til faktisk adferd, men snarere gi en indikasjon på respondentenes oppfatning. For det andre er det av vesentlig betydning hvordan spørsmålene er formulert. Dersom det stilles spørsmål om en vil «unnlate å ytre sine meninger hvis man vet at man blir overvåket» vil det være nærliggende for respondenten å svare bekreftende på dette. Svarets relevans er altså betinget av at spørsmålet er formulert på en måte som så presist som mulig gjengir de faktiske forhold. Dersom det ikke er tilfelle at «alle vil overvåkes», vil svaret basere seg på et hypotetisk premiss, og dermed ha svært begrenset verdi. Departementet vil understreke at tilrettelagt innhenting etter forslaget her ikke med rimelighet kan karakteriseres som «overvåking» av alle som befinner seg i Norge. Undersøkelser basert på et slikt premiss kan dermed ikke brukes for å underbygge en hypotese om at Etterretningstjenestens tilgang til grenseoverskridende elektronisk kommunikasjon vil medføre en nedkjølende effekt.

Departementet har ikke funnet noen studier som klart dokumenterer en vesentlig nedkjølingseffekt. Departementet har heller ikke lykkes med å finne empiriske studier som tilsier at privat og offentlig meningsutveksling har blitt dempet i sammenlignbare land som har systemer for tilrettelagt innhenting, slik som Sverige og Storbritannia.

Det finnes på den annen side også enkelte studier som på empirisk grunnlag kan tyde på at folk endrer atferdsmønster som følge av *frykt* for statlig overvåking. Studiene omtales i Lysne II-rapporten side 34. I en empirisk studie foretatt av Jonathon W. Penney ved Oxford universitet om bruken av Wikipedia i kjølvannet av Snowden-avsløringene, ble det gjort funn som tyder på at det fant sted en nedgang i antall søk på bestemte ord, og at denne nedgangen sannsynligvis kunne tilskrives brukernes frykt for statlig overvåkning av

[304] Ibid punkt 9.5.2 *ii*. s. 63.

[305] Med «teoretisk tilgang» menes at tjenesten ikke har rettslig adgang til å benytte seg av denne informasjonen med mindre dette er autorisert av en domstol.

[306] Etterretningstjenestens behandling av overskuddsinformasjon drøftes nærmere i dette kapittelet punkt 11.13.2.

Internett.[307] Det synes derfor nærliggende å legge til grunn at det oppstod en nedkjølende effekt på ytringsfriheten som følge av Snowden-avsløringene. Det er imidlertid usikkert hvor kraftig og langvarig denne atferdsendringen faktisk kan sies å være.

Departementet anser studien som interessant i den forstand at den viser at myndigheters innsamling av data for etterretningsformål vil kunne ha en negativ effekt på folks atferd dersom det ikke er implementert ordninger som ivaretar folks rettssikkerhet. Departementet vurderer imidlertid at det er flere forhold som reduserer sannsynligheten for at en slik nedkjølingseffekt vil inntre i norsk kontekst.

For det første må vurderingen av en eventuell nedkjølingseffekt ta utgangspunkt i et informert kunnskapsgrunnlag knyttet til *hva* Etterretningstjenesten lovlig kan og ikke kan gjøre. Litt forenklet sagt er dette et spørsmål om en frykt for statlig overvåkning av norske borgere er reell og kan underbygges av fakta. Informasjon om Etterretningstjenestens handlingsrom fremgår blant annet av lov, forarbeider og opplyste debatter om temaet. Departementet har bestrebet seg på å legge til rette for en åpen og informativ debatt om tilrettelagt innhenting. Det er gjort en grundig konseptuell utredning av et uavhengig utvalg, og spørsmålet gjøres til gjenstand for offentlig høring i to omganger – både ved høring av Lysne II-rapporten og av lovforslaget her. Kunnskap om den foreslåtte innhentingsaktiviteten, og de rettslige og faktiske rammer rundt denne, bidrar til å *opplyse* befolkningen og til å avverge eventuelle misforståelser knyttet til aktivitetens omfang og innretning. En vurdering av misbrukspotensiale og avbøtende tiltak knyttet til dette vil også bidra til å redusere usikkerhet. I denne forbindelse vil departementet understreke at lovforslaget her bygger på en vurdering av at Etterretningstjenestens tilgang til elektronisk informasjon som passerer den norske landegrensen er strengt nødvendig for å ivareta rikets sikkerhet og våre demokratiske institusjoner. Utformingen av regelverket bygger på menneskerettslige krav om nødvendighet og forholdsmessighet. Videre er Etterretningstjenestens virksomhet rettet mot forhold i utlandet. Etter gjeldende lov er tjenesten underlagt forbud mot å rette fordekt innhenting mot personer som befinner seg i Norge. Departementet foreslår å videreføre denne avgrensningen av Etterretningstjenestens territorielle virkeområde.[308] Samtidig vet vi at kommunikasjon mellom norske avsendere og mottakere ofte passerer landegrensen, selv om de som kommuniserer begge befinner seg i Norge. De seleksjons- og filtreringsmekanismer som finnes vil sortere vekk all norsk-til-norsk trafikk som det er mulig å identifisere før metadatalagring, basert på nasjons- eller geografibestemte identifikatorer. Et eksempel på en slik identifikator er prefikset +47. SMS og telefoni mellom norske mobiltelefoner vil derfor filtreres vekk. Utfordringen er at andre selektorer, slik som IP-adresser, ikke inneholder en nasjonsspesifikk identifikator som gjør det mulig for et filtreringssystem å avgjøre opprinnelsessted eller nasjonalitet. Følgelig er det ikke til å unngå at systemet for tilrettelagt innhenting vil lagre ikke ubetydelige mengder metadata om norsk-til-norsk kommunikasjon. Spørsmålet er om denne lagringen kan sies å innebære *overvåking*. Departementet mener at det ikke er tilfellet. At metadataene er lagret, innebærer som beskrevet over at Etterretningstjenesten har en *teoretisk* tilgang til dem. Tjenesten vil imidlertid etter lovforslaget her få *faktisk* tilgang til informasjonen først etter at det foreligger tillatelse fra domstolene i form av en rettslig kjennelse. Departementet mener at det er kunstig å sette likhetstegn mellom lagring og overvåking i en slik situasjon, da

[307] Jonathon W. Penney, *Chilling effects: Online Surveillance and Wikipedia Use*, 27. april 2016

[308] Se høringsnotatet kapittel 8

overvåking først må kunne sies å foreligge når man har *tilgang* til den lagrede informasjonen. Ordningen med forutgående domstolskontroll er behandlet i punkt 11.11 i høringsnotatet her.[309]

Enkelte vil hevde at korttidslageret står i en særstilling. Korttidslageret er nærmere beskrevet i punkt 11.14.4 og innebærer testinnhenting og testanalyser som skal sikre at filtrering og informasjonsinnhentingen er innrettet riktig. Uten denne funksjonen vil den tilrettelagte innhentingsaktiviteten miste store deler av sin etterretningsmessige verdi, og mengden overskuddsinformasjon som lagres vil bli langt større enn nødvendig. Samtidig må korttidslageret innrettes slik at de dedikerte teknikerne som skal utføre denne funksjonen må kunne se både metadata og innholdsdata. I dette tilfellet vil altså personell fra Etterretningstjenesten få tilgang til informasjon uten forutgående domstolskontroll. Det foreslås imidlertid en rekke tiltak for å minimere personverninngrepet dette utgjør. Det vil oppstilles et forbud mot å bruke informasjon fra korttidslageret til etterretningsproduksjon, og det vil bare kunne innhentes øyeblikksbilder på maksimalt 30 sekunder én gang i timen. Kombinasjonen av strenge kontrolltiltak, korte tidsintervaller og svært lav sannsynlighet for at det man kommuniserer fanges opp av øyeblikksbildene, gjør at departementet vurderer det som lite sannsynlig at korttidslageret vil medføre en nedkjølingseffekt i samfunnet.

En forutsetning for at det lovfastsatte systemet skal fungere, og for at befolkningen skal kunne ha tiltro til at ingen får tilgang til mer informasjon enn forutsatt, er at det foreligger gode og betryggende *kontrollmekanismer* som hindrer uhjemlet tilgang. Lysne II-utvalget beskriver ulike misbruksmuligheter på side 36 i sin rapport. Det fremheves her at det hypotetisk sett er tre parter som kan stå bak misbruk. Den ene er myndighetene selv, den andre er Etterretningstjenesten som organisasjon og den tredje er enkeltpersoner i organisasjonen. Datainnbrudd forårsaket av utenforstående er ikke å anse som misbruk i dette henseende, men det er også essensielt å hindre denne formen for ureglementert tilegnelse av informasjon. Dette sikres ved at data lagres på et lukket system som ikke er koblet til Internett. Etterretningstjenesten har i tillegg et av landets mest avanserte informasjonssikkerhetssystemer. At strenge menneskelige og teknologiske kontrollmekanismer skal ramme inn Etterretningstjenestens tilrettelagte innhenting har vært en grunnleggende forutsetning for hele utredningsarbeidet, og kommer til syne ved forslag til både lovregulerte og innebygde kontrollmekanismer. Som et supplement til kontrolltiltakene foreslår departementet dessuten at det lovfestes klare rammer for bruk av informasjonen; Informasjon skal bare kunne innhentes for utenlandsetterretningsformål, det skal gjelde et forbud mot deling av overskuddsinformasjon og det skal oppstilles forbud mot at informasjon som stammer fra tilrettelagt innhenting brukes som bevis mot tiltalte i straffesaker. Dette er nærmere omtalt under punkt 11.13.2 og 11.13.3.

Departementet foreslår dessuten en forhøyet terskel for behandling av *fortrolig kommunikasjon* med særlige yrkesutøvere. Terskelen som foreslås oppfyller menneskerettslige krav knyttet til myndighetenes behandling av denne typen kommunikasjon, og er begrunnet i nettopp risikoen for en nedkjølende effekt særlig på pressens tilgang på kilder. Departementet slutter seg til uttalelser fra blant andre EMD om at en uthuling av denne siden av kommunikasjonsvernet for eksempel kan medføre at personer

[309] Her fremkommer det blant annet at søk i metadatalagrene må basere seg på enten en modusselektor eller en personselektor. En modusselektor som bare angir et bestemt ord, slik som «bombe» eller «terrorist», vil ikke i seg selv være tilstrekkelig for å gi tillatelse til søk.

som besitter viktig informasjon vedrørende samfunnskritiske forhold unnlater å varsle pressen om dette i frykt for å risikere sin anonymitet. De særlige reglene som foreslås om behandling av fortrolig kommunikasjon med særlige yrkesutøvere er nærmere behandlet i høringsnotatet punkt 12.10.

Det er departementets oppfatning at Etterretningstjenesten nyter stor grad av tillit i befolkningen. Det er imidlertid, som i all virksomhet for øvrig, ikke mulig å garantere at tjenestens personell aldri vil handle i strid med regelverket. Ulovlig innhenting kan skje forsettlig eller uaktsomt. Etterretningstjenestens legitimitet er betinget av at all ulovlig innhenting kan oppdages, og at det eksisterer effektive tiltak som er egnet til å forhindre ulovlig virksomhet. Kvaliteten på de kontrollmekanismene som er innebygd i systemet vil dermed være avgjørende for folks tillit til tjenesten, og for å motvirke muligheten for at det oppstår en nedkjølende effekt. For departementet er det viktig at den høye graden av tillit ivaretas selv om tjenesten får tilrettelagt tilgang til grenseoverskridende elektronisk kommunikasjon. Tilliten kan best bevares gjennom gode kontrollordninger, og departementet har vurdert at disse bør styrkes for tjenestens innhenting og bruk av grenseoverskridende elektronisk kommunikasjon. Departementet mener at EOS-utvalget er det best egnede kontrollorganet til å ivareta denne funksjonen. Dette er nærmere beskrevet i punkt 11.12. I tillegg har departementet et alminnelig ansvar for forvaltningskontrollen. Departementet antar at den styrkede kontrollen som foreslås er egnet til å motvirke det potensialet for en nedkjølende effekt som tilrettelagt innhenting kan tenkes å føre til.

Oppsummert mener departementet at den strenge reguleringen av Etterretningstjenestens foreslåtte tilgang til etterretningsrelevant elektronisk informasjon som passerer den norske landegrensen, og den tilhørende åpenheten knyttet til dette, bidrar til å motvirke en mulig negativ nedkjølingseffekt basert på en oppfatning av at dette innebærer statlig overvåkning av norske borgere.

11.13.8.4 Nedkjølingseffekt som følge av andre aktørers etterretningsvirksomhet i Norge

Problemstillingen knyttet til en potensiell nedkjølingseffekt kan også sees fra en annen vinkel enn i drøftelsen over. Det kan nemlig argumenteres for at en ordning med tilrettelagt innhenting kan motvirke en nedkjølende effekt i den norske befolkningen som følge av andre staters etterretningsvirksomhet eller annen uønsket aktivitet fra andre trusselaktører i det digitale rom.

Norge er et land med utstrakt digitalisering i privat så vel som offentlig sektor. Fortsatt digitalisering er en ønsket utvikling, men frykt for ulovlig virksomhet i det digitale rom kan føre til at folk unnlater å ta i bruk digitale tjenester som tilbys av det offentlige. Etter departementets syn er det en forutsetning for tillit til digitaliseringsprosessen at folk kan føle seg trygge på at myndighetene har verktøy til å oppdage uønsket aktivitet rettet mot for eksempel servere med sensitiv informasjon. Datainnbruddet i systemene til Helse Sør-Øst i januar 2018 er et illustrerende eksempel på en hendelse som kunne ha fått et mindre kritisk utfall dersom Etterretningstjenesten hadde hatt adgang til å drive tilrettelagt innhenting. Innbruddet er antatt utført av en avansert og profesjonell aktør, og etterforsket som mulig

spionasje mot Norge. Hendelsen viste at våre datasystemer både er sårbare overfor denne typen handlinger og attraktive som mulige etterretningsmål for fremmede makter.[310]

11.13.8.5 Departementets vurdering

På bakgrunn av drøftelsene over vurderer departementet at det ikke foreligger holdepunkter som sannsynliggjør at det vil oppstå en negativ nedkjølende effekt i Norge som følge av tilrettelagt innhenting etter forslaget her.

Tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon vil styrke Etterretningstjenestens evne til å bidra til å sikre Norge mot uønsket aktivitet i det digitale rom. Det kan antas at dette vil skape en følelse av trygghet hos befolkningen ved bruk av digitale tjenester, og således motvirke en nedkjølende effekt snarere enn å skape en.

11.14 Utformingen av særreglene for tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon

11.14.1 Innledning

Departementet foreslår å regulere tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon i et eget kapittel i loven, se lovutkastet kapittel 7. Regler for forutgående domstolskontroll med slik innhenting foreslås i lovutkastet kapittel 8. Bestemmelsene må leses i sammenheng med lovutkastet for øvrig, som blant annet inneholder regler om Etterretningstjenestens oppgaver, styring og kontroll, grunnvilkår for innhenting og særskilte innhentingsforbud.

11.14.2 Innhentingshjemmel

Av hensyn til lovkravet foreslår departementet en innhentingshjemmel i lovutkastet § 7-1 hvor det fremgår uttrykkelig at Etterretningstjenesten for etterretningsformål kan innhente grenseoverskridende elektronisk kommunikasjon.

Innhentingshjemmelen gjelder utelukkende kommunikasjon som krysser den norske landegrensen. Begrensningen til grenseoverskridende kommunikasjon innebærer at Etterretningstjenesten ikke vil ha hjemmel til å innhente kommunikasjon som transporteres internt i det norske nettverket. Begrensningen innebærer videre at det bare er elektronisk kommunikasjon som overføres i et system for signaltransport, som kan innhentes. Lagrede data som ikke er i transitt, kan ikke innhentes med hjemmel i lovutkastet § 7-1.

Det ligger ikke i kommunikasjonsbegrepet at det må foreligge kommunikasjon mellom to eller flere parter. Også ensidig overføring av lyd, tekst, bilder eller andre data omfattes. Som påpekt av Lysne II-utvalget er dette nødvendig blant annet for å fange opp digitale angrep som ikke innebærer gjensidig kommunikasjon mellom flere aktører.[311]

Forslaget gir utelukkende hjemmel for innhenting «for etterretningsformål». Dette innebærer at innhentingen må begrunnes i en av Etterretningstjenestens oppgaver etter lovutkastet kapittel 3.

---

[310] Se mer om dette i Hackingen av Helse Sør-Øst – Oppsummert, NorSIS 19. januar 2018 (sist oppdatert 19. februar 2018).

[311] Se Lysne II-utvalgets rapport punkt 2.1 s. 10.

Lovutkastet § 7-1 oppstiller tre vilkår for innhentingen i tillegg til formålsbegrensningen. For det første må grunnvilkårene etter kapittel 5 være oppfylt, på samme måte som for alle andre former for innhenting. Disse grunnvilkårene er nærmere beskrevet i kapittel 9 i høringsnotatet. For det andre må særreglene i kapittel 7 og kapittel 8 følges. For det tredje må innhentingen ikke stride mot øvrige bestemmelser i loven, slik som for eksempel innhentingsforbudene som er nærmere beskrevet i høringsnotatet kapittel 8. At innhentingen ikke kan stride mot lovens innhentingsforbud følger riktignok allerede av lovens system. Departementet finner likevel av pedagogiske årsaker grunn til å understreke dette særskilt i utkastet til § 7-1.

Innhenting av elektronisk kommunikasjon etter kapittelet her er en undergruppe av innhentingsmetoden midtpunktinnhenting. På grunn av de særtrekkene som er beskrevet i punkt 10.5.1, bør denne undergruppen reguleres særskilt i lovforslaget. Særreglene bør derimot ikke gjelde for annen innhenting av grenseoverskridende elektronisk kommunikasjon. Skillet mot annen midtpunktinnhenting må derfor komme klart frem av lovteksten, slik at det ikke oppstår tvil om virkeområdet for særreglene. Siden loven så langt som mulig bør utformes teknologinøytralt, er det ikke ønskelig å trekke skillet gjennom en henvisning til fiberoptiske kabler. Departementet foreslår derfor å fastsette i lovutkastet § 7-1 annet ledd at særreglene bare gjelder for innhenting som nærmere bestemte tilbydere skal ha plikt til å tilrettelegge for. Denne tilretteleggingsplikten er et særtrekk som er egnet som avgrensningskriterium mot andre former for midtpunktinnhenting.

Forslaget til lovtekst i § 7-1 lyder slik:

§ 7-1 *Hjemmel for innhenting og virkeområde*

Etterretningstjenesten kan for etterretningsformål innhente elektronisk kommunikasjon som transporteres over den norske landegrensen når grunnvilkårene etter kapittel 5 er oppfylt, særreglene i kapittel 7 og 8 følges og innhenting ikke strider mot øvrige bestemmelser i loven her.

Bestemmelsene i kapittel 7 og 8 kommer bare til anvendelse for innhenting der det er nødvendig at tilbydere som nevnt i § 7-2 legger til rette for Etterretningstjenestens tilgang til den elektroniske kommunikasjonen.

11.14.3 Utvalg og filtrering

Lysne II-utvalget drøfter i sin rapport hvordan informasjonstilfanget fra tilrettelagt innhenting kan begrenses:[312]

> «Volumet av informasjon som vil kunne plukkes opp av overvåkingsutstyr plassert på de kablene som krysser landegrensen er stor, og det er problematisk å gi E-tjenesten uregulert tilgang til hele trafikktilfanget. Dette er det tre grunner til:
>
> Det er en svært liten andel av datatrafikken som er relevant for E-tjenestens samfunnsoppdrag.
>
> Juridiske forholdsmessighetsvurderinger avgjør om tiltaket er i henhold til Grunnloven, internasjonale menneskerettigheter og personvernlovgivning. Disse vurderingene vil avhenge av hvilke datastrømmer E-tjenesten får tilgang til. Uregulert tilgang til hele trafikktilfanget vil vanskelig kunne anses som forholdsmessig.
>
> Det bør legges til rette for at offentligheten får en godt begrunnet tillit til at DGF ikke kan benyttes til masseovervåkning av norske borgere.

[312] Lysne II-utvalgets rapport om digitalt grenseforsvar av 26. august 2016 punkt 8.4.1 s. 50

Dette tilsier at mye av trafikken bør filtreres ut før den gjøres tilgjengelig for etterretningsformål. Videre kan det tilsi at det bør ligge begrensninger på hvordan den trafikken som blir gjort tilgjengelig for E-tjenesten kan tillates benyttet. Det er to forskjellige former for teknologiske begrensninger man kunne tenke seg å legge inn:

Det kan være begrensninger på hvilke data fra datastrømmene som skal kunne tas vare på i et lager. Dette blir gjerne implementert ved hjelp av et logisk filter.

Det kan være begrensninger på hvordan, og av hvem, lagrede data kan benyttes.»

Om filtrering skriver utvalget:[313]

«Ideelt sett ville man ønske seg maskinell filtrering som kun ga E-tjenesten tilgang til relevant og forholdsmessig tilpasset informasjon. Forskjellige tilnærminger til dette diskuteres under. Som et gjennomgående eksempel tar vi for oss i hvilken grad man teknologisk vil kunne sikre at kommunikasjon mellom to norske borgere ikke kan gjøres til gjenstand for overvåkning. Dette er ikke den eneste filtreringsproblematikken som ligger i DGF, men det er et representativt og lett forståelig eksempel på informasjon som krysser grensen og som ligger utenfor E-tjenesten sitt arbeidsområde.

En metode for filtrering består i at man spesifiserer hva som filtreres vekk. Informasjon som ikke maskinelt gjenkjennes som noe som skal filtreres vekk vil gjøres tilgjengelig for bruk. Eksempelvis vil man i vårt tilfelle ønske å filtrere ut kommunikasjon mellom to norske statsborgere som begge befinner seg i Norge. For enkelte kommunikasjonstjenester – slik som standard telefoni og SMS – vil dette la seg gjøre. For de fremvoksende IP-baserte tjenestene vil dette være langt vanskeligere. Det vil i mange tilfeller kreve oppbygging av et register over brukernavn knyttet til norske borgere på hver av de forskjellige tjenestene. Styrken ved slik negativ filtrering er at det er lite etterretningspotensiale som går tapt selv ikke når nye kommunikasjonsplattformer dukker opp. Svakheten er at de grensene man setter for hvilken informasjon E-tjenesten skal ha tilgang til, vil bli utfordret av de samme nye kommunikasjonsplattformene. For hver ny tjeneste vil det måtte bygges opp nye registre over hvilke brukere som er norske borgere.

Ved positiv filtrering vil man på forhånd spesifisere hva som skal tillates benyttet til etterretningsformål. Alle datastrømmer som ikke maskinelt gjenkjennes som noe som skal tas vare på, blir da filtrert vekk. Positiv filtrering vil her bety at man måtte identifisere hvilke utvalgte utenlandske brukere som er av interesse. Dette vil redusere den etterretningsmessige nytten av DGF, da man mister muligheten til å gjennomgå historien til en person eller organisasjon som plutselig fremstår som etterretningsmessig viktig. Det begrenser for øvrig etterretning til kun kjente trusler og umuliggjør målutvikling og avdekking av nye trusler. Styrken til positiv filtrering er at de begrensningene man setter for DGF ikke blir utfordret av teknologisk utvikling. Til gjengjeld vil den etterretningsmessige verdien av DGF bli utfordret av den samme utviklingen.

Forskjellen i positiv og negativ filtrering kommer til syne når det er en del av datatilfanget som verken kan defineres som klart relevant eller klart irrelevant. For DGF ligger mye av det etterretningsmessige potensialet gjemt i informasjon som faller i denne ikke definerbare kategorien. Det er derfor ikke praktisk mulig å lage fullt automatiserte filtre som verken reduserer den etterretningsmessige verdien av DGF eller gir E-tjenesten tilgang på informasjon som ligger utenfor dens virkeområde.»

Departementet kan i hovedsak slutte seg til utvalgets vurderinger. Det er sentralt at mengden av ikke-etterretningsrelevant kommunikasjon som innhentes, begrenses i størst mulig grad. Det foreslås derfor en plikt for Etterretningstjenesten til å benytte seg av utvalg og filtrering for å sikre at det så langt som praktisk mulig ikke lagres metadata om

[313] Lysne II-utvalgets rapport om digitalt grenseforsvar av 26. august 2016 punkt 8.4.2 s. 50

kommunikasjon mellom en avsender og en mottaker som begge befinner seg i Norge. Departementet viser til lovutkastet § 7-5.

Plikten til *utvalg* innebærer at Etterretningstjenesten må vurdere og beslutte hvilke kommunikasjonsnett, tjenester og linker som det skal innhentes fra. Etterretningstjenesten skal prioritere innhenting fra de kommunikasjonsbærerne som antas å bære mest mulig etterretningsrelevant kommunikasjon. Kommunikasjonsbærere som ikke transporterer kommunikasjon over den norske grensen, er det ikke adgang til å velge ut. Dette følger av at innhentingshjemmelen er begrenset til grenseoverskridende kommunikasjon. Kommunikasjonsbærere som utelukkende transporterer kommunikasjon mellom avsendere og mottakere som befinner seg i Norge, skal normalt heller ikke velges ut, selv om det er tale om kommunikasjon som krysser landegrensen. Her kan det imidlertid etter omstendighetene være aktuelt med unntak hvis kommunikasjonen omfattes av unntaket etter lovutkastet § 4-2 første ledd. Det kan for eksempel være tale om en tjeneste som brukes av personer som opptrer på vegne av en fremmed makt i Norge til å kommunisere seg imellom.

Filtreringsplikten innebærer at Etterretningstjenesten skal utvikle og implementere filtre som så langt som praktisk mulig hindrer at det lagres metadata om kommunikasjon mellom en avsender og en mottaker som begge befinner seg i Norge. Som beskrevet i Lysne II-utvalgets rapport, vil slik filtrering vanskelig kunne gjennomføres fullt ut. Det er derfor ikke til å komme ifra at det vil lagres ikke ubetydelige mengder metadata om kommunikasjon mellom norske borgere. Det vil likevel være mulig å filtrere bort en del slik kommunikasjon, for eksempel basert på telefonnumre, og etter forslaget plikter Etterretningstjenesten å sørge for slik filtrering.

Lovutkastet § 7-5 er utformet slik:

§ 7-5 *Utvalg og filtrering*

Ved utvalg av kommunikasjonsnett og tjenester som transporterer elektronisk kommunikasjon over den norske landegrensen, skal Etterretningstjenesten prioritere tilgang til nett, tjenester og linker som antas å frembringe mest mulig etterretningsmessig relevant informasjon for å løse tjenestens oppgaver etter kapittel 3.

Etterretningstjenesten skal gjennom utvalg og filtrering så langt som praktisk mulig sikre at metadata som lagres i henhold til § 7-7 ikke inneholder data om kommunikasjon mellom en avsender og mottaker som begge befinner seg i Norge, med mindre avsender eller mottaker omfattes av § 4-2 første ledd.

11.14.4 Testinnhenting og testanalyse

Lysne II-utvalget har i sin rapport vurdert hvorvidt det bør åpnes for lagring av korte tidsintervaller med ufiltrert informasjon som har gått over den fiberoptiske kabelen (korttidslager).[314] Utvalget mener at en slik adgang er nødvendig for systemet, men at det må legges meget sterke begrensninger på hvordan korttidslageret kan benyttes.

Departementet slutter seg i hovedsak til utvalgets vurderinger på dette punktet. Testinnhenting og testanalyse av trafikk og nett som omfattes av innhentingshjemmelen er nødvendig for teknisk drift av systemet, blant annet for slik utvelgelse og filtrering som er beskrevet i punkt 11.14.3 over. Lysne II-utvalget uttaler følgende om dette:[315]

[314] Lysne II-utvalgets rapport om digitalt grenseforsvar av 26. august 2016 punkt 9.2.5 s. 54–55

[315] Ibid. punkt 9.2.5 s. 55

> «Dette lageret er helt nødvendig for å kunne drive kontinuerlig teknologisk oppdatering av filtrene i systemet. Uten dette lageret må man anta at kvaliteten på Filter 1 og Filter 2[316] vil bli vesentlig svekket. Det er derfor lite ønskelig å ha DGF uten dette korttidslageret. Det er nødvendig å mellomlagre data for i det hele tatt å kunne gjøre et fornuftig utvalg av kommunikasjonsbærere, herunder forstå hva slags kommunikasjon som går på bæreren, samt for å (videre)utvikle filtrerings- og seleksjonsmekanismen i DGF og etterfølgende re-prosessering.»

Testinnhenting og testanalyse må derfor sees på som grunnleggende forutsetninger både for at tjenesten kan gjøre etterretningsrelevante utvalg av informasjonen som hentes inn, og for å sikre at innholdsdata filtreres vekk. Dette skyldes særlig den raske oppdateringshurtigheten av informasjonsteknologien. Uten testinnhenting og testanalyse som verktøy vil innhentingen bli mindre målrettet, og dermed mer inngripende overfor den enkelte. Departementet deler således ikke oppfatningen til enkelte høringsinstanser som hevder at korttidslageret bidrar til å øke personverninngrepet. Departementet mener at alle elementene i systemet for tilrettelagt innhenting må sees i sammenheng og at systemet for testinnhenting og testanalyse utgjør en viktig forutsetning for å sikre at det lagres så lite overskuddsinformasjon som mulig.

Det er en grunnleggende forutsetning for departementet at testinnhenting og testanalyse *aldri* skal benyttes for etterretningsformål, men utelukkende for teknisk understøttelse, det vil si for å muliggjøre utvelgelse, filtrering, lagring, søk, reprosessering, forståelse av signalmiljø og gjenkjenning av tjenester og dataformater. Dette foreslås uttrykkelig regulert i lovutkastet, se forslag til § 7-6.

Testinnhentingen gjennomføres ved å trekke ut ufiltrert kommunikasjon fra en eller flere utvalgte kommunikasjonslinker over et kort tidsintervall. Lysne II-utvalget foreslo i sin rapport at intervallene normalt ikke burde være lengre enn ett minutt, og at det burde legges restriksjoner på hyppigheten av innsamlingsintervallene. Personvernhensyn tilsier etter departementets syn at det bør fastsettes et kortere tidsintervall enn Lysne II-utvalgets forslag om ett minutt. Departementet foreslår derfor at uttrekkene ikke skal overstige 30 sekunder, som anses tilstrekkelig til å oppfylle formålet med testinnhentingen. Departementet går videre inn for at det maksimalt kan gjøres ett uttrekk per time. Det følger av dette at det maksimalt kan gjøres 24 uttrekk per døgn.

Uttrekkene skal lagres i et eget korttidslager som holdes atskilt fra metadata som lagres i tråd med lovutkastet § 7-7, jf. punkt 11.14.5. Uttrekkene skal ikke lagres lenger enn det som er nødvendig for de angitte tekniske formålene, og aldri i mer enn 14 dager. Tekniske parametere og bearbeidede analyser av testdata som ikke kan knyttes til enkeltpersoner, kan derimot lagres så lenge det er nødvendig for de angitte formålene.

Det er grunn til å understreke at misbrukspotensialet ved testinnhenting og testanalyse er begrenset, all den tid det vil være tilfeldig hva som fanges opp av uttrekkene. Muligheten til å innrette et uttrekk mot bestemt kommunikasjon fremstår som teoretisk. Departementet vurderer at gitt at mengden kommunikasjon som til enhver tid passerer landegrensen, er det en særdeles liten sjanse for at det man kommuniserer vil plukkes opp av korttidslageret, i tillegg til at tidsintervallene er ytterst begrenset.

[316] Filtrene er nærmere beskrevet i Lysne II-utvalgets rapport om digitalt grenseforsvar av 26. august 2016 s. 54. Filter 1 har som hovedoppgave å redusere mengden data som flyter inn i systemet og Filter 2 filtrerer bort innholdsdata [departementets tilføyelse].

For å styrke tilliten til at adgangen til testinnhenting ikke misbrukes, foreslår departementet likevel å lovfeste at testinnhenting og annen teknisk understøttelse bare skal gjennomføres av et begrenset antall tekniske spesialister som har mottatt særskilt opplæring og som ikke har etterretningsanalyse som oppgave. Etterretningstjenestens analytikere vil dermed aldri ha noen befatning med korttidslagrene, i tillegg til at informasjonen som fremkommer i uttrekkene aldri tillates brukt i etterretningsproduksjon. Det ligger i dette at informasjon som kan knyttes til enkeltpersoner heller aldri vil kunne deles med andre aktører etter delingsreglene i lovforslagets kapittel 10, det være seg med justismyndighetene, andre lands etterretningstjenester mv.

Som et ytterligere tillitsskapende tiltak foreslås det lovfestet at det alltid skal være to tekniske spesialister til stede når uttrekkene settes opp og analyseres. Dette tiltaket går lenger enn Lysne-II utvalgets foreslåtte kontrolltiltak, og vil medføre økte økonomiske og administrative kostnader for Etterretningstjenesten. Tiltaket vil minimere et eventuelt misbrukspotensial ved at ingen tillates å håndtere informasjonen i korttidslagrene alene, og dermed styrke tilliten til virksomheten. Departementet anser det som hensiktsmessig at spesialistene som gjennomfører uttrekkene rulleres.

All aktivitet knyttet til korttidslageret vil logges for kontrollformål. Departementet forutsetter at EOS-utvalget utvikler god kompetanse til å forstå detaljene i hvordan korttidslageret fungerer og at dette underlegges omfattende kontroll.

Norges nasjonale institusjon for menneskerettigheter har i sin høringsuttalelse til Lysne II-utvalgets rapport uttalt at korttidslageret, slik det er beskrevet i utredningen, vil være i strid med EMK artikkel 8 og kommunikasjonsverndirektivet. Departementet kan ikke slutte seg til denne vurderingen. Det vises til at menneskerettighetene ikke er til hinder for slik innhenting som foreslås i høringsnotatet, jf. punkt 11.8. Korttidslagring og analyse av testdata må regnes som en integrert del av innhentingssystemet som er strengt nødvendig for at det skal kunne driftes, blant annet med hensyn til utvikling og oppdatering av filtrene som skal sikre at minst mulig overskuddsinformasjon lagres. Korttidslagring og analyse av testdata kan da ikke i seg selv sies å være i strid med menneskerettighetene.

Forslaget til regulering av korttidslager og behandling av testdata lyder som følger:

§ 7-6 *Korttidslager og behandling av testdata*

Etterretningstjenesten skal gjennomføre testinnhenting og testanalyser av trafikk og nett som omfattes av kapittelet her. Testinnhenting og testanalyser skal aldri benyttes for etterretningsformål, men utelukkende for teknisk å muliggjøre utvalg, filtrering, lagring og søk i lagrede data, reprosessering av data, forståelse av signalmiljø og gjenkjenning av tjenester og dataformater.

Testinnhenting skal gjennomføres ved å gjøre et uttrekk av ufiltrert kommunikasjon i en eller flere utvalgte kommunikasjonslinker. Ett uttrekk skal ikke overstige 30 sekunder. Maksimalt antall uttrekk er 1 per time.

Uttrekkene skal lagres i et korttidslager som skal holdes adskilt fra metadata som lagres etter § 7-7.

Uttrekkene skal ikke oppbevares lenger enn det som er nødvendig og skal slettes senest etter 14 dager. Tekniske parametere og bearbeidede analyser av testdata som ikke kan knyttes til enkeltpersoner kan oppbevares så lenge det er nødvendig for de formål som fremgår av første ledd annet punktum.

Testinnhenting og annen teknisk understøttelse skal bare utføres av et begrenset antall tekniske spesialister som har mottatt særskilt opplæring og som ikke har etterretningsanalyse som oppgave. Det skal alltid være to spesialister tilstede ved oppsett og analyse av uttrekk etter annet ledd.

11.14.5 Lagring av metadata

Departementet foreslår i lovutkastet § 7-7 å gi Etterretningstjenesten adgang til å lagre metadata om kommunikasjon som passerer den norske landegrensen. Det vises til punkt 11.6 og 11.7 for en nærmere beskrivelse av verdien av slik lagring. Det foreslås lovfestet at lagring bare kan finne sted etter at det er foretatt utvelgelse og filtrering etter lovutkastet § 7-5, se nærmere punkt 11.14.3.

Vilkårene for søk i metadatalageret foreslås lovfestet i lovutkastet § 7-8, se under i punkt 11.14.6. Søk vil kreve domstolens forhåndsgodkjennelse.

Lovutkastet § 7-7 gir utelukkende hjemmel for lagring av *metadata*. Adgangen til lagring av innholdsdata drøftes nærmere i under i punkt 11.14.7. Metadata defineres i utkast til § 7-7 ander ledd som «data som beskriver annen data eller som inneholder ekstra informasjon knyttet til data, herunder data som beskriver typen eller formatet på innholdet, hvem som er avsender og mottaker, og størrelse, tidspunkt og varighet for kommunikasjonen». Denne definisjonen omfatter både trafikkdata og signaleringsdata, jf. ekomforskriften § 7-1 første ledd og § 7-2 første ledd.

Som et tiltak for å hindre at det lagres innholdsdata, foreslår departementet å lovfeste at Etterretningstjenesten skal opprette og vedlikeholde en liste som spesifiserer hvilke typer data som regnes som metadata. Dette er viktig fordi noen typer data kan ha trekk både av metadata og av innholdsdata, og derfor ikke kan lagres med hjemmel i lovutkastet § 7-7. Listen skal være tilgjengelig for kontrollmyndighetene.

Et særskilt spørsmål er hvor lenge metadata bør kunne lagres. Lysne II-utvalget skriver om dette:[317]

> «Metadata vil bli lagret i så lang tid som anses nødvendig for å løse etterretningsoppdraget til E-tjenesten, og maksimalt i 18 måneder. En lagringstid på 18 måneder er av utvalget vurdert å være nødvendig og tilstrekkelig for å kunne gjennomføre en tilfredsstillende retrospektiv trafikkdataanalyse.»

Departementet tar utgangspunkt i at personvernhensyn tilsier en så kort lagringstid som mulig, mens etterretningsfaglige hensyn taler for en så lang lagringstid som mulig. Utfordringen er å finne den riktige balansen mellom disse hensynene. Departementet har i denne vurderingen tatt i betraktning at tilrettelagt innhenting skal kunne brukes for å løse alle de lovpålagte oppgavene Etterretningstjenesten har, jf. punkt 11.7. Flere av disse oppgavene kan innebære operasjoner som strekker seg over svært lang tid, noe som tilsier en lagringstid på mer enn 18 måneder. Dette gjelder særlig oppgaver knyttet til statlige aktørers virksomhet. For så vidt gjelder kontraterroroppdraget, vil en på den andre siden kunne ha god effekt av tilrettelagt innhenting også med en noe kortere lagringstid enn 18 måneder. En lagringstid på 12 måneder bør regnes som et minimum av hensyn til etterretningsverdien av lagringen, mens en av personvernhensyn neppe bør tillate lagring i mer enn 24 måneder. Departementet kan etter en samlet vurdering slutte seg til utvalgets forslag om en lagringstid på 18 måneder, som fremstår som et forsvarlig resultat etter en avveining av de motstående hensynene.

Lovutkastet § 7-7 er utformet slik:

§ 7-7 *Metadatalagring*

[317] Lysne II-utvalgets rapport om digitalt grenseforsvar av 26. august 2016 punkt 9.2.5 s. 55

Etter at det er foretatt utvalg og filtrering etter § 7-5, kan Etterretningstjenesten lagre metadata om elektronisk kommunikasjon som passerer den norske landegrensen.

Metadata er data som beskriver annen data eller som inneholder ekstra informasjon knyttet til data, herunder data som beskriver typen eller formatet på innholdet, hvem som er avsender og mottaker, og størrelse, tidspunkt og varighet for kommunikasjonen. Etterretningstjenesten skal opprette og vedlikeholde en liste over hvilke typer metadata som kan lagres, for å hindre at det lagres innholdsdata. Listen skal være tilgjengelig for EOS-utvalget.

Lagrede metadata skal slettes etter 18 måneder.

For teknisk analyse, feilsøking og oppdatering av lagrede metadata i den hensikt å muliggjøre søk, gjelder § 7-6 femte ledd første punktum tilsvarende.

11.14.6 Søk i lagrede metadata

11.14.6.1 Søk krever domstolens forhåndsgodkjennelse

Det er en grunnleggende forutsetning at Etterretningstjenesten bare skal kunne foreta søk i lagrede metadata i den utstrekning det på forhånd er godkjent av en domstol. Det vises til drøftelsen i punkt 11.11, hvor departementet konkluderer med at tilrettelagt innhenting bør kreve domstolens forhåndsgodkjennelse. Denne grunnleggende forutsetningen foreslås lovfestet i lovutkastet § 7-8 første ledd første punktum. Bestemmelsen må sees i sammenheng med lovutkastet kapittel 8, hvor det er gitt regler om saksbehandlingen for domstolen og hva domstolen skal prøve. Departementet viser spesielt til lovutkastet § 8-4, hvor det fremgår at retten skal prøve om vilkårene etter loven er oppfylt, herunder at innhentingen ligger innenfor Etterretningstjenestens oppgaver, ikke innebærer brudd på noen av de særskilte innhentingsforbudene og tilfredsstiller grunnvilkårene for innhenting. Søk i lagrede metadata vil også kunne foretas innenfor rammen av en beslutning fattet med hjemmel i lovutkastet § 8-10, som på strenge vilkår gir sjefen for Etterretningstjenesten myndighet til å gi ordre som trer i stedet for rettens kjennelse i hastesaker.

11.14.6.2 Søk skal baseres på personselektorer eller modusselektorer

Departementet foreslår å lovfeste at søk i metadatalageret skal baseres på en personselektor eller en modusselektor. Dette er i tråd med Lysne II-utvalgets forslag.[318] Departementet er således enig med utvalget i at det ikke bør tillates søk hvor både aktør og modus er ukjent. Slike søk vil kunne grense mot det vilkårlige, og bør derfor ikke aksepteres som grunnlag for å finne anomalier i metadatalageret. Personvernhensyn tilsier derfor at en ikke åpner for slike søk. Departementet har vurdert hvorvidt det bør fremgå uttrykkelig i loven at slike søk er forbudt, men har kommet til at forbudet fremgår tilstrekkelig klart av at søk skal baseres på en personselektor eller en modusselektor.

Med personselektor forstås en identifikator knyttet til en bestemt person eller virksomhet, jf. legaldefinisjonen i lovutkastet § 1-5 nr.12. Typiske personselektorer er telefonnumre, e-postadresser og identiteter på ulike nettsamfunn og meldingstjenester. Dersom rettens kjennelse identifiserer en bestemt person det skal kunne søkes på, vil Etterretningstjenesten kunne søke på alle kjente identifikatorer knyttet til personen.

Et særskilt spørsmål er hvorvidt man ved personselektorsøk skal kunne søke i ett eller flere ledd ut i personens kommunikasjonskjede.

[318] Se Lysne II-utvalgets rapport om digitalt grenseforsvar av 26. august 2016 punkt 9.2.6 s. 56–57

I Lysne II-utvalgets rapport heter det om dette:[319]

> «For søk basert på *personselektorer* knyttet til personer som domstolen har godkjent innhenting mot, antar utvalget at domstolens kjennelser i alle fall bør kunne inkludere to ledd ut i kommunikasjonskjeden. Dette vil for det første fasilitere bedre treff ved søk, og det vil i tillegg bidra til at antall rettsavgjørelser kan holdes på et håndterlig nivå.»

Datatilsynet har i sin høringsuttalelse til rapporten problematisert utvalgets forslag på dette punktet. Tilsynet viser til en studie av tre forskere ved Stanford universitet i USA som anslår at en med utgangspunkt i ett telefonnummer vil kunne få tilgang til metadata om ca. 25 000 personer forutsatt adgang til søk to ledd ut i kommunikasjonskjeden og en lagringstid på 18 måneder.

Departementet har tatt i betraktning studien som Datatilsynet viser til i sin høringsuttalelse. Slik departementet forstår studien, bygger den på et lite og ikke-representativt datasett, og funnene har ikke nødvendigvis gyldighet for norske forhold. Departementet mener derfor at en bør være varsom med å trekke slutninger fra studien. Den kan imidlertid gi en indikasjon på at Etterretningstjenesten vil kunne få tilgang til metadata om et stort antall personer med utgangspunkt i én selektor. Personvernhensyn kan derfor tilsi en hovedregel om søk kun ett ledd ut. Etterretningsfaglige hensyn tilsier derimot en adgang til søk to eller flere ledd ut. Dette gir mulighet til å danne seg et bilde av hvordan et etterretningsmåls kontakter kommuniserer, noe som er sentralt i målsøkingsarbeidet. Hensynet til en effektiv ressursbruk tilsier også adgang til søk to ledd ut. Hvis det oppstilles en hovedregel om søk kun ett ledd ut, vil det innebære at tjenesten vil måtte fremme en uoverkommelig mengde begjæringer til domstolen om søk i primærmålets kontakter.

I vurderingen må tas i betraktning at Etterretningstjenesten kun vil se grenseoverskridende kontakter (utlandet-Norge) gjennom tilrettelagt innhenting, og at den utenlandske aktørens norske kontakter ofte vil være begrenset. Mesteparten av en aktørs kommunikasjon går ikke til Norge, men samles inn på andre måter. Tilrettelagt innhenting er således bare en del av datagrunnlaget, men vil kunne vise viktige tilknytninger mellom kjente trusselaktører i utlandet og ukjente aktører i Norge.

Det er viktig for departementet å understreke at adgangen til søk to ledd ut ikke innebærer at Etterretningstjenesten vil ha adgang til å gjennomføre søk i metadata rettet mot de norske kontaktene til en norsk kontakt av et etterretningsmål, jf. forbudet mot innhenting rettet mot personer som befinner seg i Norge i lovutkastet § 4-1. Det er også viktig å understreke at tilrettelagt innhenting ikke kan brukes til å lage nettverkskart til nordmenns kontakter i Norge. Slik metadata vil dessuten være filtrert vekk så langt det er praktisk mulig, jf. lovutkastet § 7-5.

Etter en samlet vurdering mener departementet at Lysne II-utvalgets forslag fremstår som en forsvarlig balansering av hensynet til personvern, etterretningsfaglige hensyn og hensynet til en effektiv ressursbruk. Det foreslås derfor lovfestet som hovedregel at personselektorsøk maksimalt kan inkludere to ledd ut i personenes kommunikasjonskjede. Retten bør imidlertid, under hensyn til det grunnleggende kravet om forholdsmessighet, i særskilte tilfeller kunne fastsette at søk kan inkludere flere eller færre ledd i kommunikasjonskjeden.

Modusselektorsøk vil være en del av Etterretningstjenestens målsøkingsvirksomhet, se nærmere punkt 9.3. En modusselektor er et søkebegrep eller søkestreng som beskriver et

[319] Lysne II-utvalgets rapport om digitalt grenseforsvar av 26. august 2016 punkt 9.3.2 s. 58

bestemt mønster eller avgrensning, herunder handlingsmønster eller geografisk område, jf. legaldefinisjonen i lovutkastet § 1-5 nr. 7. Det ligger i sakens natur at en modusselektor normalt vil være mindre finmasket enn en personselektor. På den andre siden ligger det i grunnvilkåret om forholdsmessighet en begrensning i hvor grovkornet en modusselektor kan være. Av hensyn til risikoen for at trusselaktører vil kunne innrette seg, er det ikke mulig i høringsnotatet å gå i detalj på hvordan en modusselektor typisk vil utformes.

11.14.6.3 Hvem skal kunne foreta søk?

Søk i lagrede metadata vil være inngripende overfor enkeltpersoner. Etter departementets syn er det derfor avgjørende at enhver medarbeider i Etterretningstjenesten som skal foreta slike søk, er skikket til det, både med hensyn til faglig kompetanse og personlige egenskaper. Det foreslås derfor i lovutkastet § 7-8 annet ledd at søk bare skal utføres av personell som er skikket til det og som er utpekt av sjefen for Etterretningstjenesten eller dennes stedfortreder. Det foreslås videre at personellet må ha gjennomgått særskilt opplæring, og at den enkelte bare skal ha anledning til å utføre søk i henhold til søkeprivilegier som er tilpasset dennes oppdragsportefølje. Disse tiltakene vil etter departementets syn styrke tilliten til tjenestens bruk av tilgangen.

Av pedagogiske hensyn foreslås det presisert i lovutkastet § 7-8 tredje ledd at behandling av personopplysninger som Etterretningstjenesten har fått tilgang til etter første ledd, skal skje i samsvar med bestemmelsene i lovutkastet kapittel 9.

Utkast til § 7-8 er utformet slik:

§ 7-8 *Søk i lagrede metadata*

Etterretningstjenesten kan foreta søk i lagrede metadata innenfor rammen av rettens kjennelse etter kapittel 8. Søkene skal baseres på personselektorer eller modusselektorer. Personselektorsøk kan maksimalt inkludere to ledd ut i personenes kommunikasjonskjede, med mindre retten i særskilte tilfeller bestemmer noe annet.

Søk i lagrede metadata kan bare utføres av personell i Etterretningstjenesten som er vurdert som skikket til det og som utpekes av sjefen for Etterretningstjenesten eller dennes stedfortreder. Personellet må ha gjennomgått særskilt opplæring. Den enkelte skal bare ha anledning til å utføre søk i henhold til søkeprivilegier som er tilpasset dennes oppdragsportefølje.

Behandling av personopplysninger som Etterretningstjenesten har fått tilgang til etter første ledd, skal skje i samsvar med bestemmelsene i kapittel 9.

11.14.7 Innhenting og lagring av innholdsdata

Departementet foreslår i lovutkastet § 7-9 første ledd at Etterretningstjenesten kan innhente og lagre innholdsdata med tilhørende metadata fra elektronisk kommunikasjon som transporteres over den norske landegrensen. Det vises til nærmere beskrivelse av verdien av slik innhenting i punkt 11.6 og 11.7. Innholdsdata foreslås legaldefinert som elektronisk kommunikasjon som ikke er metadata. Det er altså innholdet i kommunikasjonen det siktes til, slik som innholdet i en SMS, epost, dokument eller melding på sosialt medium.

En vesentlig forskjell mellom lagring av innholdsdata etter lovutkastet § 7-9 og lagring av metadata etter lovutkastet § 7-7, er at sistnevnte ikke krever rettens kjennelse for selve lagringen, kun for søkene i lagrede data, jf. lovutkastet § 7-8. For lagring av innholdsdata med tilhørende metadata etter § 7-9, krever allerede lagringen domstolens forhåndsgodkjennelse.

Adgangen til innhenting og lagring gjelder utelukkende innenfor rammen av rettens kjennelse etter kapittel 8, eventuelt en ordre som trer i stedet for rettens kjennelse i hastetilfeller, se nærmere punkt 11.11 om domstolens forhåndsgodkjennelse av tilrettelagt innhenting. Det følger av dette at bestemmelsen må sees i sammenheng med lovutkastet kapittel 8, hvor det er gitt regler om saksbehandlingen for domstolen og hva domstolen skal prøve. Departementet viser særlig til lovutkastet § 8-4, hvor det fremgår at retten skal prøve om vilkårene etter loven er oppfylt, herunder at innhentingen ligger innenfor Etterretningstjenestens oppgaver, ikke innebærer brudd på noen av de særskilte innhentingsforbudene og tilfredsstiller grunnvilkårene for innhenting. Innhenting og lagring av innholdsdata etter lovutkastet § 7-9 vil alltid være *målrettet innhenting*, det vil si at det er et grunnvilkår at det foreligger konkrete holdepunkter som tilsier at det foreligger grunn til å undersøke om etterretningsmålet besitter, kommuniserer eller vil motta informasjon som er relevant for etterretningsformål, jf. lovutkastet § 5-2 første ledd.

