DET KONGELIGE
FORSVARSDEPARTEMENT

Prop. 80 L

(2019–2020)

Proposisjon til Stortinget (forslag til lovvedtak)

Lov om Etteretningstjenesten (etterretningstjenesteloven)

DET KONGELIGE
FORSVARSDEPARTEMENT

Prop. 80 L

(2019–2020)

Proposisjon til Stortinget (forslag til lovvedtak)

Lov om Etterretningstjenesten (etterretningstjenesteloven)

Innhold

DET KONGELIGE
FORSVARSDEPARTEMENT

Prop. 80 L

(2019–2020)

Proposisjon til Stortinget (forslag til lovvedtak)

Lov om Etterretningstjenesten (etterretningstjenesteloven)

Tilråding fra Forsvarsdepartementet 22. april 2020, godkjent i statsråd samme dag.
(Regjeringen Solberg)

1 Proposisjonens hovedinnhold

Forsvarsdepartementet foreslår i denne proposisjonen en ny lov om Etterretningstjenesten (etterretningstjenesteloven). Loven vil avløse etterretningstjenesteloven av 1998.

Lovforslaget bygger på departementets høringsnotat av 12. november 2018. I lys av høringen foreslås det flere endringer i proposisjonen, blant annet for å sikre en klar regulering av forholdet mellom Etterretningstjenesten og Politiets sikkerhetstjeneste og for å styrke muligheten for kontroll med etterretningsvirksomheten. Proposisjonen er utarbeidet i nær dialog med Justis- og beredskapsdepartementet og Kommunal- og moderniseringsdepartementet.

Formålet med loven vil være å bidra til å trygge Norges suverenitet, territorielle integritet, demokratiske styreform og andre nasjonale sikkerhetsinteresser. Den skal dessuten bidra til å trygge tilliten til og sikre grunnlaget for kontroll med Etterretningstjenestens virksomhet, og sørge for at virksomheten utøves i samsvar med menneskerettighetene og andre grunnleggende verdier i et demokratisk samfunn.

Den nye loven vil i hovedsak kodifisere gjeldende regelverk og praksis, men det foreslås også nyvinninger. Departementet foreslår blant annet regler om tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon. Forslaget, som blant annet følger opp Lysne II-utvalgets rapport av 26. august 2016 om digitalt grenseforsvar, vil styrke Norges selvstendige etterretningsevne og vår mulighet til å oppdage og motvirke spionasje, sabotasje, terrorhandlinger og andre trusler mot nasjonale sikkerhetsinteresser.

Et hovedformål med reformen er å gi Etterretningstjenestens virksomhet en sikker rettslig forankring, særlig med hensyn til den menneskerettslige utviklingen. Forslaget følger opp Stortingets anmodningsvedtak nr. 466 av 21. februar 2017, hvor regjeringen ble bedt om å legge frem forslag til revidert lov. Bakgrunnen for anmodningsvedtaket var EOS-utvalgets særskilte melding til Stortinget 17. juni 2016, hvor utvalget reiste spørsmål om gjeldende lov tilfredsstiller lovskravet som følger av menneskerettighetene. Av

hensyn til lovskravet foreslår departementet å regulere bruk av metoder for innhenting av informasjon som kan utgjøre et inngrep overfor den enkelte.

Den nye loven kan ses i lys av en utvikling i demokratiske rettsstater mot å regulere etterretningsvirksomheten så åpent og detaljert som mulig innenfor rammen av legitime behov for skjerming og hemmelighold. Norge bør bidra til denne utviklingen, som bygger opp under den tilliten etterretningstjenester er avhengige av i åpne og frie samfunn som det norske. Departementet har ved utformingen av loven sett hen til nærstående lands lovgivning og internasjonale anbefalinger på området.

I lovforslagets *kapittel 1* foreslår departementet bestemmelser om lovens formål og virkeområde, mens *kapittel 2* inneholder regler om organisering, styring og kontroll. Regler om Etterretningstjenestens oppgaver foreslås i lovforslagets *kapittel 3*. Forslaget er i hovedsak en videreføring av gjeldende rett, men oppgavene angis på en mer presis måte enn tidligere.

Lovforslagets *kapittel 4* inneholder forbud mot innhenting i Norge og andre særskilte forbud. Det foreslås som den store hovedregel at Etterretningstjenesten ikke kan bruke innhentingsmetoder overfor personer i Norge. Hovedregelen viderefører den territorielle begrensningen i gjeldende lov. Unntaket etter gjeldende rett for fremmed statsaktivitet videreføres, men med en viss innstramming. Det foreslås en egen bestemmelse om samordning med Politiets sikkerhetstjeneste.

Departementet foreslår å gjøre det klart at forbudet mot innhenting i Norge ikke er til hinder for å innhente informasjon om utenlandske forhold fra åpne kilder, selv om informasjonen er publisert av eller på annen måte berører personer i Norge. Det foreslås også å regulere innhenting av informasjon om personer i Norge i forbindelse med trening, øving og testing av utstyr, samt kilderekruttering og kildeverifikasjon.

Forslaget klargjør at det ikke er i strid med loven at informasjon om personer i Norge vil kunne følge med ved innhenting overfor personer i utlandet. Det tydeliggjøres også at rådata i bulk kan innhentes selv om informasjon om personer i Norge vil kunne følge med. For å tydeliggjøre formålsbegrensningen til utenlandsetterretning foreslås det å lovfeste forbud mot å innhente informasjon med politiformål og forbud mot industrispionasje.

Grunnvilkår for informasjonsinnhenting, metodebruk og utlevering av informasjon følger av lovforslagets *kapittel 5*. Det foreslås at målsøking (søk etter ukjente mål) og målrettet innhenting (mot kjente mål) kan finne sted når det foreligger grunn til å undersøke om innhenting kan frembringe informasjon som er relevant for etterretningsformål. Det foreslås også å lovfeste et grunnleggende forholdsmessighetsprinsipp som innebærer at innhenting og utlevering av informasjon ikke skal gjennomføres dersom det vil være et uforholdsmessig inngrep overfor den enkelte.

I lovforslagets *kapittel 6* foreslår departementet å lovfeste metoder for innhenting av informasjon som kan medføre inngrep overfor den enkelte. Det foreslås regler om generelle vilkår, åpne kilder, menneskebasert innhenting, systematisk observasjon, teknisk sporing, gjennomsøking, avlytting og bildeovervåkning, annen teknisk innhenting, midtpunktinnhenting, endepunktinnhenting og forberedende tiltak. Det foreslås også regler om beslutningskompetanse, beslutningens varighet og krav til beslutningen.

Lovforslagets *kapittel 7 og 8* inneholder bestemmelser om tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon. Forslaget følger opp anbefalinger fra uavhengige ekspertutredninger, inkludert Lysne II-utvalgets rapport av 26. august 2016 om digitalt grenseforsvar. Forslaget innebærer at Etterretningstjenesten får hjemmel til å innhente og lagre store mengder metadata om elektronisk kommunikasjon som krysser den norske grensen. Tilbydere av ekomtjenester skal legge til rette for innhentingen. Fordi norsk innenlandsk kommunikasjon i stor utstrekning krysser grensen, foreslås det strenge begrensninger og kontrollmekanismer. Søk i lagrede metadata krever kjennelse fra Oslo tingrett, og tjenesten kan ikke innhente og lagre innholdsdata før retten har godkjent det. Departementet foreslår også at EOS-utvalget skal føre løpende kontroll. Som ledd i denne kontrollen gis Oslo tingrett myndighet til å stanse ulovlig innhenting på begjæring fra EOS-utvalget. Av hensyn til å unngå formålsutglidning foreslås det forbud mot å utlevere overskuddsinformasjon og bevisforbud i straffesaker.

Behandling av personopplysninger for etterretningsformål reguleres i lovforslagets *kapittel 9*. Departementet foreslår regler om behandlingsgrunnlag, diskrimineringsforbud, krav til korrekte og oppdaterte personopplysninger, sletting, informasjonssikkerhet og personvernrådgiver. Det foreslås forbud mot å behandle fortrolig kommunikasjon med bestemte yrkesutøvere, for eksempel advokater, og opplysninger som er betrodd noen i deres journalistiske virke og som kan avsløre hvem som er kilde for opplysningen.

Regler om nasjonalt og internasjonalt samarbeid og informasjonsutveksling følger av lovforslagets *kapittel 10*. Forslaget viderefører i hovedsak gjeldende regelverk og praksis.

Lovforslagets *kapittel 11* inneholder regler om taushetsplikt, krav til statsborgerskap og sikkerhetsklarering. Det foreslås også regler om skjerming av operasjoner, om arkiver, informasjonssystemer og etterretningsregistre, samt om beredskap, klage og straff.

Det foreslås enkelte endringer i andre lover. I ekomloven foreslås en tilføyelse som gir grunnlag for å etablere mobilregulert sone for innhenting av informasjon om fremmed statsaktivitet i Norge. Etterretningstjenesten skal også kunne etablere mobilregulert sone for øvingsformål utenfor permanente øvingsområder. Det foreslås at offentleglova ikke skal gjelde for Etterretningstjenestens virksomhet etter etterretningstjenesteloven.

Departementet foreslår at loven trer i kraft når Kongen bestemmer, og at bestemmelsene kan settes i kraft til ulik tid.

2 Bakgrunnen for lovforslaget

2.1 Stortingets anmodningsvedtak nr. 466 (2016–2017)

Stortinget fattet 21. februar 2017 anmodningsvedtak nr. 466 (2016–2017):

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

Om bakgrunnen for vedtaket vises det til Innst. 164 S (2016–2017) fra Stortingets kontroll- og konstitusjonskomité om Særskilt melding fra Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget) om rettsgrunnlaget for Etterretningstjenestens overvåkingsvirksomhet.

Anmodningsvedtaket følges opp gjennom at det i denne proposisjonen legges frem forslag til ny lov om Etterretningstjenesten.

2.2 Høringen

Høringsnotatet med forslag til ny lov om Etterretningstjenesten ble sendt på høring 12. november 2018 med høringsfrist 12. februar 2019. Høringsbrevet ble sendt til følgende instanser:

Departementene

Høyesterett
Lagmannsrettene
Oslo tingrett
Bergen tingrett
Sør-Trøndelag tingrett

Forsvarsstaben
Etterretningstjenesten
Forsvarets sikkerhetsavdeling (FSA)
Generaladvokaten
Kripos
Politidirektoratet
Politiets sikkerhetstjeneste (PST)
Regjeringsadvokaten
Riksadvokaten
Statsadvokatembetene
Økokrim

Datatilsynet
Domstoladministrasjonen
Direktoratet for e-helse
Direktoratet for forvaltning og IKT (Difi)
Direktoratet for samfunnssikkerhet og beredskap (DSB)
Finanstilsynet
Forsvaret
Fylkesmennene
Helsedirektoratet
Kommunenes Sentralforbund (KS)
Kommunal Informasjonssikkerhet (KINS)
Kontrollutvalget for kommunikasjonskontroll
Kystverket
Nasjonal kommunikasjonsmyndighet (Nkom)
Nasjonal sikkerhetsmyndighet (NSM)
Norges Bank
Riksrevisjonen
Skatteetaten
Statens strålevern
Teknologirådet
Toll- og avgiftsdirektoratet
Utlendingsdirektoratet

Norges institusjon for menneskerettigheter (NIM)
Sivilombudsmannen
Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget)

Forsvarets forskningsinstitutt (FFI)
Institutt for forsvarsstudier (IFS)
Norges teknisk-naturvitenskapelige universitet (NTNU)
Politihøgskolen
Universitetet i Bergen
Universitetet i Oslo
Universitetet i Tromsø

Abelia
Akademikerne
Amnesty International Norge
Befalets fellesorganisasjon (BFO)

Den internasjonale juristkommisjon – norsk avdeling (ICJ-Norge)
Den Norske Advokatforening
Den norske Atlanterhavskomité (DNAK)
Den norske dataforening
Den norske dommerforening
Det norske Veritas
Finans Norge
FinansCERT
Folk og Forsvar
IKT Norge
Krigsskoleutdannede offiserers landsforening (KOL)
Landsorganisasjonen i Norge (LO)
Landsutvalget for tillitsvalgte i Forsvaret
Norges forskningsråd
Norges forsvarsforening
Norges Juristforbund
Norges ingeniør- og teknologiorganisasjon (NITO)
Norsk offisersforbund
Næringslivets Hovedorganisasjon (NHO)
Norsk Personvernforening
Norges Rederiforbund
Norges Røde Kors
Norsk senter for informasjonssikring (NorSIS)
Næringslivets Sikkerhetsråd (NSR)
Norsk Studentorganisasjon
Norsk Utenrikspolitisk Institutt (NUPI)
Politiets Fellesforbund
Politijuristene
Rettspolitisk forening
Statsadvokatenes forening
Tekna – Teknisk-naturvitenskapelig forening
Yrkesorganisasjonenes Sentralforbund (YS)

DNB ASA
Equinor ASA
IBM AS
Kongsberg Våpenfabrikk
Microsoft Norge AS
NAMMO AS
NetCom GSM AS
Norges Bank
Norsk Hydro ASA
Software Innovation
Statnett SF
Tele2 Norge AS
Telenor Norge AS
Teleplan AS
Telia Norge AS
Uninett AS

Norsk Journalistlag
Norsk Presseforbund
Norsk Redaktørforening
Norsk Rikskringkasting
Norsk Telegrambyrå
TV2 AS

Følgende høringsinstanser hadde merknader til forslaget:

Justis- og beredskapsdepartementet

Borgarting lagmannsrett
Oslo tingrett

Det nasjonale statsadvokatembetet
Etisk råd for forsvarssektoren
Generaladvokatembetet
Innlandet politidistrikt
Kripos
Politidirektoratet
Politiets sikkerhetstjeneste (PST)
Riksadvokatembetet

Datatilsynet
Domstoladministrasjonen
Direktoratet for e-helse
Direktoratet for forvaltning og ikt (Difi)
Kystverket
Nasjonal kommunikasjonsmyndighet (Nkom)
Nasjonal sikkerhetsmyndighet (NSM)
Skattedirektoratet

Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget)
Norges institusjon for menneskerettigheter (NIM)

Abelia
Amnesty International
Befalets fellesorganisasjon (BFO)
Dataskydd.net og Föreningen för digitala fri- och rättigheter
Den Norske Advokatforening
Den internasjonale juristkommisjon – norsk avdeling (ICJ-Norge)
Den norske dataforening – IT-politisk råd (DND)
Elektronisk Forpost Norge
ICJ Norge – studentnettverk Bergen
NUPI – Norsk utenrikspolitisk institutt
Norges offisers- og spesialistforbund
Norsk senter for informasjonssikring
Næringslivets Sikkerhetsråd
Næringslivets hovedorganisasjon (NHO)
Piratpartiet
SINTEF

STAFO Etatsforeningen
Tekna – Teknisk-naturvitenskapelig forening
Vær- og klimagruppen Blå Himmel

Digital Projects Consulting AS
International Business Machines AS (IBM)
Runbox Solutions AS
Telenor Norge AS
Telia Norge AS
Uninett AS

Norsk Journalistlag (NJ)
Norsk Presseforbund
Norsk Redaktørforening
NRK

Dommerne Åsne Julsrud, Erland Flaterud, Elizabeth Baumann, Anne Horn, Heidi Heggdal og Finn-Arne Selfors
Professor Morten Holmboe

Andreas Kjærstad
Arve To
Eldar Stangeland Austvoll
Emil Wisborg
Frode Roxrud Gill
Harald Øverby
Henning Norli Andersen
Marius Kjærstad
Martin Torp Dahl
Nikolai Dragnes
Oddbjørn Pedersen
Reidar I. Paasche
Richard Foss
Roland Kaufmann
Stian Oksavik

I tillegg kom det inn 18 anonyme høringsuttalelser.

Følgende høringsinstanser har uttalt at de ikke har merknader til forslaget:

Helse- og omsorgsdepartementet
Landbruks- og matdepartementet
Utenriksdepartementet
Høyesterett
Forsvarsstaben (FST)
Forsvarets forskningsinstitutt (FFI)
Norges vassdrags- og energidirektorat

Noen høringsinstanser gir uttrykk for at høringsfristen på tre måneder var for kort. Dette gjelder *Advokatforeningen*, *Datatilsynet*, *Den norske dataforening – IT-politisk råd*, *Den internasjonale juristkommisjon – norsk avdeling*, *Elektronisk Forpost Norge, Kripos*, *Norsk Presseforbund, Norsk Redaktørforening, NRK*, *Piratpartiet*, *Politidirektoratet* og *Politiets sikkerhetstjeneste*. Departementet bemerker at det følger av utredningsinstruksen at forslag til lov normalt skal legges ut på høring. Høringsfristen skal tilpasses omfanget av tiltaket og hvor viktig det er. Fristen skal normalt være tre måneder, og ikke mindre enn seks uker. Forslaget til ny etterretningstjenestelov ble lagt ut på høring med en frist på tre måneder, i samsvar med utredningsinstruksens normalfrist.

De fleste høringsinstansene har ingen innvendinger mot fristen, men departementet tar på alvor at flere mener at den var for kort. Høringsinstansene må få tilstrekkelig tid til å sette seg inn i forslaget og utarbeide sine høringsuttalelser. Samtidig må det ved fastsettelsen av høringsfristen tas hensyn til sakens fremdrift. Høringsfristen ble satt til normalfristen på tre måneder etter en avveining av disse to hensynene.

Noen høringsinstanser viser til høringsfristen for NOU 2016: 24 Ny straffeprosesslov, som var seks måneder. Departementet bemerker at den utredningen har et større omfang enn høringsnotatet med forslag til ny etterretningstjenestelov. En høringsfrist må uansett fastsettes konkret, blant annet med hensyn til sakens bakgrunn, omfang, kompleksitet og krav til fremdrift. Det har i denne saken blitt vektlagt at arbeidet med lovforslaget har høy prioritet, blant annet på grunn av den sikkerhetspolitiske og menneskerettslige betydningen av forslaget. Forslaget følger dessuten opp Stortingets anmodningsvedtak nr. 466 (2016–2017) av 21. februar 2017.

Departementet bemerker at delen av lovforslaget som under høringen har møtt sterkest kritikk, forslaget om tilrettelagt innhenting, bygger på Lysne II-utvalgets rapport om digitalt grenseforsvar, som var på høring i 2016. Høringsinstansene har derfor i noen grad allerede vært kjent med og hatt mulighet til å kommentere sentrale spørsmål som forslaget reiser.

Etter høringen har departementet hatt dialog med enkelte høringsinstanser for å få utdypet og drøftet temaer som er berørt under høringen. Departementet har blant annet hatt møter med Norges institusjon for menneskerettigheter (NIM) og medlemmer av EOS-utvalgets sekretariat.

3 Norsk utenlandsetterretning og sikkerhetspolitiske utviklingstrekk

Norsk utenlandsetterretning er et sikkerhetspolitisk virkemiddel som skal bidra til å beskytte Norges suverenitet, territorielle integritet, demokratiske styreform og andre nasjonale sikkerhetsinteresser gjennom å skaffe norske myndigheter informasjon om utenlandske forhold. Etterretningstjenesten er Norges militære og sivile utenlandsetterretningstjeneste.

Evne til å varsle om utenlandske trusler og innhente og analysere relevant informasjon er en grunnleggende forutsetning for forsvaret av Norge. Med vår geografiske plassering i et strategisk viktig område, må norske myndigheter ha oversikt over politiske og militære forhold som kan føre til spente sikkerhetspolitiske situasjoner og kriser, inkludert militærøvelser og testing av konvensjonelle og kjernefysiske militære systemer i våre nærområder. Vi må ha situasjonsforståelse til lands, over og under havoverflaten, i luften, i rommet og i det digitale domenet.

Behovet for norsk utenlandsetterretning må ses i sammenheng med aktuelle sikkerhetspolitiske utviklingstrekk og utfordringer. Departementet uttaler i Prop. 1 S (2019–2020) punkt 2.2 side 32:

> «Verda er i endring på eit anna vis enn kva vi har vore vane med dei siste tiåra. Stormaktsrivalisering kjenneteiknar dei framveksande tilhøva, og rivaliseringa er kvassare og klårare enn tidlegare. Med auka rivalisering blant dei største statane, vert dei små statane meir sårbare. Som utsett småstat har Noreg handtert denne utfordringa gjennom NATO-medlemskap og eit nært tilhøve og stønad til det internasjonale, regelbaserte systemet. No er eit slikt felles system under press. Ei årsak til rivaliseringa er at stormaktene har ulike syn på kva køyrereglar som bør gjelda for internasjonalt samkvem. Eit relatert høve er korleis engasjement gjennom fleirnasjonale kanalar og mekanismar tener deira interesser, og i kva for ein grad. Den auka rivaliseringa uttrykkjer seg på både militært og økonomisk nivå, samt gjennom ein aukande teknologisk kappestrid, særleg mellom USA og Kina.
>
> Denne kappestriden er òg reflektert ved at nye verkemiddel vert tekne i bruk, der militær makt er ein del av eit knippe politiske instrument. Eit hybrid landskap teiknar seg tydelegare. Økonomiske verkemiddel vert nytta saman med militære og paramilitære instrument. Fleire statar, medrekna Kina og Russland, har utvikla evner til å bruka slike hybride strategiar, slik at dei kan fremja interesser og sikra posisjonar utan å utløysa direkte militærkonflikt med USA. Satsinga på å utvikla ny teknologi inneber at cyber-doménet og moderne bruk av verdsrommet har vorte viktigare. Militær makt skal ikkje berre stå til rådvelde for å påverka andre land sine politiske handlingar, men òg for forsvar og avskrekking, både i meir tradisjonelle og i nye, meir ukjende kontekstar.
>
> Den raske internasjonale og teknologiske utviklinga skapar såleis fleire overlappingar og gråsoner mellom statstryggleik og samfunnstryggleik. Å taka vare på begge kan vera meir krevjande og komplisert. Evna til å sikra samfunnstryggleik vert stadig viktigare i eit hybrid landskap. All den tid Noreg i aukande grad kan vera utsett for hybride operasjonar og påverknadsfreistnader, må ein òg på norsk side sjå nærmare på korleis eit moderne norsk forsvar kan medverke til å løysa eit breitt spekter av oppdrag. Autoritære stormaktar har komparative føremoner i bruk av eit breiare knippe verkemiddel, då dei ikkje har opinion eller avgjerande demokratiske val å taka omsyn til. Brei utnytting av ulike verkemiddel gjer at fleire ikkje-militære faktorar kan få innverknad på forsvar og tryggleik. For forsvarssektoren er dette òg ei aukande utfordring.»

Den teknologiske utviklingen, blant annet moderne kommunikasjonsformer, innebærer at mulighetene til å innhente informasjon har blitt bedre. Samtidig har utviklingen gjort oss mer sårbare for angrep, spionasje, sabotasje og manipula-

sjon i det digitale rom, se for eksempel Prop. 1 S (2019–2020) punkt 2.2 side 36:

> «Dei mest alvorlege åtaka i det digitale rommet (cyberdomenet) har potensial til å setje funksjonar som er grunnleggjande for samfunnet og statstryggleiken ut av spel. Trusselen er aukande, og kjem frå primært statlege, men òg ikkje-statlege aktørar. Varslingstida har vorte kortare enn for få år sidan. Det kan ofte vere vanskeleg å slå fast at ein er under åtak, kven angriparen er og kva som er føremålet med åtaket. Ulike aktørar påverkar forståinga av røyndommen gjennom fornekting og desinformasjon i sosiale kanalar og nyhendemedium. Målet er å forme det strategiske handlingsrommet til eigen føremon. Eksempel på alvorlige åtak i cyberrommet er framand etterretningsverksemd og moglege sabotasjehandlingar. Russiske og kinesiske aktørar er framleis dei mest aktive aktørane bak nettverksbaserte etterretningsoperasjonar retta mot Noreg. Nettverksbasert sabotasje utgjer ein alvorleg, men førebels lite spesifikk trussel. Slike sabotasjeoperasjonar vil først og fremst vere aktuelle i ein alvorleg krisesituasjon, og då i kombinasjon med andre verkemiddel. Det er semje i NATO om at cyberåtak kan få like alvorlege konsekvensar som åtak med konvensjonelle våpen og at dei difor er omfatta av artikkel 5 i Atlanterhavspakta om kollektivt forsvar. Cyberdomenet er ein integrert del av militæroperasjonar, og cyberkapabilitetar vil difor vere viktige element for eit forsvar, sjølv om cyberkapabilitetar aleine neppe vil kunne avgjere mellomstatlege konfliktar.»

I Politiets sikkerhetstjenestes nasjonale trusselvurdering for 2020 heter det på side 9:

> «Datanettverksoperasjoner utgjør en vedvarende og langsiktig trussel mot Norge. Uavhengig av landegrenser og uten særlig forvarsel kan en trusselaktør påføre norske virksomheter og norsk infrastruktur stor skade. Med stor grad av anonymitet og mulighet for benektelse, kan sensitiv informasjon stjeles eller manipuleres, og kritisk infrastruktur forstyrres eller ødelegges.»

Etterretningstjenesten uttaler seg i samme retning i *Fokus 2020* på side 62:

> «Det siste tiårets tiltakende rivalisering og konfliktnivå i internasjonal stormaktspolitikk har sammenfalt med en digital revolusjon som har gjort teknologi, informasjon og internettbaserte medier langt mer tilgjengelige, og parallelt ført til en dramatisk økning i antall enheter og systemer koblet til nettet.
>
> Disse trendene har virket sammen og skapt en situasjon der påvirknings- og etterretningsaktivitet nå utgjør sentrale og integrerte virkemidler i Russlands, Kinas og andre staters kamp om status, innflytelse og økonomisk og militær makt. Etterretning brukes aktivt mot Norge og vil fortsette å utgjøre en alvorlig sikkerhetstrussel mot norske interesser framover. Etterretningsaktivitet mot politiske mål kan også være ledd i forberedelser til påvirkningsoperasjoner. Påvirkning har vedvarende stort skadepotensial, særlig i tilspissede politiske situasjoner.»

Sammensatte (hybride) trusler og «gråsoneaktiviteter» svekker tradisjonelle skillelinjer mellom fred, krise og væpnet konflikt, og kan skape usikkerhet som kan redusere Norges motstandsdyktighet og evne til krisehåndtering. God etterretningsevne er sentralt for å møte denne utfordringen.

Internasjonal terrorisme er en vedvarende trussel. Etterretningstjenesten uttaler i *Fokus 2020* på side 92:

> «De militante islamistiske miljøene i Europa har fått sin egen dynamikk basert på brede internasjonale kontaktnettverk. Disse nettverkene vil sannsynligvis utgjøre den største terrortrusselen fra militante islamister mot Europa i årene som kommer. Samtidig er det en økende oppslutning om høyrepopulistiske partier og en økning i høyreekstrem retorikk og høyreekstrem terrorisme rettet mot muslimske deler av samfunnet. Høyreekstremisme er i økende grad et internasjonalt fenomen, og bidrar til et mer sammensatt og utfordrende trusselbilde i Vesten.»

Den teknologiske utviklingen og en mer spent sikkerhetspolitisk situasjon gjør at det stilles store krav til Etterretningstjenesten. Tjenesten må være i stand til å finne de relevante informasjonsbitene i en stadig økende mengde med informasjon. De må evne å sette sammen og analysere informasjonen, og omgjøre den til etterretningsprodukter som er relevante for norske beslutningstakere. Dette forutsetter kontinuerlig utvikling og modernisering, avanserte tekniske løsninger og ansatte med høy kompetanse.

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. Koordinering av etterretningsinformasjon i internasjonale organisasjoner skjer bare unntaksvis. Samtidig har det gjennom flere år vært en økende erkjennelse av behovet for internasjonalt etterretningssamarbeid for å motvirke grenseoverskridende trusler, særlig blant land i det vestlige sikkerhetssamarbeidet. FNs sikkerhetsråd har flere ganger oppfordret til økt etterretningssamarbeid blant annet for å møte trusselen fra internasjonal terrorisme.

Norsk utenlandsetterretning må ses i sammenheng med andre sikkerhetspolitiske virkemidler. Nasjonalt samarbeid og informasjonsutveksling er avgjørende for å avdekke og motvirke grenseoverskridende trusler. Etterretningstjenesten, Politiets sikkerhetstjeneste, Nasjonal sikkerhetsmyndighet og andre relevante aktører må ha et nært samarbeid basert på gjensidig tillit.

Etterretningstjenestens virksomhet er og må være forbundet med utstrakt hemmelighold og skjerming. Samtidig er tjenesten, i et åpent og fritt samfunn som det norske, avhengig av legitimitet og tillit i befolkningen. En forutsetning for å holde hemmelig det som må holdes hemmelig, er å vise åpenhet når det er mulig. Å finne balansen mellom åpenhet og skjerming kan være vanskelig. I de senere årene har Etterretningstjenesten bidratt til mer åpenhet gjennom årlige trussel- og risikovurderinger og deltakelse i den offentlige debatten. Denne proposisjonen og utredningene som ligger til grunn for den, representerer en ytterligere omdreining i retning av åpenhet om norsk utenlandsetterretning.

4 Konstitusjonelle og menneskerettslige rammer

4.1 Innledning

Å ivareta Norges suverenitet, territorielle integritet og politiske handlingsfrihet samt borgernes rett til liv, frihet og sikkerhet er en grunnleggende oppgave for myndighetene. Grunnloven § 2 andre punktum angir demokratiet, rettsstaten og menneskerettighetene som grunnleggende verdier for vår statsform. Etterretningsvirksomhet skal bidra til å beskytte disse verdiene på en måte som lar seg forene med dem. I store trekk innebærer dette at det må treffes en balanse mellom frihet og sikkerhet.

Etterretningstjenestens virksomhet kan gripe inn i ulike rettigheter. Retten til respekt for privatlivet etter Grunnloven § 102 og EMK artikkel 8 står sentralt, og i det følgende vil departementet konsentrere seg om denne rettigheten. Virksomheten kan potensielt også gripe inn i andre rettigheter, for eksempel religionsfriheten (Grunnloven § 16 og EMK artikkel 9), ytringsfriheten (Grunnloven § 100 og EMK artikkel 10) og forenings- og forsamlingsfriheten (Grunnloven § 101 og EMK artikkel 11). Tilsvarende rettigheter følger av FNs konvensjon om sivile og politiske rettigheter (SP).

Grunnloven § 113 fastslår at myndighetenes inngrep overfor den enkelte må ha grunnlag i lov. Høyesterett har uttalt at lovskravet fremmer forutberegnelighet og legger til rette for at den enkelte kan treffe rasjonelle valg (HR-2014-2288-A avsnitt 26). Kravet motvirker vilkårlighet og usaklig forskjellsbehandling, jf. også Grunnloven § 98 første ledd, som slår fast at alle er like for loven. Lovskravet støtter Stortingets lovgiverfunksjon etter Grunnloven § 75 a og den demokratiske ideen som ligger bak 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.

4.2 Retten til respekt for privatliv, familieliv, hjem og kommunikasjon

4.2.1 Grunnloven § 102

Grunnloven § 102 lyder:

> «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.»

Det generelle vernet for privatlivets fred i § 102 første ledd første punktum er utformet som en individuell rettighet, men vernet gjelder ikke absolutt. Som på de fleste andre områder i samfunnet, må ulike hensyn balanseres. Menneskerettighetsutvalget uttaler i sin rapport på side 178:

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

Utvalget minner om at det under utøvelsen av slik overvåkning og kontroll må 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 (Innst. 186 S (2013–2014) punkt 2.1.9 side 27):

> «Det alternativ f l e r t a l l e t stiller seg bak, gjør retten til privatliv mv. i første ledd til en rettighet for den enkelte. Når retten er til «respekt for» privatlivet, er det likevel for å synliggjøre at lovlig etterretning ikke er utelukket, som

også diskutert av Menneskerettighetsutvalget.»

4.2.2 EMK artikkel 8

EMK artikkel 8 lyder i norsk oversettelse:

> «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.»

Etterretningstjenestens fordekte innhenting av informasjon om personer og påfølgende registrering av personopplysninger, vil utgjøre et inngrep hvis 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. En naturlig språklig forståelse tilsier at begrepet «privatliv» og «hjem» ikke får anvendelse på steder der offentligheten har fri adgang, og som dermed ikke tilhører individets privatsfære. Å samle inn åpent tilgjengelig informasjon om personer eller holde dem under oppsikt på offentlig sted, vil dermed normalt ikke utgjøre et inngrep. Mer systematiske former for innhenting og spaning vil derimot utgjøre et inngrep (*Peck mot Storbritannia*, 28. januar 2003). Dessuten vil systematisk innsamling og systematisering av offentlig tilgjengelige opplysninger etter forholdene kunne utgjøre et inngrep, særlig dersom opplysningene gjelder forhold som ligger langt tilbake i tid (*Rotaru mot Romania*, 4. mai 2000). I *Uzun mot Tyskland* (2. september 2010) 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.

Ikke bare individer, men også juridiske personer kan etter omstendighetene være vernet av EMK artikkel 8. 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 nr. 1. 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. EMD har lagt til grunn at ikke bare innsamling av innhold i kommunikasjon, men også av trafikkdata og metadata (data om kommunikasjon), er et inngrep i privatlivet (*Malone mot Storbritannia* 2. august 1984, avsnitt 84).

Innsamling av kommunikasjon utgjør et inngrep i seg selv, men det gjør også senere lagring, undersøkelse og bruk av informasjonen. Deling av innsamlet informasjon vil utvide gruppen som har kjennskap til de personlige opplysningene, og utgjør dermed et selvstendig inngrep. Også selve eksistensen av lovgivning som tillater hemmelig overvåkning av kommunikasjon, kan etter omstendighetene utgjøre et inngrep.

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. 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 er i den psykiske integritet, ikke den fysiske.

4.3 Myndighetenes adgang til å gjøre inngrep i rettighetene

4.3.1 Generelt

Menneskerettighetene er ikke uttømmende balansert mot hverandre, og det enkelte individs rettigheter kan dermed komme i konflikt med andres rettigheter eller med samfunnets 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.

4.3.2 Lovskravet

Myndighetenes inngrep overfor den enkelte må ha grunnlag i lov, jf. Grunnloven § 113. Også EMK

oppstiller som grunnvilkår at inngrep har hjemmel i lov. Når Høyesterett har innfortolket en tilsvarende inngrepsadgang i Grunnloven som etter EMK, har forutsetningen vært at inngrepet har «tilstrekkelig hjemmel», se HR-2015-206-A avsnitt 60 og HR-2014-2288-A avsnitt 23 til 30, som begge gjaldt Grunnloven § 102 og EMK artikkel 8. Dette innebærer at Grunnlovens hjemmelskrav i § 113 på dette området må tolkes og anvendes i samsvar med lovskravet i EMK.

Metodene som foreslås regulert i lovforslaget, innebærer i hovedsak handlinger som etter departementets vurdering krever hjemmel i lov. Reguleringen oppfyller kravet om at det må foreligge rettslig grunnlag i eller i medhold av nasjonal lov.