Innhenting og lagring av innholdsdata med tilhørende metadata etter lovutkastet § 7-9 vil skje målrettet med høy presisjon, slik at det ikke lagres data som ikke omfattes av rettens kjennelse. Målrettet innhenting av innholdsdata kan også skje mot aktører (fysiske eller juridiske personer) som er identifisert som en trusselaktør eller annet etterretningsmål basert på konkrete holdepunkter, selv om den reelle identiteten til personen eller virksomheten som står bak ennå ikke er kjent. Et eksempel kan være en utenlandsk IP-adresse som benyttes til cyberangrep mot mål i Norge. Etterretningstjenesten vil her, forutsatt at domstolen samtykker til det, kunne innhente og lagre innholdsdata i kommunikasjonen som går ut fra IP-adressen, selv om cyberangrepet ennå ikke er attribuert til en bestemt aktør. Innhenting og lagring av innholdsdata i et slikt eksempel vil derimot være avgjørende blant annet nettopp for å kunne avgjøre hvem som står bak angrepet.

Av pedagogiske hensyn foreslås det presisert i lovutkastet § 7-9 annet ledd at behandling av personopplysninger som Etterretningstjenesten har fått tilgang til etter første ledd, skal skje i samsvar med bestemmelsene i lovutkastet kapittel 9.

Departementet foreslår følgende ordlyd:

§ 7-9 *Innhenting og lagring av innholdsdata*

Innenfor rammen av rettens kjennelse etter kapittel 8 kan Etterretningstjenesten innhente og lagre innholdsdata med tilhørende metadata fra elektronisk kommunikasjon som transporteres over den norske landegrensen.

Innholdsdata er data som ikke er metadata.

Behandling av personopplysninger som Etterretningstjenesten har fått tilgang til etter første ledd, skal skje i samsvar med bestemmelsene i kapittel 9.

11.15 Tilretteleggingsplikt for ekomindustrien

11.15.1 Bør det oppstilles en tilretteleggingsplikt for ekomindustrien?

Innhenting av grenseoverskridende elektronisk kommunikasjon i fiberoptiske kabler krever tilrettelegging fra aktører i ekomindustrien. Etterretningstjenesten vil for eksempel ha behov for å installere og operere utstyr på steder som kontrolleres av tilbydere. Et første spørsmål

er hvorvidt en plikt for relevante aktører til å tilrettelegge for innhentingen, bør lovfestes. Lysne II-utvalget skriver om spørsmålet i sin rapport:[320]

> «En slik medvirknings- og tilretteleggingsplikt er nødvendig for å oppnå formålet med DGF, og for å unngå at hensynet til viktige nasjonale interesser overlates til den enkelte tilbyder å vurdere viktigheten av. En plikt til utlevering og medvirkning vil stille alle tilbydere likt, og man vil unngå at enkelte tilbydere unnviker et samarbeid ut fra konkurransemessige eller andre hensyn, herunder eventuelt press fra utenlandske eierinteresser som ikke har den samme motivasjon til å bidra til å trygge norske viktige interesser. På den annen side ligger det i sakens natur at formelle pålegg kun vil være et aktuelt middel dersom frivillig samarbeid ikke fører frem.»

Departementet slutter seg til dette. Hensyn til likebehandling og forutberegnelighet tilsier at det bør lovfestes en tilretteleggingsplikt som gjelder likt for alle relevante aktører. Det vil ikke være tilfredsstillende om Etterretningstjenesten skal være henvist til å inngå avtaler med den enkelte aktør basert på frivillighet. Departementet går på denne bakgrunn inn for å lovfeste plikten til å tilrettelegge for Etterretningstjenestens tilgang i lovutkastet § 7-2.

11.15.2 Hvem skal tilretteleggingsplikten gjelde for?

Det neste spørsmålet er hvem tilretteleggingsplikten skal gjelde for. Lysne II-utvalget skriver om dette:[321]

> «I utgangspunktet vil tilretteleggingsplikten gjelde for alle tilbydere som definert i ekomloven § 1-5. Det er på forhånd ikke gitt å identifisere hvilke tilbydere av kommunikasjonstjenester som vil bli mest berørt av lovforslaget. Dette vil bero på testvirksomhet og analyser av hvem som antas å bære størst andel av utenlandsetterretningsrelevant kommunikasjon, og det må også tas høyde for raske og mer langsiktige endringer av dette bildet. I utgangspunktet vil enhver tilbyder kunne bli berørt, i den utstrekning de kan gi tilgang til elektronisk kommunikasjon som går over landegrensene.»

Departementet er enig med utvalget i at tilretteleggingsplikten bør gjelde for alle som regnes som tilbydere etter definisjonen i ekomloven § 1-5 nr. 16,[322] det vil si enhver fysisk eller juridisk person som tilbyr andre tilgang til elektronisk kommunikasjonsnett eller -tjeneste. Det vil i tillegg være behov for tilrettelegging fra tilbydere av innholdstjenester som ikke er omfattet av definisjonen i ekomloven, typisk internettbaserte «over the top-tjenester» (OTT-tjenester) som kan brukes til overføring av tekst, lyd og bilder. Departementet foreslår at også tilbydere av slike tjenester i Norge skal være omfattet av tilretteleggingsplikten når det er nødvendig for å sikre Etterretningstjenestens tilgang til grenseoverskridende elektronisk kommunikasjon. Det vil for eksempel kunne være behov for å sørge for tilgang til kommunikasjon uten hinder av kryptering som tjenestetilbyderen kontrollerer.

11.15.3 Tilretteleggingspliktens innhold

Tilretteleggingsplikten innebærer på et generelt nivå at relevante tilbydere skal legge til rette for at Etterretningstjenesten får tilgang til elektronisk kommunikasjon som transporteres over den norske landegrensen. Det nærmere innholdet av plikten vil blant annet avhenge av

[320] Lysne II-utvalgets rapport om digitalt grenseforsvar av 26. august 2016 punkt 9.5.4 s. 69

[321] Ibid punkt 9.5.4 s. 69

[322] Lov av 4. juli 2003 nr. 83 om elektronisk kommunikasjon

hvilket nett eller tjeneste det er snakk om, og vil i takt med den teknologiske utviklingen kunne variere over tid. Departementet foreslår på denne bakgrunn å lovfeste en generell plikt i lovutkastet § 7-2 første ledd, som konkretiseres ved hjelp av en ikke-uttømmende opplisting i annet ledd.

Tilretteleggingsplikten bør for det første inkludere plikt til å gi informasjon om signalmiljø, dataformater, tekniske innretninger og fremgangsmåter, i den utstrekning det er nødvendig for å oppfylle tilretteleggingspliktens formål, jf. annet ledd bokstav a.

Etterretningstjenesten vil ha behov for å installere og operere utstyr på steder som kontrolleres av tilbyder, jf. annet ledd bokstav b. Tilbyder vil ha plikt til å tillate slik virksomhet, for eksempel ved å gi adgang til teknisk personell fra Etterretningstjenesten og stille til disposisjon plass til utstyr. Etter anmodning fra Etterretningstjenesten vil tilbyder også ha plikt til å medvirke til teknisk drift og vedlikehold av etablerte løsninger.

Tilretteleggingsplikten bør også inkludere en plikt til å bidra til at Etterretningstjenesten kan gjennomføre testinnhenting og testanalyser av trafikk i nett og tjenester, jf. annet ledd bokstav c. Det vises til punkt 11.14.4 over og lovutkastet § 7-6.

Når det gjelder kryptering, uttaler Lysne II-utvalget i sin rapport:[323]

> «Det er antatt at utviklingen innen sikkerhetsteknologi vil gjøre bruken av sterk kryptering av samband og tjenester mer vanlig i årene fremover. Dette er et positivt tiltak for kommunikasjonsfriheten og for generelt å hindre uvedkommende adgang til informasjon. Utviklingen vil samtidig kunne vanskeliggjøre E-tjenestens samfunnsoppdrag. Tjenestetilbydernes tilretteleggingsplikt må ta høyde for utviklingen innen kryptering. Tilretteleggingsplikten for teletilbyderne må derfor omfatte leveranse av datastrøm uten linkkryptering dersom dette er implementert på den grensekryssende forbindelsen. Tilretteleggingsplikten bør imidlertid ikke inneholde krav om støtte til omgåelse av krypto utover dette. F.eks. vil brukergenerert kryptering ikke være omfattet av tilretteleggingsplikten.»

Departementet slutter seg til dette, og foreslår å lovfeste at tilretteleggingsplikten inkluderer en plikt til å sørge for tilgang til kommunikasjon uten hinder av linkkryptering eller lignende kryptering som tilbyder kontrollerer, jf. annet ledd bokstav d. Tilretteleggingsplikten skal derimot ikke innebære en plikt til å bidra til annen omgåelse av kryptering, og departementets forslag går dermed ikke lenger enn Lysne II-utvalgets anbefaling.

Tilretteleggingsplikten bør dessuten omfatte plikt til å medvirke til sikkerhetsmessig forsvarlige løsninger, herunder at Etterretningstjenestens utstyr og tilstedeværelse gjøres kjent for færrest mulig personer hos tilbyder og bare for de som har tjenstlig behov for det, jf. annet ledd bokstav e.

Det foreslås i lovutkastet § 7-2 tredje ledd at departementet kan fastsette nærmere regler om tilretteleggingsplikten i forskrift.

11.15.4 Plassering og utforming av bestemmelsen om tilretteleggingsplikt

Departementet har vurdert om bestemmelsen om tilretteleggingsplikt bør inntas i lovutkastet her eller i ekomloven. At plikten primært retter seg mot aktører som omfattes av ekomloven, kan tale for å plassere bestemmelsen der. På den andre siden vil det være en klar fordel å samle bestemmelsene om tilrettelagt innhenting i lov om Etterretningstjenesten.

[323] Lysne II-utvalgets rapport om digitalt grenseforsvar av 26. august 2016 punkt 9.5.4 s. 68–69

Departementet antar derfor at det er mest hensiktsmessig å plassere bestemmelsen om tilretteleggingsplikt i lovutkastet kapittel 7. For sammenhengens skyld kan det eventuelt inntas en henvisning i ekomloven til bestemmelsen i lovutkastet her. Departementet ber om høringsinstansenes syn på spørsmålet.

Bestemmelsen om tilretteleggingsplikt kan plasseres i lovutkastet § 7-2 og utformes slik:

§ 7-2 *Tilretteleggingsplikt*

Tilbydere som omfattes av ekomloven § 1-5 nr. 16 og tilbydere av internettbaserte kommunikasjons- eller meldingstjenester som er tilgjengelige for allmennheten skal legge til rette for at Etterretningstjenesten kan innhente elektronisk kommunikasjon som transporteres over den norske landegrensen.

Tilretteleggingsplikten innebærer plikt til på egnet måte å speile og gjøre kommunikasjonsstrømmene tilgjengelige for Etterretningstjenesten, og på annen måte tilrettelegge for at Etterretningstjenesten kan gjennomføre utvalg, filtrering, testing, lagring og søk som beskrevet i kapittelet her, herunder

a. gi informasjon om signalmiljø, dataformater, tekniske innretninger og fremgangsmåter, i den utstrekning det er nødvendig for å oppfylle tilretteleggingspliktens formål,
b. tillate at Etterretningstjenesten installerer utstyr og etablerer midlertidig eller permanent tilstedeværelse for å drifte utstyr på steder som kontrolleres av tilbyder, og etter anmodning fra Etterretningstjenesten medvirke til teknisk drift og vedlikehold av etablerte løsninger,
c. bidra til at Etterretningstjenesten kan gjennomføre testinnhenting og testanalyser av trafikk i nett og tjenester,
d. sørge for tilgang til kommunikasjon uten hinder av linkkryptering eller lignende kryptering som tilbyder kontrollerer, og
e. medvirke til sikkerhetsmessig forsvarlige løsninger, herunder at Etterretningstjenestens utstyr og tilstedeværelse gjøres kjent for færrest mulig personer hos tilbyder og bare for de som har tjenstlig behov for det.

Departementet kan gi forskrift om tilretteleggingsplikten.

En eventuell henvisningsbestemmelse i ekomloven kan plasseres i et nytt fjerde ledd i ekomloven § 2-8 og lyde slik:

Regler om tilretteleggingsplikt for Etterretningstjenestens innhenting av elektronisk kommunikasjon som transporteres over den norske landegrensen følger av lov om Etterretningstjenesten § 7-2.

Et siste alternativ er å plassere hele bestemmelsen (som formulert i utkast til § 7-2) i ekomloven som ny § 2-8 a.

11.15.5 Taushetsplikt

Departementet foreslår i lovutkastet § 7-3 første ledd at den som er underlagt tilretteleggingsplikt, plikter å bevare taushet om Etterretningstjenestens tilgang, tekniske løsninger og andre forhold knyttet til gjennomføring av tilretteleggingen. Det samme skal gjelde enhver som utfører arbeid eller tjeneste for den som er underlagt tilretteleggingsplikt eller som på annen måte bistår i gjennomføring av tilrettelegging. Taushetsplikten skal gjelde også etter at vedkommende har avsluttet arbeidet eller tjenesten. En slik taushetsplikt er nødvendig for å skjerme Etterretningstjenestens virksomhet. Etter lovutkastet § 7-3 annet ledd skal taushetsplikten imidlertid ikke være til hinder for å gi opplysninger til EOS-utvalget eller Nasjonal kommunikasjonsmyndighet.

Departementet foreslår følgende bestemmelse:

§ 7-3 *Taushetsplikt*

Den som er underlagt tilretteleggingsplikt etter § 7-2 plikter å bevare taushet om Etterretningstjenestens tilgang, tekniske løsninger og andre forhold knyttet til gjennomføring av tilretteleggingen. Taushetsplikten gjelder også for enhver som utfører arbeid eller tjeneste for den som er underlagt tilretteleggingsplikt etter § 7-2 eller som på annen måte bistår i gjennomføring av tilrettelegging. Taushetsplikten fortsetter å gjelde også etter at vedkommende har avsluttet arbeidet eller tjenesten.

Taushetsplikten er ikke til hinder for å gi opplysninger til EOS-utvalget eller Nasjonal kommunikasjonsmyndighet.

11.15.6 Utgiftsdekning

11.15.6.1 Generelt

Som det fremgår av drøftelsen over foreslås det et system der ekomtilbyderne speiler eller på annen måte gjør grenseoverskridende kommunikasjonsstrømmer tilgjengelige for lagring. Lysne II-utvalget la i sin rapport til grunn som prinsipp at staten ville dekke merutgiftene for tilbyderne knyttet til tilretteleggingsplikten.[324]

Departementet vil i det følgende vurdere hvorvidt Lysne II-utvalgets anbefaling bør støttes. I dette ligger spørsmålet om *hvem* som står nærmest til å dekke utgiftene, *hvilke* utgifter som i så fall bør dekkes og *hvorvidt* prinsippet for utgiftsdekningen skal fremgå av loven eller av annet regelverk.

11.15.6.2 Hvem bør dekke utgiftene?

Departementet mener at det i denne vurderingen er naturlig å se hen til hvordan utgiftsdekningen løses i ekomsektoren for øvrig. Ekomtilbyderne er pålagt en generell tilretteleggingsplikt i ekomloven § 2-8.[325] Kostnadsfordelingen er regulert av bestemmelsens annet ledd, hvor det følger at tilbyders driftskostnader knyttet til oppfyllelse av tilretteleggingsplikten dekkes av staten for de merkostnader som følger av disse tjenestene. Politiets kommunikasjonskontroll er et relevant eksempel i denne sammenheng. Departementet mener det er et tungtveiende argument at det gjeldende prinsippet i ekomsektoren er at staten dekker driftsutgifter forbundet med all tilsvarende lovbestemt tilretteleggingsplikt. Departementet ser ikke at det foreligger gode grunner for å avvike fra dette prinsippet for et tiltak som gjøres av hensyn til nasjonal sikkerhet.

Et annet argument er at selv om tilretteleggingsplikten i utgangspunktet gjelder likt for alle tilbydere jf. lovforslaget § 7-2 første ledd, så er det ikke på forhånd gitt hvilke tilbydere som faktisk vil berøres av plikten til enhver tid. Det er lite sannsynlig at man vil være i stand til å innhente grenseoverskridende kommunikasjon fra alle ekomtilbydere som omfattes av lovforslaget. Etterretningstjenesten vil derfor måtte velge ut de kommunikasjonsstrømmene som antas å være aller mest etterretningsrelevante. Rent faktisk vil dermed tilretteleggingsplikten kunne medføre en uforutsigbarhet for markedsaktørene, og det kan fremstå som urimelig at enkelte tilbydere blir pålagt å dekke en utgift som andre slipper unna. Dette vil potensielt kunne få en utilsiktet konkurransemessig effekt. Utgiftene forbundet med tilretteleggingsplikten vil dessuten kunne ramme små aktører hardere enn

[324] Lysne II-utvalgets rapport om digitalt grenseforsvar av 26. august 2016 punkt 9.5.4 s. 68

[325] Lov av 4. juli 2003 nr. 83 om elektronisk kommunikasjon. Det bemerkes at e-komloven bruker begrepet «merkostnader». Departementet legger kontantprinsippet til grunn og bruker derfor begrepet «merutgifter».

større selskaper, som ofte vil ha bedre økonomiske forutsetninger for å håndtere uforutsette utgiftsposter.

For det tredje er det av hensyn til nasjonal sikkerhet lite ønskelig at utgifter forbundet med tilretteleggingsplikten skal fremgå av ekomtilbydernes regnskaper fordi dette kan avsløre Etterretningstjenestens geografiske innhentingsfokus samt gi trusselaktører varsel om å unngå bestemte tjenester. Det vil være behov for å skjerme slik informasjon for å hindre innsyn i hvilke kommunikasjonsstrømmer man innhenter informasjon fra. Motsatt vil etterretningsaktører kunne innrette sin handlemåte etter dette. Skjermingsplikten følger både av sikkerhetsloven og etterretningstjenesteloven. Det vises også til vedtak av Kongen i statsråd 29. januar 1993 og av Stortinget 13. mars 1993 om skjerming av Etterretningstjenestens regnskaper. Skjermingsbehovet vurderes å lettere kunne ivaretas gjennom etterhånds merutgiftsdekning fordi utlegg fra det offentlige til den enkelte tilbyder vil enklere kunne inkluderes i inntektsposter på en måte som ikke offentlig spesifiserer tilretteleggingsplikt for Etterretningstjenesten. Det anses tilstrekkelig at spesifikasjon av merutgiftsdekningen og andre detaljer på vanlig måte vil kontrolleres av Riksrevisjonen i forbindelse med revisjon og kontroll av Etterretningstjenestens regnskaper.

Departementet mener disse argumentene i sum taler for at staten dekker merutgiftene for teletilbyderne. At staten har anledning til å pålegge rettssubjekter plikter uten å kompensere dette økonomisk er ikke i seg selv et argument for å anbefale en slik løsning.

11.15.6.3 Hvilke utgifter bør dekkes?

Neste spørsmål er om staten bør dekke merutgifter både til investering og drift, eller utelukkende merutgifter knyttet til *drift*. I utgangspunktet vil det være naturlig å legge den norm til grunn som gjelder i ekomsektoren forøvrig. Det vil tilsi at bare driftsutgiftene dekkes. Samtidig har departementet vurdert investeringsutgiftene som så marginale sett i forhold til de utgifter som tilrettelagt innhenting vil beløpe seg til totalt sett, at det har lite for seg å skille mellom investering og drift i dette tilfellet. På samme tid kan eventuelle investeringsutgifter fremstå som en uforutsett kostnad for den enkelte tilbyder, og dermed falle urimelig ut. Det vises til det som er sagt om dette over. Departementet anbefaler derfor at det ikke skilles mellom merutgifter til investering og drift etter lovforslaget.

Et annet spørsmål er hvilke utgifter som bør omfattes av begrepet «merutgifter». Som et naturlig utgangspunkt bør begrepet kun omfatte direkte merutgifter som klart kan henføres til tiltak tilbyderen har gjort for å oppfylle tilretteleggingsplikten. Negativt betegnet bør «merutgifter» ikke omfatte utgifter som tilbyderne uansett ville hatt, for eksempel som følge av oppfyllelse av plikter etter konsesjon eller sikkerhetsloven. Utgangspunktet etter sikkerhetsloven er at den enkelte virksomhet som omfattes av loven må finansiere utgiftene forbundet med forebyggende sikkerhetstiltak selv, og at utgiftene dekkes av det enkelte pliktsubjekt etter loven. Dette vil kunne stille seg annerledes dersom tilbyderen utelukkende omfattes av sikkerhetsloven som følge av tilretteleggingsplikten. I slike tilfeller kan utgiftene for oppfyllelse av sikkerhetslovens krav henføres til tilrettelagt innhenting, slik at staten er nærmest til å dekke disse.

Beregningen av utgifter bør skje på en slik måte at staten ikke i realiteten dekker utgifter som tilbyderen uansett ville hatt. For eksempel vil utgifter til vedlikehold av utstyr og oppgradering av programvare som ikke benyttes utelukkende til tilrettelagt innhenting ikke kunne pålegges staten å betale. Videre bør det gjelde et prinsipp om kostnadsminimering. Dette innebærer for eksempel at tilbyderen ikke kan foreta investeringer uten at driftskostnadene er vurdert

og søkt redusert i den grad det er mulig. Nærmere bestemmelser om definering og beregning av merutgifter foreslås fastsatt i forskrift, jf. § 7-4 andre ledd.

Departementet vurderer at ordningen kan etableres som en kompensasjonsordning hvor dokumenterte og direkte påløpte utgifter til tilretteleggingsplikten kan søkes kompensert av staten. Gjennomføringen av en slik ordning bør skje på en måte som sikrer forutberegnelighet og innrettelsesbehov for partene, samt behovet for skjerming.

11.15.6.4 Hvordan bør utgiftsdekningen reguleres?

Departementet vurdert hvorvidt det er behov for å fastsette normen for utgiftsdekning i loven. Reglene for hvordan kompensasjonen rent praktisk skal beregnes og gjennomføres vil uansett måtte fastsettes i underliggende regelverk. Dette trekker i retning av at man delegerer til forskrift å fastsette de nærmere prinsipper for utgiftsdekning, eventuelt supplert med veiledende omtale i lovens forarbeider. En slik løsning vil sikre mer fleksibilitet i regelverket. På den annen side er prinsippet i ekomloven fastlagt i lov. Lovregulering skaper dessuten større grad av forutsigbarhet for tilbyderne.

Etter en avveining har departementet kommet frem til at man vil anbefale at prinsippet fremgår av loven, men ønsker særlig høringsinstansenes syn på dette.

11.15.6.5 Får EØS-avtalens regler om statsstøtte anvendelse?

Departementet har vurdert om merutgiftsdekningen som foreslås omfattes av EØS-avtalen artikkel 61 om statsstøtte. Bestemmelsens første ledd oppstiller en rekke kumulative vilkår for at noe skal anses som statsstøtte, og lyder som følger:

> Med de unntak som er fastsatt i denne avtale, skal støtte gitt av EFs medlemsstater eller EFTA-statene eller støtte gitt av statsmidler i enhver form, som vrir eller truer med å vri konkurransen ved å begunstige enkelte foretak eller produksjonen av enkelte varer, være uforenlig med denne avtales funksjon i den utstrekning støtten påvirker samhandelen mellom avtalepartene.

For at en utbetaling av statsmidler skal anses som «støtte» etter EØS-avtalen, må den altså begunstige mottakeren økonomisk på en måte som kan være konkurransevridende og således kan påvirke samhandelen mellom partene i EØS-avtalen. Med andre ord må utbetalingen av statsmidler gi mottakeren en økonomisk fordel.

Departementets forslag vil utelukkende kompensere for en økonomisk byrde som normalt ikke belastes de angjeldende virksomhetenes budsjett. Ordningen vil således ikke begunstige tilbyderne, men heller stille dem økonomisk som om tilretteleggingsplikten ikke hadde blitt pålagt dem. Ordningen kan således ikke anses å inneholde støtteelementer som gir mottagende virksomhet en økonomisk fordel. Departementet konkluderer på denne bakgrunn med at statsstøttereglene ikke får anvendelse på merutgiftsdekningen slik den er beskrevet i kapittelet her.

11.15.6.6 Departementets forslag

Departementet foreslår følgende regulering av utgiftsdekningen:

§ 7-4 *Utgiftsdekning*

> Merutgifter for tilbyder som følge av tilretteleggingsplikten dekkes av staten.
> Departementet kan gi forskrift om prinsipper for utregning av merutgiftene.

11.16 Økonomiske og administrative konsekvenser

11.16.1 Innledning

Departementet vurderer at forslaget om tilrettelagt innhenting som beskrevet i kapittelet her vil medføre direkte ressursmessige konsekvenser for Etterretningstjenesten, tilbyderne som omfattes av tilretteleggingsplikten, Oslo tingrett og EOS-utvalget. Departementet vil i det følgende drøfte hvilke økonomiske og administrative konsekvenser dette forventes å være. Videre er spørsmålet om, og i tilfelle hvordan, slike ressursmessige konsekvenser kan søkes redusert uten at dette får vesentlig negativ betydning for personvernet og rettssikkerheten.

Departementet har etterstrebet å konkretisere kostnadsdriverne og beregne kostnadene så godt som mulig. Det samme gjelder beregningen av de økonomiske og administrative konsekvensene som en implementering av tilrettelagt innhenting kan medføre for aktørene som berøres av lovforslaget. Kostnadsberegninger utover de som følger av drøftelsene i høringsnotatet her vil foretas på et senere tidspunkt, se nærmere om dette i punkt 11.16.5.2 under.

11.16.2 Kort om behovet for tilrettelagt innhenting[326]

Den teknologiske utviklingen medfører store gevinster for Norge. Private og offentlige personer og virksomheter benytter digitale løsninger i stadig større grad. Dette skjer både på det nasjonale og det internasjonale plan. Kommunikasjon over landegrensene kan skje enkelt og hurtig. Det er ingenting som tyder på at utviklingen vil stagnere.

Dette er ikke utelukkende positivt. Trusselaktører finner stadig nye muligheter til å kommunisere seg imellom, formidle propaganda, planlegge terrorhandlinger og gjennomføre digitale anslag, og det digitale rom benyttes for spionasje og påvirkningsoperasjoner rettet mot norske myndigheter og borgere. Den teknologiske utviklingen bringer følgelig med seg sårbarheter og utfordringer som, dersom de ikke håndteres på riktig måte, kan medføre store samfunnsmessige konsekvenser i både økonomisk og menneskelig forstand.

De siste årene har vi fått erfare hvilke alvorlige samfunnsmessige og økonomiske konsekvenser terror- og cyberrelaterte hendelser kan medføre. Selv om terroranslaget 22. juli 2011 ikke var av utenlandsk opprinnelse, og dermed utenfor Etterretningstjenestens oppgavesett, kan det tjene som et eksempel. Kostnadene for bygging av et nytt regjeringskvartal er ikke beregnet fullt ut ennå, men Statsbygg har gitt foreløpige estimater om at kostnadene kan beløpe seg til 5,8 mrd. kroner.[327] De økonomiske tapene som kan knyttes til materielle skader blekner imidlertid i forhold til de enorme menneskelige tapene og skadene etter terrorangrepene i regjeringskvartalet og på Utøya.

Et annet eksempel på en alvorlig hendelse er de omfattende og alvorlige nettverksoperasjonene mot datasystemene til Helse Sør-Øst som ble avdekket i januar 2018, hvor fremmede aktører fikk tilgang til 2,9 millioner nordmenns pasientdata. Det er

[326] Departementet har utførlig redegjort for behovet for tilrettelagt innhenting og de alternative løsningene som har vært vurdert i punkt 11.6 og 11.7.

[327] Dette vil bli nærmere utredet i det pågående forprosjekteringsarbeidet. Kostnadene skal deretter ekstern kvalitetssikres før et prosjekt legges frem for Stortinget med forslag til kostnadsramme for investeringen, sannsynligvis i 2019.

vanskelig å tallfeste de økonomiske konsekvensene knyttet til slike cyberhendelser, men tyveri av sensitiv informasjon kommer utvilsomt med en pris av både personvernmessig og økonomisk art. Det er sannsynlig at angrepet mot Helse Sør-Øst kunne vært stanset tidligere dersom Etterretningstjenesten hadde hatt tilgang til grenseoverskridende elektronisk kommunikasjon på tidspunktet da hackingen skjedde.

Enkelte andre trusler som Etterretningstjenesten forsøker å avdekke kan etter sin art være krevende å kostnadsfeste. Verdien av at et valgresultat *ikke* blir manipulert lar seg vanskelig måle i kroner og øre. Det samme gjelder andre former for påvirkningsoperasjoner i det digitale rom.[328]

Lovforslaget her innebærer å gi Etterretningstjenesten et *hjemmelsgrunnlag for å innhente informasjon* som tjenesten ikke har tilgang til i dag. Hjemmelsgrunnlaget er en nødvendig forutsetning for at det på et senere tidspunkt kan *investeres* i et system som gir den nevnte aksessen, og som gir Etterretningstjenesten anledning til å avdekke og følge uønsket aktivitet rettet mot Norge. Tilrettelagt innhenting vil da være et virkemiddel for å avverge at trusler får manifestere seg, og ha særlig betydning for Etterretningstjenestens arbeid mot grenseoverskridende terrorisme, digitale anslag mot norske myndigheter eller borgere, samt sabotasje og spionasje i det digitale rom.

11.16.3 Hvilke økonomiske og administrative konsekvenser kan tilrettelagt innhenting medføre?

Generelt kan de kostnadsdrivende faktorene kategoriseres som følger:

- behov for nye stillingshjemler, og følgelig utgifter til lønn og andre personellutgifter,
- utgifter knyttet til utstyr, eiendom, bygg og anlegg,
- behov for administrative investeringer og
- behov for midler til drift og oppgradering av tekniske løsninger.

De administrative konsekvensene av løsningen kan generelt oppsummeres i følgende momenter:

- etablering av nye rutiner og prosedyrer,
- opplæring av personell, herunder etterutdanning, og
- enkelte krav til personell i forbindelse med beslutnings- eller handlingskompetanse.

11.16.4 Hvilken samfunnsnytte kan tilrettelagt innhenting gi?

Samfunnsnytten av tilrettelagt innhenting kan oppsummeres som følger:

- forbedret nasjonal evne til å rettidig avdekke alvorlige hendelser og angrep og økt evne til rask og adekvat håndtering,
- bedre og tidligere deteksjon av potensielle trusler i det digitale rom og etterretningsrelevant kommunikasjon mellom trusselaktører sammenlignet med det som er tilfelle i dag,
- bidrag til å forhindre at norsk infrastruktur blir brukt for å understøtte angrep mot andre land,

[328] I Fokus 2018 viser Etterretningstjenesten til at fremmede makter manipulerer og undertrykker folks virkelighetsoppfatning gjennom spredning av desinformasjon og propaganda, se side 30.

- forbedret evne til situasjonsforståelse, herunder forståelse av trusselaktører, omfanget av trusler og tilknytningspunkter mellom ulike aktører,
- forbedret evne til retrospektiv analyse av etterretningsrelevant informasjon og
- ervervelse av verdifull etterretningsinformasjon til partnere nasjonalt og internasjonalt.

Det vises for øvrig til punkt 11.6 som redegjør det for behovet for tilgang til grenseoverskridende elektronisk kommunikasjon og til punkt 11.7 hvor alternative løsningsforslag drøftes.

11.16.5 Økonomiske og administrative konsekvenser for Etterretningstjenesten

11.16.5.1 Økonomiske og administrative konsekvenser

De ressursmessige konsekvensene av lovforslaget om tilrettelagt innhenting vil få størst betydning for Etterretningstjenesten. Departementet har parallelt med utredningen av herværende lovforslag hatt dialog med tjenesten for å få kartlagt hvilke økonomiske og administrative konsekvenser dette vil medføre for tjenesten. I tillegg til usikkerheten som hefter rundt en eventuell anskaffelse på nåværende tidspunkt, er departementet tilbakeholdent med å estimere økonomiske konsekvenser knyttet til personell og materielle investeringer av hensyn til sensitiviteten som generelt gjelder for Etterretningstjenestens virksomhet, samt gradering av enkelte detaljopplysninger. Full åpenhet om dette vil kunne være verdifull informasjon for aktører som ønsker å kartlegge Norges kapasiteter.

Som følge av Etterretningstjenestens særskilte behov for skjerming av kapasiteter, metoder og utenlandske samarbeidspartnere har tjenesten organisert anskaffelsesvirksomheten som en integrert del av organisasjonen. Sjefen for Etterretningstjenesten gjør anskaffelser og rapporterer til Forsvarsdepartementet gjennom den styringen som er beskrevet i høringsnotatet punkt 6.5. Anskaffelsene planlegges langsiktig i form av investeringsplaner med samme tidshorisont og finansielle forutsetninger som gjelder for øvrige deler av forsvarssektoren.

Investeringsvirksomheten i Etterretningstjenesten følger alminnelige lover og regler for offentlige anskaffelser, og legger Forsvarsdepartementets rammeverk for materiellanskaffelser[329] og for anskaffelse av eiendom, bygg og anlegg (EBA) til grunn. Etterretningstjenestens planer for investeringer legges frem for, og godkjennes av, Forsvarsdepartementet. Det er et betydelig samarbeid med Forsvarsmateriell og Forsvarsbygg for anskaffelser til Etterretningstjenesten.

Gjennom arbeidet så langt har departementet identifisert administrative og økonomiske konsekvenser knyttet til *prosjektering* og selve *anskaffelsen* og *installeringen* av systemene for tilrettelagt innhenting. Utgifter for etablering av tiltaket i en oppstartsfase, inkludert materiell, EBA og personell, er *foreløpig* estimert til ca. 700 mill. kroner. En eventuell anskaffelse vil bli lagt frem for Stortingets godkjennelse. Periodiseringen av utgiftene utredes etter hvert som prosjektarbeidet drives fremover. Prosjekteringen vil medføre behov for å styrke Etterretningstjenesten personellmessig. Personellbehovet er antatt å øke gradvis fra prosjektstart frem til driftssetting.

Videre må det påregnes utgifter knyttet til *drift av systemene.* Etter driftssetting av den tilrettelagte innhentingen vil Etterretningstjenesten ha behov for en permanent styrking av sin

[329] https://forsvaret.no/prinsix

personellstruktur med tilhørende økning i personelldriftsutgiftene. Også vedlikehold av utstyr og programvare vil etter all sannsynlighet være en kostnadsdriver.

Det kan anslås at forslaget om tilrettelagt innhenting vil medføre økning på færre enn hundre nye stillinger. Personellutgifter knyttet til nytilsatte ved Etterretningstjenesten vil knyttes til lønn, arbeidsgiveravgift, reiseutgifter, kompetanseutvikling o.l. Også eksisterende personell som skal involveres i tilrettelagt innhenting må gis nødvendig kompetanseheving som er kostnadsberegnet som en del av gjennomførings- og driftsutgiftene. Behovet for tilførsel av stillinger kan påvirkes av endringer i trusselbildet, aktuelle tjenesteleverandører i Norge og den teknologiske utviklingen i verden generelt.

Tilrettelagt innhenting vil medføre behov for å etablere enkelte nye *administrative* rutiner for å følge opp særskilte forhold. Dette inkluderer rutiner rundt rettsanmodninger og –kjennelser, vedlikehold av filtreringsløsninger og dialog med tjenesteleverandører. I tillegg vil det være behov for administrative rutiner knyttet til EOS-utvalgets styrkede kontroll av Etterretningstjenestens bruk av tilrettelagt innhenting.

Forslaget vil videre medføre utgifter til etablering og eie eller leie av eiendom, bygg og anlegg. Driverne bak behovet vil være økningen i antall stillinger, forhold rundt samband til tjenesteleverandørene, samt utvidelse av løsninger tilknyttet Etterretningstjenestens systemer for prosessering og lagring. Usikkerhetsmomenter knyttet til EBA på nåværende tidspunkt er i noen grad usikkerhet rundt faktisk teknisk løsning og forventet personellbehov, og i særlig grad det reelle omfanget av tilbydernes tilrettelegging.

11.16.5.2 Særlig om departementets prosjektarbeid knyttet til tilrettelagt innhenting

Departementet har etablert et prosjekt som skal ivareta behovet for nødvendige utredninger og kostnadsberegninger forut for en eventuell implementering av tilrettelagt innhenting. Prosjektet vil sørge for at påkrevde samfunnsøkonomiske analyser og andre kost/nytte-vurderinger foretas.

Prosjektet har som formål å tilrettelegge for og eventuelt gjennomføre en anskaffelse forutsatt at lovforslaget om tilrettelagt innhenting blir vedtatt. Prosjektet skal utarbeide nødvendige grunnlag for beslutninger i departementet, regjeringen og Stortinget. Det understrekes at anskaffelse av tilrettelagt innhenting forutsetter at Stortinget har besluttet at tilrettelagt innhenting skal innføres.

Arbeidet ledes av departementet og gjennomføres i samarbeid med Etterretningstjenesten. Prosjektarbeidet tilpasses tjenestens særegne behov i den grad dette er nødvendig, slik som hensynet til sikkerhetsgradering av informasjon.

I det pågående arbeidet legges det til grunn et overordnet konsept for tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon. Konseptet danner rammene for etableringen av den tekniske løsningen. Den endelige systemløsningen vil være basert på alternative designvalg avhengig av praktiske forhold som må avklares nærmere når systemet skal utformes, implementeres og realiseres. Detaljprosjekteringen må basere seg på nærmere utredning og testing av mulighetsrommet i samvirke med utvalgte tilbydere. Dette vil kunne resultere i mer formålstjenlige scenarier og løsningsvalg enn det som så langt har vært mulig å avklare. Dette er ikke en uvanlig fremgangsmåte i prosjekter som involverer anskaffelser av blant annet IKT-utstyr.

Kostnadene for innføringen av tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon utredes i prosjektdefinisjonsfasen. Basert på en gitt ambisjon er det

beregnet utgifter innenfor ulike utgiftstyper som EBA, materiell og personell. Kostnadsestimatene er basert på erfaringstall med tanke på energiutgifter, sikringsutgifter og utgifter for EBA. I tillegg er personellutgifter beregnet ut fra forventet lønnstrinn og andre personellutgifter.

Utgifter for materiell tar utgangspunkt i datamengde i en skissert løsning samt innhenting av priser på ulike typer utstyr. Det er også gjort anslag over utgifter for spesialutstyr og leie/eie av fiber.

11.16.6 Økonomiske og administrative konsekvenser knyttet til kontrollmekanismene

11.16.6.1 Generelt

Departementet foreslår at tilrettelagt innhenting implementeres med en rekke kontroll- og sikkerhetsmekanismer. Kontrollen av tilrettelagt innhenting vil i en viss utstrekning bygge på allerede eksisterende kompetanse og innretninger ved at det er domstolen og EOS-utvalget som foreslås å utføre kontrolloppgavene. I tillegg vil Nasjonal kommunikasjonsmyndighet (Nkom) og Nasjonal sikkerhetsmyndighet (NSM) føre kontroll etter deres respektive rettsgrunnlag, uten at dette forventes å medføre kostnader av nevneverdig betydning. Departementet foreslår ikke at det opprettes særorganer for å forestå kontrollen av tilrettelagt innhenting. Departementet vurderer at det vil være kostnadsreduserende å tillegge kontrolloppgavene til allerede eksisterende organer, samtidig som hensynene til effektiv og uavhengig kontroll ivaretas på en god og egnet måte.

Departementets forslag om innretningen av kontrollmekanismene følger til dels av menneskeretts- og personvernforpliktelser. De utgiftene som kan henføres til tiltak med formål å oppfylle menneskerettslige krav er etter departementets syn uunngåelige. I tillegg er omfanget av kontroll- og sikkerhetsmekanismene begrunnet i ytterligere hensyn som departementet har vektlagt tungt ved utformingen av forslaget, herunder:

- rettssikkerhet og personvern for den enkelte,
- forhindre misbruk av innretningen,
- sørge for effektiv kontroll av Etterretningstjenesten,
- sørge for at kontrollmekanismene får en disiplinerende effekten overfor Etterretningstjenestens personell, og
- befolkningens tillit til Etterretningstjenesten.

Departementet mener på generelt grunnlag at utgiftene som vil kunne henføres til kontrollregimet og andre sikkerhetsmekanismer er nødvendige for å ivareta behovet for en uavhengig og helhetlig kontroll. Disse utgiftene bør ikke søkes redusert dersom det kan svekke ivaretakelsen av hensynene nevnt over.

11.16.6.2 Forutgående domstolskontroll

Departementet vurderer at forutgående domstolskontroll vil bidra til å sikre legitimiteten til Etterretningstjenestens innhenting og faktiske tilgang til grenseoverskridende elektronisk kommunikasjon. I høringsnotatet punkt 11.11 redegjøres det for forslaget om at den forutgående domstolskontrollen av tilrettelagt innhenting bør legges til Oslo tingrett.

Utgifter tilknyttet den forutgående domstolskontrollen forventes først og fremst å være tilførsel og spesialisering av dommer(e), utgifter til særskilt advokat, eventuelt nye

saksbehandlere ved domstolen, ivaretakelse av krav til sikkerhet, herunder etablering av rom med tilstrekkelig graderingsnivå, og domstolens saksbehandling.

Departementets forslag om krav til domstolsbehandlingen følger av lovforslagets kapittel 8, og er til en viss grad inspirert av PSTs saker i det forebyggende- og avvergende sporet jf. politiloven § 17 d. Sammenligningen med PST-sakene er nyttig både av hensyn til domstolens administrasjon av sakene og av hensyn til kostnadsberegninger som følger av forslaget. Eksempelvis anser departementet at domstolen vil kunne trekke på erfaringer fra PST-sakene i forbindelse med krav til sikkerhetsgradering, behov for rask tilgang til domstolene og krav til saksbehandlingstid, samt ressursbruken knyttet til oppnevning av særskilt advokat.

Et viktig moment er at utgiftene knyttet til nødvendig personell beror på antallet begjæringer som fremmes. Kravene som stilles til begjæringenes utforming, herunder om hver begjæring må være individualisert eller om den kan omfatte et sakskompleks, vil dermed ha betydning for behovet for ekstra personell. Sakenes kompleksitet vil også ha betydning. Departementet har i lovforslaget ikke lagt opp til noe krav om at begjæringene må individualiseres. Etterretningstjenesten vil derfor etter forslaget kunne fremme begjæringer som består av et sakskompleks. Motsetningsvis, altså dersom det skulle innføres krav til at hvert søk på hver enkelt selektor må fremmes i en egen begjæring for domstolen, vil omfanget begjæringer kunne bli titalls per dag. Departementet anslår at domstolen i henhold til forslaget her gjennomsnittlig vil kunne motta 1-2 begjæringer i uken.

Domstolsadministrasjonen har forelagt tall for departementet som viser beregningen av årsverk. Personellutgiftene knyttet til én dommer i dag anslås å være 1,44 mill. kroner per år. For en saksbehandler anslås personellutgiftene å være 630.000,- per år. Estimatet viser at det påregnes mellom 5 og 10 arbeidstimer i saker etter politiloven § 17 d. Det er på nåværende tidspunkt utfordrende å si med sikkerhet om dette også vil være tilfellet i sakene etter lovforslaget her, men departementet legger dette foreløpig til grunn. De faktiske sakstallene og timetallene per sak vil være avgjørende for den endelige kostnadsberegningen.

Når det gjelder utgifter til særskilt oppnevnt advokat legger departementet anslagsvis til grunn at advokaten vil bruke gjennomsnittlig tre timer per sak. Ved beregningen har departementet tatt utgangspunkt i antallet timer som offentlig oppnevnte advokater benytter i saker om PSTs kommunikasjonskontroll. Dersom offentlige salærsatser for straffesaker legges til grunn vil dette beløpe seg til kroner 1020,- per time uten mva., og totalt et gjennomsnitt på kroner 3060,- uten mva. per sak. Advokaten vil måtte gå igjennom saken og skrive sin uttalelse i de sikkerhetsgraderte lokalene i domstolen. Departementet anslår at dersom man oppretter en fast gruppe med advokater som oppnevnes til denne typen saker vil saksbehandlingstiden måtte forventes å være noe høyere enn tre timer per sak i en oppstartsfase, men at tidsbruken vil gå ned etter noe tid.

Befatning med Etterretningstjenestens begjæringer stiller svært strenge krav til sikkerheten, og det antas at det må etableres et eget rom for behandling av sakene. Kravene til sikkerhetstiltak vil i så fall følge av sikkerhetsloven med tilhørende forskrifter. Domstolen må ved etableringen gjøre en verdi- og skadevurdering og få på plass tilstrekkelig sikring av rom, teknisk materiell og personell. Kostnadsdrivende sikkerhetstiltak vil særlig være bygging og sikring av rom. Dette må utformes med tilstrekkelig graderingsnivå som imøtekommer NSMs krav for teknisk godkjenning. Dersom dagens satser for graderingsnivå

HEMMELIG legges til grunn, vil utgiftene for etablering av rom beløpe seg til ca. 1,6 mill. kroner. Ved behov for høyere gradering må det påregnes en høyere utgift for etablering av rom for behandling av Etterretningstjenestens begjæringer. I tillegg må det påregnes utgifter for NSMs autorisering av rommet etter bygging. Andre potensielt kostnadsdrivende sikkerhetstiltak vil være klarering av personell, sikring av bygg og testing av eksisterende sikkerhetstiltak.

11.16.6.3 EOS-utvalget

Styrket kontroll av Etterretningstjenestens bruk av tilrettelagt innhenting vil etter departementets syn forhindre misbruk av systemet og skjerpe kontrollen av Etterretningstjenestens virksomhet generelt, og på denne måten bidra til å sikre tjenestens legitimitet. I høringsnotatet punkt 11.12 redegjøres det for departementets forslag til slik styrket kontroll, som vil komme i tillegg til EOS-utvalgets alminnelige etterfølgende kontroll i henhold til EOS-kontrolloven. Departementet har igangsatt utredningen av hvilke økonomiske og administrative konsekvenser den ekstra kontrolloppgaven kan få for EOS-utvalget.

Departementet legger til grunn at lovforslaget her vil medføre behov for å utvide den tekniske og juridiske kompetansen i EOS-utvalgets sekretariat. EOS-utvalget er etter det departementet kjenner til nylig styrket med teknologisk ekspertise. Departementet anslår at en innføring av tilrettelagt innhenting vil medføre et ytterligere behov for styrking av dette området. Etter departementets beregninger vil en styrking av EOS-utvalgets sekretariat med fire årsverk være tilstrekkelig for å ivareta kontrollfunksjonen. Lønnsutgiftene forbundet med ett årsverk beregnes til 1 mill. kroner per år. For å sikre umiddelbar effektiv kontroll og god kunnskap til systemet bør EOS-utvalgets sekretariat styrkes med dedikert kapasitet allerede på utviklingsstadiet.

I tillegg til tilførsel av personell vil effektiv kontroll av tilrettelagt innhenting medføre behov for opplæring og kontinuerlig kompetanseutvikling. Departementet forventer at dette i noen grad vil være kostnadsdrivende.

11.16.7 Økonomiske og administrative konsekvenser for tilbyderne som omfattes av lovforslaget

11.16.7.1 Generelt

Tilbydere som omfattes av lovforslaget § 7-2 vil plikte å utføre en rekke tiltak for å legge til rette for at Etterretningstjenesten kan få tilgang til grenseoverskridende elektronisk kommunikasjon. Hvilke tiltak som omfattes er ikke-uttømmende beskrevet i § 7-2 annet ledd bokstav a til e.

Tilretteleggingsplikten er en nødvendig forutsetning for å oppnå formålet med tilrettelagt innhenting og for å unngå at hensynet til viktige nasjonale interesser overlates til den enkelte tilbyder å vurdere viktigheten av. På bakgrunn av hensynet til likebehandling og forutberegnelighet foreslår departementet at det bør lovfestes en tilretteleggingsplikt som gjelder likt for alle relevante aktører.

Tilretteleggingsplikten vil kunne medføre enkelte merutgifter for teletilbyderne. Det er imidlertid forventet at det her er snakk om forholdsvis små beløp fordi teletilbyderne ikke

pålegges å lagre eller på annen måte prosessere data, og fordi det er Etterretningstjenesten som vil investere i nødvendig utstyr.[330]

Potensielle kostnadsdrivere for teletilbyderne vil være vedlikehold og drift av Etterretningstjenestens utstyr, i den grad tjenesten ikke gjør dette selv. Strømutgifter er et eksempel på en slik kostnad. Videre tilkommer utgifter til eventuelle konsulentoppdrag og opplæring av relevant personell.

Departementet viser til den nærmere drøftelsen i punkt 11.15. 6.

11.16.8 Særlig om bestemmelser som åpner for skjønn og betydningen dette har for vurderingen av økonomiske og administrative konsekvenser

Ved utformingen av bestemmelsene i forslaget til ny etterretningstjenestelov har departementet gjennomgående tatt stilling til hvor stor grad av skjønn som bør tillates i lovteksten. Fordelen med skjønnspregede bestemmelser er at det gir fleksibilitet ved lovanvendelsen. Dette kan anses som et gode i enkelte henseender, for eksempel der regelverket skal virke på et område som er i stadig utvikling og hvor det ikke er mulig å forutse de faktiske forhold på forhånd. Imidlertid kan det være vanskelig å forutberegne hvilke følger slike bestemmelser kan få, herunder rekkevidden av økonomiske og administrative konsekvenser.

Generelt har departementet etterstrebet å utforme reglene om tilrettelagt innhenting så presist og uttømmende som mulig. Imidlertid er det enkelte aspekter ved lovforslaget som ikke kan konkretiseres av hensyn til den teknologiske utviklingen. Dette gjelder særlig lovforslaget § 7-2 annet ledd, som fastslår at tilretteleggingsplikten innebærer at tilbyderne *på egnet måte* skal speile og tilgjengeliggjøre kommunikasjonsstrømmene for Etterretningstjenesten. Videre skal tilbyderne *på annen måte* tilrettelegge for utvalg, filtrering etc. Et spørsmål her har vært hvilke tiltak som kan pålegges tilbyderne innenfor rammen av denne bestemmelsen. Meningen med bestemmelsens skjønnsmessige utforming har vært å sikre at tilbyder oppgraderer de tekniske løsningene når dette er nødvendig for å speile kommunikasjonen på egnet måte. For øvrig skal tilbyder tilrettelegge på den måten som er nødvendig for at Etterretningstjenesten skal kunne gjennomføre tilrettelagt innhenting. En annen bestemmelse med skjønnsmessig utforming i forslaget om tilrettelagt innhenting er lovutkastet § 7-5 annet ledd. Bestemmelsen fastsetter at Etterretningstjenesten gjennom utvalg og filtrering *så langt som praktisk mulig* skal sikre at lagrede metadata ikke inneholder norsk-norsk kommunikasjon.

For departementet er det viktig å understreke at de skjønnsmessige formuleringene er gitt av hensyn til uforutsigbarheten som følger av den teknologiske utviklingen. I denne sammenheng finner departementet det hensiktsmessig å nevne at løsningene som velges må holdes på et så lavt utgiftsmessig nivå som mulig i den grad dette ikke gjør løsningen uforsvarlig av hensyn til sikkerhet og egnethet. Anskaffelser som vil medføre utgifter for det offentlige skal skje i henhold til alminnelige styringsprinsipper.

[330] Se også Lysne II-utvalgets rapport om digitalt grenseforsvar av 26. august 2016 s. 68, hvor det uttales at «Innføring av DGF innebærer intet pålegg til tjenesteleverandører om å lagre data. Det vil heller ikke innebære noen nevneverdige administrative eller økonomiske kostnader for tilbyderne.»

11.16.9 Departementets vurdering av de samlede økonomiske og administrative konsekvensene som følger av forslaget om tilrettelagt innhenting

På bakgrunn av forholdene som fremkommer over vurderer departementet at det vil være behov for økonomiske ressurser til Etterretningstjenesten ved innføring og drift av tilrettelagt innhenting. Behovet vil avhenge av en senere beslutning om å investere i nødvendige systemer for å benytte mulighetene som følger av lovforslaget. Departementets forslag til kontrollmekanismene gjennom EOS-utvalget og Oslo tingrett medfører mindre utgifter.

Det har vært utfordrende for departementet *på nåværende tidspunkt* å beregne de investerings- og driftsmessige konsekvensene for tilbyderne og staten som følger av tilretteleggingsplikten. Kostnadsberegninger knyttet til investeringer og drift av tilrettelagt innhenting vil måtte foretas ved utredningen av et beslutningsgrunnlag forut for en senere anskaffelse av systemet for tilrettelagt innhenting.