Lovskravet har også en kvalitativ side. Det stilles krav om at lovgivningen må være tilstrekkelig *klar* og *forutberegnelig*. I dette ligger blant annet at lovgivningen må være tilgjengelig og utformes i tråd med alminnelige rettsstatsprinsipper. Lovskravet har som formål å verne mot vilkårlige myndighetsinngrep. Jo større inngrepet anses for å være, desto strengere krav har EMD stilt til lovgrunnlaget. EMD oppsummerte sin praksis i *Roman Zakharov mot Russland* (4. desember 2015) avsnitt 228:

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

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 har mulighet til å forstå innholdet. For eksempel vil fragmentert og sterkt skjønnsmessig lovgivning kunne være både vanskelig å finne frem til og forstå rekkevidden av. At lovforslaget i proposisjonen 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 Etterretningstjenestens oppgaver og metoder, og dermed større demokratisk legitimitet.

En annen grunntanke ved klarhetskravet er at den enkelte skal ha mulighet til 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 dette 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 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 formålet med informasjonsinnhentingen. EMD uttaler om dette i *Roman Zakharov mot Russland* avsnitt 229:

> «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.»

I denne forbindelse er det et viktig poeng at Etterretningstjenestens oppgave er å oppfylle myndighetenes informasjonsbehov, og i motsetning til politi- og sikkerhetstjenester ikke har håndhevelses- eller beslutningsmyndighet overfor enkeltpersoner. Selv om tjenestens virksomhet i seg selv kan være inngripende, innebærer dette at informasjon som innhentes om personer, ikke blir brukt til å treffe beslutninger som direkte berører disse uten at dette først vurderes, besluttes og effektueres av en eller flere andre aktører, for eksempel av politiet som grunnlag for å be retten om kjennelse om 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 begrunner lovskravet i ny etterretningstjenestelov. 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. Domstolen uttaler for eksempel i *Roman Zahkarov mot Russland* avsnitt 229:

> «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. *Demokratihensynet* er også viktig. Når inngrep bare kan skje i henhold til fastsatte normer som tilfredsstiller minstekrav til notoritet og publisitet, reduseres faren for myndighetsoverskridelse. Tilstrekkelig klart utformede regler bidrar til å forhindre vilkårlighet og sikre kontrolladgangen, og motvirker dermed risikoen for myndighetsmisbruk. Som en generell rettesnor oppstiller EMD krav om at lovgivningen må være «particularly precise» (*Kruslin mot Frankrike*, 24. april 1990). 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 skjulte inngrep. EMD uttaler i *Roman Zakharov mot Russland* 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 seks minstekrav til hva et lovverk som hjemler skjulte innhentingsmetoder må regulere. Bestemmelsene må si noe om karakteren av de handlinger som kan begrunne et tiltak, hvem tiltaket kan ramme, varigheten av tiltaket, prosedyreregler for innsamling, undersøkelse, bruk og lagring av informasjon, samt bestemmelser om deling og om sletting av informasjon. EMD uttalte følgende i *Roman Zakharov mot Russland* avsnitt 231 og *Centrum for rättvisa mot Sverige* (ikke rettskraftig kammerdom) 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 HR-2014-2288-A. Saken gjaldt bruk av overskuddsmateriale fra politiets kommunikasjonskontroll som bevis i en straffesak. Førstvoterende uttalte i avsnitt 30 at det ikke er tilstrekkelig at loven formelt sett er i orden og at den etter alminnelige tolkningsprinsipper gir grunnlag for lagringen, det gjelder også kvalitative krav:

> «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 og presist 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 lovteksten kan utformes, kan potensielt føre til at lovgiver avstår fra å vedta lover som samfunnet har behov for. Dette vil igjen kunne ha en negativ effekt på folks rettsoppfatning. EMD uttaler om dette i *Szabó og Vissy mot Ungarn* (12. januar 2016) avsnitt 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 gir uttrykk for tilsvarende synspunkter i *Roman Zakharov mot Russland* avsnitt 247, og tilføyer:

> «By their very nature, threats to national security may vary in character and may be unanticipated or difficult to define in advance.»

Samtidig er domstolen på vakt mot skjønnsmessige vilkår som legger stor diskresjonær kompetanse til utøvende myndighet, se *Roman Zakharov mot Russland* avsnitt 230 og 247 og *Szabó og Vissy mot Ungarn* avsnitt 65:

> «[T]he 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 lovskravet være. EMD har samtidig understreket at det ikke er grunn til 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 spillerommet for bruk av skjønn (*Kennedy mot Storbritannia* 18. mai 2010, avsnitt 162).

Departementet legger på bakgrunn av denne drøftelsen til grunn at loven må utformes med et tilstrekkelig presisjonsnivå med hensyn til hvilke oppgaver Etterretningstjenesten skal løse, hvilke inngripende metoder tjenesten kan ta i bruk for å løse disse oppgavene og hvilke prosedyrer som skal gjelde for innhenting og behandling av informasjon, herunder regler om bruk, deling og sletting. Det er dessuten avgjørende at reglene utformes på en måte som legger til rette for en effektiv kontroll med tjenestens virksomhet.

4.3.3 Legitimt formål

For at et inngrep skal kunne tillates, må det forfølge et *legitimt formål*. For eksempel må inngrep i EMK artikkel 8 om privatlivets fred være nødvendig av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forbygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter eller friheter. Generelt vil Etterretningstjenestens virksomhet falle inn under formålene nasjonal sikkerhet og offentlig trygghet.

4.3.4 Forholdsmessighetsvurderingen

Det tredje grunnkravet for at inngrep 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, og at interessene som begrunner inngrepet etter en samlet vurdering anses som mer tungtveiende enn de interessene som krenkes. «Nødvendig» er ikke det samme som «absolutt nødvendig» eller «uunnværlig», men på samme tid kreves det 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 det må forventes å ha effekt. Inngripende tiltak som settes i verk for sikkerhets skyld, eller fordi de kanskje vil ha effekt, 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 forebyggende øyemed. Menneskerettighetene krever ikke at trusselen på forhånd må ha manifestert seg gjennom konkrete handlinger.

Det er videre et krav at formålet ikke kan ivaretas gjennom andre rimelige og mindre inngripende tiltak. Hvorvidt inngrepet er forholdsmessig, må vurderes konkret i den enkelte sak, og alle relevante hensyn kan tas i betraktning. I vurderingen må det tas hensyn til hvilken skjønnsmargin EMD normalt tilkjenner statene på det aktuelle samfunnsområdet. EMD har lagt til grunn at statene har en nokså vid skjønnsmargin med hensyn til hvilke midler som kan benyttes for å ivareta nasjonal sikkerhet. I *Klass mfl. mot Tyskland* (6. september 1978) aksepterte domstolen systemer for hemmelig avlytting under henvisning til den rådende nasjonale terrortrusselen. I *Weber og Saravia mot Tyskland* (29. juni 2006) uttalte domstolen i avsnitt 106:

> «[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.»

Under henvisning til denne uttalelsen heter det i *Centrum för rättvisa mot Sverige* (ikke rettskraftig kammerdom) avsnitt 112:

> «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 systemer for hemmelig innhenting av informasjon kan misbrukes under dekke av å ivareta nasjonal sikkerhet, og dermed kan ende opp med å undergrave demokratiet eller til og med ødelegge det, er det behov for effektive garantier mot misbruk. Domstolen uttaler i *Weber og Saravia mot Tyskland* avsnitt 106:

> «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 and 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 authorise, carry out and supervise them, and the kind of remedy provided by the national law.»

EMD har derfor lagt til grunn at selv om statene har en vid skjønnsmargin når det gjelder hvilket etterretningsregime som er nødvendig av hensyn til nasjonal sikkerhet, vil skjønnsmarginen være snevrere når det gjelder den nærmere utformingen av tiltakene. Om dette heter det i *Centrum för rättvisa mot Sverige* (ikke rettskraftig kammerdom) 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 minimise the risk of abuses of power […]«

Disse seks rettsikkerhetsgarantiene er listet opp i punkt 4.3.2 over. Det understrekes at statene i utformingen av konkrete tiltak har en viss skjønnsmargin. Det understrekes dessuten at den konkrete bruken av et tiltak også må oppfylle kravene etter EMK artikkel 8, se nærmere punkt 9.5.3 og lovforslaget § 5-4, som lovfester et grunnleggende prinsipp om forholdsmessighet.

Sentralt i proporsjonalitetsvurderingen er hvorvidt det eksisterer tilstrekkelige og effektive garantier mot misbruk og vilkårlighet. Den som er gjenstand for fordekt informasjonsinnhenting, vil som utgangspunkt ikke selv være kjent med det, og vil dermed ikke kunne påklage inngrepet. EMD har derfor innfortolket et krav til effektiv og uavhengig kontroll for å hindre myndighetsmisbruk. EMD foretar en samlet vurdering av alle systemets mekanismer og samspillet mellom dem, på tvers av minstekravene. EMD vurderer blant annet karakteren, omfanget og varigheten 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.

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 (*Klass mfl. mot Tyskland* avsnitt 55 til 56 og *Kennedy mot Storbritannia* avsnitt 167.) 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. Domstolen fant i *Klass mfl. mot Tyskland* at kontroll av en parlamentarisk komité med balansert politisk sammensetning og en uavhengig myndighetskommisjon var tilstrekkelig.

Kontrolltiltakene spiller inn i alle stadier i prosessen: Når inngrepet igangsettes, mens det utfø-

res og etter at det er avsluttet. 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 det. Dette stiller ekstra strenge krav til kontrollens kvalitet. Når det gjelder den etterfølgende kontrollen, legger EMD særlig vekt på hvilken mulighet den enkelte har til å få prøvd lovmessigheten av et mulig eller faktisk inngrep. EMD har lagt stor vekt på klageadgang som en garanti mot myndighetsmisbruk. Dette behovet kan ivaretas ved underretning (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 å sannsynliggjøre at et inngrep har funnet sted, kan avhjelpe manglende underretning.

4.4 Krav til effektive rettsmidler

4.4.1 Utgangspunkter

Det følger av EMK artikkel 13 at enhver som har fått sine konvensjonsrettigheter krenket, skal ha en effektiv prøvingsrett ved en nasjonal myndighet. En lignende bestemmelse finnes i FNs konvensjon om sivile og politiske rettigheter (SP) artikkel 2 nr. 3. Departementet tar i det følgende utgangspunkt i 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. Saker som angår nasjonal sikkerhet skiller seg ut fra andre saker når det gjelder EMK artikkel 13. I denne type saker har statene vist til at det i lys av nasjonale sikkerhetshensyn bare kan være begrenset grad av overprøving. 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 i *Klass mfl. mot Tyskland* avsnitt 69:

> «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.

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 i *Roman Zakharov mot Russland* som unødvendig å behandle spørsmålet om rett til en effektiv prøvingsrett separat.

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 være.

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 mfl. mot Tyskland* slik at enhver som hevder at vedkommendes konvensjonsrettigheter er blitt krenket, har en slik rett (avsnitt 64). I senere saker har imidlertid EMD presisert dette til at klager må ha «an arguable claim» (en prosedabel grunn) til å hevde at vedkommende er blitt utsatt for en konvensjonskrenkelse, se for eksempel *Leander mot Sverige* (26. mars 1987) avsnitt 77.

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. Personer innenfor statens territorium er klart nok innenfor statens jurisdiksjon. Det foreligger mer usikkerhet knyttet til i hvilken utstrekning EMK får anvendelse på informasjonsinnhenting i statlig regi som skjer eller får virkning utenfor statens territorium, altså spørsmålet om konvensjonens ekstraterritorielle anvendelse i slike situasjoner.

4.4.2 Er klageadgangen etter gjeldende rett tilstrekkelig vid?

4.4.2.1 Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (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 overvåkning.

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». Spørsmålet om utvalgets adgang til å behandle klager fra personer som ikke er bosatt i Norge, ble vurdert av det stortingsoppnevnte Evalueringsutvalget for EOS-utvalget, som ble nedsatt 27. mars 2014. Utvalget uttaler på side 139 i sin rapport (Dokument 16 (2015–2016)):

> «Etter Evalueringsutvalgets syn er det, på bakgrunn av den utvikling av menneskerettighetenes geografiske virkeområde 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. 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.

Evalueringsutvalgets uttalelser synes å forutsette at EOS-utvalgets adgang til å gjøre unntak fra hovedregelen der «særskilte grunner tilsier det», i tilstrekkelig grad åpner for at personer som befinner seg innenfor norsk jurisdiksjon kan klage, selv om de ikke er bosatt eller har tilhold i Norge, jf. EMK artikkel 1 og 13. Departementet er enig i dette, og legger til grunn at klageadgangen til EOS-utvalget etter gjeldende rett er tilstrekkelig vid.

4.4.2.2 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. Vilkårene for å fremme en sivil sak for domstolene er regulert i tvisteloven § 1-3. Den som reiser saken må ha et «rettskrav» og 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». Departementet legger til grunn at tvisteloven § 1-3 gir 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 er innenfor den norske statens jurisdiksjon, jf. særlig EMK artikkel 1 og EMDs praksis knyttet til denne.

4.4.3 Institusjonelle og materielle krav til en effektiv prøvingsrett

4.4.3.1 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* avsnitt 77:

> «[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.»

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, jf. *Klass mfl. mot Tysland* avsnitt 55 til 56 og *Kennedy mot Storbritannia* avsnitt 167. EMD har ikke oppstilt som krav at myndigheten er en domstol («judicial authority»), men hvis den ikke er det, vil graden av uavhengighet og garantiene som er tillagt den aktuelle myndigheten være relevante i vurderingen av om prøvingsretten er effektiv, se for eksempel *Leander mot Sverige* avsnitt 77 og 83 og *Rotaru mot Romania* avsnitt 69. Som nevnt under punkt 4.3.4 fant EMD i *Klass mfl. mot Tyskland* at en parlamentarisk komité med balansert politisk sammensetning og en uavhengig myndighetskommisjon var tilstrekkelig (avsnitt 70).

Videre må klageorganet ha kompetanse til å vurdere klagens *materielle innhold* samt til å gi passende *oppreisning* («appropriate relief»), se *Rotaru mot Romania* avsnitt 67. 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 begåtte krenkelser. EMD vil også legge vekt på om klageorganet har tilgang til sikkerhetsgradert materiale som er nødvendig for å foreta en reell overprøving, se *Kennedy mot Storbritannia*.

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 må ha kompetanse til treffe en formelt bindende avgjørelse som stanser eller kompenserer for krenkelser.

I *Centrum för rättvisa mot Sverige* (ikke rettskraftig kammerdom) fant EMD etter en helhetsvurdering at summen av de tilgjengelige rettsmidlene i Sverige var effektive selv om ingen av klageorganene (*Justitieombudsmannen* og *Justitiekanslern*) 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 fullt ut av den svenske etterretningstjenesten. I tillegg viste retten til at kontrollorganet kunne vurdere erstatning dersom en menneskerettskrenkelse hadde fått alvorlige følger for klager som hadde medført økonomisk tap.

4.4.3.2 Underretning (notifikasjon)

Et annet særskilt spørsmål er i hvilken grad personer som er blitt utsatt for inngrep i form av informasjonsinnhenting må underrettes (notifiseres) 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 ikke kan kreves at den enkelte skal varsles eller på annen måte kunne forutse når overvåkningen vil bli gjennomført, se for eksempel *Roman Zakharov mot Russland* avsnitt 229.

EMD legger i samme dom til grunn at hvis, og så snart, det kan skje uten å undergrave formålet med overvåkningstiltaket eller tjenestens virksomhet, bør i utgangspunktet den overvåkede personen notifiseres om overvåkningen i etterkant (avsnitt 234 og 288). Men dette er ikke et absolutt krav dersom 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.

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. 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.

4.4.4 Oppfyller norsk rett kravene til en effektiv prøvingsrett?

4.4.4.1 Uavhengighet

Departementet finner det klart at både EOS-utvalget og domstolene oppfyller kravet til uavhengighet fra myndighetene som beslutter å gjennomføre informasjonsinnhentingen. EOS-utvalget utnevnes av Stortinget. Det følger av EOS-kontrolloven § 1 femte ledd at utvalget skal utføre sitt verv selvstendig og uavhengig av Stortinget.

4.4.4.2 Kompetanse til å prøve sakens materielle innhold

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

Departementet legger også til grunn at domstolene har kompetanse til å prøve hvorvidt det har funnet sted en menneskerettskrenkelse. Det kan imidlertid reises spørsmål om tvisteloven § 22-1 er til hinder for en reell prøving. 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. 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. Bevisforbudsregelen kan utgjøre et hinder for materiell vurdering av saken, men den må ikke gjøre det. Regjeringen vil måtte vurdere hver sak konkret, herunder hvilke tiltak som kan treffes for å sikre forsvarlig informasjonssikkerhet knyttet til bevisføring, samt hvorvidt klager har tilgang til andre effektive rettsmidler. I kongelig resolusjon 10. januar 2020 ble det gitt tillatelse til å føre graderte dokumenter i en sak i Oslo tingrett (19-026476TVI-OTIR/07) under forutsetning av nødvendige skjermingstiltak for å ivareta hensynet til nasjonal sikkerhet. Denne saken illustrerer at bevisforbudsregelen ikke nødvendigvis utgjør et hinder for reell prøving i domstolen av denne typen saker.

I alle tilfeller betyr ikke bevisforbudsregelen at det ikke foreligger et effektivt rettsmiddel etter norsk rett dersom klage til EOS-utvalget alene anses som tilstrekkelig effektivt. Det må som nevnt legges til grunn at EOS-utvalget har tilstrekkelig kompetanse til å foreta en reell prøving.

4.4.4.3 Kompetanse til å sikre at en krenkelse opphører

Det neste spørsmålet er om norsk rett tilfredsstiller kravet om at klagebehandlingen må munne ut i at menneskerettskrenkelsen opphører eller rettes opp.

Domstolene har kompetanse til å sikre at en menneskerettskrenkelse opphører. EOS-utvalget har derimot 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 de avgir uttalelser som oppfordrer til å iverksette tiltak eller treffe beslutninger, be mottaker om å gi tilbakemelding om hva som blir foretatt, jf. § 14 sjette ledd. Dette innebærer at dersom utvalget ber om at en feil rettes opp, vil utvalget få beskjed 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. Utvalgets kontroll ble vurdert av Evalueringsutvalget for EOS-utvalget, som avga sin rapport 29. februar 2016 (Dokument 16 (2015–2016)). 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. EOS-utvalgets kontroll er både ment å legge grunnlag for Stortingets behandling av kontrollsaker og å utgjøre et selvstendig kontrollelement. Utvalget er på denne måten et hjelpemiddel for Stortinget til å sikre at den etterfølgende parlamentariske kontrollen blir effektiv, og til å verne borgerne mot urett. Selv om utvalget på denne måten er en viktig ressurs for Stortinget, er EOS-utvalget et selvstendig og uavhengig organ, jf. EOS-kontrolloven § 1 femte ledd.

EOS-utvalget ble opprettet i 1996. Den historiske årsaken var at det over tid hadde bygget seg opp en mistillit mot EOS-tjenestene og regjeringens kontroll av dem. For å kompensere for manglende innsyn i tjenestenes virksomhet ble EOS-utvalget opprettet og gitt i oppgave å kontrollere tjenestene på vegne av Stortinget og den norske befolkning. Evalueringsutvalget uttaler i sin rapport at EOS-utvalgets forankring i Stortinget først og fremst er en styrke, og anbefaler at ordningen 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 kontrollmodellen. Disse har sitt utspring

i vårt konstitusjonelle system og maktfordelingsprinsippene mellom den utøvende og lovgivende makt. Evalueringsutvalget uttaler om dette i rapporten side 126, under henvisning til NOU 1994: 4, Ot.prp. nr. 84 (1993–94) og Innst. O nr. 11 (1994–95)):

> «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 prinsippet om etterfølgende kontroll. En annen konsekvens er at EOS-utvalget må være tilbakeholdne med å overprøve EOS-tjenestenes skjønnsutøvelse. 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. 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.»

Å gi EOS-utvalget beslutningsmyndighet overfor Etterretningstjenesten står i spenning med grunnleggende prinsipper i vår statsform, og departementet kan ikke anbefale en slik løsning. Etter departementets vurdering forutsetter større strukturelle endringer en bred evaluering av hele det norske kontrollsystemet, slik Evalueringsutvalget antyder i rapporten på side 129. På grunn av EOS-utvalgets parlamentariske forankring antar departementet at en eventuell utredning bør initieres av Stortinget. Etter høringen foreslår imidlertid departementet at Oslo tingrett, på begjæring fra EOS-utvalget, skal ha myndigheten til å stanse pågående innhenting etter lovforslagets kapittel 7 og pålegge sletting av lagrede data, se punkt 11.10.4.

Departementet mener i alle tilfeller at problemstillingen ikke kommer på spissen. Selv om EOS-utvalget ikke kan treffe bindende avgjørelser overfor forvaltningen, er det utviklet gode og effektive systemer for å følge opp rapporterte avvik. Det vises i denne forbindelse til punkt 6.2 om utvalgets kontroll av Etterretningstjenesten. Departementet peker spesielt på EOS-utvalgets rolle som hjelpemiddel for Stortingets kontroll. Dersom aktivitet som EOS-utvalget mener er ulovlig, ikke avsluttes, enten på tjenestens eget initiativ eller etter instruks fra departementet, kan Stortinget holde regjeringen eller statsråden ansvarlig. Departementet peker spesielt på Stortingets mulighet til å vedta mistillit mot regjeringen eller statsråden. Stortinget har også mulighet til å reise riksrettssak mot statsråden hvis vilkårene etter Grunnloven § 86 og ansvarlighetsloven er oppfylt. Det er liten tvil om at dette har en disiplinerende effekt på forvaltningen, og at EOS-utvalgets kontroll i praksis alltid blir fulgt opp. Departementet mener på denne bakgrunn at kravet til at klageorganet skal kunne sørge for at krenkelsen opphører, er oppfylt.

4.4.4.4 Kompetanse til å sikre passende oppreisning

Det siste spørsmålet er om klageorganet har anledning til å gi passende oppreisning («appropriate relief»). Det er ingen tvil om at domstolen kan idømme krav om erstatning og oppreisning. 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 erstatning til personer utsatt for krenkelser (rapporten side 129). Utvalget konstaterte at problemstillingen reiser spørsmål av både prinsipiell og praktisk art, og som 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. Departementet slutter seg til dette, og mener at et slikt forslag må baseres på en bredere utredning av behovet for endringen og virkningene for alle EOS-tjenestene.

4.4.4.5 Konklusjon

Etter departementets vurdering oppfyller norsk rett kravet til effektive rettsmidler etter EMK artikkel 13. Departementet mener dessuten at klageadgangen er tilstrekkelig vid til at det ikke kan oppstilles krav om underretning av personer som har vært gjenstand for informasjonsinnhenting, se nærmere punkt 14.6.

5 Formål og virkeområde

5.1 Formål

5.1.1 Gjeldende rett

Formålet med gjeldende etterretningstjenestelov følger av § 1. Loven skal 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. Dessuten skal loven trygge tilliten til og sikre grunnlaget for kontroll av Etterretningstjenestens virksomhet.

5.1.2 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 5.1.2 enkelte endringer i formålsbestemmelsen for å tilpasse denne til lovforslaget for øvrig. Det ses blant annet hen til formålsbeskrivelsen i ny sikkerhetslov § 1-1 om «å bidra til å trygge Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser», som anses å være dekkende for Etterretningstjenestens samfunnsoppdrag.

Det vises til at «nasjonale sikkerhetsinteresser» er et fellesbegrep som favner både trusler mot statssikkerheten, alvorlige trusler mot samfunnssikkerheten og andre forhold som kan ha relevans for ivaretakelsen av prioriterte norske og allierte utenriks, forsvars- og sikkerhetspolitiske interesser. Det vektlegges imidlertid i større grad at det er *utenlandske* trusler som står i fokus.

Formålet knyttet til å trygge tilliten og sikre grunnlaget for kontroll foreslås videreført. Det foreslås dessuten å tilføye et tredje element i formålsbestemmelsen for å synliggjøre betydningen av menneskerettighetene og andre sentrale rettsprinsipper og demokratiske verdier i en rettsstat, herunder rettssikkerhet for den enkelte.

5.1.3 Høringsinstansenes syn

Riksadvokaten stiller seg kritisk til at loven skal ha en formålsbestemmelse, og uttaler:

> «Alle lover har et formål, men dette fremkommer som oftest i lovens forarbeider og ikke i lovbestemmelsene. Det vises i den forbindelse til f.eks. lov om politiet. Å innta målformuleringer for loven som sådan, uten at dette strengt tatt er nødvendig, bidrar til at loven blir mer omfangsrik enn nødvendig, uten at dette nødvendigvis verken påvirker tjenesteutøvelsen i Etterretningstjenesten eller er påkrevet for forståelsen av andre bestemmelser.»

Norges institusjon for menneskerettigheter (NIM) påpeker at det følger av Grunnloven og menneskerettsloven at loven må anvendes innenfor menneskerettighetenes rammer, men mener likevel at en egen bestemmelse som henviser eksplisitt til at Etterretningstjenestens virksomhet skal utøves i samsvar med menneskerettighetene har en pedagogisk funksjon, og at det er ryddig å understreke dette på en tydelig måte i lovteksten.

Teknisk-naturvitenskapelig forening (Tekna) uttaler at det er viktig for befolkningens tillit til Etterretningstjenesten – og landets myndigheter i videre forstand – at det er en god balanse mellom nasjonale sikkerhetsbehov og individuelle rettigheter. Tekna peker på at lovforslaget § 1-1 om lovens formål nettopp spesifiserer at loven skal «bidra til å trygge tilliten til» Etterretningstjenesten, samt sikre at tjenestens virksomhet «utøves i samsvar med menneskerettighetene og øvrige grunnleggende rettsprinsipper og verdier i et demokratisk samfunn».

5.1.4 Departementets vurdering

Departementet mener at loven bør ha en formålsbestemmelse som angir de grunnleggende hensyn og verdier som ligger bak loven, og som loven skal tjene til å ivareta. Det er flere grunner til dette. En formålsbestemmelse kan ha rettslig betydning ved at den gir retning for tolkningen og anvendelsen av andre bestemmelser i loven, særlig slike som åpner for skjønnsmessige vurderinger. Formålsbestemmelsen kan dessuten ha en viktig pedagogisk funksjon ved å synliggjøre de grunnleggende verdiene som loven skal tjene.

Dette kan bidra til økt bevissthet hos Etterretningstjenestens ansatte og andre som bruker loven.

Hensynet til at loven ikke bør være mer omfangsrik enn nødvendig, som *riksadvokaten* trekker frem, er et relevant mothensyn, men bør etter departementets syn ikke tillegges stor vekt. En formålsparagraf er vanlig i moderne lovgivning som retter seg mot offentlig forvaltning, se for eksempel NOU 2019: 5 Ny forvaltningslov punkt 10.10.1 side 148 og sikkerhetsloven § 1-1. Departementet går etter dette inn for å innlede loven med en formålsbestemmelse som foreslått i høringsnotatet, med enkelte språklige justeringer.

5.2 Virkeområde

5.2.1 Gjeldende rett

Virkeområdet til etterretningstjenesteloven er ikke uttrykkelig fastsatt i loven. Det følger av forarbeidene (Ot.prp. nr. 50 (1996–97) punkt 6.1 side 6) at loven gjelder for Etterretningstjenesten, og at dette henviser til tjenesten som organisatorisk, ikke funksjonelt, begrep. Etterretningstjenesteloven regulerer den strategiske etterretningstjeneste, ikke øvrig informasjonsinnsamling i Forsvaret (feltetterretning mv.).

I den grad enheter eller personer i Forsvaret midlertidig inngår som en del av Etterretningstjenesten, vil disse være bundet av tjenestens rettsgrunnlag. Det kreves i disse tilfellene at man er reelt underlagt Etterretningstjenesten og står under kontroll av sjefen for Etterretningstjenesten. Kommandooverføringen kan være av midlertidig eller gjentakende karakter, men det skal være et tydelig skille både formelt og i praksis for når enheten eller personen er under kommando av sjefen for Etterretningstjenesten og når enheten eller personen ikke er det.

Det gjelder ingen geografiske avgrensninger for etterretningstjenestelovens anvendelsesområde. Loven får anvendelse for all etterretningsvirksomhet som Etterretningstjenesten utøver, uavhengig av hvor virksomheten utøves eller har effekt.

5.2.2 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 5.2 at loven bare skal gjelde for Etterretningstjenestens utøvelse av *etterretningsvirksomhet*, og ikke for administrativ, forvaltningsmessig eller annen virksomhet som utøves av Etterretningstjenesten. Med «etterretningsvirksomhet» siktes det til systematisk innhenting og bearbeiding av informasjon som angår utenlandske forhold. Sondringen mot annen virksomhet enn etterretningsvirksomhet knyttes særlig til hva som er aktivitetens intensjon og hva informasjonen skal brukes til. Det foreslås at all virksomhet som har et *etterretningsformål*, altså å ivareta en eller flere av Etterretningstjenestens oppgaver etter lovutkastet kapittel 3, reguleres av loven.

At Etterretningstjenesten er et organisatorisk og ikke funksjonelt begrep foreslås videreført. Loven foreslås å gjelde i den grad personell eller enheter er kommandooverført til tjenesten. Det legges til grunn at lovforslaget i utgangspunktet bør gjelde globalt, og uavhengig av om etterretningsvirksomheten utøves i, på eller fra et område eller overfor en person som er underlagt norsk jurisdiksjon.

Etterretningsvirksomhet i internasjonale operasjoner med folkerettslig mandat foreslås i høringsnotatet punkt 5.2.4.4 å falle utenfor lovens virkeområde. Forutsetningen for unntaket er at informasjonsinnhentingen og -behandlingen skjer for operasjonens formål. Motsetningsvis, der informasjonen beholdes for nasjonal bruk, foreslås det at loven skal komme til anvendelse. Sondringen begrunnes med at etterretningsvirksomhet innenfor rammene av en internasjonal operasjon utøves direkte med hjemmel i det internasjonale mandatet for operasjonen og i henhold til fastsatte engasjementsregler. Unntaket foreslås for å hindre overlappende regulering.

Selv om det er et alminnelig prinsipp at fredstidslovgivningen fortsetter å gjelde i en krisesituasjon inntil noe annet er bestemt, foreslås det i høringsnotatet punkt 5.2.5 at loven gjelder i hele krisespennet, det vil si i fred, krise og væpnet konflikt. Forslaget begrunnes med å forhindre eventuell tolkningstvil.

5.2.3 Høringsinstansenes syn

Dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors kommenterer forslaget om at loven ikke bør komme til anvendelse på informasjonsinnhenting som ledd i en internasjonal operasjon med folkerettslig mandat. De mener at det er vanskelig å se at de forholdene som trekkes frem, tilsier et helt generelt unntak fra loven:

> «Det er mulig at en del bestemmelser passer dårlig i slike operasjoner, f.eks. fordi de dublerer tilsvarende normer som er gitt spesielt for operasjonen. Det er antakeligvis ikke tilsiktet at virksomheten skal skje […] helt uhindret av

> alle bestemmelser i loven, slik at heller ikke mer grunnleggende prinsipper kommer til anvendelse. Man kan også reise spørsmål om hva konsekvensene av at loven ikke gjelder, er for lovens bestemmelser om annen norsk lovgivning ikke gjelder for Etterretningstjenesten. Det har neppe vært meningen at de da «vekkes til live», men slik kan lovforslaget på dette punkt tolkes.»

De mener på denne bakgrunn at lovens anvendelse på internasjonale operasjoner under folkerettslig mandat bør overveies nærmere.

Riksadvokaten og *Kripos* mener det er unødvendig å fastslå at loven gjelder i fred, krise og væpnet konflikt, fordi dette i praksis vil omfatte alle situasjoner. *Riksadvokaten* legger til at vedtatte lover, med enkelte spesielle unntak, vanligvis alltid gjelder. Det er etter *Kripos'* syn begrensninger i dette utgangspunktet som eventuelt må fremgå av loven.

5.2.4 Departementets vurdering

5.2.4.1 Lovens saklige virkeområde

Departementet viderefører forslaget i høringsnotatet om at loven skal gjelde for Etterretningstjenesten, og at det med dette vises til tjenesten som organisatorisk og ikke funksjonelt begrep. Det følger av dette at informasjonsinnhenting utført av andre enheter i Forsvaret ikke reguleres av loven. Departementet viderefører imidlertid forslaget i høringsnotatet om at loven skal gjelde for personer og enheter for det tidsrom de er under kommando av sjefen for Etterretningstjenesten. Loven vil også komme til anvendelse for andre enn Etterretningstjenesten i den utstrekning det følger av den enkelte bestemmelse, for eksempel tilretteleggingsplikten som pålegges ekomtilbydere etter § 7-2.

Departementet opprettholder vurderingen i høringsnotatet av at loven ikke bør regulere Etterretningstjenestens virksomhet av administrativ eller forvaltningsmessig karakter. Slik aktivitet reguleres av den alminnelige lovgivningen. Foruten reguleringen av tjenestens organisering, styring og kontroll i lovforslaget kapittel 2, regulerer lovforslaget Etterretningstjenestens innhenting og annen behandling av informasjon for etterretningsformål. Departementet viderefører ikke begrepet *etterretningsvirksomhet* fra høringsnotatet.

Departementet opprettholder forslaget i høringsnotatet om at loven ikke bør regulere annen aktivitet som Etterretningstjenesten kan bli satt til å utføre som del av Forsvaret. Slike oppgaver vil, som i dag, ha et annet rettslig grunnlag enn etterretningstjenesteloven.

5.2.4.2 Lovens geografiske virkeområde

Departementet opprettholder forslaget i høringsnotatet om at loven får anvendelse for Etterretningstjenestens oppgaveløsning etter lovforslaget kapittel 3 uavhengig av hvor virksomheten geografisk utøves eller hvor den har effekt. Departementet mener det ikke er behov for å spesifisere dette særskilt i lovteksten.

Departementet presiserer at Etterretningstjenesten er underlagt begrensninger når det gjelder innhenting av informasjon i Norge, jf. lovforslaget kapittel 4. Dette innebærer imidlertid ikke at lovens virkeområde som sådan er geografisk begrenset. Departementet presiserer videre at når loven anvender begrepet «Norge», omfatter dette alt norsk territorium, det vil si det norske land-, sjø- og luftterritoriet, herunder Svalbard, Jan Mayen og bilandene.