Departementet vil komme tilbake til de budsjettmessige virkningene i den ordinære budsjettbehandlingen, men *foreløpige* kostnadsestimat kan oppsummeres som følger:

AKTØR	KOSTNADSDRIVERE	ESTIMERTE INVESTERINGS-UTGIFTER	ESTIMERTE DRIFTSUTGIFTER PER ÅR
Etterretnings-tjenesten*	• Nytt personell • Kompetanseutvikling hos nytt og eksisterende personell • Materiell (investering og drift) • EBA (investering og drift)	Ca. 700 mill. kroner, inkludert estimerte materiell- og EBA-investeringskostnader, samt prosjektets egne driftsutgifter	100-150 mill. kroner, inkludert estimerte utgifter knyttet til personell, materiell og EBA
Domstolen	• Behandling av begjæringer • Sikkerhetstiltak ihht sikkerhetsloven • Etablering av rom • Nytt personell • Utgifter til særskilt advokat • Kompetanse-utvikling	1,6 - 3 mill. kroner for etablering av sikkerhetstiltak ihht sikkerhetsloven, herunder etablering av rom	1,07 – 2,13 mill. kroner basert på en forutsetning om at domstolen vil behandle 1-2 saker per uke og ha behov for et halvt eller ett nytt dommerårsverk og saksbehandler-årsverk 160 000– 320 000 kroner i året i advokatutgifter
EOS-utvalget	• Nytt personell • Kompetanse-utvikling hos nytt og eksisterende personell • EBA	Ca. 1 mill. kroner for etablering av kontorplasser til nytt personell	Ca. 5 mill. kroner basert på en forutsetning om at EOS-utvalget vil ha behov for fire nye årsverk
SUM		**702,6 - 704 mill. kroner**	**106,23 - 157,45 mill. kroner**

* Utgiftene for investering og drift er under utredning. Disse kan bli endret etter hvert som prosjektarbeidet går fremover. Usikkerheten i kostnadsbildet angis derfor i intervaller med relativt stor spredning.

12 Behandling av personopplysninger m.m.

12.1Innledning

Alle mennesker har en ukrenkelig egenverdi. Som enkeltmenneske har man derfor rett på en privat sfære som man selv kontrollerer, og hvor man kan handle fritt uten tvang eller innblanding fra staten eller andre mennesker. Dette prinsippet kommer blant annet til uttrykk i EMK artikkel 8, i Grunnloven § 102 og § 100 fjerde ledd, samt i en rekke EØS-relevante direktiver og forordninger. Interessene som vernes er «privatlivets fred», «personvern» og «personopplysningsvern». Disse betegnelsene benyttes ofte om hverandre, men begrepene «personvern» og «personopplysningsvern» dekker også ulike sider av retten til privatliv. I Menneskerettighetsutvalgets rapport ble følgende definisjoner av begrepene lagt til grunn:[331]

> «Personvern dreier seg om ivaretakelse av personlig integritet; ivaretakelse av enkeltindividers mulighet for privatliv, selvbestemmelse (autonomi) og selvutfoldelse. […]
>
> Personopplysningsvern dreier seg om regler og standarder for behandling av personopplysninger som har ivaretakelse av personvern som hovedmål. Reglenes formål er å sikre enkeltindivider oversikt og kontroll over behandling av opplysninger om dem selv. Med visse unntak skal enkeltpersoner ha mulighet til å bestemme hva andre skal få vite om hans/hennes personlige forhold. Det er denne delen av personvernretten som er underlagt den mest omfattende lovregulering i for eksempel personopplysningsloven, helseregisterloven, regler om taushetsplikt og så videre.»

I det følgende legger departementet disse forståelsene av begrepene til grunn når det er tale om personvern og personopplysningsvern. Departementets forslag til legaldefinisjon av «personopplysning» omtales i punkt 12.4.1 under.

Departementet anser personvernet ikke bare som en viktig menneskerettighet som skal sikre hensynet til den enkeltes personlige integritet og privatliv. Personvernet er også viktig for å sikre felles goder i et demokratisk samfunn. Uten rett til respekt for den private sfære vil det ikke være mulig for det enkelte menneske å skape seg et rom til å utvikle refleksjoner, vurderinger og ytringer på et selvstendig grunnlag, uten å bli forstyrret eller kontrollert av andre. Vernet er imidlertid ikke *absolutt*, men må ses i sammenheng med sin funksjon i samfunnet og avveies i forhold til andre grunnleggende rettigheter i overensstemmelse med forholdsmessighetsprinsippet. Det må også tas i betraktning at staten også har en plikt til å motvirke trusler som kan utfordre personvernet til den enkelte.

Innsamling, vurdering, systematisering, lagring og utlevering av opplysninger er vesentlig og nødvendig for å kunne utøve utenlandsetterretningsvirksomhet, herunder for å kunne effektivt bidra til å kartlegge og motvirke ytre trusler mot rikets selvstendighet og sikkerhet og sikre andre viktige nasjonale interesser. Samtidig har slik bruk av opplysninger konsekvenser for personvernet.

De internasjonale krav til personvern, som i stor grad må sies å være foranlediget av den teknologiske utviklingen, har gjort det dels nødvendig og dels ønskelig å foreslå endringer i det fragmentariske regelverket som i dag gjelder for Etterretningstjenestens behandling av personopplysninger. Hensikten med lovforslaget er å bidra til effektiv løsning av tjenestens

[331] Dokument nr. 16 (2011–2012) punkt 30.6.2 s. 173

oppgaver, og samtidig sikre en beskyttelse av personvernet og forutberegnelighet for den enkelte ved tjenestens behandling av opplysninger.

12.2 Dagens regulering

12.2.1 Internasjonalt

De folkerettslige rammene for Etterretningstjenestens behandling av personopplysninger er i hovedsak EMK, FNs konvensjon om sivile og politiske rettigheter og Europarådets konvensjon nr. 108 av 28. januar 1981 om personvern i forbindelse med elektronisk databehandling av personvern (Europarådets personvernkonvensjon).[332] EØS-relevant EU-rett får ikke direkte anvendelse for utenlandsetterretningsvirksomhet. I Traktaten om Den europeiske union artikkel 4 nr. 2 slås det fast at nasjonal sikkerhet er statenes eneansvar. EØS-relevante forordninger og direktiver har derfor mindre betydning ved utformingen av nasjonal lovgivning knyttet til nasjonal sikkerhet. Likevel mener departementet at en ikke kan se fullstendig bort fra disse, ettersom de gir et bilde på rettstilstanden i Europa og hvilke internasjonale impulser som påvirker de nasjonale systemene til enhver tid. De viktigste EU-rettsaktene på personopplysningsvernets område er:

- EUs personvernforordning 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og fri utveksling av slike opplysninger (personopplysningsforordningen).
- EU-direktiv 2002/58/EF om behandling av personopplysninger og beskyttelse av privatlivets fred i den elektroniske kommunikasjonssektor (kommunikasjonsverndirektivet).

Felles for disse er at de, blant annet under henvisning til EMK, bygger på utgangspunktet om vern av personopplysninger og av privatlivets fred, herunder kommunikasjonsfortroligheten. Grunnprinsippene i de nevnte rettsaktene vil i det følgende omtales der de har hatt betydning for departementets forslag til regulering av Etterretningstjenestens behandling av personopplysninger.

Europarådets personvernkonvensjon har som formål å

> «sikre respekt for enhver enkeltpersons rettigheter og grunnleggende friheter og især retten til privatlivets fred på territoriet til enhver part, uten hensyn til statsborgerskap eller bopel, i forbindelse med elektronisk databehandling av personopplysninger som vedrører ham.»
>
> Konvensjonen gir enhver rett til å vite om det eksisterer et elektronisk persondataregister, registerets formål og til å få vite om man er registrert og om det eventuelt er korrigert eller slettet opplysninger som er lagret i strid med konvensjonen, samt ha klageadgang dersom disse rettighetene ikke respekteres, jf. konvensjonens artikkel 8. Personopplysninger defineres som «enhver opplysning som gjelder en bestemt eller identifiserbar enkeltperson», og konvensjonen artikkel 5 slår fast at personopplysninger skal:
>
> «a) innsamles og bearbeides på rettferdig og lovlig vis;
>
> b) lagres for bestemte og lovlige formål og ikke nyttes på en måte som er uforenlig med disse formål;

[332] Se høringsnotatet kapittel 4 for en nærmere redegjørelse av de folkerettslige rammene som gjelder generelt ved utformingen av lovforslaget.

c) være adekvate, relevante og ikke for omfattende i relasjon til de formål de lagres til;

d) være nøyaktige og, der det er nødvendig, holdt a jour;

e) oppbevares på en måte som ikke gir anledning til å identifisere datasubjektene lenger enn nødvendig for det formål som disse opplysningene lagres til.»

Videre slår konvensjonen fast at personopplysninger som åpenbarer rasemessig opprinnelse, politiske oppfatninger samt religiøs eller annen tro, så vel som personopplysninger vedrørende helse eller seksualliv og personopplysninger som gjelder domfellelser for straffbare handlinger skal nyte et særskilt vern, jf. artikkel 6. I likhet med EMK artikkel 8 nr. 2 kan det gjøres unntak fra de nevnte bestemmelsene i konvensjonen når dette er fastsatt i lov og er et nødvendig tiltak i et demokratisk samfunn av hensyn til beskyttelse av statens sikkerhet, offentlig sikkerhet, statens økonomiske interesser eller bekjempelse av kriminelle handlinger eller beskyttelse av datasubjektet eller andres rettigheter og friheter.

Drøftelsene nedenfor vil i hovedsak knytte seg til EMK artikkel 8. Departementet vurderer at dette også vil være dekkende for de skranker for lovgivningen på området som vil kunne utledes av SP artikkel 17 og Europarådets personvernkonvensjon.

12.2.2 Nasjonalt

Nasjonalt er personopplysningsvern inngående regulert i en rekke lover og forskrifter. Den generelle reguleringen følger av er personopplysningsloven 2018,[333] som implementerer EUs personvernforordning.[334] Forgjengeren til 2018-loven, personopplysningsloven 2000,[335] implementerer EUs personverndirektiv 1995. Personopplysningsloven 2000 har blitt gitt direkte anvendelse for Etterretningstjenestens behandling av personopplysninger der etterretningstjenesteloven har manglet egen regulering, og ellers som tolkningsfaktor.[336]

Det følger av § 1 bokstav c i overgangsreglene om behandling av personopplysninger, [337] som er fastsatt i forskrift i medhold av ny personopplysningsloven 2018, at loven ikke gjelder for Etterretningstjenestens behandling av opplysninger for etterretningsformål.[338] I herværende lovforslag fremmer departementet forslag til særregler for Etterretningstjenestens behandling av personopplysninger. Frem til ny lov om Etterretningstjenesten trer i kraft vil personopplysningsloven 2000 fortsatt gjelde.

[333] Lov av 15. juni 2018 nr. 38 om behandling av personopplysninger

[334] Forordning (EU) 2016/679

[335] Lov av 14. april 2000 nr. 31 om behandling av personopplysninger

[336] Det presiseres at det følger av personverndirektivets artikkel 3, som regulerer direktivets saklige virkeområde, at direktivet ikke gjelder behandling av personopplysninger i forbindelse med virksomhet som faller utenfor fellesskapsrettens område, og ikke under noen omstendighet behandling som gjelder offentlig sikkerhet, forsvar, statens sikkerhet og statens virksomhet på det strafferettslige området. At loven fra 2000 likevel har blitt gitt anvendelse på Etterretningstjenestens behandling av personopplysninger skyldes mangel på egen (fullstendig) regulering i etterretningstjenesteloven 1998.

[337] Forskrift av 15. juni 2018 nr. 877 om overgangsregler om behandling av personopplysninger

[338] Det er viktig å merke seg at dette innebærer at heller ikke EUs personvernforordning (forordning 2016/679 av 27. april 2016) gjelder for Etterretningstjenestens virksomhet.

Etterretningstjenesteloven har enkelte bestemmelser som ivaretar personopplysningsvernet. I fastleggelsen av gjeldende rett vil man derfor legge de relevante bestemmelser for behandling av personopplysninger i etterretningstjenesteloven til grunn, i tillegg til at personopplysningsloven 2000 gjelder utfyllende der etterretningstjenesteloven mangler regulering. Etterretningstjenesteloven § 3 gir særskilt behandlingsgrunnlag for Etterretningstjenestens behandling av personopplysninger med et etterretningsformål.

Etterretningstjenestens behandling av opplysninger ved utøvelsen av arbeidsrettslige, sikkerhetsmessige eller andre forhold som ikke skjer med etterretningsformål, reguleres i dag av personopplysningsloven 2018, sammenholdt med annen spesiallovgivning.

Annet regelverk som setter rammer for tjenestens behandling av personopplysninger med et etterretningsformål er menneskerettsloven,[339] instruks om samarbeid mellom Etterretningstjenesten og PST[340] og Forsvarsdepartementets utfyllende bestemmelser om innsamling mot norske personer i utlandet samt for utlevering av personopplysninger til utenlandske samarbeidende tjenester.[341] Det gjøres ikke endringer i dette regelverket som følge av lovforslaget her.

12.3 Behovet for særskilt regulering av personopplysningsvern

12.3.1 Innledning

Etterretningstjenestens behandling av personopplysninger er fragmentarisk regulert i ulike regelverk. Departementet vil fremheve at behandling av personopplysninger utført av en etterretningstjeneste skiller seg fra behandling av personopplysninger utført av andre aktører i samfunnet, og at dette taler for en særregulering. Den alminnelige personvernlovgivningen er på mange områder blitt helt eller delvis erstattet med særskilte personvernbestemmelser. De viktigste særlovene i så måte er helseregisterloven[342], helseforskningsloven[343], politiregisterloven[344], arbeidsmiljøloven[345] og ekomloven[346].

Det å samle inn, vurdere, systematisere, lagre og utlevere opplysninger er en vesentlig og nødvendig side ved etterretningsarbeid. Formålet med behandlingen, samt behovet for diskresjon og skjerming gir også særlige forutsetninger. Forskjellene gir seg for eksempel utslag ved det alminnelige kravet til underrettelse til en person hvis personopplysninger er behandlet. Som vist i drøftelsen under punkt 4.3.5.2 kan ikke Etterretningstjenesten underrette etterretningsmål som den innhenter informasjon om, uten at formålet med innhentingen ved dette fullstendig forfeiles.

[339] Lov av 21 mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett

[340] «Samarbeidsinstruksen» fastsatt ved kongelig resolusjon av 13. oktober 2006 nr. 1151

[341] Instruks fastsatt av Forsvarsdepartementet den 24. juni 2013

[342] Lov av 20. juni 2014 nr. 43 om helseregistre og behandling av helseopplysninger

[343] Lov av 20. juni 2008 nr. 44 om medisinsk og helsefaglig forskning

[344] Lov av 28. mai 2010 nr. 16 om behandling av personopplysninger i politiet og påtalemyndigheten, se særlig kapittel 2

[345] Lov av 17. juni 2005 nr. 62 om arbeidsmiljø, arbeidstid og stillingsvern mv.

[346] Lov av 4. juli 2003 nr. 83 om elektronisk kommunikasjon

Et annet sentralt moment er, som nevnt over, at utenlandsetterretning faller utenfor EU-retten og dermed også EØS-avtalen. Samtidig er den alminnelige personvernlovgivningen i stor grad basert på EU-rett.

Videre mener departementets at en særskilt regulering vil sørge for et helhetlig regelsett og dermed bedre oversikt over hvilke krav som gjelder. Dette er for det første positivt for Etterretningstjenestens oppdragsløsning. Dessuten vil en samling av dagens fragmentariske regulering gjøre regelverket lettere tilgjengelig, og således også mer forutberegnelig, for den enkelte. I tillegg vil regelverket legge bedre til rette for kontroll med tjenesten.

Stortinget har allerede lagt til grunn, gjennom behandlingen og vedtakelsen av ny personopplysningslov i 2018, at den nye personopplysningsloven ikke skal gjelde for Etterretningstjenesten. Det foreslås som forutsatt derfor egne tilpassede regler for Etterretningstjenestens behandling av personopplysninger i lovutkastet her.[347] Forslagene til bestemmelser bygger på de krav som kan utledes av Grunnloven og internasjonale personvernforpliktelser, herunder EMK. I tillegg vil grunnleggende personvernprinsipper gi viktige retningslinjer. Innenfor denne rammen mener departementet at reglene må utformes på en måte som sikrer en forsvarlig balanse mellom personvernhensyn og etterretningsfaglige hensyn, og som trygger befolkningens tillit til Etterretningstjenestens virksomhet.

12.3.2 Forholdet til annen lovgivning

12.3.2.1. Avgrensning

Klarhetshensyn tilsier at det bør lovfestes at ny lov om Etterretningstjenesten gir spesialregler for tjenestens behandling av personopplysninger for etterretningsformål, og at personopplysningsloven ikke gjelder.

Forslaget til ny etterretningstjenestelov gir *behandlingsgrunnlag* for å behandle personopplysninger med *etterretningsformål*. Tjenesten må imidlertid også kunne behandle opplysninger for å kunne *avklare* om disse oppfyller kravene til nødvendighet og formålsbestemthet. Dette er nærmere omtalt under.

Kapittelets virkeområde bør etter departementets syn formuleres slik i § 9-1 første ledd:

> Personopplysningsloven gjelder ikke for behandling av personopplysninger etter loven her.

12.3.2.2 Presiseringer og unntak

For behandling av personopplysninger for andre formål enn etterretningsformål, foreslår departementet at den alminnelige personvernlovgivningen som et utgangspunkt fortsatt skal gjelde, se punkt 12.2.2 over. Eksempler på «andre formål» er arbeidsgiverformål, sikkerhetsformål og avtaleformål.

Forslaget gjelder imidlertid ikke uten unntak. For det første foreslår departementet en videreføring av dagens regel om at Etterretningstjenesten er unntatt fra Datatilsynet og

[347] EUs nye personvernforordning og den norske gjennomføringsloven gjelder i utgangspunktet både innenfor og utenfor EØS-avtalens virkeområde, jf. personopplysningsloven § 2 første ledd første punktum. Det følger imidlertid av personopplysningsloven § 2 første ledd annet punktum at loven og forordningen ikke gjelder når annet er bestemt i eller i medhold av lov. Det åpnes dermed for at det kan gjøres unntak i særlovgivningen. I en overgangsperiode til ny etterretningstjenestelov er trådt i kraft gjelder personopplysningsloven 2000. Dette fremgår av forskrift 15. juni nr. 877 om Overgangsregler om behandling av personopplysninger § 1 første ledd bokstav c.

Personvernnemndas tilsynsmyndighet uavhengig av formålet med behandlingen. Det samme gjelder kontroll- og sanksjonsbeføyelser. Dette har sammenheng med Etterretningstjenestens skjermingsbehov, men er også begrunnet i hensynet til et enhetlig kontrollregime som innebærer at EOS-utvalget også kontrollerer Etterretningstjenestens behandling av personopplysninger uavhengig av formål.

For det andre foreslår departementet at det bør gjøres unntak ved anvendelsen av eventuelle tilpassede skjermingsregler som følger av bestemmelser gitt i medhold av lovutkastet § 11-5 om skjerming mot offentlig eksponering av ansatte, kilder, kapasiteter, metoder og operasjoner. Personopplysningene vil i denne forbindelse behandles etter reglene om forslag til ny lov om Etterretningstjenesten.

Departementet foreslår følgende formulering i utkast til § 9-1 andre ledd:

> For behandling av personopplysninger for andre formål enn etter loven her gjelder bestemmelsene i personopplysningsloven eller særlovgivningen, med de unntak som følger av § 2-10 første ledd og eventuelle tilpassede skjermingsregler i medhold av § 11-5.

12.3.3 Sentrale prinsipper og hensyn

Som nevnt i punkt 12.2.2 gjelder verken personopplysningsloven av 2018 eller EUs personvernforordning for Etterretningstjenestens behandling av personopplysninger for etterretningsformål. Samtidig er det naturlig å ta utgangspunkt i de sentrale personvernprinsipper som også 2018-loven (og forordningen) er basert på, i utformingen av lovforslaget her. Dette gjelder særlig prinsippene om formålsbestemthet, nødvendighet, dataminimering, krav til opplysningens kvalitet, lagringsbegrensning samt integritet og respekt for fortrolig kommunikasjon. Gode kontrollordninger og datasikkerhet er også vesentlige elementer for å sikre et godt personvern.

Anvendelsen av enkelte andre prinsipper, slik som rett til innsyn, rett til underrettelse og rett til å kunne kreve at uriktige opplysninger blir rettet, må tilpasses på grunn av de særlige hensyn som gjør seg gjeldende for Etterretningstjenesten. Dette reflekteres i lovforslaget.

At det er adgang til å gjøre unntak fra den registrertes rettigheter etter en avveining mot andre hensyn ser vi også eksempler på i den alminnelige personvernreguleringen.[348]

12.4 Personopplysning

12.4.1 Nærmere om begrepet personopplysning

Departementet foreslår følgende legaldefinisjon av «personopplysninger» i lovforslaget § 1-4 nr. 11:

> «Personopplysninger; enhver opplysning og vurdering som med enkle midler kan knyttes til en identifisert eller identifiserbar fysisk person.»

[348] I personopplysningsloven 2000 § 23 første ledd oppstilles det for eksempel visse generelle unntak fra innsynsrettighetene og informasjonsplikten i §§ 18 til 22. Eksempelvis omfattes ikke opplysninger som vil kunne skade rikets sikkerhet, landets forsvar eller forholdet til fremmede makter eller internasjonale organisasjoner av retten til innsyn og informasjon. I personopplysningloven 2018 § 16 første ledd bokstav a er unntaket fra retten til informasjon og innsyn og plikten til underretning av slike opplysninger videreført. Det samme foreslås å gjelde i ny lov om Etterretningstjenesten, se lovforslaget §§ 11-6 annet ledd og 11-8 som er nærmere omtalt i høringsnotatet kapittel 14.8 og 14.9.

Departementets forslag tilsvarer materielt sett legaldefinisjonen i EUs personvernforordning 2016, artikkel 4. Det innebærer at alle opplysninger som direkte eller indirekte kan knyttes til en person, må regnes som «personopplysninger» i lovens forstand. Det innebærer at også opplysninger som bare indirekte kan knyttes til en person gjennom identifiserende kjennetegn faller inn under loven. Opplysninger knyttet til et kundenummer eller lignende er således «personopplysninger».

At opplysningen må kunne «knyttes til» en person innebærer et krav om identifikasjon. I identifikasjonskravet ligger en forutsetning om at en opplysning med stor grad av sikkerhet må kunne knyttes til en spesifikk person. Dersom opplysninger er knyttet til et IP-nummer, altså identifikasjonsnummeret på en datamaskin tilknyttet Internett, og denne maskinen har flere brukere, vil det kunne være usikkert hvilken person opplysningene om bruken av tjenestene på nettet gjelder. Er det flere personer som kan knyttes til denne informasjonen, vil ikke opplysningene kunne regnes som personopplysninger fordi tilknytningen til en bestemt person er for usikker. Hensynet bak personopplysningsvernet er således ikke til stede, da opplysningen ikke kan knyttes til en konkret enkeltperson.

En opplysning regnes som en personopplysning selv om *selve identifiseringen* av en person ikke har skjedd. Det er med andre ord nok at en slik identifisering *kan* skje for at en opplysning skal falle inn under definisjonen av «personopplysning». Likevel er ikke enhver fjern mulighet for identifisering tilstrekkelig til at opplysningen regnes som en personopplysning. Et spørsmål som reiser seg er hvor stor innsats som kreves av et forsøk på identifisering. Lovforslaget bruker begrepet «med enkle midler» som innebærer at det ikke kan stilles for høye krav. På generelt grunnlag kan man si at jo mer alvorlig de mulige følgene for personvernet antas å kunne bli, jo mindre skal til for at noe regnes for å være en personopplysning. Legger man en slik formodning til grunn, vil opplysninger om sensitive forhold kunne bli regnet som personopplysninger selv om det er usikkert hvilken person opplysningene gjelder.

12.4.2 Sensitive personopplysninger. Diskrimineringsforbud.

Departementet har vurdert om det er behov for å skille mellom behandling av personopplysninger og sensitive personopplysninger. Etter personopplysningsloven 2000 kan sensitive personopplysninger behandles dersom det er fastsatt i lov, jf. § 9 første ledd bokstav b. Etterretningstjenesteloven §§ 3 og 4 annet ledd gir i dag Etterretningstjenesten rettslig grunnlag til å behandle sensitive personopplysninger for utenlandsetterretningsformål.

Departementet har ikke funnet behov for å innføre bestemmelser om behandling av sensitive personopplysninger. Det vises til at hele det foreslåtte regelverket bærer preg av at Etterretningstjenesten vil behandle nettopp sensitive personopplysninger. Personopplysningenes grad av sensitivitet vil være et sentralt moment i vurderingen av *inngrepets art og omfang*, som igjen har betydning for hvilke krav som stilles til inngrepshjemmelen og forholdsmessigheten. I likhet med EUs personvernforordning og personopplysningsloven 2018 bør det kreves at behandlingen har et *behandlingsgrunnlag*, som vil si at den har hjemmel i lov.

Departementet mener at det bør lovfestes et uttrykkelig forbud mot å behandle opplysninger om en person *utelukkende* på bakgrunn av hva som er kjent om personens etnisitet eller nasjonale bakgrunn, politiske, religiøse eller filosofiske overbevisning, språk, politiske

virksomhet, fagforeningstilhørighet eller opplysninger om helsemessige eller seksuelle forhold. Den samme regelen kan utledes av Grunnloven § 98 annet ledd og EMK artikkel 14, samt kravene om formålsbestemthet og nødvendighet. Departementet finner likevel at klarhetshensyn tilsier at det inntas et uttrykkelig forbud i loven.

Det at personopplysninger ikke kan behandles «utelukkende på bakgrunn» av de nevnte personlige egenskapene innebærer ikke et forbud mot å behandle slike opplysninger når dette er nødvendig for etterretningsformål. Behandlingen må da knyttes til andre grunner eller omstendigheter enn *utelukkende* de forhold som er opplistet i bestemmelsen. Etterretningstjenesten vil for eksempel kunne behandle opplysninger om religiøs tilhørighet hvis tjenesten følger et ekstremistisk miljø i utlandet som baserer seg på rekruttering av personer med en spesiell trosretning. Det vil her være behov for å registrere en persons tilknytning til miljøet. Likeledes vil det kunne være grunnlag for å behandle opplysninger om etnisk bakgrunn fordi opplysningene kan være av betydning for gjenkjennelse. Bestemmelsen har således til hensikt å forby behandling av opplysninger om en person *utelukkende* på bakgrunn av de opplistede forhold.

Departementet foreslår følgende bestemmelse:

§ 9-4 *Diskrimineringsforbud*

Etterretningstjenesten skal ikke behandle personopplysninger utelukkende på bakgrunn av hva som er kjent om en persons etnisitet eller nasjonale bakgrunn, politiske, religiøse eller filosofiske overbevisning, språk, politiske virksomhet, fagforeningstilhørighet eller helsemessige eller seksuelle forhold.

12.5 Behandlingsgrunnlag

12.5.1 Krav til behandlingsgrunnlag. Gjeldende rett

Grunnloven § 102 og EMK artikkel 8 stiller krav til rettsgrunnlaget når behandling av personopplysninger utgjør et inngrep i retten til respekt for privatliv mv. Vilkårene for å gjøre inngrep i noens menneskerettigheter er behandlet i kapittel 4 i høringsnotatet her.

EMD har i sin praksis lagt til grunn at offentlige myndigheters lagring av personopplysninger som knytter seg til privatlivet i bestemmelsens forstand, utgjør et inngrep i retten etter EMK artikkel 8 nr. 1.[349] Inngrep i privatlivet er tillatt etter Grunnloven § 102 og EMK artikkel 8 nr. 2 dersom det har tilstrekkelig hjemmel, forfølger et legitimt formål og er forholdsmessig. Det er kravet om *tilstrekkelig hjemmel* som er særlig relevant i spørsmålet om regulering av behandlingsgrunnlag.

Det rettslige behandlingsgrunnlaget for å behandle personopplysninger følger i dag av etterretningstjenesteloven § 3 første ledd. Etterretningstjenesten kan etter dagens lovregulering bare behandle personopplysninger dersom behandlingen kan antas å ha betydning for ivaretakelsen av tjenestens oppgaver etter loven § 3 og prioriteringsdokumentet fastsatt i medhold av instruks om Etterretningstjenesten § 12. Dette gjelder uavhengig av nasjonalitet og lokasjon.

[349] *Amann mot Sveits* avsagt 16. februar 2000, avsnitt 65 og *S. og Marper mot Storbritannia* avsagt 4. desember 2008, avsnitt 67

Etterretningstjenesteloven § 3 oppstiller som vilkår at Etterretningstjenesten skal «innhente, bearbeide og analysere» informasjon «i den utstrekning det kan bidra til» utførelsen av oppgavesettet. Etterretningstjenesten må dermed foreta en nødvendighetsvurdering av om opplysningen kan og skal behandles. Vurderingen er av etterretningsfaglig karakter, og kan variere etter fagområde, tema og andre omstendigheter. Det er tilstrekkelig at informasjonen *kan* være informasjon som er egnet – alene eller sett sammen øvrig informasjon – til å bidra til å sikre viktige nasjonale interesser. Egnethetsvurderingen er basert på erfaring og kompetansebaserte formodninger, og om informasjonen kan relateres til annen informasjon som tjenesten allerede besitter.

Etterretningstjenesteloven § 4 annet ledd supplerer det generelle behandlingsgrunnlaget i § 3 når det gjelder *oppbevaring* av opplysninger om norske fysiske og juridiske personer. Etterretningstjenesten kan bare oppbevare informasjon som gjelder norske fysiske og juridiske personer dersom informasjonen har direkte tilknytning til ivaretakelsen av Etterretningstjenestens oppgaver etter § 3 eller er direkte knyttet til en slik persons arbeid eller oppdrag for tjenesten. Bestemmelsen har til hensikt å tydeliggjøre at innhentingsforbudet etter første ledd ikke skal tolkes dithen at Etterretningstjenesten ikke kan behandle opplysninger om norske fysiske og juridiske personer.

Utlevering av informasjon er en viktig behandlingsform. I henhold til etterretningstjenesteloven § 3 annet ledd kan Etterretningstjenesten etablere og opprettholde etterretningssamarbeid med andre land. Utveksling av informasjon med samarbeidende tjenester i utlandet er en forutsetning for og en viktig del av slikt samarbeid. Selv om det ikke følger uttrykkelig av lovteksten er det ikke omtvistet at Etterretningstjenesten også kan dele informasjon med norske myndigheter og virksomheter. Særskilt grunnlag og vilkår for tjenestens adgang til å utveksle informasjon er nærmere redegjort for i kapittel 13.

Formålsbestemthet er et grunnleggende personvernprinsipp som innebærer at personopplysninger ikke skal brukes til formål som er uforenlige med det opprinnelige formål med behandlingen. En av de viktigste funksjonene med formålsangivelsen er å angi grensen for sekundærbruk, det vil si når opplysningene brukes til et annet formål enn det de er innhentet for. Formålsangivelsen må være så presis som mulig.

Gjeldende regulering av prinsippet om formålsbestemthet for Etterretningstjenesten følger av personopplysningsloven 2000 § 11 bokstav b og c.

Etterretningstjenesteloven § 3 gir Etterretningstjenesten et særskilt grunnlag for å behandle personopplysninger. Bestemmelsen er imidlertid begrenset til å gi behandlingsgrunnlag for opplysninger som behandles med et *etterretningsformål*. Skal tjenesten behandle opplysninger med andre formål, må det enten foreligge samtykke eller annen lovhjemmel.

12.5.2 Departementets vurdering

Lovforslaget innebærer ingen endring fra dagens krav til formålsbestemthet, men har til hensikt å presisere hvilke formål Etterretningstjenesten kan behandle personopplysninger for. Departementet foreslår å definere etterretningsformål i § 1-4 nr. 6 på følgende måte:

> Etterretningsformål; formål å ivareta en eller flere av Etterretningstjenestens oppgaver etter kapittel 3.

Etter departementets vurdering vil forslaget om en uttømmende angivelse av Etterretningstjenestens oppgaver i lovens kapittel 3 styrke vernet mot sekundærbruk. Dessuten vil det bidra til å styrke forutberegneligheten. Etterretningstjenestens oppgaver er nærmere redegjort for i høringsnotatet kapittel 7.

Departementet har vurdert hvorvidt Etterretningstjenestens oppgaver etter lovforslaget kapittel 3 skal anses som *ett* eller flere behandlingsformål. Departementet mener at oppgavene bør ses som ett behandlingsformål. Til sammenligning viser departementet til at Justis- og beredskapsdepartementet i forarbeidene til politiregisterloven vurderte at PSTs virksomhet er å anse som ett behandlingsformål.[350]

Når det gjelder behandlingsformen *informasjonsinnhenting*, i kortform kalt *innhenting*, er dette gjenstand for særskilte reguleringer andre steder i lovforslaget, se særlig lovutkastet kapittel 3 til 8 og kravene til nødvendighets- og forholdsmessighetsvurderinger. Departementet mener denne behandlingsformen allerede er hensiktsmessig regulert, og at kapittelet om behandling av personopplysninger derfor ikke bør kommer til anvendelse, med unntak fra diskrimineringsforbudet i lovutkastet § 9-4.

Departementet foreslår følgende bestemmelser knyttet til kravet om formålsbestemthet og behandlingsgrunnlag for innhenting av personopplysninger:

§ 9-2 *Formålsbestemthet*
Etterretningstjenesten kan behandle personopplysninger for etterretningsformål.

§ 9-3 *Innhenting av personopplysninger*
Med unntak av §§ 9-2 og 9-4 gjelder bestemmelsene i kapittelet her ikke for behandling i form av innhenting. Behandling i form av innhenting reguleres i kapittel 3-8.

12.6 Nødvendighet

12.6.1 Krav om at behandlingen må være nødvendig. Gjeldende rett

Nødvendighetsprinsippet er et grunnleggende personvernprinsipp som innebærer at det ikke er lovlig å behandle en personopplysning som det ikke er *nødvendig* å behandle *for det aktuelle formålet*. Prinsippet gjelder for alle behandlingsformer som utgjør et inngrep i noens privatliv, jf. EMK artikkel 8 nr. 2.[351] I den nye personvernforordningen er nødvendighetsprinsippet, sammen med prinsippene om adekvans og relevans, en del av det nye prinsippet om «dataminimering».

Personopplysningsloven 2000 oppstiller ikke uttrykkelig krav om nødvendighet for at en opplysning skal kunne behandles. Det gjelder likevel et implisitt krav om nødvendighet etter § 28 første ledd første punktum, som fastslår at behandlingsansvarlig ikke skal lagre personopplysninger lenger enn det som er «nødvendig» for å gjennomføre formålet med behandlingen.

Videre oppstiller personopplysningsloven 2000 et relevanskrav, jf. § 11 første ledd bokstav c. Det er imidlertid det særskilte relevanskravet i etterretningstjenesteloven § 3 som i dag er avgjørende for Etterretningstjenestens behandlingsadgang. Bestemmelsens første ledd

[350] Ot.prp. nr. 108 (2008–2009) pkt. 9.2 s. 74–76

[351] *Amann mot Sveits* 16. februar 2000 avsnitt 65 og *S. og Marper mot Storbritannia* 4. desember 2008 avsnitt 67.

oppstiller som vilkår at informasjon bare behandles dersom den «kan bidra til å sikre viktige nasjonale interesser».

12.6.2 Departementets forslag

12.6.2.1 Innledning

Departementet foreslår å lovfeste et særskilt nødvendighetskrav knyttet til hvilke opplysninger som kan behandles av Etterretningstjenesten. Kravet om opplysningens relevans vil være ett av flere momenter i nødvendighetsvurderingen; dersom opplysningen *ikke er relevant* å behandle for etterretningsformål, så er den heller *ikke nødvendig* å behandle.

12.6.2.2 Nødvendighetskravet

Nødvendighetskravet vil være en rettslig standard som vil variere fra situasjon til situasjon og endres i takt med tiden og utviklingen. Et bærende synspunkt er at Etterretningstjenestens systemer og tilgang til informasjon skal sette tjenesten i stand til å utføre sitt samfunnsoppdrag på en effektiv og hensiktsmessig måte. Kunnskap om utenlandske og grenseoverskridende trusler og forhold for øvrig krever et stort tilfang av informasjon, som deretter må sammenstilles og analyseres for å danne et helhetlig bilde. Utviklingen de senere årene viser at vi står overfor et mer fragmentert og uoversiktlig trusselbilde, noe som fører til at det i det praktiske etterretningsarbeidet er avgjørende å kunne bearbeide store mengder opplysninger over tid. Etterretning er som et stort og nitid puslespill hvor historisk informasjon er egnet til å gi forståelse av nåtiden og fremtiden. Sammenstilling av informasjon over tid er egnet til å gi et normalbilde som er nødvendig for å kunne detektere avvik, herunder trusler mot Norges selvstendighet og sikkerhet. Etterretningstjenesten må derfor ha adgang til å behandle alle opplysninger som kommer inn fra egne sensorer, fra andre tjenester og fra offentlige myndigheter, for deretter å kunne avgjøre om disse er nødvendige for utførelsen av tjenestens lovpålagte oppdrag. Departementet foreslår å videreføre terskelen uendret for når en personopplysning anses nødvendig å behandle med et etterretningsformål.

Hvilke opplysninger som det er *nødvendig* å behandle for etterretningsformål beror på en etterretningsfaglig vurdering. Sentrale momenter i denne vurderingen er formålet med og omfanget av behandlingen, inngrepets karakter, samt hvor relevant informasjonen er for formålet. Det vil alltid måtte foretas en forholdsmessighetsvurdering for å avgjøre om nødvendighetskravet er oppfylt. Det er også av betydning om Etterretningstjenesten allerede er i besittelse av opplysninger som gjør de nye opplysningene overflødige og således ikke nødvendige å behandle.

12.6.2.3 Tidspunkt for nødvendighetsvurdering

Etterretningstjenesten kommer daglig i besittelse av omfattende mengder informasjon, både fra partnersamarbeid og gjennom egen innhenting. Departementet har på denne bakgrunn vurdert hvorvidt det er behov for å regulere tidspunktet for *når* nødvendighetsvurderingen skal foretas. Personvernhensyn, og da særlig hensynet til forholdsmessighet, taler for en slik regulering.

Departementet har i denne forbindelse sett hen til politiregisterloven § 8, som gir politiet adgang til å behandle personopplysninger i 4 måneder dersom det er nødvendig for å avklare om kravene til behandling er oppfylt. Departementet har på denne bakgrunn vurdert om det bør settes opp en tilsvarende tidsbestemt evalueringsfrist for Etterretningstjenesten,

men har kommet frem til at dette hverken vil være en hensiktsmessig eller praktisk løsning. Begrunnelsen for dette er at de faktiske og rettslige forutsetningene for en strategisk utenlandsetterretningstjeneste ikke uten videre kan sammenlignes med politiets eller andre etaters informasjonsbehandling. Metodikken som ligger til grunn for utøvelsen av utenlandsetterretning tilsier at det er nødvendig med et stort informasjonsgrunnlag, og det vil ikke være mulig for Etterretningstjenesten å evaluere all informasjon innenfor en 4-månedersfrist. Et slikt krav ville enten innebære behov for en betydelig økning i antall ansatte, med utelukkende dette som oppgave, alternativt at store mengder informasjon vil måtte slettes uten forutgående evaluering.

På denne bakgrunn foreslår departementet for det første at Etterretningstjenesten skal foreta en nødvendighetsvurdering første gang opplysningen vurderes brukt for etterretningsformål. Dette vil for eksempel være tilfelle når en opplysning inntas i et etterretningsprodukt som planlegges distribuert utenfor tjenesten eller informasjonen flyttes fra en plattform til en annen for videre analyse og vurdering. For det andre bør Etterretningstjenesten foreta en nødvendighetsvurdering når ny informasjon eller andre omstendigheter tilsier at det er påkrevd for å ivareta nødvendighetskravet på en forsvarlig måte. Departementet presiserer at de alternative tidspunktene for nødvendighetsvurderingen i enkelte tilfeller kan være sammenfallende.

12.6.2.4 Behandling i den registrertes interesse

Departementet foreslår at prinsippet om at en behandlingsansvarlig kan behandle en personopplysning dersom det er nødvendig for å ivareta den registrertes vitale interesser, kun delvis skal videreføres som et selvstendig behandlingsgrunnlag for Etterretningstjenesten. Departementet foreslår at behandlingsgrunnlaget skal begrenses til behandling av personopplysninger om kilder som ikke ønsker å samarbeide med Etterretningstjenesten. Bakgrunnen for forslaget er utelukkende hensynet til personen selv. Behandling av personopplysninger med dette formålet bør begrenses til det som er strengt nødvendig for å sørge for at tjenesten ikke tar kontakt med vedkommende igjen. Dette behandlingsgrunnlaget bør etter departementets syn fremgå direkte av lovforslaget.

12.6.2.5 Forslag til bestemmelse

Det understrekes at nødvendighetsprinsippet gjelder for alle deler av en behandling og alle behandlingsformer, med unntak av innhenting.[352] Den nærmere vurderingen av om nødvendighetskravet er oppfylt avhenger av hva slags form for behandling det er tale om. Etter forholdene kan det f.eks. tenkes at innsamling av opplysninger er nødvendig, men at utlevering av dem ikke er det.

Departementet foreslår følgende bestemmelse:

§ 9-5 *Nødvendighetskrav*

Etterretningstjenesten skal vurdere om personopplysninger er nødvendige å behandle for etterretningsformål. For personopplysninger som er rådata i bulk skal nødvendighetsvurderingen gjennomføres samlet når rådataen lagres og ellers når ny informasjon eller andre omstendigheter tilsier det.

For personopplysninger som ikke er rådata i bulk skal nødvendighetsvurderingen senest gjennomføres når personopplysningene vurderes brukt for etterretningsformål, herunder når opplysningene inntas i et produkt som planlegges distribuert utenfor Etterretningstjenesten. Det skal foretas en nødvendighetsvurdering hvis ny informasjon eller andre omstendigheter tilsier det.

[352] Innhenting er særskilt regulert i kapittel 5, 6, 7 og 8 i lovforslaget.

Personopplysninger om kilder som ikke ønsker å samarbeide med Etterretningstjenesten kan behandles for å hindre at vedkommende kontaktes igjen. Behandlingen skal være begrenset til det som er strengt nødvendig for dette formålet.

12.6.3 Unntak fra kravene til formålsbestemthet og nødvendighet

12.6.3.1 Nærmere om rådata

Problemstillingen knytter seg til oppbevaring og håndtering av rådata. Rådata er informasjon som Etterretningstjenesten besitter, men der man enda ikke har vurdert hvorvidt informasjonen er nødvendig å behandle for etterretningsformål. Informasjonen kan være innsamlet av Etterretningstjenesten selv eller mottatt fra andre. Det kan være store datasett (bulk), men det er ikke noe krav til størrelsen på informasjonstilfanget for at noe skal kvalifisere som rådata. Det avgjørende er at etterretningsverdien ikke er vurdert. Felles for disse er at opplysningene har kommet i Etterretningstjenestens besittelse med den presumsjon at de er nødvendige å behandle med et etterretningsformål.

12.6.3.2 Gjeldende rett

Behandlingsformen som er relevant for rådata er behandling i form av *lagring.*[353] Slik lagring av rådata har i dag behandlingsgrunnlag både etter personopplysningsloven § 8 sammenholdt med etterretningstjenesteloven § 3 samt de lovregulerte grunnlagene gitt i personopplysningsloven § 8 bokstav d og e, fordi behandlingen anses nødvendig for at Etterretningstjenesten skal kunne utføre sine lovpålagte oppgaver. Sistnevnte må sies å være av «allmenn interesse» i lovens forstand.

Grunnkravene for behandling av personopplysninger, herunder at de ikke skal lagres lenger enn nødvendig ut fra formålet med behandlingen, og at rådataene ikke skal benyttes til formål som er uforenlige med det opprinnelige formålet, jf. § 11 bokstav c og e, gjelder også for rådata. Det er i dag for rådataens vedkommende, som for andre opplysninger Etterretningstjenesten behandler, etterretningstjenesteloven § 3 og personopplysningsloven § 28 som regulerer tjenestens sletteplikt.

Behandling av rådata som utgjør et inngrep i noens privatliv må oppfylle vilkårene etter Grunnloven § 102 og EMK art. 8. Departementets forståelse av EMDs praksis og øvrige rettskilder på området er at det først og fremst er selve registreringen og lagringen av rådata som er inngrepet som må kunne forsvares som nødvendig i et demokratisk samfunn, uavhengig av de nærmere vilkår for myndighetenes tilgang. Dette innebærer ikke at reglene for tilgang og videre bruk av dataene er irrelevante. Disse utgjør avgjørende rettssikkerhetsgarantier. Registrering og lagring av større datasett hvor en konkret nødvendighetsvurdering av hver personopplysning ikke gjennomføres, det vil si lagring av informasjon innhentet ved bulk, er blant annet basert på EMDs uttalelse i saken *Big Brother Watch m. fl. mot Storbritannia* ansett for å ikke være i strid med menneskerettighetene.[354] Dommens betydning i forhold til bulkinnsamling er nærmere redegjort for i kapittel 11.7.6.

12.6.3.3 Departementets forslag

Når Etterretningstjenesten mottar informasjon fra andre nasjonale myndigheter, virksomheter eller internasjonale samarbeidende tjenester, deles disse med

[353] Lagring av informasjon som inneholder personopplysninger utgjør i henhold til personopplysningsloven § 2 nr. 2 «behandling av personopplysninger».

[354] Dommen er en kammerdom og ble avsagt 13. september 2018. Den er i skrivende stund ikke rettskraftig.

Etterretningstjenesten fordi avgiver av informasjonen vurderer at opplysningene er nødvendige for Etterretningstjenestens oppdrag. Det er imidlertid Etterretningstjenesten selv som må vurdere om opplysningene er nødvendig å behandle med et etterretningsformål eller om de må slettes.

Når Etterretningstjenesten selv innhenter informasjon, så velges denne ut basert på konkrete kriterier og etterretningsfaglig forankrede hypoteser, slik at en viss nødvendighetsvurdering allerede er foretatt på innsamlingstidspunktet. Målet er å fremskaffe etterretningsrelevant informasjon.

Formålet med lagringen av rådata er at Etterretningstjenesten skal kunne innhente, bearbeide og analysere etterretningsrelevant informasjon i henhold til tjenestens oppgavesett. Av tekniske og praktiske årsaker er det umulig å foreta rutinemessige gjennomganger av samtlige lagrede rådata på Etterretningstjenestens innsamlingsplattformer for å vurdere om informasjonen er nødvendig å behandle med et etterretningsformål eller ikke. Dette gjelder uavhengig av omfanget til den konkrete innsamlede dataen, og uavhengig av om det skjer ved bulkinnsamling eller ikke. Selv om enkeltinformasjon ikke kan anses for å vært innhentet i bulk, vil den kunne lagres i bulk. Tjenesten mottar og innhenter store mengder data for å ha et adekvat datagrunnlag for å gjøre målrettede søk i, eksempelvis for å finne en fremmed trusselaktør. Et krav om gjennomgang av samtlige data vil kreve at man dedikerer hundrevis av personer til denne oppgaven. I tillegg vil det være negative personvernmessige konsekvenser av å oppstille et slikt krav. Det meste av rådata i bulk som Etterretningstjenesten innhenter eller mottar vil aldri bli gjenstand for evaluering, fordi det som ikke er relevant blant dataene sjelden fremkommer som et resultat av den målrettede søkingen i datasettene. Et krav om gjennomgang av all data for å vurdere nødvendighet opp mot tjenestens oppdrag vil dermed kunne representere et ytterligere inngrep i personvernet, som kommer i tillegg til selve lagringen, samt medføre at Etterretningstjenesten får innsikt i informasjon som tjenesten ikke skal ha innsikt i, før informasjonen slettes.

For rådata som innhentes i bulk vil det som i dag foretas en samlet vurdering forut for innhentingen av om datasettet som sådan er nødvendig å behandle for etterretningsformål. Dette foreslås lovfestet i § 9-5 annet ledd.

Departementet foreslår at Etterretningstjenestens behandling av uevaluerte data videreføres, og foreslår følgende regulering av behandling av rådata:

§ 9-7 *Unntak fra kravene til formålsbestemthet og nødvendighet*
Opplysninger kan behandles dersom det er nødvendig for å avklare om kravene i § 9-2, § 9-5 eller § 9-6 er oppfylt.

12.6.4 Nærmere om sletteplikt.

12.6.4.1 Innledning

Kravet om sletting er et aspekt av nødvendighetskravet i den forstand at dersom opplysningen ikke er *nødvendig* å behandle ut ifra formålet, så skal den slettes. Kravet om sletting er også påkrevd etter menneskerettighetene, med særlig forankring i rettspraksis fra EMD knyttet til EMK artikkel 8. I det følgende vil departementet redegjøre for hvilke krav som gjelder for Etterretningstjenestens sletting av personopplysninger, samt forslag til hvordan sletteplikten bør utformes i lovutkastet. Departementet har for øvrig valgt å behandle sletteplikten for informasjon innsamlet ved bulk særskilt.

12.6.4.2 Gjeldende rett

Sletteplikten til Etterretningstjenesten følger i dag først og fremst forutsetningsvis av etterretningstjenesteloven § 3. I tillegg gjelder slettebestemmelsen i personopplysningsloven 2000 § 28 første ledd.

Sletting er å anse som et grunnkrav etter personopplysningsloven 2000, jf. § 11 første ledd bokstav e med videre henvisning til § 28. Sletteplikten innebærer at behandlingsansvarlig ikke skal lagre personopplysninger lenger enn det som er nødvendig for å gjennomføre formålet med behandlingen. Videre skal personopplysningene slettes med mindre de skal oppbevares i henhold til arkivloven eller annen lovgivning, jf. personopplysningsloven av 2000 § 28 annet punktum. Kravet om nødvendighet er i denne sammenheng både et vurderingstema for om Etterretningstjenesten kan behandle opplysningen, og en frist for når sletting skal finne sted.

12.6.4.3 Departementets forslag

Departementet foreslår å videreføre kravet for når en personopplysning skal slettes og tidspunktet for vurdering av sletteplikten for opplysninger som er evaluert av Etterretningstjenesten. Sletteplikten må særlig ses i sammenheng med nødvendighetsvilkåret. Etter departementets vurdering kan forhåndsfastsatte tidsfrister for sletting av evaluert informasjon vanskelig fastsettes, da dette vil kunne medføre at tjenesten må slette opplysninger som det fortsatt er nødvendige å behandle for etterretningsformål. Slike regler vil ha negative konsekvenser for oppdragsløsningen, og en slik type slettefrist er det heller ikke tradisjon for å oppstille i personvernlovgivningen.

Sletteplikten innebærer plikt til å slette informasjonen fra operative systemer. Arkivverdig materiale som skal lagres i henhold til arkivplikten skal oppbevares adskilt fra operative systemer. I enkelte informasjonssystemer er det teknisk mulig å rekonstruere informasjon som er slettet. Departementet vil for ordens skyld klargjøre at selv om systemet gir en slik mulighet, vil en endelig sletting i de operative systemene anses for å oppfylle sletteplikten selv om det er teoretisk mulig å få informasjonen rekonstruert. Klarhetshensyn tilsier en lovfesting av *når* sletteplikten skal anses oppfylt.

I relasjon til krav om sletting vil departementet bemerke at menneskelige og tekniske feil kan medføre at Etterretningstjenesten erverver informasjon i strid med materielle eller prosessuelle bestemmelser. Erfaringsmessig skjer dette sjelden, fordi Etterretningstjenesten retter stor oppmerksomhet mot å hindre rettsstridig ervervelse av informasjon. Tilfeller av rettsstridig innhenting kan for eksempel skyldes rene tastefeil, eller det kan forekomme svikt i rutiner som medfører at det innhentes informasjon i en lengre tidsperiode enn besluttet. Informasjon som er innhentet i strid med en bestemmelse vil kunne vurderes for videre bruk for etterretningsformål dersom det dreier seg om brudd på interne prosedyrer som kan avhjelpes i ettertid. For innhenting av informasjon som objektivt er i strid med materielle lovbegrensninger, vil dette stille seg annerledes. Hovedregelen vil her være at informasjonen skal slettes, med mindre det dreier seg om informasjon som ikke medfører inngrep overfor enkeltpersoner og øvrige vilkår for videre behandling foreligger. Utenom nødrettstilfellene er det for øvrig uavklart om og i tilfelle i hvilke særskilte situasjoner gjeldende rett åpner for at videre bruk av rettsstridig ervervet informasjonen kan være forholdsmessig etter en konkret vurdering. Departementet ser ikke grunn til å lovregulere disse særlige tilfellene, og viser til at dette heller ikke er gjort for så vidt gjelder politiets bruk av etterretningsinformasjon ervervet i strid med gjeldende bestemmelser.

Departementet foreslår følgende bestemmelse om sletting:

§ 9-9 *Sletting*

Personopplysninger skal slettes når de ikke lenger er nødvendige å behandle etter bestemmelsene i loven her. Opplysninger som er fortrolig kommunikasjon etter § 9-6 skal slettes uten unødig opphold dersom de ikke kan behandles etter § 9-6 første ledd.

Rådata i bulk skal slettes senest 15 år fra lagringstidspunktet, med mindre vesentlige hensyn tilsier at sletting utsettes. Beslutning om utsatt sletting treffes av sjefen for Etterretningstjenesten for ikke mer enn fem år av gangen.

Sletting av personopplysninger i operative systemer og registre som er tilgjengelige for etterretningsproduksjon, er ikke til hinder for lagring av opplysningene etter arkivloven eller annen lovgivning. Sletting er heller ikke til hinder for lagring for historiske, statistiske eller vitenskapelige formål, dersom samfunnets interesse i at opplysningene lagres klart overstiger de ulemper den kan medføre for den enkelte.

Sletting skal anses gjennomført selv om slettede data teoretisk kan rekonstrueres ved hjelp av avansert teknisk gjenfinningsverktøy og innsats fra personer med spesielle systemrettigheter. Etterretningstjenesten skal etablere rutiner som sikrer at slettede data ikke blir rekonstruert for etterretningsformål.

12.6.5 Særlig om sletting av rådata i bulk

12.6.5.1 Innledning

Som det fremgår av forrige kapittel skal Etterretningstjenesten slette personopplysninger den ikke lenger vurderer å være nødvendig for oppdragsløsningen. En slik sletteplikt forutsetter at personopplysningen har vært gjenstand for en konkret nødvendighetsvurdering. Dette vil som nevnt i punkt 12.6.3 ikke være tilfelle for personopplysninger i form av rådata innhentet i bulk. Det bør likevel gjelde en sletteplikt for slike data. Departementet vurderer at det er hensiktsmessig å oppstille en konkret tidsfrist for sletting av rådata i bulk. Dette underbygges nærmere i det følgende.

12.6.5.2 Nærmere om plikten til å slette rådata

Enkelte sammenlignbare land har ikke regulert noen plikt for deres etterretningstjenester til å slette rådata. Dataene slettes formodentlig avhengig av lagringskapasitet. Enkelte andre land har fastsatt en generell grense for sletting av rådata. Sletteplikten inntredelse er imidlertid ulikt regulert i de ulike landene. I Danmark ble det lovfestet en sletteplikt som skulle inntreffe 10 år etter at rådataene var registrert første gang av dansk etterretningstjeneste. Slettefristen ble vurdert til å være for kort sett opp mot tjenestens behov for å ha tilgang på retrospektive data for å se trender og utvikling. Dansk etterretningstjeneste fikk derfor i 2017 utvidet slettefristen til 15 år etter at informasjonen er registrert.

Denne formen for sletting er praktisk gjennomførbar, ettersom det generelt må legges til grunn at rådata etter 15 år hovedsakelig er av historisk verdi, og at man slipper å vurdere hver enkelt databits etterretningsrelevans og derigjennom om nødvendighetsvilkåret er oppfylt. Likevel kan det være rådata som er av åpenbar interesse utover 15 år. Dette taler for at det bør inntas en sikkerhetsventil som i unntakstilfeller kan gi tjenesten mulighet til å lagre rådata utover den standardiserte tidsfristen for sletting av rådata.

12.6.5.3 Departementets vurdering

Det etterretningsfaglige spørsmålet om når rådata mister sin etterretningsverdi er vanskelig å besvare generelt. Det kan imidlertid legges til grunn at dataene etter et gitt antall år hovedsakelig vil ha historisk verdi, selv om det ikke kan utelukkes at enkelte rådatasett fremdeles vil ha etterretningsverdi. I vurderingen av hvor lenge det er nødvendig å

oppbevare rådata i bulk, er departementet av det syn at følgende forhold må vektlegges: For det første er *formålet* med lagringen vesentlig, samt *hvordan* dataene lagres. Etterretningstjenesten er avhengig av å kunne innsamle og lagre store mengder rådata som tjenesten gjennom komplekse søk, og med tjenstlig behov, kan få tilgang til for deretter å hente ut de data som har størst etterretningsmessig verdi. Allerede ved lagringen må det skje en utvelgelse basert på en vurdering av hvilke data som antas å ha størst etterretningsverdi.

Ved innhenting av store datasett vil størsteparten av informasjonen ligge usett av menneskeøyne i tjenestens systemer. Bakgrunnen for dette er at bulkinnsamling innebærer at høystakken blir innsamlet for å finne nålene. Det er kun disse «nålene», altså informasjonen som har etterretningsmessig verdi, som aktivt hentes ut og brukes for etterretningsformål. Etterretningsrelevansen av datasettene som sådan vil kunne eksistere over lengre tid. Dette synliggjøres blant annet gjennom metodikken som benyttes for å finne relevant etterretningsinformasjon. Man ser etter mønstre i store datamengder som er innsamlet over lengre tid, for å finne det etterretningsrelevante.

Personopplysninger som aktivt hentes ut fra rådatamaterialet og som brukes for etterretningsformål, må etter departementets syn underlegges legalitetskontroll og nødvendighetsvurdering så snart de er overført til systemene for *etterretningsproduksjon*. Det er først på dette tidspunktet at dataene blir «sett på» og det foreligger tilstrekkelig grunnlag for å vurdere nødvendigheten av å behandle opplysningene for etterretningsformål. Dersom man anser at opplysningene ikke er nødvendige å behandle for etterretningsformål, eller vurderer opplysningene som overskuddsinformasjon, vil opplysningene bli slettet fra systemene i tjenesten.

Departementet foreslår at Etterretningstjenestens langvarige praksis vedrørende lagring av rådata videreføres, men at det gis en eksplisitt lovfastsatt frist for å slette rådata. Det foreslås en sletteplikt som inntrer senest etter 15 år fra rådataene ble innsamlet. Er det fra rådataene tatt ut opplysninger for videre analyse og etterretningsfaglig vurdering, skal opplysningene følge slettebestemmelsen som gjelder for vurderte data i lovforslaget § 9-9.

Begrepet «senest» skal forstås slik at datasett som er rådata skal slettes på et tidligere tidspunkt dersom Etterretningstjenesten vurderer at datasettet som sådan ikke lenger har etterretningsmessig verdi. Dersom det i fremtiden skulle skje en endring i Etterretningstjenestens prioriterte oppgaver så skal for eksempel datasett innsamlet ved bulk i relasjon til en oppgave som bortfaller slettes. Det vil også kunne tilkomme ny informasjon eller være andre omstendigheter som tilsier at Etterretningstjenesten skal slette opplysningene på et tidligere tidspunkt. Likeledes vil det kunne være en type rådata innsamlet ved bulk som det vil være behov for å behandle utover 15 år. Departementet foreslår derfor å gi en snever unntaksbestemmelse for å kunne behandle rådata i bulk utover 15 år. Departementet vurderer at det bare er dersom det foreligger *vesentlige* etterretningsfaglige hensyn at sletting kan utsettes. Dette formodes kun å være tilfelle unntaksvis, og vil måtte kreve hyppigere vurdering av rådataens nødvendighet for tjenestens oppdragsløsning. Det foreslås at dette skjer ved en fornyet vurdering av sjefen for Etterretningstjenesten senest etter 5 år.

Departementet foreslår følgende bestemmelse i § 9-9 andre ledd:

Rådata i bulk skal slettes senest 15 år fra lagringstidspunktet, med mindre vesentlige hensyn tilsier at sletting utsettes. Beslutning om utsatt sletting treffes av sjefen for Etterretningstjenesten for ikke mer enn fem år av gangen.

12.7 Krav til opplysningens kvalitet

12.7.1 Innledning

Ettersom Etterretningstjenestens hovedoppgave er å klarlegge et korrekt faktum, har tjenesten en sterk egeninteresse i at opplysningene den behandler er så fullstendige og utfyllende som mulig. I denne sammenheng reiser det seg særlige spørsmål i forbindelse med behandlingen av *ikke-verifiserte* opplysninger. Også for denne opplysningstypen har tjenesten en sterk egeninteresse i å bekrefte eller avkrefte opplysningens riktighet. Tema i det følgende er hvilke kvalitetskrav som bør oppstilles for Etterretningstjenestens behandling av personopplysninger.

12.7.2 Gjeldende rett

Det følger av alminnelige personvernprinsipper at personopplysninger som blir behandlet skal være korrekte og oppdaterte. For Etterretningstjenesten følger prinsippet i dag av personopplysningsloven 2000 § 11 første ledd bokstav e.[355] Kravet innebærer at opplysningene må være fullstendige, det vil si utfyllende og detaljerte, og korrekte. Det siste skal sørge for at opplysningene ikke gir et misvisende eller uriktig bilde av en person eller en situasjon. Kravet innebærer også at personopplysninger som ikke imøtekommer kvalitetskravet skal rettes.

Det gjelder også et prinsipp om at ikke-verifiserte opplysninger kan behandles dersom det er nødvendig ut fra formålet med behandlingen. Med «ikke-verifiserte» menes opplysninger hvis riktighet ikke er avklart. Til sammenligning fastsetter politiregisterloven regler om politiets behandling av ikke-verifiserte opplysninger i henholdsvis § 6 om krav til opplysningens kvalitet og § 20 om utlevering av denne typen opplysninger. Det utledes fra disse bestemmelsene at det foreligger en plikt til så langt mulig å verifisere opplysningene, samt at det skal fremgå at opplysningene er ikke-verifiserte.

Reglene om behandling av ikke-verifiserte opplysninger må ses i sammenheng med kravet om korrekthet: I de tilfellene der behandling av ikke-verifiserte opplysninger anses nødvendig, vil korrekthetskravet i praksis kun forby behandling av opplysninger som den behandlingsansvarlige *vet* er feilaktige. Dette innebærer at opplysninger som har vist seg å være ukorrekte, men som ikke nødvendigvis er feilaktige, faller over i kategorien ikke-verifiserte og må behandles deretter.

Opplysninger som ikke lenger er nødvendige å behandle eller som ikke lar seg korrigere skal etter gjeldende personvernprinsipper sperres eller slettes.

EMK artikkel 8 nr. 2 stiller ikke etter sin ordlyd krav til opplysningens kvalitet ved behandling av opplysninger, men det følger av praksis av EMD at behandling av personopplysninger som er feilaktige ikke vil oppfylle forholdsmessighetsvurderingen i nødvendighetskravet, og dermed vil være ulovlig å behandle etter bestemmelsen.

[355] I EUs personvernforordning er prinsippet videreført som et krav til riktighet, se artikkel 5 nr. 1 bokstav d.

12.7.3 Departementets vurdering

Av hensyn til den opplysningene gjelder foreslår departementet at det inntas en regel om at Etterretningstjenesten snarest mulig skal rette eller slette ukorrekte opplysninger. I tillegg foreslås det å pålegge Etterretningstjenesten å sørge for at behandlingen av uriktige opplysninger så langt som mulig ikke får betydning for den eller de det gjelder. Det vil for eksempel innebære en rimelig aktivitetsplikt for tjenesten dersom den blir kjent med at den har delt de uriktige opplysningene med en samarbeidende tjeneste. Også dette vil være en kodifisering av gjeldende praksis.

Det er ikke omtvistet at uriktige registrerte opplysninger i seg selv er et inngrep i personvernet. Likevel kan det ikke være tvilsomt at tjenestens mulighet til å kunne behandle ikke-verifiserte opplysninger er en klar forutsetning for en effektiv utøvelse av Etterretningstjenestens oppgaver. Det er departementet syn at det må være adgang til å behandle ikke-verifiserte opplysninger dersom det er nødvendig ut fra formålet med behandlingen. Ettersom etterretningsvirksomhet nettopp er å kartlegge korrekt faktum blant annet gjennom en vurdering av kildens troverdighet, vil det at en opplysning er ikke-verifisert forutsetningsvis måtte fremgå i beskrivelsen eller konteksten opplysningen blir brukt i. Etter gjeldende praksis fremkommer det således av opplysningene selv eller av sammenhengen for øvrig at opplysningene er ikke-verifiserte. Departementet vurderer at dette er en god praksis som bør lovfestes.

Departementet foreslår følgende bestemmelse i § 9-8:

§ 9-8 *Krav til opplysningenes kvalitet*

Etterretningstjenesten skal så langt det er mulig påse at personopplysninger som behandles og som ikke er rådata i bulk, er korrekte og oppdaterte. Opplysninger som ikke er korrekte skal uten opphold slettes eller korrigeres. Etterretningstjenesten skal så langt som mulig sørge for at feilen ikke får betydning for den det gjelder.

Ikke-verifiserte opplysninger kan behandles dersom det er nødvendig ut fra formålet med behandlingen. Det skal fremgå av Etterretningstjenestens produkter dersom ikke-verifiserte personopplysninger er behandlet.

12.8 Integritet og konfidensialitet

12.8.1 Krav om sikker behandling. Gjeldende rett

Prinsippene om integritet og konfidensialitet er grunnleggende i personopplysningsretten. Formålet er å påse at personopplysningene behandles på en måte som sørger for tilstrekkelig sikkerhet ved å innføre egnede tekniske eller organisatoriske tiltak som skal sikre mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade. Dette innebærer at Etterretningstjenesten som behandlingsansvarlig må foreta en risikovurdering og vurdering av egnede tiltak for å sikre personopplysningene som behandles, både mot utenforstående og mot ansatte som ikke har tjenstlig behov for kjennskap til opplysningene. Etterretningstjenesten må videre sikre at de som skal ha tilgang til personopplysninger faktisk får det, slik at inntrykket av en person ikke blir feilaktig. Prinsippene om integritet og konfidensialitet må dermed ses i sammenheng med kravet om opplysningenes kvalitet, se over i punkt 12.7.

EMK artikkel 8 oppstiller ikke etter sin ordlyd krav om integritet og konfidensialitet ved behandlingen av personopplysninger, men det kan tenkes at kravet til forholdsmessighet

ikke vil være oppfylt dersom Etterretningstjenesten ikke behandler personopplysninger i tråd med disse prinsippene.

Det følger av personopplysningsloven og sikkerhetslovens[356] regler at Etterretningstjenesten selv har et ansvar for å hindre sikkerhetsbrudd som kan skade eller ødelegge lagrede data eller krenke personvernet. Av særlig relevans er personopplysningsloven 2000 § 13 første ledd, hvor det fastslås at:

> Den behandlingsansvarlige og databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger.

I tillegg ivaretas informasjonssikkerheten knyttet til informasjonen gjennom samarbeid med Nasjonal sikkerhetsmyndighet (NSM), som også fører overordnet tilsyn med tjenesten innenfor rammen av sikkerhetsloven med utfyllende forskrifter.

12.8.2 Departementets forslag

Lovforslaget innehar en bestemmelse om informasjonssikkerhet i utkast til § 11-4, hvor det heter at:

> Etterretningstjenestens arkiver, informasjonssystemer og etterretningsregistre skal være betryggende sikret og utilgjengelig for andre enn eget autorisert personell med tjenstlig behov for tilgang og personer som er satt til å føre kontroll og tilsyn med Etterretningstjenesten.

Bestemmelsen foreslås ikke først og fremst av personvernmessige årsaker, men av sikkerhetsmessige hensyn. Ettersom det alt vesentlige av Etterretningstjenestens opplysninger vil være sikkerhetsgradert informasjon i henhold til sikkerhetsloven, vurderer departementet at dersom tjenestens informasjonssikkerhetstiltak tilfredsstiller sikkerhetslovens krav til behandling av sikkerhetsgraderte opplysninger, bør de to grunnleggende personvernprinsippene integritet og konfidensialitet også anses tilfredsstilt. Bakgrunnen for dette er at sikkerhetslovens krav antas å stille høyere krav til sikkerhet for opplysningene og autorisasjonsadgang mv. enn det som følger av prinsippene om integritet og konfidensialitet. Bestemmelsen må således tolkes i lys av de til enhver tid gjeldende sikkerhetskrav som følger av sikkerhetsloven. Som en følge av dette vil et brudd på sikkerhetslovens strenge krav til informasjonssikkerhet mv. innebære et brudd på personopplysningskravene om integritet og konfidensialitet.

Det er etter departementets syn likevel grunn til å lovfeste en særskilt regel om informasjonssikkerhet ved behandling av personopplysninger. De to kravene sett i sammenheng innebærer at det stilles høyere krav til integritet og konfidensialitet for Etterretningstjenesten enn for andre offentlige etater og kommersielle aktører som behandler personopplysninger etter den alminnelige personopplysningslovgivningen. Departementet vurderer dette som rimelig, gitt virksomhetens særpreg. Departementet legger til at Etterretningstjenesten på flere områder har implementert et langt høyere sikkerhetsnivå enn det som følger av sikkerhetslovens minimumsregler.

Departementet foreslår følgende bestemmelse:

§ 9-11 *Informasjonssikkerhet*

[356] Lov om forebyggende sikkerhet av 20. mars 1998. Ny sikkerhetslov er vedtatt, men i skrivende stund ikke trådt i kraft.

Etterretningstjenesten skal gjennom systematiske tiltak sikre konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger. Tiltakene skal utformes i samsvar med bestemmelsene i sikkerhetsloven og annen relevant lovgivning og være basert på risikovurdering, sikkerhetsrevisjon, sikkerhetsovervåking og internkontroll.

Personopplysninger skal ikke gjøres tilgjengelige for flere personer enn nødvendig for å oppfylle formålet med behandlingen.

12.9 Særlig om behandling av personopplysninger i forbindelse med trening, øving og testing

12.9.1 Behovet for trening, øving og testing. Gjeldende rett.

En forutsetning for å drive etterretningsvirksomhet er at det i forkant er utført trening og øving av personell, og at utstyr er tilstrekkelig testet. Særlig gjelder dette ved utførelsen av etterretningsoppdrag, samt for å sikre styrkebeskyttelse av Forsvarets personell som befinner seg i konfliktsoner. På grunn av den teknologiske utviklingen må Etterretningstjenestens kapasiteter testes og øves jevnlig. Det stilles høye krav til den enkelte operatør om å være oppdatert om hvordan systemene fungerer til enhver tid. Ved deployering til konfliktsoner vil det kunne ha store konsekvenser både for operasjonen som sådan og for operatørens liv og helse om ikke operatøren er kjent med og kan håndtere de ulike innsamlingsmetodene på riktig måte; Etterretningstjenesten kan derfor ikke starte opptrening av operatører eller testing av tekniske kapasiteter i fiendtlige omgivelser i utlandet.

De rettslige rammene for Etterretningstjenestens behandling følger av Grunnloven § 102 og EMK artikkel 8, gjeldende etterretningstjenestelov, og personopplysningsloven av 2000. Behandling av opplysninger i forbindelse med trening, øving og testing reguleres altså av de samme nasjonale og internasjonale bestemmelsene som gjelder for øvrig behandling av opplysninger for etterretningsformål. Trenings-, øvings- og testaktivitetene er også inngående regulert i interne prosedyrer. Prosedyrene skal sikre riktig etterlevelse av lovgivningen.

12.9.2 Departementets forslag

Departementet foreslår at *behandlingsgrunnlaget* for å behandle opplysninger i forbindelse med trening, øving og testing fastsettes i en egen bestemmelse i lovutkastet kapittel 9. Departementets forslag til *innhentingshjemmel* fremgår av lovutkastet § 3-5. Både menneskebaserte og tekniske innsamlingskapasiteter omfattes. Departementet mener at denne formen for innhenting fordrer at det utformes særlige slettebestemmelser som sikrer at opplysningene oppbevares kortest mulig tid.

Det kan tenkes tilfeller der operatørene i ettertid, for læringsformål, ønsker å gjennomgå materialet fra en trening eller testing og sammenholde det med tidligere treninger eller tester for å avdekke eventuelle konfigurasjonsfeil mv. Departementet mener at slik videre behandling av opplysningene må kreve samtykke fra den som opplysningene gjelder. Alternativt må opplysningene anonymiseres slik at de ikke lenger er å anse som personopplysninger.

Departementet foreslår at det oppstilles en plikt til å behandle opplysningene adskilt fra opplysninger som behandles for andre etterretningsformål enn trening, øving og testing.

Opplysningene skal være gjenstand for kontroll av EOS-utvalget på lik linje som øvrige opplysninger.

Forslaget innebærer en kodifisering av tjenestens praksis vedrørende behandling av opplysninger ved trening, øving og testing av innhentingskapasiteter på norsk territorium.

Departementet foreslår følgende bestemmelse:

§ 9-10 *Opplysninger innhentet ved trening, øving og testing*
Behandling av personopplysninger i forbindelse med testing av teknisk utstyr eller trening og øving skal skje adskilt fra Etterretningstjenestens øvrige behandling av opplysninger.
Personopplysninger innhentet ved virksomhet etter første ledd skal slettes snarest mulig etter at treningen, øvingen eller testvirksomheten er avsluttet, og skal ikke arkiveres i henhold til arkivloven. Unntak gjelder dersom den enkelte berørte person har avgitt uttrykkelig samtykke til videre behandling.

12.10 Særlig om behandling av fortrolig kommunikasjon med særlige yrkesutøvere

12.10.1 Innledning

Fortrolig kommunikasjon med visse yrkesutøvere, slik som mellom advokat og klient, journalist og kilde, og helsepersonell og pasient, er for yrkesutøveren underlagt lovfestet og/eller yrkesetisk taushetsplikt. Myndighetenes innhenting og behandling av kommunikasjon mellom to parter som anses å ha et særlig beskyttet forhold, er inngripende i et personvern- og ytringsfrihetsperspektiv. Slik kommunikasjon omtales i det følgende som *fortrolig kommunikasjon* med *særlige yrkesutøvere*.[357] Informasjonen er underlagt et særlig vern som skal sikre fortrolighet og konfidensialitet. Hensynet bak vernet er at borgerne skal kunne søke profesjonell behandling, hjelp eller råd eller varsle om kritikkverdige forhold uten å risikere at de opplysninger som de gir fra seg, gjøres kjent eller gis videre. Myndighetene kan derfor ikke fritt samle inn og behandle opplysninger som stammer fra fortrolig kommunikasjon.

Innledningsvis mener departementet at det er grunn til å understreke at Etterretningstjenestens virksomhet retter seg mot utlandet. Det er etter lovutkastet § 4-1 forbudt for Etterretningstjenesten å rette innhenting mot personer som befinner seg i Norge. Tjenesten vil derfor bare unntaksvis komme i besittelse av fortrolig kommunikasjon med særlige yrkesutøvere i Norge, for eksempel i tråd med unntaksbestemmelsen i lovutkastet § 4-2 første ledd, der Etterretningstjenesten vil kunne rette innhenting mot en slik yrkesutøver dersom denne opptrer på vegne av fremmed makt.

I det følgende vil departementet redegjøre for innholdet i og rekkevidden av vernet om fortrolig kommunikasjon, og hvilke regler departementet mener bør gjelde for Etterretningstjenestens behandling av slik kommunikasjon.

[357] Begrepet «særlige yrkesutøvere» foreslås som samlebegrep som omfatter samtlige yrkesgrupper hvis kommunikasjon kan være fortrolig.

12.10.2 Hvorfor har Etterretningstjenesten behov for å behandle fortrolig kommunikasjon?

Etterretningstjenestens virksomhet handler litt forenklet sagt om å samle sammen informasjonsbiter og sette dem sammen til et helhetlig bilde. Bakgrunnen for dette sammenstillingsbehovet er for å gi beslutningstakerne et så korrekt situasjonsbilde som mulig. I dette arbeidet er i utgangspunktet all innhenting som kan frembringe etterretningsrelevant informasjon av interesse, og det er analytikernes jobb å evaluere informasjonens etterretningsrelevans- og verdi. Etterretningstjenestens behov for å behandle fortrolig kommunikasjon er i og for seg ikke spesielt sammenlignet med behovet for å behandle annen kommunikasjon. Det som gjør at behandlingen av fortrolig kommunikasjon krever en spesiell begrunnelse, er at den vernede interessen – altså det fortrolige forholdet mellom de særlige yrkesutøverne og deres respektive klienter, kilder, pasienter e.l. – er av en slik art at terskelen for å behandle den ligger høyere enn ved annen kommunikasjon. I noen tilfeller må imidlertid vernet vike. Det gjelder spesielt, men ikke bare, i tilfeller hvor behandling av fortrolig kommunikasjon kan være av særlig betydning for å vurdere en potensielt alvorlig trussel mot Norge.

I tillegg er det et vesentlig moment at et absolutt forbud mot behandling av slik informasjon vil være egnet for misbruk gjennom at etterretningsmål tilpasser sin opptreden for å slippe unna Etterretningstjenestens søkelys. Et eksempel på dette kan være at terrorister eller ekstremister oppretter tidsskrifter for det formål å rekruttere og oppfordre til terrorhandlinger. Et annet eksempel kan være advokaten eller helsearbeideren som under påskudd av å drive alminnelig virksomhet i realiteten fasiliterer for et miljø som truer Norge, eller som for eksempel driver etterretningsvirksomhet mot Norge ved å kartlegge norske militære kapasiteter.

12.10.3 Rettslige rammer for behandling av fortrolig kommunikasjon

Den rettslige rammen som reguleringen av Etterretningstjenestens behandling av fortrolig kommunikasjon må være innenfor, vil være Grunnloven og Norges menneskerettslige forpliktelser. Av særlig betydning er retten til privatliv etter Grunnloven § 102 første ledd første punktum og EMK artikkel 8, samt retten til ytringsfrihet etter Grunnloven § 100 og EMK artikkel 10. Myndighetene vil kunne gripe inn i de respektive rettighetene såfremt den inngripende handlingen har forankring i lov, er nødvendig for å oppfylle et legitimt formål og er forholdsmessig.[358] Som det vil fremkomme av drøftelsene under gjelder det en høy terskel for inngripende myndighetsutøvelse på dette området. Det kan imidlertid ikke utledes et absolutt forbud mot behandling av fortrolig kommunikasjon.

Etter nasjonal rett er fortrolig kommunikasjon vernet i tvisteloven[359] og straffeprosessloven.[360] Etterretningstjenestens virksomhet reguleres ikke av disse regelsettene. Bestemmelsene i tvisteloven og straffeprosessloven vil også ha begrenset overføringsverdi sett hen til at hensynene bak prosessretten ikke er hensynet til rikets sikkerhet, men en balanse mellom hensynet til at domstolen fatter flest riktige avgjørelser sett opp mot personvernhensyn. Utformingen av reglene om behandling av fortrolig

[358] Se nærmere om dette i høringsnotatet kapittel 4.

[359] Lov av 17. juni 2005 nr. 90 om mekling og rettergang i sivile tvister

[360] Lov av 22. mai 1981 om rettergangsmåten i straffesaker

kommunikasjon etter lovforslaget her må derfor gjøres i lys av de særegne hensyn som gjør seg gjeldende for en utenlandsetterretningstjeneste, og innenfor rammen av Grunnloven og menneskeretthetene.

12.10.4 Nærmere om kallsmessig taushetsplikt som grunnlag for vern

I den alminnelige lovgivningen er en rekke beskyttede relasjoner ivaretatt ved at det er oppstilt rettslig sterk taushetsplikt for yrkesutøveren. Denne type taushetsplikt blir kalt «kallsmessig taushetsplikt».

For at borgerne risikofritt skal kunne søke profesjonell hjelp som nevnt, må de ha krav på at de opplysningene som yrkesutøveren får ved slike konsultasjoner blir mellom dem. Dette konfidensialitetsbehovet er så viktig at yrkesutøverens taushetsplikt ved slike konsultasjoner må anses beskyttet av EMK artikkel 8 nr. 1.[361]

Det finnes i dag hjemler i den alminnelige lovgivningen som gjør inngrep i den kallsmessige taushetsplikten. Et eksempel er at kommunikasjonskontroll av telefon som tilhører advokat, lege, prest eller andre som erfaringsmessig fører samtaler av fortrolig art, samt telefon som tilhører redaktør eller journalist, kan gjennomføres når det foreligger særlige grunner, jf. straffeprosessloven § 216 c. Det gjelder altså ikke et absolutt forbud mot å gjøre inngrep i form av innhenting og behandling av opplysninger undergitt kallsmessig taushetsplikt etter norsk rett. Det samme antas å gjelde etter internasjonal rett, se særlig Veneziakommisjonens[362] rapport, hvor det uttales at: [363]

> "The ECtHR`s case law, inter alias Klass v. FRG, Kopp v. Switzerland and a letter interception case, Erdem v. Germany, indicate that the Convention does not require states to abstain totally from engaging in surveillance of "privileged communications."

Denne tolkningen av EMK artikkel 8 er også lagt til grunn i norsk høyesterettspraksis, jf. Rt 2008 s. 158 og Rt. 2011 s. 296.

Det avgjørende for om myndighetene kan behandle opplysninger som er underlagt kallsmessig taushetsplikt, vil etter dette være *alvorlighetsgraden* av det forholdet som den fortrolige kommunikasjonen omhandler og om behandling av opplysningene er *forholdsmessig* i det konkrete tilfellet.

12.10.5 Nærmere om kildevernet

Kildevernet skal sikre at personer som besitter informasjon om forhold som er av allmenn interesse kan formidle dette via pressen uten frykt for straff eller represalier. Formålet med kildevernet er ikke å verne kilden som sådan, men snarere å verne om medias evne til å formidle om kritikkverdige forhold og på den måten sette befolkningen i stand til å kunne stille makthavere eller andre til ansvar.[364]

---

[361] Vernet om kallsmessig taushetsplikt i er forankret i retten til vern om «korrespondanse» i EMK artikkel 8. Dette må etter EMDs praksis på området tolkes teknologinøytralt, jf. *Andre mot Frankrike* avsagt 24. juli 2008 og *Affaire Michaud mot Frankrike* avsagt 6. desember 2012.

[362] Veneziakommisjonen består av en gruppe folkerettseksperter oppnevnt av Europarådet.

[363] Update of the 2007 Report on the Democratic Oversight of the Security Services and Report of the Democratic Oversight of Signals Intelligence Agencies" (CSL-AD(20015)006, Study No. 719/2013).

[364] Se for eksempel Rt. 2010 s. 1381 og Rt. 2013 s. 1290

Det følger av Grunnloven § 100 sjette ledd at myndighetene skal «legge forholdene til rette for en åpen og opplyst offentlig debatt.» Dette tyder på at lovgiver er forpliktet til å vedta lovgivning som sikrer kilders rett til å være anonyme, slik at pressen ikke forhindres fra å tilrettelegge for en åpen og opplyst debatt på grunn av mangel på kilder. Lovgivning som ikke i tilstrekkelig grad ivaretar kildevernet *kan* svekke potensielle kilders tillit til at pressen vil sikre anonymitet, og *kan* ha som konsekvens at det oppstår en nedkjølende effekt på pressens kildetilfang. Uten tilgang på kilder er det nærliggende å anta at pressens samfunnsoppdrag ikke kan løses på en god måte. I tillegg er ytringen også en viktig forutsetning for et demokrati. Denne siden av nedkjølingseffekten må tas på alvor, noe som også er understreket i både nasjonal og internasjonal rettspraksis.[365]

Kildevernet er rettslig forankret i Grunnloven § 100 og EMK artikkel 10. Ved reguleringen av Etterretningstjenestens håndtering av vernet materiale faller en derfor tilbake på rammer som følger av disse bestemmelsene, samt rettspraksis fra EMD. Selv om det ikke fremgår direkte av bestemmelsen, er det klart at EMK artikkel 10 sikrer journalisters kildevern. Eksempelvis uttalte EMD følgende i saken *Goodwin mot Storbritannia*:

> «Protection of journalistic sources is one of the basic conditions for press freedom.
>
> […]
>
> Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result the vital public watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected. Having regard to the importance of the protection of journalistic sources for press freedom in a democratic society and the potentially chilling effect an order of disclosure has on the exercise of freedom, such a measure cannot be compatible with Article 10 (art. 10) of the Convention unless it is justified by an overriding requirement in the public interest.[366]
>
> […]
>
> In sum, limitations on the confidentiality of journalistic sources call for the most careful scrutiny by the Court.»[367]

Av *Goodwin*-dommen kan det sluttes at det må foreligge betydelig interesseovervekt for de motstående hensyn for at kildevernet skal vike, og videre at unntak bare kan være aktuelt der meget tungtveiende hensyn kan oppveie de hensyn som taler for kildevern.[368]

I avgjørelsen *Big Brother Watch mot Storbritannia* ble Storbritannia ansett for å ha opptrådt i strid med EMK artikkel 10 ettersom det britiske bulkinnsamlingsregimet ikke i tilstrekkelig grad vernet om konfidensielt journalistisk materiale.[369] EMD la avgjørende vekt på at det ikke eksisterte offentlig tilgjengelige bestemmelser som regulerte analytikeres adgang til å søke etter og analysere slik informasjon fra bulkdatalageret, herunder regler som anga terskelen for å behandle denne type informasjon. Dommen gir anvisning på at det ikke er tilstrekkelig

---

[365] Se for eksempel Rt. 2015 s. 1286; *Nagla mot Latvia* av 16. juli 2013; *Big Brother Watch mot Storbritannia* av 13. september 2018 (sistnevnte er når dette skrives ikke rettskraftig).

[366] *Goodwin mot Storbritannia* avsagt 27. mars 1996 avsnitt 39

[367] Ibid. avsnitt 40

[368] Ot.prp.nr.55 (1997-1998) Om lov om endringer i rettergangslovene m m (kildevern og offentlighet i rettspleien) punkt 3.2.6.5 s. 27

[369] Dommen er ikke rettskraftig.

at et høyt terskelkrav praktiseres, all den tid terskelen og tolkningsgrunnlaget for denne ikke er forankret i regelverk som er *tilgjengelig* for allmennheten. EMD er således fortsatt av den oppfatning at kildevernet ikke er absolutt, men at adgangen til å behandle slik informasjon må være regulert på en slik måte at det sikrer forutberegnelighet.

I likhet med hva som gjelder for opplysninger som er underlagt kallsmessig taushetsplikt vil spørsmålet om behandling av materiale underlagt kildevernet avgjøres på bakgrunn av en konkret helhetsvurdering av om terskelen for behandling er nådd – altså om inngrepet er «justified by an overriding requirement in the public interest»,[370] herunder om behandling av opplysningene er forholdsmessig i det konkrete tilfellet.

12.10.6 Departementets vurdering

12.10.6.1 Innledning

På bakgrunn av redegjørelsene over mener departementet at det må lovfestes særlige regler for Etterretningstjenestens behandling av fortrolig kommunikasjon. De vurderingene som departementet har foretatt ved utformingen av forslaget, herunder *hvem* og *hva* som er omfattet av vernet og *hvilken* terskel som bør legges til grunn, fremkommer i det følgende.

12.10.6.2 Hvilke yrkesgrupper bør omfattes?

Departementet foreslår å bruke sekkebetegnelsen «særlig yrkesutøver» for å angi hvilke yrkesutøvere som er omfattet av bestemmelsen. Med «særlig yrkesutøver» mener departementet yrkesutøvere som er underlagt lovbestemt eller yrkesetisk taushetsplikt (kallsmessig taushetsplikt), eller journalister o.l. som har rett til å forholde seg taus om identiteten til kilder for opplysninger (kildevern). Enkelte yrkesgrupper, slik som advokater, helsepersonell og journalister, tilhører kjernen av de som er tilkjent et særlig menneskerettslig vern og foreslås nevnt særskilt.

Yrkesutøvere som anses å inneha en kallsmessig taushetsplikt etter nasjonal rett er angitt i straffeprosessloven § 119 og tvisteloven § 22-5 som prester i statskirken, prester eller forstandere i registrert trossamfunn, advokater, forsvarere i straffesaker, meklingsmenn i ekteskapssaker, leger, psykologer, apotekere, jordmødre eller sykepleiere. Bestemmelsene må anses som en uttømmende liste over de relasjoner som er særlig beskyttet etter norsk rett. Departementet har vurdert om en tilsvarende opplisting bør inntas i lovforslaget, men har falt ned på at det er mer hensiktsmessig å lage en sekkebestemmelse som gir nødvendig grad av fleksibilitet hva angår yrkesgrupper som det ikke er like enkelt å identifisere i *utlandet* som det er i Norge. Et eksempel på en slik yrkesgruppe er «prester eller forstandere i registret trossamfunn» ettersom det ikke kan legges til grunn at andre land har tilsvarende krav om registrering i trossamfunn som det norske regelverket.

At bestemmelsen gir Etterretningstjenesten adgang til å ha en fleksibel tilnærming til spørsmålet om en konkret person tilhører en «særlig yrkesgruppe» vurderes på denne bakgrunn som hensiktsmessig. En slik løsning vil også åpne for at vernet kan fastlegges i takt med samfunnsutviklingen. Dette understreker at vernet er *funksjonelt*, ikke formelt. I vurderingen vil det ha stor betydning i hvilken utstrekning den særlige yrkesutøveren opererer i tråd med de profesjonelle og yrkesetiske krav som bærer det særlige vernet. For

[370] Jf. for eksempel *Big Brother Watch m. fl. mot Storbritannia* av 13. august 2018 avsnitt 488 og 492. Dommen er når dette skrives ikke rettskraftig, men samme formulering benyttes også i tidligere dommer fra EMD.

eksempel vil ikke enhver blogger eller driver av et nettsted kunne likestilles med en journalist.

Personkretsens rekkevidde må nødvendigvis bero på en konkret vurdering, herunder en vurdering av om yrkestittelen er reell eller et skalkeskjul for virksomhet som ikke gir grunnlag for vern. For eksempel kan en person som oppgir seg for å være sjelesørger i realiteten drive med ulovlig spredning av masseødeleggelsesvåpen. Som nevnt innledningsvis vil en person aldri være å regne som «særlig yrkesutøver» dersom det sannsynliggjøres at en yrkestittel misbrukes. I slike tilfeller er selvsagt ikke kommunikasjonen vernet. Det kan også tenkes at en person som *de facto* fungerer som særlig yrkesutøver *også* bedriver illegal virksomhet i arbeidstiden. I slike tilfeller må det vurderes konkret hvilke opplysninger som må regnes som «fortrolige».

12.10.6.3 Hva er omfattet av begrepet «fortrolig kommunikasjon»?

For at opplysninger skal regnes som særlig vernet, er det avgjørende at de, etter en konkret vurdering, er å anse som «fortrolig kommunikasjon» mellom to personer som anses å ha et særlig beskyttet forhold, slik som blant annet forholdet mellom advokat og klient, en person og vedkommende sin sjelesørger, helsepersonell og pasient eller journalist og kilde.

Det er kommunikasjonens *karakter* som er avgjørende; det at noen har kommunisert noe til en person som ledd i utførelsen av dennes yrke, er altså ikke ensbetydende med at kommunikasjonen er «fortrolig». På den annen side er det en nødvendig forutsetning for at kommunikasjonen skal anses som «fortrolig» at denne er gitt til en person som faller inn i kategorien «særlig yrkesutøver». Sagt med andre ord: ikke all kommunikasjon gitt til en «særlig yrkesutøver» er «fortrolig», men all «fortrolig kommunikasjon» er gitt til en «særlig yrkesutøver».

I tillegg til yrkesgruppen må opplysningene ha blitt gitt til vedkommende yrkesutøver i forbindelse med utøvelsen av vedkommende sin stilling – det skilles altså mellom profesjonell og privat kommunikasjon. Opplysninger som ikke har sammenheng med yrkesutøverens særlige funksjon, omfattes ikke av vernet. Vennekommunikasjon og lignende er dermed ikke vernet. Denne forståelsen av vernets rekkevidde er også lagt til grunn i norsk prosessrett, og er ikke særegen for det departementet foreslår skal gjelde for Etterretningstjenesten.

12.10.6.4 Nærmere om terskelen for behandling av fortrolig kommunikasjon

Departementet mener at en uthuling av det særlige vernet av fortrolig kommunikasjon kan påvirke samfunnet så vel som den enkelte på en negativ måte. Departementet tar faren for en nedkjølende effekt knyttet til pressens kildetilfang og bruk av tjenester der yrkesutøveren er underlagt kallsmessig taushetsplikt på alvor. Et absolutt forbud mot behandling av privilegert kommunikasjon kan imidlertid ikke utledes av Norges menneskerettslige forpliktelser, og noe slikt forbud bør etter departementets syn heller ikke oppstilles i loven gitt de samfunnsmessige verdier Etterretningstjenesten har som oppgave å verne. Sentrale siktemål har derfor vært å utforme lovgivningen på en måte som i størst mulig grad forhindrer at slike alvorlige konsekvenser realiserer seg, samtidig som handlingsrommet for Etterretningstjenestens oppgaveløsning ivaretas, og muligheten for omgåelse av regelverket snevres inn.

Spørsmålet om Etterretningstjenesten kan behandle fortrolig kommunikasjon må avgjøres på bakgrunn av en konkret helhetsvurdering. Det vil etter departementets syn ikke være tilstrekkelig at Etterretningstjenesten anser det som nødvendig å behandle informasjonen;

terskelen må være såpass høy at tjenesten vurderer behandling av fortrolig kommunikasjon som strengt nødvendig for å ivareta samfunnets interesser. I forholdsmessighetsvurderingen som må foretas bør samfunnets interesse i at det særlige vernet overholdes veies opp mot hensynet til nasjonal sikkerhet. I praksis vil kravet til streng nødvendighet innebære at opplysningene må være av vesentlig betydning for utførelsen av et konkret oppdrag, og informasjon må være umulig å tilveiebringe på noen annen praktikabel og mindre inngripende måte. Terskelen må tolkes og anvendes i lys av Norges menneskerettslige forpliktelser.

Departementet foreslår på denne bakgrunn at fortrolig kommunikasjon bare kan behandles dersom *vektige samfunnshensyn* gjør behandlingen *strengt nødvendig*. Som en garanti mot misbruk foreslår departementet at adgangen til å behandle fortrolig kommunikasjon bør være underlagt særlige kontrollmekanismer, herunder en begrenset delingsadgang. Departementet foreslår at opplysninger som stammer fra fortrolig kommunikasjon som ikke kan behandles av Etterretningstjenesten heller ikke skal kunne utleveres som ledd i nasjonalt eller internasjonalt samarbeid, se utkast til § 10-8 tredje ledd. Det samme foreslås å gjelde for fortrolig kommunikasjon som vurderes som overskuddsinformasjon. Slike lovfestede delingsforbud vil etter departementets syn være effektive tiltak mot potensielle negative konsekvenser, herunder risikoen for en nedkjølende effekt.

Departementet foreslår som en ytterligere sikkerhetsgaranti at beslutningen om å behandle privilegert kommunikasjon bør fattes av sjefen for Etterretningstjenesten, og i enkelte tilfeller av departementet selv. Videre bør det oppstilles en plikt til særskilt å merke opplysninger som stammer fra fortrolig kommunikasjon. Formålet med merkingen vil da være å fasilitere for EOS-utvalgets kontroll, herunder hvordan tjenesten praktiserer kravet om streng nødvendighet.

Departementet foreslår følgende bestemmelse:

§ 9-6 *Nødvendighetskrav for behandling av fortrolig kommunikasjon med særlige yrkesutøvere*

Etterretningstjenesten skal ikke behandle opplysninger som er fortrolig kommunikasjon mellom advokat og klient, helsepersonell og pasient, journalist og kilde eller tilsvarende fortrolig kommunikasjon som nyter særlig menneskerettslig vern, med mindre vektige samfunnshensyn gjør behandlingen strengt nødvendig.

Beslutning om å behandle opplysninger etter første ledd treffes av sjefen for Etterretningstjenesten, med mindre beslutning tilligger departementet etter § 2-7.

Opplysningene skal merkes særskilt for kontrollformål.

§ 10-8 *Utlevering av overskuddsinformasjon*

Overskuddsinformasjon kan deles med norske offentlige myndigheter når vilkårene etter § 10-5 er oppfylt, med unntak av vilkåret om at Etterretningstjenesten kan behandle opplysningene etter kapittel 9.

Overskuddsinformasjon som fremkommer gjennom innhenting etter kapittel 7, reguleres av § 7-12.

Overskuddsinformasjon som er fortrolig kommunikasjon etter § 9-6 kan ikke utleveres.

12.11 Personvernrådgiver

Personvernombudsordningen i dagens personopplysningsregelverk er ikke obligatorisk, med mindre annet er bestemt i lov. Forut for gjennomføringen av personvernforordningen eksisterte det ingen generell plikt i norsk rett til å ha personvernombud. Etter vedtakelsen har behandlingsansvarlige og databehandlere på nærmere vilkår en plikt til å utpeke

personvernombud. Videre oppstiller forordningen detaljerte regler om personvernombudets oppgaver og uavhengige posisjon i virksomheten.

Etterretningstjenesten har siden 2014 hatt en egen ansatt som er utpekt som tjenestens personvernrådgiver. Personvernrådgiveren har hatt som oppgave å påse at Etterretningstjenesten behandler personopplysninger i overenstemmelse med personvernlovgivningen, samt å utarbeide rutiner og opplæring for å sikre at behandlingen av personopplysninger er i tråd med gjeldende rett.

Som nevnt over gjelder ikke personopplysningsloven 2018 for Etterretningstjenestens virksomhet, med mindre det er tale om behandling av personopplysninger for andre formål enn etterretningsformål. Departementet foreslår likevel å lovfeste en plikt for Etterretningstjenesten til å ha en eller flere personvernrådgivere ansatt i egen organisasjon med spesifikt ansvar for å ivareta personopplysningsvernet i utøvelsen av etterretningsvirksomhet.. Personvernrådgiveren skal bidra til intern legalitetskontroll, notoritet og at behandling av personopplysninger i Etterretningstjenesten skjer i overensstemmelse med lovgivningen og folkerettslige forpliktelser. Personvernrådgiveren vil også, slik som i dag, kunne fungere som en varslingskanal internt i Etterretningstjenesten, og som en rådgiver for de ansatte i personvernfaglige spørsmål.

Den eller de som fungerer som personvernrådgiver i tjenesten bør ha dybdekunnskap om personvernlovgivning og praksis på området. Departementet foreslår følgende regulering av Etterretningstjenestens plikt til å utpeke en eller flere personvernrådgivere:

§ 9-12 *Personvernrådgiver*

Etterretningstjenesten skal i egen organisasjon ha minst én personvernrådgiver som skal bidra til etterlevelse av bestemmelsene i kapittelet her gjennom opplæring, rådgivning, veiledning og internkontroll.

Sjefen for Etterretningstjenesten skal sikre at personvernrådgiveren involveres i spørsmål som gjelder vern av personopplysninger.

Enhver i Etterretningstjenesten kan kontakte personvernrådgiveren om spørsmål relatert til behandling av personopplysninger eller for å rapportere om brudd og avvik knyttet til behandling av personopplysninger.

13 Nasjonal og internasjonal informasjonsdeling mv.

13.1 Behovet for nasjonalt og internasjonalt samarbeid

Et godt nasjonalt og internasjonalt etterretningssamarbeid er viktig for norsk sikkerhet og nødvendig for at Etterretningstjenesten skal kunne løse sitt samfunnsoppdrag på en adekvat og effektiv måte.

Det er en fast og langvarig tradisjon for at etterretningstjenester samarbeider med hverandre. *Internasjonalt* samarbeid er nødvendig for at Etterretningstjenesten skal få en bredest mulig forståelse av trusselbildet, trender og utviklingstrekk som er av felles interesse med den samarbeidende aktøren. Dette bidrar blant annet til at konkrete trusler mot Norge kan håndteres på bakgrunn av mer sammensatte etterretningsanalyser, hvor informasjonsbiter fra ulike hold er vurdert, satt i sammenheng og verifisert opp mot hverandre. Det er av avgjørende betydning for et relativt lite land som Norge å trekke fordeler ved et internasjonalt etterretningspartnerskap. Et godt samarbeid fordrer et

tillitsforhold som bygger på etablert produktivt samarbeid over tid og fravær av motstridende interesser, selv om man kan ha ulike prioriteringer eller oppgaver å ivareta. Videre kreves at samarbeidspartnerne er villige til å dele informasjon med hverandre. I noen sammenhenger kan samarbeid i form av informasjonsdeling, herunder deling av kunnskap og analyse, ha multipliserende effekt i form av en samlet og forbedret felles etterretningsproduksjon og situasjonsforståelse.

På enkelte områder foreligger det etter internasjonale rettsregler i tillegg en *plikt* til å dele informasjon. Det gjelder for eksempel i kampen mot internasjonal terrorisme, jf. en rekke kontraterrorkonvensjoner[371] og noen folkerettslig bindende sikkerhetsrådsresolusjoner, blant annet UNSCR 2178 (2014) og 2249 (2015).[372]

En god håndtering av grenseoverskridende trusler krever tett samarbeid og utstrakt informasjonsdeling mellom Etterretningstjenesten og andre *norske* offentlige myndigheter. Det er derfor behov for gode og effektive samarbeidsmekanismer på det nasjonale plan. Særlig, men ikke utelukkende, gjelder dette for samarbeidet mellom Etterretningstjenesten og Politiets sikkerhetstjeneste (PST). PST er landets innenlandske etterretnings- og sikkerhetstjeneste, hvis informasjonsbehov overlapper med Etterretningstjenestens på enkelte områder. Trygghet i Norge er avhengig av god etterretning i utlandet, og god etterretning i utlandet er avhengig av god etterretning i Norge. Særlig gjelder det ved grenseoverskridende trusler, hvor Etterretningstjenesten og PST bør ha en sømløs informasjonsdeling for å håndtere trusler som vedkommende tjeneste har ansvar for å følge. Hensynet til grunnleggende nasjonale sikkerhetsinteresser tilsier at det i samvirket mellom nasjonale myndigheter bør være færre rettslige hindre for informasjonsdeling.

Et siste viktig poeng er at deling mellom nasjonale myndigheter og samarbeid i form av koordinering av eksterne relasjoner kan være nødvendig for å sikre nasjonal informasjonskontroll, og på den måten unngå at utenlandske tjenester og aktører spiller den ene nasjonale myndigheten ut mot den andre.

Nasjonalt og internasjonalt samarbeid reiser særlige rettslige problemstillinger knyttet spesielt til forholdet mellom informasjonsdeling og den enkeltes personvern og rettssikkerhet. Etterretningstjenestens informasjonsdeling er et prioritert kontrollområde for EOS-utvalget.

Departementet vil i kapittelet her gjennomgå hvordan behovet for nasjonalt og internasjonalt samarbeid søkes dekket og regulert etter gjeldende rett. Departementet vil deretter vurdere hvilke utfordringer som gjør seg gjeldende ved dagens regulering, og på denne bakgrunn foreslå tilpassede bestemmelser som balanserer de ulike hensyn som gjør seg gjeldende.