5.2.4.3 Unntak for internasjonale operasjoner

Departementet viderefører forslaget i høringsnotatet om at loven ikke bør regulere Etterretningstjenestens informasjonsinnhenting i internasjonale operasjoner med folkerettslig mandat. Forutsetningen er at innhentingen skjer med hjemmel i folkeretten, altså at det foreligger rettslig grunnlag for utøvelse av statlig selvforsvar eller at virksomheten er hjemlet i en sikkerhetsrådsresolusjon eller i samtykke fra vertsstaten. Dessuten gjelder det bare norske styrker som opererer som del av (under kommando av eller til støtte for) en konkret internasjonal operasjon som ledes av annen stat, flere stater i fellesskap (en koalisjon) eller en internasjonal organisasjon. I tillegg er det krav om at innhentingen finner sted innenfor operasjonens mandat og engasjementsregler, og at informasjonsinnhentingen skjer på vegne av operasjonen, altså den stat, koalisjon eller internasjonale organisasjon som leder operasjonen.

Dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors stiller i sin høringsuttalelse spørsmål ved om etterretningsvirksomhet i internasjonale operasjoner skal skje helt uhindret av alle bestemmelser i loven, slik at heller ikke de grunnleggende prinsippene kommer til anvendelse. D e p a r t e m e n t e t presiserer at selv om lovens regler ikke kommer til anvendelse i disse tilfellene, vil folkeretten og engasjementsreglene

sette rammer for hva Etterretningstjenesten kan gjøre.

Dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors påpeker at det er mulig å tolke unntaket fra lovens anvendelsesområde dit hen at andre lover som ikke skal gjelde for tjenesten, blant annet offentleglova og personopplysningsloven, vil «vekkes til live», slik at de får anvendelse for tjenestens aktivitet i internasjonale operasjoner. Departementet ser en slik løsning som uhensiktsmessig, og presiserer at lovforslaget ikke skal forstås slik.

5.2.4.4 Lovens virkeområde i tid

Det er et alminnelig prinsipp i norsk rett at fredstidslovgivningen fortsetter å gjelde i en krisesituasjon, inntil noe annet 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». Om nødvendig kan det i bestemmelsene gjøres avvik fra gjeldende lov. Departementet viser for øvrig til drøftelsene i punkt 8.4.4 om forslaget til § 4-2 tredje ledd.

Av pedagogiske grunner ble det i høringsnotatet foreslått å presisere at loven skulle gjelde i fred, krise og væpnet konflikt. En slik presisering er ikke uvanlig i lovgivningen, se for eksempel ekomloven § 2-10, forsvarsloven § 2 og postloven § 17. På bakgrunn av de kritiske merknadene til *riksadvokaten* og *Kripos* foreslår departementet likevel å sløyfe presiseringen.

5.3 Forholdet til folkeretten

5.3.1 Gjeldende rett

Norsk etterretningsvirksomhet må utøves innenfor folkerettslige rammer, herunder de regler som følger av FN-pakten og internasjonal sedvanerett. Internasjonale menneskerettighetskonvensjoner danner også en viktig ramme. I væpnet konflikt gjelder dessuten krigens folkerett. I internasjonale operasjoner kan særskilte begrensninger, eksempelvis geografiske restriksjoner, følge av operasjonens mandat og engasjementsregler.

Forholdet til folkeretten er ikke regulert i dagens etterretningstjenestelov, men det følger av presumpsjonsprinsippet at loven så langt mulig skal tolkes og anvendes i samsvar med Norges folkerettslige forpliktelser.

Den europeiske menneskerettskonvensjon (EMK) gjelder som norsk lov i samsvar med menneskerettsloven § 2 nr. 1, og går ved motstrid foran annen norsk lovgivning, jf. § 3. FN-konvensjonen om sivile og politiske rettigheter (SP) er også inkorporert i norsk rett etter menneskerettsloven, og inneholder mange lignende rettighetsbestemmelser som EMK.

For at en stat skal kunne holdes ansvarlig etter EMK, er det et grunnvilkår at individet det gjelder er innenfor statens jurisdiksjon i konvensjonens forstand. Dette følger av EMK artikkel 1, som fastsetter at statspartene «skal sikre enhver innen sitt myndighetsområde» de rettigheter og friheter som er fastlagt i konvensjonen. Det følger av rettspraksis fra Den europeiske menneskerettsdomstol (EMD) at en stats jurisdiksjon etter EMK artikkel 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. EMD har oppstilt to hovedunntak fra territorialprinsippet: Situasjoner hvor statlige agenter utøver «myndighet og kontroll» over personer utenfor eget territorium, og situasjoner hvor staten utøver «effektiv kontroll» over et område.

Personer på norsk territorium er innenfor norsk jurisdiksjon i EMKs forstand. Spørsmålet om jurisdiksjon kommer på spissen der Etterretningstjenesten innhenter informasjon om utlendinger og norske borgere i utlandet. Rekkevidden av EMKs anvendelsesområde for informasjonsinnhenting i utlandet utført av en utenlandsetterretningstjeneste er ikke avklart. Hvorvidt det foreligger effektiv kontroll over et område eller myndighet og kontroll over en person, og dermed forpliktelser etter EMK utenfor eget territorium, må vurderes konkret i den enkelte sak.

5.3.2 Forslaget i høringsnotatet

Det foreslås i høringsnotatet en bestemmelse om forholdet til folkeretten. Høringsnotatet gir i kapittel 4 en deskriptiv omtale av de folkerettslige rammene, men uten å drøfte lovutkastet § 1-3 nærmere. Det foreslås i § 1-3 første ledd at loven skal gjelde med de begrensninger som er anerkjent i folkeretten eller følger av overenskomst med fremmed stat. Forslaget til andre ledd slår fast at Etterretningstjenesten ikke skal gjennomføre eller medvirke til virksomhet som innebærer en reell risiko for at ufravikelige eller andre grunnleggende menneskerettigheter krenkes.

I høringsnotatet punkt 4.1.3 redegjøres det for EMKs ekstraterritorielle virkning. Det fremheves at jurisdiksjonsspørsmålet i utgangspunktet vil

måtte vurderes konkret i det enkelte tilfellet. Samtidig presiseres det at lovforslaget er utformet slik at det tilfredsstiller menneskerettighetene uavhengig av utfallet av den konkrete jurisdiksjonsvurderingen. Det vises til at lovverket er utformet generisk, og ikke legger opp til å differensiere ut fra hvor eller overfor hvem aktiviteten finner sted. Det heter i høringsnotatet at man i så måte kan si at regelverket er utformet nasjonalitets- og geografinøytralt, og at prinsipper og krav som utledes av våre menneskerettslige forpliktelser i praksis blir anvendt overfor alle individer som Etterretningstjenesten får befatning med. Det understrekes i høringsnotatet at en nøytral utforming ikke er et resultat av en rettslig forpliktelse, men gjøres av policy- og praktiske hensyn.

5.3.3 Høringsinstansenes syn

Flere høringsinstanser, herunder *Norges institusjon for menneskerettigheter (NIM)*, *Kripos* og *dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors*, har innvendinger mot forslaget i høringsnotatet. NIM fremhever at det er uklart hvordan lovutkastet § 1-3 første og andre ledd henger sammen, og hvordan de skal forstås. Etter NIMs syn konsumerer første ledd i stor grad andre ledd, fordi menneskerettsforpliktelsene nettopp fremgår av folkeretten og våre traktatforpliktelser. NIM peker på at høringsnotatet ikke forklarer hva som er ment med begrepet «ufravikelige og andre grunnleggende menneskerettigheter» i andre ledd, og heller ikke drøfter implikasjonene av denne spesifiseringen. NIM understreker at andre ledd kan oppfattes som en begrensning av første ledd. NIM mener at det gir liten rettslig mening å snakke om grunnleggende menneskerettigheter (i motsetning til ikke-grunnleggende rettigheter). Det påpekes at ingen konvensjoner gjør en slik sondring, og at rettighetene utgjør et universelt hele.

NIM oppsummerer sitt syn slik:

> «Det er etter NIMs oppfatning uklart hva departementet har ment å gjøre gjennom § 1-3 annet ledd. Man har trolig ment å avgrense e-tjenestens virksomhet mot operasjoner som innebærer en reell risiko for at noen utsettes for tortur eller krigsforbrytelser, men dette kan altså motsetningsvis forstås dit at krenkelser av andre menneskerettigheter som en følge av E-tjenestens virksomhet ikke omfattes. Uansett burde det være unødvendig med en slik presisering, særlig i lys av formålsbestemmelsen.»

Dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors omtaler lovutkastet § 1-3 i sin gjennomgang av de vilkår domstolen settes til å prøve etter utkastet § 8-4. De peker på at domstolen etter § 1-3 andre ledd skal føre kontroll med at virksomheten ikke innebærer en reell risiko for at ufravikelige og «andre grunnleggende menneskerettigheter krenkes». De poengterer at det er uklart hvilke menneskerettigheter lovforslaget viser til. Det fremstår dermed ikke klart hvordan de «grunnleggende menneskerettighetene» skal utgjøre en skranke for Etterretningstjenestens virke, slik det er forutsatt i § 8-4.

Kripos uttaler at lovutkastet § 1-3 fremstår som lite hensiktsmessig, og påpeker at det grunnleggende forholdet til folkeretten er ivaretatt gjennom Grunnloven og menneskerettsloven. Utover dette bør man etter Kripos' syn være forsiktig med å lovfeste folkerettslige begrensninger, fordi «[d]et ligger i etterretningstjenestens natur at den vil kunne måtte operere i et grenseland her.» Videre fremhever Kripos at det er uklart hva som ligger i begrepene «reell risiko» og «medvirke» i utkastet § 1-3 andre ledd. Kripos uttaler dessuten at man ut fra formuleringen i andre ledd motsetningsvis kan spørre hvilke grunnleggende menneskerettigheter man mener eventuelt kan fravikes.

Den internasjonale juristkommisjon – norsk avdeling (ICJ-Norge) understreker at statens menneskerettighetsforpliktelser gjelder der staten har jurisdiksjon, og at dette omfatter mer enn kun statens territorium. ICJ-Norge peker på at uttalelser i høringsnotatet kan tyde på at departementet mener at rettstilstanden omkring EMK artikkel 1 er usikker fordi EMD ikke selv har tatt stilling til spørsmålet. ICJ-Norge viser til subsidiaritetsprinsippet, som innebærer at norske rettsanvendere selv må anvende EMK basert på de tolkningsprinsippene som EMD anvender og selv komme til et resultat basert på de tilgjengelige kildene. Norge kan følgelig ikke vente på at EMD avklarer alle rettsspørsmål som springer ut av konvensjonen, men må foreta en selvstendig vurdering.

ICJ-Norge peker på at det er uklart hvilke konsekvenser det får at konvensjonen skal respekteres ut fra praktiske hensyn og policybetraktninger, slik det anføres i høringsnotatet. ICJ-Norge ber om at Stortinget klargjør og slår fast at en slik beslutning om at menneskerettighetene gjelder for alle, uansett hvor de befinner seg, ikke vil være gjenstand for politiske beslutninger senere eller innebære at Etterretningstjenesten i realiteten gis fullmakt til å anvende en «mildere rettighetsnorm» i disse tilfellene.

NIM er enige med departementet i at det vil kunne være vanskelig å fastslå i hvilke tilfeller EMK får ekstraterritoriell anvendelse der utlendinger eller norske borgere overvåkes i utlandet fra Norge, og der Etterretningstjenesten opererer i utlandet uten tilknytning til norsk territorium. NIM mener imidlertid det er uklart hva som menes når det sies i høringsnotatet at regelverket er utformet «nasjonalitets- og geografinøytralt». Denne forståelsen fremkommer ikke av selve lovteksten. NIM viser til at forslaget til lovtekst henviser til menneskerettighetene, altså slik de er bindende for Norge, også jurisdiksjonsmessig. NIM støtter dette, men mener omtalen i høringsnotatet er uheldig:

> «NIM mener det er et uheldig grep å si i forarbeidene at menneskerettighetene skal gjelde uten de begrensninger som følger av menneskerettighetskonvensjonenes jurisdiksjonsregler. Selv om anvendelsen av reglene kan være utfordrende å fastslå i enkelte tilfeller, er det likevel en risiko for utvanning av menneskerettsvernet når man hevder å skulle sikre universell anvendelse av alle menneskerettigheter over alt. Norge har ikke praktisk mulighet eller plikt, (jf. EMK artikkel 1 og SP artikkel 2) til å sikre alle rettigheter i EMK eller SP overfor for eksempel potensielle opprørere i Afghanistan eller andre personer i E-tjenestens søkelys.»

NIM uttaler videre:

> «At reglene i EMK og SP skal gjelde for E-tjenestens virksomhet er ikke til hinder for at rettighetsbeskyttelsen differensieres avhengig av hvor virksomheten utøves og hvem som berøres.»

Det er etter NIMs syn gode grunner til at personer på norsk territorium og norske borgere kan ha behov for sterkere rettighetsvern enn utlendinger i utlandet, uten at det med det fremholdes at den sistnevnte gruppen ikke skal ha et vern som oppfyller de til enhver tid gjeldende reglene i EMK eller SP. NIM trekker frem at personer i Norge er eksponert for mulige statlige inngrep eller sanksjoner, mens utlendinger i utlandet i utgangspunktet ikke er eksponert for denne typen mulige følgevirkninger av hemmelig overvåkning. På samme måte vil de potensielle skadevirkningene for samfunnet være større i Norge enn i utlandet, for eksempel en nedkjølingseffekt på kildevernet.

NIM mener på denne bakgrunn at det kan være grunn til å vurdere en lovtekst som er basert på Norges menneskerettsforpliktelser, både materielt og jurisdiksjonsmessig. Dette innebærer sterkere rettssikkerhetsmekanismer ved overvåkning som direkte berører personer på norsk territorium og norske borgere.

5.3.4 Departementets vurdering

Departementet har på bakgrunn av høringen vurdert behovet for en egen bestemmelse om forholdet til folkeretten. Flere høringsinstanser påpeker at lovutkastet § 1-3 har fått en uhensiktsmessig utforming som er egnet til å skape misforståelser. Departementet er enig i dette. Som *Kripos* fremhever, er forholdet til menneskerettighetene ivaretatt gjennom Grunnloven og menneskerettsloven. I tillegg gjelder presumpsjonsprinsippet i norsk rett, som innebærer at loven så langt mulig skal tolkes og anvendes i samsvar med Norges folkerettslige forpliktelser. På bakgrunn av dette har departementet kommet til at det ikke er behov for en egen bestemmelse som angir forholdet til folkeretten.

Departementet ønsker i lys av høringen å knytte noen kommentarer til spørsmålet om EMKs ekstraterritorielle virkning.

Som redegjort for under punkt 5.3.1, har spørsmålet om EMKs ekstraterritorielle virkning vært gjenstand for utvikling i EMDs rettspraksis. Det fremheves i høringsnotatet at spørsmålet om jurisdiksjon i utgangspunktet vil måtte vurderes konkret i det enkelte tilfellet. Samtidig vises det til at lovutkastet er utformet i tråd med menneskerettighetenes krav, og dermed sikrer at disse etterleves alle steder loven praktiseres.

Tilnærmingen i høringsnotatet har blitt oppfattet ulikt av høringsinstansene som har kommentert den. *ICJ-Norge* peker på at det er uklart hvilke konsekvenser det får at EMK skal respekteres ut fra praktiske hensyn og policybetraktninger, og ber Stortinget om å slå fast at menneskerettighetene gjelder for alle, uansett hvor de befinner seg. På den andre siden mener *Norges institusjon for menneskerettigheter (NIM)* at det er uheldig å si at menneskerettighetene skal gjelde uten de begrensninger som følger av reglene om jurisdiksjon. Selv om anvendelsen av reglene kan være utfordrende å fastslå i enkelte tilfeller, innebærer det etter NIMs syn en risiko for utvanning av menneskerettsvernet når man hevder å skulle sikre universell anvendelse av alle menneskerettigheter over alt.

Departementet erkjenner at høringsnotatets omtale er egnet til å skape misforståelser, og understreker at forpliktelsene etter menneskerettighetskonvensjonene bare gjelder i den utstrekning som følger av jurisdiksjonsreglene. Når det foreslås at lovforslaget ikke skal ha et begrenset geografisk virkeområde, innebærer ikke det at EMK skal gjelde i større utstrekning enn det som følger av artikkel 1. Det vernet av individuelle rettigheter som ligger innbakt i flere av lovens bestemmelser, vil i praksis likevel strekke seg noe lenger enn det som er strengt nødvendig etter EMK. Dette innebærer etter departementets syn ikke en risiko for utvanning av menneskerettsvernet. Departementet ser det ikke som ønskelig å avgrense loven mot etterretningsvirksomhet overfor utlendinger i utlandet, da det er slik virksomhet som i hovedsak søkes regulert i loven. Samtidig har departementet forståelse for NIMs synspunkter om betydningen av å differensiere vernet. Som NIM påpeker, vil personer som oppholder seg i Norge være eksponert for mulige inngrep eller sanksjoner fra norske myndigheter, i motsetning til utlendinger i utlandet. På samme måte vil potensielle skadevirkninger for samfunnet være større i Norge enn i utlandet. Den viktigste differensieringen følger av lovforslaget § 4-1, som fastsetter som hovedregel at Etterretningstjenesten ikke kan bruke innhentingsmetoder etter kapittel 6 overfor personer som er i Norge. Tilrettelagt innhenting etter lovforslaget kapittel 7 og 8 berører personer i Norge i større grad enn annen innhenting, og for slik innhenting foreslås det derfor strengere kontrollmekanismer og garantier mot misbruk og vilkårlighet. Et konkret utslag av NIMs høringsinnspill er forslaget om at personer som vernes etter lovforslaget §§ 9-5 og 9-6 (kildevern mv.) må ha en form for tilknytning til Norge, se nærmere punkt 12.8.

5.4 Definisjoner

5.4.1 Forslaget i høringsnotatet

Forslagene til definisjoner omtales ikke i et eget kapittel i høringsnotatet, men fortløpende og i forbindelse med de materielle drøftelsene.

Det foreslås et system der kun de begrepene som benyttes flere steder i lovteksten defineres i definisjonsbestemmelsen. Begreper som bare brukes én gang forklares i den enkelte bestemmelse. Dette gjelder først og fremst begreper i lovutkastet kapittel 6 om metoder.

5.4.2 Høringsinstansenes syn

Riksadvokaten uttaler at hensikten med en egen lovbestemmelse som inneholder definisjoner normalt vil være at definisjonene samles ett sted for å øke oversiktligheten. Riksadvokaten registrerer at det både er inntatt en egen bestemmelse som inneholder definisjoner, samtidig som flere andre bestemmelser inneholder ytterligere definisjoner. Etter riksadvokatens syn burde det vært en mer enhetlig tilnærming til hvordan man inntar definisjoner i lovteksten.

Riksadvokaten viser til at sentrale begreper i lovutkastet, slik som «infiltrasjon» og «provokasjon», ikke er definert. Dette gjør det vanskelig å bedømme om begrepene innholdsmessig sammenfaller med måten de brukes på i politiet. Riksadvokaten mener dessuten at meningsinnholdet i definisjonen av begrepet «kilde» er uklart.

Kripos mener at det fremstår fornuftig å flytte definisjonen av personopplysninger fra nummer 11 til nummer 1, da denne definisjonen bør komme forut for definisjonen av «behandling av personopplysninger».

5.4.3 Departementets vurdering

Departementet viderefører forslaget i høringsnotatet om å definere enkelte sentrale begreper som brukes flere ganger i lovteksten i en egen bestemmelse. Bestemmelsen inntas i lovforslaget § 1-3. På bakgrunn av høringen foreslås det noen justeringer. For å komme *riksadvokaten* i møte foreslår departementet flere lovtekniske justeringer i lovforslaget kapittel 6, se nærmere punkt 10.6.3. *Kripos'* forslag om å endre rekkefølgen av definisjonene tas til følge.

6 Organisering, styring og kontroll

6.1 Organisering og styring

6.1.1 Gjeldende rett

Etterretningstjenesten er Norges utenlandsetterretningstjeneste og har som oppgave å støtte både sivile og militære myndigheter.

Det følger av etterretningstjenesteloven § 2 at Etterretningstjenesten er 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 gjelder for Etterretningstjenesten som for Forsvaret for øvrig, med mindre tjenesten er unntatt eller det er fastsatt særlig tilpassede reguleringer. Forsvarssjefen utøver sitt kommando- og etatssjefsansvar for Etterretningstjenesten som del av Forsvaret.

Som en følge av Etterretningstjenestens særlige oppgaver som nasjonal utenlandsetterretningstjeneste har Forsvarsdepartementet et særlig styringsansvar. Det følger av instruks om Etterretningstjenesten (e-instruksen) § 3 at Forsvarsdepartementet, gjennom forsvarssjefen, formulerer oppdrag og utøver politisk styring og kontroll med Etterretningstjenesten. Deler av Etterretningstjenestens virksomhet er av en slik art at departementet har en særlig rolle i den operative styringen og får konkrete saker forelagt for vurdering og beslutning. Etter e-instruksen § 13 omfatter foreleggelsesplikten fire kategorier saker: Etablering av samarbeid med utenlandske tjenester og internasjonale organisasjoner, organiseringen av okkupasjonsberedskapen, iverksettelse av særskilte etterretningsoperasjoner som kan reise politiske problemstillinger og andre saker av særlig viktighet eller prinsipiell karakter.

Etterretningstjenestens bistand til sivile og militære myndigheter og det omfattende behov for unntak fra offentlig innsyn stiller særlige krav til overordnet styring og kontroll, beslutningsnotoritet og dokumenterbare prosesser. Forsvarsdepartementet koordinerer de nasjonale etterretningsbehovene og vurderer og prioriterer disse innenfor rammen av tjenestens samlede ressurser. Resultatet av prioriteringen fremkommer i et årlig styringsdokument for Etterretningstjenestens virksomhet som fastsettes av departementet (prioriteringsdokumentet for nasjonale etterretningsbehov, forkortet PNEB).

Etterretningsbehov som dukker opp, formidles gjennom informasjonsforespørsler (*request for information*, forkortet RFI). Slike forespørsler kan for eksempel omfatte behov for særlige vurderinger og orienteringer knyttet til nye situasjoner eller bakgrunnsinformasjon i forbindelse med politisk behandling. Forespørslene prioriteres og vurderes med hensyn til PNEB og formidles fra Forsvarsdepartementet til Etterretningstjenesten eller etter Forsvarsdepartementets anvisning.

Etterretningstjenestens behov for å skjerme budsjett og økonomiske disposisjoner 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 person med fast representasjon i utvalget. Personen har gjennomført revisjonen og hatt innsyn i alle deler av tjenestens økonomiske virksomhet. I 1993 ble formålet og oppgavene til K-utvalget formalisert av Stortinget gjennom en sikkerhetsgradert stortingsproposisjon. Stortingsbeslutningen er det formelle grunnlaget for dagens ordning. Utvalget ble fra 1993 benevnt Koordineringsutvalget for Etterretningstjenesten (K-utvalget).

Økonomi- og virksomhetsstyringen i staten er underlagt enhetlige prosesser gjennom blant annet reglement og bestemmelser for økonomistyring i staten. For Forsvarsdepartementets underlagte virksomheter er det fastsatt utfyllende instruks for økonomi- og virksomhetsstyring basert på overordnet regelverk og Statens bevilgningsreglement. Etterretningstjenesten er ikke omfattet av denne instruksen, men er i stedet underlagt K-utvalgets særskilt tilpassede proses-

ser etter stortingsbeslutningen av 1993 og tilhørende instruks for K-utvalget.

Forsvarsdepartementet har i den senere tid oppdatert og strukturert K-utvalget som det overordnede forum for økonomi- og virksomhetsstyring av Etterretningstjenesten. Det ble i 2017 fastsatt en Instruks om Koordineringsutvalget for Etterretningstjenesten som klargjør og formaliserer K-utvalgets funksjon og prosessuelle rammer i tråd med prinsippene som gjelder økonomi- og virksomhetsstyring i staten for øvrig.

En av Etterretningstjenestens hovedoppgaver er å varsle og rapportere til oppdragsgivere om forhold som ligger innenfor tjenestens oppdrag. E-instruksen § 11 åpner for at Etterretningstjenesten kan varsle og rådgi norske og utenlandske juridiske og fysiske personer innenfor rammen av sikkerhetsloven. I tillegg pålegger instruksen § 14 tjenesten å holde Forsvarsdepartementet, og etter Forsvarsdepartementets anvisning andre berørte departementer, orientert om relevante endringer i den militære og politiske situasjon i norsk interesseområde.

6.1.2 Forslaget i høringsnotatet

I høringsnotatet punkt 6.2 til 6.5 foreslås det å regulere enkelte forhold knyttet til organiseringen og styringen av Etterretningstjenesten. Det vises til flere grunner som gjør en slik regulering hensiktsmessig. For det første er organiseringen av tjenesten allerede i dag delvis fastlagt i lov, jf. gjeldende etterretningstjenestelov § 2. Videre er økonomi- og virksomhetsstyringen av Etterretningstjenesten gjennom K-utvalget forankret i Stortinget. For det tredje er Etterretningstjenestens virksomhet av en slik karakter at det er behov for særskilt tilpasset styring og kontroll.

Det foreslås å videreføre Etterretningstjenesten som en del av Forsvaret, underlagt forsvarssjefens kommando. I tillegg foreslås det å synliggjøre at departementet i større utstrekning enn for annen virksomhet i Forsvaret vil ha en direkte styringsrolle.

6.1.3 Høringsinstansenes syn

Riksadvokaten mener formuleringen i lovutkastet § 2-1 om Etterretningstjenestens «sektorovergripende samfunnsoppdrag» er egnet til å skape uklarhet om hvor grensene for Etterretningstjenestens faktiske ansvars- og myndighetsområde går. Riksadvokaten mener dette bør presiseres, slik at grenseflatene mot andre myndigheter med funksjoner innen stats- og samfunnssikkerhetsarbeidet er klare.

Justis- og beredskapsdepartementet anbefaler at utlevering av sikkerhetsgradert informasjon i forbindelse med varsling og rapportering bør utformes i tråd med virksomhetsikkerhetsforskriftens unntaksregel for utlevering av sikkerhetsgradert informasjon uten nødvendig autorisasjon eller klarering.

6.1.4 Departementets vurdering

Departementet viderefører i hovedsak forslaget i høringsnotatet. Bestemmelsene i lovutkastet kapittel 2 ivaretar etter departementets syn balansen mellom nødvendig regulering av viktige prinsipper og styrings- og kontrollmekanismer på den ene siden, og tilstrekkelig fleksibilitet i utøvelsen av forvaltningsansvaret på den andre siden. Det foreslås enkelte lovtekniske og språklige justeringer. Utkastet til §§ 2-1 til 2-3 er slått sammen til én bestemmelse.

Forsvarsministeren har det konstitusjonelle ansvaret for hele forsvarssektoren, herunder Etterretningstjenesten som del av Forsvaret. Tjenestens sektorovergripende oppgaver tilsier at Forsvarsdepartementet må ha en direkte rolle i styring og kontroll av tjenesten. Dette ivaretas gjennom fastsettelse av overordnede styringsdokumenter, beslutninger i saker som tjenesten plikter å forelegge for departementet, og gjennom K-utvalget.

I høringsutkastets forslag til § 2-1 presiseres det at Etterretningstjenesten har et sektoroverskridende samfunnsoppdrag. Dette innebærer at tjenesten støtter både militære og sivile myndigheter i utøvelsen av sin virksomhet. Departementet merker seg *riksadvokatens* synspunkt om at denne presiseringen kan være egnet til å skape uklarheter rundt tjenestens ansvars- og myndighetsområde. Tjenestens ansvar og myndighet er etter departementets vurdering tilstrekkelig klarlagt i lovforslagets kapittel 3 om oppgaver. Departementet foreslår derfor å fjerne henvisningen til tjenestens sektoroverskridende samfunnsoppdrag i lovforslaget § 2-1, i tråd med riksadvokatens anbefaling.

Varslings- og rapporteringsplikten er en av Etterretningstjenestens primærfunksjoner, og bør lovfestes særskilt. Varslingsplikten er primært knyttet til særlig kritiske situasjoner som gjør det nødvendig å varsle norske myndigheter om en trussel direkte. Det typiske her vil være en nært forestående trussel mot Norge eller norske interesser, som krever umiddelbare tiltak. Rappor-

teringsplikten er mer generell, og har ikke den samme tidskritiske karakteren som varslingsplikten. Det foreslås at Etterretningstjenesten skal rapportere om «utenlandske forhold av betydning for Norge og norske interesser» innenfor rammen av de lovfestede oppgavene i kapittel 3 og overordnet myndighets prioriteringer og oppdrag etter § 2-2.

Departementet mener at det er ønskelig å klargjøre at det ved en varslingssituasjon vil være anledning til å utlevere sikkerhetsgradert informasjon til personer uten autorisasjon og sikkerhetsklarering dersom det er strengt nødvendig og sikkerhetsmessig forsvarlig. *Justis- og beredskapsdepartementet* anbefaler i sin høringsuttalelse at forslaget til bestemmelse om utlevering av sikkerhetsgradert informasjon bør utformes i tråd med sikkerhetsloven. Departementet er enig i at det bør være en tydeligere kobling til sikkerhetsloven, men understreker at det legges opp til en annen terskel enn bare nødrettssituasjoner som følger av virksomhetsikkerhetsforskriften § 71. Departementet foreslår derfor en mindre justering for å presisere at dette er ment å være et snevert unntak fra kravet til autorisasjon og sikkerhetsklarering i sikkerhetsloven § 8-1. Unntaket inntas i lovforslaget § 2-4 tredje ledd andre punktum.

Deler av Etterretningstjenestens virksomhet er av en art som tilsier at departementet bør ha en direkte rolle i den operative styringen og få saker forelagt for vurdering og beslutning i ethvert tilfelle. Det følger av lovforslaget § 2-5 at etablering av samarbeid og avtaler med utenlandske tjenester eller internasjonale organisasjoner, iverksettelse av særskilte etterretningsoperasjoner som kan reise politiske problemstillinger og andre særlig viktige saker, skal forelegges departementet for beslutning. Forslaget viderefører gjeldende praksis. Etterretningstjenestens plikt til å holde departementet generelt orientert om okkupasjonsberedskapen foreslås regulert i lovforslaget § 3-3.

6.2 Kontroll av Etterretningstjenesten

6.2.1 Generelt

Etterretningstjenestens virksomhet kontrolleres av flere instanser. Disse kontrollerer ulike sider av virksomheten, og har forskjellige rettslige grunnlag for sine kontrollfunksjoner.

Forsvarsdepartementet ivaretar den forvaltningsmessige styringen og kontrollen av Etterretningstjenesten. Stortingets kontrollutvalg for etterretnings- overvåkings- og sikkerhetstjeneste (EOS-utvalget) fører uavhengig kontroll av Etterretningstjenesten.

Riksrevisjonen ivaretar, på vegne av Stortinget, revisjon og kontroll av at statens midler og verdier forvaltes i tråd med Stortingets beslutninger. Riksrevisjonen reviderer Etterretningstjenesten. For å ivareta de særskilte skjermingsbehov som knytter seg til tjenestens virksomhet, gjennomføres revisjonen av utpekte personer i Riksrevisjonen med nødvendig sikkerhetsklarering og autorisasjon. De overordnede rammene framgår av lov og instruks om Riksrevisjonen. Det vises forøvrig til punkt 6.1.1 for beskrivelse av representasjon fra Riksrevisjonen i K-utvalget.

Domstolenes kompetanse til å behandle søksmål med påstand om ulovlig etterretningsvirksomhet følger av de alminnelige reglene i tvisteloven.

6.2.2 EOS-utvalgets kontroll med Etterretningstjenesten

EOS-utvalget kontrollerer etterretnings- overvåkings- og sikkerhetstjeneste som utføres av den offentlige forvaltning eller under styring av eller på oppdrag fra denne, jf. EOS-kontrolloven § 1. I etterretningstjenesteloven § 6 første ledd er det presisert at tjenesten er underlagt EOS-utvalgets kontroll. EOS-utvalget er oppnevnt av Stortinget og utfører sitt verv selvstendig og uavhengig.

Hovedformålet med EOS-utvalgets kontroll er å ivareta den enkeltes rettssikkerhet. Utvalget skal klarlegge om og forebygge at noens rettigheter krenkes, påse at EOS-tjenestene ikke benytter seg av mer inngripende midler enn det som er nødvendig og at tjenestene respekterer menneskerettighetene. EOS-tjenestenes virksomhet er i stor grad skjermet for offentligheten. Utvalget kontrollerer EOS-tjenestene på samfunnets vegne for å sikre legitimitet for og tillit til tjenestene.

Utvalget følger prinsippet om etterfølgende kontroll. Det innebærer at kontrollen gjøres gjennom inspeksjoner, behandling av klagesaker og behandling av saker som tas opp av eget tiltak.

6.2.2.1 Innsynsretten og unntak for «særlig sensitiv informasjon«

EOS-utvalget har som hovedregel uinnskrenket tilgang til, og innsyn i alt av opplysninger i alle arkiver og registre, jf. EOS-kontrolloven § 8. EOS-utvalgets legitimitet som kontrollorgan forutsetter uinnskrenket tilgang til, og innsyn i alt av opplysninger i alle arkiver og registre i Etterretningstje-

nesten som er nødvendig for at utvalget skal kunne utføre sin kontrolloppgave.

Det gjelder en begrensning i utvalgets innsynsrett for det som omtales som «særlig sensitiv informasjon». Departementet fastsatte i 2014 en ugradert definisjon av begrepet som er gjengitt i Innst. 431 L (2016–2017) side 4:

> «[I]nformasjon 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.»

Rekkevidden av innsynsretten har tidligere vært gjenstand for noe ulik fortolkning. En meget liten del av Etterretningstjenestens saker er av særlig sensitiv karakter og har et særdeles stort skadepotensiale. Behovet for særlig skjerming av slik informasjon er bakgrunnen for at denne type informasjon er unntatt EOS-utvalgets generelle innsyn.

På bakgrunn av tidligere uklarheter rundt innsynsretten, ble det i forbindelse med Stortingets revisjon av EOS-kontrolloven i 2017 foreslått å lovfeste unntak fra innsyn i «særlig sensitiv informasjon». I komiteens merknader heter det imidlertid (Innst. 431 L (2016–2017) side 9):

> «K o m i t e e n 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.»

Rettstilstanden når det gjelder unntaket fra innsyn i «særlig sensitiv informasjon» er etter revisjonen av EOS-kontrolloven å anse som avklart selv uten at unntaket fremkommer direkte av lovteksten.

6.2.3 Forslaget i høringsnotatet

I høringsnotatet punkt 6.7 videreføres i stor grad de eksisterende rammer for kontroll med Etterretningstjenesten, det vil si at EOS-utvalget skal føre kontroll med tjenesten som fastsatt i EOS-kontrolloven. I tillegg foreslås det at utvalget skal føre styrket kontroll med tjenestens bruk av tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon.

Etterretningstjenesten foreslås underlagt revisjon og kontroll av Riksrevisjonen i medhold av riksrevisjonsloven. Tjenestepersoner som skal gjennomføre revisjon og kontroll må ha norsk statsborgerskap og være sikkerhetsklarert for STRENGT HEMMELIG. Videre foreslås det å lovfeste plikten til å orientere stortingspresidenten om tjenestens virksomhet.