---

[371] Siden 1963 har FN utarbeidet 19 kontraterrorkonvensjoner. Mange av disse oppfordrer eller forplikter statene til å samarbeide om og dele informasjon relatert til de forbrytelser som konvensjonene omhandler (særlig relatert til terrorhandlinger mot sivil luftfart og internasjonal sjøfart, finansiering av terrorisme og nukleær terrorisme). Se en oversikt over konvensjonene på FNs kontor for kontraterror sin hjemmeside; http://www.un.org/en/counterterrorism/legal-instruments.shtml

[372] United Nations Security Council Resolutions, *Threats to international peace and security caused by terrorist acts*, S/RES/2178 (2014) og S/RES/2249 (2015)

13.2 Samarbeidenes karakter og omfang

13.2.1 Gjeldende rett og eksisterende samarbeidsmekanismer

13.2.1.1 Samarbeid mellom Etterretningstjenesten og PST[373]

Viktigheten av samarbeidet mellom Etterretningstjenesten og PST er understreket også i forarbeidene til gjeldende etterretningstjenestelov.[374] Her fremheves det at det er av avgjørende betydning for en effektiv etterretnings, - overvåkings- og sikkerhetstjeneste at det på alle plan er et nært og tillitsfullt samarbeid mellom organene som har ansvaret for disse tjenestene. Videre er behovet for et mer aktivt samarbeid mellom de to tjenestene understreket flere ganger de senere år, blant annet i 22. juli-kommisjonens rapport.[375]

Etterretningstjenestens oppdrag følger av gjeldende lov om Etterretningstjenesten med tilhørende instruks, og er i korte trekk å *innhente* relevant informasjon om *utenlandske* forhold, herunder avdekke og avverge trusler mot rikets sikkerhet, som er nødvendig for at norske myndigheter skal kunne treffe gode beslutninger knyttet til ivaretakelsen av viktige nasjonale interesser. PSTs oppgavesett følger av politiloven §§ 17 b og c. Kort fortalt har PST som oppgave og ansvar å *forebygge og etterforske* straffbare handlinger mot rikets sikkerhet.

Etterretningstjenesten og PST er sammenlignbare i den forstand at de begge kan benytte *fordekte metoder* for å innhente informasjon som er relevant for utførelsen av deres respektive oppgavesett. For øvrig er tjenestene grunnleggende forskjellige hvis man ser på den *samfunnsmessige funksjonen* de er satt til å ivareta, noe som igjen er avgjørende for hvilke formål tjenestene kan innhente informasjon om, og hvordan den informasjonen de besitter kan behandles. Av særlig viktighet er det at Etterretningstjenesten, i motsetning til PST, ikke er et rettshåndhevende organ med oppgave å forebygge og bekjempe kriminalitet. Etterretningstjenesten er følgelig ikke satt til å innhente informasjon med et etterforskningsformål eller med formål å samle inn bevis i straffesaker. Videre følger det av etterretningstjenesteloven § 4 at tjenesten ikke på norsk territorium kan overvåke eller på annen fordekt måte innhente informasjon om norske fysiske eller juridiske personer. Bestemmelsen er inntatt i loven blant annet for å angi at tjenestens virksomhet skal være rettet mot forhold som ligger *utenfor* norsk territorium. Se kapittel 8 for en nærmere redegjørelse.

Etterretningstjenesten og PST samarbeider innenfor rammen av sine respektive rettsgrunnlag.[376] Samarbeidet mellom Etterretningstjenesten og PST er særlig regulert i det som kalles samarbeidsinstruksen.[377] Utfyllende rutiner for samarbeidet er fastsatt av tjenestesjefene i 2009. Samarbeidsinstruksen har blant annet som formål å fremme samarbeidet mellom tjenestene på områder av felles interesse og å bidra til at tjenestene

[373] Grensedragningen mellom Etterretningstjenesten og PST er beskrevet i høringsnotatet punkt 8.2 og 8.8.

[374] Ot prp nr 50 (1996-97) s. 10, sp. 1.

[375] Se f.eks. NOU 2012: 14 *Rapport fra 22. juli-kommisjonen* s. 393-395

[376] Når Etterretningstjenesten bistår politiet etter politiloven § 27 a opererer de på politiets rettsgrunnlag, se nærmere om dette i punkt 13.5.

[377] Kongelig resolusjon 13. oktober 2006 nr. 1151 om instruks om samarbeidet mellom Etterretningstjenesten og Politiets sikkerhetstjeneste

med deres samlede ressurser og gjennom informasjonsutveksling, samhandling og arbeidsdeling skal kunne møte aktuelle trusler og sikkerhetsutfordringer. De prioriterte områdene for gjensidig informasjonsutveksling og annet samarbeid er terrorisme, spredning av masseødeleggelsesvåpen, fremmed etterretningsvirksomhet og andre prioriterte forhold som berører viktige norske interesser, jf. samarbeidsinstruksen § 3. Bestemmelsen speiler behovet for etterretning på de såkalte kontraområdene (kontraterror, kontraspredning og kontraetterretning). Videre tar instruksen hensyn til at Etterretningstjenestens og PSTs prioriterte områder endrer seg i takt med trussel- og aktørbildet, og er tilnærmet sammenfallende på enkelte områder. Det er for eksempel illustrerende at tjenestenes felles oppmerksomhet var rettet mot andre nasjoners etterretningsvirksomhet i Norge under den kalde krigen. I kjølvannet av terrorangrepet i USA 11. september 2001 ble fokuset på terrorbekjempelse dimensjonerende for etterretningsvirksomhet i et globalt perspektiv, og dette fikk også konsekvenser nasjonalt, blant annet gjennom et økt samarbeid. I dag er fokuset også tilbake på andre lands etterretningsvirksomhet mot Norge og norske interesser.

Videre skal tjenestene så langt mulig bistå hverandre i konkrete saker gjennom informasjonsinnhenting, utveksling av informasjon og vurderinger av felles interesse, analysebistand eller ved annen støttevirksomhet, herunder ved utlån av utstyr eller annen teknisk bistand, jf. samarbeidsinstruksen § 7. Denne formen for bistand må ikke forveksles med bistand etter politiloven § 27 a.

13.2.1.2 Særlig om Felles kontraterrorsenter

Både Etterretningstjenesten og PST har et ansvar for å hindre at Norge og norske interesser rammes av terror gjennom å bidra til å dekke relevante myndigheters informasjonsbehov. Felles kontraterrorsenter (FKTS) ble opprettet i 2014 for å sikre et effektivt samarbeid innen de to tjenestenes tilstøtende oppgaver knyttet til kontraterror, med vekt på grenseoverskridende trusler. Rammene for FKTS' virksomhet og organisering følger av samarbeidsinstruksen § 9. FKTS er et permanent senter med representasjon fra tjenestenes relevante fagmiljøer. Ansvaret for eget personell og kapasiteter tilligger hver enkelt tjeneste, og de ansatte utfører oppgavene – her som under samarbeid mellom tjenestene for øvrig – innenfor sine respektive rettsgrunnlag. Senteret har ikke egne operative oppgaver eller operasjonelle kapasiteter, men bidrar til at tjenestene kan oppnå mer effekt gjennom økt samhandling og bedre koordinering. FKTS bidrar til ivaretakelsen av rettidig og relevant informasjonsutveksling, koordinering og tilrettelegging av et effektivt operativt samarbeid mellom tjenestene samt ved utarbeidelse av felles trusselanalyser knyttet til terrorisme rettet mot Norge og norske interesser. Gjennom senteret blir tjenestene i stand til å danne seg et helhetlig bilde av terrortrusselen der denne har både internasjonale og nasjonale dimensjoner som må ses i sammenheng for å gi adekvat situasjonsforståelse og størst mulig avvergingsrom.

13.2.1.3 Særlig om Felles cyberkoordineringssenter

Etterretningstjenesten inngår som en fast part i Felles cyberkoordineringssenter (FCKS), som ble etablert i 2017.[378] Øvrige faste parter er Nasjonal sikkerhetsmyndighet (NSM), PST og Kripos. FCKS skal styrke den nasjonale evnen til effektivt forsvar mot og håndtering av

[378] Oppdraget om å etablere senteret ble formalisert i brev 18. september 2016 fra Justis- og beredskapsdepartementet, omforent med Forsvarsdepartementet. Samarbeidet mellom partene i senteret er nærmere beskrevet i «Retningslinjer for cybersamarbeid» inngått mellom partenes sjefer 20. mars 2017. Retningslinjene er offentlig tilgjengelige.

alvorlige hendelser i det digitale rom, og bidra til mer koordinert bruk av nasjonale ressurser, styrke informasjonsdelingen, legge forholdene til rette for mer effektiv og rettidig hendelseshåndtering, samt ivareta koordinert varsling til og frembringelse av helhetlige beslutningsgrunnlag for overordnede myndigheter. FCKS er et permanent og samlokalisert fagmiljø, bestående av faste representanter fra hver av senterets parter. Hver av partene opererer innenfor rammen av sine respektive rettsgrunnlag, og senteret endrer ikke på ansvarsgrensene mellom partene eller mellom partene og andre myndighetsaktører.

13.2.1.4 Annet nasjonalt samarbeid

Etterretningstjenesten samarbeider også med en rekke andre nasjonale myndigheter og virksomheter, primært begrunnet i fem noe ulike forhold:

1. Etterretningstjenesten innhenter aldri informasjon for sin egen del. En rekke offentlige virksomheter er *oppdragsgivere* for tjenesten, dette reflekteres i Forsvarsdepartementets årlige dokument om prioriterte nasjonale etterretningsbehov eller oppdukkende informasjonsbehov. Et viktig element i dette er *oppdragsdialogen* med oppdragsgiverne, blant annet for å klarlegge oppdragsgivers informasjonsbehov og på hvilken måte informasjonsbehovet skal møtes. Oppdragsdialogen har elementer av samarbeid i seg.
2. Etterretningstjenesten samarbeider med andre avdelinger i Forsvaret, i kraft av tjenestens fagmyndighet for all etterretningsvirksomhet i Forsvaret og i kraft av oppdraget om å understøtte militære operasjoner ute og hjemme.
3. På saksavgrensede områder samarbeider tjenesten regelmessig med andre offentlige myndigheter, eksempelvis med Tolletaten i eksportkontrollsaker (spredningssaker).
4. Etterretningstjenesten har etter E-instruksen § 11 adgang til å drive et sikkerhetsmessig og saklig avgrenset samarbeid med private virksomheter i form av varsling og rådgivning i forebyggende øyemed om forhold som faller innenfor tjenestens oppgaver. Nærmere retningslinjer er gitt av Forsvarsdepartementet.
5. Ad hoc-samarbeid i konkrete saker og operasjoner.

13.2.1.5 Internasjonalt samarbeid

Grenseoverskridende trusler og sammenfallende interesser medfører behov for å dele informasjon etterretningstjenester imellom. En etterretningstjeneste kan vanskelig dimensjoneres for å kunne innhente enhver relevant etterretning. Følgelig er tjenestene tjent med å understøtte hverandre.

Etterretningstjenesten har alltid samarbeidet med viktige allierte og med NATO. Internasjonalt etterretningssamarbeid er omtalt nærmere i punkt 7.8, se også lovutkastet § 3-4. Etterretningssamarbeidet er bi- og multilateralt og er av ulik karakter og omfang. Noe samarbeid bærer preg av å være løpende, for eksempel innenfor internasjonal terrorisme, mens annet samarbeid er mer hendelsespreget. Nærmere detaljer om hvilke tjenester Etterretningstjenesten samarbeider med og hva det samarbeides om, kan ikke redegjøres for i et offentlig dokument.

13.2.2 Departementets vurdering

Departementet vurderer at det bør fremgå i lovforslaget at nasjonalt og internasjonalt samarbeid kan finne sted, og at dette særlig kan skje gjennom informasjonsutveksling og felles operasjoner. Dette er en videreføring av gjeldende rett. Tilsvarende vurderer departementet det som formålstjenlig at lovforslaget også trekker opp en overordnet ramme for *nasjonalt* samarbeid. I tillegg foreslås det å presisere uttrykkelig at utlevering av

informasjon som ledd i et slikt samarbeid bare kan skje dersom nærmere angitte vilkår, vilkårene i §§ 10-5 eller 10-8, er oppfylt, se nærmere om dette nedenfor.

Bestemmelsen i lovforslaget § 3-4 om *internasjonalt* etterretningssamarbeid er en bestemmelse som hjemler *innhenting* av informasjon som antas å være av vesentlig betydning for samarbeid, når dette anses å være i norsk interesse. Det anses i tillegg hensiktsmessig å videreføre dagens hjemmel i etterretningstjenesteloven § 3 annet ledd om at Etterretningstjenesten kan *etablere og opprettholde* et internasjonalt etterretningssamarbeid. Gjeldende lov § 3 annet ledd omtaler kun etterretningssamarbeid med «andre land». I praksis er bestemmelsen tolket til også å hjemle etterretningssamarbeid med forsvarsallianser som Norge deltar i. Særlig fremtredende er det langvarige etterretningssamarbeidet i NATO, og andre relevante organisasjoner. Tolkningen er også innarbeidet i E-instruksen § 7 tredje ledd. Det kan i den forbindelse bemerkes som et eksempel at FN nylig har vedtatt at visse former for etterretning kan inkluderes i internasjonale operasjoner under FNs mandat og kommando. For at Etterretningstjenesten skal kunne etablere nye samarbeid og avtaler på dette området kreves departementets godkjenning, se lovforslaget § 2-7 bokstav a. Departementet mener denne foreleggelsesplikten bør videreføres, og mener av pedagogiske hensyn det er hensiktsmessig å henvise til denne.

Departementet mener også at det bør fremgå klart i lovs form at Etterretningstjenesten kan samarbeide med andre norske offentlige myndigheter. Selv om dette fremgår i relasjon til PST i dag, mener departementet loven bør gi en generell hjemmel for slikt samarbeid. Hva samarbeidet kan omfatte, herunder de krav som stilles til deling av informasjon, vil følge av de særskilte lovbestemmelser.

Departementet foreslår etter dette følgende lovbestemmelse om nasjonalt samarbeid:

§ 10-1 *Nasjonalt samarbeid*
Etterretningstjenesten kan samarbeide med andre norske offentlige myndigheter, herunder gjennom informasjonsutveksling og felles operasjoner.
Etterretningstjenesten skal samarbeide med andre norske offentlige myndigheter om grenseoverskridende trusler, forsvar mot og håndtering av alvorlige hendelser i det digitale rom, samt andre prioriterte saksfelt.
Etterretningstjenesten kan bare utlevere informasjon til norske offentlige myndigheter dersom vilkårene i §§ 10-5 eller 10-8 er oppfylt.

Departementet foreslår følgende regulering av internasjonal samarbeid:

§ 10-4 *Internasjonalt etterretningssamarbeid*
Etterretningstjenesten skal etablere og opprettholde bi- og multilateralt etterretningssamarbeid med andre land, forsvarsallianser som Norge deltar i og andre relevante internasjonale organisasjoner. Departementets beslutning skal innhentes i saker som nevnt i § 2-7.

13.3Utlevering av informasjon

13.3.1 Innledning

Utlevering av personopplysninger til en tredjepart vil ofte være et nytt menneskerettslig inngrep overfor den personen som informasjonen gjelder, fordi flere personer og instanser vil få innsyn i opplysningene. Det kreves derfor at utleveringsadgangen har tilstrekkelig forankring i lov. De gjeldende reglene for utlevering av informasjon til andre myndigheter i

Norge kan utledes både av nasjonal lovgivning, etablerte rettsprinsipper og Etterretningstjenestens interne instrukser og retningslinjer.

Departementet har vurdert om det skal gjøres endringer i hvilke *vilkår* som bør gjelde for at utlevering skal kunne finne sted, hvilke *prosedyrer* som bør gjelde ved utlevering, og hvem som skal tillegges *beslutningskompetanse*. Departementet har også vurdert hvilke reguleringer som bør lovfestes, og hva som bør følge av interne reguleringer.

Departementet vil presisere at man i etterretningssamarbeid gjerne snakker om «deling» av informasjon. Begrepet brukes ulike steder i høringsnotatet. I rettslige termer er det imidlertid mer presist å bruke begrepet «utlevering» av informasjon, og dette anvendes i lovforslaget og omtalen under.

13.3.2 Gjeldende rett

13.3.2.1 Generelle regler og prinsipper for utlevering til nasjonale myndigheter mv.
Etterretningstjenesten innhenter informasjon *til bruk for oppdragsgiverne*. Dette innebærer at informasjonen som tjenesten innhenter for dette formålet kan videreformidles til oppdragsgivernes kunnskap. Etterretningstjenesten kan også utlevere *overskuddsinformasjon*[379] til «rette norske offentlige myndighet», jf. E-instruksen § 5 første ledd. Utlevering av overskuddsinformasjon er særlig omtalt i punkt 13.3.5 nedenfor.

Et rettslig utgangspunkt er at utlevering av informasjon kan skje så lenge folkerettslige eller nasjonalrettslige regler ikke er til hinder for det. Folkerettslig kan utlevering i enkelte tilfeller anses som et uforholdsmessig inngrep, jf. EMK artikkel 8, i den utstrekning det dreier seg om utlevering av personopplysninger. Nasjonalrettslig kan f. eks. lovbestemt taushetsplikt hindre utlevering. Innenfor disse rammene er det gjennom instrukser fra overordnet myndighet, og praksis knyttet til enkeltsaker, etablert ytterligere vilkår som må hensyntas. Et eksempel på dette er at det forutsettes at utlevering av informasjon bare kan skje dersom dette kan bidra til løsningen av enten avgiverorganets eller mottakerorganets samfunnsoppdrag.

Lovbestemt taushetsplikt vil i utgangspunktet ikke hindre utlevering av informasjon fra Etterretningstjenesten til andre offentlige myndigheter, forutsatt at mottakerne har et behov for å motta informasjonen («need to know») og har de nødvendige sikkerhetsklareringer og autorisasjoner til det. Utlevering skal imidlertid ikke gjennomføres på en måte som uforsvarlig eksponerer beskyttede kilder, metoder og kapasiteter.[380]

Etterretningstjenesten kan selvsagt ikke utlevere informasjon *med sikte på* at mottaker skal innhente informasjon i tjenestens interesse, i tilfeller hvor tjenesten selv lovlig ikke kunne ha innhentet informasjonen. Dette ville være en omgåelse av lovbestemte forbud som gjelder for Etterretningstjenesten, og vil normalt også være lovstridig for mottakeren. Derimot vil tjenesten kunne utlevere informasjon til en nasjonal mottaker for at denne i *egen* interesse og på selvstendig grunnlag kan vurdere innhenting eller tilsvarende tiltak. Dette vil ikke være en omgåelse, selv om mottakeren skulle gjennomføre tiltaket og informasjon derfra skulle bli delt med tjenesten i etterkant.

[379] Overskuddsinformasjon er informasjon som er uten selvstendig interesse for etterretningsformål men som tjenesten likevel kommer i besittelse av gjennom utførelsen av sine oppgaver.

[380] Taushetsplikten omtales nærmere i høringsnotatet punkt 14.3 og 14.4

Videre gjelder et *informasjonseierskapsprinsipp* som vil si at Etterretningstjenesten eier informasjonen den har innhentet. Dette innebærer at Etterretningstjenesten kan oppstille vilkår for mottakeren dersom informasjonen utleveres. Et slikt vilkår vil alltid være at mottakeren ikke kan dele opplysningen videre med tredjeparter, uten at Etterretningstjenesten på forhånd har samtykket til det. Det samme gjelder dersom opplysningene skal brukes til andre formål enn forutsatt. Eksempelvis kan informasjon som Etterretningstjenesten har delt med PST ikke inngå i «sakens dokumenter»[381] i en senere etterforskningssak, dersom Etterretningstjenesten ikke har gitt (nytt) samtykke til det.

En variant av informasjonseierskapsprinsippet er det såkalte *tredjepartsprinsippet*. Dette innebærer at Etterretningstjenesten ikke kan utlevere opplysninger som den har mottatt fra en tredjepart uten samtykke fra den opprinnelige informasjonseieren. Prinsippet er blant annet nedfelt i samarbeidsinstruksen mellom Etterretningstjenesten og PST § 10 annet ledd, som lyder:

> Informasjon utlevert fra den ene tjenesten til den andre tjenesten kan ikke gis videre til tredjepart uten at utleverende tjeneste på forhånd har samtykket til det.

I samarbeidet mellom Etterretningstjenesten og PST gjelder det imidlertid noen unntak fra tredjepartsprinsippet. For det første er det underforstått at verken PST eller Etterretningstjenesten er «tredjepart» dersom en utenlandsk etterretnings- eller sikkerhetstjeneste deler informasjon med den ene tjenesten, med mindre noe annet er bestemt av vedkommende utenlandske tjeneste. For det andre anses ikke nasjonale kontrollmyndigheter (altså EOS-utvalget i norsk kontekst) som «tredjepart» i denne sammenheng. Tredjepartsprinsippet kan derfor aldri påberopes for å unnlate å gi EOS-utvalget tilgang til informasjon.

For øvrig gjelder det såkalte *«buyer beware»-prinsippet*. Dette innebærer at det er den instans som etterspør eller mottar informasjon som har ansvaret for å vurdere om ens eget rettsgrunnlag tillater å etterspørre informasjonen og behandle mottatt informasjon. Utleverende instans har derimot ansvaret for å vurdere om eget rettsgrunnlag tillater utlevering.

Etterretningstjenesten er videre forpliktet etter menneskerettighetene til å foreta en konkret vurdering av om utlevering av personopplysninger vil være nødvendig og forholdsmessig i det enkelte tilfellet. Dette fordrer at mottakeren synliggjør hvorfor den trenger opplysningene og hva informasjonen skal brukes til. Dersom Etterretningstjenesten deler rådata, det vil si informasjon som ikke er evaluert for etterretningsverdi, skal tjenesten ha en begrunnet formening om hva slags type data dette dreier seg om og hvor dataene stammer fra.

13.3.2.2 Regler og prinsipper for utlevering til utenlandske samarbeidspartnere

Enkelte av de samme prinsipper som gjelder for utlevering av informasjon nasjonalt gjelder ved utlevering av informasjon som ledd i internasjonalt etterretningssamarbeid, herunder kravet om at utleveringen av opplysninger må ha et legitimt formål. I tillegg gjelder at utlevering internasjonalt må være knyttet til Etterretningstjenestens lovbestemte oppgaver og være i norsk interesse. Utleveringen må med andre ord skje for etterretningsformål. I tillegg gjelder det noen ytterligere regler og grunnprinsipper. Disse kan utledes både av folkerettslige prinsipper, nasjonal lovgivning, utfyllende bestemmelser og internt regelverk. Etterretningstjenesten har interne instrukser og retningslinjer som oppstiller nærmere

[381] Jf. straffeprosessloven §§ 242, 264 og 267

praktiske prosedyrer for utlevering. Rettsreglene gjelder uavhengig av jurisdiksjon og uavhengig av om det deles personopplysninger om norske eller ikke-norske personer.

Eksempler på nasjonalt regelverk er taushetspliktbestemmelser og Forsvarsdepartementets utfyllende bestemmelser av 24. juni 2013 for Etterretningstjenestens innsamling mot norske personer i utlandet samt for utlevering av personopplysninger til utenlandske samarbeidende tjenester. Videre har informasjonssikkerhetsforskriften,[382] bestemmelser om utlevering av sikkerhetsgradert informasjon til fremmede stater og internasjonale organisasjoner, jf. § 3-2. I utgangspunktet kreves det inngåelse av sikkerhetsavtale med vedkommende land eller internasjonale organisasjon, men innen forsvars- og justissektoren kan det likevel gjøres unntak dersom det ikke er praktisk mulig å inngå slik avtale og det er i Norges interesse å utlevere informasjonen. Unntaket er tidvis aktuelt for Etterretningstjenestens internasjonale samarbeid, særlig ved konkrete hendelser.

Et annet sentralt regelsett følger av personopplysningsloven 2000 kapittel V, som fastslår bestemmelser om overføring av personopplysninger til utlandet. Hovedregelen følger av lovens § 29, som fastslår at personopplysninger bare kan overføres til stater som sikrer en forsvarlig behandling av opplysningene. Lovens § 30 oppstiller enkelte unntak fra dette forsvarlighetskravet, herunder dersom overføringen av personopplysninger er «nødvendig eller følger av lov for å beskytte en viktig samfunnsinteresse». Dette unntaket er særlig aktuelt for Etterretningstjenesten.

Utleveringen må skje *i norsk interesse* og være underlagt *nasjonal kontroll*. Dette følger i dag av E-instruksen § 4 første ledd annet punktum. At utlevering av informasjon til utenlandske stater eller internasjonale organisasjoner skal være under nasjonal kontroll, skal etter lang tids tolkningspraksis ikke forstås som et krav om at hvert eneste databruddstykke som overføres først skal være analysert og vurdert av Etterretningstjenesten. Særlig gjelder det mengdeinformasjon (bulk) innhentet ved tekniske innsamlingsmetoder. Et slikt krav er vurdert å gå vesentlig lenger enn formålet med bestemmelsen. Det vil i slike tilfeller være tilstrekkelig at man har foretatt en vurdering som er tilstrekkelig til å avgjøre hva slags *type* data det er tale om og hvor de stammer fra, slik at man i ettertid kan redegjøre for *karakteren* av de opplysninger som ble utlevert.

Videre kan ikke utlevering under noen omstendighet skje dersom det ut fra de konkrete omstendigheter er en reell risiko for at utleveringen vil lede til at personer blir utsatt for brudd på såkalte *jus cogens*-regler – det vil si menneskerettslige regler som aldri kan fravikes ved nasjonal lov. Dette er nærmere konkretisert i instruks om etterretningssamarbeid med stater hvor det foreligger risiko for tortur eller annen grusom, umenneskelig eller nedverdigende behandling eller straff.[383] Utlevering kan heller ikke skje dersom det ut fra de konkrete omstendigheter er en reell risiko for å bidra til andre former for folkerettsbrudd, herunder brudd på krigens folkerett. Det samme gjelder dersom formålet er at mottakeren skal treffe innhentingstiltak på bakgrunn av informasjonen *på vegne av* Etterretningstjenesten, med mindre Etterretningstjenesten selv kunne ha gjennomført tiltaket innenfor rammen av eget

[382] Fastsatt av Forsvarsdepartementet 1. juli 2001 i medhold av sikkerhetsloven av 1998. Det tas sikte på å videreføre prinsippet i gjeldende forskrift i nye forskrifter til den nye sikkerhetsloven av 2018.

[383] Instruks fastsatt av Sjefen for Etterretningstjenesten av 26. november 2012 om etterretningssamarbeid med stater hvor det foreligger risiko for tortur eller annen grusom, umenneskelig eller nedverdigende behandling eller straff, se https://forsvaret.no/fakta_/ForsvaretDocuments/Instruks%20om%20etterretningssamarbeid.pdf

rettsgrunnlag. Dette vil som redegjort for tidligere være en omgåelse. Har ikke Etterretningstjenesten selv et rettslig grunnlag for å innhente informasjonen, kan tjenesten heller ikke be andre om å gjøre det.

13.3.3 Departementets vurdering

13.3.3.1 Generelle regler (lovutkastet § 10-5)

Departementet vurderer at gjeldende prinsipper og bestemmelser for utlevering av informasjon på en god måte balanserer hensynet til effektivt samarbeid opp mot hensyn av personvern- og menneskerettslig karakter. Departementet anbefaler derfor at gjeldende praksis videreføres, men at utleveringsadgangen bør fremgå tydelig av ny etterretningstjenestelov. Bestemmelsene bør samles og inntas i et eget kapittel. En slik samlet lovfesting av vilkårene for informasjonsutlevering vil sikre bedre forutberegnelighet og klargjøre rettstilstanden sett i forhold til dagens fragmentariske regelsituasjon. Dette vil i seg selv kunne ha positive rettssikkerhetsmessige konsekvenser og legge bedre til rette for EOS-utvalgets legalitetskontroll.

Det bør av samme grunn være et lovbestemt krav at all utlevering skal skje med notoritet for å sikre sporbarhet. Av kontrollhensyn er det sentralt at EOS-utvalget konkret kan kontrollere hvilke opplysninger som er delt, og med hvem.

Gitt at utgangspunktet for utleveringsadgangen er de samme i både nasjonalt og internasjonalt etterretningssamarbeid mener departementet at *grunnvilkåret* kan formuleres likt for begge samarbeidsformer. I tillegg mener departementet det bør gjelde enkelte særregler for utlevering til internasjonale partnere. Dette foreslås regulert i en egen bestemmelse (lovutkastet § 10-6).

Vurdering av om vilkårene foreligger må gjøres konkret for hver enkelt sak eller gruppe av like saker. For den forholdsmessighetsvurdering som skal foretas, foreslår departementet å vise til lovforslagets generelle forholdsmessighetsregel, som etter sin ordlyd også foreslås å gjelde for «utlevering av informasjon», se forslaget til § 5-4.

Departementet foreslår etter dette følgende *generelle vilkår* for utlevering av informasjon fra Etterretningstjenesten som ledd i nasjonalt eller internasjonalt samarbeid:

§ 10-5 *Utlevering av etterretningsinformasjon som ledd i nasjonalt eller internasjonalt samarbeid*

Etterretningstjenesten kan utlevere etterretningsinformasjon dersom følgende kumulative vilkår er oppfylt:

a. Utleveringen skjer for etterretningsformål eller er nødvendig for å fremme mottakerens oppgaver eller for å hindre at virksomhet blir utøvd på en uforsvarlig måte.
b. Utlevering av informasjon som Etterretningstjenesten har mottatt fra en tredjepart skjer med dennes samtykke.
c. Utlevering av personopplysninger bare skjer dersom Etterretningstjenesten kan behandle opplysningene etter kapittel 9 og utleveringen vurderes å være forholdsmessig etter § 5-4.
d. Utleveringen vurderes som forsvarlig i lys av opplysningenes kvalitet, hvem som er mottaker av opplysningene og hvordan mottaker antas å bruke dem.
e. Utleverte opplysninger forventes å bli forsvarlig sikkerhetsmessig behandlet hos mottaker.
f. Utleveringen skjer med notoritet.

Utlevering med sikte på innhenting eller andre tiltak hos mottaker på vegne av og i Etterretningstjenestens interesse, kan bare skje dersom Etterretningstjenesten selv lovlig kunne ha gjennomført innhentingen eller tiltaket.

Paragrafen her gjelder ikke for utlevering av informasjon til EOS-utvalget og andre tilsyns- og kontrollinstanser.

13.3.3.2 Særregler om utlevering til utenlandske partnere

Departementet mener at det bør lovfestes enkelte tilleggsvilkår for utlevering av informasjon som ledd i internasjonalt samarbeid.

Dagens praksis for utlevering av informasjon til internasjonale samarbeidspartnere bygger på prinsipper utledet fra personopplysningsretten og menneskerettighetene. Departementet vurderer at det er gjort en hensiktsmessig avveining mellom de ulike hensyn knyttet til utlevering, og mener derfor denne praksisen kan videreføres, nå i lovs form.

Departementet foreslår å kodifisere gjeldende utleveringspraksis i internasjonalt samarbeid med en egen særregel:

§ 10-6 *Tilleggsvilkår for utlevering av etterretningsinformasjon som ledd i internasjonalt samarbeid*
Ved utlevering til tjenester eller myndigheter i andre stater eller til internasjonale organisasjoner skal, i tillegg til vilkårene i § 10-5, følgende kumulative vilkår være oppfylt:

a. Utleveringen er under nasjonal kontroll og vurderes å være i norsk interesse.
b. Det oppstilles vilkår om at opplysningene ikke kan benyttes som grunnlag for innhenting rettet mot personer som oppholder seg på norsk territorium, med mindre det dreier seg om en person som omfattes av § 4-2 første ledd og som det er i norsk interesse at mottakeren gjennomfører innhenting mot.
c. Utleveringen skjer i overensstemmelse med særskilte prosessuelle og materielle bestemmelser som skal sikre overholdelse av forbudet i § 1-3 annet ledd.

13.3.4 Videreformidling av opplysninger på vegne av andre norske offentlige myndigheter

Etterretningstjenesten har i enkelte situasjoner bedre forutsetninger enn andre for å være en ren *formidler* av informasjon til utenlandske tjenester og myndigheter, for eksempel som følge av at Etterretningstjenesten har et etablert sikkert samband som kan benyttes for dette formål.

Etter gjeldende internt regelverk vil tjenestens utøvelse av denne «postkassefunksjonen» ikke kreve en konkret vurdering av om utlevering kan finne sted. Opplysningene anses i disse situasjonene ikke for å være «utlevert» av tjenesten, men av den andre norske myndigheten som ønsker at tjenesten skal være behjelpelig med å få gjennomført *denne myndighetens utlevering* til vedkommende lands tjeneste. Det er en klar forutsetning at det med notoritet fremgår at Etterretningstjenesten ikke er opphav til utleveringen og at tjenesten ellers ikke opptrer på en måte som tilsier at tjenesten har interesser i saken.

Departementet vurderer at praktiske og sikkerhetsmessige forhold tilsier en videreføring av gjeldende ordning, og foreslår dette lovfestet slik:

§ 10-7 *Videreformidling av opplysninger på vegne av andre norske offentlige myndigheter*
Etterretningstjenesten kan på vegne av annen norsk offentlig myndighet videreformidle opplysninger til og fra en utenlandsk samarbeidende tjeneste, når følgende kumulative vilkår er oppfylt:

a. Den norske myndigheten har anmodet Etterretningstjenesten om å formidle opplysningene.
b. Det fremstår klart for den samarbeidende tjenesten at videreformidlingen skjer på vegne av den norske myndigheten.
c. Etterretningstjenesten ikke endrer opplysningene, legger til egen informasjon eller ber mottaker om å handle på en bestemt måte i lys av opplysningene.
d. Det fremstår klart for den samarbeidende tjenesten at videreformidling til tredjepart krever samtykke fra den norske myndigheten eller at slikt samtykke allerede er gitt.
e. Formidlingen skjer med notoritet.

13.3.5 Særlig om utlevering av overskuddsinformasjon

13.3.5.1 Nærmere om overskuddsinformasjon

Overskuddsinformasjon er informasjon om forhold som ligger utenfor Etterretningstjenestens ansvarsområde, og som således er uten etterretningsverdi, men som tjenesten likevel kommer i besittelse av som følge av sin lovlige innhentingsaktivitet. Etter gjeldende rett kan overskuddsinformasjon fritt deles med «rette norske offentlige myndighet», jf. E-instruksen § 5 første ledd. I dette ligger en presumsjon om at opplysningene må ha relevans for denne norske offentlige myndighetens oppgaveløsning. Spørsmålet som vurderes i det følgende er om dagens adgang til å utlevere overskuddsinformasjon til rette norske myndighet bør videreføres.

Etterretningstjenesten kommer sjelden i besittelse av overskuddsinformasjon. Det skyldes at tjenestens innhenting, analyse og øvrige behandling av opplysninger utelukkende har fokus på løsningen av tjenestens egne oppgaver. I sjeldne unntakstilfeller kan likevel egeninnhentet materiale eller informasjon delt fra nasjonale eller internasjonale partnere frembringe overskuddsinformasjon, for eksempel opplysninger om at et etterretningsmål har begått en straffbar handling slik som for eksempel narkotikasmugling. Informasjon om slike handlinger har ikke nødvendigvis sammenheng med eller kontekstuell betydning for tjenestens oppgaveløsning. Det er derfor ikke nødvendig å behandle opplysningen for etterretningsformål. Normalt vil spørsmålet gjelde et forhold i utlandet som faller utenfor norsk strafferettsjurisdiksjon, eller den norske utlendingsforvaltningens eller andre norske myndigheters ansvarsområder, men dersom personen eksempelvis er norsk fremmedkriger i utlandet kan dette stille seg annerledes.

De mest praktiske eksemplene på utlevering av overskuddsinformasjon gjelder imidlertid informasjon mottatt fra andre lands etterretningstjenester om norske personer, som grunnet usikkerhet om norske myndigheters oppgavedeling, eller av andre grunner, formodentlig skulle vært utlevert direkte til PST eller til det ordinære politiet.

13.3.5.2 Departementets forslag

Departementet mener det er behov for å videreføre hovedregelen om at overskuddsinformasjon kan deles og at dette bør lovfestes med dertil tilhørende vilkår.

Departementet foreslår at begrepet overskuddsinformasjon legaldefineres slik i § 1-4 nr. 11:

> Overskuddsinformasjon; informasjon som er uten selvstendig interesse for etterretningsformål

Når det gjelder adgangen til å dele overskuddsinformasjon vurderer departementet at det bør gjelde et vilkår om at Etterretningstjenesten må finne utleveringen *nødvendig* for å fremme mottakerens oppgaver eller for å hindre at virksomhet blir utøvd på en uforsvarlig måte. Videre at utleveringen vurderes *forholdsmessig* etter lovforslaget § 5-4. Dessuten at utleveringen anses *forsvarlig* i lys av opplysningenes kvalitet, hvem som er mottaker og hvordan mottaker antas å bruke dem. Mottakere av opplysningene foreslås begrenset til norske offentlige myndigheter.

Lovfestingen vil på enkelte områder innebære en skjerpelse sammenlignet med dagens regulering. Innskjerpingen antas ikke å medføre ulemper eller andre negative konsekvenser verken for Etterretningstjenesten eller andre norske offentlige myndigheter, da de samme vilkårene langt på vei praktiseres av tjenesten allerede i dag.

Departementet foreslår enkelte unntak fra utgangspunktet om at overskuddsinformasjon kan deles. For det første gjelder dette overskuddsinformasjon som fremkommer gjennom

tilrettelagt innhenting etter lovforslagets kapittel 7, hvor departementet foreslår et delingsforbud.[384] Dette er i korte trekk begrunnet i at det kan tenkes at søk i grenseoverskridende elektronisk kommunikasjon i større grad vil frembringe overskuddsinformasjon enn ved bruk av andre aksesser. For det andre foreslår departementet at det bør gjelde et forbud mot deling av overskuddsinformasjon som er fortrolig kommunikasjon. Det redegjøres nærmere for hvilken kommunikasjon som etter forslaget skal regnes som *fortrolig* i punkt 12.10.

Forslaget til lovbestemmelse lyder:

§ 10-8 *Utlevering av overskuddsinformasjon*

Overskuddsinformasjon kan deles med norske offentlige myndigheter når vilkårene etter § 10-5 er oppfylt, med unntak av vilkåret om at Etterretningstjenesten kan behandle opplysningene etter kapittel 9.

Overskuddsinformasjon som fremkommer gjennom innhenting etter kapittel 7 reguleres av § 7-12.

Overskuddsinformasjon som er fortrolig kommunikasjon etter § 9-6 kan ikke utleveres.

13.4 Utlevering av informasjon fra norske offentlige myndigheter til Etterretningstjenesten

13.4.1 Gjeldende rett

13.4.1.1 Innledning

En rekke norske virksomheter besitter, eller er i posisjon til å komme i besittelse av, utenlandsetterretningsrelevant informasjon. Etterretningstjenesten er i stor grad avhengig av å motta denne informasjonen for å få utført oppgavene sine på en så effektiv og målrettet måte som mulig. Særlig gjelder det informasjon fra PST i relasjon til grenseoverskridende trusler, men det vil i varierende grad også gjelde en rekke andre offentlige myndigheter, og til dels også private virksomheter. Spørsmålet om utlevering av informasjon til Etterretningstjenesten reiser imidlertid noen sentrale problemstillinger, hvorpå avveiningen av *prinsippet om frivillig samarbeid med og mellom norske offentlige myndigheter* mot *lovbestemt taushetsplikt* er av særlig viktighet.

Problemstillingen må blant annet forstås i lys av økende grenseoverskridende trusler, hvilket også medfører større behov for at Etterretningstjenesten samhandler med innenlandske myndigheter. Internasjonalt er det en styrket erkjennelse av at informasjon må deles både over og innenfor landegrensene. I noen sammenhenger, særlig på kontraterrorområdet, har FNs sikkerhetsråd i bindende resolusjoner oppfordret statene om å dele opplysninger nasjonalt i større grad, som en forutsetning for å lykkes i kampen mot internasjonal terrorisme. I forenklede termer kan en si at prinsippet om «*need to share*» er på enkelte områder blitt viktigere enn «*need to know*».

Innledningsvis bør det nevnes at Etterretningstjenesten i utgangspunktet kan både motta og etterspørre informasjon fra andre så lenge dette er innenfor rammen av eget rettsgrunnlag. Dette følger av *«buyer beware»*-prinsippet, som nevnt over under punkt 13.2.1.2. Prinsippet innebærer at det er den instansen som etterspør eller mottar informasjon som har ansvaret for å vurdere om ens eget rettsgrunnlag tillater dette. Tilsvarende må den instansen som blir

[384] Se nærmere om dette i punkt 11.13.2

forespurt vurdere om den har hjemmel til å utlevere. Det er sistnevnte problemstilling som er tema i det følgende; altså hvilke gjeldende rettslige skranker utfordrer Etterretningstjenestens oppgaveløsning i dag, og videre; I hvilken grad etterretningsrelevante opplysninger som andre norske virksomheter besitter bør kunne utleveres til Etterretningstjenesten. Den røde tråden i avveiningen som må foretas, er om hensynet til rikets sikkerhet tilsier at hensynene bak de ulike lovbestemte taushetspliktene settes til side.

13.4.1.2 Nærmere om prinsippet om frivillig informasjonsdeling. Distinksjonen mellom aktiv innhenting og passivt mottak av opplysninger

Gjeldende etterretningstjenestelov forutsetter at innhenting av informasjon som angår forhold som gjelder utlandet og som omfattes av lovens formål og Etterretningstjenestens oppgaver, også kan skje gjennom *frivillig informasjonsdeling*.[385] Loven åpner dermed opp for at andre virksomheter kan samarbeide, herunder dele informasjon, dersom vedkommende virksomhet selv er villig til dette.

Departementet finner grunn til å presisere her at frivillig informasjonsdeling ikke faller inn under innhentingsforbudet i dagens etterretningstjenestelov § 4 første ledd, som fastslår at:[386]

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

For at innhenting skal kategoriseres som «fordekt» må Etterretningstjenesten *aktivt* innhente eller aktivt delta i innhenting av informasjon som ikke er offentlig tilgjengelig gjennom egne fordekte tiltak. Å motta eller etterspørre informasjon som andre besitter karakteriseres ikke som aktiv eller operativ egeninnhenting. Denne lovforståelsen er basert på hensynet bak bestemmelsen,[387] men kan også sies å følge direkte av etterretningstjenesteloven § 4 annet ledd for så vidt gjelder mottak av opplysninger om norske personer. Tilsvarende tolkning er lagt til grunn for deling av informasjon fra andre myndigheter enn PST. Forståelsen er også omtalt i kapittel 8 om den territorielle begrensningen for Etterretningstjenestens informasjonsinnhenting.[388]

At Etterretningstjenesten kan motta informasjon fra andre myndigheter gjelder imidlertid ikke uten begrensninger. Særlig gjelder at Etterretningstjenesten kun kan etterspørre informasjon som vurderes relevant for Etterretningstjenestens egen oppgaveløsning og som tjenesten selv kan behandle. Videre kan Etterretningstjenesten kun be andre offentlige myndigheter om, på Etterretningstjenestens vegne og i Etterretningstjenestens interesse, fordekt å innhente informasjon dersom Etterretningstjenesten kunne gjort dette selv i henhold til eget

---

[385] Etterretningstjenesteloven § 4 første ledd forstås slik at *mottak* av informasjon fra andre offentlige myndigheter eller kilder som ikke involverer Etterretningstjenesten i den operative innhentingen av informasjonen, *ikke* er å anse som fordekt innhenting. Det redegjøres nærmere for forståelsen av § 4 i høringsnotatet punkt 8.4.

[386] Se nærmere om denne distinksjonen i punkt 8.4 om begrepsforståelsen knyttet til den territorielle begrensningen.

[387] Se forutsetningsvis i Ot.prp. nr. 50 (1996-97) s.11

[388] Lovforståelsen fremgår i EOS-utvalgets årsmelding for 2008 (Dokument 18 (2008-2009) s. 31-32). EOS-utvalget konkluderte med at «informasjonsutveksling mellom PST og E-tjenesten ikke kan anses som å 'overvåke eller på annen fordekt måte innhente informasjon'».

rettsgrunnlag. Derimot er det antatt at det ikke vil være noe til hinder for at Etterretningstjenesten anmoder andre offentlige myndigheter om å vurdere innhentingstiltak etter deres respektive lovgrunnlag og innenfor deres egne oppgaver, selv om utfallet av en slik innhenting potensielt også kan være av interesse for Etterretningstjenesten.

Etterretningstjenestelovens primære fokus er rettet mot innhenting av informasjon utenfor landets grenser, fortrinnsvis ved fordekt innhenting gjennom de tradisjonelle innhentingsdisipliner, og i mindre grad på frivillig informasjonsdeling med norske virksomheter. Det har derfor vært noe uklart i hvilken utstrekning tjenesten kan motta informasjon fra andre norske virksomheter som på frivillig basis ønsker å dele slik informasjon, uten hinder av lovbestemt taushetsplikt. Lovgiver tok ikke uttrykkelig stilling til dette ved vedtakelsen av dagens lov, men forarbeidene synes å forutsette at tjenesten skal samarbeide med andre virksomheter uavhengig av lovbestemt taushetsplikt:[389]

> «E-tjenesten skal, utover å anvende egne innsamlingsmidler, samarbeide med andre ledd i Forsvaret og med andre som disponerer midler som kan nyttes for etterretningsmessig innsamling.»

Behovet for et nært og tillitsfullt samarbeid med PST understrekes også samme sted.

13.4.1.3 Nærmere om lovbestemt taushetsplikt som skranke mot informasjonsdeling

Lovbestemt taushetsplikt kan forhindre utlevering av etterretningsrelevant informasjon. Etterretningstjenesten har i flere saker erfart at offentlige så vel som private virksomheter har måttet avstå fra å utlevere viktig informasjon under henvisning til lovbestemt taushetsplikt, selv om informasjonen berører rikets sikkerhet. I noen saker har behovet for informasjonsdeling vært så påtrengende at man har erfart at utlevering likevel har skjedd av hensyn til sakens viktighet, selv om forholdet til gjeldende taushetspliktregler har voldt betydelig tvil.

Informasjon innhentet ved PSTs bruk av tvangsmidler kunne lenge ikke utleveres til Etterretningstjenesten som følge av taushetspliktbestemmelsene i politiloven og straffeprosessloven. Ved lovendring i 2017 ble straffeprosessloven § 216 i og politiloven § 17 f endret ved at det ble etablert et unntak fra taushetsplikten for utlevering av opplysninger fra skjulte tvangsmidler til Etterretningstjenesten.[390] Taushetsplikten er begrenset til informasjon som er nødvendig for forebyggelses- og sikkerhetsmessige formål knyttet til Etterretningstjenestens oppgaver etter lov om Etterretningstjenesten. Også rådata og informasjon til bruk for målsøking kan utleveres. Lovendringene innebærer ingen utleveringsplikt, kun en utleverings*rett*. Dette gir utleverende organ anledning til å foreta en nødvendighets- og forholdsmessighetsvurdering forut for utlevering, og på den bakgrunn vurdere om deling kan og bør skje. Etterretningstjenesten kan bidra med informasjon om det faktum som ligger til grunn for anmodningen om utlevering.

Hva angår utlevering av opplysninger fra private rettssubjekter, kan dette unntaksvis skje etter en konkret vurdering av om taushetsplikten vil hindre ivaretakelse av rikets sikkerhet sett opp mot de hensyn som taushetsplikten verner. I vurderingen må det også tas hensyn til om utleveringen ivaretar aktverdige og tilbørlige reelle hensyn, innebærer andre brudd på materielle bestemmelser i spesiallovgivningen, eller innebærer inngripende tiltak mot enkeltpersoner i strid med legalitetsprinsippet. Utleveringen må også anses forsvarlig etter

[389] Se Ot. prp. nr. 50 (1996-1997) s. 10

[390] Prop. 61 L (2016-2017) og Innst. 264 L (2016-2017)

den rettslige grunnsetning om innskrenkende tolkning av straffebud som etter etablert rettsoppfatning må tolkes innskrenkende og leses med forbehold om unntakssituasjoner som lovgiver ikke har ment å ramme. I tillegg må utleveringen være forsvarlig ut fra den alminnelige rettsstridsreservasjonen i norsk strafferett om at når handlingen ikke er utilbørlig og straffverdig i relasjon til den interesse som straffebudet tar sikte på å beskytte, er den heller ikke straffbar. I ytterste konsekvens kan utlevering i noen situasjoner også begrunnes i doktrinen om lovlige myndighetshandlinger, prinsippet om at spesiell lov går foran generell lov, og nødrett (at formålet med utleveringen er å redde liv, helse, eiendom eller annen interesse fra en fare for skade som ikke kan avverges på annen rimelig måte, og at denne skaderisikoen er langt større enn skaderisikoen ved å bryte eller tøye lovbestemt taushetsplikt). Eksempelvis vil dette kunne gjelde utlevering av opplysninger som er nødvendig for å bidra til å skjerme Etterretningstjenestens kilder i utlandet. I visse deler av verden vil kompromittering av tjenestens kilder kunne få svært alvorlige følger.

13.4.1.4 Eksempler på utfordringer med dagens rettstilstand

Både de generelle taushetspliktreglene etter forvaltningsloven og taushetspliktregler i særlovgivningen kan hindre at viktig og relevant informasjon kommer Etterretningstjenesten i hende. Noen hypotetiske eksempler kan illustrere dette.

Utlendingsmyndighetene og utenrikstjenesten vil gjennom sitt virke og sin saksbehandling besitte viktig landinformasjon og annen informasjon om utenlandske forhold (herunder personopplysninger) som Etterretningstjenesten etter omstendighetene bør kunne motta. Dersom utlendingsmyndighetene mottar opplysninger om terroristtreningsleire i en asylsøkers hjemland, bør slik informasjon kunne bringes til Etterretningstjenestens kunnskap. Det samme gjelder dersom utenrikstjenesten som ledd i sin konsulære virksomhet mottar opplysninger som kan bidra til løsningen av Etterretningstjenestens lovpålagte oppdrag.

Etterretningstjenesten vil kunne ha god nytte av informasjon som besittes av *tollmyndighetene og norske bedrifter om sensitive forhold knyttet til eksport og tollbehandling av varer*, for å kunne bidra til mer tidsriktig informasjon om det internasjonale ikke-spredningsarbeidet, internasjonal våpenhandel og andre viktige lovpålagte oppgaver. Når det gjelder innhenting av informasjon om internasjonal terrorisme kan blant annet opplysninger som tollmyndighetene besitter om utenlandske leverandører av materiale til fremstilling av eksplosiver kunne være av interesse. Tjenesten har særlige fortrinn ved å kunne analysere slik informasjon i lys av annen informasjon som den besitter. Tollovens[391] regler om unntak fra taushetsplikt, jf. tolloven § 12-1 nr. 2, vil ikke alltid være tilstrekkelig dekkende for at tollmyndighetene kan gjøre unntak fra taushetsplikten og dele informasjon med tjenesten. Det vises også til drøftelsen nedenfor om hvorvidt rettsgrunnlaget for Etterretningstjenesten «klart forutsetter» at taushetsplikten ikke skal være til hinder for å gi opplysningene.

Informasjon som *forskningsinstitusjoner* besitter om utenlandske samarbeidspartneres og utenlandske borgeres virksomhet i utlandet kan ha betydelig utenlandsetterretningsmessig verdi. Slik informasjon kan blant annet bidra til å kartlegge andre staters og organisasjoners strukturer og intensjoner, samt kunne benyttes som grunnlag for senere samarbeid mellom vedkommende institusjoner/personer og tjenesten. Bestemmelsene om taushetsplikt i

[391] Lov av 21. desember 2007 nr. 119 om toll og vareførsel

forvaltningsloven §§ 13 til 13e gjelder tilsvarende for universiteter og høgskoler, jf. universitets- og høyskoleloven § 7-6.[392]

Sjøfarts- og luftfartsmyndighetene bør kunne gi Etterretningstjenesten informasjon som er av betydning for tjenestens oppdrag, eksempelvis om erfarte fysiske eller digitale trusler mot sjøfarten i utlandet og om stater, organisasjoner eller personer som er involvert i slik virksomhet.