6.2.4 Høringsinstansenes syn

Justis- og beredskapsdepartementet mener at det bør vurderes å lovfeste at utpekte tjenestepersoner hos Riksrevisjonen ikke kan inneha annet statsborgerskap enn norsk.

Advokatforeningen uttaler:

> «Lovforslaget underlegger i meget begrenset grad Etterretningstjenesten en reell og uavhengig kontroll. Først og fremst består kontrollen av generelt etterhåndstilsyn ved EOS-utvalget. Etter Advokatforeningens syn vil imidlertid EOS-utvalget i praksis ikke være i stand til å utøve effektiv kontroll med de omfangsrike inngrep som lovforslaget medfører hva gjelder overvåkningsvirksomhet og informasjonsinnhenting. Domstolkontroll er ifølge lovforslaget begrenset til forhåndsprøvelse av begjæringer om bulkinnsamling av elektronisk kommunikasjon etter kapittel 7. Etter Advokatforeningens skjønn vil domstolenes forutsetninger for selvstendig prøvelse være begrenset.»

Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget) mener at det bør inntas en bestemmelse om tilretteleggingsplikt fra Etterretningstjenestens side overfor EOS-utvalget. Videre mener utvalget at unntaket fra utvalgets innsynsrett i informasjon som tjenesten selv har definert som særlig sensitiv informasjon, bør vurderes inntatt i forslaget til § 2-8, eventuelt i EOS-kontrolloven § 8.

Utvalget mener dessuten at lovteksten i § 2-10 bør reflektere at EOS-utvalget kun kontrollerer behandling av personopplysninger som faller inn under kontrollområdet, som er etterretnings-, overvåkings- og sikkerhetstjeneste.

Næringslivets sikkerhetsråd (NSR) mener at de foreslåtte kontrollmekanismer synes å tilfredsstille den nødvendige tillit til at enkeltborgeres personvern blir ivaretatt. NSR ønsker likevel å påpeke at EOS-utvalget må styrkes med nødvendig teknologisk kompetanse for å kunne utføre

reelle kontroller med Etterretningstjenestens aktiviteter på dette området.

6.2.5 Departementets vurdering

Departementet tar som utgangspunkt at effektiv kontroll er avgjørende for å skape og opprettholde legitimitet for, og tillit til, Etterretningstjenesten. Det ligger i sakens natur at etterretningsvirksomheten i stor utstrekning må skjermes og holdes hemmelig, jf. kapittel 3. Når dette er situasjonen, er det viktig at rammene for kontrollen er klare og fremgår av loven. På den andre siden er det klart at ikke alle detaljer knyttet til kontrollen kan lovfestes, blant annet fordi disse vil kunne variere over tid. Departementet understreker at det er viktig å se alle de forskjellige kontrollmekanismene under ett i vurderingen av om Etterretningstjenesten er underlagt tilstrekkelig kontroll og tilsyn. Departementet er ikke enig med *Advokatforeningen* i at lovforslaget i meget begrenset grad underlegger Etterretningstjenesten en reell og uavhengig kontroll, men tar på alvor tilbakemeldingene om at kontrollmulighetene bør styrkes. På bakgrunn av høringen foreslås det derfor flere endringer som tar sikte på å styrke mulighetene for effektiv og reell kontroll, særlig med hensyn til tilrettelagt innhenting. Det vises til punkt 11.9 (domstolens forhåndskontroll) og 11.10 (EOS-utvalgets løpende kontroll) for en nærmere drøftelse.

Departementet viderefører i all hovedsak forslaget i høringsnotatet om EOS-utvalgets og Riksrevisjonens kontroll. Bestemmelsen inntas i lovforslaget § 2-6. Rammene for EOS-utvalgets kontrollmyndighet vil ikke begrenses eller utvides som følge av lovforslaget, med unntak av utvidelsen knyttet til tilrettelagt innhenting, jf. punkt 11.10. EOS-utvalget vil som før kunne kontrollere alle deler av Etterretningstjenestens virksomhet som faller inn under kontrollområdet, jf. EOS-kontrolloven.

EOS-utvalget mener at det bør inntas en bestemmelse om tilretteleggingsplikt fra Etterretningstjenestens side overfor EOS-utvalget. Utvalget mener tilrettelegging er en forutsetning for effektiv kontroll, spesielt for eventuell fremtidig kontroll med tilrettelagt innhenting. Det følger forutsetningsvis av EOS-kontrolloven at Etterretningstjenesten må legge til rette for og samarbeide med EOS-utvalget i forbindelse med kontroll, og departementet ser ikke behov for å regulere en slik generell plikt i etterretningstjenesteloven. Departementet mener imidlertid at det er hensiktsmessig å lovfeste en særskilt plikt til å legge teknisk til rette for den løpende kontrollen av tilrettelagt innhenting. En slik bestemmelse inntas i lovforslaget § 7-11 tredje ledd, se nærmere punkt 11.10.4.

EOS-utvalget presiserer i sin høringsuttalelse at utvalget kun kontrollerer behandling av personopplysninger som faller inn under kontrollområdet. Departementet slutter seg til denne presiseringen, og sløyfer forslaget i høringsnotatet til § 2-10 første ledd andre punktum.

EOS-utvalget foreslår i sin høringsuttalelse å lovfeste unntaket fra utvalgets innsynsrett i såkalt «særlig sensitiv informasjon». Unntaket etter gjeldende rett, som er beskrevet under punkt 6.2.2.1, må anses avklart. Departementet er enig i at det kan være grunner som tilsier å lovregulere unntaket, men en slik bestemmelse har ikke vært på høring og foreslås ikke nå. Det kan være aktuelt å komme tilbake til spørsmålet på et senere tidspunkt.

Justis- og beredskapsdepartementet tar til orde for å lovfeste at tjenestepersoner hos Riksrevisjonen som gjennomfører revisjon av Etterretningstjenesten ikke bør kunne ha annet statsborgerskap enn norsk. Departementet foreslår ikke en slik endring, da sikkerhetsbehovene må anses tilstrekkelig ivaretatt gjennom klareringsprosessen.

7 Etterretningstjenestens oppgaver

7.1 Innledning

Hovedformålet med norsk utenlandsetterretning er å bidra til å beskytte Norges suverenitet, territorielle integritet, demokratiske styreform og andre nasjonale sikkerhetsinteresser. Etterretningstjenesten skal skaffe rettidig, pålitelig og relevant informasjon om verden rundt oss som beslutningsgrunnlag for sivile og militære myndigheter.

Beskrivelsen av Etterretningstjenestens oppgaver i lovforslaget kapittel 3 danner rammen for hva tjenesten kan innhente av informasjon, men loven oppstiller også en rekke andre vilkår for innhenting og behandling av informasjon. Kapittel 3 må blant annet leses i sammenheng med innhentingsforbudene i kapittel 4, grunnvilkårene og metodene for innhenting i kapittel 5 og 6, særreglene om tilrettelagt innhenting i kapittel 7 og 8 og reglene om behandling av personopplysninger etter innhenting i kapittel 9.

7.2 Andre lands rett

7.2.1 Sverige

Det følger av *lag (2000:130) om försvarsunderrättelseverksamhet* 1 § at etterretningsvirksomheten bare skal knytte seg til utenlandske forhold og utføres til støtte for svensk utenriks-, sikkerhets- og forsvarspolitikk og for å identifisere eksterne trusler mot landet. Det inkluderer å delta i det internasjonale sikkerhetssamarbeidet. Loven avgrenser mot oppgaver som faller innenfor myndigheten til politiet, sikkerhetspolitiet og andre myndigheter som driver med kriminalitetsforebyggende arbeid.

Etter *lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet* skal signalspaningen blant annet skje med det formål å kartlegge eksterne militære trusler mot landet, utvikling og spredning av masseødeleggelsesvåpen, alvorlige eksterne trusler mot samfunnets infrastruktur og fremmed etterretningsvirksomhet mot svenske interesser. I tillegg skal signalspaningen kartlegge forhold knyttet til internasjonal terrorisme og annen alvorlig grenseoverskridende kriminalitet.

7.2.2 Danmark

Lov om Forsvarets Efterretningstjeneste (FE) § 1 regulerer oppgavene til den danske utenlandsetterretningstjenesten. Det følger av bestemmelsen at etterretningsvirksomheten skal være rettet mot forhold i utlandet. Tjenestens hovedoppgaver er i korte trekk å samle inn, innhente, bearbeide, analysere og formidle opplysninger om forhold i utlandet av betydning for Danmark og danske interesser, og på den måten gi et etterretningsmessig grunnlag for dansk utenriks-, sikkerhets- og forsvarspolitikk. FE skal også medvirke til å forebygge og motvirke trusler mot Danmark og danske interesser.

FE er i tillegg ansvarlig for å lede den militære sikkerhetstjenesten og ivaretar funksjonen som nasjonal sikkerhetsmyndighet i forsvarssektoren. FE utøver også oppgaven som it-sikkerhetsmyndighet, militær varslingstjeneste for internettrusler og statlig varslingstjeneste for internettrusler.

7.2.3 Finland

Lag om militär underrättelseverksamhet (590/2019) inneholder ikke en egen bestemmelse som regulerer oppgavene til de militære etterretningsmyndighetene. Det følger imidlertid av 4 § at den militære etterretningsvirksomheten retter seg mot virksomhet som drives av fremmed stats væpnede styrker, etterretningsvirksomhet mot Finlands forsvar, planlegging, tilvirking, spredning og anvendelse av masseødeleggelsesvåpen, fremmed stats utvikling og spredning av militært materiell, krise og virksomhet som alvorlig truer internasjonal fred og sikkerhet, virksomhet som alvorlig truer sikkerheten til Finlands internasjonale bistandsarbeid og annen internasjonal virksomhet og fremmed stats virksomhet som alvorlig truer det finske forsvar eller som setter samfunnets vitale funksjoner i fare.

Departementet viser dessuten til angivelsen av oppgavene til finsk sivil etterretning i *polislagen*

(2011/872) 5 a kap. 3 § og *lag om civil underrättelseinhämtning avseende datatrafik (582/2019)* 3 §.

7.3 Utenlandske trusler og andre utenlandske forhold

7.3.1 Gjeldende rett

Etterretningstjenesten skal bidra til å kartlegge og motvirke ytre trusler mot rikets selvstendighet og sikkerhet og andre viktige nasjonale interesser, jf. formålsbestemmelsen i etterretningstjenesteloven § 1. Det følger av loven § 3 at tjenesten 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. Paragrafen oppregner deretter ti saksfelt som kan utgjøre slike viktige nasjonale interesser, nemlig utformingen av norsk utenriks-, forsvars- og sikkerhetspolitikk, beredskapsplanlegging og korrekt episode- og krisehåndtering, langtidsplanlegging og strukturutvikling i Forsvaret, effektiviteten i Forsvarets operative avdelinger, støtte til forsvarsallianser som Norge deltar i, norske styrker som deltar i internasjonale militære operasjoner, tilveiebringelse av informasjon om internasjonal terrorisme, tilveiebringelse av informasjon om overnasjonale miljøproblemer, tilveiebringelse av informasjon om ulike former for spredning av masseødeleggelsesvåpen og utstyr og materiale for fremstilling av slike våpen, og grunnlaget for norsk deltakelse i og oppfølging av internasjonale avtaler om nedrustnings- og rustningskontrolltiltak.

Vilkåret «viktige nasjonale interesser» er et fleksibelt begrep som sammenfatter det som til enhver tid er norske myndigheters informasjonsbehov. Opplistingen i loven § 3 er ikke uttømmende jf. ordet «herunder». Hva som er andre viktige nasjonale interesser, vil avhenge av hvilke sikkerhetsutfordringer Norge til enhver tid står overfor, jf. instruks om Etterretningstjenesten (e-instruksen) § 7 andre ledd.

Det er ikke slik at alle tjenestens oppgaver vil ha like høy prioritet til enhver tid. Etterretningsvirksomhet er ressurskrevende, og prioriteringen beror derfor på en konkret vurdering fra oppdragsgiver. Etterretningstjenestens oppgaver prioriteres av Forsvarsdepartementet i det årlige prioriteringsdokumentet (PNEB), jf. e-instruksen §§ 7 første ledd og 12. For oppdukkende etterretningsbehov benyttes et system med informasjonsforespørsler (RFI, *request for information*). Dette innebærer at all innhenting og behandling av informasjon som tjenesten gjennomfører, i tillegg til å ligge innenfor rammen av loven § 3, skal kunne knyttes til et oppdrag nedfelt i prioriteringsdokumentet eller i en informasjonsforespørsel.

At Etterretningstjenestens innhenting skal være rettet mot utenlandske forhold, følger av loven § 3 («i forhold til fremmede stater, organisasjoner eller individer»). Utenlandske forhold vil ofte være grenseoverskridende, og dermed også ha en forbindelse til Norge.

7.3.2 Forslaget i høringsnotatet

Det gis i høringsnotatet punkt 7.3 en redegjørelse for utviklingstrekk og dimensjonerende faktorer som er styrende for norske myndigheters informasjonsbehov knyttet til det sikkerhetspolitiske landskapet, trusselbildet og politikkutforming. I punkt 7.5 redegjøres det for utfordringer mot stats- og samfunnssikkerheten, fremmed etterretningsvirksomhet mot Norge og annen påvirkning, og dessuten grenseoverskridende terrorisme og spredning av våpen og teknologi. I punkt 7.6 beskrives etterretningsbehovet knyttet til Norges utenriks, sikkerhets- og forsvarspolitiske interesser samt til utøvelsen av beredskap, krisehåndtering og operasjoner. Det slås fast at unik kunnskap om nevnte saksfelt er viktig som beslutningsstøtte for norske myndigheter.

Det foreslås i høringsnotatet at Etterretningstjenestens oppgaver formuleres i et eget kapittel i lovutkastet. Innhenting av informasjon om utenlandske trusler foreslås regulert i en egen bestemmelse i § 3-1, og innhenting av informasjon om andre utenlandske militære og sivile forhold foreslås regulert i § 3-2. Det foreslås ingen vesentlige endringer i innhentingsoppgavene sammenlignet med gjeldende rett. En viktig forskjell er likevel at hjemlene for innhenting foreslås uttømmende regulert i loven. Det foreslås også å gå bort fra det skjønnsmessige begrepet «viktige nasjonale interesser», for å sikre bedre formålsbegrensning og forutberegnelighet.

7.3.3 Høringsinstansenes syn

Ingen høringsinstanser går imot de foreslåtte hjemlene for innhenting av informasjon om utenlandske trusler og andre utenlandske forhold. Flere kommenterer imidlertid at de er vidt formulert. *Advokatforeningen, Borgarting lagmannsrett, Datatilsynet, dommerne Julsrud, Flaterud, Bau-*

mann, Horn, Heggdal og Selfors og *Norges institusjon for menneskerettigheter (NIM)* har uttalelser i denne retningen. Innspillene knytter seg primært til forhåndskontrollen av søk i informasjon fra tilrettelagt innhenting etter lovforslaget kapittel 7 og 8. *Borgarting lagmannsrett* uttaler i denne forbindelse:

> «Formålene for innhenting fremgår i utkastet kap. 3 om Etterretningstjenestens oppgaver. Som grunnlag for inngrep er formålsangivelsen vid og vag. Nær sagt all informasjon kan hevdes å ligge innenfor ett av formålene i kap. 3.»

Dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors uttaler seg i lignende ordelag. De trekker frem ivaretakelsen av prioriterte utenriks-, forsvars- og sikkerhetspolitiske interesser i lovforslaget § 3-2 første ledd bokstav a som et særlig vidt og vagt formål. Også *Datatilsynet* og *NIM* viser til at oppgavene i lovutkastet § 3-2 er lite presise, og at særlig første ledd bokstav a synes å ha få klare avgrensninger. NIM tilføyer at dette bokstavpunktet umiddelbart fremstår som å ha en videre rekkevidde enn kun nasjonal sikkerhet. *Advokatforeningen* mener at utformingen av inngrepshjemlene i lovforslaget ikke oppfyller de krav til presisjon som må stilles etter legalitetsprinsippet og EMK, blant annet fordi inngrepshjemlene gjennomgående knyttes til de generelle og vide bestemmelsene i kapittel 3 om tjenestens oppgaver. I dette ligger det etter Advokatforeningens syn en fare for formålsutglidning. Advokatforeningen legger til at lovforslaget lar tjenesten selv, for alle praktiske formål, etter eget skjønn gjennomføre de tiltak den finner nødvendig for å utføre sine vidt formulerte oppgaver.

Nasjonal sikkerhetsmyndighet (NSM) slutter seg til den beskrivelsen som høringsnotatet gir av de digitale truslene som samfunnet står overfor i dag. NSM uttaler også at høringsnotatet på en grundig måte gjennomgår, redegjør for og vurderer de ulike sider av Etterretningstjenestens samfunnsoppdrag.

Riksadvokaten mener at lovutkastet § 1-1 bokstav a er en mer treffende beskrivelse av Etterretningstjenestens formål enn fragmentene som fremkommer av lovutkastet § 2-1 og kapittel 3. Riksadvokaten anbefaler at bokstavpunkt a i lovutkastet § 1-1 flyttes til § 3-1 og gjøres til nytt første ledd i denne bestemmelsen og slik danner en overbygging for § 3-1.

7.3.4 Departementets vurdering

7.3.4.1 Generelt

Departementet fastholder at Etterretningstjenestens oppgaver bør reguleres i et eget kapittel i loven, strukturert i henhold til tema. For å sikre forutberegnelighet viderefører departementet forslaget om å regulere tjenestens oppgaver uttømmende i loven, selv om dette fjerner noe fleksibilitet i oppgaveløsningen. Oppgavene må til gjengjeld være beskrevet på en slik måte at de gjør det mulig å holde tritt med utviklingen. Lovforslaget er utformet med sikte på å treffe den riktige balansen mellom disse hensynene.

7.3.4.2 Informasjonsinnhenting om utenlandske trusler

Departementet viderefører forslaget til bestemmelse om informasjonsinnhenting om utenlandske trusler i § 3-1, med kun mindre språklige endringer. Bestemmelsen beskriver de mest alvorlige truslene mot norsk stats- og samfunnssikkerhet med opprinnelse fra utlandet. Ingen høringsinstanser kommenterer bestemmelsen direkte, og departementet oppfatter at det er bred enighet om at dette er en kjerneoppgave for Etterretningstjenesten.

7.3.4.3 Informasjonsinnhenting om andre utenlandske forhold

Departementet viderefører forslaget til bestemmelse om informasjonsinnhenting om andre utenlandske forhold i § 3-2, med kun mindre språklige endringer. Noen høringsinstanser mener at bestemmelsen, særlig første ledd bokstav a, er vid og vag. Departementet har forståelse for at bestemmelsen etter sin ordlyd kan fremstå som vid. Samtidig har norske myndigheter utvilsomt et legitimt behov for kunnskap om verden også utover ytre trusler mot Norge. Kunnskap om prioriterte forhold i andre land og regioner er avgjørende for å kunne utforme Norges utenriks-, forsvars- og sikkerhetspolitikk. Departementet tilføyer at innhenting om andre utenlandske forhold er en vanlig oppgave for etterretningstjenester også etter andre lands rett.

Departementet understreker at adgangen til å innhente informasjon med hjemmel i en av bestemmelsene i kapittel 3, i dette tilfellet § 3-2 første ledd bokstav a, ikke beror på en tolkning av denne bestemmelsen alene, men må leses i sammenheng med vilkår i loven for øvrig, herunder kravet til forholdsmessighet etter lovforslaget § 5-

4. Formålet med innhentingen er et sentralt moment i denne vurderingen. Dette har igjen betydning for hvilke metoder som Etterretningstjenesten kan benytte seg av etter lovforslaget kapittel 6. Jo viktigere formålet er, jo mer inngripende metodebruk kan aksepteres.

Videre vil departementet knytte noen kommentarer til forholdet mellom bestemmelsene i §§ 3-1 og 3-2. Paragraf 3-1 kommer først til anvendelse dersom man står overfor en *trussel*. Lovforslaget gir ingen nærmere beskrivelse av *når* noe regnes som en trussel. Det må avgjøres konkret i den enkelte situasjon. Likevel er det klart at forholdet må være av en viss alvorlighetsgrad for å kunne utgjøre en trussel. Dersom Etterretningstjenesten utelukkende skal innhente informasjon om etablerte trusler og kjent truende aktivitet, vil den ikke evne å avdekke fremtidens trusselbilde. Etterretningsvirksomhet er prediktiv i sin natur, og det å detektere avvik fra normalen er en viktig oppgave. For å kunne varsle om avvik fra det normale, må normaltilstanden være kjent. Forholdet mellom §§ 3-1 og 3-2 kan illustreres med et eksempel fra våre nærområder. Norges forhold til Russland er i stor grad preget av forutsigbarhet. Russland utgjør ingen militær trussel mot Norge i dag. Vår geografiske plassering i forhold til russiske strategiske kapasiteter betyr likevel at utviklingen i Russland og nordområdene har vedvarende stor betydning for norsk og alliert sikkerhet. God og tidsriktig situasjonsforståelse, herunder inngående kunnskap om utviklingen i russisk utenriks- og innenrikspolitikk og om moderniseringen av den russiske militærmakten i våre nærområder, er dermed avgjørende forutsetninger for å kunne utforme norsk utenriks-, forsvars- og sikkerhetspolitikk. Uten hjemmel til å innhente informasjon om disse forholdene, som ikke kan karakteriseres som en trussel, men som et prioritert område, vil man ikke besitte den dybdekunnskapen som kreves for å evne å varsle om endringer av betydning. Litt forenklet sagt vil derfor informasjonsinnhenting etter § 3-2 ofte være en avgjørende forutsetning for å kunne innhente informasjon om trusler etter § 3-1.

Departementet vil dessuten understreke at ikke enhver utenriks-, forsvars, og sikkerhetspolitisk interesse kan begrunne innhenting etter § 3-2 første ledd bokstav a. Det er kun de *prioriterte* interessene som kvalifiserer. Dette utgjør en viktig begrensning, og henviser til prioriteringer av etterretningsbehov fra overordnet myndighet i samsvar med lovforslaget § 2-2.

Departementet merker seg at enkelte høringsinstanser tar til orde for en strengere formålsavgrensning for midtpunktinnhenting i form av tilrettelagt innhenting etter lovforslagets kapittel 7. Dette drøftes nærmere i punkt 11.8.1.

Advokatforeningen uttaler at utformingen av inngrepshjemlene i lovforslaget ikke oppfyller de krav til presisjon som følger av legalitetsprinsippet og EMK, blant annet fordi inngrepshjemlene knyttes til de generelle og vide bestemmelsene i kapittel 3 om tjenestens oppgaver. Departementet er enig i at lovgivningen må være tilstrekkelig klar og forutberegnelig for å oppfylle lovskravet. I dette ligger blant annet at lovgivningen må være tilgjengelig og utformes i tråd med alminnelige rettsstatsprinsipper. Departementet opprettholder vurderingen av at lovforslaget balanserer hensynet til en tilstrekkelig presis angivelse av hvilke formål som kan begrunne informasjonsinnhenting med hensynet til et tilstrekkelig fleksibelt regelverk som kan følge utviklingen. Det vises til punkt 4.3.2 for en nærmere drøftelse av lovskravet og til merknaden til bestemmelsen for en nærmere utdypning av lovens vilkår.

Departementet har vurdert *riksadvokatens* innspill til strukturelle endringer i §§ 1-1 og 3-1, men tar ikke disse til følge. Etter departementets vurdering bør den overordnede beskrivelsen av lovens formål i § 1-1 bokstav a fremgå av en egen formålsbestemmelse fremfor som en del av Etterretningstjenestens oppgaver etter § 3-1, se punkt 5.1.

7.4 Okkupasjonsberedskap

7.4.1 Gjeldende rett

Det følger av etterretningstjenesteloven § 3 tredje ledd at Etterretningstjenesten skal sikre ivaretakelse av en nasjonal evne til å innhente og formidle informasjoner og etterretninger til norske myndigheter fra et helt eller delvis okkupert Norge. Dette omtales gjerne som okkupasjonsberedskap. Forsvarsdepartementet skal holdes generelt orientert om okkupasjonsberedskapen og forelegges saker om organiseringen av denne, jf. instruks om Etterretningstjenesten § 13 bokstav b. Etter direktiv fra forsvarsministeren har tjenesten 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 planverk og gjennomføring av trening og øving. Det ligger i dagen at informasjon om beredskapens organisasjon, ledelse, aktivitet

og forberedelser er å anse som særlig sensitiv og krever en spesielt høy grad av beskyttelse og skjerming, også internt i Etterretningstjenesten.

7.4.2 Forslaget i høringsnotatet

Det foreslås i høringsnotatet å videreføre Etterretningstjenestens oppgaver i forbindelse med okkupasjonsberedskapen. Det foreslås å regulere oppgaven i en egen bestemmelse i lovutkastet § 3-3 med tilnærmet samme ordlyd som i gjeldende lov. Det foreslås også å lovfeste at departementet skal holdes generelt orientert om okkupasjonsberedskapen.

7.4.3 Høringsinstansenes syn

Ingen høringsinstanser kommenterer forslaget.

7.4.4 Departementets vurdering

Departementet viderefører forslaget i høringsnotatet.

7.5 Internasjonalt etterretningssamarbeid

7.5.1 Gjeldende rett

Det følger av etterretningstjenesteloven § 3 andre ledd at Etterretningstjenesten kan etablere og opprettholde etterretningssamarbeid med andre land. I forarbeidene fremheves dette som en viktig oppgave for tjenesten, og det forutsettes at internasjonalt etterretningssamarbeid kan utgjøre et selvstendig grunnlag for informasjonsinnhenting, jf. Ot.prp. nr. 50 (1996–97) side 15:

> «Etablering og opprettholdelse av etterretningssamarbeid med andre land [...] er en av tjenestens hovedoppgaver. Det ligger også i denne bestemmelsen at Etterretningstjenesten kan innhente informasjon om forhold som er av betydning for samarbeidende lands tjenester, selv om forholdene ikke direkte er 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 [...]»

7.5.2 Forslaget i høringsnotatet

I høringsnotatet foreslås en egen bestemmelse om informasjonsinnhenting som ledd i internasjonalt etterretningssamarbeid i lovutkastet § 3-4. Bestemmelsen viderefører gjeldende rett og foreslås å gjelde både for bilateralt og multilateralt samarbeid. Det foreslås uttrykkelig presisert at innhentingen bare kan skje når det er i norsk interesse. Det understrekes i høringsnotatet at innhentingshjemmelen må ses i sammenheng med vilkårene for å dele opplysninger med andre land, som er regulert i lovutkastet kapittel 10.

7.5.3 Høringsinstansenes syn

Ingen høringsinstanser kommenterer forslaget.

7.5.4 Departementets vurdering

Departementet opprettholder forslaget i høringsnotatet. Det er behov for internasjonalt etterretningssamarbeid for å motvirke grenseoverskridende trusler og ivareta andre sammenfallende interesser. Norsk utenlandsetterretningstjeneste har alltid samarbeidet nært med viktige allierte. Slikt samarbeid har vært, og er, avgjørende for Norges etterretningsevne i våre nærområder. Etterretningstjenesten samarbeider med en rekke partnere over hele verden, både i og utenfor NATO. Departementet mener at det bør fremgå av loven at tjenesten kan innhente informasjon om utenlandske trusler og andre forhold som antas å være av vesentlig betydning i slikt samarbeid, når dette er i Norges interesse.

7.6 Evneinformasjon

7.6.1 Gjeldende rett

Etterretningstjenesteloven inneholder ingen bestemmelser som direkte regulerer innhenting av informasjon som utgjør en nødvendig forutsetning for å kunne innhente etterretningsinformasjon (evneinformasjon). En slik adgang vurderes å følge forutsetningsvis av informasjonsinnhentingsbegrepet i etterretningstjenesteloven § 3.

7.6.2 Forslaget i høringsnotatet

Det foreslås i høringsnotatet at innhenting av evneinformasjon lovfestes i § 3-5. Det beskrives i høringsnotatet punkt 7.9 at Etterretningstjenesten 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 så målrettet og risikofritt som mulig. Begrepet «evneinformasjon» er ment å illustrere at innhentingen ikke gjelder innhenting av etterretningsinformasjon som sådan, men utgjør en nødvendig forutsetning for *evnen* til informasjonsinnhenting. Innhentingen foreslås begrenset til fire formål, nemlig for å kunne sørge for at innhentingen av etterretningsinformasjon ikke skjer i større utstrekning enn nødvendig, for å ivareta sikkerheten til tjenestens personell og operasjoner, for å gjennomføre testing av teknisk utstyr og annen trenings- og øvingsaktivitet, og for å opprettholde og videreutvikle tjenestens aksesser og metodiske, teknologiske og øvrige evne til å utføre pålagte oppgaver.

7.6.3 Høringsinstansenes syn

Dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors kommenterer:

> «Etterretningstjenesten skal kunne innhente og analysere informasjon for bl.a. [å] sørge for at innhentingen ikke skjer i større grad enn nødvendig, altså som ledd i en slags egenkontroll. De skal også kunne innhente informasjon for å teste teknisk utstyr og i trenings- og øvingsaktivitet.»

Politiets sikkerhetstjeneste (PST) kommenterer lovforslaget § 3-5 bokstav c om testing, trening og øving i forbindelse med den territorielle begrensningen i lovutkastet § 4-2 femte ledd. Det reises spørsmål ved behandlingsreglene knyttet til trening og øving i Norge.

7.6.4 Departementets vurdering

Departementet opprettholder forslaget i høringsnotatet med enkelte språklige endringer. I tillegg foreslås det å gjøre oppregningen i bokstav a til d uttømmende. Adgangen til å innhente nødvendig informasjon i forkant av innhenting av etterretningsinformasjon leses i dag ut av innhentingsbegrepet i etterretningstjenesteloven § 3. Uten slike forberedelser, for eksempel trening og øving eller kartlegging av sikkerhetssituasjonen eller signalmiljøet i et område, vil innhentingen av etterretningsinformasjon gjøres mer komplisert og farefull og mindre spisset enn nødvendig. Etter departementets syn er det ønskelig å uttrykkelig lovfeste adgangen til å innhente evneinformasjon, som ledd i den helhetlige lovreguleringen av tjenestens informasjonsinnhentingsvirksomhet. Hjemmelen foreslås inntatt i lovforslaget kapittel 3 for å knytte den til innhentingshjemlene i §§ 3-1 til 3-4. Ingen høringsinstanser har uttrykt innvendinger mot forslaget. Kommentaren til *Politiets sikkerhetstjeneste* knyttet til den territorielle begrensningen behandles i punkt 8.7.

8 Forbud mot innhenting i Norge og andre særskilte forbud

8.1 Innledning

Etterretningstjenestens oppgaver følger av lovforslaget kapittel 3. 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 for politiformål.

8.2 Andre lands rett

8.2.1 Sverige

Etter *lag (2000:130) om försvarsunderrättelseverksamhet* skal etterretningsvirksomheten bare rette seg mot utenlandske forhold. Det følger imidlertid ingen eksplisitt territoriell begrensning av loven som regulerer innhenting av informasjon på svensk territorium eller annen innhenting mot svenske borgere.

Lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet fastsetter at det ikke skal innhentes signaler mellom avsender og mottaker som begge befinner seg i Sverige. Utover dette er forholdet til innhenting av informasjon på svensk territorium ikke regulert.

8.2.2 Danmark

Lov om Forsvarets Efterretningstjeneste (FE) fastsetter at FEs etterretningsmessige virksomhet er rettet mot forhold i utlandet. Innhenting og bruk av opplysninger om personer som er hjemmehørende og oppholder seg i Danmark, kan likevel skje dersom opplysningene fanges opp i forbindelse med utenlandsetterretning, jf. § 3. FE kan også innhente opplysninger om en fysisk person som er hjemmehørende i Danmark, men som befinner seg i utlandet. Forutsetningen for dette 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.

8.2.3 Finland

Lag om militär underrättelseverksamhet (590/2019) fastsetter at den militære etterretningsvirksomheten skal rette seg mot militær virksomhet mot Finland og annen virksomhet som alvorlig truer det finske forsvaret eller samfunnets vitale funksjoner. Det er ikke fastsatt en territoriell begrensning av loven som angir forholdet til innhenting av informasjon på finsk territorium. I forbindelse med innhenting av informasjon om datatrafikk som krysser Finlands grenser i kommunikasjonsnettet, fremgår det imidlertid at det ikke vil være anledning til å benytte søkebegreper som identifiserer teleterminalutstyr eller teleadresse som innehas av eller antas å brukes av en person som oppholder seg i Finland.

8.3 Forbud mot innhenting i Norge

8.3.1 Gjeldende rett

Det følger av etterretningstjenesteloven § 4 første ledd at Etterretningstjenesten på norsk territorium ikke skal overvåke eller på annen fordekt måte innhente informasjon om norske fysiske eller juridiske personer.

Selv om forbudet etter sin ordlyd er begrenset til å gjelde *norske* fysiske og juridiske personer, praktiseres det slik at også utlendinger med fast eller midlertidig lovlig opphold i riket, for eksempel i form av å være turist eller asylsøker, omfattes.

Forbudet gjelder på *norsk* territorium. Dette omfatter det norske land-, sjø-, og luftterritoriet, herunder Svalbard, Jan Mayen og bilandene. Områder som kun er underlagt norsk jurisdiksjon, slik som norske utenriksstasjoner eller norskregistrerte fartøyer på åpent hav eller i utlandet, faller utenfor. Forbudet er ikke i veien for innhenting av etterretningsrelevant informasjon om norske personer som befinner seg i utlandet.

Forbudet er etter sin ordlyd begrenset til å *overvåke* eller på *annen fordekt måte* innhente informasjon om norske personer i Norge. Begrepene «overvåkning» og «fordekt» tilsier at det bare er innhenting som skjer i skjul, uten at den som berøres er kjent med det, som omfattes. Videre tilsier ordlyden at innhenting av åpent tilgjengelig informasjon ikke omfattes av forbudet, fordi slik innhenting ikke kan regnes som «fordekt». Forbudet gjelder *innhenting* av informasjon. Innhentingsbegrepet forutsetter en aktiv opptreden fra Etterretningstjenestens side. Frivillig samkvem mellom norske personer og tjenesten rammes følgelig ikke. Forbudet er heller ikke til hinder for at tjenesten kan motta informasjon fra andre.

Bestemmelsen forbyr ikke Etterretningstjenesten å etterspørre informasjon som andre besitter om fysiske eller juridiske personer i Norge. Den som forespørselen retter seg mot, må selv vurdere om de lovlig kan dele informasjonen. Etterretningstjenesten har anledning til å oppbevare relevant informasjon om norske borgere som oppholder seg i Norge, jf. loven § 4 andre ledd.