Også fra *andre deler av Forsvaret* kan det være behov for å meddele opplysninger til Etterretningstjenesten uten hinder av lovbestemt taushetsplikt. Som eksempel kan nevnes kystvaktloven[393] § 20 første ledd, som etter omstendighetene kan hindre utlevering av opplysninger fra Kystvakten til Etterretningstjenesten om forhold som erfares under kystvakttjenesten, ved at anledningen til å gi opplysninger etter denne bestemmelsen uten hinder av taushetsplikt kun gjelder i forhold til «vedkommende kontrollmyndighet, politi eller påtalemyndighet».

Det kan tenkes at Etterretningstjenesten vil ha behov for å få utlevert taushetsbelagte opplysninger fra *Folkeregisteret*, bl.a. for å avklare en persons identitet og status som norsk person. Folkeregisterloven[394] § 10-2 kan etter omstendighetene hindre utlevering av slike opplysninger.

Forvaltningsloven[395] §§ 13 flg. gjelder for *enhver som utfører tjeneste eller arbeid for et forvaltningsorgan*. Bestemmelsene er også gjort tilsvarende gjeldende for enkelte andre, se eksempelet ovenfor om universitets- og høgskoleloven. Taushetsplikten gjelder etter § 13 det man i forbindelse med tjenesten eller arbeidet får vite om «noens personlige forhold» eller «tekniske innretninger og fremgangsmåter samt drifts- og forretningsforhold som det vil være av konkurransemessig betydning å hemmeligholde av hensyn til den som opplysningen angår». Unntakene fra taushetsplikten i §§ 13 a flg. vil ikke nødvendigvis dekke videreformidling av etterretningsrelevant informasjon til Etterretningstjenesten, fordi slik videreformidling etter omstendighetene verken innebærer at «opplysningene brukes for oppnå det formål de er gitt eller innhentet for» (§ 13 b nr. 2) eller at videreformidlingen fremmer avgiverorganets oppgaver (§ 13 b nr. 5). Utlevering av slike opplysninger kan for øvrig bare formidles til andre dersom det er fastsatt i lov eller klart forutsatt at taushetsplikten ikke skal gjelde (§ 13 f annet ledd). I enkelte sammenhenger har det blitt lagt til grunn at Etterretningstjenestens innhentingshjemmel er å anse som en tilstrekkelig hjemmel i lov i forhold til annen lovgivning som krever slik lovhjemmel. Etterretningstjenesteloven har likevel ikke en spesifikk bestemmelse om rett til å kreve eller motta innsyn i taushetslagte opplysninger. Det er derfor ikke grunnlag for generelt å slå fast at gjeldende lov «klart forutsetter» at taushetsplikten ikke skal gjelde for opplysninger som gis tjenesten og som ellers er undergitt taushetsplikt etter forvaltningsloven eller andre lovbestemmelser.

[392] Lov av 1. april 2005 nr. 15 om universiteter og høyskoler

[393] Lov av 13. juni 1997 nr. 42 om Kystvakten

[394] Lov av 9. desember 2016 nr. 88 om folkeregistrering

[395] Lov av 10. februar 1967 om behandlingsmåten i forvaltningssaker

Ytterligere eksempler er omtalt i høringsnotat fra Justis- og beredskapsdepartementet som lå til grunn for endringer i straffeprosessloven og politiloven for å gi en utvidet adgang til utlevering av opplysninger fra PST til Etterretningstjenesten, hvorfra hitsettes:[396]

> «Slik informasjon kan for eksempel være opplysninger om statlige og ikke-statlige aktører og forhold, bl.a. i form av informasjon om utenlandske telefonnumre, e-postadresser, IP-adresser, nettverk, personer og forhold, og som vil bidra til E-tjenestens målutvikling, innhenting og analyse av utenlandske forhold og aktører. Andre opplysninger som kan være av stor betydning for E-tjenestens oppgaveløsning kan være ulike typer informasjon tilknyttet utenlandske etterretningsmål, informasjon om politiske forhold innad i regimer, om fremmede lands våpensystemer, informasjon som kan avdekke koplinger mellom utenlandsk organisert kriminalitet og statlige organisasjoner, tekniske opplysninger om hvorledes et utenlandsk nettverk av interesse kommuniserer, samt informasjon om personer i utenlandske tjenester som det bør knyttes kontakter med.»

Slike opplysninger kan også andre offentlige myndigheter enn PST besitte, og informasjonen kan være undergitt lovbestemt taushetsplikt etter forvaltningsloven eller særbestemmelser i sektorlovgivning.

13.4.2 Departementets vurdering

Departementet vurderer at det er behov for å bygge ned de rettslige hindringene som vanskeliggjør at ressursene finner hverandre i det samlede offentlige arbeidet med å forebygge, avdekke og motvirke utenlandske trusler mot Norge og norske interesser. Departementet har få eksempler på at lovgiver har tatt uttrykkelig stilling til om taushetsplikten i særlovgivningen også skal gjelde overfor Etterretningstjenesten. Hensynene bak de ulike taushetspliktene kan variere, og vil veie ulikt opp mot hensynet til rikets sikkerhet.

Erfaring tilsier at de fleste frivillig vil samarbeide med Etterretningstjenesten om forhold som man forstår kan være viktig for å bidra til å kartlegge og motvirke utenlandske trusler mot grunnleggende nasjonale sikkerhetsinteresser. Departementet mener derfor at det bør slås fast at lovbestemt taushetsplikt *ikke er til hinder* for at offentlige myndigheter[397] utleverer informasjon til Etterretningstjenesten dersom det er nødvendig for forebyggelses- og sikkerhetsmessige formål innenfor rammen av Etterretningstjenestens oppgaver etter kapittel 3. Formuleringen «ikke er til hinder» foreslås for å understreke at det vil være tale om å etablere en *rett* – og ikke en plikt – til å utlevere informasjon. Det vil altså være opp til den offentlige myndigheten å avgjøre om informasjon skal utleveres, herunder om utleveringen er forholdsmessig, og om det skal oppstilles vilkår for en eventuell utlevering.

Departementet vurderer at en slik utleveringsrett vil gi utleverende myndighet rom til å foreta en konkret vurdering av *inngrepets karakter* og om utlevering er nødvendig og

---

[396] Høringsnotat av 1. februar 2016 fra Justis- og beredskapsdepartementet som lå til grunn for Prop. 61 L (2016-2017) om endringer i straffeprosessloven og politiloven (utlevering av informasjon fra PST til tjenesten) s. 10-11

[397] Med «offentlige myndigheter» menes her alle typer offentlige forvaltningsorganer, inkludert statsforvaltningen, fylkesmannsembeter, fylkeskommuner, kommuner, forvaltningsbedrifter, høgskoler, universiteter og forskningsinstitusjoner, offentlige regulerings-, kontroll- og tilsynsmyndigheter, offentlige fond og finansinstitusjoner, samt andre etater og offentlige organer, styrer og råd. Statseide selskaper som opererer som kommersielle aktører i et marked er ment å falle utenfor begrepet. Også statsforetak og særlovsselskaper som f.eks. regionale helseforetak bør falle utenfor.

forholdsmessig, herunder rom til å vurdere omfanget og arten av de opplysninger som potensielt skal deles opp mot taushetspliktens formål og hensynet til den opplysningene gjelder. I denne forbindelse vil departementet påpeke at hensynet til rikets sikkerhet og andre viktige nasjonale sikkerhetsinteresser normalt vil veie tyngre enn hensynet til de individuelle interesser som taushetsplikten skal beskytte. Dette gjelder for eksempel i forhold til personopplysninger som et offentlig organ måtte ha om personer tilknyttet terrornettverk i utlandet. I slike tilfeller vil den enkeltes personvern som oftest måtte vike for de sikkerhetsmessige interesser som Etterretningstjenestens lovpålagte samfunnsoppdrag hviler på.

Departementet vurderer at lovbestemt taushetsplikt ikke bør være til hinder for utlevering av personopplysninger dersom utlevering er «nødvendig for forebyggelses- og sikkerhetsmessige formål». Departementet foreslår en slik formulering fordi den harmonerer med PSTs adgang til å utlevere informasjon som stammer fra tvangsmiddelbruk til Etterretningstjenesten, jf. straffeprosessloven § 216 i bokstav i. I forarbeidene til denne bestemmelsen ble det lagt til grunn at begrepet «forebyggelses- og sikkerhetsmessige formål» også dekker informasjon som er av betydning for norsk utenriks-, sikkerhets- og forsvarspolitikk, jf. formuleringen «blant annet […] oppgaver etter etterretningstjenesteloven § 3 første ledd bokstav a, b, f, g og i». Departementet vurderer derfor at begrepet i praksis vil kunne dekke det alt vesentlige av Etterretningstjenestens oppgaver etter lovutkastet kapittel 3. Det presiseres her at den konkrete nødvendighets- og forholdsmessighetsvurderingen vil hindre utlevering dersom formålet med Etterretningstjenestens bruk av opplysningene har en for fjern sammenheng med utførelsen av oppgavesettet. Sammenlignet med dagens rettstilstand representerer lovforslaget her en presisering og uttømmende avgrensning av Etterretningstjenestens oppgaver og hva som regnes som etterretningsformål etter lovforslaget kapittel 3. Grensen for utlevering av informasjon gjennom frivillig samarbeid bør følge de grensene som fastslås i lovforslaget kapittel 3.

En annen årsak til at departementet vil benytte tilsvarende formulering som i straffeprosessloven § 216 i bokstav i, er at ny lov om Etterretningstjenesten ikke bør åpne opp for utlevering i større grad enn det Stortinget anså som legitimt ved vedtakelsen av denne bestemmelsen. I denne sammenheng er det også et poeng at den informasjonen som andre offentlige myndigheter besitter ikke vært innhentet gjennom tvangsmidler, slik at utlevering fra andre myndigheter enn PST normalt vil være mindre inngripende. Dette taler etter departementets syn for at det også bør åpnes for en utleveringsrett for andre myndigheter.

Departementet har vurdert om forslaget her bør åpne for at private virksomheter får en *generell* adgang til å utlevere opplysninger til Etterretningstjenesten. Etter departementets syn kan en slik lovendring ramme den særlige tillit som taushetsplikt for enkelte yrkesutøvere er ment å ivareta, blant annet i forholdet mellom helsepersonell og pasienter og mellom advokater og klienter. Etter departementets syn er imidlertid denne problemstillingen såpass sensitiv at den eventuelt bør utredes særskilt.

For ordens skyld bemerkes at utleveringsadgangen er avgrenset mot personer som arbeider i eller for en offentlig myndighet er å anse som særlige yrkesutøvere som har særskilt kallsmessig taushetsplikt eller tilsvarende sterk formålsbegrenset bruk av opplysninger. Lovforslaget her skal ikke forstås å sette denne særskilt sterke taushetsplikten til side.

Departementet foreslår følgende bestemmelse i lovutkastet § 10-2:

§ 10-2 *Utlevering av informasjon til Etterretningstjenesten fra norske offentlige myndigheter*
Lovbestemt taushetsplikt er ikke til hinder for at offentlige myndigheter utleverer informasjon til Etterretningstjenesten dersom det er nødvendig for forebyggelses- og sikkerhetsmessige formål innenfor rammen av Etterretningstjenestens oppgaver etter kapittel 3.

13.5 Bistand til politiet

Rammene for Forsvarets bistand til politiet følger av politiloven § 27 a sammenholdt med tilhørende instruks om Forsvarets bistand til politiet (bistandsinstruksen[398]). Etterretningstjenesten kan, etter anmodning fra politisjef, Politidirektoratet eller PST, bistå politiet på politiets hjemmelsgrunnlag, og på eventuelle vilkår satt av Etterretningstjenesten, ved de situasjoner som følger av politiloven § 27 a og bistandsinstruksen § 3. Generelt vil bistanden kunne omfatte materiell og personell, og vil kunne være av både administrativ og operativ karakter.[399] Bistand kan også være aktuelt ved større og alvorlige hendelser i Norge. Fra foredraget til bistandsinstruksen hitsettes:

> «Til sist nevnes at […] Etterretningstjenestens bistand til politiet ikke lenger faller utenfor instruksen. Dette er praktisk og nødvendig gitt at Etterretningstjenesten spiller en viktig rolle, særlig i store og komplekse operasjoner slik maritime kontraterroroperasjoner vil være.»[400]

I lovutkastet § 4-4 foreslår departementet en bestemmelse om at bistand til politiet etter dette regelverket ikke er å anse som brudd på forbudet mot å utføre oppgaver med politiformål. Det skyldes at bistand ikke skjer for etterretningsformål, men skjer på *politiets rettsgrunnlag* og for å løse *politiets oppdrag*. Bakgrunnen for bistandsregimet er at man i særskilte tilfeller må bruke de samfunnsresursene som er tilgjengelig for å løse et oppdrag. Etter avgivelse av bistandsressursen vil denne være under politiets ledelse og instruksjonsmyndighet. Politiet eier all informasjon som eventuelt innhentes som ledd i politioperasjonen, og slik informasjon skal ikke anses utlevert til Etterretningstjenesten.

Bistand etter dette regelverket må ikke sammenblandes med «bistand» etter samarbeidsinstruksen mellom Etterretningstjenesten og PST. Sistnevnte er et samarbeid som skjer innenfor rammen av tjenestenes respektive rettsgrunnlag.

Bistand gjelder i prinsippet innenfor hele politiets virkeområde, også i situasjoner som ikke krever maktbruk. Det følger både av ordlyden i § politiloven 27 a og forarbeidene.[401] For å unngå en teoretisk mulighet for formålsglidning i forhold til tilrettelagt innhenting etter kapittel 7 i lovforslaget her, i form av at politiet skal kunne anmode om bistand fra Etterretningstjenesten i form av direkte bruk av denne tilgangen eller utlevering av opplysninger fremskaffet gjennom denne tilgangen, må det etter departementets syn fastsettes i lov at dette ikke skal finne sted. Det foreslås følgende bestemmelse, samtidig som det bemerkes at bestemmelsens første punktum er en ren informasjonsbestemmelse som allerede følger av politiloven § 27 a:

§ 10-3 *Bistand til politiet*

---

[398] Kongelig resolusjon av 16. juni 2017 nr. 789.

[399] Jf. Prop.79 L (2014-2015) s. 22

[400] PRE-2017-06-16-789 Fastsetting av ny instruks om Forsvarets bistand til politiet, se kapittel 3 merknad til § 12

[401] Prop.79 L (2014-2015) s. 22

Etterretningstjenesten kan yte bistand til politiet etter politiloven § 27 a. Bistand i form av informasjonsinnhenting etter reglene i kapittel 7 eller utlevering av informasjon etter § 7-12 annet ledd, kan ikke finne sted.

14 Avsluttende bestemmelser

14.1Innledning

Departementet foreslår at bestemmelser knyttet til saksbehandling, taushetsplikt, skjerming av informasjon mv. samles i et eget kapittel i loven. Av hensyn til Etterretningstjenestens egenart er det behov for å fastsette regler som på enkelte områder divergerer fra det som ellers gjelder i forvaltningen. I sin daglige virksomhet driver imidlertid Etterretningstjenesten også alminnelig forvaltningsvirksomhet. Det foreslås ingen endringer fra den generelle lovgivningen på disse områdene.

14.2 Forvaltningslovens anvendelse

14.2.1 Innledning

Forvaltningsloven[402] gjelder i utgangspunktet for alle forvaltningsorganer. Departementet har vurdert nærmere i hvilken grad forvaltningsloven kommer anvendelse på Etterretningstjenestens virksomhet, og hvordan forholdet mellom forvaltningsloven og etterretningsvirksomheten bør reguleres i lovforslaget.

14.2.2 Forholdet mellom forvaltningsloven og etterretningsvirksomhet

Forvaltningsloven gjelder «virksomhet som drives av forvaltningsorganer». Som et forvaltningsorgan regnes «ethvert organ for stat eller kommune», jf. forvaltningsloven § 1 første og andre punktum. Etterretningstjenesten er organisatorisk en del av Forsvaret, og følgelig et organ for staten. Forvaltningslovens regler kommer til anvendelse så fremt ikke annet følger av annen lov. Videre må Etterretningstjenestens virksomhet utøves innenfor rammen av alminnelige forvaltningsrettslige prinsipper om god forvaltningsskikk og forsvarlig saksbehandling.

Forvaltningsloven stiller særlige krav til saksbehandlingen dersom forvaltningsorganet treffer vedtak som generelt eller konkret er bestemmende for rettigheter eller plikter til private personer, jf. forvaltningsloven § 2 første ledd bokstav a. Vedtak kan enten være enkeltvedtak som retter seg mot en eller flere bestemte personer, eller forskrift som retter seg mot et ubestemt antall eller en ubestemt krets av personer, jf. forvaltningsloven § 2 bokstav b og c. Fordi det som ledd i informasjonsinnhentingsvirksomheten ikke treffes enkeltvedtak i forvaltningslovens forstand, får saksbehandlingsreglene i kapittel IV-VI ikke anvendelse for denne aktiviteten, jf. forvaltningsloven § 3.

[402] Lov av 10. februar 1967 om behandlingsmåten i forvaltningssaker

14.2.3 Departementets vurdering

Departementet vurderer at Etterretningstjenesten under utøvelsen av sine lovpålagte oppgaver etter etterretningstjenesteloven ikke treffer avgjørelser som er normerende og dermed bestemmende for noens rettigheter eller plikter. Bestemmelsene i forvaltningsloven får dermed i liten grad anvendelse på Etterretningstjenestens saksbehandling, og departementet vurderer derfor at det bør fremgå klart av ny lov om Etterretningstjenesten hvilke bestemmelser som bør gjelde. Til sammenligning ble det i 2005 gitt egne og presiserende bestemmelser om forvaltningslovens og offentlighetslovens anvendelse for PSTs saksbehandling tilknyttet tvangsmidler i forebyggende øyemed, se politiloven § 17 e tredje ledd. Hensynet bak å gi et helhetlig regelverk for saksbehandling for PST i disse sakene er tilnærmet sammenfallende som bakgrunnen for at departementet nå foreslår å gjøre unntak fra forvaltningslovens saksbehandlingsregler for saksbehandling knyttet til Etterretningstjenestens etterretningsvirksomhet.

Departementet mener at det bør fremgå at forvaltningsloven ikke kommer til anvendelse for saksbehandling som knytter seg til utførelsen av Etterretningstjenestens oppgaver etter lovforslaget, med unntak av bestemmelsene om taushetsplikt i §§ 13 til 13 f. Bakgrunnen for dette er at forvaltningslovens bestemmelser om taushetsplikt, herunder begrensinger i taushetsplikten, også gjør seg gjeldende for behandling av opplysninger, uavhengig av om det er personopplysninger eller ikke, som tjenesten behandler med et etterretningsformål. Ved å videreføre forvaltningslovens bestemmelser om taushetsplikt for Etterretningstjenestens behandling av opplysninger, uansett formål, sikres det også taushetsplikt der opplysningen ikke er å anse som sikkerhetsgradert etter sikkerhetslovens bestemmelser. Departementet foreslår ingen endring vedrørende forvaltningslovens anvendelse på den øvrige forvaltningsmessige virksomheten til Etterretningstjenesten.

Departementet foreslår følgende bestemmelse:

§ 11-7 *Forholdet til forvaltningsloven*

Med unntak av forvaltningsloven §§ 13 til 13 f om taushetsplikt, kommer forvaltningsloven ikke til anvendelse for saksbehandlingen som knytter seg til utførelsen av Etterretningstjenestens oppgaver etter loven her.

14.3 Behovet for særlig regulering av taushetsplikten

14.3.1 Innledning

Bestemmelser om taushetsplikt knyttet til utøvelsen av etterretningsvirksomhet følger av flere lover og forskrifter. Departementet har konkludert med at det i tillegg til disse bør foreslås en særlig bestemmelse om taushetsplikt i lovforslaget som skjerper plikten. Departementets vurdering vil utdypes i det følgende.

14.3.2 Gjeldende rett

Taushetsplikten for Etterretningstjenestens personell og personer som har tilgang til sikkerhetsgradert informasjon som ledd i oppdrag eller verv for Etterretningstjenesten er først og fremst regulert i sikkerhetsloven § 5-4 annet ledd.[403] Bestemmelsen lyder:

[403] Lov om nasjonal sikkerhet ble vedtatt av Stortinget den 27. februar 2018, men vil ikke tre i kraft før i 2019 etter at tilhørende forskrifter er vedtatt.

Enhver som får tilgang til sikkerhetsgradert informasjon som ledd i arbeid eller tjeneste for en virksomhet som omfattes av loven, har taushetsplikt om innholdet. Taushetsplikten gjelder også etter at arbeidet eller tjenesten er avsluttet.

Som nevnt over i punkt 14.2.3 kommer forvaltningslovens bestemmelser om taushetsplikt etter §§ 13-13 f til anvendelse der ikke andre taushetspliktbestemmelser regulerer forholdet særskilt. I korte trekk får forvaltningsloven §§ 13 til 13 f anvendelse der informasjonen ikke er gradert, herunder hvor Etterretningstjenesten driver annen forvaltningsvirksomhet enn for etterretningsformål.

14.3.3 Departementets vurdering

Departementet vurderer at sikkerhetslovens og forvaltningslovens bestemmelser om taushetsplikt bør videreføres som generelle taushetspliktsregler for Etterretningstjenestens personell. I tillegg mener departementet at det bør inntas en egen taushetspliktbestemmelse i lovforslaget som fanger opp Etterretningstjenestens behov for særlige regler som går lenger enn den alminnelige taushetsplikten.

For det første foreslår departementet at det bør gjelde en strengere strafferamme ved brudd på taushetsplikten for personer som er ansatt eller gjør tjeneste for Etterretningstjenesten, enn det som ellers gjelder i samfunnet. Videre mener departementet at taushetsplikten bør være livsvarig, noe som bør tydeliggjøres i lovs form.

Departementet foreslår at den særlige taushetspliktbestemmelsen bør avgrenses til kun å gjelde *skjermingsverdig informasjon*, og at legaldefinisjonen fremgår av bestemmelsen. «Skjermingsverdig informasjon» bør etter departementets syn defineres som informasjon som kan skade nasjonale sikkerhetsinteresser dersom den blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig. Det bør videre presiseres at informasjon kan være «skjermingsverdig» selv om den ikke er *merket* som sikkerhetsgradert i henhold til sikkerhetslovens regler – det avgjørende ved vurderingen vil være om informasjonen etter en konkret vurdering må anses som «skjermingsverdig». Definisjonen etter lovforslaget her bør være innholdsmessig sammenfallende med begrepet «skjermingsverdig informasjon» i sikkerhetsloven.

Departementets forslag gjør dessuten enkelte tilpasninger og unntak for å harmonisere taushetsplikten med de øvrige bestemmelsene i lovforslaget. Særlig mener departementet at det bør komme klart frem at det gjelder unntak fra taushetsplikten der norske kontroll- og tilsynsmyndigheter får tilgang til opplysninger som ledd i deres oppgaveløsning.

Videre mener departementet at taushetsplikten ikke bør være til hinder for at opplysninger utleveres der det foreligger hjemmelsgrunnlag, eller at opplysninger gjøres kjent for andre i Etterretningstjenesten i samsvar med gjeldende autorisasjonsregler og prinsippet om tjenstlig behov. Klarhetshensyn, og særlig av hensyn til forutberegnelighet for den enkelte, tilsier en regel som slår dette fast, ettersom denne begrensningen i taushetsplikten er særlig aktuell for Etterretningstjenestens virksomhet sammenlignet med øvrige forvaltningsorganer.

Departementet foreslår følgende lov formulering:

§ 11-1 *Taushetsplikt*

Enhver som gjør arbeid eller tjeneste for Etterretningstjenesten skal bevare livsvarig taushet om skjermingsverdig informasjon som de blir kjent med gjennom arbeidet eller tjenesten. Tilsvarende taushetsplikt gjelder for kilder og oppdragstakere som har undertegnet særskilt taushetserklæring utstedt av Etterretningstjenesten.

Med skjermingsverdig informasjon menes informasjon som kan skade nasjonale sikkerhetsinteresser dersom informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig. Informasjonen kan være skjermingsverdig selv om den ikke har blitt merket som sikkerhetsgradert informasjon etter sikkerhetsloven.

Skjermingsverdig informasjon etter første ledd kan ikke utnyttes i virksomhet utenfor Etterretningstjenesten.

Taushetsplikten er ikke til hinder for at opplysninger utleveres etter bestemmelsene i loven her eller etter regler fastsatt i annen lov når det er uttrykkelig bestemt eller klart forutsatt at taushetsplikt ikke skal gjelde, eller at opplysninger gjøres kjent for andre i Etterretningstjenesten i samsvar med gjeldende autorisasjonsregler og prinsippet om tjenstlig behov.

14.4 Konsekvenser ved brudd på taushetsplikten

14.4.1 Innledning

Brudd på lov- eller forskriftsregulert taushetsplikt er normalt belagt med straff. Brudd på taushetsplikter kan også ha andre konsekvenser, herunder for arbeidsforholdet. Departementet vil i det følgende vurdere hvorvidt de straffesanksjoner som følger av gjeldende rett er tilstrekkelige, eller om disse bør skjerpes i en egen bestemmelse i lovforslaget her.

14.4.2 Gjeldende rett

Straffesanksjonering av brudd på lov- eller forskriftsbestemt taushetsplikt reguleres først og fremst av det generelle straffebudet i straffeloven § 209 om brudd på taushetsplikt. Bestemmelsens første og andre ledd lyder:

Med bot eller fengsel inntil 1 år straffes den som røper opplysning som han har taushetsplikt om i henhold til lovbestemmelse eller forskrift, eller utnytter en slik opplysning med forsett om å skaffe seg eller andre en uberettiget vinning.

Første ledd gjelder tilsvarende ved brudd på taushetsplikt som følger av gyldig instruks for tjeneste eller arbeid for statlig eller kommunalt organ.

Det følger av bestemmelsens fjerde ledd at grov uaktsomhet straffes på samme måte. Av bestemmelsens siste ledd fremgår det at medvirkning ikke er straffbart.

Etter straffeloven § 210 er det gitt en strafferamme på inntil 3 års fengsel for *grovt brudd* på taushetsplikten. Etter andre ledd skal det ved avgjørelsen av om taushetsbruddet er grovt legges særlig vekt på om gjerningspersonen har hatt forsett om uberettiget vinning og om handlingen har ført til tap eller for fare for tap for noen. Også uaktsomhet knyttet til følgen av en handling hvis resultat er at taushetsplikten er brutt, vil ha betydning ved vurderingen av om bruddet er grovt. Det samme gjelder dersom vedkommende har unnlatt etter evne å avverge følgen etter å ha blitt oppmerksom på at den kunne inntre, jf. straffeloven § 24.

Straffesanksjonering av brudd på taushetsplikten etter sikkerhetsloven følger sikkerhetsloven § 11-4 annet ledd, som lyder:[404]

[404] Lov om nasjonal sikkerhet ble vedtatt av Stortinget den 27. februar 2018, men vil ikke tre i kraft før i 2019 etter at tilhørende forskrifter er vedtatt.

Den som forsettlig eller grovt uaktsomt bryter taushetsplikt etter § 5-4 andre ledd eller § 6-6 femte ledd, straffes med bot eller fengsel inntil 1 år eller begge deler, hvis ikke forholdet går inn under en strengere straffebestemmelse.

Bestemmelsen får etter sin ordlyd kun anvendelse når bruddet på taushetsplikten omfatter informasjon som er skjermingsverdig etter sikkerhetsloven. For brudd på taushetsplikt om informasjon som ikke anses som «skjermingsverdig» vil man fortsatt kunne straffeforfølges for brudd på taushetsplikten etter forvaltningslovens regler om taushetsplikt sammenholdt med straffeloven §§ 209 og 210.

Videre fastsetter straffeloven §§ 123 og 124 straff for den som «uten aktverdig grunn» offentliggjør, overleverer eller på annen måte avslører en hemmelig opplysning som kan skade grunnleggende nasjonale interesser. Det presiseres i § 123 at «den som avslører en slik opplysning til en fremmed stat eller terrororganisasjon, anses ikke for å ha en aktverdig grunn.» At opplysningen er sikkerhetsgradert, vil være et moment i vurderingen av skadevirkningen, men er ikke i seg selv tilstrekkelig til å oppfylle vilkåret for straff slik som det er for straffebestemmelsen i sikkerhetsloven. Ileggelse av straff etter bestemmelsene krever at det er utvist forsett ettersom ikke annet er bestemt, jf. straffeloven § 21. I tillegg vil avsløringen ikke være straffbar dersom den er gjort med *aktverdig grunn*. Lund-utvalget uttaler følgende i forbindelse med hva som anses som «aktverdig grunn»:[405]

> «Forutsetningen for straffefrihet er altså at det påvises en aktverdig grunn til å samle inn eller motta opplysningene. Dette må innebære ikke bare krav om at innsamling og mottak av sensitivt materiale kan sies å være en del av vedkommende person/institusjons legitime oppgaver, men også at det foreligger en konkret aktverdig grunn. Pressen kan således ikke ha frikort til å drive etterretningsvirksomhet med sikte på hemmeligheter av betydning for grunnleggende nasjonale interesser i håp om å finne noe å sette fingeren på.»

I en sak hvor noen har avslørt statshemmeligheter vil forholdet kunne vurderes etter §§ 123 og 124. Imidlertid vil det kunne være vanskelig å bevise at vilkårene for straff er oppfylt. I slike tilfeller vil en etter gjeldende rett falle tilbake på straffebestemmelsene i straffeloven § 209 og 210.

14.4.3 Departementets vurdering

Grunnet den særlige tilliten Etterretningstjenesten er avhengig av å ha i samfunnet sammenholdt med behovet for streng konfidensialitet og skjerming, foreslår departementet en høyere strafferamme for brudd på taushetsplikt enn de som følger av sikkerhetsloven § 11-4 og straffeloven §§ 209 og 210. I vurderingen av behovet for en slik bestemmelse er det også sett hen til straffeloven §§ 123 og 124 om avsløring av statshemmeligheter, hvor strafferammen er vesentlig høyere, særlig ved grove brudd. Departementet vurderer at det kan oppstå saker hvor vilkårene for straff etter straffeloven §§ 123 og 124 ikke er oppfylt og hvor strafferammen etter §§ 209 og 210 anses for lav på grunn av lovbruddets karakter. Departementet mener derfor at det er behov for en egen taushetspliktbestemmelse med skjerpet strafferamme.

Hvor allmenn- eller individualpreventivt en forhøyning av strafferammen vil virke, anses ikke relevant i denne henseende. Det er etter departementets syn først og fremst *lovbruddets karakter* som er av en slik straffverdighet som rettferdiggjør den høyere strafferammen. I

[405] NOU 2003:18 punkt 7.1.2 s. 73

disse sakene tilsier også hensynet til rikets sikkerhet at politiet ved mistanke om brudd på taushetsplikt kan ta i bruk alle relevante tvangsmidler. Også dette taler for en høy strafferamme.

Departementet er av det syn at et brudd på taushetsplikten av enhver som arbeider eller gjør tjeneste for Etterretningstjenesten, herunder også kilder og oppdragstakere som har undertegnet særskilt taushetserklæring utstedt av tjenesten, er av en så straffverdig karakter at alle disse persongruppene bør være omfattet av den særskilte straffebestemmelsen. Om personen anses å gjøre «arbeid» for Etterretningstjenesten» avhenger av om personen kan anses å ha et arbeidsforhold hos Etterretningstjenesten i arbeidsmiljølovens forstand. «Tjeneste» refererer til det forhold hvor en person formelt er ansatt i en annen avdeling i Forsvaret eller i annen offentlig organ, men hvor personen i en konkret periode er underlagt Etterretningstjenestens styringsrett. For «kilder» og «oppdragstakere» vil det avgjørende være om personen har signert taushetserklæring utstedt av Etterretningstjenesten.

Den særskilte straffebestemmelsen bør etter departementets syn bare få anvendelse for brudd på taushetsplikten der informasjonen er «skjermingsverdig». Skyldkravet foreslås å være forsett eller grov uaktsomhet, slik som i sikkerhetsloven. Dersom noen uaktsomt bryter taushetsplikten, vil personen kunne ilegges straff etter sikkerhetsloven § 11-4 første ledd jf. 5-2. Bestemmelsen som foreslås gjelder personer som arbeider eller gjør tjeneste for Etterretningstjenesten, herunder oppdragstaker og kilder dersom disse som nevnt har signert taushetserklæring. Er taushetserklæring ikke signert vil det være straffeloven § 123 som er mest aktuelle hjemmel.

Departementet foreslår på denne bakgrunn en bestemmelse som fastsetter straff for den som forsettlig eller grovt uaktsomt bryter taushetsplikt etter § 11-1. Strafferammen bør etter departementets syn settes til bot eller fengsel inntil 1 år eller begge deler, hvis ikke forholdet går inn under en strengere straffebestemmelse. Departementets forslag skiller seg altså fra straffeloven § 209 ved at straff også kan ilegges dersom personen har opptrådt grovt uaktsomt. For øvrig er strafferammen og den objektive gjerningsbeskrivelsen sammenfallende med første alternativ i § 209 første ledd.

Videre foreslår departementet en forhøyet strafferamme ved grovt brudd på taushetsplikten, og at denne settes til fengsel inntil 6 år. Ved avgjørelsen av om bruddet er grovt skal det særlig legges vekt på graden av skyld, herunder om eventuelle uforsettlige følgeskader innebærer skjerpelse jf. straffeloven § 24, og om bruddet har skadet Etterretningstjenestens virksomhet eller lett kunne ha ført til slik skade.

Departementet forslår følgende straffebestemmelser for brudd på taushetsplikten i lovforslaget § 12-1 første og andre ledd:

§ 12-1 *Straff*

Den som forsettlig eller grovt uaktsomt bryter taushetsplikt etter § 11-1, straffes med bot eller fengsel inntil 1 år eller begge deler, hvis ikke forholdet går inn under en strengere straffebestemmelse.

Grovt brudd på taushetsplikten straffes med fengsel inntil 6 år. Ved avgjørelsen av om bruddet er grovt skal det særlig legges vekt på graden av skyld og om bruddet har skadet Etterretningstjenestens virksomhet eller lett kunne ha ført til slik skade.

14.5 Sikkerhetsklarering

14.5.1 Innledning

Etterretningstjenesten behandler høygradert informasjon i et stort omfang. Det følger av sikkerhetsloven at enhver som får tilgang til sikkerhetsgradert informasjon som ledd i arbeid, oppdrag eller verv for en virksomhet som loven gjelder for, må oppfylle kravene som følger av sikkerhetsloven.[406] Departementet har vurdert om det i tillegg bør inntas en egen bestemmelse i lovforslaget som presiserer hvilke krav som stilles til Etterretningstjenestens personell for at de skal kunne arbeide for Etterretningstjenesten, herunder få tilgang til og behandle den informasjonen som tjenesten kommer i befatning med.

14.5.2 Gjeldende rett

Etter sikkerhetsloven § 8-1 annet ledd er det krav om at personer som skal autoriseres for tilgang til informasjon gradert KONFIDENSIELT eller høyere, må ha gyldig sikkerhetsklarering. Paragraf 8-2 første og annet ledd bestemmer videre at:

> Personer skal sikkerhetsklareres dersom de skal ha tilgang til informasjon gradert KONFIDENSIELT eller høyere etter § 5-3.
>
> Det samme gjelder personer som gjennom arbeidet sitt vil kunne få tilgang til slik informasjon. Sikkerhetsklarering skal likevel ikke gjennomføres dersom risikoen for tilgang til slik informasjon kan fjernes gjennom andre og enklere sikkerhetstiltak.

Første ledd vil omfatte det personellet i Etterretningstjenesten som i arbeidet sitt vil måtte behandle informasjon gradert KONFIDENSIELT eller høyere, mens annet ledd vil omfatte de som innehar stilling som i sitt arbeid vil kunne få tilgang til sikkerhetsgradert informasjon ved at de fysisk har tilgang til rom hvor annet personell arbeider med informasjon gradert KONFIDENSIELT eller høyere, for eksempel administrativt personell.

Det er gitt særskilte bestemmelser om sikkerhetsklarering for personell i Etterretningstjenesten i E-instruksen[407] § 4 andre ledd om nasjonal kontroll som lyder:

> Etterretningstjenestens personell skal som hovedregel være sikkerhetsklarert for STRENGT HEMMELIG. Sjefen for Etterretningstjenesten kan for særskilte stillinger med lavere klareringsbehov bestemme at personellet skal være sikkerhetsklarert for HEMMELIG**.**

14.5.3 Departementets vurdering

Ettersom Etterretningstjenesten i stort omfang behandler høyt sikkerhetsgradert informasjon, er departementet av den vurdering at ny lov bør videreføre instruksens krav til sikkerhetsklareringsnivå for enhver som gjør arbeid eller tjeneste for Etterretningstjenesten. Videre foreslås det at unntaket for særskilte stillinger også videreføres. Departementet er av det syn at en videreføring av kravet til sikkerhetsklarering ikke vil medføre noen utilsiktede virkninger. Det bør være en selvfølgelighet at de som arbeider eller gjør tjeneste hos den etaten i landet som i størst utstrekning behandler høyt gradert informasjon, også er tilstrekkelig vurdert for skikkethet og sikkerhet for å kunne behandle slike opplysninger. Dette

[406] Jf. sikkerhetsloven 2018 § 5-4 annet ledd (2018-loven er vedtatt og forventes å tre i kraft i 2019)

[407] Instruks av 31. august 2001 nr. 1012 om Etterretningstjenesten

vil også fungere som en rettssikkerhetsgaranti, samt at kravet også vil ivareta informasjonssikkerheten i et personvernperspektiv ytterligere.

Gjennomføringen av personkontroll, vurderingsgrunnlaget for sikkerhetsklareringen m.m. er utførlig regulert i sikkerhetsloven og tilhørende forskrifter. Departementet foreslår ingen endringer knyttet til disse.

Departementet foreslår imidlertid at det stilles som vilkår at personer som skal arbeide eller tjenestegjøre i Etterretningstjenesten må være norsk statsborger. Dette vil være en kodifisering av gjeldende praksis. Etterretningstjenesten skal innhente informasjon om *fremmed* makt. Det vil derfor kunne være problematisk, både av sikkerhetshensyn og hensyn til Etterretningstjenestens tillit, at personer som ikke innehar norsk statsborgerskap arbeider eller gjør tjeneste i Etterretningstjenesten. Etterretningstjenestens oppdrag er å ivareta norske interesser, en særlig tilknytning til en annen stat som statsborgerskap utgjør kan også gjøre at personen ikke utviser den fulle lojalitet til tjenestens oppdrag som er nødvendig. Innehar personen dobbelt statsborgerskap, hvor ett av disse er norsk, vil dette som den klare hovedregel utelukke en ansettelse eller oppdrag for tjenesten. I helt spesielle unntakssituasjoner bør loven likevel ikke hindre dette, etter en særskilt vurdering og forutsatt at kravet om sikkerhetsklarering og øvrige vilkår er oppfylt.

Departementet vil presisere at forslaget til bestemmelse ikke omfatter oppdragstakere og kilder. Sikkerhetsloven vil heller ikke komme til anvendelse for disse personkategoriene. Departementet foreslår følgende lovforslag:

§ 11-2 *Sikkerhetsklarering*

Enhver som gjør arbeid eller tjeneste i Etterretningstjenesten skal være norsk statsborger, og skal være sikkerhetsklarert for STRENGT HEMMELIG.

Sjefen for Etterretningstjenesten kan for særskilte stillinger med lavere klareringsbehov bestemme at personellet skal være sikkerhetsklarert for HEMMELIG.

14.6 Beredskap

14.6.1 Innledning

Forsvaret har egne beredskapsplaner blant annet for å ivareta installasjoner, personell og evne til å utøve sine oppgaver i alvorlige krisesituasjoner eller væpnet konflikt. Etterretningstjenesten skal i hele krise- og konfliktspekteret kunne produsere etterretninger som gir overordnede militære og politiske myndigheter grunnlag for å håndtere konflikten i henhold til nasjonale målsettinger, understøtte militære etterretningsbehov, samt bidra til NATOs fellesforsvar. Departementet har vurdert om det er hensiktsmessig å innta en egen bestemmelse i lovforslaget knyttet til Etterretningstjenestens beredskap.

14.6.2 Gjeldende rett

Det følger av E-instruksen[408] § 6 at Etterretningstjenesten skal utarbeide og vedlikeholde beredskapsplaner basert på Forsvarets beredskapsplanverk, og kunne opprettholde de spesielle krav til sikkerhet og konfidensialitet:

[408] Instruks av 31. august 2001 nr. 1012 om Etterretningstjenesten

Etterretningstjenesten skal utarbeide og vedlikeholde beredskapsplaner basert på Forsvarets beredskapsplanverk.

Tjenesten skal være i stand til å opprettholde de spesielle krav til sikkerhet og konfidensialitet som er en forutsetning for at den skal kunne ivareta sine oppgaver.

Bestemmelsen har i praksis medført at Etterretningstjenesten har implementert sikkerhetstiltak ut over de som følger av sikkerhetsloven, samt nødvendiggjort unntak fra enkelte regelverk og ordninger som ellers gjelder i Forsvaret for å unngå unødvendig spredning av særlig sensitiv informasjon.

14.6.3 Departementets vurdering

Departementet vurderer at det bør fremgå av loven at Etterretningstjenesten skal ivareta egen beredskap i tilfelle krise eller væpnet konflikt. Det bør synliggjøres i lovteksten at Etterretningstjenesten skal utarbeide og vedlikeholde beredskapsplaner som blant annet skal inneha tiltak som skal sikre at tjenestens informasjon og systemer ikke kommer under kontroll av uvedkommende i tilfellet krise eller væpnet konflikt, selv om dette allerede følger av det generelle planverket for Forsvaret. Utarbeidelsen av beredskapsplaner må nødvendigvis basere seg på Nasjonalt beredskapssystem og Forsvarets operative planverk. Bestemmelsen vil være en videreføring av gjeldende rett.

Departementet foreslår følgende lovtekst:

§ 11-3 *Beredskap*

Etterretningstjenesten skal utarbeide og vedlikeholde beredskapsplaner, herunder forberedte tiltak for å sikre at Etterretningstjenestens informasjon og systemer ikke skal komme under kontroll av uvedkommende i krise eller væpnet konflikt, basert på Nasjonalt beredskapssystem og Forsvarets operative planverk.

14.7 Etterretningstjenestens arkiver, informasjonssystemer og etterretningsregistre

14.7.1 Innledning

Informasjonssikkerhet omfatter både tekniske og organisatoriske tiltak for å fremme en tilfredsstillende beskyttelse av opplysninger med hensyn til konfidensialitet, integritet og tilgjengelighet. *Konfidensialitet* skal sikre at informasjonen ikke blir gjort tilgjengelig for uvedkommende, *integritet* innebærer at informasjon ikke endres utilsiktet eller av uvedkommende, og *tilgjengelighet* stiller krav om at informasjonen er tilgjengelig for rettmessige brukere. Departementet vurderer at gjeldende regler om Etterretningstjenestens arkiver, informasjonssystemer og etterretningsregistre bør videreføres. Dette vil utdypes i det følgende.

14.7.2 Gjeldende rett

Gjeldende etterretningstjenestelov § 5 første ledd lyder:

Informasjon som innhentes eller utarbeides av Etterretningstjenesten, skal systematisk ordnes i arkiv som skal være betryggende sikret og utilgjengelig for andre enn tjenestens egne embeds- og tjenestemenn med tjenstlig behov for tilgang og personer som er satt til å føre kontroll eller tilsyn med tjenestens virksomhet.

Bestemmelsen har både et sikkerhetsperspektiv og et arkivperspektiv. Forholdet mellom denne bestemmelsen og arkivloven har blant resultert i at Etterretningstjenestens arkivalia ikke er underlagt de alminnelige reglene om avlevering og bortsetting til Riksarkivet.

14.7.3 Departementets vurdering

Som beskrevet i høringsnotatet punkt 12.2 foreslås det at personopplysningsloven 2000 ikke lenger skal få anvendelse for Etterretningstjenestens virksomhet når ny lov om Etterretningstjenesten trer i kraft. Som det fremgår av drøftelsen foreslår departementet likevel langt på vei å ivareta de grunnleggende personopplysningsprinsippene fullt ut.

Kravet om informasjonssikkerhet som følger av den alminnelige *personopplysnings*lovgivningen foreslås videreført i ny etterretningstjenestelov. Informasjonssikkerhet i et *sikkerhet*sperspektiv reguleres i dag av sikkerhetsloven og informasjonssikkerhetsforskriften. Det foreslås ikke å gjøre noe endring i dagens rettstilstand.

Av pedagogiske grunner og hensynet til et helhetlig regelverk foreslår departementet likevel at det oppstilles særskilte krav til informasjonssikkerhet for tjenestens arkiver, informasjonssystemer og etterretningsregistre. Pliktene bør gjelde uavhengig av om arkivet, systemet eller registeret er et manuelt/fysisk eller et elektronisk arkiv. Sikringstiltakene må tilpasses arkivets karakter og sikkerhetsgradering. Bestemmelsen har også til hensikt å videreføre etterretningstjenesteloven § 5 om at arkivene til Etterretningstjenesten skal være under tjenestens faktiske kontroll. Avleveringsplikten mv til Riksarkivet kommer som en følge av dette ikke til anvendelse. Dette er en videreføring av gjeldende rett.

Unntak for personell som er autorisert og har tjenstlig behov følger i dag av sikkerhetsloven[409] § 5-4 første ledd. Bestemmelsen vil således ikke medføre noe endring på området enn det som allerede gjelder. At Etterretningstjenestens arkiver, informasjonssystemer og etterretningsregistre også skal være tilgjengelig for personer som er satt til å føre kontroll og tilsyn med Etterretningstjenesten medfører heller ingen rettslig endring i dagens regelverk, se kapittel 14.3 om taushetsplikt. Tilgjengelighetskravet vurderes også til å ytterligere kunne ivareta det grunnleggende personopplysningsvern prinsippet om integritet, konfidensialitet og tilgjengelighet.

Departementet foreslår følgende lovforslag:

§ 11-4 *Etterretningstjenestens arkiver, informasjonssystemer og etterretningsregistre*
Etterretningstjenestens arkiver, informasjonssystemer og etterretningsregistre skal være betryggende sikret og utilgjengelig for andre enn eget autorisert personell med tjenstlig behov for tilgang og personer som er satt til å føre kontroll og tilsyn med Etterretningstjenesten.

14.8 Informasjonsplikt og innsyn

14.8.1 Innledning

Lovfestet rett til informasjon om behandling av personopplysninger er utledet av grunnprinsipper i personopplysningsvernet. Retten innebærer i korte trekk at enhver *i*

[409] Loven ble vedtatt av Stortinget den 27. februar 2018, men vil ikke tre i kraft før i 2019 etter at tilhørende forskrifter er vedtatt.

utgangspunktet har rett til å vite hva private foretak og offentlige etater behandler av informasjon om seg selv. Dette gjelder imidlertid ikke uten unntak. Departementet har vurdert hvordan de motstående hensyn bør avveies og hvordan dette bør reguleres i lovforslaget her. Dette vil utdypes i det følgende.

14.8.2 Gjeldende rett

Innsynsrettprinsippet fremkommer ikke direkte av ordlyden i EMK, men er forutsatt i EMDs praksis for å ivareta vilkåret om *effektive rettsmidler*. Dette behandles nærmere i høringsnotatet punkt 4.3.

Reglene om informasjon om behandling av personopplysninger følger av personopplysningsloven 2000 kapittel III.[410] Personopplysningsloven av 2000 § 18 lovfester den grunnleggende retten til innsyn, mens de resterende bestemmelsene i kapittelet regulerer behandlingsansvarliges informasjonsplikt, hvordan informasjon skal gis, samt unntak fra innsyn- og informasjonsplikten. Innsynsretten gir den registrerte rett til å be om innsyn i hvilke opplysninger virksomheten behandler om vedkommende, og hvilke sikkerhetstiltak virksomheten har rundt bruken av opplysningene. Prinsippene om innsynsrett og informasjonsplikt er tilnærmet uendret videreført i ny personvernforordning artikkel 13, 14 og 15.[411]

Innsynsretten og informasjonsplikten som gjelder i den alminnelige personvernlovgivningen er imidlertid, etter en avveining opp mot andre hensyn, avgrenset til visse typer opplysninger, jf. personopplysningloven 2000 § 23. Retten til innsyn og behandlingsansvarliges informasjonsplikt er blant annet avgrenset mot opplysninger som «om de ble kjent, ville kunne skade rikets sikkerhet, landets forsvar eller forhold til fremmede makter eller internasjonale organisasjoner», jf. alternativ a i § 23 første ledd. Bestemmelsen tar sikte på å avklare forholdet til sikkerhetslovens bestemmelser som pålegger å hindre at uvedkommende får tilgang til sikkerhetsgraderte opplysninger. Unntaket fra innsynsretten og informasjonsplikten er videreført i ny personopplysninglov 2018 § 16 første ledd bokstav a som er gitt med hjemmel i personvernsforordningen artikkel 23 nr. 1 a) - c).

14.8.3 Departementets vurdering

Departementet foreslår å videreføre begrensingen i innsynsretten som er gitt i personopplysningsloven 2000 § 23. Bakgrunnen for dette er at informasjonen Etterretningstjenesten behandler i hovedsak omhandler sensitive forhold av betydning for rikets sikkerhet, og at informasjonen i all hovedsak er sikkerhetsgradert.

Ved vedtakelse av ny politiregisterlov i 2010 ble det for PSTs vedkommende fastsatt en bestemmelse som unntar PSTs arkiver og registre fra innsyn og informasjonsplikt etter offentlighetsloven, se politiregisterloven § 66. Begrunnelsen for denne regelen gjør seg også, om ikke i desto større utstrekning, gjeldende for Etterretningstjenesten.[412] Blant annet forutsettes det også for Etterretningstjenestens virksomhet ved mottak av opplysninger fra

[410] Se nærmere om dette i punkt 12.3

[411] Personopplysningsloven av 2018 §§ 16 og 17 fastsetter unntak fra retten til innsyn og informasjon etter forskriften.

[412] Se Ot. prp. nr. 108 (2008-2009) punkt 17.4.1 s. 276-278 og punkt 17.4.3 s. 278-279

utlandet at avsender av opplysningene forventer av sikkerhetshensyn at det ikke gis innsyn i opplysningene, da disse som regel er gradert av utsteder. Selv om man unntaksvis i den enkelte sak kunne gitt innsyn til den registrerte, vil opplysninger fra flere saker kunne sammenholdes på en slik måte at opplysningene likevel røper sikkerhetsgradert informasjon slik som kilder, arbeidsmetoder eller samarbeid med utenlandske tjenester som kan medføre skade om opplysningene offentliggjøres eller kommer vedkommende i hende på annen måte.

En eventuell innsynsordning for opplysninger i Etterretningstjenesten ville mest sannsynlig ikke medføre en reell innsynsrett, idet unntakene fra innsyn på grunn av hensynet til rikets sikkerhet, kildevern og metodebruk ville komme til anvendelse i nærmest samtlige tilfeller. I så måte kan det også for Etterretningstjenestens vedkommende trekkes paralleller fra offentlighetsloven med tilhørende forskrifter, der innsyn fra Etterretningstjenestens dokumenter og journaler av samme grunn kan unntas i sin helhet, jf. § 9 tredje ledd i forskrift til offentlighetsloven. Det nevnes også at innsynsretten i ny personopplysningslov 2018 begrenser innsynsretten mot informasjon om nasjonale forsvars- og sikkerhetsinteresser, jf. § 16 første ledd bokstav a.

Departementet vurderer at den registrertes personvern vil være tilstrekkelig ivaretatt gjennom muligheten til å be EOS-utvalget om kontroll med henblikk på om en eventuell behandling av opplysninger er i samsvar med loven, jf. EOS-kontrolloven § 3 annet ledd.[413] Departementet foreslår å lovfeste klageretten av hensyn til den enkelte. At det opplyses om klageadgang har en rent pedagogisk funksjon.