Forbudet i etterretningstjenesteloven § 4 første ledd gjelder informasjonsinnhenting *om* norske personer. Hva begrepet «om» innebærer, er et tolkningsspørsmål. I praksis har begrepet «om» blitt tolket som å forby informasjonsinnhenting *rettet mot* etterretningsmål i Norge, men ikke til å forby alle metoder for innhenting av informasjon som kan berøre personer i Norge, så fremt innhentingen er rettet mot etterretningsmål i utlandet. Dette har i praksis blitt omtalt som at det innfortolkes et krav om overvåkningshensikt i begrepet «om».

8.3.2 Forslaget i høringsnotatet

Det foreslås i høringsnotatet at den territorielle begrensningen i etterretningstjenesteloven § 4 videreføres, men i en noe annen utforming. Forslaget formulerer hovedregelen i en egen bestemmelse i lovutkastet § 4-1, og presiseringer og unntak følger av § 4-2.

I hovedregelen i utkast til § 4-1 første ledd oppstilles det et forbud mot å rette innhenting av informasjon mot en fysisk person som oppholder seg i Norge. I andre ledd foreslås et tilsvarende forbud mot å rette innhenting av informasjon mot virksomheter i Norge. Tredje ledd presiserer at dersom Etterretningstjenesten er i tvil om en person oppholder seg eller driver virksomhet i Norge, skal tjenesten søke å avklare forholdet basert på den informasjon som er tilgjengelig eller som for dette formål kan skaffes til veie fra åpne kilder, samarbeid eller egen innhenting.

I høringsnotatet redegjøres det for hvordan begrepene «overvåkning eller annen fordekt innhenting» og ordet «om» tolkes og praktiseres etter gjeldende lov § 4 første ledd. Det understrekes at den grunnleggende forutsetningen er at gjeldende utgangspunkter videreføres i ny lov, men at formuleringene må tilpasses dagens trusselbilde og teknologiske forutsetninger. Man foreslår i denne forbindelse å gå bort fra begrepet «om» og at forbudet mot informasjonsinnhenting mot personer og virksomheter i Norge burde formuleres på en tydeligere måte. Det foreslås en hovedregel som forbyr innhenting «rettet mot» personer og virksomheter i Norge. Vilkåret bygger på en forutsetning om at forbudet bare gjelder der det foreligger overvåkningshensikt fra Etterretningstjenestens side. Dette anses å være i tråd med gjeldende praksis.

8.3.3 Høringsinstansenes syn

De høringsinstansene som har uttalt seg om spørsmålet, støtter en videreføring av forbudet mot å innhente informasjon om personer i Norge. Flere har likevel kritiske merknader til utformingen av hovedregelen i § 4-1 og unntaksbestemmelsen i § 4-2, og mener at det fremstår som uklart hvor grensen for Etterretningstjenestens adgang til å innhente informasjon i Norge vil gå. Noen er skeptiske til at det skal være avgjørende hvorvidt tjenesten har overvåkningshensikt eller ikke, og anser dette som et lite egnet vurderingstema. Blant høringsinstansene som gir uttrykk for at forslaget er uklart eller legger opp til en vanskelig avgrensning, er *Borgarting lagmannsrett, Datatilsynet, dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors, Justis- og beredskapsdepartementet (JD), Kripos, Norges institusjon for menneskerettigheter (NIM), Politidirektoratet (POD), Politiets sikkerhetstjeneste (PST), riksadvokaten, Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget)* og *Teknisk-naturvitenskapelig forening (Tekna)*.

Borgarting lagmannsrett fremhever at det i den foreslåtte domstolskontrollen i kapittel 8 kan være vanskelig for domstolen å føre reell kontroll med at forbudene i kapittel 4 blir overholdt. Etter lagmannsrettens syn er det til dels uklart hva som ligger i begrepet «rettet mot» i utkastet til § 4-1, og dette bør etter lagmannsrettens syn omtales nærmere i forarbeidene. Dette synspunktet deles av

dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors.

Norges institusjon for menneskerettigheter (NIM) påpeker at rekkevidden av forbudet i § 4-1 fremstår som uavklart. NIM uttaler at det er usikkert om det er ment å oppstilles en mellomkategori av tilfeller der det innhentes informasjon om personer i Norge uten at innhentingen er «rettet mot» personen, og dermed går klar av forbudet i forslaget til § 4-1, men der innhentingen heller ikke er direkte regulert i unntaksbestemmelsen i § 4-2. Også *EOS-utvalget* har innvendinger til lovforslaget, og mener at dette ikke løser sentrale uklarheter knyttet til Etterretningstjenestens overvåkning av personer i Norge. Utvalget er ikke enig i høringsnotatets beskrivelse av gjeldende rett når det hevdes at begrepet «om» i dagens etterretningstjenestelov § 4 må forstås som «rettet mot». Etter utvalgets mening innebærer forslaget til regulering dermed ikke en videreføring av gjeldende rett, men en utvidelse av tjenestens mulighet til å innhente relevant informasjon i Norge sammenlignet med i dag. Utvalget uttaler:

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

Om kravet til overvåkningshensikt uttaler EOS-utvalget at dette er lite egnet fordi begrepet «rettet mot» kan tilsløre det faktum at Etterretningstjenestens metoder rent faktisk kan benyttes i etterretningsøyemed overfor kommunikasjon til personer som oppholder seg i Norge, så lenge innsamlingen er «rettet mot» forhold eller personer i utlandet. Dette kan etter utvalgets syn på sikt medføre en uthuling av territorialforbudet. Utvalget bemerker at det kan bli vanskelig å kontrollere hva slags *hensikt* tjenesten har i det enkelte tilfellet. Innhentingsforbudet må etter utvalgets syn klargjøres i det videre lovarbeidet. Utvalget fremholder at Stortinget som lovgiver må ta stilling til hvorvidt tjenesten bør være pålagt en begrensning i muligheten til å innhente relevant informasjon i Norge.

Datatilsynet deler skepsisen mot et krav om overvåkningshensikt, og fremholder at dette fremstår som en retorisk øvelse. Etter Datatilsynets oppfatning er det uvesentlig for den enkelte som berøres av innhentingen om innhentingen er rettet mot vedkommende eller mot noen andre, all den tid det samles inn informasjon om personen. Datatilsynet mener at dette ikke kommer klart frem av loven. Et lignende argument fremføres av *Tekna*, som viser til at et krav om overvåkningshensikt fremstår som konstruert.

Om bestemmelsens geografiske begrensning reiser *Datatilsynet* spørsmål om hvorfor norske borgere som oppholder seg i utlandet ikke skal ha samme beskyttelse som de som befinner seg i Norge. Datatilsynet kan ikke se noen god begrunnelse for at retten til privatliv ikke skal være lik, uavhengig av hvor man oppholder seg.

Norges offisers- og spesialistforbund (NOF) anser at utkastet til ny lov gir et klarere bilde av Etterretningstjenestens oppgaver. NOF viser spesielt til ansvarsfordelingen med PST, samt hva som er å regne som norske statsborgere.

Flere aktører i justissektoren uttaler seg om grensesnittet mellom Etterretningstjenesten og politiets oppgaver, og mener at lovforslaget på dette området ikke er tydelig nok. *Justis- og beredskapsdepartementet (JD)* viser til at grensedragningen mellom Etterretningstjenesten og Politiets sikkerhetstjeneste (PST) har vært gjenstand for grundige vurderinger gjennom årene. Siden lovforslaget er ment å kodifisere gjeldende rett, påpeker JD at man må sikre at territorialforbudet i § 4-1 gis en utforming som på best mulig måte ivaretar de grensedragningene som følger av gjeldende rett. JD presiserer at grenseflater og samarbeid mellom Etterretningstjenesten og andre aktører bør være avklart så godt som mulig, ved at lovverket gir minst mulig rom for tolkningstvil, og at forarbeidene gir god tolkningsstøtte for aktørene. JD mener at man på bakgrunn av høringen bør se nærmere på om lovforslaget kan justeres slik at grensedragning og hjemler for informasjonsutveksling kommer klarere frem.

Kripos mener at det er hensiktsmessig å klargjøre den territorielle begrensningen, men savner en mer utførlig drøftelse av hvor grensen for innhentingsvirksomheten vil gå i praksis, og indikerer at et krav om «overvåkningshensikt» er en uklar begrensning.

Politidirektoratet (POD) uttaler at det ikke kan være tvilsomt at det er politiet som har ansvaret for å forebygge og etterforske ulovlig etterretningsvirksomhet på norsk territorium. Dette prinsipielle skillet mellom politiet og Forsvaret må etter PODs syn iakttas i lovforslaget kapittel 4.

Politiets sikkerhetstjeneste (PST) uttaler:

> «Det påpekes flere steder i høringsnotatet at loven ikke er ment å innebære endringer i oppgavefordelingen og ansvarsområdene mellom Etterretningstjenesten og PST. Imidlertid kan lovteksten og uttalelser i forarbeidene skape uklarheter og tolkningstvil relatert til Etterretningstjenestens innhenting og ansvar på norsk territorium, samt grensedragningen mot PST. Selv om en slik grensedragning ikke er et primærformål for lovreguleringen, er det likevel avgjørende med klare rammer for hva som er henholdsvis Etterretningstjenestens og PSTs mandat.»

PST legger til at lovforslagets §§ 4-1 og 4-2 er utformet på en slik måte at det er egnet til å skape tvil knyttet til Etterretningstjenestens adgang til å operere på norsk jord. PST tar også til orde for at den delen av Etterretningstjenestens metodebruk som berører personer eller virksomheter innenfor norsk jurisdiksjon, bør underlegges domstolskontroll.

Riksadvokaten mener at det er vanskelig å se hvor Etterretningstjenestens handlingsrom i Norge slutter, noe som kan føre til overlapping med PST eller etterretningssvikt. Etter riksadvokatens syn bør lovforslaget endres slik at det blir klarere med hensyn til hvem Etterretningstjenesten kan rette sine aktiviteter mot og med hvilket formål. Forskjellen til politiets oppgaver bør fremkomme tydeligere.

8.3.4 Departementets vurdering

Departementet fastholder som grunnleggende utgangspunkt at Etterretningstjenesten ikke skal drive fordekt informasjonsinnhenting overfor personer eller virksomheter på norsk territorium. Høringen har vist bred støtte til denne tilnærmingen. Hovedregelen bør derfor fortsatt være at Etterretningstjenestens innhentingsvirksomhet er territorielt begrenset.

Samtidig tar departementet på alvor de innsigelser som har kommet mot utformingen av forslaget i høringsnotatet. Lovverket må så klart og tydelig som mulig angi grensene for Etterretningstjenestens handlingsrom på norsk jord.

Det er dessuten viktig at grensen mellom Etterretningstjenesten og PST angis klart. Et uklart grensesnitt mellom tjenestene kan på den ene siden føre til overlappende innhenting og rapportering, og på den andre siden til at ingen innhenter den relevante informasjonen. Begge situasjonene kan lede til etterretningssvikt. Departementet tar på alvor at PST mener at lovforslaget og uttalelser i høringsnotatet kan skape uklarheter og tolkningstvil relatert til Etterretningstjenestens innhenting og ansvar på norsk territorium, samt grensedragningen mot PST.

Departementet har på denne bakgrunn justert, omformulert og omredigert hovedregelen og unntakene for å gjøre dem tydeligere og enklere å forstå. Arbeidet har vært foretatt i nært samråd med Justis- og beredskapsdepartementet. Det foreslås etter dette å gå bort fra et forbud mot å rette informasjonsinnhenting mot personer i Norge og et krav om overvåkningshensikt. Hovedregelen i § 4-1 foreslås i stedet formulert som et forbud mot bruk av metoder for innhenting av informasjon overfor personer i Norge. Med personer menes både fysiske og juridiske personer. Forbudet knyttes til kapittel 6, som regulerer metoder for innhenting av informasjon som kan utgjøre et inngrep i noens menneskerettigheter. Fordelen med en slik innretning er at det ikke vil være et tolkingsspørsmål hvorvidt tjenesten benytter en innhentingsmetode etter kapittel 6. All metodebruk må besluttes i henhold til prosedyrebestemmelsene i lovforslaget §§ 6-12 og 6-13, som sikrer notoritet. Lovteknisk fjerner man dermed bruk av skjønnsmessige vilkår som det kan være vanskelig å kontrollere. Å knytte det territorielle forbudet opp mot et klart avgrenset kriterium imøtekommer etter departementets syn kritikken fra høringsrunden.

Et forbud mot bruk av innhentingsmetoder overfor personer i Norge kan ikke oppstilles uten unntak. I samsvar med gjeldende rett foreslås derfor enkelte unntak fra hovedregelen, se nærmere i punkt 8.4 til 8.7 nedenfor. Det presiseres at forbudet ikke uten videre innebærer et forbud mot informasjonsinnhenting utenfor Norge som direkte eller indirekte berører personer i Norge, se nærmere om dette i punkt 8.8 og lovforslaget § 4-7.

Norges institusjon for menneskerettigheter (NIM) reiser i sin høringsuttalelse spørsmål om hovedregelen med unntak og presiseringer er ment å være en uttømmende regulering, eller om det kan tenkes mellomkategorier. Departementet presiserer at lovforslaget skal forstås uttømmende, det vil si at det ikke kan brukes metoder etter kapittel 6 overfor personer på norsk territorium hvis ikke et av unntakene fra hovedregelen får anvendelse.

I lys av høringsuttalelsen til *Datatilsynet* presiserer departementet at forbudet mot å innhente informasjon om personer i Norge har bakgrunn i ansvarsfordelingen mellom Etterretningstjenesten og Politiets sikkerhetstjeneste. Det er klart

at norske myndigheter må kunne innhente informasjon om norske trusselaktører i utlandet. Denne oppgaven er i dag lagt til Etterretningstjenesten, og lovforslaget tar ikke sikte på å endre den gjeldende ansvarsfordelingen mellom norske myndigheter.

8.4 Fremmed statsaktivitet i Norge

8.4.1 Gjeldende rett

Etterretningstjenesteloven § 4 første ledd slår fast at Etterretningstjenesten ikke på norsk territorium skal overvåke eller på annen fordekt måte innhente informasjon om «norske» fysiske eller juridiske personer. En naturlig språklig forståelse av ordlyden tilsier at Etterretningstjenesten kan overvåke *utenlandske* personer og virksomheter i Norge, så fremt lovens vilkår for øvrig er oppfylt. Skillet mellom norske og utenlandske personer understrekes også i forarbeidene til gjeldende lov, der det heter at forbudet ikke rammer «innhenting av informasjon om utenlandske statsborgere som oppholder seg i Norge og annen fremmed aktivitet i Norge, så fremt dette er nødvendig for å gjennomføre Etterretningstjenestens oppgaver […]» (Ot.prp. nr. 50 (1996–97) side 11).

Selv om lovens ordlyd og forarbeider er klare, har bestemmelsen på dette punktet blitt tolket innskrenkende, og praktiseres i dag slik at Etterretningstjenesten bare innhenter informasjon om utenlandske fysiske og juridiske personer i Norge som opptrer *på vegne av* fremmed makt. Slik praksis var etablert lenge før vedtakelsen av etterretningstjenesteloven i 1998, og omtales blant annet i Lund-rapporten, som viser til tjenestens veletablerte avlytting av såkalte «utenlandske kontorer» i Norge.

Et annet spørsmål er om Etterretningstjenesten også kan overvåke *norske* personer som opptrer på vegne av fremmed makt i Norge. En slik adgang kan ikke leses ut av lovteksten. Det følger imidlertid av instruks om Etterretningstjenesten (e-instruksen) § 5 tredje ledd at loven ikke er til hinder for at tjenesten innhenter 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 den «klargjør spørsmål som hittil har fremgått som forutsetninger i proposisjonen som lå til grunn for loven». I proposisjonen heter det blant annet (Ot.prp. nr. 50 (1996–97) side 11):

> «E-tjenesten må ha full innsikt i fremmed etterretningsvirksomhet i Norge rettet mot den norske etterretningstjenesten, for – i samarbeid med overvåkingstjenesten – 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. Etter sin ordlyd er instruksen dermed uten betydning for tjenestens forhold til utenlandske personer som oppholder seg i Norge.

Innhenting om norske fysiske og juridiske personer i Norge for kontraetterretningsformål skal etter e-instruksen § 5 tredje ledd andre punktum skje gjennom, eller etter samtykke fra, PST. Dette er begrunnet i PSTs primæransvar for å forebygge og motvirke ulovlig etterretningsvirksomhet på norsk territorium. Som følge av at § 5 tredje ledd ikke regulerer tjenestens innhenting om utenlandske personer, kan bestemmelsen tolkes slik at det ikke gjelder et samtykkekrav i disse tilfellene. I praksis har imidlertid samtykke blitt innhentet i alle tilfeller hvor formålet har vært å innhente informasjon om fremmed etterretningsvirksomhet i Norge.

Regler om samarbeidet mellom Etterretningstjenesten og PST er fastsatt i instruks 13. oktober 2006 om samarbeidet mellom Etterretningstjenesten og Politiets sikkerhetstjeneste (samarbeidsinstruksen). Det følger av § 8 tredje ledd at tjenestene så langt som mulig skal samarbeide og utveksle informasjon med sikte på å unngå unødvendig etterretningsinnsamling og analyse vedrørende samme forhold. Det følger av dette at PST skal informeres dersom Etterretningstjenesten innhenter informasjon om utenlandske personer i Norge.

8.4.2 Forslaget i høringsnotatet

Det vises i høringsnotatet punkt 8.5.1 til at det er behov for å videreføre et unntak som sikrer at Etterretningstjenesten kan innhente informasjon om fremmed aktivitet i Norge, men at unntaket bør tydeliggjøres i forslaget til ny lov. Det drøftes hvilke personkategorier i Norge som Etterretningstjenesten bør kunne innhente informasjon om, og om det burde gjelde en formålsbegrensning. Det løftes frem som en grunnleggende forutsetning at unntaket i lovforslaget skal bygge på gjeldende ansvars- og oppgavefordeling mellom Etterretningstjenesten og PST.

Det foreslås i høringsnotatet at Etterretningstjenesten ikke lenger bør ha adgang til å innhente informasjon om *norske* statsborgere i Norge for kontraetterretningsformål, og heller ikke for andre formål i fredstid. Det vises til at det ligger innenfor oppgavene til PST å forebygge og etterforske slik aktivitet etter politiloven, og at Etterretningstjenesten vil ha anledning til å treffe adekvate forebyggende tiltak for å ivareta egen sikkerhet etter sikkerhetsloven § 4-3 med forskrifter.

Det vises til at dette stiller seg annerledes dersom det foreligger konkrete holdepunkter for at en *virksomhet*, enten virksomheten er norsk eller ikke-norsk, opptrer i Norge på vegne av fremmed makt. I slike tilfeller vil innhentingen være rettet mot virksomheten som sådan, og ikke mot fysiske personer. Det understrekes at de personvernhensyn som gjør seg gjeldende for fysiske personer, ikke i samme grad gjør seg gjeldende overfor virksomheter.

Det anbefales i høringsnotatet at Etterretningstjenesten fortsatt bør kunne innhente informasjon om *utenlandske* statsborgere som opptrer på vegne av fremmed makt i Norge. Det vises til at det foreligger en fast og langvarig praksis for slik innhenting, som vurderes å ha åpenbar utenlandsetterretningsmessig relevans.

Når det gjelder samtykkekrav for innhenting i Norge, vises det til at e-instruksen § 5 kan tolkes slik at den kun oppstiller krav om samtykke fra PST der Etterretningstjenesten innhenter informasjon om norske personer i Norge i kontraetterretningsøyemed. Det foreslås at det fremdeles bør gjelde et samtykkekrav dersom informasjonsinnhenting gjelder fremmed etterretningsvirksomhet i Norge. I tråd med forslaget om at Etterretningstjenesten ikke lenger skal kunne innhente informasjon om norske personer i Norge, vil samtykkekravet gjelde innhenting om utenlandske statsborgere og norske og utenlandske virksomheter som opptrer på vegne av fremmed makt. Det foreslås ikke krav om samtykke fra PST til innhenting om fremmed aktivitet i Norge med andre formål enn kontraetterretning.

8.4.3 Høringsinstansenes syn

Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget) og *Kripos* bemerker at Etterretningstjenestens innhenting om norske statsborgere i Norge foreslås å bortfalle i forslaget til ny lov. *Kripos* slutter seg til en slik innsnevring, men tilføyer at innhenting mot virksomheter som sådan står i et annet lys.

Enkelte høringsinstanser, herunder *Advokatforeningen* og *Kripos*, hevder at det oppstilles forholdsvis omfattende unntak fra innhentingsforbudet og at det på nærmere vilkår åpnes for vidtrekkende metodebruk på norsk jord, basert på til dels uklare skjønnsmessige rammer og med lav grad av legalitetskontroll. *Advokatforeningen* tilføyer at Etterretningstjenesten etter forslaget selv skal vurdere om det foreligger «konkrete holdepunkter» for at noen opptrer på vegne av fremmed makt. *Kripos* refererer at det ikke foreslås krav om sannsynlighetsovervekt for tilknytning til fremmed makt, men at det må foreligge ett eller flere objektive holdepunkter for dette.

Både *Kripos* og *Politiets sikkerhetstjeneste (PST)* mener at lovforslaget etablerer en uklar grenseflate mellom ansvarsområdene til Etterretningstjenesten og PST. *Kripos* begrunner dette i at den nærmere rekkevidden av unntakene fra innhentingsforbudet er vanskelig å få tak på. Samme høringsinstans fremhever at kravet om tilknytning til fremmed makt er en uforutsigbar terskel, og at begrepet «fremmed makt» fremstår som uklart utenfor begrepets kjerneområde. *Kripos* viser i forlengelsen av dette til Stortingets behandling av EOS-utvalgets særskilte melding av juni 2016, hvor det ble vist til at regelverket må legge til rette for en effektiv oppgaveløsning og ivaretakelse av sikkerhetshensyn, og at Etterretningstjenesten er nødt til å være utrustet med nødvendige virkemidler for å kunne utføre sitt oppdrag. Kripos uttaler at de støtter dette, og har forståelse for at utøvelsen av fremmed etterretningsvirksomhet i Norge må ligge innenfor tjenestens innhentingsfokus.

PST mener at den praksis som høringsnotatet beskriver, der innhenting om utenlandske personer i Norge skal skje gjennom eller etter samtykke fra PST bare i kontraetterretningstilfellene, ikke kan leses tydelig ut av gjeldende lov, instruks eller forarbeider. *PST* uttaler i denne forbindelse:

> «Det fremstår med andre ord uklart hva som faktisk er henholdsvis Etterretningstjenestens og PSTs oppgaver på dette feltet, og om tjenestenes respektive nedslagsfelt er tenkt å overlappe hverandre.»

All den tid praksisen nå ønskes lovfestet, mener *PST* at Etterretningstjenestens virke i Norge, samt grenseflaten mot PSTs oppgaver, bør underlegges en sammensatt og grundig vurdering. PST frykter dessuten delvis parallellitet i tjenestenes oppgaver og risiko for etterretningssvikt. Dette kan etter PSTs syn få konsekvenser for norske beslutningstakere og internasjonalt etterretnings-

samarbeid. PST skriver at de ikke kan se noen mekanismer i lovforslaget som sikrer at tjenestenes respektive operasjoner holdes adskilt eller eventuelt koordineres.

EOS-utvalget viser til at utvalgets kontrolloppgave i dag ikke omfatter virksomhet «som angår utlendinger hvis opphold er knyttet til tjenesten for fremmed stat» jf. EOS-kontrolloven § 5 femte ledd. Gitt at denne begrensningen bortfaller med forslaget til ny EOS-kontrolloven § 5 femte ledd, mener *utvalget* det bør vurderes en eksplisitt varslingsplikt til EOS-utvalget i de tilfeller der PST har gitt samtykke til at Etterretningstjenesten kan bedrive etterretningsvirksomhet i Norge etter lovforslaget § 4-2 første ledd siste punktum. Samme varslingsplikt bør etter utvalgets syn gjelde også der Etterretningstjenesten eventuelt iverksetter innhenting uten samtykke fra PST, mot personer eller virksomheter som opptrer på vegne av fremmed makt (annen fremmed aktivitet).

8.4.4 Departementets vurdering

8.4.4.1 Persongrupper og samordningsplikt

Departementet mener at Etterretningstjenesten fortsatt bør kunne innhente informasjon om *utenlandske* personer som opptrer på vegne av fremmed stat i Norge. Dette kan blant annet dreie seg om statlig styrte operasjoner på norsk jord som krenker norsk suverenitet. På samme måte som i høringsnotatet mener departementet derimot at Etterretningstjenesten ikke lenger bør kunne innhente informasjon om *norske fysiske personer* som opptrer på vegne av fremmed stat i Norge. Som beskrevet i høringsnotatet, anser departementet det som tilstrekkelig at PST ivaretar denne oppgaven, og at Etterretningstjenesten, for å sikre egen virksomhet, treffer beskyttelsestiltak i henhold til sikkerhetsloven § 4-3.

Departementet gikk i høringsnotatet inn for at unntaket skulle omfatte innhenting av informasjon om *norske virksomheter* som opptrer på vegne av fremmed makt. På bakgrunn av innspill i høringsrunden videreføres ikke forslaget. Departementet viser til at slike virksomheter ofte vil ha en tilknytning til Norge som tilsier at de bør behandles på lik linje med norske fysiske personer. Forslaget innebærer en innsnevring i forhold til gjeldende rett. Departementet mener derimot at Etterretningstjenesten ikke bør være avskåret fra å innhente informasjon om *utenlandske* virksomheter i Norge som opptrer på vegne av fremmed stat.

Departementet foreslår at lovteksten, på samme måte som ellers i kapittelet, forenkles til kun begrepet «personer», som omfatter både fysiske og juridiske personer.

På bakgrunn av høringen foreslås begrepet «fremmed makt» erstattet med «fremmed stat eller statslignende aktør», som er mer presist. Statsbegrepet skal forstås på samme måte som i folkeretten. Det bør også være anledning til å innhente informasjon om utenlandske personer i Norge som handler på vegne av *statslignende* aktører, det vil si aktører som har klare statslignende trekk, men uten å oppfylle alle de fire kriteriene som folkeretten oppstiller til en stat. Det kan for eksempel være aktører som er anerkjent av norske myndigheter som en politisk aktør eller som det internasjonale samfunn aksepterer at opptrer med en viss folkerettslig handleevne, men uten å være en stat i formell forstand.

Flere aktører fra justissektoren har under høringen kommet med viktige innspill knyttet til grensesnittet mellom Etterretningstjenesten og PST. Departementet understreker at nært samarbeid, informasjonsdeling og gjensidig respekt er sentrale forutsetninger for at tjenestene skal kunne ivareta nasjonens og befolkningens sikkerhet, og for en effektiv bruk av samfunnets ressurser.

På samme måte som i høringsnotatet legger lovforslaget til grunn at den gjeldende arbeidsfordelingen mellom Etterretningstjenesten og PST videreføres. Samtidig viser høringen at dagens regelverk kan forstås på ulike måter. Dette understreker behovet for en tydeligere lovregulering. Det er sentralt at regelverket legger til rette for at den enkelte tjeneste kan ivareta sine oppgaver, samtidig som man motvirker overlappende innhenting og etterretningssvikt. Overlappende innhenting er dårlig bruk av samfunnets ressurser, kan være negativt for operasjonssikkerheten, og kan gi et skjevt eller uriktig beslutningsgrunnlag fordi informasjon som i virkeligheten stammer fra én kilde, vil kunne fremstå som om den har to kilder. Instruks 13. oktober 2006 om samarbeidet mellom Etterretningstjenesten og Politiets sikkerhetstjeneste (samarbeidsinstruksen) sikrer generell samordning mellom tjenestene. Når det gjelder samordning knyttet til innhenting om fremmed statsaktivitet i Norge, vurderer departementet etter høringen at det er grunn til å fastsette en egen informasjons- og samtykkebestemmelse i etterretningstjenesteloven. Forslaget fremgår av § 4-3.

Departementet foreslo en samtykkebestemmelse også i høringsnotatet, men denne var begrenset til innhenting av informasjon om fremmed etterretningsvirksomhet i Norge. I lys av inn-

spill under høringen samt påfølgende dialog med Justis- og beredskapsdepartementet, mener departementet at plikten til å innhente samtykke bør utvides til å gjelde alle tilfeller der innhentingsoppdraget også faller inn under en av oppgavene til PST, slik disse er beskrevet i politiloven § 17 b. Dette understreker at det er PST som er landets innenlands sikkerhets- og etterretningstjeneste, med det primære ansvaret for å innhente informasjon om trusselaktører i Norge.

Etterretningstjenesten kan innhente informasjon om fremmed statsaktivitet i Norge som faller utenfor politiloven § 17 b, for eksempel om rent militære eller andre strategiske forhold som faller utenfor oppgavene til PST. I slike tilfeller er det ikke riktig å oppstille krav om samtykke fra PST. Departementet mener likevel at det bør oppstilles en plikt til å *informere* PST om innhentingen, av hensyn til å samordne tjenestenes aktiviteter i Norge. Informasjonsplikten sikrer også at PST kan reise innsigelser dersom de mener at innhentingen er av en karakter som forutsetter samtykke.

Departementet følger ikke opp forslaget fra *EOS-utvalget* om at det bør lovfestes en generell varslingsplikt til utvalget i løpende saker. En slik varslingsordning samsvarer ikke med EOS-kontrollovens system og prinsippet om etterfølgende kontroll. Departementet legger til grunn at EOS-utvalget vil kunne kontrollere vurderingen som ligger bak samtykke og informasjonshenvendelsen, og departementet forutsetter at Etterretningstjenesten vil legge særskilt til rette for EOS-utvalgets kontroll i disse sakene dersom EOS-utvalget mener det er behov for det.

8.4.4.2 Beredskapssituasjoner o.l.

Dersom det skulle oppstå en beredskapssituasjon eller væpnet konflikt på norsk territorium, vil Etterretningstjenesten ha en særskilt rolle i å understøtte nasjonale og allierte militære operasjoner med informasjon. Etterretningstjenesten skal også legge forholdene til rette for at etterretningsarbeidet i alle deler av Forsvaret skal skje så koordinert og effektivt som mulig. Tidlig varsling og evne til å avdekke forberedende militære handlinger fra en potensiell fiende er avgjørende. I slike situasjoner vil motstanderen selv utøve militær etterretningsvirksomhet på norsk territorium.

Fiendtlige styrkers aktivitet i Norge vil alltid være å anse som opptreden *på vegne av fremmed stat*, og vil derfor dekkes av lovforslaget § 4-2 første ledd. I opptakten til og under en væpnet konflikt vil Etterretningstjenesten også ha behov for å innhente informasjon om *norske personer og forhold*, i den utstrekning dette er nødvendig og forholdsmessig for å understøtte Forsvarets evne til å håndtere fiendtlig militær aktivitet på norsk territorium. Blant annet vil det kunne være behov for å innhente informasjon om norske personer som bør evakueres eller som samhandler med fiendestaten. Det kan også være aktuelt å innhente opplysninger om norske virksomheter, særlig med hensyn til hvilke sårbarheter disse har, i den hensikt å vurdere konsekvenser ved fiendtlige aktiviteter og anslag. Det vil også kunne være nødvendig å danne et etterretningsmessig normalbilde i et geografisk område, som kan inkludere opplysninger om norske personer og virksomheter, for å avdekke unormal fiendtlig aktivitet i det aktuelle området. Slik innhenting bør være formålsbegrenset til informasjon som har betydning for Forsvarets evne til å håndtere fiendtlig militær aktivitet.

Det er sentralt å sikre at hjemmelen ikke kan benyttes i fredstid. Departementet foreslår derfor at den utelukkende kan benyttes når riket er i krig eller krig truer eller rikets selvstendighet og sikkerhet står i fare, hvilket tilsvarer kriteriene i beredskapsloven § 3 og annen beredskapslovgivning. På samme måte som i beredskapsloven § 3 foreslås det å legge beslutningsmyndigheten til Kongen. Siden beredskapsloven § 3 gir hjemmel til å treffe tiltaket, er det rettslig sett ikke nødvendig med en spesifikk lovregulering av det. Departementet har etter en nærmere vurdering likevel kommet til at hensyn til klarhet og demokratisk forankring tilsier en særskilt lovregulering av tiltaket. Bestemmelsen foreslås inntatt i § 4-2 tredje ledd. For å sikre forutsigbarhet i beredskapsplanleggingen kan det være aktuelt å la bestemmelsen danne grunnlag for et tiltak i Nasjonalt beredskapssystem.

8.5 Åpne kilder som berører personer i Norge

8.5.1 Gjeldende rett

Etterretningstjenesteloven § 4 første ledd forbyr overvåkning og annen fordekt innhenting om norske personer og virksomheter i Norge. En naturlig språklig forståelse av ordlyden tilsier at innhenting av åpent tilgjengelig informasjon ikke omfattes av forbudet, da slik innhenting ikke kan regnes som «fordekt». Forbudet er dermed ikke til hinder for at Etterretningstjenesten benytter åpent tilgjengelig informasjon som den besitter, herunder opplysninger om norske personer eller

virksomheter, som grunnlag for innhenting om utenlandske forhold eller personer. Søk vil eksempelvis kunne foregå på sosiale medier til norske personer, for eksempel fordi disse har hatt kontakt med terroristnettverk i utlandet.

8.5.2 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 8.8.3 å lovfeste at det ikke er i strid med forbudet mot å rette innhenting mot personer i Norge å innhente informasjon gjennom åpne kilder 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.

8.5.3 Høringsinstansenes syn

Datatilsynet kommenterer at det følger av lovforslaget § 6-2 at Etterretningstjenesten kan innhente informasjon fra åpne kilder, og at dette kan gjøres mot personer og virksomheter i Norge, jf. forslaget til § 4-2 åttende ledd. Tilsynet mener dette potensielt er svært personverninngripende, ettersom omfanget av personopplysninger som deles på nettet er enormt.

Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget) problematiserer forslaget i høringsnotatet om å presisere at innhenting av informasjon fra åpne kilder ikke strider mot den territorielle begrensningen. Utvalget er dessuten ikke enig i forståelsen av fordektbegrepet. Utvalget uttaler at det er vanskelig å se at innsamlingen fra åpne kilder ikke også vil være «rettet mot» personen i Norge:

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

Utvalget viser dessuten til at de i 2018 reiste spørsmål om hjemmelen for Etterretningstjenestens innsamling av informasjon fra åpne kilder tilhørende personer som var godkjente innhentingsmål i utlandet, men som oppholdt seg i Norge:

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

Om forståelsen av begrepet «fordekt» uttaler utvalget:

> «Så lenge informasjonen innhentes i skjul av E-tjenesten, må dette anses som «fordekt».»