Departementet foreslår, i tillegg til å videreføre dagens bestemmelser for innsynsrett og informasjonsplikt i ny etterretningstjenestelov, at Etterretningstjenesten unntas fra *meroffentlighetsprinsippet* i offentlighetsloven. På samme måte som for PST vil det etter departementets oppfatning ikke være noen hensiktsmessig sammenheng dersom Etterretningstjenesten er unntatt fra innsynsretten og informasjonsplikten, men likevel må behandle innsynsbegjæringer på bakgrunn av meroffentlighetsprinsippet. Av hensyn til regelharmonisering og kostnadseffektivitet foreslår derfor departementet å avgrense meroffentlighetsprinsippet mot Etterretningstjenestens virksomhet. Forslaget vil ikke medføre behov for lovendring i andre lover da både offentlighetsloven, forvaltningsloven og personverndirektivet åpner for å gjøre unntak fra retten til offentlig innsyn i særlovgivningen. Departementet foreslår følgende lovforslag:

§ 11-6 *Innsyn i opplysninger i Etterretningstjenesten*

Offentleglova gjelder ikke for innsyn i opplysninger som behandles av Etterretningstjenesten etter loven her.

Av sikkerhetsmessige grunner har en person ikke rett til innsyn i

a. etterretningsinformasjon som Etterretningstjenestens behandler eller har behandlet om vedkommende, eller
b. om Etterretningstjenesten behandler eller har behandlet, herunder utlevert til andre, etterretningsinformasjon om vedkommende.

Begjæringer om innsyn som nevnt i annet ledd skal avvises. Enhver som mener at Etterretningstjenesten har begått urett mot seg, kan klage til EOS-utvalget etter EOS-kontrollovens bestemmelser.

[413] EMD konkluderte i tråd med denne forståelsen knyttet til en lignende ordning i Storbritannia i *Big Brother Watch m. fl. mot Storbritannia* avsagt den 13. september 2018, se særlig s. 151. Dommen er i skrivende stund ikke rettskraftig.

14.9 Underretning

14.9.1 Innledning

Det ligger i sakens natur at Etterretningstjenesten ikke kan informere etterretningsmål eller andre om at informasjonsinnhenting skal finne, eller finner sted. Også etterhåndsnotifikasjon er problematisk fordi dette som den store hovedregel vil bidra til å avsløre Etterretningstjenestens innhentingsaktivitet, metodebruk og kapasiteter. Det finnes ingen bestemmelse i gjeldende etterretningstjenestelov som direkte regulerer spørsmålet om underretning. Departementet mener det er behov for en slik bestemmelse i ny lov.

14.9.2 Gjeldende rett

Når Etterretningstjenesten innhenter informasjon skjer det nesten utelukkende uten at personen som innhentingen retter seg mot er kjent med det. Det samme gjelder for personer som kan bli berørt av innhentingen. Det informeres ikke om innhentingstiltak, uavhengig av om disse skjer ved bruk av åpne kilder eller ved fordekte metoder, og verken før eller etter bruken av metoden. De som informasjonsinnhentingen angår vil derfor ikke ha mulighet adgang til å uttale seg i forkant av innhentingen. Etterretningstjenesten informerer heller ikke den enkelte om at den behandler opplysninger om denne.

Adgangen til å unnlate underretning er hjemlet i personopplysningsloven 2000 § 23. I tillegg er Etterretningstjenestens personell underlagt taushetsplikt som, ved brudd, medfører strenge straffer, se punkt 14.3 og 14.4. Taushetspliktsreglene gjør ikke eksplisitt unntak som åpner for å gi underretning. Det er heller ikke praksis for å innfortolke en ulovfestet adgang til å gjøre unntak fra taushetspliktbestemmelsene for å kunne underrette de det gjelder.

I flere dommer har EMD lagt til grunn at statene har en relativ vid skjønnsmargin på dette området. EMD har i den forbindelse slått fast at unnlatelse av underretning når den skjulte innhentingen har opphørt ikke i seg selv er et uforholdsmessig inngrep i EMK i artikkel 8, se for eksempel *Klass mot Tyskland*, hvor EMD uttalte følgende:[414]

> "In the opinion of the Court, it has to be ascertained whether it is even feasible in practice to require subsequent notification in all cases.
>
> The activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures. Subsequent notification to each individual affected by a suspended measure might well jeopardise the long-term purpose that originally prompted the surveillance. Furthermore, as the Federal Constitutional Court rightly observed, such notification might serve to reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents. In the Court`s view, in so far as the "interference" resulting from the contested legislation is in principle justified under Article 8 para. 2 (art. 2-2) (see paragraph 48 above), the fact of not informing the individual once surveillance has ceased cannot itself be incompatible with this provision since it is this very fact which ensures the efficacy of the "interference."

[414] *Klass m. fl. mot Tyskland* avsagt 6. september 1978, avsnitt 58

14.9.3 Departementets vurdering

Det foreslås å lovregulere dette spørsmålet uttrykkelig for Etterretningstjenesten i ny lov. Den grunnleggende rettigheten om at en selv bestemmer hvem som skal kunne behandle ens egne personopplysninger vil i all hovedsak i et etterretningsperspektiv settes til side. Dette kan også gjøres som ledd i andre offentlige etaters virksomhet. Forskjellen er imidlertid at behandlingen av personopplysninger med et etterretningsformål ikke bare skjer uten samtykke, men også uten at personen har eller har krav på kjennskap til behandlingen.

En underrettelse før eller under tidsperioden der Etterretningstjenesten innhenter og/eller behandler opplysninger om en person vil kunne avsløre "fields of operation of the intelligence services" jf. sitatet fra *Klass mot* Tyskland over, og kan avsløre metoder Etterretningstjenesten benytter. Dette vil igjen medføre at personen selv kan endre sin atferd slik at tjenesten ikke får nødvendig informasjonstilfang for å løse sitt oppdrag. Underretningen kan også skade informasjonstilfanget ytterligere ved at opplysninger om Etterretningstjenestens innhenting om et miljø eller organisasjon, aksessmuligheter og nærmere metodebruk blir kjent for også andre som personen har i sin bekjentskapskrets. De samme hensyn kan legges til grunn etter at innhentingen eller behandlingen av opplysninger er avsluttet. En underretningsplikt for tjenesten vil også kunne ha alvorlige sikkerhetspolitiske konsekvenser. En plikt til å underrette personer som arbeider for fremmed makt vil kunne medføre uopprettelige skader i norske myndigheters relasjon til den andre nasjonen. Videre vil en underrettelsesplikt kunne medføre at tjenesten må innhente ytterligere informasjon om en person i utlandet og behandle informasjon om denne for å finne kontaktinformasjon for å gi selve underrettelsen.

Departementet deler Justis- og beredskapsdepartementets forståelse om at underrettelsesretten ikke er en absolutt rettighet etter EMK artikkel 8. Justisdepartementet uttaler at:[415]

> «Departementet legger til grunn at spørsmålet om underretning til siktede fortsatt bare inngår som et moment i forholdsmessighetsvurderingen, hvor det sentrale er om det foreligger tilfredsstillende og effektive garantier mot misbruk av metodene.»

Dette er også i overensstemmelse med etablert praksis for de fleste sammenlignbare utenlandske etterretningstjenester.

Departementet finner etter dette at gjeldende ordning og en kodifisering av denne, ikke vil være i strid med EMK artikkel 8. Det vises for øvrig til høringsnotatet kapittel 4 der menneskerettighetenes krav er drøftet mer i detalj, og der spørsmålet om hvordan manglende underrettelse forholder seg til kravet til effektive rettsmidler etter EMK artikkel 13 vurderes.

Departementet foreslår følgende lovforslag:

§ 11-8 *Underretning*

Den som har vært gjenstand for informasjonsinnhenting som kan innebære inngrep i dennes menneskerettigheter, har ikke krav på underretning om inngrepet.

[415] Prop. 68 L (2015-2016) punkt 6.10.6.1 s. 80

14.10 Skjerming mot eksponering av ansatte, kilder, kapasiteter, metoder og operasjoner

14.10.1 Innledning

Etterretningstjenesten søker så langt mulig å skjerme personell, kilder, kapasiteter, metoder og operasjoner mot eksponering som kan gå på bekostning av sikkerheten og/eller operasjonelle forhold. I praksis skjer dette blant annet ved at man søker å unngå å vise tilknytningen til Etterretningstjenesten, norske myndigheter og Norge.

Departementet har vurdert om det bør lovfestes adgang til bruk av virkemidler for skjerming, herunder bruk av dekkstrukturer og fiktive identiteter og dokumenter mv. I det følgende redegjøres det for behovet for slike regler, og for departementets vurdering av og forslag til lovbestemmelse.

14.10.2 Behovet for særlige regler om skjerming mot eksponering

Etterretningstjenestens informasjonsinnhentingsarbeid kan innebære særlig høy risiko for operativt personell og deres kilder. For eksempel kan det være tvingende nødvendig å reise under dekke av å være en annen person av operasjons- og/eller sikkerhetsmessige hensyn. Eksponering av identiteten til operativt personell og kilder, eller påstander om at bestemte personer innehar slike roller, vil kunne stille personene i en særlig sårbar situasjon, og kan være forbundet med risiko for de involverte. Eksponering vil også kunne kompromittere tidligere og pågående operativ virksomhet som disse har vært involvert i. I denne sammenheng er det et poeng at risikoen ved eksponering løper lengre enn den enkelte operasjons varighet, i det selve tilknytningen til Etterretningstjenesten kan utgjøre en risiko for disse. Et annet moment er at utilstrekkelig skjerming av ansatte, kilder mv. vil gå hardt ut over rekrutteringen til Etterretningstjenesten.

Dersom aktører som besitter eller har tilgang til etterretningsrelevant informasjon har kjennskap til hva som er Etterretningstjenestens prioriterte innhentingsmål og metodebruk vil disse personene kunne endre sin atferd og dermed unndra seg Etterretningstjenestens søkelys. Kjennskap til tjenestens innhentingsmål, metoder, kilder og kapasiteter kan også skade informasjonstilfanget ytterligere ved at opplysningene blir offentlig kjent eller kjent for andre som personen har i sin bekjentskapskrets.

14.10.3 Gjeldende rett

Offentlige rapporteringsplikter kan i flere tilfeller utfordre Etterretningstjenestens skjermingsbehov. Det er for eksempel plikt til å rapportere til Tolletaten dersom man bringer med seg valuta tilsvarende kr 25 000 til eller fra Norge. Bestemmelsen er begrunnet i hensynet til å bekjempe hvitvasking.

«A-ordningen» er en samordnet måte for arbeidsgiver å rapportere opplysninger om inntekt og ansatte til NAV, Statistisk sentralbyrå og Skatteetaten. Opplysningene skal rapporteres minst en gang i måneden. Opplysningene distribueres også videre etter samtykke eller hjemmel i lov til UDI, Statens lånekasse, banker m.m. Rapporteringskravet innebærer blant annet plikt til å rapportere om ansatte som har arbeidet i utlandet i en periode. Rapporteringsplikten er ikke etter sin ordlyd i samsvar med taushetspliktbestemmelsen i sikkerhetsloven§ 12 (i sikkerhetsloven 2018 er dette § 5-4 annet ledd), og må følgelig tolkes

i lys av kravet om at sikkerhetsgradert informasjon ikke skal offentliggjøres til personer uten nødvendig sikkerhetsklarering og autorisasjon. I tillegg er løsningen elektronisk, og oppfyller ikke kravene til behandling av sikkerhetsgradert informasjon etter informasjonssikkerhetsforskriften.

I tillegg vil krav om skattemessig innrapportering av vederlag til Etterretningstjenestens kilder være problematisk i et skjermingsperspektiv.

14.10.4 Departementets vurdering

Departementet understreker at skjerming mot eksponering av Etterretningstjenestens innhentingsvirksomhet er en avgjørende forutsetning for å i det hele tatt å kunne drive etterretning. På denne bakgrunn har departementet vurdert at dagens praksis hva gjelder å ta kontroll, modifisere eller utplassere elektronisk utstyr for å hemmeligholde og gjennomføre Etterretningstjenestens oppgaver bør lovfestes. Departementet vil innledningsvis understreke at det ikke er tale om å gi en innhentingshjemmel – disse følger av lovforslagets kapittel 3 – men å tydeliggjøre at Etterretningstjenesten kan treffe visse forberedende tiltak med sikte på innhenting eller på annen måte skjerme tjenestens operasjoner og operasjonenes tilknytning til Norge og Etterretningstjenesten.

Grunnet hensynet til å skjerme menneskelige kilder, da disse i mange tilfeller løper en stor risiko ved å bistå Etterretningstjenesten, foreslår departementet at vederlag som overstiger utlegg kilden måtte ha i forbindelse med oppdraget til tjenesten ikke bør anses som skattepliktig inntekt etter norsk rett. Vederlaget bør heller ikke inngå i grunnlag for beregning eller avkortning av sosiale ytelser eller lignende. Begrunnelsen for dette er at kilder ofte har økonomiske motiver for å bidra med informasjon. Dersom vederlag basert på oppdrag for Etterretningstjenesten skal innrapporteres vil dette medføre at kildeforholdet vanskelig kan holdes skjult. Utfordringen dukker bare opp for den delen av vederlaget som overstiger eventuelle utlegg personen måtte ha som en følge av at han eller hun bistår Etterretningstjenesten. For eksempel vil kostanden ved transport og overnatting i denne forbindelse ikke være å anse som skattepliktig inntekt etter den alminnelige skattelovgivningen.

Ved utformingen av lovforslaget har departementet lagt tung vekt på at offentlige rapporteringsplikter kan si noe om *hvor* Etterretningstjenesten utøver sine aktiviteter, tjenestens *kapasiteter* og *ressurser* ved å se på antall reiser og reisedøgn. Departementet understreker at Etterretningstjenesten må forholde seg til gjeldende regler om skattelegging av lønn til ansatte og andre offentligrettslige krav. Tjenesten har i dag etablert ulike løsninger som ivaretar skjermingshensynet samtidig som gjeldende etater får ivaretatt sine oppgaver. Dersom det ikke er mulig å ivareta de to etatenes oppgaver, er departementet av det syn at skjermingshensyn i de fleste tilfeller må veie tyngre enn hensynet til offentlige rapporteringsplikter eller andre oppgaver.

Departementet anser det som ønskelig at tjenesten kan utøve en forsvarlig virksomhet uten at dette bryter med plikter i annen regulering. På denne bakgrunn foreslår departementet at Kongen i statsråd bør gis hjemmel til å fastsette nærmere bestemmelser som avviker fra bestemmelser i annen lovgivning dersom det er strengt nødvendig for å skjerme Etterretningstjenestens ansatte, kilder, kapasiteter, metoder og operasjoner mot risiko for offentlig eksponering eller kompromittering overfor annen stat. En slik delegert og avgrenset lovgivningskompetanse er motivert av behovet for særlige regler som unntar tjenesten fra

ulike rapporteringsplikter mv, og fleksibilitet til å følge fremtidige teknologiske og samfunnsmessige utviklingstrekk. Det presiseres at kompetansen etter forslaget ikke kan delegeres videre.

Departementet foreslår følgende lovbestemmelse for å ivareta tjenestens behov for skjerming:

§ 11-5 *Skjerming mot offentlig eksponering av ansatte, kilder, kapasiteter, metoder og operasjoner*

Etterretningstjenesten skal være i stand til å opprettholde de spesielle krav til sikkerhet og konfidensialitet som er nødvendig for å kunne ivareta sine oppgaver.

Det kan benyttes dekkstrukturer og uriktige, falske eller villedende identiteter, dokumenter og opplysninger, samt tas kontroll over, modifiseres eller utplasseres elektronisk utstyr, for å hemmeligholde og gjennomføre Etterretningstjenestens operasjoner.

Bestemmelser i annen lov om plikt til å rapportere opplysninger gjelder ikke for vederlag som Etterretningstjenesten yter til kilder og oppdragstakere som ikke er ansatt i Etterretningstjenesten. Slike vederlag og betalinger skal heller ikke for mottaker regnes som skattepliktig inntekt eller inngå i grunnlag for beregning eller avkortning av sosiale ytelser eller lignende.

Kongen i statsråd kan gi bestemmelser som fraviker bestemmelser i annen lov, herunder lovbestemte krav om rapportering av informasjon til offentlige registre, i den utstrekning det er strengt nødvendig for å skjerme Etterretningstjenestens ansatte, kilder, kapasiteter, metoder og operasjoner mot risiko for offentlig eksponering eller kompromittering overfor annen stat.

15 Straff

15.1 Straffebestemmelse

Lovutkastet fastsetter en rekke handlingsnormer av ulik karakter. Departementet har med utgangspunkt i prinsippene for kriminalisering vurdert i hvilken utstrekning overtredelser av disse handlingsnormene bør kunne straffes.[416]

Brudd på taushetsplikten etter § 11-1 kan ha store skadevirkninger for Etterretningstjenestens virksomhet og vil normalt være straffverdig. Departementet viser til omtalen av taushetsplikten i punkt 14.3 og 14.4. Alvorlige brudd på taushetsplikten bør derfor kunne møtes med en fengselsstraff av betydelig lengde. Mindre alvorlige overtredelser bør kunne straffes med bøter, eventuelt i kombinasjon med en kortere fengselsstraff. Departementet foreslår på denne bakgrunn en oppdeling i en vanlig og en grov overtredelse. Vanlig overtredelse skal etter lovutkastet § 12-1 første ledd kunne straffes med bot eller fengsel inntil 1 år eller begge deler. Grovt brudd skal etter annet ledd kunne straffes med fengsel inntil 6 år. Departementet foreslår at det ved avgjørelsen av om bruddet er grovt særlig skal legges vekt på graden av skyld og om bruddet har skadet Etterretningstjenestens virksomhet eller lett kunne ha ført til slik skade.

Det bør også fastsettes en straffetrussel for ødeleggelse eller manipulasjon av aktivitetslogger som nevnt i lovutkastet § 7-10. Aktivitetsloggene er sentrale for kontrollen med Etterretningstjenestens virksomhet, og ødeleggelse eller manipulasjon av loggene bør kunne møtes med en ikke ubetydelig fengselsstraff. Departementet foreslår derfor en strafferamme på bot eller fengsel inntil 1 år eller begge deler, se lovutkastet § 12-1 tredje ledd.

[416] Se for eksempel Ot.prp. nr. 90 (2003–2004) punkt 7.5 s. 88-93

Tilbydere som omfattes av tilretteleggingsplikten etter lovutkastet § 7-2, bør etter departementets syn kunne straffes for brudd på plikten. Det samme gjelder brudd på taushetsplikt etter lovutkastet § 7-3. Departementet mener at en strafferamme på bot eller fengsel inntil 6 måneder eller begge deler vil være tilstrekkelig, se lovutkastet § 12-1 fjerde ledd. Ved brudd på tilretteleggingsplikten vil det ofte kunne være aktuelt med foretaksstraff, jf. straffeloven §§ 27 og 28.

Departementet legger for øvrig til grunn at brudd på en rekke av handlingsnormene som oppstilles i loven, vil kunne straffes som tjenestefeil eller misbruk av offentlig myndighet etter straffeloven §§ 171 til 173. Dette gjelder for eksempel brudd på forbudet mot innhenting rettet mot personer som befinner seg i Norge (lovutkastet § 4-1) og forbudet mot industrispionasje (lovutkastet § 4-3). Departementet har derfor ikke sett behov for å innta ytterligere straffetrusler i lovutkastet.

Det følger av straffeloven § 21 at straffelovgivningen bare rammer forsettlige lovbrudd med mindre annet er bestemt. Departementet har vurdert om straffebestemmelsen også bør ramme uaktsomme overtredelser. Etter departementets syn tilsier straffverdighetsbetraktninger at også grovt uaktsomme brudd på taushetsplikten etter § 11-1 bør kunne straffes. Departementet ser derimot ikke behov for å gjøre unntak fra hovedregelen om forsett som skyldkrav for de andre overtredelsene som rammes av straffebudet.

Medvirkning vil kunne straffes i tråd med straffeloven § 15. Forsøk på overtredelser etter lovutkastet § 12-1 første, annet og tredje ledd vil kunne straffes i samsvar med straffeloven § 16. Forsøk på overtredelser etter lovutkastet § 12-1 fjerde ledd vil på grunn av strafferammen ikke kunne straffes.

Overtredelser som kan straffes etter lovutkastet § 12-1, vil etter omstendighetene også rammes av strengere straffebestemmelser. Departementet viser særlig til straffeloven kapittel 17 om vern av Norges selvstendighet og grunnleggende nasjonale interesser. Departementet foreslår at lovutkastet § 12-1 i så fall ikke skal anvendes sammen med det strengere straffebudet i idealkonkurrens.

Departementet foreslår følgende straffebestemmelse:

§ 12-1 *Straff*

Den som forsettlig eller grovt uaktsomt bryter taushetsplikt etter § 11-1, straffes med bot eller fengsel inntil 1 år eller begge deler, hvis ikke forholdet går inn under en strengere straffebestemmelse.

Grovt brudd på taushetsplikten straffes med fengsel inntil 6 år. Ved avgjørelsen av om bruddet er grovt skal det særlig legges vekt på graden av skyld og om bruddet har skadet Etterretningstjenestens virksomhet eller lett kunne ha ført til slik skade.

Den som ødelegger eller manipulerer aktivitetslogger som nevnt i § 7-10, straffes med bot eller fengsel inntil 1 år eller begge deler, hvis ikke forholdet går inn under en strengere straffebestemmelse.

Den som overtrer bestemmelser gitt i eller i medhold av §§ 7-2 eller 7-3, straffes med bot eller fengsel inntil 6 måneder eller begge deler, hvis ikke forholdet går inn under en strengere straffebestemmelse.

Grove brudd på taushetsplikten kan som nevnt ha store skadevirkninger for Etterretningstjenestens virksomhet. Departementet mener at det i etterforskningen av grove brudd etter lovutkastet § 12-1 annet ledd kan være nødvendig med bruk av skjulte tvangsmidler som i utgangspunktet er forbeholdt handlinger som kan straffes med fengsel i

10 år eller mer. Dette gjelder skjult kameraovervåking på privat sted (straffeprosessloven § 202 a), visse former for teknisk sporing (straffeprosessloven § 202 c), kommunikasjonsavlytting (straffeprosessloven § 216 a) og dataavlesing (straffeprosessloven § 216 o). Departementet foreslår derfor følgende lovendring:

I lov 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker skal «lov om Etterretningstjenesten § 12-1 annet ledd» føyes til i opplistingen av bestemmelser i §§ 202 a annet ledd bokstav b, 202 c første ledd, 216 a første ledd bokstav b og 216 o første ledd bokstav b.

15.2 Straffrihet for lovlige tjeneste- eller oppdragshandlinger

Departementet har vurdert om det bør gis en lovbestemmelse som tydeliggjør at ansatte i og kilder eller oppdragstakere for Etterretningstjenesten ikke kan straffes for lovlige tjeneste- eller oppdragshandlinger.

Ansatte i og kilder eller oppdragstakere for Etterretningstjenesten må fra tid til annen handle i strid med den objektive gjerningsbeskrivelsen i straffebestemmelser som ledd i lovlig tjeneste- eller oppdragsutførelse. Et eksempel kan være plikten til å deklarere utførsel av større kontantbeløp. Slike *lovlige tjeneste- eller oppdragshandlinger* kan ikke straffes etter norsk rett. Dette antas etter gjeldende rett å følge av innhentingshjemmelen i etterretningstjenesteloven § 3, eventuelt supplert med offentlig myndighetsutøvelse som ulovfestet straffrihetsgrunn. Straffrihet kan også følge av *den alminnelige rettsstridsreservasjonen*, som innebærer at alle straffebud må leses med forbehold for situasjoner som det ikke har vært meningen å ramme med straff. Loven tolkes i slike tilfeller innskrenkende, det vil si at den forstås snevrere enn det en naturlig språklig forståelse av lovteksten (ordlyden) tilsier.[417]

En bestemmelse om straffrihet vil vanskelig kunne gi noe svar på hva som er en *lovlig* tjeneste- eller oppdragshandling. Det vil si at straffriheten vil avhenge av en nærmere vurdering av handlingens lovlighet med grunnlag i normer utenfor bestemmelsen selv, på samme måte som etter gjeldende rett. Formålet med en lovbestemmelse må derfor være å minne rettsanvenderen om at straffebud tidvis må tolkes innskrenkende. Det vil fremdeles være rettsanvenderne, i siste omgang domstolene, som må foreta den endelige avveiningen. Den kan derfor hevdes at en lovfesting vil ha liten rettslig betydning.

Man kan også problematisere hvorvidt en slik regel i etterretningstjenesteloven utilsiktet kan føre til antitetiske tolkinger av andre regelverk, der man ikke har en tilsvarende straffrihetsbestemmelse, men der man har lent seg på den alminnelige rettsstridsreservasjonen. Risikoen for dette forventes imidlertid ikke å være særlig stor.

Departementet mener gode grunner taler for at personer som opptrer i henhold til oppdrag fra myndighetene, ikke skal frykte personlig straffeforfølgelse for brudd på norsk regelverk. Forutsetningen må naturligvis være at oppdraget holdes innenfor det som er tillatt etter lovforslaget her. Også pedagogiske grunner taler for å synliggjøre at lovlige tjeneste- og oppdragshandlinger ikke kan straffes. En slik synliggjøring kan blant annet antas å virke positivt for Etterretningstjenestens evne til å rekruttere ansatte, kilder og oppdragstakere.

[417] Ot.prp. nr. 90 (2003–2004) punkt 14.3.5.3 side 214.

Departementet ber særskilt om høringsinstansenes syn på hvorvidt en bestemmelse om straffrihet bør tas inn i loven.

En bestemmelse om straffrihet for lovlige tjeneste- eller oppdragshandlinger kan plasseres i § 12-2 og utformes slik:

§ 12-2 *Straffrihet for lovlige tjeneste- eller oppdragshandlinger*
Ansatte i og kilder eller oppdragstakere for Etterretningstjenesten kan ikke straffes for lovlige tjeneste- eller oppdragshandlinger.

16 Ikrafttredelse og endringer i andre lover

16.1 Endringer i andre lover

16.1.1 innledning

I forbindelse med utarbeidelsen av lovutkastet har departementet foretatt en gjennomgåelse av enkelte andre lover med grensesnitt mot Etterretningstjenesten. Departementet foreslår på denne bakgrunn enkelte endringer i straffeloven, straffeprosessloven, ekomloven og EOS-kontrolloven.

16.1.2 Endring i straffeloven § 123 – offentliggjøring av identiteten til operativt personell og operative kilder

Departementet foreslår en endring i straffeloven § 123 som styrker det rettslige vernet mot offentliggjøring eller annen avsløring av identiteten til Etterretningstjenestens og PSTs personell og kilder.

Etterretningstjenesten søker så langt mulig å skjerme operativt personell og sine kilder. Dette skjer blant annet ved at man søker å unngå å vise knytningen til tjenesten, norske myndigheter og Norge. Hjemmel for skjermingstiltak er inntatt i lovforslaget § 11-5.

Dagens virkemidler for skjerming er likevel ikke tilstrekkelig til å sikre at identiteten til operativt personell og operative kilder forblir ukjent. Operativt personell, operative kilder og deres familier bør ikke utsettes for den risiko en identifisering kan innebære. Det foreligger derfor et sterkt og legitimt behov for et styrket strafferettslig vern mot at dette personellets virkelige identitet blir offentliggjort. Departementet understreker at behovet kun gjelder for operativt personell i og operative kilder for Etterretningstjenesten, og ikke for enhver person som er ansatt i eller har utført innhentingstjeneste for Etterretningstjenesten. Begrepene «operativt» og «operative» sikter til personer som er i aktiv tjeneste og deltar i eller kommer til å delta i sensitive etterretningsoperasjoner, og som ikke en gang for alle har avsluttet slik deltakelse.

Etter departementets vurdering gir ikke dagens regelverk tilstrekkelig mulighet til å sikre at identiteten til operativt personell eller kilder eller disse sine nærstående, ikke offentliggjøres. En persons identitet kan ikke på generelt grunnlag sikkerhetsgraderes etter sikkerhetsloven. En eventuell skjerming etter sikkerhetsloven er begrenset til informasjon om bestemte forhold eller operasjoner. Og selv om man skulle anse identitetsopplysningene som sikkerhetsgraderte, kommer sikkerhetslovens straffebestemmelse kun til anvendelse for personer i virksomheter som er underlagt loven.

Straffeloven § 123 lyder:

> Med bot eller fengsel inntil 3 år straffes den som uten aktverdig grunn offentliggjør, overleverer eller på annen måte avslører en hemmelig opplysning som kan skade grunnleggende nasjonale interesser som nevnt i § 121. Den som avslører en slik opplysning til en fremmed stat eller terrororganisasjon, anses ikke for å ha en aktverdig grunn.

Departementets utgangspunkt er at det er svært vanskelig å se at noen kan ha en «aktverdig grunn» til å avsløre opplysninger om identiteten til operativt personell i og operative kilder for Etterretningstjenesten. Departementet ser at bestemmelsen kan berøre ytringsfriheten, men mener at det for eksempel er fullt mulig å drive kritisk journalistikk uten å måtte *offentliggjøre identiteten* til slike enkeltpersoner. Departementet foreslår derfor en endring i straffeloven § 123 annet punktum som tydeliggjør at den som offentliggjør en hemmelig opplysning som gjelder operativt personell i og operative kilder for Etterretningstjenesten, ikke anses for å ha aktverdig grunn. Dersom en offentliggjøring helt unntaksvis skulle være vernet av ytringsfriheten, vil forholdet ikke kunne straffes fordi straffebestemmelser som kolliderer med Grunnloven vil måtte tolkes innskrenkende.[418]

Departementet viser for øvrig til at en offentliggjøring av identiteten til operative kilder og personell de facto også alltid vil innebære offentliggjøring til en fremmed stat eller en terrororganisasjon, som allerede er regulert i straffeloven § 123.

Selv om operativt personell i og operative kilder for PST i mindre utstrekning opererer i utlandet, ser departementet at de samme hensyn som tilsier en spesialbestemmelse i straffeloven for å beskytte operativt personell og operative kilder i Etterretningstjenesten, i vesentlig utstrekning også gjør seg gjeldende for tilsvarende personell i PST. Departementet foreslår derfor at bestemmelsen dekker angjeldende kategorier personell tilknyttet begge tjenestene.

Departementet ser at forslaget reiser vanskelige avveininger og ber særlig om høringsinstansenes synspunkter på dette.

Departementet foreslår følgende endring i straffeloven § 123 annet punktum:

> Den som avslører en slik opplysning til en fremmed stat eller terrororganisasjon*, eller som offentliggjør en slik opplysning om identiteten til operativt personell i eller operative kilder for Etterretningstjenesten eller Politiets sikkerhetstjeneste,* anses ikke for å ha en aktverdig grunn.

16.1.3 Endringer i lov om elektronisk kommunikasjon – mobilregulert sone

Departementet har under punkt 8.5.1 redegjort for Etterretningstjenestens innhenting av informasjon rettet mot personer eller virksomheter som opptrer på vegne av fremmed makt i Norge. Slik innhenting i Norge vil blant annet kunne medføre at Etterretningstjenesten må ta i bruk frekvenser i det elektromagnetiske frekvensspekteret som er tildelt andre.

Nasjonal kommunikasjonsmyndighet (Nkom) har ansvar for forvaltningen av det elektromagnetiske frekvensspekteret i Norge, og etter ekomloven[419] kapittel 6 er det de som fastsetter den nasjonale planen for forvaltningen av frekvensspekteret og tildeler frekvenser. Lovens hovedregel er at individuelle frekvenstillatelser ikke kan benyttes av andre enn innehaveren. Det er imidlertid gjort unntak fra denne hovedregelen i § 6-2 a, som omhandler

[418] Jf Ot.prp. nr. 90 (2003–2004) punkt 14.3.5.3 s. 214

[419] Lov om elektronisk kommunikasjon 4. juli 2003 nr. 83

mobilregulerte soner. Unntaksbestemmelsen gir politiet og Nasjonal sikkerhetsmyndighet (NSM) anledning til å ta i bruk frekvenser uten tillatelse fra Nkom på visse vilkår. Dersom vilkårene, som fremgår av straffeprosessloven, politiloven og sikkerhetsloven er oppfylt for henholdsvis politiet og NSM, kan det etableres en mobilregulert sone. En slik sone vil si et begrenset geografisk område der kommunikasjon i det elektroniske kommunikasjonsnettet til bruk for offentlig mobilkommunikasjon påvirkes eller hindres gjennom lovlig identifikasjonsfanging eller jamming. Departementet viser til Etterretningstjenestens behov for å kunne rette innhenting mot representanter for fremmed makt i Norge, hvilket tilsier at det vil være behov for å gjøre inngrep i radiokommunikasjonsforbindelser mellom mobilt brukerutstyr, eksempelvis en telefon eller en PC, og mobilnettet. Dette kan gjøres ved at det etableres falske basestasjoner som avslører mobiltelefonens identitet, og deretter eventuelt overtar kontakten mellom telefonen og nettilbyders basestasjon. Slike inngrep vil innebære at frekvenser som er tildelt andre tas i bruk.

I ekomloven § 6-2 a annet ledd pålegges politiet og NSM å varsle myndighetene uten ugrunnet opphold etter at frekvenser som er tildelt andre er tatt i bruk. Departementet foreslår at Etterretningstjenesten av tungtveiende sikkerhetsmessige grunner ikke pålegges en tilsvarende plikt. Fravær av varslingsplikt kan avhjelpes ved at tjenestens inngrep med stor sannsynlighet ikke vil forårsake noen form for skadelig interferens for øvrige brukere av mobilnettet. Skadelig interferens vil si interferens som alvorlig reduserer kvaliteten på, hindrer eller gjentatte ganger avbryter radiokommunikasjon som drives i samsvar med fastsatte krav, jfr. ekomloven § 1-5, punkt 10. Videre vil tiltakene som Etterretningstjenesten benytter seg av primært være identitetsfanging og målrettet innhenting, og ikke eksempelvis jamming. Sistnevnte vil si aktiv utsending av radiosignaler i den hensikt å hindre bestemte radiokommunikasjonssystemer eller deler av disse i å virke i et begrenset geografisk område. Dermed er det lite trolig at Etterretningstjenestens tiltak vil ha konsekvenser for andre sivile brukere i området eller for frekvensenes rettighetshavere. Det gjøres også oppmerksom på at Etterretningstjenesten alltid benytter seg av tekniske filtreringsmekanismer der dette er mulig, for å unngå å samle inn irrelevante data. Departementet understreker her at ekomloven § 6-2 a femte ledd gjelder tilsvarende for Etterretningstjenestens virksomhet. Bestemmelsen fastslår at bruken av mobilregulert sone skal skje på en måte som i minst mulig grad griper inn i og forstyrrer eksisterende frekvensinnehaveres rettigheter. Ved all bruk av mobilregulert sone vil konsekvensene for personvernet vurderes, og hensynet til å sikre samfunnets behov for uavbrutt elektronisk kommunikasjon vil være tungtveiende. Av denne grunn foreslår departementet at det inntas et kvalifiserende vilkår om at Etterretningstjenesten i *særskilte tilfeller* og i *korte tidsrom* kan ta i bruk frekvenser når dette er *strengt nødvendig* for å få innhentet informasjon etter ny § 4-2 første ledd. Det vil i den sammenheng måtte vurderes hvorvidt mindre inngripende midler kan tas i bruk, og sakens viktighet vil tillegges betydning. De øvrige vilkår for innhenting etter ny lov kapittel 5 må naturligvis også være oppfylt for at slik innhenting skal kunne iverksettes. Utover dette har EOS-utvalget full innsikt i denne delen av Etterretningstjenestens virksomhet, og vil kontrollere at personer i Norge under slik virksomhet ikke påføres urett av Etterretningstjenesten.

På denne bakgrunn foreslår departementet følgende lovtekst til nytt § 6-2 a første ledd siste punktum i ekomloven:

> Etterretningstjenesten kan i særskilte tilfeller og i korte tidsrom uten tillatelse fra eller varsel til myndigheten ta i bruk frekvenser som er tildelt andre når dette er et strengt nødvendig tiltak for

innhenting av informasjon rettet mot person eller virksomhet som omfattes av lov om Etterretningstjenesten § 4-2 første ledd.

Ekomloven § 6-2 a tredje ledd regulerer Forsvarets og politiets etablering av mobilregulert sone for øvingsformål. I bestemmelsens tredje punktum er det inntatt en egen begrensning som kun gjelder Forsvarets etablering av mobilregulert sone for øvingsformål. Slik aktivitet skal utelukkende foregå innenfor Forsvarets *permanente øvingsområder*. Gitt Etterretningstjenestens behov for å øve med teknisk utstyr i Norge, som er redegjort for i punkt 12.9.1, mener departementet at denne begrensningen hindrer tjenestens mulighet til å gjennomføre hensiktsmessig og realistisk øving. Hensynene bak begrensningen, som er å skjerme sivile brukere av mobilnettet fra eventuell skadelig interferens som følge av den mobilregulerte sonen, samt beskytte frekvensenes rettighetshavere fra inngrep, vil i svært liten grad gjøre seg gjeldende gitt innretningen av Etterretningstjenestens øving av slike tekniske kapasiteter. Øving vil foregå innenfor klart definerte og avgrensede områder, der sannsynligheten for å interferere med sivile brukere av mobilnettet er minimal. Den tekniske innretningen av øvelsen kan også gjøres på en slik måte at skadelig interferens unngås, og at inngrepet ikke medfører ulempe for frekvensenes rettighetshavere. Slike øvelser skal uansett godkjennes av Nkom, hvilket betyr at øvelser som ikke i tilstrekkelig grad evner å hindre skadelig interferens eller ulempe for frekvensenes rettighetshavere, vil bli avslått. På denne bakgrunn legger departementet til grunn at Forsvarets etablering av mobilregulert sone, på lik linje som for politiet, ikke bør avgrenses til permanente øvingsområder.

Departementet foreslår på denne bakgrunn å oppheve ekomloven § 6-2 a tredje ledd tredje punktum.

16.1.4 Endringer i EOS-kontrolloven

Departementet har under punkt 4.3.4.1 drøftet klageadgangen overfor EOS-utvalget som reguleres i EOS-kontrolloven § 5 annet ledd. Herunder er det drøftet om klageadgangen anses tilstrekkelig vid, særlig med henblikk på dagens begrensning som gjelder «personer som ikke er bosatt i riket og organisasjoner som ikke har tilhold her». På bakgrunn av redegjørelsen i kapittel 4, foreslår departementet følgende endring i § 5 femte ledd i EOS-kontrolloven:

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

Under punkt 4.3.6 har departementet videre vurdert EOS-utvalgets kompetanse til å sikre passende oppreisning der det er konstatert at en person er utsatt for en menneskerettighetskrenkelse av EOS-tjenestene i Norge. Evalueringsutvalget[420] konstaterte i sin gjennomgang av EOS-utvalgets kontroll med de hemmelige tjenestene i Norge, at problemstillingen reiser spørsmål av både prinsipiell og praktisk art, og at den følgelig burde vurderes som ledd i en helhetlig vurdering av det norske systemet. Departementet slutter seg til Evalueringsutvalgets konklusjon, men anser at kravet etter EMK artikkel 13 og relevant rettspraksis fra EMD til «appropriate relief», tilsier at EOS-utvalget bør kunne *uttale* seg om mulig erstatningsansvar i klagesaker mot tjenestene. Dette anses i vesentlig grad å kunne styrke klagernes mulighet til å søke om erstatning fra det offentlige der det er konstatert at tjenestenes overvåkningsmessige virksomhet har medført kritikk.

[420] Dokument 16 (2015-2016) punkt 31.4 s. 129

Departementet foreslår følgende endring i § 15 første ledd tredje punktum i EOS-kontrolloven:

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 for det offentlige overfor klageren.*

17 Økonomiske og administrative konsekvenser

17.1 Innledning

Bakgrunnen for revideringen av gjeldende lov om Etterretningstjenesten er behovet for å oppdatere regelverket i lys av den samfunnsmessige, rettslige og digitale utvikling som har funnet sted siden gjeldende lov ble vedtatt på slutten av 1990-tallet. Som en del av arbeidet med revisjon av loven utreder departementet hvordan Etterretningstjenestens tilgang til grenseoverskridende elektronisk kommunikasjon gjennom tilrettelagt innhenting bør lovreguleres. Etterretningstjenesten har ikke tilsvarende tilgang i dag. En eventuell etablering og drift av tilrettelagt innhenting vil, fordi dette vil være en nyvinning, være det tiltaket som foreslås i loven som vil kreve klart mest økonomiske ressurser. Det redegjøres særskilt for de økonomiske og administrative konsekvensene knyttet til dette i høringsnotatets punkt 11.16. Her omtales også utgiftene til domstolene og EOS-utvalget.

17.2 Økonomiske og administrative konsekvenser av forslaget

Med unntak av tilrettelagt innhenting forventes ikke lovforslaget å få administrative eller økonomiske konsekvenser av større betydning sammenlignet med gjeldende praksis. Enkelte deler av forslaget kan tenkes å få administrative virkninger. Her kan nevnes at departementet foreslår å lovfeste enkelte personelle og prosessuelle krav knyttet til Etterretningstjenestens metodebruk. Imidlertid legger departementet til grunn at lovforslaget i stor grad kodifiserer de prosedyrer og rutiner som allerede praktiseres i Etterretningstjenesten.

Departementet kan ikke utelukke at samvirket mellom tilrettelagt innhenting og allerede eksisterende informasjonskilder vil kunne få betydning for Etterretningstjenestens virksomhet for øvrig. Departementet utelukker ikke at tilrettelagt innhenting vil bidra til å avdekke flere utenlandske forhold av interesse for Etterretningstjenesten, og at andre metoder benyttes for å følge opp disse. Det er imidlertid vanskelig å forutsi hvordan samvirket mellom tilrettelagt innhenting og virksomheten for øvrig vil bli i praksis og hva dette vil bety for prioriteringen av Etterretningstjenestens arbeid.

17.3 Lovforslaget sett i sammenheng med den øvrige styrkingen av Etterretningstjenesten

Etterretningstjenestens bidrag til sivile myndigheter i form av informasjon og analyse er økende, og omfatter blant annet innsamling av informasjon om internasjonal terrorisme og om fremstilling og spredning av masseødeleggelsesvåpen. Videre krever økt usikkerhet i verdenssamfunnet, den teknologiske utviklingen og økt etterspørsel etter Etterretningstjenestens analyser ytterligere prioritering for å holde tjenesten relevant og i

stand til å utføre sine lovpålagte oppgaver. Det er blant annet disse forholdene som danner bakteppet for at Stortinget i 2016 vedtok en bevilgningsøkning på til sammen 370 mill. kroner for å modernisere tjenesten både teknologisk og kapasitetsmessig, og gjøre tjenesten i bedre stand til å håndtere dagens og fremtidens utfordringer.

Regjeringen har prioritert utviklingen av Etterretningstjenesten ytterligere i langtidsplanen for forsvarssektoren i perioden 2017–2020 for å kunne øke kapasitet, kompetanse og relevans innenfor tjenestens ansvarsområde. Prioriteringene omfatter ytterligere investeringer og en styrking av driften for å skape rom for ny teknologi, økt kapasitet innenfor innsamling og analyse, en satsing innenfor rombasert etterretning og overvåking og nødvendige utbedringer av infrastruktur. I den prioriteringen som regjeringen legger opp til i langtidsplanen er det også kapasiteter som systemet for tilrettelagt innhenting vil kunne dra nytte av, noe som reduserer det samlede økonomiske behovet i Etterretningstjenesten for innføringen.

Selv om lovarbeidet og bevilgningsøkningen ikke har direkte sammenheng, springer behovet for begge ut av de samme realiteter: fremtredende utviklingstrekk både nasjonalt og internasjonalt gjør det nødvendig å sikre at tjenesten er i stand til å utøve sitt oppdrag. Departementets siktemål har særlig vært å ajourføre lovgrunnlaget med de krav som følger av rettsutviklingen på særlig menneskerettighets- og personvernområdet.

17.4 Samfunnsmessige konsekvenser av forslaget

Departementet mener at de samfunnsmessige konsekvensene av lovforslaget i all hovedsak vil være positive. For det første anses det som en samfunnsmessig verdi i seg selv at statlige aktørers virksomhet har en sikker forankring i lov som er innenfor rammen av Grunnloven og menneskerettighetene. I forlengelsen av dette, og i lys av legalitetsprinsippet, er det klart at et tydelig lovgrunnlag er en forutsetning for myndighetenes virksomhet. Etterretningstjenestens handlingsrom er ikke større enn det de rettslige rammene tillater. Formålet med lovforslaget er å oppdatere regelverket i tråd med gjeldende krav på en måte som er tilstrekkelig fleksibelt til å holde tritt med samfunnsutviklingen i den grad det er mulig. Lovforslaget kan derfor ses på som et sikkerhetspolitisk så vel som juridisk verktøy som sikrer at Etterretningstjenesten kan utøve sin virksomhet innenfor klart definerte og lovmessige rammer.

Videre er Etterretningstjenesten avhengig av legitimitet og tillit i befolkningen. Manglende tillit vil kunne få negative konsekvenser for Etterretningstjenestens effektivitet og evne til å trygge norsk sikkerhet og ivareta norske interesser. Departementets anser at herværende lovforslag, og offentligheten og åpenheten rundt lovarbeidet, har vært og vil fortsette å være viktig for å ivareta befolkningens tillit til Etterretningstjenestens virksomhet. Lovreguleringen setter den norske befolkningen bedre i stand til å forstå tjenestens ansvarsområde og oppgaver. Dette anser departementet som en samfunnsnyttig konsekvens i seg selv.

I tillegg mener departementet at lovforslaget, lest i lys av omfattende forarbeider, skaper et klarere, samlet og mer uttømmende lovgrunnlag for Etterretningstjenesten, og således være et velegnet verktøy for de som skal forvalte regelverket. Dette gjelder særlig Etterretningstjenesten selv og EOS-utvalget.

17.5 Departementets vurdering

Departementet mener herværende lovforslag ikke medfører vesentlige økonomiske eller administrative konsekvenser utover de som kan knyttes til tilrettelagt innhenting.

18 Forslag til lovtekst

FORSLAG TIL LOV OM ETTERRETNINGSTJENESTEN

Kapittel 1. Formål, virkeområde og definisjoner

§ 1-1 *Formål*

Loven skal

a. bidra til å trygge Norges suverenitet, territorielle integritet, demokratiske styreform og andre nasjonale sikkerhetsinteresser, herunder forebygge, avdekke og motvirke utenlandske trusler mot Norge og norske interesser,
b. bidra til å trygge tilliten til og sikre grunnlaget for kontroll med Etterretningstjenestens virksomhet, og
c. sørge for at Etterretningstjenestens virksomhet utøves i samsvar med menneskerettighetene og øvrige grunnleggende rettsprinsipper og verdier i et demokratisk samfunn.

§ 1-2 *Virkeområde*

Loven gjelder for Etterretningstjenesten.

Loven gjelder også for andre personer og enheter for det tidsrom de er under kommando eller instruksjonsmyndighet av sjef Etterretningstjenesten.

Loven gjelder ikke etterretningsvirksomhet som gjennomføres av Etterretningstjenesten som ledd i en internasjonal operasjon med folkerettslig mandat, dersom etterretningsvirksomheten skjer for operasjonens formål og innhentet informasjon kun behandles av Etterretningstjenesten for formål som kan henføres til den internasjonale operasjonen.

Loven gjelder i fred, krise og væpnet konflikt.

§ 1-3 *Forholdet til folkeretten*

Loven gjelder med de begrensninger som er anerkjent i folkeretten eller følger av overenskomst med fremmed stat.

Etterretningstjenesten skal ikke gjennomføre eller medvirke til virksomhet som innebærer en reell risiko for at ufravikelige og andre grunnleggende menneskerettigheter krenkes.

§ 1-4 *Definisjoner*

I loven her menes med

1. Behandling av personopplysninger; enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, for eksempel innhenting, registrering, organisering, strukturering, lagring, tilpasning, eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring.
2. Bulk; informasjonssamlinger og datasett hvorav en vesentlig andel av informasjonen antas å være irrelevant for etterretningsformål.
3. Etterretningsformål; formål å ivareta en eller flere av Etterretningstjenestens oppgaver etter kapittel 3.
4. Etterretningsmål; objekt, person, virksomhet eller annet som informasjonsinnhentingen retter seg mot.
5. Kilde; person som kultiveres, rekrutteres eller føres av Etterretningstjenesten for å gjennomføre menneskebasert innhenting, eller person som utfører oppdrag for Etterretningstjenesten ved å tilrettelegge for menneskebasert innhenting. En organisasjon eller et miljø kan fungere som kilde inntil relevante enkeltpersoner innenfor organisasjonen eller miljøet er identifisert.

6. Kildeverifikasjon; innhenting og vurdering av informasjon for å fastslå hvorvidt en potensiell eller eksisterende kilde besitter eller kan skaffe tilgang til relevant informasjon for etterretningsformål, samt fastslå motivasjon, troverdighet og egnethet.
7. Modusselektor; et søkebegrep eller søkestreng som beskriver et bestemt mønster eller avgrensning, herunder handlingsmønster eller geografisk område.
8. Målrettet innhenting; systematisk arbeid for å finne informasjon knyttet til identifiserte etterretningsmål.
9. Målsøking; systematisk arbeid for å identifisere nye etterretningsmål.
10. Overskuddsinformasjon; informasjon som er uten selvstendig interesse for etterretningsformål.
11. Personopplysninger; enhver opplysning og vurdering som med enkle midler kan knyttes til en identifisert eller identifiserbar fysisk person.
12. Personselektor; en identifikator tilknyttet en bestemt person eller virksomhet, for eksempel et telefonnummer, en epostadresse eller et brukernavn på en gitt tjeneste.
13. Rådata; ubearbeidet eller automatisk bearbeidet informasjon i enhver form hvis etterretningsverdi ikke er vurdert.
14. Utlevering; enhver formidling av opplysninger, både skriftlig og muntlig, til mottaker utenfor Etterretningstjenesten som ikke utfører tjeneste eller oppdrag for Etterretningstjenesten.

Kapittel 2. Organisering, styring og kontroll

§ 2-1 *Nasjonal tjeneste*

Etterretningstjenesten er Norges nasjonale utenlandsetterretningstjeneste, og har et sektoroverskridende samfunnsoppdrag.

§ 2-2 *Organisasjon*

Etterretningstjenesten er organisatorisk en del av Forsvaret og kommandomessig underlagt forsvarssjefen.

§ 2-3 *Nasjonal kontroll*

Etterretningstjenesten skal være under norsk kontroll. Det skal sikres norsk kontroll med hvilken informasjon som gjøres kjent for utenlandske samarbeidspartnere.

§ 2-4 *Oppdragsstyring*

Departementet formulerer oppdrag, prioriterer sivile og militære etterretningsbehov og koordinerer etterretningsbehov fra berørte departementer. Den overordnede prioriteringen av oppdragene til Etterretningstjenesten fastsettes av departementet årlig i et prioriteringsdokument for nasjonale etterretningsbehov.

Departementet bestemmer prosedyrer for etterretningsbehov som ikke dekkes i prioriteringsdokumentet. Forsvarssjefen bestemmer prosedyrer for etterretningsbehov i Forsvaret som ikke dekkes i prioriteringsdokumentet.

§ 2-5 *Departementets styring og kontroll*

Departementet ivaretar politisk styring og kontroll med Etterretningstjenesten gjennom forsvarssjefen dersom annet ikke er fastsatt i loven her.

Departementets økonomi- og virksomhetsstyring ivaretas gjennom Koordineringsutvalget for Etterretningstjenesten (K-utvalget). Departementet kan opprette andre særlige fora og ordninger som sikrer nødvendig styring og kontroll.
Departementet fastsetter rapporteringsrutiner for ivaretakelse av styring og kontroll.

§ 2-6 *Varsling og rapportering*

Innenfor rammen av oppgavene etter kapittel 3 skal Etterretningstjenesten:

1. Varsle norske myndigheter om trusler og andre forhold som Etterretningstjenesten blir kjent med og som krever umiddelbar handling eller av andre årsaker er av tidskritisk natur.

2. Rapportere til norske myndigheter om utenlandske forhold av betydning for Norge og norske interesser.

Etterretningstjenesten skal varsle og rapportere til militære myndigheter i samsvar med forsvarssjefens bestemmelser, og til sivile myndigheter i samsvar med departementets bestemmelser.

Etter departementets nærmere bestemmelser kan Etterretningstjenesten varsle og rådgi norske og utenlandske juridiske og fysiske personer om trusler som faller inn under Etterretningstjenestens oppgaver etter kapittel 3. Utlevering av sikkerhetsgradert informasjon kan bare skje i den grad dette er strengt nødvendig og anses sikkerhetsmessig forsvarlig.

§ 2-7 *Saker som skal forelegges for departementets beslutning*

Etterretningstjenesten skal forelegge for departementets beslutning

a. Etablering av samarbeid og avtaler med utenlandske tjenester eller internasjonale organisasjoner.
b. Iverksettelse av særskilte etterretningsoperasjoner som kan reise politiske problemstillinger.
c. Andre saker av særlig viktighet eller prinsipiell karakter.

§ 2-8 *EOS-utvalgets og Riksrevisjonens kontroll*

Etterretningstjenesten er underlagt kontroll som fastsatt i EOS-kontrolloven. EOS-utvalget fører styrket kontroll med etterlevelse av særreglene i kapittel 7 om tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon.

Etterretningstjenesten er underlagt revisjon og kontroll av Riksrevisjonen etter riksrevisjonsloven. Riksrevisjonen utpeker bestemte tjenestepersoner for å ivareta revisjon og kontroll av Etterretningstjenesten. Utpekte tjenestepersoner skal være norske statsborgere og sikkerhetsklarert for STRENGT HEMMELIG.

Riksrevisjonen skal være representert i K-utvalget.

§ 2-9 *Orientering til stortingspresidenten*

Statsråden som er ansvarlig for Etterretningstjenesten orienterer stortingspresidenten årlig om Etterretningstjenestens virksomhet.

Sjefen for Etterretningstjenesten skal delta ved orienteringen. Stortingspresidenten bestemmer øvrig deltakelse.

§ 2-10 *Øvrig tilsyn og kontroll*

Etterretningstjenesten er unntatt fra Datatilsynets og Personvernnemndas kontroll-, tilsyns- og sanksjonsbeføyelser og deres tilgang til opplysninger og lokaler mv. Etterretningstjenestens behandling av personopplysninger kontrolleres av EOS-utvalget.

Kapittel 10 i ekomloven gjelder ikke for informasjon og områder som vil gi myndigheten etter ekomloven innsyn i Etterretningstjenestens virksomhet.

Domstolene fører forhåndskontroll etter kapittel 8 med søk som gjennomføres etter bestemmelsene i kapittel 7.

Kapittel 3. Oppgaver

§ 3-1 *Informasjonsinnhenting om utenlandske trusler*

Etterretningstjenesten skal innhente og analysere informasjon om utenlandske militære og sivile forhold som kan bidra til å avdekke og motvirke

a. trusler mot Norges selvstendighet og sikkerhet, territorielle integritet og politiske og økonomiske handlefrihet,
b. alvorlige trusler mot samfunnssikkerheten i Norge,
c. alvorlige trusler mot norske interesser i utlandet,
d. fremmed etterretningsvirksomhet,
e. fremmede sabotasje- og påvirkningsoperasjoner,
f. grenseoverskridende terrorisme,
g. spredning av masseødeleggelsesvåpen og utstyr og materiale for fremstilling av slike våpen,
h. internasjonal våpenhandel som kan utgjøre en alvorlig sikkerhetstrussel, og

i. eksport av sanksjonerte, listeførte eller sensitive varer og tjenester.

§ 3-2 *Informasjonsinnhenting om andre utenlandske forhold*

Etterretningstjenesten skal innhente og analysere informasjon om utenlandske militære og sivile forhold som kan bidra til

a. ivaretakelse av prioriterte utenriks-, forsvars- eller sikkerhetspolitiske interesser knyttet til forhold og utviklingstrekk i andre stater og regioner,
b. nasjonal beredskapsplanlegging,
c. episode- og krisehåndtering, og
d. planlegging og gjennomføring av nasjonale eller internasjonale militære operasjoner.

§ 3-3 *Okkupasjonsberedskap*

Etterretningstjenesten skal ivareta nasjonal evne til å innhente og formidle etterretninger til norske myndigheter fra et helt eller delvis okkupert Norge.

Departementet skal holdes generelt orientert om organisering og planlegging av okkupasjonsberedskapen.

§ 3-4 *Internasjonalt etterretningssamarbeid*

Når det er i norsk interesse kan Etterretningstjenesten innhente og analysere informasjon om utenlandske trusler og andre forhold som nevnt i kapittelet her som antas å være av vesentlig betydning i bi- eller multilateralt etterretningssamarbeid som Etterretningstjenesten deltar i.

§ 3-5 *Innhenting av evneinformasjon*

Etterretningstjenesten kan innhente og analysere informasjon om forhold som utgjør nødvendige forutsetninger for å kunne gjennomføre innhenting etter kapittelet her, herunder for å kunne

a. sørge for at innhenting ikke skjer i større utstrekning enn nødvendig,
b. ivareta sikkerheten til Etterretningstjenestens personell og operasjoner,
c. gjennomføre testing av teknisk utstyr og annen trenings- og øvingsaktivitet, og
d. opprettholde og videreutvikle Etterretningstjenestens aksesser og metodiske, teknologiske og øvrige evne til å utføre pålagte oppgaver.

Kapittel 4. Territoriell begrensning og andre særskilte forbud

§ 4-1 *Forbud mot innhenting rettet mot personer som befinner seg i Norge*

Det er forbudt for Etterretningstjenesten å rette innhenting av informasjon mot en fysisk person som oppholder seg i Norge.

Det er forbudt for Etterretningstjenesten å rette innhenting av informasjon mot virksomhet i Norge som utøves av en juridisk person.

Hvis Etterretningstjenesten er i tvil om en person oppholder seg eller driver virksomhet i Norge, skal den søke å avklare forholdet basert på den informasjon som er tilgjengelig eller for dette formål kan skaffes til veie fra Politiets sikkerhetstjeneste, andre partnere, åpne kilder eller egen innhenting.

§ 4-2 *Unntak fra og presiseringer av forbudet i § 4-1*

Etterretningstjenesten kan rette innhenting av informasjon mot en utenlandsk statsborger eller statsløs person, eller mot en norsk eller utenlandsk virksomhet i Norge, dersom det foreligger konkrete holdepunkter for at personen opptrer på vegne av fremmed makt eller virksomheten utøves av fremmed makt. Innhenting av informasjon om fremmed etterretningsvirksomhet i Norge skal skje etter samtykke fra Politiets sikkerhetstjeneste.

Etterretningstjenesten kan rette innhenting av informasjon mot personer eller virksomheter i Norge dersom formålet med innhentingen er å frembringe relevant informasjon for å finne potensielle kilder eller gjennomføre kildeverifikasjon.

Ved innhenting etter annet ledd skal det ikke innhentes mer informasjon enn det som fremstår som strengt nødvendig. Informasjon skal innhentes gjennom åpne kilder, utlevering av opplysninger fra andre norske myndigheter, eller med samtykke fra den det gjelder. Dersom det foreligger tungtveiende sikkerhetsmessige grunner kan strengt nødvendig informasjon likevel innhentes i en avgrenset tidsperiode uten å oppgi tilknytning til Etterretningstjenesten eller norske offentlige myndigheter, samt ved bruk av metoder som nevnt i §§ 6-3 og 6-4 i loven her. Øvrige metoder kan kun benyttes med samtykke fra den som innhentingen rettes mot.

Forbudet i § 4-1 er ikke til hinder for at Etterretningstjenesten mottar eller for etterretningsformål ber om å få utlevert informasjon som andre besitter om personer eller virksomhet i Norge.

Forbudet i § 4-1 er ikke til hinder for at det innhentes informasjon som er strengt nødvendig for å kunne gjennomføre testing av utstyr eller trening og øving i Norge.

Innhenting av rådata i bulk er ikke å anse som rettet mot personer eller virksomhet omfattet av § 4-1, selv om rådata kan inneholde informasjon om personer som oppholder seg eller virksomhet som utøves i Norge.

Søk i rådata med utgangspunkt i en personselektor som kan knyttes til en person som omfattes av § 4-1, kan gjennomføres dersom søket ikke er rettet mot denne personen og søket anses å ha eller kunne få vesentlig betydning for ivaretakelsen av Etterretningstjenestens oppgaver etter kapittel 3.

Dersom formålet med innhentingen er rettet mot forhold eller personer i utlandet, er innhenting av informasjon gjennom åpne kilder ikke å anse som rettet mot personer eller virksomhet i Norge, selv om det innhentes informasjon som er publisert av eller berører personer i Norge eller som befinner seg på sosiale profiler, hjemmesider eller lignende media som er knyttet til personer i Norge.

§ 4-3 *Forbud mot industrispionasje*

Etterretningstjenesten skal ikke innhente eller medvirke til å innhente, bearbeide eller utlevere informasjon med formål å gi selskaper eller andre kommersielle virksomheter eller sektorer konkurransemessige fortrinn.

§ 4-4 *Forbud mot å utføre oppgaver med politiformål*

Etterretningstjenestens virksomhet skal ikke ha som formål å løse kriminalitetsforebyggende eller kriminalitetsbekjempende oppgaver som tilligger politiet eller andre norske rettshåndhevende myndigheter.

At informasjon innhentet for etterretningsformål også kan være relevant for politiet eller andre norske rettshåndhevende myndigheter, er ikke i strid med forbudet etter første ledd. Det samme gjelder at Etterretningstjenesten kan bistå politiet innenfor politiets rettsgrunnlag i medhold av politiloven § 27 a og § 10-3 i loven her.

Kapittel 5. Grunnvilkår for informasjonsinnhenting, metodebruk og utlevering av informasjon

§ 5-1 *Grunnvilkår for målsøking*

Etterretningstjenesten kan iverksette målsøking når det foreligger grunn til å undersøke om innhenting kan bidra til å frembringe informasjon som er relevant for etterretningsformål.

§ 5-2 *Grunnvilkår for målrettet innhenting*

Etterretningstjenesten kan iverksette målrettet innhenting når konkrete holdepunkter tilsier at det foreligger grunn til å undersøke om etterretningsmålet besitter, kommuniserer eller vil motta, eller om innhenting på annen måte kan frembringe, informasjon som er relevant for etterretningsformål.

§ 5-3 *Grunnvilkår for innhenting av og søk i rådata i bulk*

Rådata kan innhentes i bulk når det er nødvendig for å få tilgang til et relevant og tilstrekkelig informasjonsgrunnlag i den hensikt å gjennomføre målsøking eller målrettet innhenting i dette informasjonsgrunnlaget.

Alle søk i bulkinnhentede rådata skal tilfredsstille grunnvilkårene for målsøking eller målrettet innhenting og logges for kontrollformål.

§ 5-4 *Forholdsmessighet*

Innhenting og utlevering av informasjon skal ikke gjennomføres dersom det vil være et uforholdsmessig inngrep overfor den enkelte. Ved vurderingen skal det tas hensyn til om mindre inngripende tiltak i tilstrekkelig grad kan ivareta formålet, inngrepets virkning for den som rammes, sakens betydning og forholdene ellers.

Kapittel 6. Metodebruk for innhenting av informasjon som medfører inngrep overfor den enkelte

§ 6-1 *Generelle vilkår og virkeområde*

Etterretningstjenesten kan for etterretningsformål benytte metoder etter bestemmelsene i kapittelet her, når grunnvilkårene etter kapittel 5 er oppfylt og innhentingen ikke strider mot øvrige bestemmelser i denne loven. Metodebruk etter kapittelet her kan skje fordekt overfor personer som er gjenstand for eller som på annen måte berøres av metodebruken. Metodebruk skal avsluttes dersom det blir klart at vilkårene etter loven her ikke lenger er til stede.

Bestemmelsene i kapittelet her kommer bare til anvendelse for innhenting som medfører inngrep overfor den enkelte.

Bestemmelsene i kapittelet her kommer ikke til anvendelse for tilrettelagt innhenting av elektronisk kommunikasjon som transporteres over den norske landegrensen og som reguleres av kapitlene 7 og 8.

§ 6-2 *Åpne kilder*

Etterretningstjenesten kan innhente informasjon fra åpne kilder.

Etterretningstjenesten kan bruke fiktive brukeridentiteter og -kontoer for å skjerme hvem som står bak innhentingen.

Med åpne kilder menes informasjon som er åpent tilgjengelig. Informasjon er ikke åpent tilgjengelig dersom tilgang krever forsering av passord eller lignende beskyttelsesmekanismer, eller dersom tilgang krever aktiv fordekt opptreden.

§ 6-3 *Menneskebasert innhenting*

Etterretningstjenesten kan ved aktiv opptreden i det fysiske eller digitale rom gjennomføre menneskebasert innhenting og kildeverifikasjon.

Menneskebasert innhenting kan inkludere infiltrasjon og provokasjon.

Med menneskebasert innhenting menes systematisk innhenting av informasjon gjennom samhandling mellom mennesker.

§ 6-4 *Systematisk observasjon*

Etterretningstjenesten kan foreta systematisk observasjon på offentlig sted hvor etterretningsmål med sannsynlighet antas å befinne seg eller oppsøke. Det samme gjelder mot privat lukket sted dersom den som observerer befinner seg utenfor.

Det kan tas i bruk hjelpemidler for observasjon, opptak og annen dokumentasjon.

Med systematisk observasjon menes planlagte visuelle iakttakelser i det fysiske rom av en person eller gruppe av personer, eiendom, virksomhet, område eller andre relevante etterretningsmål.

§ 6-5 *Teknisk sporing*

Etterretningstjenesten kan ta i bruk teknisk sporing for å lokalisere en person eller gjenstand.

Med teknisk sporing menes plassering av tekniske peilemekanismer i det fysiske rom på eller ved et etterretningsmål, i den hensikt å kartlegge målets posisjon og bevegelser.

§ 6-6 *Gjennomsøking, avlytting, skjult bildeovervåkning og annen innhenting med tekniske midler*

Etterretningstjenesten kan gjennomføre gjennomsøking, avlytting, skjult bildeovervåkning og annen innhenting med tekniske midler. Dersom tiltaket gjennomføres på eller mot sted som etter sin

art ikke er tilgjengelig for alle, kan tiltaket bare gjennomføres dersom tiltaket anses strengt nødvendig for ivaretakelsen av Etterretningstjenestens oppgaver etter kapittel 3.

Med gjennomsøking menes undersøkelse av bolig, rom, oppbevaringssted eller person for å søke etter informasjon eller gjenstander.

Med avlytting og skjult bildeovervåking menes utplassering av kamera, mikrofon eller andre tekniske sensorer på eller i nærheten av et sted hvor det er rimelig å anta at et etterretningsmål vil oppholde seg.

Med annen innhenting med tekniske midler menes enhver innhenting ved bruk av tekniske sensorer eller metoder som ikke reguleres av §§ 6-7 eller 6-8, herunder bildeovervåking av enkeltpersoner fra rombaserte sensorer eller luftbårne plattformer.

§ 6-7 *Midtpunktinnhenting*

Etterretningstjenesten kan gjennomføre midtpunktinnhenting.

Med midtpunktinnhenting menes innhenting av elektronisk kommunikasjon og kartlegging av kommunikasjonsinfrastruktur. Med elektronisk kommunikasjon menes kommunikasjon ved bruk av et transport- eller overføringssystem som muliggjør overføring av lyd, tekst, bilder eller andre data.

§ 6-8 *Endepunktinnhenting*

Etterretningstjenesten kan gjennomføre endepunktinnhenting av informasjon i systemer og tjenester som etterretningsmål besitter eller antas å ville benytte. Dersom det er grunn til å tro at innhentingen vil inneholde data som ikke er ment for kommunikasjon, skal tiltaket bare iverksettes dersom det anses strengt nødvendig for ivaretakelsen av Etterretningstjenestens oppgaver etter kapittel 3.

Med endepunktinnhenting menes teknisk observasjon av og innhenting av ikke åpent tilgjengelig elektronisk informasjon i datasystem eller lignende system eller tjeneste, når innhentingen ikke er å anse som midtpunktinnhenting.

§ 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.

§ 6-10 *Beslutningsprosess for metodebruk*

Sjefen for Etterretningstjenesten eller den han eller hun bemyndiger treffer beslutning om bruk av metoder regulert i kapittelet her, med mindre beslutning tilligger departementet etter § 2-7.

Beslutninger om metodebruk skal dokumenteres skriftlig gjennom innhentingsplan, operasjonsordre eller lignende skriftlig dokumentasjon. Dokumentasjonen skal angi det eller de etterretningsoppdrag som ligger til grunn for metodebruken, og det eller de etterretningsmål eller kategorier av etterretningsmål som metoden retter seg mot. Vurdering av forholdsmessighet etter § 5-4 skal fremgå av dokumentasjonen.

I hastetilfeller kan beslutning treffes muntlig, men skal snarest mulig formaliseres skriftlig.

Dokumentasjonen som nevnt i annet ledd skal revurderes minst en gang i året. Dersom omstendighetene som lå til grunn for en beslutning vesentlig endres, skal beslutningen snarest mulig revurderes.

Kapittel 7. Særregler for tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon

§ 7-1 *Hjemmel for innhenting og virkeområde*

Etterretningstjenesten kan for etterretningsformål innhente elektronisk kommunikasjon som transporteres over den norske landegrensen når grunnvilkårene etter kapittel 5 er oppfylt, særreglene i kapittel 7 og 8 følges og innhenting ikke strider mot øvrige bestemmelser i loven her.

Bestemmelsene i kapittel 7 og 8 kommer bare til anvendelse for innhenting der det er nødvendig at tilbydere som nevnt i § 7-2 legger til rette for Etterretningstjenestens tilgang til den elektroniske kommunikasjonen.

§ 7-2 *Tilretteleggingsplikt*

Tilbydere som omfattes av ekomloven § 1-5 nr. 16 og tilbydere av internettbaserte kommunikasjons- eller meldingstjenester som er tilgjengelige for allmennheten skal legge til rette for at Etterretningstjenesten kan innhente elektronisk kommunikasjon som transporteres over den norske landegrensen.

Tilretteleggingsplikten innebærer plikt til på egnet måte å speile og gjøre kommunikasjonsstrømmene tilgjengelige for Etterretningstjenesten, og på annen måte tilrettelegge for at Etterretningstjenesten kan gjennomføre utvalg, filtrering, testing, lagring og søk som beskrevet i kapittelet her, herunder

a. gi informasjon om signalmiljø, dataformater, tekniske innretninger og fremgangsmåter, i den utstrekning det er nødvendig for å oppfylle tilretteleggingspliktens formål,
b. tillate at Etterretningstjenesten installerer utstyr og etablerer midlertidig eller permanent tilstedeværelse for å drifte utstyr på steder som kontrolleres av tilbyder, og etter anmodning fra Etterretningstjenesten medvirke til teknisk drift og vedlikehold av etablerte løsninger,
c. bidra til at Etterretningstjenesten kan gjennomføre testinnhenting og testanalyser av trafikk i nett og tjenester,
d. sørge for tilgang til kommunikasjon uten hinder av linkkryptering eller lignende kryptering som tilbyder kontrollerer, og
e. medvirke til sikkerhetsmessig forsvarlige løsninger, herunder at Etterretningstjenestens utstyr og tilstedeværelse gjøres kjent for færrest mulig personer hos tilbyder og bare for de som har tjenstlig behov for det.

Departementet kan gi forskrift om tilretteleggingsplikten.

§ 7-3 *Taushetsplikt*

Den som er underlagt tilretteleggingsplikt etter § 7-2 plikter å bevare taushet om Etterretningstjenestens tilgang, tekniske løsninger og andre forhold knyttet til gjennomføring av tilretteleggingen. Taushetsplikten gjelder også for enhver som utfører arbeid eller tjeneste for den som er underlagt tilretteleggingsplikt etter § 7-2 eller som på annen måte bistår i gjennomføring av tilrettelegging. Taushetsplikten fortsetter å gjelde også etter at vedkommende har avsluttet arbeidet eller tjenesten.

Taushetsplikten er ikke til hinder for å gi opplysninger til EOS-utvalget eller Nasjonal kommunikasjonsmyndighet.

§ 7-4 *Utgiftsdekning*

Merutgifter for tilbyder som følge av tilretteleggingsplikten dekkes av staten.

Departementet kan gi forskrift om prinsipper for utregning av merutgiftene.

§ 7-5 *Utvalg og filtrering*

Ved utvalg av kommunikasjonsnett og tjenester som transporterer elektronisk kommunikasjon over den norske landegrensen, skal Etterretningstjenesten prioritere tilgang til nett, tjenester og linker som antas å frembringe mest mulig etterretningsmessig relevant informasjon for å løse tjenestens oppgaver etter kapittel 3.

Etterretningstjenesten skal gjennom utvalg og filtrering så langt som praktisk mulig sikre at metadata som lagres i henhold til § 7-7 ikke inneholder data om kommunikasjon mellom en avsender og mottaker som begge befinner seg i Norge, med mindre avsender eller mottaker omfattes av § 4-2 første ledd.

§ 7-6 *Korttidslager og behandling av testdata*

Etterretningstjenesten skal gjennomføre testinnhenting og testanalyser av trafikk og nett som omfattes av kapittelet her. Testinnhenting og testanalyser skal aldri benyttes for etterretningsformål,

men utelukkende for teknisk å muliggjøre utvalg, filtrering, lagring og søk i lagrede data, reprosessering av data, forståelse av signalmiljø og gjenkjenning av tjenester og dataformater.

Testinnhenting skal gjennomføres ved å gjøre et uttrekk av ufiltrert kommunikasjon i en eller flere utvalgte kommunikasjonslinker. Ett uttrekk skal ikke overstige 30 sekunder. Maksimalt antall uttrekk er 1 per time.

Uttrekkene skal lagres i et korttidslager som skal holdes adskilt fra metadata som lagres etter § 7-7.

Uttrekkene skal ikke oppbevares lenger enn det som er nødvendig og skal slettes senest etter 14 dager. Tekniske parametere og bearbeidede analyser av testdata som ikke kan knyttes til enkeltpersoner kan oppbevares så lenge det er nødvendig for de formål som fremgår av første ledd annet punktum.

Testinnhenting og annen teknisk understøttelse skal bare utføres av et begrenset antall tekniske spesialister som har mottatt særskilt opplæring og som ikke har etterretningsanalyse som oppgave. Det skal alltid være to spesialister tilstede ved oppsett og analyse av uttrekk etter annet ledd.

§ 7-7 *Metadatalagring*

Etter at det er foretatt utvalg og filtrering etter § 7-5, kan Etterretningstjenesten lagre metadata om elektronisk kommunikasjon som passerer den norske landegrensen.

Metadata er data som beskriver annen data eller som inneholder ekstra informasjon knyttet til data, herunder data som beskriver typen eller formatet på innholdet, hvem som er avsender og mottaker, og størrelse, tidspunkt og varighet for kommunikasjonen. Etterretningstjenesten skal opprette og vedlikeholde en liste over hvilke typer metadata som kan lagres, for å hindre at det lagres innholdsdata. Listen skal være tilgjengelig for EOS-utvalget.

Lagrede metadata skal slettes etter 18 måneder.

For teknisk analyse, feilsøking og oppdatering av lagrede metadata i den hensikt å muliggjøre søk, gjelder § 7-6 femte ledd første punktum tilsvarende.

§ 7-8 *Søk i lagrede metadata*

Etterretningstjenesten kan foreta søk i lagrede metadata innenfor rammen av rettens kjennelse etter kapittel 8. Søkene skal baseres på personselektorer eller modusselektorer. Personselektorsøk kan maksimalt inkludere to ledd ut i personenes kommunikasjonskjede, med mindre retten i særskilte tilfeller bestemmer noe annet.

Søk i lagrede metadata kan bare utføres av personell i Etterretningstjenesten som er vurdert som skikket til det og som utpekes av sjefen for Etterretningstjenesten eller dennes stedfortreder. Personellet må ha gjennomgått særskilt opplæring. Den enkelte skal bare ha anledning til å utføre søk i henhold til søkeprivilegier som er tilpasset dennes oppdragsportefølje.

Behandling av personopplysninger som Etterretningstjenesten har fått tilgang til etter første ledd, skal skje i samsvar med bestemmelsene i kapittel 9.

§ 7-9 *Innhenting og lagring av innholdsdata*

Innenfor rammen av rettens kjennelse etter kapittel 8 kan Etterretningstjenesten innhente og lagre innholdsdata med tilhørende metadata fra elektronisk kommunikasjon som transporteres over den norske landegrensen.

Innholdsdata er data som ikke er metadata.

Behandling av personopplysninger som Etterretningstjenesten har fått tilgang til etter første ledd, skal skje i samsvar med bestemmelsene i kapittel 9.

§ 7-10 *Aktivitetslogger for kontrollformål*

Etterretningstjenestens informasjonssystemer skal ha en funksjonalitet som sikrer at alle søk skal kunne kontrolleres i ettertid gjennom aktivitetslogger.

Aktivitetsloggene skal oppbevares i 10 år, og skal til enhver tid være tilgjengelig for kontroll, jf. § 7-11.

§ 7-11 *EOS-utvalgets kontroll*

EOS-utvalget skal føre styrket kontroll med at Etterretningstjenesten bare gjennomfører søk i henhold til rettens kjennelser, at korttidslageret og testdata ikke benyttes til etterretningsformål, og at de øvrige bestemmelsene i kapittelet her etterleves.

EOS-utvalget skal ha uhindret adgang til all informasjon, interne retningslinjer og prosedyrer, lokaler, utstyr, programvare, filteroppdateringer, aktivitetslogger og annet som benyttes for gjennomføring av virksomhet etter kapittelet her.

§ 7-12 Forbud mot utlevering av overskuddsinformasjon

Etterretningstjenesten skal ikke utlevere overskuddsinformasjon fremkommet gjennom innhenting etter kapittelet her. Straffeloven §§ 196 og 226 gjelder ikke for Etterretningstjenestens personell i den utstrekning de får kunnskap om det aktuelle forholdet gjennom innhenting etter kapittelet her.

Forbudet etter første ledd gjelder ikke overskuddsinformasjon om en straffbar handling som omfattes av straffeloven kapittel 17 eller 18 og som kan avverges. Sjefen for Etterretningstjenesten beslutter skriftlig om utlevering skal skje.

Informasjon som ikke er overskuddsinformasjon kan utleveres dersom vilkårene i kapittel 10 er oppfylt.

§ 7-13 *Bevisforbud*

Informasjon fremkommet gjennom innhenting etter kapittelet her kan ikke brukes som grunnlag for ileggelse av straff eller andre strafferettslige reaksjoner.

§ 7-14 *Informasjonssikkerhet*

Etterretningstjenesten plikter å hindre at uvedkommende får tilgang til informasjon som lagres og behandles etter bestemmelsene i kapittelet her. Etterretningstjenesten skal gjennomføre sikkerhetstiltak etter §§ 9-11 og 11-4 for å sikre at informasjonen bare er tilgjengelig for de som har lovmessig tilgang til den.

Kapittel 8. Domstolskontroll med tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon

§ 8-1 *Kjennelse om tillatelse til tilrettelagt innhenting*

Retten kan ved kjennelse gi Etterretningstjenesten tillatelse til søk etter § 7-8 og innhenting og lagring etter § 7-9.

Retten kan oppstille vilkår i kjennelsen. Kjennelsen skal begrunnes. Retten kan omgjøre kjennelsen.

Rettens avgjørelse skal treffes så raskt som mulig.

Avgjørelsen treffes uten at den som avgjørelsen retter seg mot eller ellers rammer gis adgang til å uttale seg. Kjennelsen blir ikke meddelt dem.

Kjennelsen skal meddeles Etterretningstjenesten. Tjenesten skal gjøre kjennelsen tilgjengelig for EOS-utvalget.

§ 8-2 *Krav til begjæringen*

Etterretningstjenestens begjæringer skal være skriftlige og angi hva eller hvem innhentingen retter seg mot og opplysninger om det rettslige og faktiske grunnlaget for innhentingen.

Begjæringen fremmes for Oslo tingrett av sjefen for Etterretningstjenesten eller den som sjefen bemyndiger.

§ 8-3 *Rettsmøte*

Retten kan beslutte muntlige forhandlinger. Etterretningstjenesten møter ved sjefen for tjenesten eller den som sjefen bemyndiger. Tjenesten kan medbringe fagkyndige dersom dette anses nødvendig for å opplyse saken.

Rettsmøtene holdes for lukkede dører.

§ 8-4 *Hva retten skal prøve*

Retten skal prøve om vilkårene etter loven her er oppfylt, herunder at innhentingen ligger innenfor Etterretningstjenestens oppgaver etter kapittel 3, ikke innebærer brudd på forbudene i §§ 1-3 annet ledd, 4-1, 4-3, 4-4 eller 9-4, og tilfredsstiller grunnvilkårene etter kapittel 5.

§ 8-5 *Oppnevning av særskilt advokat*

Retten kan beslutte at det skal oppnevnes en særskilt advokat for å ivareta rettighetene til den eller de som innhentingen retter seg mot og eventuelle tredjepersoner. Advokaten beskikkes fra den særlige krets av sikkerhetsklarerte advokater, og kan ikke la seg representere eller møte ved annen advokat eller fullmektig.

Advokaten skal gjøres kjent med Etterretningstjenestens begjæring og annen informasjon som legges frem i retten, men har utover dette ingen innsynsrett. Advokaten skal varsles om rettsmøter i saken og har rett til å delta i dem. Advokaten har rett til å uttale seg før retten treffer avgjørelse.

Advokaten må ikke sette seg i forbindelse med den som saken gjelder.

Departementet kan gi forskrift om oppnevning av særskilt advokat.

§ 8-6 *Varighet*

Rettens tillatelse etter § 8-1 skal ikke gis for lengre tid enn nødvendig. Tillatelsen kan ikke overstige ett år når innhentingen gjelder målsøking og seks måneder når innhentingen gjelder målrettet innhenting.

Etterretningstjenesten skal avslutte pågående innhenting dersom vilkårene etter loven her ikke lenger er til stede.

§ 8-7 *Informasjonssikkerhet*

Rettens kjennelse skal sikkerhetsgraderes etter sikkerhetslovens regler.

Domstolen skal sørge for at informasjon og dokumenter med høyeste sikkerhetsgrad kan behandles i henhold til sikkerhetsloven hos domstolen som ledd i skriftlige eller muntlige forhandlinger.

Domstolen skal legge til rette for at særskilte advokater oppnevnt etter § 8-5 kan gjøres kjent med sikkerhetsgradert informasjon i domstolens lokaler.

§ 8-8 *Taushetsplikt*

Retten og den særskilte advokaten plikter å bevare livsvarig taushet om begjæringer, rettsmøter, kjennelser og andre opplysninger de får kjennskap til i saker etter kapittelet her.

Taushetsplikten er ikke til hinder for å gi opplysninger til EOS-utvalget.

§ 8-9 *Anke*

Etterretningstjenesten og den særskilte advokaten kan anke rettens kjennelse. Anke fra den særskilte advokaten har ikke oppsettende virkning.

Straffeprosessloven kapittel 26 gjelder så langt reglene passer.

§ 8-7 gjelder tilsvarende for ankedomstolen.

§ 8-10 *Hastekompetanse*

Dersom det ved opphold er stor fare for at etterretningsinformasjon av vesentlig betydning for utførelsen av Etterretningstjenestens oppgaver etter kapittel 3 kan gå tapt, kan ordre fra sjefen for Etterretningstjenesten tre i stedet for rettens kjennelse. I slike tilfeller skal Etterretningstjenesten straks og senest innen 24 timer etter at innhentingen ble påbegynt forelegge saken for retten.

Retten avgjør ved kjennelse om innhentingen kan tillates, jf. § 8-1. Kommer retten til at innhentingen var urettmessig, skal retten meddele dette til EOS-utvalget og pålegge Etterretningstjenesten å slette innhentet informasjon.

Kapittel 9. Behandling av personopplysninger m.m.

§ 9-1 *Forholdet til annen lovgivning*

Personopplysningsloven gjelder ikke for behandling av personopplysninger etter loven her.

For behandling av personopplysninger for andre formål enn etter loven her gjelder bestemmelsene i personopplysningsloven eller særlovgivningen, med de unntak som følger av § 2-10 første ledd og eventuelle tilpassede skjermingsregler i medhold av § 11-5.

§ 9-2 *Formålsbestemthet*

Etterretningstjenesten kan behandle personopplysninger for etterretningsformål.

§ 9-3 *Innhenting av personopplysninger*

Med unntak av §§ 9-2 og 9-4 gjelder bestemmelsene i kapittelet her ikke for behandling i form av innhenting. Behandling i form av innhenting reguleres i kapittel 3-8.

§ 9-4 *Diskrimineringsforbud*

Etterretningstjenesten skal ikke behandle personopplysninger utelukkende på bakgrunn av hva som er kjent om en persons etnisitet eller nasjonale bakgrunn, politiske, religiøse eller filosofiske overbevisning, språk, politiske virksomhet, fagforeningstilhørighet eller helsemessige eller seksuelle forhold.

§ 9-5 *Nødvendighetskrav*

Etterretningstjenesten skal vurdere om personopplysninger er nødvendige å behandle for etterretningsformål. For personopplysninger som er rådata i bulk skal nødvendighetsvurderingen gjennomføres samlet når rådataen lagres og ellers når ny informasjon eller andre omstendigheter tilsier det.

For personopplysninger som ikke er rådata i bulk skal nødvendighetsvurderingen senest gjennomføres når personopplysningene vurderes brukt for etterretningsformål, herunder når opplysningene inntas i et produkt som planlegges distribuert utenfor Etterretningstjenesten. Det skal foretas en nødvendighetsvurdering hvis ny informasjon eller andre omstendigheter tilsier det.

Personopplysninger om kilder som ikke ønsker å samarbeide med Etterretningstjenesten kan behandles for å hindre at vedkommende kontaktes igjen. Behandlingen skal være begrenset til det som er strengt nødvendig for dette formålet.

§ 9-6 *Nødvendighetskrav for behandling av fortrolig kommunikasjon med særlige yrkesutøvere*

Etterretningstjenesten skal ikke behandle opplysninger som er fortrolig kommunikasjon mellom advokat og klient, helsepersonell og pasient, journalist og kilde eller tilsvarende fortrolig kommunikasjon som nyter særlig menneskerettslig vern, med mindre vektige samfunnshensyn gjør behandlingen strengt nødvendig.

Beslutning om å behandle opplysninger etter første ledd treffes av sjefen for Etterretningstjenesten, med mindre beslutning tilligger departementet etter § 2-7.

Opplysningene skal merkes særskilt for kontrollformål.

§ 9-7 *Unntak fra kravene til formålsbestemthet og nødvendighet*

Opplysninger kan behandles dersom det er nødvendig for å avklare om kravene i § 9-2, § 9-5 eller § 9-6 er oppfylt.

§ 9-8 *Krav til opplysningenes kvalitet*

Etterretningstjenesten skal så langt det er mulig påse at personopplysninger som behandles og som ikke er rådata i bulk, er korrekte og oppdaterte. Opplysninger som ikke er korrekte skal uten opphold slettes eller korrigeres. Etterretningstjenesten skal så langt som mulig sørge for at feilen ikke får betydning for den det gjelder.

Ikke-verifiserte opplysninger kan behandles dersom det er nødvendig ut fra formålet med behandlingen. Det skal fremgå av Etterretningstjenestens produkter dersom ikke-verifiserte personopplysninger er behandlet.

§ 9-9 *Sletting*

Personopplysninger skal slettes når de ikke lenger er nødvendige å behandle etter bestemmelsene i loven her. Opplysninger som er fortrolig kommunikasjon etter § 9-6 skal slettes uten unødig opphold dersom de ikke kan behandles etter § 9-6 første ledd.

Rådata i bulk skal slettes senest 15 år fra lagringstidspunktet, med mindre vesentlige hensyn tilsier at sletting utsettes. Beslutning om utsatt sletting treffes av sjefen for Etterretningstjenesten for ikke mer enn fem år av gangen.

Sletting av personopplysninger i operative systemer og registre som er tilgjengelige for etterretningsproduksjon, er ikke til hinder for lagring av opplysningene etter arkivloven eller annen lovgivning. Sletting er heller ikke til hinder for lagring for historiske, statistiske eller vitenskapelige formål, dersom samfunnets interesse i at opplysningene lagres klart overstiger de ulemper den kan medføre for den enkelte.

Sletting skal anses gjennomført selv om slettede data teoretisk kan rekonstrueres ved hjelp av avansert teknisk gjenfinningsverktøy og innsats fra personer med spesielle systemrettigheter. Etterretningstjenesten skal etablere rutiner som sikrer at slettede data ikke blir rekonstruert for etterretningsformål.

§ 9-10 *Opplysninger innhentet ved trening, øving og testing*

Behandling av personopplysninger i forbindelse med testing av teknisk utstyr eller trening og øving skal skje adskilt fra Etterretningstjenestens øvrige behandling av opplysninger.

Personopplysninger innhentet ved virksomhet etter første ledd skal slettes snarest mulig etter at treningen, øvingen eller testvirksomheten er avsluttet, og skal ikke arkiveres i henhold til arkivloven. Unntak gjelder dersom den enkelte berørte person har avgitt uttrykkelig samtykke til videre behandling.

§ 9-11 *Informasjonssikkerhet*

Etterretningstjenesten skal gjennom systematiske tiltak sikre konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger. Tiltakene skal utformes i samsvar med bestemmelsene i sikkerhetsloven og annen relevant lovgivning og være basert på risikovurdering, sikkerhetsrevisjon, sikkerhetsovervåking og internkontroll.

Personopplysninger skal ikke gjøres tilgjengelige for flere personer enn nødvendig for å oppfylle formålet med behandlingen.

§ 9-12 *Personvernrådgiver*

Etterretningstjenesten skal i egen organisasjon ha minst én personvernrådgiver som skal bidra til etterlevelse av bestemmelsene i kapittelet her gjennom opplæring, rådgivning, veiledning og internkontroll.

Sjefen for Etterretningstjenesten skal sikre at personvernrådgiveren involveres i spørsmål som gjelder vern av personopplysninger.

Enhver i Etterretningstjenesten kan kontakte personvernrådgiveren om spørsmål relatert til behandling av personopplysninger eller for å rapportere om brudd og avvik knyttet til behandling av personopplysninger.

Kapittel 10. Nasjonalt og internasjonalt samarbeid. Informasjonsutveksling.

§ 10-1 *Nasjonalt samarbeid*

Etterretningstjenesten kan samarbeide med andre norske offentlige myndigheter, herunder gjennom informasjonsutveksling og felles operasjoner.

Etterretningstjenesten skal samarbeide med andre norske offentlige myndigheter om grenseoverskridende trusler, forsvar mot og håndtering av alvorlige hendelser i det digitale rom, samt andre prioriterte saksfelt.

Etterretningstjenesten kan bare utlevere informasjon til norske offentlige myndigheter dersom vilkårene i §§ 10-5 eller 10-8 er oppfylt.

§ 10-2 *Utlevering av informasjon til Etterretningstjenesten fra norske offentlige myndigheter*

Lovbestemt taushetsplikt er ikke til hinder for at offentlige myndigheter utleverer informasjon til Etterretningstjenesten dersom det er nødvendig for forebyggelses- og sikkerhetsmessige formål innenfor rammen av Etterretningstjenestens oppgaver etter kapittel 3.

§ 10-3 *Bistand til politiet*

Etterretningstjenesten kan yte bistand til politiet etter politiloven § 27 a. Bistand i form av informasjonsinnhenting etter reglene i kapittel 7 eller utlevering av informasjon etter § 7-12 annet ledd, kan ikke finne sted.

§ 10-4 *Internasjonalt etterretningssamarbeid*

Etterretningstjenesten skal etablere og opprettholde bi- og multilateralt etterretningssamarbeid med andre land, forsvarsallianser som Norge deltar i og andre relevante internasjonale organisasjoner. Departementets beslutning skal innhentes i saker som nevnt i § 2-7.

§ 10-5 *Utlevering av etterretningsinformasjon som ledd i nasjonalt eller internasjonalt samarbeid*

Etterretningstjenesten kan utlevere etterretningsinformasjon dersom følgende kumulative vilkår er oppfylt:

a. Utleveringen skjer for etterretningsformål eller er nødvendig for å fremme mottakerens oppgaver eller for å hindre at virksomhet blir utøvd på en uforsvarlig måte.
b. Utlevering av informasjon som Etterretningstjenesten har mottatt fra en tredjepart skjer med dennes samtykke.
c. Utlevering av personopplysninger bare skjer dersom Etterretningstjenesten kan behandle opplysningene etter kapittel 9 og utleveringen vurderes å være forholdsmessig etter § 5-4.
d. Utleveringen vurderes som forsvarlig i lys av opplysningenes kvalitet, hvem som er mottaker av opplysningene og hvordan mottaker antas å bruke dem.
e. Utleverte opplysninger forventes å bli forsvarlig sikkerhetsmessig behandlet hos mottaker.
f. Utleveringen skjer med notoritet.

Utlevering med sikte på innhenting eller andre tiltak hos mottaker på vegne av og i Etterretningstjenestens interesse, kan bare skje dersom Etterretningstjenesten selv lovlig kunne ha gjennomført innhentingen eller tiltaket.

Paragrafen her gjelder ikke for utlevering av informasjon til EOS-utvalget og andre tilsyns- og kontrollinstanser.

§ 10-6 *Tilleggsvilkår for utlevering av etterretningsinformasjon som ledd i internasjonalt samarbeid*

Ved utlevering til tjenester eller myndigheter i andre stater eller til internasjonale organisasjoner skal, i tillegg til vilkårene i § 10-5, følgende kumulative vilkår være oppfylt:

a. Utleveringen er under nasjonal kontroll og vurderes å være i norsk interesse.
b. Det oppstilles vilkår om at opplysningene ikke kan benyttes som grunnlag for innhenting rettet mot personer som oppholder seg på norsk territorium, med mindre det dreier seg om en person som omfattes av § 4-2 første ledd og som det er i norsk interesse at mottakeren gjennomfører innhenting mot.
c. Utleveringen skjer i overensstemmelse med særskilte prosessuelle og materielle bestemmelser som skal sikre overholdelse av forbudet i § 1-3 annet ledd.

§ 10-7 *Videreformidling av opplysninger på vegne av andre norske offentlige myndigheter*

Etterretningstjenesten kan på vegne av annen norsk offentlig myndighet videreformidle opplysninger til og fra en utenlandsk samarbeidende tjeneste, når følgende kumulative vilkår er oppfylt:

a. Den norske myndigheten har anmodet Etterretningstjenesten om å formidle opplysningene.
b. Det fremstår klart for den samarbeidende tjenesten at videreformidlingen skjer på vegne av den norske myndigheten.
c. Etterretningstjenesten ikke endrer opplysningene, legger til egen informasjon eller ber mottaker om å handle på en bestemt måte i lys av opplysningene.
d. Det fremstår klart for den samarbeidende tjenesten at videreformidling til tredjepart krever samtykke fra den norske myndigheten eller at slikt samtykke allerede er gitt.
e. Formidlingen skjer med notoritet.

§ 10-8 *Utlevering av overskuddsinformasjon*

Overskuddsinformasjon kan deles med norske offentlige myndigheter når vilkårene etter § 10-5 er oppfylt, med unntak av vilkåret om at Etterretningstjenesten kan behandle opplysningene etter kapittel 9.

Overskuddsinformasjon som fremkommer gjennom innhenting etter kapittel 7 reguleres av § 7-12.

Overskuddsinformasjon som er fortrolig kommunikasjon etter § 9-6 kan ikke utleveres.

Kapittel 11. Forskjellige bestemmelser

§ 11-1 *Taushetsplikt*

Enhver som gjør arbeid eller tjeneste for Etterretningstjenesten skal bevare livsvarig taushet om skjermingsverdig informasjon som de blir kjent med gjennom arbeidet eller tjenesten. Tilsvarende taushetsplikt gjelder for kilder og oppdragstakere som har undertegnet særskilt taushetserklæring utstedt av Etterretningstjenesten.

Med skjermingsverdig informasjon menes informasjon som kan skade nasjonale sikkerhetsinteresser dersom informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig. Informasjonen kan være skjermingsverdig selv om den ikke har blitt merket som sikkerhetsgradert informasjon etter sikkerhetsloven.

Skjermingsverdig informasjon etter første ledd kan ikke utnyttes i virksomhet utenfor Etterretningstjenesten.

Taushetsplikten er ikke til hinder for at opplysninger utleveres etter bestemmelsene i loven her eller etter regler fastsatt i annen lov når det er uttrykkelig bestemt eller klart forutsatt at taushetsplikt ikke skal gjelde, eller at opplysninger gjøres kjent for andre i Etterretningstjenesten i samsvar med gjeldende autorisasjonsregler og prinsippet om tjenstlig behov.

§ 11-2 *Sikkerhetsklarering*

Enhver som gjør arbeid eller tjeneste i Etterretningstjenesten skal være norsk statsborger, og skal være sikkerhetsklarert for STRENGT HEMMELIG.

Sjefen for Etterretningstjenesten kan for særskilte stillinger med lavere klareringsbehov bestemme at personellet skal være sikkerhetsklarert for HEMMELIG.

§ 11-3 *Beredskap*

Etterretningstjenesten skal utarbeide og vedlikeholde beredskapsplaner, herunder forberedte tiltak for å sikre at Etterretningstjenestens informasjon og systemer ikke skal komme under kontroll av uvedkommende i krise eller væpnet konflikt, basert på Nasjonalt beredskapssystem og Forsvarets operative planverk.

§ 11-4 *Etterretningstjenestens arkiver, informasjonssystemer og etterretningsregistre*

Etterretningstjenestens arkiver, informasjonssystemer og etterretningsregistre skal være betryggende sikret og utilgjengelig for andre enn eget autorisert personell med tjenstlig behov for tilgang og personer som er satt til å føre kontroll og tilsyn med Etterretningstjenesten.

§ 11-5 *Skjerming mot offentlig eksponering av ansatte, kilder, kapasiteter, metoder og operasjoner*

Etterretningstjenesten skal være i stand til å opprettholde de spesielle krav til sikkerhet og konfidensialitet som er nødvendig for å kunne ivareta sine oppgaver.

Det kan benyttes dekkstrukturer og uriktige, falske eller villedende identiteter, dokumenter og opplysninger, samt tas kontroll over, modifiseres eller utplasseres elektronisk utstyr, for å hemmeligholde og gjennomføre Etterretningstjenestens operasjoner.

Bestemmelser i annen lov om plikt til å rapportere opplysninger gjelder ikke for vederlag som Etterretningstjenesten yter til kilder og oppdragstakere som ikke er ansatt i Etterretningstjenesten. Slike vederlag og betalinger skal heller ikke for mottaker regnes som skattepliktig inntekt eller inngå i grunnlag for beregning eller avkortning av sosiale ytelser eller lignende.

Kongen i statsråd kan gi bestemmelser som fraviker bestemmelser i annen lov, herunder lovbestemte krav om rapportering av informasjon til offentlige registre, i den utstrekning det er strengt nødvendig for å skjerme Etterretningstjenestens ansatte, kilder, kapasiteter, metoder og operasjoner mot risiko for offentlig eksponering eller kompromittering overfor annen stat.

§ 11-6 *Innsyn i opplysninger i Etterretningstjenesten*

Offentleglova gjelder ikke for innsyn i opplysninger som behandles av Etterretningstjenesten etter loven her.

Av sikkerhetsmessige grunner har en person ikke rett til innsyn i

a. etterretningsinformasjon som Etterretningstjenestens behandler eller har behandlet om vedkommende, eller
b. om Etterretningstjenesten behandler eller har behandlet, herunder utlevert til andre, etterretningsinformasjon om vedkommende.

Begjæringer om innsyn som nevnt i annet ledd skal avvises. Enhver som mener at Etterretningstjenesten har begått urett mot seg, kan klage til EOS-utvalget etter EOS-kontrollovens bestemmelser.

§ 11-7 *Forholdet til forvaltningsloven*

Med unntak av forvaltningsloven §§ 13 til 13 f om taushetsplikt, kommer forvaltningsloven ikke til anvendelse for saksbehandlingen som knytter seg til utførelsen av Etterretningstjenestens oppgaver etter loven her.

§ 11-8 *Underretning*

Den som har vært gjenstand for informasjonsinnhenting som kan innebære inngrep i dennes menneskerettigheter, har ikke krav på underretning om inngrepet.

Kapittel 12. Straff

§ 12-1 *Straff*

Den som forsettlig eller grovt uaktsomt bryter taushetsplikt etter § 11-1, straffes med bot eller fengsel inntil 1 år eller begge deler, hvis ikke forholdet går inn under en strengere straffebestemmelse.

Grovt brudd på taushetsplikten straffes med fengsel inntil 6 år. Ved avgjørelsen av om bruddet er grovt skal det særlig legges vekt på graden av skyld og om bruddet har skadet Etterretningstjenestens virksomhet eller lett kunne ha ført til slik skade.

Den som ødelegger eller manipulerer aktivitetslogger som nevnt i § 7-10, straffes med bot eller fengsel inntil 1 år eller begge deler, hvis ikke forholdet går inn under en strengere straffebestemmelse.

Den som overtrer bestemmelser gitt i eller i medhold av §§ 7-2 eller 7-3, straffes med bot eller fengsel inntil 6 måneder eller begge deler, hvis ikke forholdet går inn under en strengere straffebestemmelse.

§ 12-2 *Straffrihet for lovlige tjeneste- eller oppdragshandlinger*

Ansatte i eller kilder eller oppdragstakere for Etterretningstjenesten kan ikke straffes for lovlige tjeneste- eller oppdragshandlinger.

Kapittel 13. Ikrafttredelse og endringer i andre lover

§ 13-1 *Ikrafttredelse*

Loven trer i kraft fra det tidspunktet Kongen bestemmer. De ulike bestemmelsene kan settes i kraft til ulik tid.

§ 13-2 *Opphevelse*

Fra det tidspunktet loven trer i kraft oppheves lov 31. august 1998 nr. 11 om Etterretningstjenesten.

§ 13-3 *Endringer i andre lover*

Fra det tidspunktet loven trer i kraft gjøres følgende endringer i andre lover:

1. I lov 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker skal «lov om Etterretningstjenesten § 12-1 annet ledd» føyes til i opplistingen av bestemmelser i §§ 202 a annet ledd bokstav b, 202 c første ledd, 216 a første ledd bokstav b og 217 o første ledd bokstav b.

2. I lov 3. februar 1995 nr. 7 om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste gjøres følgende endringer:

   § 5 femte ledd skal lyde:

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

   § 15 første ledd tredje punktum skal lyde:

   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 for det offentlige overfor klageren.*

3. I lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon gjøres følgende endringer:
   § 2-8 nytt fjerde ledd skal lyde:

   Regler om tilretteleggingsplikt for Etterretningstjenestens innhenting av elektronisk kommunikasjon som transporteres over den norske landegrensen følger av lov om Etterretningstjenesten § 7-2.

   § 6-2 a første ledd nytt siste punktum skal lyde:
   Etterretningstjenesten kan i særskilte tilfeller og i korte tidsrom uten tillatelse fra eller varsel til myndigheten ta i bruk frekvenser som er tildelt andre når dette er et strengt nødvendig tiltak for innhenting av informasjon rettet mot person eller virksomhet som omfattes av lov om Etterretningstjenesten § 4-2 første ledd.

   § 6-2 a tredje ledd tredje punktum oppheves. Nåværende fjerde punktum blir tredje punktum.

4. I lov 20. mai 2005 nr. 28 om straff skal § 123 annet punktum lyde:
   Den som avslører en slik opplysning til en fremmed stat eller terrororganisasjon, *eller som offentliggjør en slik opplysning om identiteten til operativt personell i eller operative kilder for Etterretningstjenesten eller Politiets sikkerhetstjeneste,* anses ikke for å ha en aktverdig grunn.