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

8.5.4 Departementets vurdering

På bakgrunn av de strukturelle endringene som foreslås i lovforslaget kapittel 4, foreslår departementet at innhenting av informasjon om utenlandske forhold fra åpne kilder som berører personer i Norge reguleres i en egen bestemmelse i lovforslaget § 4-4. Unntaket er nødvendig fordi innhenting fra åpne kilder er en innhentingsmetode etter lovforslaget § 6-2, og dermed i utgangspunktet forbudt etter § 4-1.

Departementet foreslår i det oppdaterte lovforslaget å gå bort fra begrepet «rettet mot» og et krav om overvåkingshensikt. Begrepet «fordekt» brukes heller ikke i forslaget til lovregulering av den territorielle begrensningen. Departementet antar at disse endringene imøtekommer flere av innvendingene i EOS-utvalgets høringsuttalelse.

EOS-utvalget gir uttrykk for at søk i åpne kilder tilhørende personer som oppholder seg i Norge må vurderes likt som søk i lagrede metadata knyttet til norske rettssubjekter i Norge. Departementet deler ikke dette synspunktet. Metadatasøk med utgangspunkt i et norsk søkebegrep (selektor) bør etter departementets syn bare tillates i formålsavgrensede unntakstilfeller der det anses strengt nødvendig, se nærmere i punkt 8.9. Dette er fordi informasjonen det søkes i vil være innhentet fordekt, og fra kilder der det ikke forventes at andre vil få tilgang, for eksempel fra elektronisk kommunikasjon. Informasjon som ligger i åpne kilder er åpent tilgjengelig for alle, og det eksisterer etter departementets syn ikke en berettiget forventning om samme vern. At informasjonen kan være tilgjengeliggjort av andre enn den det gjelder, slik EOS-utvalget bemerker, endrer ikke på dette.

Informasjonsinnhenting fra åpne kilder faller i utgangspunktet inn under den alminnelige handlefrihet. Som påpekt av EOS-utvalget vil systematisk og målrettet innhenting av informasjon fra åpne kilder i enkelte tilfeller likevel kunne tenkes å utgjøre et inngrep overfor den enkelte i menneskerettslig forstand. Kravet om hjemmel i lov er i disse tilfellene tilfredsstilt gjennom bestemmelsene i lovutkastet §§ 4-4 og 6-2. Det understrekes at innhentingen vil være underlagt lovens vilkår for øvrig, herunder formålsbegrensningen, grunnvilkårene for innhenting, kravet til forholdsmessighet og bestemmelsene om behandling av personopplysninger.

8.6 Kildevirksomhet i Norge

8.6.1 Gjeldende rett

Det følger av etterretningstjenesteloven § 4 andre ledd at tjenesten kan «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 (Ot.prp. nr. 50 (1996–97) side 11):

> «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.»

I tråd med forutsetningene i forarbeidene heter det i e-instruksen § 5 andre ledd:

> «Tjenesten kan gjennomføre tiltak for å verifisere sine kilders troverdighet.»

Gjeldende lov og instruks angir ikke hvilke tiltak som kan gjennomføres i Norge for å rekruttere og verifisere kilder. I henhold til praksis er hovedregelen at tjenesten tilnærmer seg potensielle kilder åpent. I en innledende, avklarende fase er det imidlertid ikke krav om å tilkjennegi tilhørighet til norske myndigheter. De fordekte innhentingstiltak som benyttes, er menneskebasert innhenting, som i praksis innebærer samtaler der det ikke oppgis tilknytning til tjenesten, samt systematisk observasjon på offentlig sted. Slike fordekte tiltak gjennomføres bare dersom det foreligger tungtveiende sikkerhetsmessige grunner.

8.6.2 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 8.5.2 å videreføre gjeldende rett og praksis knyttet til rekruttering og verifisering av kilder i Norge. Etter forslaget kan Etterretningstjenesten 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. Hovedregelen foreslås å være at informasjonen skal innhentes gjennom åpne kilder, utlevering av opplysninger fra andre norske myndigheter, eller med samtykke fra den det gjelder. Det skal ikke innhentes mer informasjon enn det som fremstår som strengt nødvendig. Dersom det foreligger tungtveiende sikkerhetsmessige grunner, foreslås det at strengt nødvendig informasjon likevel kan innhentes i en avgrenset tidsperiode gjennom menneskebasert innhenting eller bruk av systematisk observasjon på offentlig sted. Det foreslås at annen metodebruk bare tillates dersom det foreligger samtykke.

I høringsnotatet er regler om kilderekruttering og kildeverifikasjon inntatt i lovutkastet § 4-2 andre og tredje ledd.

8.6.3 Høringsinstansenes syn

Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget) uttaler at forslaget synes å innebære en utvidelse av hjemlene etter gjeldende rett, og at det kan bli utfordrende å kontrollere de skjønnsmessige vilkårene i bestemmelsen:

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

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

Politiets sikkerhetstjeneste (PST) mener at forslaget muliggjør til dels vidtrekkende innhenting mot norske statsborgere og andre personer og virksomheter i Norge, og uttaler:

> «PST ser for seg at selv om informasjonen innhentes med kildeverifikasjonsformål, kan innhentet informasjon benyttes videre dersom den viser seg relevant for etterretningsformål etter at den er innhentet. Dette betyr at informasjonen også kan utleveres til andre, herunder PST, etter reglene i §§ 10-5 og 10-8.»

8.6.4 Departementets vurdering

Innhenting av informasjon fra menneskelige kilder, både norske og utenlandske, er viktig for Norges etterretningsevne. For å kunne føre kilder må kildene finnes og rekrutteres, og deres egnethet og troverdighet må vurderes. Det sistnevnte omtales som kildeverifikasjon, og er viktig for å unngå kompromittering av operasjoner eller personell. For eksempel er det sentralt å kunne forsikre seg om at kilden er den han eller hun utgir seg for å være, og ikke i realiteten handler på vegne av en annen stats etterretningstjeneste. Kildeverifikasjon er derfor en løpende prosess som ikke kan avsluttes når en kilde er rekruttert. I forkant av selve rekrutteringen må tjenesten først vurdere om den aktuelle personen besitter eller kan få tilgang til utenlandsetterretningsrelevant informasjon.

Departementet foreslår at hovedregelen, på samme måte som i dag, skal være at Etterretningstjenesten tilnærmer seg potensielle kilder i Norge åpent, og oppgir tilknytning til norske myndigheter eller tjenesten. Tjenestens frivillige samarbeid med menneskelige kilder over tid bør være basert på et informert samtykke fra kildene. I forkant av at det tas kontakt, kan det være nødvendig å innhente informasjon for å ta stilling til om en aktuell person vil være egnet som kilde. Det kan også være behov for å innhente informasjon om et relevant miljø eller organisasjon for å finne egnede kilder der. Slik innhenting må av sikkerhetsmessige årsaker kunne gjøres uten at det opplyses om det. For å minimere inngrepet bør bare de minst inngripende formene for innhenting av informasjon tillates. Det foreslås derfor som hovedregel at informasjonen skal innhentes fra åpne kilder eller ved utlevering fra norske myndigheter.

Departementet presiserer at hensikten med informasjonsinnsamlingen i kildeøyemed aldri er å innhente etterretningsrelevant informasjon om miljøer i Norge eller innenlandske forhold. Dette ligger utenfor Etterretningstjenestens mandat. Hensikten er utelukkende å avklare forhold knyttet til kildeoppdraget, nemlig den potensielle kildens troverdighet, egnethet, motivasjon, sikkerhet mv.

I noen situasjoner vil det være nødvendig å opptre fordekt overfor potensielle og eksisterende kilder, for eksempel dersom det finnes indikasjoner på at personen opererer på vegne av fremmed stats etterretningstjeneste. Departementet mener at slik fordekt informasjonsinnhenting bare bør tillates i unntakstilfeller, og fastholder forslaget i høringsnotatet om at slike metoder bare kan brukes hvis det foreligger tungtveiende sikkerhetsmessige grunner. På samme måte som i høringsnotatet mener departementet at det ikke bør kunne brukes andre metoder enn menneskebasert innhenting (lovforslaget § 6-3) og systematisk observasjon (lovforslaget § 6-4). Dette er i tråd med dagens praksis. Det vil ikke være hjemmel for å benytte øvrige metoder etter kapittel 6, med mindre det viser seg at kilden opptrer på vegne av fremmed stat eller statslignende aktør og innhenting kan skje etter § 4-2.

EOS-utvalget fremholder i sin høringsuttalelse at forslaget i høringsnotatet synes å innebære en utvidelse av hjemlene etter gjeldende rett, uten å utdype synspunktet. Departementet fastholder at lovforslaget viderefører gjeldende rett og praksis, men har etter høringen bestrebet seg på å formulere unntaksreglene i kapittel 4 på en tydeligere måte. Reglene om kildevirksomhet i Norge inntas i en egen bestemmelse i lovforslaget § 4-5, og justeres for å tydeliggjøre tjenestens handlingsrom og begrensninger.

EOS-utvalget uttaler også at det vil bli utfordrende for utvalget å kontrollere vilkårene «strengt nødvendig» og «tungtveiende sikkerhetsmessige grunner». Departementet har forståelse for at det kan være krevende å kontrollere

skjønnsmessige vilkår. Samtidig er det ikke til å komme fra at lovgivningen må basere seg på en viss grad av skjønn, for eksempel i dette tilfellet. Ordlyden viser at det skal mye til for at vilkårene er oppfylt, med en høyere terskel enn det som ellers følger av kravet til forholdsmessighet etter § 5-4. Det må nødvendigvis vurderes konkret hvorvidt vilkårene er oppfylt i den enkelte sak. Det vises for øvrig til merknadene til bestemmelsen.

Politiets sikkerhetstjeneste (PST) reiser i sin høringsuttalelse spørsmål om sekundærbruk av informasjon hentet inn for kildeverifikasjonsformål. Departementet foreslår i lys av merknadene til PST å endre bestemmelsen slik at det kommer klart frem at informasjon som hentes inn i forbindelse med kildevirksomhet i Norge, utelukkende kan brukes for å finne, rekruttere og verifisere kilder. Regelen innebærer at informasjonen ikke kan brukes til andre formål, herunder etterretningsproduksjon. Informasjonen kan ikke deles med andre myndigheter etter lovforslaget kapittel 10, hvis ikke formålet er kildesamarbeid.

8.7 Trening, øving og testing i Norge

8.7.1 Gjeldende rett

Innhenting av informasjon som ledd i utenlandsetterretningsvirksomhet krever at man trener og øver personell og tester utstyr og fremgangsmåter. Dette gjelder generelt, men er særlig viktig med hensyn til etterretningsoppdrag i konfliktsoner og andre fiendtlige miljøer. Også den teknologiske utviklingen tilsier at Etterretningstjenestens kapasiteter testes og øves jevnlig.

Etterretningstjenesten innhenter i dag opplysninger som ledd i trening, øving og testing i Norge. Dette reguleres ikke uttrykkelig i dagens regelverk, men er lagt til grunn som en forutsetning for i det hele tatt å kunne drive informasjonsinnhenting i utlandet, og kan på denne måten sies å implisitt følge av etterretningstjenesteloven § 3. Trenings-, øvings- og testaktivitetene er i dag regulert i interne prosedyrer som skal sikre at innhentingen ikke skjer i strid med de rettslige rammene som følger av Grunnloven § 102, EMK artikkel 8, gjeldende etterretningstjenestelov og personopplysningsloven 2000.

8.7.2 Forslaget i høringsnotatet

Innhenting av informasjon i trenings-, øvings- og testøyemed foreslås regulert i lovutkastet § 3-5 om evneinformasjon, mens egne behandlingsregler foreslås i lovutkastet § 9-10. I lovutkastet § 4-2 femte ledd foreslås en bestemmelse som presiserer at innhenting av informasjon som er strengt nødvendig for å kunne gjennomføre trening, øving og testing i Norge ikke er i strid med innhentingsforbudet i § 4-1. Bestemmelsen begrunnes med ønsket om å rydde av veie eventuell tvil om at innhentingen vil kunne komme i konflikt med hovedregelen om territoriell begrensning.

Det understrekes i høringsnotatet at innhenting av informasjon som ledd i trening, øving og testing ikke skal inngå i etterretningsproduksjon.

8.7.3 Høringsinstansenes syn

Politiets sikkerhetstjeneste (PST) viser til at innhentede opplysninger skal slettes «snarest mulig» etter at treningen, øvingen eller testvirksomheten er avsluttet, og uttaler:

> «Fordi denne øvings- og testingsvirksomheten ikke synes å ha noen lovpålagt tidsavgrensning, ser PST at det potensielt kan innhentes svært mye informasjon under dette formålet. Den behandlingsregelen som er foreslått i § 9-10 sier at informasjon skal slettes snarest mulig, men PST kan ikke se at det er oppstilt noe forbud mot å bruke informasjonen videre dersom den i perioden fra innhenting til sletting skulle vise seg å ha relevans for etterretningsformål, slik at behandlingsgrunnlaget skifter.
>
> Dersom det er tilfelle at informasjonen kan brukes til etterretningsformål dersom den viser seg relevant, vil det etter PSTs forståelse også bety at informasjonen også kan utleveres til andre dersom vilkårene er oppfylt. Dersom slik videre bruk av informasjonen ikke er tilsiktet, men denne uten unntak skal slettes nærmest umiddelbart, bør det kommenteres i forarbeidene slik at dette ikke er tvilsomt.»

PST uttaler følgende om forholdet mellom lovutkastet § 4-2 femte ledd og § 3-5:

> «Under forutsetning av at vi har forstått bestemmelsen riktig, stiller PST spørsmål ved om § 3-5 om innhenting av såkalt evneinformasjon, vil innebære at personkretsen som rammes av unntaket fra territorialforbudet i § 4-2, blir ytterligere utvidet.»

PST mener en konsekvens av § 3-5 første ledd bokstav c er at uvedkommende tredjepersoner kan bli rammet i ikke ubetydelig grad.

Riksadvokaten uttaler at unntaket favner vidt, og at det er vanskelig å se hvor grensene faktisk trekkes. Bestemmelsen vil etter riksadvokatens syn åpne for en generell adgang til å rette aktivitetene mot fysiske eller juridiske personer i Norge når dette begrunnes med et strengt behov for å kunne teste utstyr, trene og øve i vårt land.

8.7.4 Departementets vurdering

Departementet viderefører forslaget i høringsnotatet, men med enkelte endringer som følge av høringen. Unntaket knyttet til trening, øving og testing av utstyr i Norge inntas i en egen bestemmelse i lovforslaget § 4-6.

Ingen *høringsinstanser* bestrider behovet for at Etterretningstjenesten trener, øver og tester utstyr i Norge. Departementet tar som utgangspunkt at etterretningsvirksomhet stiller store krav til den enkelte tjenesteperson. Ved operasjoner i konfliktsoner vil det kunne få store konsekvenser, både for operasjonen i seg selv og tjenestepersonens liv og helse, dersom tjenestepersonen ikke er kjent med og kan håndtere innsamlingsmetodene på riktig måte. Etterretningstjenesten kan derfor ikke starte opptrening av tjenestepersoner eller testing av tekniske kapasiteter i fiendtlige omgivelser i utlandet. Det samme gjelder for øving og trening i menneskebasert innhenting. For at trening, øving og testing av utstyr skal ha effekt, må det skje under så realistiske forhold som mulig. Det er derfor nødvendig å la operatørene øve på innhenting av reell informasjon. Et eksempel på et slikt øvingsmoment kan være å finne ut hvem som jobber i en bestemt organisasjon, eller å få tak i telefonnummeret til en bestemt person gjennom samtale med vedkommende. Et eksempel på utstyrstest kan være å passivt kartlegge signalmiljøet i et bestemt område.

Som i dag forutsetter departementet at all aktivitet knyttet til trening, øving og testing reguleres nøye i forutgående øvingsordre, som er tilgjengelig for EOS-utvalget. Så langt mulig skal innhenting skje overfor markører, det vil si personer som deltar i øvingsaktiviteten. Ut over dette, og for å begrense inngrepet, mener departementet at innhenting bare kan skje dersom det er *strengt nødvendig* for å oppnå hensikten med treningen, øvingen eller testingen. Selv om det i prinsippet kan trenes og øves på alle innhentingsmetoder, går det en grense for hvilke metoder som kan brukes mot uvitende tredjepersoner i Norge. Det kan for eksempel neppe regnes som strengt nødvendig å teste utstyr for teknisk sporing overfor en uvitende tredjeperson i Norge.

Politiets sikkerhetstjeneste (PST) reiser i sin høringsuttalelse spørsmål om sekundærbruk av informasjon innhentet for trening, øving og testing. Departementet foreslår i lys av PSTs merknader å lovfeste at informasjonen utelukkende skal brukes for å trene, øve og teste utstyr. Dette innebærer at informasjonen aldri kan brukes til andre formål, som for eksempel etterretningsproduksjon. Informasjonen kan heller ikke deles med andre.

Departementet finner det mest hensiktsmessig å samle reglene for behandling av informasjon som er innhentet i Norge for trening, øving og testing i lovforslaget § 4-6, og viderefører ikke forslaget om en egen behandlingsregel i kapittel 9. Departementet opprettholder forslaget om at informasjonen som hentes inn skal slettes snarest mulig, og senest når treningen, øvingen eller testingen avsluttes. Det ligger i dette at informasjonen ikke kan oppbevares lenger enn det som er nødvendig for å få et treningsutbytte. Dette begrenser hvor mye informasjon tjenesten kan hente inn, og innebærer at informasjonen bare kan oppbevares over en kortere periode. Departementet viderefører forslaget fra høringsnotatet om at informasjonen ikke skal behandles sammen med annen informasjon. Dette tydeliggjør at informasjonen utelukkende skal brukes for trening, øving og testing, og ikke på noen måte blandes sammen med etterretningsinformasjon. For ordens skyld foreslås det også lovfestet at opplysningene ikke skal arkiveres i henhold til arkivloven.

Departementet viderefører forslaget fra høringsnotatet om at opplysninger kan behandles videre dersom det foreligger samtykke fra den opplysningene gjelder. Det foreslås ikke noe unntak fra formålsbegrensningen, så det vil fortsatt gjelde et vilkår om at informasjonen utelukkende brukes til trening, øving eller testing, og ikke til etterretningsproduksjon. Informasjonen kan imidlertid være nyttig for fremtidig opplæring. Det ligger i sakens natur at en person ikke kan samtykke til slik behandling dersom opplysningene dreier seg om andre personer eller forhold som den samtykkende ikke rår over.

8.8 Aksessorisk informasjon om personer i Norge

8.8.1 Gjeldende rett

Det følger av etterretningstjenesteloven § 1 bokstav a at tjenesten skal «bidra til å kartlegge og motvirke ytre trusler mot rikets selvstendighet og

sikkerhet og andre viktige nasjonale interesser». Etter § 3 første ledd skal tjenesten innhente informasjon «som angår norske interesser sett i forhold til fremmede stater, organisasjoner eller individer». Bestemmelsene viser at forbindelsen mellom *utenlandske etterretningsmål* på den ene siden og *norske interesser* på den andre siden står sentralt for tjenesten. Som en følge av dette vil tjenesten få befatning med informasjon som berører personer i Norge. Det er for eksempel ikke tvilsomt at tjenesten skal søke å innhente informasjon om utenlandske trusselaktørers kontakt med sine nettverk i Norge, utenlandske digitale angrep mot norsk infrastruktur og andre forsøk på sabotasje, spionasje mv. i Norge med opprinnelse fra utlandet. Felles for eksemplene er at det er tale om *grenseoverskridende aktivitet* med en utenlandsk og en norsk ende, og at tjenesten retter sin innhenting mot den *utenlandske enden*.

Etterretningstjenesteloven § 4 andre ledd fastslår at tjenesten kan oppbevare informasjon som gjelder norske fysiske eller juridiske personer dersom informasjonen har direkte tilknytning til ivaretakelsen av tjenestens oppgaver etter § 3. Tjenesten kan altså etter gjeldende rett oppbevare etterretningsinformasjon om norske personer, herunder om den norske enden i etterretningsrelevant grenseoverskridende aktivitet. Det kan for eksempel være informasjon om hvilke norske virksomheter en fremmed stat forsøker å angripe i det digitale rom, eller hvilke personer i Norge som en fremmed etterretningstjeneste eller et internasjonalt terrornettverk har kontakt med. Slik informasjon kan betegnes som *aksessorisk* i den forstand at informasjonen følger med ved innhenting rettet mot den utenlandske enden. Tjenesten kan derimot ikke på fordekt måte innhente informasjon om den norske enden av den grenseoverskridende aktiviteten, jf. § 4 første ledd.

Loven inneholder ingen spesifikk regulering av *rådata i bulk*, det vil si ubearbeidet eller automatisk bearbeidet informasjon der etterretningsverdien ikke er vurdert, og der en vesentlig andel av informasjonen antas å være uten interesse for etterretningsformål.

8.8.2 Forslaget i høringsnotatet

Det foreslås i høringsnotatet et forbud mot å rette innhenting av informasjon mot personer som oppholder seg i Norge i lovutkastet § 4-1. Det vurderes i høringsnotatet ikke som nødvendig å innta en presisering i lovteksten om at innhenting mot etterretningsmål i utlandet ikke strider mot forbudet, selv om det ved innhentingen vil kunne følge med informasjon om personer i Norge.

Det foreslås i høringsnotatet å presisere i lovteksten at innhenting av rådata i bulk ikke er å anse som rettet mot personer eller virksomheter i Norge selv om datasettet kan inneholde informasjon om personer i Norge (lovutkastet § 4-2 sjette ledd). Forslaget har bakgrunn i EOS-utvalgets særskilte melding til Stortinget 17. juni 2016, og har til hensikt å fjerne den rettslige usikkerheten knyttet til innhenting av rådata i bulk som EOS-utvalget peker på i meldingen. Det understrekes i høringsnotatet at stadig mer av den etterretningsrelevante informasjonen i dag befinner seg i det digitale domenet, og at den teknologiske utviklingen må reflekteres i et nytt og oppdatert rettslig rammeverk.

8.8.3 Høringsinstansenes syn

International Business Machines AS (IBM) deler departementets intensjon om en tydelig presisering av at innhenting av rådata i bulk ikke er å anse som rettet mot personer og virksomheter som befinner seg i Norge, selv om rådata kan inneholde opplysninger om disse. IBM anbefaler imidlertid å vurdere en annen formulering enn «å anse».

Norges institusjon for menneskerettigheter (NIM) omtaler den territorielle begrensningen i lovutkastet kapittel 4 i forbindelse med sine innspill til forslaget om tilrettelagt innhenting, og uttaler i den sammenheng at det er en naturlig konsekvens av hvordan bulkinnsamling fungerer at innhenting av rådata i bulk ikke rammes av forbudet i § 4-1.

Riksadvokaten bemerker at lovutkastet § 4-2 sjette ledd er utformet «nærmest i form av en slags definisjon», og uttaler at bestemmelsen i praksis vil kunne åpne for innhenting av informasjon om personer og virksomheter «i langt større omfang enn hva en er kjent med foregår i dag». Det pekes på at innhentingen ikke vil være undergitt domstolskontroll, og at informasjonen etter behandlingsreglene i kapittel 9 vil kunne lagres i inntil 15 år med mulighet for ytterligere forlengelse.

Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget) viser til at utvalget i særskilt melding til Stortinget i 2016 konkluderte med at det forelå rettslig usikkerhet knyttet til innhenting av metadata som kan inneholde opplysninger om norske borgere i Norge. Det heter videre:

> «Utvalget konstaterer at våre merknader til E-tjenestens praksis med innhenting av metadata

> i bulk som kan inkludere kommunikasjon til og fra norske rettssubjekter i Norge, er omgjort til et unntak fra innhentingsforbudet for E-tjenesten i forslaget § 4-2 sjette ledd.»

Utvalget uttaler dessuten at det foreslåtte unntaket fra innhentingsforbudet er knyttet til rådata i bulk generelt, og ikke begrenset til metadata:

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

EOS-utvalget fremhever videre at det er viktig å styrke utvalgets etterfølgende kontroll av Etterretningstjenestens innhenting av rådata i bulk, blant annet ved at utvalget får egne verktøy for kontroll i tjenestens systemer.

8.8.4 Departementets vurdering

Departementet har på bakgrunn av høringen omredigert forslaget til unntaksbestemmelse i § 4-2 og splittet den opp i flere paragrafer. Etter departementets vurdering bør det i en egen paragraf gjøres klart at forbudet mot innhenting i Norge ikke er til hinder for at det ved innhenting av informasjon om etterretningsmål i utlandet følger med informasjon om personer i Norge. En slik bestemmelse om *aksessorisk informasjon om personer i Norge* inntas i lovforslaget § 4-7. På samme måte som ellers i kapittelet omfatter personbegrepet både fysiske og juridiske personer.

Ordet «aksessorisk» betegner at informasjonen om personen i Norge *følger med* ved innhenting av informasjon om etterretningsmål i utlandet. Den norske informasjonen er *aksessorisk til* informasjonen om det fremmede målet i den forstand at hvis det ikke var for innhentingen mot det fremmede målet, ville ikke tjenesten ha kommet i befatning med den norske informasjonen. Det kan være *tilsiktet* eller *utilsiktet* at det ved innhenting mot et mål i utlandet følger med informasjon om personer i Norge. For eksempel vil det være *tilsiktet* å se hvilke norske mål fremmede aktører forsøker å ramme i en påvirkningsoperasjon, slik som påvirkning av valg eller andre demokratiske prosesser, eller i et digitalt angrep med sikte på sabotasje eller spionasje. Det vil også være tilsiktet å forsøke å avdekke grenseoverskridende terrorplanlegging eller hvilke forgreininger et internasjonalt nettverk som sprer masseødeleggelsesvåpen har til Norge. Felles for disse eksemplene er at Etterretningstjenesten innhenter informasjon om den utenlandske enden av en grenseoverskridende trussel, hvor informasjon om den norske forbindelsen også er etterretningsrelevant. Innhenting av informasjon rettet mot den norske enden ligger derimot utenfor tjenestens mandat. Slik innhenting må utføres av andre myndigheter, som Politiets sikkerhetstjeneste. Departementet understreker at Etterretningstjenesten ikke kan benytte innhentingsmetoder overfor personer i Norge med mindre en av unntaksbestemmelsene etter lovforslaget kapittel 4 kommer til anvendelse, typisk ved fremmed statsaktivitet i Norge etter lovforslaget § 4-2.

Informasjon om norske personer kan også være informasjon som er uten interesse for etterretningsformål, altså overskuddsinformasjon. At Etterretningstjenesten kommer i besittelse av overskuddsinformasjon er en *utilsiktet* konsekvens av innhenting mot etterretningsmål i utlandet, typisk ved innhenting av rådata i bulk. Departementet opprettholder forslaget i høringsnotatet om å presisere i lovteksten at innhenting av rådata i bulk ikke strider mot forbudet mot innhenting i Norge selv om informasjon om personer i Norge kan følge med i datasettet. En slik presisering fjerner den rettslige usikkerheten som EOS-utvalget peker på i sin særskilte melding 17. juni 2016, og bidrar til å sørge for at innhenting av rådata i bulk har trygg rettslig forankring. Presiseringen er inntatt i lovforslaget § 4-7 andre ledd.

I lys av høringsuttalelsen til *EOS-utvalget* presiserer departementet at forslaget ikke er begrenset til metadata eller innhenting av kommunikasjonssignaler i transitt mellom en avsender eller en mottaker, men skal gjelde generelt. Bulkinnhenting er nærmere omtalt under punkt 9.4. Selv om slik innhenting er særlig relevant når det gjelder kommunikasjonsetterretning, kan det i prinsippet brukes ved enhver innhentingsmetode. Departementet slutter seg til EOS-utvalgets merknad knyttet til betydningen av kravet til forholdsmessighet i denne sammenhengen. På samme måte som ved annen innhenting må Etterretningstjenesten vurdere nødvendighet og forholdsmessighet etter lovforslaget § 5-4 når de

henter inn informasjon i bulk. Det må i denne forbindelse vurderes om inngrepet vil utgjøre et uforholdsmessig inngrep overfor den enkelte. Dette innebærer en vurdering av om mindre inngripende tiltak i tilstrekkelig grad kan ivareta formålet, virkningen for de som rammes, sakens betydning og forholdene ellers. Hvorvidt og i hvilken utstrekning bulkdatasettet kan inneholde informasjon om personer i Norge, vil være et relevant moment i vurderingen av forholdsmessighet.

Selv om det sjelden vil være mulig å garantere at det ikke ligger informasjon om personer i Norge i et bulkdatasett, er det et grunnleggende utgangspunkt å søke å unngå dette i størst mulig grad. Ved tilrettelagt innhenting av metadata i bulk (lovforslaget § 7-7) vil det samles inn store mengder data om norsk innenlandsk kommunikasjon. Dette skyldes at det av tekniske årsaker ikke er mulig å filtrere ut all norsk innenlandsk kommunikasjon. Det vises til punkt 11.8.2 for en nærmere redegjørelse. Bulkinnhenting fra andre kilder vil i langt mindre grad berøre norsk innenlandsk kommunikasjon. For eksempel vil det ved bulkinnhenting fra satellittkommunikasjon aldri være slik at begge endene av kommunikasjonen stammer fra Norge, og over 99 % av innhentede data vil ikke være knyttet til norske personer.

Å forby innhenting i bulk fordi det ikke kan utelukkes at datasettene kan inneholde informasjon om personer i Norge, er etter departementets syn ikke et reelt alternativ. Bulkinnsamling er en forutsetning for moderne kommunikasjonsetterretning. Det vises til drøftelsen av behovet for bulkinnhenting i punkt 9.4. Departementet er enig med EOS-utvalget i at utvalgets muligheter til etterfølgende kontroll av Etterretningstjenestens innhenting av rådata i bulk bør styrkes, blant annet ved at utvalget får egnede verktøy for kontroll i tjenestens systemer. Etterretningstjenesten tilrettelegger allerede i dag for slik kontroll. I tillegg kommer at utvalgets kontroll med tilrettelagt innhenting foreslås styrket, se punkt 11.10. Departementet antar at den kontrollmetodikk og de kontrollverktøy som vil utvikles og benyttes i forbindelse med tilrettelagt innhenting, også vil kunne benyttes i kontrollen med annen bulkinnhenting.

8.9 Søk i lagrede rådata med utgangspunkt i norsk søkebegrep

8.9.1 Gjeldende rett

Etterretningstjenesten kan i noen tilfeller ha behov for å bruke et søkebegrep (selektor), for eksempel et telefonnummer, tilknyttet en person i Norge som utgangspunkt for søk i lagrede rådata med sikte på å finne utenlandske etterretningsmål. Slike søk er ikke direkte regulert i etterretningstjenesteloven. Loven forbyr i § 4 første ledd *overvåkning og annen fordekt innhenting* av informasjon om norske personer på norsk territorium. Ordlyden kan tilsi at søk i data som er lovlig innhentet, ikke rammes, da søk i lagrede data ikke innebærer «fordekt innhenting» av informasjon. Det følger av § 4 andre ledd at Etterretningstjenesten kan oppbevare informasjon som gjelder norske personer dersom informasjonen har direkte tilknytning til ivaretakelsen av tjenestens oppgaver etter § 3.

EOS-utvalget drøftet rettsgrunnlaget for metadatasøk med utgangspunkt i et norsk søkebegrep i sin særskilte melding til Stortinget 17. juni 2016. Utvalget kom til at søkene har en rettslig uavklart stilling, og uttalte på side 21 i meldingen:

> «Utvalget anser det som en lovgiveroppgave å ta stilling til om E-tjenesten skal kunne innhente informasjon av utenlandsetterretningsmessig relevans via selektorer knyttet til norske rettssubjekter i Norge, og i tilfelle hvilke vilkår og kontrollmekanismer som skal gjelde for dette.»

Under henvisning til den rettslige uklarheten og den etterretningsfaglige vurderingen av behovet for søkene, fant EOS-utvalget ikke grunnlag for å rette kritikk mot Etterretningstjenesten. Utvalget uttalte at det heller ikke forelå grunn til å anmode tjenesten om å suspendere innhentingsmetoder i påvente av en eventuell stortingsbehandling av de spørsmålene som ble reist i den særskilte meldingen.

8.9.2 Forslaget i høringsnotatet

I høringsnotatet punkt 8.7 drøftes behovet og begrunnelsen for søk i rådata med utgangspunkt i et norsk søkebegrep (selektor). Det vises til at en slik adgang, dersom den skal opprettholdes, må gis en tydelig forankring i loven.

Det anbefales i høringsnotatet at adgangen bør opprettholdes. Det legges avgjørende vekt på at søkene er rettet mot utenlandske forhold og at det ikke foreligger overvåkningshensikt overfor personen eller virksomheten i Norge. Formålet med søkene er ikke å skaffe til veie informasjon om norske personer og innenlandske forhold, men å finne frem til ukjente trusselaktører i utlandet som er i kontakt med den norske selektoren. Søkene vurderes som en forberedende aktivitet

med det formål å frembringe nødvendig grunnlagsmateriale slik at tjenesten på et senere tidspunkt kan innhente informasjon om et utenlandsk etterretningsmål.

På denne bakgrunn foreslås det i lovutkastet § 4-2 syvende ledd at søk i rådata med utgangspunkt i et søkebegrep som kan knyttes til en norsk person eller virksomhet i Norge, kan gjennomføres dersom søket ikke er rettet mot denne personen. Fordi unntaket vil kunne berøre personer i Norge, foreslås det et forhøyet terskelkrav; søket må ha eller kunne få «vesentlig betydning» for ivaretakelsen av Etterretningstjenestens oppgaver etter kapittel 3.

8.9.3 Høringsinstansenes syn

Dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors uttaler at utkastet til § 4-2 har til dels kompliserte unntak og at disse innenfor rammen av tilrettelagt innhenting skal kontrolleres av domstolen. Forslaget til bestemmelse i lovutkastet § 4-2 syvende ledd trekkes av dommerne frem som et eksempel på et slikt komplisert unntak.

Norges institusjon for menneskerettigheter (NIM) kommenterer utkastet til § 4-2 syvende ledd i forbindelse med sin omtale av forslaget om tilrettelagt innhenting. NIM viser til drøftelsen av menneskerettslige krav knyttet til statlig overvåkning av egne borgere, og uttaler at dette stiller strengere krav til reguleringen:

> «På bakgrunn av EMDs praksis som er redegjort for ovenfor, er det nærliggende at dette vil bli ansett som overvåking av egne borgere og følgelig underlagt et krav om «strict necessity». NIM mener derfor at dette bør reflekteres i lovteksten slik at det fremgår at dette kun er tillatt når det er «strengt nødvendig». Antageligvis kan dette kravet også medføre en begrensning i hvilke av E-tjenestens oppgaver som kan berettige søket, og det bør derfor vurderes om den generelle henvisningen til oppgavene i forslaget kapittel 3 reflekterer dette.»

Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget) viser til at utvalget i sin særskilte melding 17. juni 2016 uttalte at søk i lagrede metadata knyttet til norske rettssubjekter i Norge står i et problematisk forhold til etterretningstjenesteloven § 4. Utvalget uttaler:

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

EOS-utvalget mener det er utfordrende å se hvordan man kan utføre søk i informasjon som er innhentet fordekt gjennom Etterretningstjenestens tekniske innsamlingssystemer, ved bruk av selektorer tilhørende personer i Norge, uten at dette er «rettet mot» personen i Norge. Utvalget tilføyer at selv om det anføres at søk i slike rådata ikke er «rettet mot» personen i Norge, vil i hvert fall personens kommunikasjon rent faktisk være gjenstand for tjenestens aktive etterretningsvirksomhet. I denne forbindelse uttaler utvalget at det vil være vanskelig for utvalget å kontrollere at søkene i realiteten ikke er «rettet mot» personen i Norge.

8.9.4 Departementets vurdering

Departementet tar som utgangspunkt at det oppdaterte forslaget i § 4-1 oppstiller et forbud mot metodebruk etter lovforslaget kapittel 6 overfor personer i Norge. Det kan hevdes at søk i lovlig innhentet informasjon med utgangspunkt i et søkebegrep (selektor) som kan knyttes til en person i Norge, for eksempel et telefonnummer, ikke bryter med forbudet, fordi det ikke innebærer bruk av metoder etter kapittel 6. På den andre siden kan det hevdes at slike søk står i en spenning med begrunnelsen for forbudet, nemlig at Etterretningstjenesten skal befatte seg med utenlandske forhold.

Det er ikke tvilsomt at Etterretningstjenesten har som en sentral oppgave å finne forbindelsen mellom utenlandske etterretningsmål og Norge, se nærmere punkt 7.3. Én måte å gjøre dette på, er å søke etter forbindelsen til Norge med utgangspunkt i utenlandske søkebegreper som tjenesten besitter. Hvis denne fremgangsmåten er mulig, bør den benyttes. I noen tilfeller kan det derimot være nødvendig å søke med utgangspunkt i et norsk søkebegrep, fordi man ikke besitter noen andre relevante inngangsverdier. Departementet understreker at søket ikke kan ta sikte på å finne informasjon om innenlandske forhold, som for eksempel de norske kontaktene til et norsk telefonnummer eller IP-adresse. Det er utelukkende forgreiningene til utlandet som ligger innenfor Etterretningstjenestens mandat, og som søket skal ta sikte på å avdekke.

Fordi søk med utgangspunkt i et norsk søkebegrep kan hevdes å stå i et spenningsforhold til

forbudet mot å bruke innhentingsmetoder overfor personer i Norge, foreslår departementet etter høringen å innsnevre adgangen sammenlignet med forslaget i høringsnotatet. Med bakgrunn i høringsuttalelsen til *NIM* mener departementet at adgangen til å foreta slike søk bør formålsbegrenses. I det oppdaterte lovforslaget § 5-3 tredje ledd kan søk i rådata med utgangspunkt i et søkebegrep som kan knyttes til en person i Norge, ikke gjennomføres med mindre det er strengt nødvendig for å ivareta en oppgave som nevnt i § 3-1, det vil si for å avdekke og motvirke utenlandske trusler mot Norge. Det ligger i kravet til streng nødvendighet at dersom det er mulig å nå fram til det samme resultatet ved å søke med utgangspunkt i utenlandske søkebegreper, skal det ikke søkes med utgangspunkt i et norsk søkebegrep.

Søk med utgangspunkt i et norsk søkebegrep kan for eksempel være aktuelt dersom tjenesten besitter telefonnummeret til en person i Norge som tilhører et internasjonalt miljø som søker å spre masseødeleggelsesvåpen. På cyberområdet kan det være aktuelt å benytte en norsk IP-adresse som har vært utsatt for et dataangrep som søkebegrep for å forsøke å finne kommunikasjon til og fra adressen som kan identifisere den utenlandske aktøren som står bak angrepet og dennes handlingsmønster. Et annet eksempel kan være søk med utgangspunkt i søkebegreper knyttet til en person som har gjennomført terrorhandlinger i Norge, med sikte på å identifisere forgreininger til utenlandske trusselaktører.

Departementet vurderer at dersom ikke Etterretningstjenesten skal kunne foreta slike søk i rådatamateriale som tjenesten allerede besitter, vil man være i en situasjon der heller ingen andre norske myndigheter har mulighet til å skaffe til veie det som kan være avgjørende opplysninger for ivaretakelsen av norsk sikkerhet. Det er bare Etterretningstjenesten som sitter på et slikt utenlandsetterretningsrelevant rådatagrunnlag. Behovet er balansert mot en formålsbegrensning og et forhøyet terskelkrav som gjør at dette er en adgang som bare vil kunne brukes i unntakstilfeller. Hensynet som begrunner den territorielle begrensningen vurderes dermed å være ivaretatt.

Fordi søk i et rådatagrunnlag som Etterretningstjenesten allerede besitter ikke innebærer innhenting av ny informasjon ved metoder som nevnt i lovforslaget kapittel 6, hører ikke forslaget til bestemmelse lenger hjemme i kapittel 4. Departementet foreslår derfor at bestemmelsen inntas i lovforslaget kapittel 5 om grunnvilkår for innhenting og utlevering av informasjon, som tredje ledd i § 5-3.

8.10 Mottak av informasjon fra andre

8.10.1 Gjeldende rett

Etterretningstjenesten kan etter gjeldende rett både motta og anmode om å få utlevert informasjon om fysiske og juridiske personer i Norge. Å motta opplysninger som andre frivillig deler med tjenesten, eller å be om informasjon fra andre, rammes ikke av forbudet i etterretningstjenesteloven § 4 første ledd mot overvåkning og annen fordekt innhenting av norske personer i Norge. Det følger av § 4 andre ledd at tjenesten kan oppbevare opplysninger om norske personer dersom informasjonen har direkte tilknytning til ivaretakelsen av tjenestens oppgaver etter § 3. Når relevansvilkåret ikke lenger er oppfylt, skal opplysningene slettes.

Et illustrerende eksempel kan være at Etterretningstjenesten mottar opplysninger fra PST om norske fremmedkrigere selv om disse på utleveringstidspunktet befinner seg på norsk territorium. Det er behov for å få tidlig informasjon om disse, for å kunne være forberedt på å rette innhenting mot personene dersom de reiser til utlandet og på den måten 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, se punkt 8.6.

8.10.2 Forslaget i høringsnotatet

Det vises i høringsnotatet punkt 8.5.3 til at det fortsatt er behov for at Etterretningstjenesten kan motta og anmode om å få utlevert opplysninger om personer og virksomheter i Norge, når dette er direkte relevant for ivaretakelsen av tjenestens oppgaver. Det foreslås en presisering i lovutkastet § 4-2 fjerde ledd om at dette ikke kommer i konflikt med hovedregelen i utkast til § 4-1.

Det understrekes at adgangen ikke skal kunne brukes for å omgå Etterretningstjenestens eget regelverk og begrensninger. Eksempelvis skal ikke forespørsler fra tjenesten til andre undergrave den territorielle begrensningen. EOS-utvalget vil kunne undersøke og kontrollere at slike omgåelser ikke finner sted.

8.10.3 Høringsinstansenes syn

Ingen høringsinstanser har kommentert forslaget.

8.10.4 Departementets vurdering

Departementet fastholder vurderingen i høringsnotatet om at Etterretningstjenesten må kunne motta informasjon fra andre om personer eller virksomheter i Norge, og be andre om å utlevere slik informasjon til tjenesten, forutsatt at informasjonen er relevant for etterretningsformål.

Etter høringen er lovforslaget § 4-1 omformulert til et forbud mot å bruke metoder etter lovforslaget kapittel 6 overfor personer i Norge. Mottak av informasjon innenfor rammene av nasjonalt og internasjonalt samarbeid er ikke en innhentingsmetode etter kapittel 6, men reguleres i kapittel 10. Mottak av informasjon fra noen som utleverer denne uoppfordret til tjenesten, i form av tips eller annet, er heller ikke en innhentingsmetode. Disse måtene å komme i besittelse av informasjon på som kan omfatte norske forhold dekkes dermed ikke av forbudet i det oppdaterte forslaget til § 4-1. Departementet finner det derfor ikke nødvendig å videreføre forslaget i høringsnotatet om å lovfeste at det ikke strider med forbudet etter § 4-1 å motta eller be om å få motta slik informasjon. Den som utleverer informasjonen, må selv vurdere om det foreligger hjemmel for å dele opplysningene med Etterretningstjenesten.

Regler om behandling av informasjon som tjenesten mottar fra andre, er gitt i lovforslaget kapittel 9. Departementet understreker at informasjonen bare kan behandles dersom den er relevant for etterretningsformål.

8.11 Forbud mot å innhente informasjon med politiformål

8.11.1 Gjeldende rett

Det følger av etterretningstjenesteloven § 1 at tjenesten skal bidra til å kartlegge og motvirke ytre trusler mot rikets selvstendighet og sikkerhet og andre viktige nasjonale interesser. Loven fastslår i § 3 første ledd at tjenesten 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. Tjenesten har derimot ingen oppgaver knyttet til å forebygge, etterforske og straffeforfølge kriminalitet. Dette er oppgaver som tilligger Politiets sikkerhetstjeneste (PST), politiet for øvrig og påtalemyndigheten.

Samtidig er det slik at fremmede trusler mot Norge kan berøre både Etterretningstjenesten og PST eller politiet for øvrig. For eksempel kan fremmed etterretningsvirksomhet mot Norge være både en ytre trussel mot nasjonal sikkerhet og en straffbar handling. Et annet eksempel er terrorisme som stammer fra utlandet. I slike saker skal tjenestene samarbeide og utveksle informasjon. Regler om samarbeidet er gitt i instruks 13. oktober 2006 om samarbeidet mellom Etterretningstjenesten og Politiets sikkerhetstjeneste (samarbeidsinstruksen). Instruksen skal fremme samarbeid mellom tjenestene på områder av felles interesse, og bidra til at tjenestene gjennom informasjonsutveksling, samhandling og arbeidsdeling effektivt kan møte aktuelle trusler og sikkerhetsutfordringer (samarbeidsinstruksen § 1). Det følger av instruksen § 2 at samarbeidet mellom tjenestene skal skje innenfor rammen av de respektive overordnede rettsgrunnlag som gjelder for hver enkelt tjeneste. Det innebærer for eksempel at Etterretningstjenesten ikke kan motta informasjon fra politiet dersom det allerede på utleveringstidspunktet er klart at informasjonen ikke har eller vil kunne få noen relevans for Etterretningstjenestens oppgaver.

Etterretningstjenesten kan i dag, på lik linje med resten av Forsvaret, bli anmodet om å bistå politiet etter politiloven § 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.

8.11.2 Forslaget i høringsnotatet

Det foreslås i høringsnotatet ingen endringer av gjeldende oppgavefordeling mellom Etterretningstjenesten på den ene siden, og politiet og påtalemyndigheten på den andre siden. Det vurderes likevel i høringsnotatet punkt 8.10 som formålstjenlig å oppstille et forbud i lovutkastet § 4-4 som fastsetter at Etterretningstjenestens virksomhet ikke skal ha som formål å løse kriminalitetsforebyggende eller kriminalitetsbekjempende oppgaver som tilligger politiet eller andre rettshåndhevende myndigheter. Hensikten med bestemmelsen er å understreke at tjenesten innhenter og analyserer informasjon med et utenlandsetterretningsformål, ikke politiformål.

Samtidig vektlegges det i høringsnotatet at Etterretningstjenesten og PST er pålagt å samarbeide nært på en rekke prioriterte områder, og at økt samarbeid har vært, og er, en ønsket utvikling. Det vises til at det de senere år er etablert flere samarbeidssentre, slik som Felles kontraterrorsenter (FKTS) og Felles cyberkoordinerings-

senter (FCKS). Mer samhandling og samarbeid mellom innenlands- og utenlandstjenester er dessuten en klar trend internasjonalt, særlig som følge av flere grenseoverskridende trusler og moderne kommunikasjonsteknologi. Bestemmelsen er ikke ment å legge noen hindre i veien for de etablerte ordninger for utveksling av informasjon som er innhentet av de respektive tjenester etter eget rettsgrunnlag.

8.11.3 Høringsinstansenes syn

Flere høringsinstanser i justissektoren stiller spørsmål ved behovet for og utformingen av bestemmelsen. *Kripos* oppfatter forslaget som overflødig fordi bestemmelsen ikke sier mer enn hva som ellers følger av lovens formålsbegrensning og gjeldende regelverk rundt Forsvarets bistand til politiet. *Politiets sikkerhetstjeneste (PST)* og *Politidirektoratet (POD)* stiller spørsmål ved hvordan en slik bestemmelse vil bli forstått av de som skal praktisere regelverket. PST stiller i denne forbindelse spørsmål ved om bestemmelsen, dersom den innføres:

> «[…] i praksis vil oppstille en kanskje utilsiktet skranke for Etterretningstjenestens mulighet til å motta informasjon fra PST, særlig for det tilfellet at delingen ikke på utleveringstidspunktet umiddelbart kan begrunnes utelukkende for Etterretningstjenestens formål.»

PST er enig i at det ikke skal tilligge Etterretningstjenesten å forebygge og etterforske kriminalitet, men stiller spørsmål ved om det er nødvendig å lovfeste et uttrykkelig forbud utover den positive formålsangivelsen av Etterretningstjenestens oppgaver. PST er av den oppfatning at man må unngå at loven setter begrensninger eller skaper tvil om Etterretningstjenestens mulighet til å motta og behandle opplysninger fra PST. Det fremheves at uklarheter i loven kan innebære et forsinkende element for en effektiv og tidsriktig utveksling av informasjon.

POD mener at lovutkastet ikke i tilstrekkelig grad tar innover seg politiets beredskapsmessige rolle og betydningen av etterretning for politiets arbeid. For det annet peker POD på at det som etter lovutkastet § 3-1 er definert som Etterretningstjenestens oppgaver (informasjonsinnhenting om utenlandske trusler), også vil være oppgaver med politiformål. POD uttaler videre:

> «Politidirektoratet forstår at forbudet etter § 4-4 betyr at Etterretningstjenesten ikke av eget tiltak kan innhente informasjon om alvorlig kriminalitet som begås i utlandet selv om slik informasjon etter omstendighetene kan ha stor betydning for norsk eller utenlandsk politi for å forebygge eller iretteføre slik kriminalitet. Dette vil blant annet bety at Etterretningstjenesten har forbud mot å dele informasjon med Den internasjonale straffedomstolen som ble opprettet mot å straffeforfølge enkeltindivider for krigsforbrytelser, forbrytelser mot menneskeheten og folkemord. Selv om slik etterretningsinformasjon er av avgjørende betydning for at domstolen skal kunne iretteføre denne type straffesaker. Videre at forbudet betyr at Etterretningstjenesten ikke skal innhente informasjon om internasjonal og grenseoverskridende kriminalitet som menneskehandel og narkotikavirksomhet.
>
> Etter Politidirektoratets oppfatning framstår § 4-4 som uklar når Etterretningstjenestens oppgaver etter lovutkastet § 3-1 i det alt vesentlige oppgir polisiære oppgaver, samt at forbudet i et samfunnssikkerhetsperspektiv ikke ivaretar norske interesser. Dette vil særlig ha betydning for lovforslaget om forbud mot utlevering av overskuddsinformasjon.»

Etter PODs oppfatning gir lovutkastet § 4-4 ikke en dekkende fremstilling av politiets oppdrag:

> «Lovforslaget vektlegger politiets kriminalitetsforebyggende og kriminalitetsbekjempende oppgaver, dette gjelder ikke minst lovforslagets § 4-4. Etter Politidirektoratets oppfatning er dette ikke en dekkende fremstilling av politiets oppdrag. Paragrafen bruker for øvrig begrepet «bekjempe», som ikke er i samsvar med etablert terminologi for politiet. Det er Forsvaret som i en væpnet konflikt kan bekjempe en fiende hvor krigens rett oppstiller andre rettslige regler for forholdsmessighet og nødvendighet når makt anvendes.»

Norges institusjon for menneskerettigheter (NIM) har også kommentert forslaget. Innspillet er formulert innenfor rammen av NIMs kommentarer til anvendelsesområdet for tilrettelagt innhenting. *NIM* siterer utkast til § 4-4 andre ledd første punktum og uttaler:

> «Det er helt uklart hva som menes med denne bestemmelsen isolert sett. Hvis meningen er å klargjøre at forbudet ikke er til hinder for at E-tjenesten i medhold av bestemmelsene i forslaget kapittel 10 deler informasjon som opprinne-

lig ble innhentet for etterretningsformål, bør det fremkomme klarere.»

Når det gjelder den menneskerettslige vurderingen av et system som tilrettelagt innhenting mener imidlertid NIM at en slik bestemmelse som innsnevrer systemets virkeområde, vil være et viktig moment:

> «For så vidt gjelder virkeområde vil det trolig være et viktig moment i vurderingen etter EMK artikkel 8 at bulkovervåkingssystemet i utgangspunktet er avgrenset til utenlandsetterretningsformål, og at regelverket er innrettet for å hindre formålsutglidning i praksis, f.eks. i form av at systemet helt eller delvis også brukes for å innhente informasjon til politiformål. Slik sett er NIM positive til forbudene i §§ 4-4 og 10-3.»

8.11.4 Departementets vurdering

Departementet er enig med høringsinstansene som har påpekt at forslaget i høringsnotatet rettslig sett er overflødig ved siden av den positive angivelsen av Etterretningstjenestens oppgaver i lovforslaget kapittel 3. På den andre siden kan bestemmelsen ha en pedagogisk funksjon gjennom å synliggjøre i form av en negativ avgrensning hva som *ikke* er formålet til Etterretningstjenesten. Som påpekt av *NIM*, kan formålsavgrensningen være et viktig moment i vurderingen etter EMK artikkel 8.

På denne bakgrunn viderefører departementet forslaget, men med noen justeringer som følge av høringen. I lys av høringsuttalelsene til *Politidirektoratet* og *Politiets sikkerhetstjeneste* foreslås det uttrykkelig lovfestet at bestemmelsen ikke er til hinder for utveksling av informasjon etter lovforslaget kapittel 10. Det følger av dette at bestemmelsen verken er til hinder for å motta informasjon fra politiet eller utlevere informasjon til politiet, forutsatt at reglene etter lovforslaget kapittel 10 er oppfylt. Det foreslås også uttrykkelig lovfestet at bestemmelsen ikke er til hinder for bistand til politiet i medhold av politiloven § 27 a. Departementet understreker at det gjelder egne regler for informasjon som stammer fra tilrettelagt innhenting. I lovforslaget § 7-13 oppstilles det et forbud mot å dele overskuddsinformasjon som stammer fra tilrettelagt innhenting. Det fastsettes også i § 10-7 at tilrettelagt innhenting ikke kan brukes som bistand til politiet.

8.12 Forbud mot industrispionasje

8.12.1 Gjeldende rett

Etterretningstjenesteloven inneholder ikke et eksplisitt forbud mot at tjenesten innhenter informasjon med sikte på å gi norske virksomheter eller sektorer konkurransemessige fortrinn. Det er imidlertid antatt at et slikt forbud kan utledes av en tolkning av loven § 3 om tjenestens oppgaver og Instruks om Etterretningstjenesten § 11 om hvilken informasjon som kan tilflyte private personer og virksomheter. Det må trekkes en grense mellom industrispionasje (med formål å gi et konkurransemessig fortrinn) og økonomisk etterretningsvirksomhet (med formål å besvare norske myndigheters prioriterte informasjonsbehov innenfor økonomiske og finansielle områder).

8.12.2 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 8.9 å lovfeste et forbud mot industrispionasje i lovutkastet § 4-3. Bestemmelsen angir at Etterretningstjenesten ikke skal innhente eller medvirke til å innhente, bearbeide eller utlevere informasjon med formål å gi selskaper eller andre kommersielle virksomheter eller sektorer konkurransemessige fortrinn.

8.12.3 Høringsinstansenes syn

Kripos uttaler at en egen bestemmelse om industrispionasje er overflødig ved siden av angivelsen og begrensningen av Etterretningstjenestens oppgaver i kapittel 3:

> «Å se behov for positivt å forby tjenesten å tjene et åpenbart usaklig, antagelig ulovlig, formål underbygger på ingen måte troverdighet for at man vil innrette seg etter de formålsbegrensninger som ligger i loven ellers.»

International Business Machines AS (IBM) uttaler at selv om § 4-3 representerer en stadfesting av praksis, er det et viktig signal i den globale virkeligheten vi ser nå.

8.12.4 Departementets vurdering

Departementet bemerker at det i de senere år har vært en gryende sedvanerettsutvikling i retning av et folkerettslig forbud mot 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 slik spionasje mellom statene. Dessuten avga Storbritannia og Kina i 2015 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 ICT [Information and Communications Technology] 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.»

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 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, selv om gjeldende lov § 3 ikke direkte forbyr slik innhenting. Det er departementets syn at loven bør reflektere denne utviklingen. Forbudet vil ikke innskrenke eller hindre tjenestens mulighet til å innhente økonomiske og finansielle opplysninger som kan tjene til å løse oppgavene som fremgår av lovforslaget kapittel 3.

Departementet deler ikke Kripos' bekymring om at et forbud vil kunne svekke Etterretningstjenestens troverdighet. Tvert om gir bestemmelsen et viktig signal om hvor grensene for lovlig og ulovlig etterretningsvirksomhet skal trekkes, og bidrar til å støtte opp om en viktig internasjonal normutvikling på dette området.

9 Grunnvilkår for innhenting og utlevering av informasjon

9.1 Gjeldende rett

Etterretningstjenesteloven § 3 fastslår at tjenesten skal innhente, bearbeide og analysere informasjon som angår norske interesser sett i forhold til fremmede stater, organisasjoner eller individer. Det følger av dette at informasjonsinnhentingen er *formålsbegrenset til utenlandske forhold*. For øvrig oppstiller loven ingen grunnvilkår som må være oppfylt for at tjenesten skal kunne innhente informasjon.

Innhenting som utgjør et inngrep overfor den enkelte, for eksempel i retten til respekt for privatlivet etter Grunnloven § 102 og Den europeiske menneskerettskonvensjon (EMK) artikkel 8, må være forholdsmessig. Dette innebærer at innhentingen ikke kan finne sted dersom det etter en samlet avveining av alle relevante hensyn vil være et uforholdsmessig inngrep. Det skal blant annet tas hensyn til inngrepets styrke og sakens betydning.

9.2 Fremmed rett

9.2.1 Sverige

Lagen (2000:130) om försvarsunderrättelseverksamhet 1 § fastsetter at etterretningsvirksomheten bare omfatter utenlandske forhold. Loven oppstiller for øvrig ingen grunnvilkår for innhenting av informasjon.

Etter *lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet* 5 § kan det bare gis tillatelse til signalspaning hvis formålet med innhentingen ikke kan oppnås på en mindre inngripende måte. Oppdraget må dessuten antas å gi informasjon hvis verdi er klart større enn inngrepet som innhentingen kan innebære.

9.2.2 Danmark

Det følger av *lov om Forsvarets Efterretningstjeneste (FE)* § 1 at den etterretningsmessige virksomheten til FE er rettet mot forhold i utlandet. Dersom det innhentes opplysninger på kontraterrorfeltet om en person i utlandet som er hjemmehørende i Danmark, følger det av § 3 a stk. 2 at inngrepet i kommunikasjonsvernet ikke må være uforholdsmessig. For øvrig oppstiller loven ingen grunnvilkår for innhenting av informasjon.

9.2.3 Finland

Etter *lag om militär underrättelseverksamhet (590/2019)* 3 og 4 §§ retter den militære etterretningsvirksomheten seg mot militær virksomhet mot Finland og annen virksomhet som alvorlig truer det finske forsvaret eller samfunnets vitale funksjoner. Prinsippet om formålsbegrensning i 8 § fastslår at myndigheten bare får brukes for de formål som angis i loven. Et forholdsmessighetsprinsipp framgår av 6 §: De tiltak som treffes, skal kunne forsvares ut fra hvor viktige opplysningene er, hvor mye oppdraget haster, målet for innhentingen, inngrepet i rettighetene som tiltaket medfører og forholdene ellers.

Forholdsmessighetsprinsippet i 6 § henger nært sammen med prinsippet om minste inngrep i 7 §. Bestemmelsen fastslår at innhentingen ikke skal gripe inn i noens rettigheter i større utstrekning enn det som er nødvendig, og ingen skal utsettes for større skade eller uleilighet enn det som er nødvendig. Inngrep i vernet av fortrolig kommunikasjon skal være så målrettet og begrenset som mulig.

9.3 Grunnvilkår for målsøking og målrettet innhenting

9.3.1 Forslaget i høringsnotatet

I høringsnotatet punkt 9.5 foreslås det å lovfeste grunnvilkår for når Etterretningstjenesten kan søke etter nye etterretningsmål (målsøking) og innhente informasjon om identifiserte etterretningsmål (målrettet innhenting).

Det foreslås at informasjonsinnhenting gjennom målsøking og målrettet innhenting bare kan gjennomføres dersom det foreligger *grunn til å undersøke* om innhenting kan bidra til å frembringe informasjon som er relevant for etterretningsformål. Dette innebærer at det ikke vilkårlig

kan innhentes informasjon. Innhentingen må skje på bakgrunn av enkelte ledetråder, for eksempel erfaringsbaserte hypoteser eller andre holdepunkter. For målrettet innhenting må det foreligge *konkrete holdepunkter*.

Grunnvilkåret angir både at det må foreligge en legitim grunn for søket eller innhentingen, og at det må være en viss sannsynlighet for at søket eller innhentingen vil frembringe etterretningsrelevant informasjon. Fordi etterretningsvirksomhet dreier seg om å hente inn og analysere informasjon over tid, må terskelen ligge forholdsvis lavt. Terskelen skal motvirke vilkårlighet, og innebærer at tjenesten må kunne underbygge hvorfor den henter inn informasjonen.

9.3.2 Høringsinstansenes syn

Borgarting lagmannsrett uttaler i forbindelse med domstolsprøving av tilrettelagt innhenting:

> «Grunnvilkårene i kap. 5 vil være sentrale ved domstolskontrollen. Grunnvilkåret både i § 5-1 (målsøking) og § 5-2 (målrettet innhenting) er «grunn til å undersøke». Dette er en lav terskel, og det er presisert i høringsnotatet side 156 at denne standarden er en «isolert etterretningsterskel» som ikke har eller skal ha noen sammenheng med tilsvarende begreper i politiloven og straffeprosessloven. I politiloven og straffeprosessloven dreier det seg om sannsynlighet for at noen har begått eller vil begå straffbare handlinger, 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. Dette vil være uvant for domstolene.»

Datatilsynet uttaler at grunnvilkårene for innhenting i §§ 5-1 og 5-2 er så vidt formulerte at det er vanskelig å tenke seg en reell prøving av om de er oppfylt. Grunnvilkåret for målsøking, jf. § 5-1, er at det foreligger grunn til å undersøke om innhenting kan bidra til å frembringe informasjon som er relevant for etterretningsformål. Etterretningstjenesten kan altså gjøre søk dersom det i det hele tatt er en mulighet for at selve innhentingen kan bidra til informasjon som kan være relevant for etterretningsformål. Med så vide oppgaver, og så vide hjemler for søk, vil det være vanskelig å si hva som er relevant informasjon eller ikke.

Dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors mener at ordlyden og forarbeidene ikke gir mange holdepunkter for å forstå hva som gjør at det er «grunn til å undersøke». De mener at vilkåret bør operasjonaliseres på en måte som blir forståelig for dommerne og andre som skal kontrollere. For eksempel kan det i ordlyden eller forarbeidene stå noe om at det må foreligge konkrete holdepunkter for at man mistenker at det er eller bygges opp kapasitet til eller intensjon om terror. For de øvrige formålene må det trolig angis andre vurderingstemaer. Det antas at disse kan være svært ulike ut fra hvilket formål man innhenter til.

Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget) ser positivt på lovfesting av grunnvilkår for målsøking og målrettet innhenting, men ser noen utfordringer med forslaget i høringsnotatet:

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

Utvalget understreker imidlertid at kravet til dokumentasjon vil gjøre at utvalget kan kontrollere at grunnvilkårene er oppfylt og at metodebruken er innrettet på minst mulig inngripende måte.

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

Norges institusjon for menneskerettigheter (NIM) fremholder at kriteriet «grunn til å undersøke» synes å gi tjenesten et utstrakt skjønn som det er vanskelig å overprøve. NIM mener at vilkåret bør operasjonaliseres nærmere, slik at det blir tydeligere hvor terskelen ligger. Dette vil også bidra til at saken opplyses bedre ved domstolsprøvingen i saker om tilrettelagt innhenting. NIM har vanskelig for å se hvordan domstolen ellers på en hensiktsmessig måte skal kunne vurdere forbudet mot diskriminering og det generelle spørsmålet om forholdsmessighet, som er helt sentralt menneskerettslig.

Norsk Presseforbund mener i tilknytning til tilrettelagt innhenting at grunnvilkårene er vage og rundt formulert, og gir en altfor lav terskel for et alvorlig inngrep i ytringsfriheten og personvernet. *NRK* gir uttrykk for lignende synspunkter.

Politiets sikkerhetstjeneste påpeker at terskelen som følger av §§ 5-1 og 5-2 er «lav», men gir ikke direkte uttrykk for innvendinger mot bestemmelsene.

9.3.3 Departementets vurdering

Departementet viderefører forslaget i høringsnotatet med enkelte lovtekniske justeringer. Grunnvilkårene er ment å motvirke vilkårlighet gjennom å oppstille en inngangsterskel for når Etterretningstjenesten kan innhente informasjon. Som departementet kommer tilbake til, foreslås det også andre vilkår som begrenser hvilken informasjon som kan innhentes og på hvilken måte. Grunnvilkårene må ses i sammenheng med lovens øvrige vilkår for innhenting av informasjon.

Borgarting lagmannsrett, Datatilsynet, *dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors, Kripos* og *NIM* påpeker i sine høringsuttalelser at det legges til grunn en lav terskel for innhenting, og at det i relasjon til tilrettelagt innhenting kan være vanskelig for domstolen å overprøve denne. *Norsk Presseforbund* og *NRK* gir uttrykk for lignende synspunkter. *Dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors* og *NIM* mener at vilkåret «grunn til å undersøke» bør operasjonaliseres, slik at det blir tydeligere hvor terskelen ligger.

Norske myndigheter har behov for informasjon om utenlandske trusler og andre forhold av betydning for nasjonale sikkerhetsinteresser. Etterretningstjenesten innhenter informasjon for å redusere usikkerhet hos norske beslutningstakere. Vilkåret «grunn til å undersøke» må vurderes i lys av at det ikke er mulig å avdekke ukjente trusler knyttet til fremmede stater, organisasjoner og personer uten å innhente, sammenstille og analysere informasjon over lang tid. For å kunne finne de ukjente aktørene og den relevante informasjonen, må tjenesten gå bredt ut. Det er bare gjennom å sammenstille informasjon som er samlet inn fra forskjellige kilder og ved bruk av ulike metoder, at tjenesten kan få det helhetlige bildet som er nødvendig for å utarbeide gode analyser og vurderinger. I motsetning til politiet og påtalemyndigheten, som opererer med grader av sannsynlighet for at noen har foretatt eller forbereder en straffbar handling, forholder Etterretningstjenesten seg til om innhentingen vil besvare norske myndigheters informasjonsbehov. Det er uten betydning om noen har gjort eller kan komme til å gjøre noe straffbart, og tjenesten har ingen oppgaver knyttet til straffeforfølgning. På grunn av disse særtrekkene mener departementet at terskelen for når tjenesten kan innhente informasjon, må være lav. Dette er avgjørende for at tjenesten skal kunne løse oppgavene som følger av lovforslaget kapittel 3.

Departementet mener på denne bakgrunn at det ikke bør oppstilles strengere krav til grunnvilkår enn det som følger av forslaget i høringsnotatet. Departementet tilføyer at det i den tilsvarende lovgivningen til nærstående land normalt ikke oppstilles noen terskel ved siden av formålsbegrensningen og forholdsmessighetsprinsippet, og at lovforslaget på dette punktet derfor kan hevdes å innebære en strengere regulering enn det som er vanlig.

Departementet understreker dessuten at Etterretningstjenesten på ingen måte står fritt til å innhente informasjon bare grunnvilkårene er oppfylt. Innhentingen må også være i tråd med andre lovbestemte vilkår. Departementet peker særlig på formålsbegrensningen som følger av lovforslaget kapittel 3, kravet til forholdsmessighet etter lovforslaget § 5-4, forbudet mot å bruke inngripende metoder overfor personer i Norge etter lovforslaget § 4-1 og diskrimineringsforbudet etter lovforslaget § 9-4. Det understrekes også at innhenting forutsetter en beslutning fra sjefen for tjenesten som må oppfylle nærmere bestemte krav, jf. lovforslaget §§ 6-12 og 6-13. Tilrettelagt innhenting krever rettens forhåndsgodkjennelse etter reglene i lovforslaget kapittel 8. Tjenestens virksomhet er dessuten oppdragsstyrt av overordnet myndighet etter reglene i lovforslaget kapittel 2.

NIM og *dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors* etterlyser i sine høringsuttalelser en operasjonalisering av grunnvilkårene. Dommerne foreslår at det for eksempel kan oppstilles krav til mistanke om kapasitet til

eller intensjon om terror, mens det for andre områder kan angis andre vurderingstemaer. Departementet anser ikke en slik løsning som hensiktsmessig, da de bestemt angitte vurderingstemaene fort vil kunne rekke enten for vidt eller for snevert i et skiftende trusselbilde. Det understrekes dessuten at Etterretningstjenesten også innhenter informasjon som ikke gjelder konkrete trusler, for eksempel om andre staters langsiktige styrking av militære kapasiteter i våre nærområder.

EOS-utvalget fremhever at den flytende overgangen mellom målsøking og målrettet innhenting kan gjøre det utfordrende å kontrollere grunnvilkårene. Departementet er enig med utvalget i at det kan være en flytende overgang, da det i enkelte tilfeller vil bli innhentet informasjon om et identifisert etterretningsmål (målrettet innhenting) samtidig som det vil søkes etter nye etterretningsmål i kretsen rundt målet (målsøking). Av hensyn til utvalgets kontrollmuligheter forutsetter departementet at Etterretningstjenesten utvikler rutiner og systemer som sikrer at det fremgår tydelig hvorvidt innhenting gjennomføres som ledd i målsøking eller som målrettet innhenting. Der hvor det kan være vanskelig å kategorisere innhentingen, bør dette også fremgå tydelig.

Datatilsynet stiller spørsmål ved om domstolskontrollen av tilrettelagt innhenting etter lovforslaget kapittel 7 og 8 vil være reell. Spørsmålet drøftes i punkt 11.9.

9.4 Grunnvilkår for innhenting av og søk i rådata i bulk

9.4.1 Forslaget i høringsnotatet

Det foreslås i høringsnotatet å oppstille et eget grunnvilkår for innhenting av og søk i rådata i bulk. Bulk foreslås definert som «informasjonssamlinger og datasett hvorav en vesentlig andel av informasjonen antas å være irrelevant for etterretningsformål». I punkt 9.5.6.3 i høringsnotatet redegjøres det for de teknologiske forutsetningene som gjør at det er nødvendig å innhente data i bulk. Det fremheves at det som oftest er teknisk umulig å gjøre utvalg, analyse og filtrering mens dataene er i transitt, slik at de må lastes ned og lagres før man kan finne de informasjonsbitene som er av interesse.

For å hindre at informasjon samles inn i bulk på vilkårlig grunnlag, foreslås det lovfestet at slik innhenting bare kan skje dersom det er nødvendig for å få et relevant og tilstrekkelig informasjonsgrunnlag. Videre understrekes det at søk i rådata som er innhentet i bulk må tilfredsstille grunnvilkårene for målsøking eller målrettet innhenting, og at søkene skal logges for kontrollformål.

9.4.2 Høringsinstansenes syn

Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget) er positive til at det foreslås lovfesting av grunnvilkår for innhenting av og søk i rådata i bulk. Ingen andre høringsinstanser har merknader til forslaget. Noen har imidlertid merknader knyttet til hvorvidt Etterretningstjenesten skal ha anledning til å innhente informasjon i bulk i det hele tatt. Disse høringsuttalelsene knytter seg primært til forslaget om tilrettelagt innhenting av grenseoverskridende elektroniske kommunikasjon etter lovforslaget kapittel 7 og 8, og behandles i kapittel 11.

9.4.3 Departementets vurdering

Det ble i høringsnotatet vurdert at det bør oppstilles et grunnvilkår for innhenting av og søk i rådata i bulk. Departementet fastholder vurderingen, og viderefører forslaget i høringsnotatet med noen mindre lovtekniske justeringer.

Behovet for et tilstrekkelig datagrunnlag til å søke etter nye etterretningsmål gjør det nødvendig å innhente rådata i bulk. At Etterretningstjenesten er avhengig av å kunne innhente og lagre rådata i bulk for å løse oppgavene i lovforslaget kapittel 3, ble også presisert i Lysne II-utvalgets rapport om digitalt grenseforsvar punkt 3.3.2 side 16. Det påpekes i den sammenheng at alternativene til bulkinnsamling er få. Manglende mulighet til å gjennomføre søk i og analyser av rådata samlet inn i bulk, vil kunne medføre at tjenesten må ta i bruk mer inngripende metoder for å løse oppgavene sine. Innhenting i bulk gir mulighet til å fokusere på den mest relevante informasjonen, og raskt utelukke informasjon som ikke er av interesse.

Grunnvilkåret for innhenting av rådata i bulk innebærer at Etterretningstjenesten må vurdere om det foreligger mindre inngripende alternativer som gir tilgang på et adekvat informasjonsgrunnlag.

Rådata er ubearbeidet eller automatisk bearbeidet informasjon hvor etterretningsverdien av informasjonen ikke er vurdert. Innhenting av rådata i bulk innebærer innhenting av informasjonssamlinger og datasett hvor en vesentlig andel av informasjon antas å være irrelevant for

etterretningsformål. Informasjonssamlingene og datasettene kan potensielt inneholde informasjon om personer som oppholder seg i Norge. Ved innhenting av metadata fra satellittkommunikasjon vil mer enn 99 % av informasjonen gjelde rent utenlandsk kommunikasjon, men det kan ikke utelukkes at en liten andel kan gjelde personer i Norge. Ved tilrettelagt innhenting etter lovforslaget kapittel 7 og 8 er situasjonen en annen, fordi store mengder metadata om norsk innenlandsk kommunikasjon av tekniske grunner vil bli hentet inn og lagret. Etter høringen foreslår departementet å lovfeste at søk i rådata med utgangspunkt i et søkebegrep (for eksempel et telefonnummer eller et brukernavn på en kommunikasjonstjeneste) tilknyttet en person i Norge, ikke kan gjennomføres med mindre det er strengt nødvendig for å ivareta en oppgave som nevnt i lovforslaget § 3-1 (utenlandske trusler). Bestemmelsen foreslås inntatt i lovforslaget § 5-3 tredje ledd. Det foreslås presisert i bestemmelsen at begrensningen ikke skal gjelde dersom personen omfattes av unntaket for fremmed statsaktivitet i lovforslaget § 4-2. Forslaget drøftes nærmere i punkt 8.9.

Departementet understreker at lagrede rådata skal slettes når de ikke lenger er nødvendige for formålet med behandlingen, og senest etter 15 år, jf. lovforslaget § 9-8. Metadata som er lagret i bulk i samsvar med reglene i lovforslaget kapittel 7 (tilrettelagt innhenting), skal slettes senest etter 18 måneder, jf. § 7-7 tredje ledd.

9.5 Forholdsmessighet

9.5.1 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 9.5.3 å lovfeste et prinsipp om forholdsmessighet ved menneskerettslige inngrep overfor den enkelte. Prinsippet får betydning både for valg av innhentingsmetode og for hvordan innhentingen skal gjennomføres. Kravet til forholdsmessighet vil få betydning for om en bestemt metode kan benyttes i den aktuelle situasjonen, og for hvor lenge innhentingen kan pågå. For enkelte metoder foreslås det en høyere terskel (streng nødvendighet) for å synliggjøre at det legges til grunn en strengere forholdsmessighetsvurdering.

Vurderingen av om innhentingen vil være forholdsmessig må gjennomføres før den finner sted. Det må gjøres en ny forholdsmessighetsvurdering dersom forholdene som ligger til grunn for innhentingen endrer seg på en slik måte at det må anses påkrevd.

Det fremheves i høringsnotatet at også utlevering av informasjon vil utgjøre et inngrep overfor den enkelte, slik at kravet til forholdsmessighet også bør gjelde ved utlevering. Det understrekes at behandling etter innhenting også utgjør et inngrep, men at kravene til behandling av personopplysninger etter innhenting reguleres i et eget kapittel.

9.5.2 Høringsinstansenes syn

Borgarting lagmannsrett skriver i relasjon til domstolskontroll av tilrettelagt innhenting at kravet til forholdsmessighet i praksis vil bli en viktigere skranke enn terskelen «grunn til å undersøke». Lagmannsretten uttaler:

> «Domstolene [er] vant til å foreta forholdsmessighetsvurderinger. Forholdsmessighetskravet er nærmere omtalt i høringsnotatet punkt 9.5.3 på side152-154. Vilkåret innebærer at inngrepet må være nødvendig for å oppnå formålet, herunder at det er egnet og at formålet ikke kan oppnås med mindre inngripende tiltak. Forholdsmessighetsvurderingen vil være en avveining av på den ene side alvorligheten av inngrepet for den enkelte og på den annen side den samfunnsmessige betydning av å fremskaffe den aktuelle informasjonen (mao. en balansering av private og offentlige interesser). I lys av at søkene gjennomføres i en stor mengde rådata, hvor det meste er knyttet til personer og forhold som ikke er relevante for etterretningstjenestens oppgaveløsning, reiser Borgarting lagmannsrett spørsmål om ikke terskelen for når inngrepet blir uproporsjonalt er lagt for høyt i høringsnotatet. Det må her også ses hen til EMK artikkel 8 og EMDs praksis. Både Big Brother Watch vs. Storbritannia og Centrum for Rättvisa vs. Sverige, som omtales i høringsnotatet, er for øvrig nå henvist til behandling i storkammer i EMD. Etter utkastet § 7-8 første ledd kan personselektorsøk inkludere to ledd ut i personenes kommunikasjonskjede. Gitt det store antall personer som da vil inngå i søket, er lagmannsrettens umiddelbare syn at dette lett kan bli vurdert som uforholdsmessig.»

Dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors uttaler at det kan synes som om forarbeidene begrenser domstolens mulighet til å kunne foreta en selvstendig og reell vurdering av forholdsmessigheten i forhold til hva ordlyden isolert sett tilsier. De uttaler videre at lovgiver bør

konkretisere hva som anses som forholdsmessig og uforholdsmessig. Etter dommernes syn er det særlig betenkelig at det skal være anledning til å innhente metadata inntil to ledd ut fra alle treff i de søkene som godkjennes.

Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget) uttaler at det er positivt at det lovfestes et krav til forholdsmessighet, og at kravet til dokumentasjon gjør at dette er noe som kan kontrolleres. Utvalget uttaler videre at kravet «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». Utvalget påpeker at det vil være en utpreget etterretningsfaglig vurdering å ta stilling til «om informasjon kan innhentes i det hele tatt» og «på hvilken måte informasjon kan innhentes».

9.5.3 Departementets vurdering

Departementet viderefører forslaget i høringsnotatet om å lovfeste forholdsmessighetsprinsippet. Krav til forholdsmessighet ved inngrep overfor den enkelte følger allerede av menneskerettighetene etter Grunnloven og internasjonale konvensjoner som gjelder som norsk lov etter menneskerettsloven, men pedagogiske grunner tilsier at prinsippet synliggjøres direkte i loven.

Kravet til forholdsmessighet utgjør en sentral skranke for Etterretningstjenestens bruk av inngripende metoder. Tjenesten må foreta en konkret vurdering av forholdsmessighet før det innhentes informasjon som kan utgjøre et inngrep i rettighetene til den enkelte. Kravet innebærer at tiltaket må være nødvendig for å oppnå formålet, herunder at det er egnet og at formålet ikke kan oppnås med mindre inngripende tiltak. Det må også foretas en samlet avveining av de beskyttede individuelle interessene og det legitime samfunnsbehovet for informasjonsinnhenting.

Forholdsmessighetsvurderingen må foretas i lys av den konkrete saken. Alle relevante hensyn kan tas i betraktning. Utgangspunktet for vurderingen vil på den ene siden være *styrken av inngrepet i de beskyttede individuelle interessene* som innhentingen eller utleveringen innebærer, og på den andre siden *sakens betydning*. Styrken av inngrepet i de beskyttede individuelle interessene vil kunne variere avhengig av hvilken metode det er tale om å benytte. Jo mer alvorlig og tidskritisk saken er, jo større inngrep vil være tillatt. Motsatt vil det stilles større krav til fremgangsmåten hvis tjenesten har god tid til rådighet.

Dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors uttaler at det kan synes som om beskrivelsen av forholdsmessighetsvurderingen i høringsnotatet begrenser domstolenes mulighet til å foreta en selvstendig og reell vurdering av forholdsmessigheten i forhold til hva ordlyden isolert sett tilsier. De uttaler videre at lovgiver bør konkretisere hva som er forholdsmessig og uforholdsmessig. Departementet understreker at retten skal foreta en selvstendig og reell forholdsmessighetsvurdering i saker om forhåndsgodkjennelse av tilrettelagt innhenting. Vurderingen er i sin natur åpen og avhengig av forholdene i saken, og derfor er det på forhånd ikke mulig fullt ut å konkretisere hva som er eller ikke er forholdsmessig, slik dommerne etterlyser. En slik konkretisering vil fort kunne rekke enten for vidt eller for snevert, og medfører en risiko for at rettsanvenderne i for stor grad konsentrerer seg om de spesifiserte omstendighetene, som vanskelig vil kunne rekke over alle de relevante hensyn som vil kunne gjøre seg gjeldende i konkrete saker. Det vises imidlertid til merknadene til lovforslaget § 5-4 for en beskrivelse av hensyn som ofte vil kunne være aktuelle.

Borgarting lagmannsrett og *dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors* stiller i relasjon til tilrettelagt innhenting spørsmål ved forholdsmessigheten av at det som hovedregel skal være anledning til å søke i metadata inntil to ledd ut fra alle treff i de søkene som godkjennes av domstolen. Departementet har etter høringen kommet til at forslaget ikke videreføres. Det vises til punkt 11.8.5.3 for en nærmere omtale.

10 Metoder for innhenting av informasjon som kan medføre inngrep overfor den enkelte

10.1 Gjeldende rett

Etterretningstjenesteloven § 3 fastslår at tjenesten skal «innhente» nærmere bestemt informasjon om utenlandske forhold. Bestemmelsen omtaler ikke hvilke metoder eller hvilken teknologi som kan brukes for å innhente informasjonen. Loven er med andre ord teknologi- og metodenøytral. Det følger av dette at tjenesten, innenfor rammen av overordnede rettsregler, herunder spesielt menneskerettighetene slik de er vernet blant annet av Grunnloven og Den europeiske menneskerettskonvensjon (EMK), kan bruke enhver metode for å innhente informasjon om relevante utenlandske forhold. I forarbeidene til loven vises det til at tjenesten bruker tekniske og andre metoder for å innhente informasjon (Ot.prp. nr. 50 (1996–97) punkt 6.4 side 8). Det vises dessuten til at tjenesten må ha nødvendig innsamlingskapasitet for prioriterte behov (punkt 8 side 10).

10.2 Andre lands rett

10.2.1 Sverige

Det følger av *lagen (2000:130) om försvarsunderrättelseverksamhet* 2 § at den eller de myndigheter som driver forsvarsetterretningsvirksomhet, kan innhente informasjon ved hjelp av teknisk og personbasert innhenting.

Visse bestemmelser om teknisk innhenting er gitt i *lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet*, som gir grunnlag for innhenting av elektronisk informasjon som krysser den svenske grensen. Se nærmere om dette i punkt 11.3.1.

10.2.2 Danmark

I medhold av *lov om Forsvarets Efterretningstjeneste (FE)* § 3 kan FE innsamle og innhente opplysninger som kan ha betydning for tjenestens etterretningsmessige virksomhet. Loven er utformet på en teknologi- og metodenøytral måte. Ved innhenting på kontraterrorområdet som medfører et inngrep i kommunikasjonsvernet til en person i utlandet som er hjemmehørende i Danmark, skal innhentingen godkjennes av en domstol.

10.2.3 Finland

Lagen om militär underrättelseverksamhet (590/2019) 4 kap. regulerer hvilke metoder de militære etterretningsmyndighetene kan bruke for å innhente informasjon. Loven regulerer systematisk observasjon, fordekt innhenting av informasjon og teknisk observasjon (22 til 33 §§), innhenting i telenett (34 til 42 §§), dekkoperasjoner og bevisprovokasjon gjennom kjøp (43 til 50 §§), bruk av informasjonskilder (51 til 53 §§), plasspesifikk innhenting og kopiering (54 til 59 §§), radiosignalspaning, innhenting som gjelder utenlandske datasystemer og innhenting i utlandet (60 til 64 §§) og innhenting som gjelder datatrafikk (65 til 74 §§).

Myndighet til å fatte beslutning om bruk av en metode er dels lagt til tjenestepersoner i de militære etterretningsmyndighetene, og dels til tingretten i Helsingfors på begjæring fra en slik tjenesteperson. Etter 64 § fatter hovedstabens etterretningssjef beslutning om militær etterretningsinnhenting og anvendelse av metoder for etterretningsinnhenting som skjer utenfor Finland.

10.3 Lovregulering av innhentingsmetoder

10.3.1 Høringsnotatet

Det tas i høringsnotatet utgangspunkt i at dagens etterretningstjenestelov gir hjemmel for bruk av inngripende metoder. Bruk av slike metoder er nærmere regulert i internt regelverk. Det har imidlertid vært reist spørsmål om tjenestens bruk av inngripende metoder bør få klarere grunnlag i lov.

I høringsnotatet vises det til at professor Erling Johannes Husabø, i en utredning vedlagt rapporten fra Evalueringsutvalget for EOS-utvalget (Dokument 16 (2015–2016)), uttaler at det er tvilsomt om dagens hjemmelsgrunnlag tilfredsstiller de kravene som nå stilles etter Den europeiske menneskerettskonvensjon (EMK). Det vises så til at EOS-utvalget i en særskilt melding til Stortinget 17. juni 2016 uttaler at det kan være grunn til å utrede nærmere om en lov som ikke regulerer metoder for innhenting av opplysninger om individer, tilfredsstiller lovskravet som er nedfelt i EMK (Dokument 7:2 (2015–2016) side 15). Det vises deretter til at Stortingets kontroll- og konstitusjonskomité i sin innstilling om den særskilte meldingen uttaler (Innst. 164 S (2016–2017) side 9):

> «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 bakgrunn av innstillingen besluttet Stortinget 21. februar 2017 å be regjeringen om å legge frem forslag til revidert lov om Etterretningstjenesten (vedtak 466).

Det heter i høringsnotatet at de refererte vurderingene tilsier en lovregulering av Etterretningstjenestens metoder. Lovskravet 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. Det må samtidig tas hensyn til behovet for å verne konkrete opplysninger om tjenestens kilder, metoder og kapasiteter.

10.3.2 Høringsinstansenes syn

Abelia mener at den økte graden av lovregulering av Etterretningstjenestens virksomhet bidrar til mer åpenhet rundt tjenestens formål, rammer og samfunnsoppdrag, og gir økt demokratisk styring og kontroll av virksomheten.

Advokatforeningen mener at rammene for metodebruk hører hjemme i formell lov. De grunnleggende hensyn som bærer legalitetsprinsippet og lovskravet i EMK artikkel 8, særlig tilgjengelighet og demokratisk kontroll, tilsier at hovedprinsippene om metodebruk plasseres i loven. Advokatforeningen støtter dette initiativet fra departementets side, men har merknader knyttet til enkelte av bestemmelsene.

Amnesty International bemerker at det er meget positivt at regjeringen har tatt initiativ til en ny lov som regulerer Etterretningstjenestens virksomhet. Amnesty har merket seg at tjenesten selv har etterlyst oppdaterte og tydeligere lovbestemmelser for å sikre at deres aktiviteter er i tråd med menneskerettighetene og lovgiverens ønsker. At de hemmelige tjenestene selv etterstreber størst mulig rettslig og demokratisk forankring, i stedet for å prøve å skape og benytte seg av smutthull, er etter Amnestys syn betryggende i en tid der et økende antall stater bruker sikkerhetsargumentet som påskudd for å undergrave og begrense menneskerettighetene.

International Business Machines AS (IBM) støtter den teknologinøytrale tilnærmingen i lovutkastet kapittel 6. IBM viser til at det er avgjørende for tjenestens effektivitet at den har adgang til kontinuerlige oppgraderinger, oppdatert metodebruk og de mest avanserte tekniske løsninger.

Politiets sikkerhetstjeneste (PST) er som et utgangspunkt positive til at de mest inngripende metodene som Etterretningstjenesten kan benytte, lovfestes. PST er imidlertid uenige i forslaget om å lovfeste innhenting gjennom åpne kilder (§ 6-2) og systematisk observasjon (§ 6-4), og uttrykker bekymring for at uttalelser og synspunkter i forbindelse med lovarbeidet kan få en smitteeffekt til spørsmålet om lovfesting av per nå ulovfestede politimetoder. PST savner en nærmere drøftelse av hvilken grad av målrettethet og intensitet som skal til før slik innhenting anses som et inngrep overfor den enkelte.

Riksadvokaten uttaler:

> «Kapitlet inneholder ulike bestemmelser om tekniske metoder for innhenting av informasjon som innebærer inngrep overfor personer eller virksomheter. En finner igjen grunn til å understreke at utgangspunktet er at metodebruk rettet mot fysiske eller juridiske personer i Norge er en politioppgave. Behovet for hjemler for Etterretningstjenesten til metodebruk mot fysiske og juridiske personer i Norge kan derfor diskuteres. I den grad slike aktiviteter skjer på territorium undergitt annen stats jurisdiksjon, vil en lovfesting i Norge uansett ikke ha noen betydning.»

10.3.3 Departementets vurdering

Det vurderes i høringsnotatet at det er grunn til å lovregulere hvilke inngripende metoder Etterretningstjenesten kan ta i bruk for å innhente informasjon, blant annet under henvisning til at Stortingets kontroll- og konstitusjonskomité i Innst. 164 S (2016–2017) side 9 tar til orde for å lovregulere tjenestens virkemidler. Departementet fastholder denne vurderingen, som i hovedsak har fått støtte fra de høringsinstansene som har uttalt seg om spørsmålet.

Departementet understreker at hensikten med forslaget er å gi klarere rettslige rammer for Etterretningstjenestens bruk av inngripende metoder, av hensyn til det menneskerettslige lovskravet. Med unntak for forslaget om å åpne for tilrettelagt innhenting, som behandles særskilt i kapittel 11, har forslaget ikke til hensikt å gi tjenesten videre fullmakter enn det som følger av gjeldende rett. Den teknologinøytrale tilnærmingen som følger av gjeldende rett, videreføres. Som påpekt av *IBM*, er det avgjørende for tjenestens effektivitet at den har adgang til oppdatert metodebruk og de mest avanserte tekniske løsningene.

I sin høringsuttalelse reiser *riksadvokaten* spørsmål om behovet for en lovregulering av Etterretningstjenestens metoder. Departementet er enig med riksadvokaten i at det i Norge i fredstid normalt er politiet som har myndighet til å bruke inngripende metoder overfor personer i Norge. Etterretningstjenesten skal som den store hovedregel ikke bruke inngripende metoder overfor personer i Norge. Det er samtidig ikke tvilsomt at tjenesten i noen tilfeller kan bruke inngripende metoder for å innhente informasjon om personer i Norge, for eksempel om fremmed stats virksomhet. Dette er sikker rett som med enkelte endringer foreslås videreført i lovforslaget kapittel 4. Det vises til drøftelsen i kapittel 8. Av hensyn til det menneskerettslige lovskravet er det derfor ønskelig med en mer spesifikk lovregulering enn i dag av hvilke inngripende metoder som kan tas i bruk.

Riksadvokaten viser i sin høringsuttalelse også til at lovregulering er uten betydning for bruk av metoder utenfor Norge. Departementet deler synspunktet et stykke på vei, men ikke fullt ut, da bruk av inngripende metoder i utlandet kan aktualisere lovskravet hvis Norge etter omstendighetene regnes for å ha menneskerettslig jurisdiksjon utenfor eget territorium (ekstraterritoriell jurisdiksjon).

Politiets sikkerhetstjeneste (PST) gir i sin høringsuttalelse uttrykk for bekymring for at lovforslaget kan ha en smitteeffekt til spørsmålet om lovfesting av hittil ulovfestede politimetoder. På denne bakgrunn vil departementet presisere at det i dette lovarbeidet ikke tas stilling til spørsmålet om lovfesting av ulovfestede politimetoder.

Departementet understreker at Etterretningstjenesten innhenter informasjon om relevante utenlandske forhold ved hjelp av en rekke metoder som ikke utgjør et inngrep overfor den enkelte, for eksempel innen akustisk etterretning, radaretterretning og geografisk etterretning. Det er ikke nødvendig å lovfeste disse metodene av hensyn til lovskravet. Departementet ser det heller ikke av andre grunner som nødvendig eller hensiktsmessig å lovfeste disse metodene.

I tillegg til egen innhenting av informasjon ved bruk av metoder, mottar tjenesten også informasjon fra andre, for eksempel fra andre deler av forvaltningen og fra utenlandske samarbeidspartnere. Regler om slikt samarbeid følger av lovforslaget kapittel 10. Regler om behandling av informasjon som Etterretningstjenesten har kommet i besittelse av, følger av lovforslaget kapittel 9.

10.4 Generelle vilkår

10.4.1 Forslaget i høringsnotatet

I høringsnotatet foreslås det regler om generelle vilkår og saklig virkeområde i lovutkastet § 6-1. Det foreslås at Etterretningstjenesten for etterretningsformål kan benytte metoder etter bestemmelsene i lovutkastet kapittel 6 når grunnvilkårene etter kapittel 5 er oppfylt og innhentingen ikke strider mot øvrige bestemmelser i loven. Det foreslås at metodene kan brukes fordekt overfor personer som er gjenstand for eller på annen måte berøres av dem. Metodebruk skal avsluttes dersom det blir klart at vilkårene etter loven ikke lenger er til stede.

Det foreslås at bestemmelsene i kapittelet bare skal komme til anvendelse for innhenting som medfører inngrep overfor den enkelte. Det foreslås videre at bestemmelsene ikke skal komme til anvendelse for tilrettelagt innhenting av elektronisk kommunikasjon som transporteres over den norske grensen, som reguleres i lovutkastet kapittel 7 og 8.

10.4.2 Høringsinstansenes syn

Den internasjonale juristkommisjon – norsk avdeling (ICJ-Norge) uttaler at selv om forholdsmessigheten av metodebruken skal vurderes konkret i

hvert tilfelle, må lovgiver gi flere føringer enn forslaget legger opp til. Det vil for eksempel være større rom for inngripende metodebruk dersom formålet er å oppdage trusler mot Norge, enn det vil være for å innhente informasjon med det formål å fremme Etterretningstjenestens aksesser eller for å dele med utenlandske samarbeidspartnere. Et endelig lovforslag bør derfor drøfte i detalj om det er nødvendig å åpne opp for metodebruk for å understøtte alle lovens formål.

Kripos mener at regelen i lovutkastet § 6-1 første ledd siste punktum om at metodebruk skal avsluttes dersom det blir klart at vilkårene ikke lenger er oppfylt, er så selvsagt at den ikke bør lovfestes.

10.4.3 Departementets vurdering

Departementet viderefører forslaget i høringsnotatet, som i det vesentlige ikke har møtt negative merknader under høringen. Det foreslås enkelte lovtekniske justeringer.

I lovutkastet § 6-1 andre ledd ble det foreslått å lovfeste at bestemmelsene i kapittel 6 bare kommer til anvendelse for metoder som utgjør et inngrep overfor den enkelte. Regelen har ingen selvstendig betydning, og etter høringen har departementet derfor kommet til at den ikke bør videreføres.

I lovutkastet § 6-1 tredje ledd ble det foreslått å lovfeste at bestemmelsene i kapittel 6 ikke kommer til anvendelse for tilrettelagt innhenting av elektronisk kommunikasjon som transporteres over den norske grensen og som reguleres av kapitlene 7 og 8. Regelen foreslås flyttet til § 6-9 om midtpunktinnhenting. Dette innebærer ingen realitetsendring, men tydeliggjør at tilrettelagt innhenting er en form for midtpunktinnhenting, og derfor omfattes av forbudet i lovforslaget § 4-1 om å benytte innhentingsmetoder etter kapittel 6 overfor personer i Norge.

Kripos tar i sin høringsuttalelse til orde for at regelen i § 6-1 første ledd siste punktum er overflødig og ikke bør videreføres. Departementet har forståelse for synspunktet, men mener av pedagogiske hensyn at regelen bør fremgå uttrykkelig av loven. En slik regel inntas i lovforslaget § 6-1 tredje ledd.

ICJ-Norge reiser i sin høringsuttalelse spørsmål om det er nødvendig å åpne for bruk av metoder for å understøtte alle lovens formål. Høringsinstansen viser for eksempel til at det vil være større rom for inngripende metodebruk dersom formålet er å oppdage trusler mot Norge, enn hvis formålet er å fremme aksesser eller dele informasjon med utenlandske samarbeidspartnere. Departementet er enig i at utenlandske trusler mot Norge er i kjernen av hva som kan begrunne bruk av inngripende metoder, men det er ikke grunn til å begrense adgangen utelukkende til trusler. Det kan være glidende overganger mellom utenlandske sikkerhets-, forsvars- og utenrikspolitiske forhold og utenlandske trusler mot Norge, og for å kunne oppdage en utenlandsk trussel er det av betydning å kunne danne seg et bilde av den utenlandske sikkerhets-, forsvars- og utenrikspolitiske normalsituasjonen. Alle oppgavene beskrevet i kapittel 3 har til hensikt å ivareta nasjonale sikkerhetsinteresser. Departementet viser dessuten til at en slik begrensning ikke er vanlig i nærstående land, som Danmark, Sverige og Finland.

Som påpekt av ICJ-Norge, må det konkrete inngrepet tilfredsstille kravet til forholdsmessighet som følger av lovforslaget § 5-4. I vurderingen skal det blant annet tas hensyn til sakens betydning. Hvis saken gjelder en trussel som nevnt i lovforslaget § 3-1, vil det normalt kunne begrunne et sterkere inngrep enn dersom saken for eksempel gjelder forhold og utviklingstrekk i andre stater og regioner etter lovforslaget § 3-2. Departementet viser også til at det foreslås en strengere terskel for bruk av de mest inngripende metodene.

Departementet understreker at Etterretningstjenesten ikke står fritt med hensyn til hva tjenesten skal innhente informasjon om. Virksomheten er styrt av prioriteringene til overordnede myndigheter, se lovforslaget § 2-2 om oppdragsstyring. Det vises også til lovforslaget § 6-13, som fastsetter at det i beslutningen må angis hvilket oppdrag som innhentingen knytter seg til.

10.5 Åpne kilder

10.5.1 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 10.5.7 å lovfeste at Etterretningstjenesten kan innhente informasjon fra åpne kilder. Det vises til at åpne kilder er en svært relevant metode for å samle inn etterretningsinformasjon i dagens samfunn, enten på selvstendig grunnlag eller for å understøtte andre metoder. Et eksempel på dette er omfanget av informasjon som deles digitalt av personer i umiddelbar nærhet av viktige hendelser. I høringsnotatet er regler om åpne kilder inntatt i lovutkastet § 6-2.

10.5.2 Høringsinstansenes syn

Politiets sikkerhetstjeneste (PST) stiller seg kritiske til forslaget om å lovfeste innhenting fra åpne kilder. PST viser til risikoen for at forslaget vil ha en smitteeffekt til spørsmålet om å lovfeste politimetoder som per nå er ulovfestede. Ingen andre høringsinstanser har merknader til lovutkastet § 6-2, men *Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget)* har merknader knyttet til innhenting av informasjon fra åpne kilder som angår personer som oppholder seg i Norge, se punkt 8.5.

10.5.3 Departementets vurdering

Departementet viderefører forslaget i høringsnotatet med enkelte lovtekniske justeringer. Det er i utgangspunktet ikke behov for å lovfeste en adgang til å innhente informasjon fra åpne kilder, da dette normalt ikke vil være et inngrep overfor den enkelte. Slik innhenting om én og samme person kan etter omstendighetene likevel få et slikt omfang at det kan reises spørsmål om den utgjør et inngrep overfor vedkommende. For å unngå tvil knyttet til det menneskerettslige lovskravet foreslår departementet derfor å lovregulere metoden.

Departementet kan ikke se at standpunktet til *PST* med avgjørende vekt taler mot forslaget. Det understrekes at det i dette lovarbeidet ikke tas stilling til spørsmålet om lovfesting av ulovfestede politimetoder.

Bestemmelsen inntas i lovforslaget § 6-2. Det vises til merknadene til bestemmelsen for en nærmere beskrivelse av metoden. Departementet viderefører ikke forslaget om å lovfeste i § 6-2 en adgang til å bruke fiktive brukeridentiteter i, da regelen er overflødig ved siden av den generelle regelen i lovforslaget § 11-4 første ledd.

Merknadene fra *EOS-utvalget* om innhenting av informasjon fra åpne kilder som angår personer som oppholder seg i Norge, drøftes i punkt 8.5.

10.6 Menneskebasert innhenting

10.6.1 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 10.5.8 at Etterretningstjenesten kan gjennomføre menneskebasert innhenting, det vil si systematisk innhenting av informasjon gjennom samhandling mellom mennesker. Samhandlingen kan skje både i det fysiske og i det digitale rom. Forslaget kodifiserer og presiserer gjeldende rammer og praksis.

Det vises i høringsnotatet til at menneskebasert innhenting i kjernen innebærer å finne, rekruttere, trene og føre individer i den hensikt å innhente informasjon som ikke er offentlig tilgjengelig, eller tilrettelegge for slik informasjonsinnhenting. Metoden er den eldste etterretningsmetoden, og den forblir relevant i et høyteknologisk samfunn. Den kan ikke erstattes av andre metoder, uavhengig av teknologisk utvikling. For eksempel vil en aktørs intensjoner ikke nødvendigvis være registrert i en form som kan samles inn teknisk. Menneskebasert innhenting er videre godt egnet som et supplement til, eller til å bli supplert av, andre innhentingsmetoder.

Det heter i høringsnotatet at menneskebasert innhenting kan skje ved at kilden tar kontakt eller blir kontaktet, og ønsker å bistå ved å tilby informasjon. Menneskebasert innhenting kan imidlertid også inkludere infiltrasjon og provokasjon.

I høringsnotatet er regler om menneskebasert innhenting inntatt i lovutkastet § 6-3.

10.6.2 Høringsinstansenes syn

Kripos mener at det bør presiseres hva som menes med begrepene infiltrasjon og provokasjon i lovutkastet § 6-3 andre ledd. Kripos reiser spørsmål om begrepene skal forstås på samme måte som i politiet, hva det innebærer at slik virksomhet kan «inkluderes» i menneskebasert innhenting, og hvorvidt forslaget forsøker å hjemle aktivitet som ellers ville være ulovlig.

Politiets sikkerhetstjeneste (PST) savner en bredere vurdering av behovet for å lovfeste metoden i lys av Grunnloven og EMK. PST bemerker i tillegg at det synes som begrepene infiltrasjon og provokasjon tillegges et noe annet innhold enn i straffeprosessen. PST mener at det fremstår som noe uheldig at begrepene ikke er direkte definert i lovutkastet, da man ellers lett kan få inntrykk av at begrepene skal forstås på samme måte som i politiet. *Riksadvokaten* gir uttrykk for at det er vanskelig å bedømme hvorvidt begrepene skal forstås på samme måte som i politiet.

10.6.3 Departementets vurdering

Departementet viderefører forslaget i høringsnotatet om å lovfeste menneskebasert innhenting som metode, men har etter høringen omformulert bestemmelsen med sikte på å gjøre den klarere og enklere å forstå. Blant annet foreslås det i lys av høringsuttalelsene til *Kripos*, *Politiets sikkerhetstjeneste* og *riksadvokaten* å sløyfe regelen i lovutkastet § 6-3 andre ledd om at menneskebasert inn-

henting kan inkludere infiltrasjon og provokasjon. Dette er ikke ment å utgjøre noen realitetsforskjell fra forslaget i høringsnotatet, da det følger av de generelle reglene i lovforslaget § 6-1 andre ledd og § 11-4 første ledd at metoden kan brukes fordekt, og at det kan brukes uriktige, falske eller villedende identiteter. Det følger av dette at en tjenesteperson for eksempel kan infiltrere et miljø eller organisasjon gjennom å utgi seg for å være en annen, og i den forbindelse påvirke handlingsmønsteret til andre mennesker, for eksempel gjennom å etterspørre informasjon som det for en annen person er ulovlig å selge eller på annen måte gi fra seg etter et annet lands rett. Departementet viser for øvrig til lovforslaget § 6-3 og merknadene til bestemmelsen for en nærmere beskrivelse av metoden.

10.7 Systematisk observasjon

10.7.1 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 10.5.9 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.

Det vises i høringsnotatet til at ikke alle spaningslignende tiltak krever hjemmel i lov, men at gode grunner likevel taler for å lovhjemle grensene for systematisk observasjon for slik å angi klare rammer for metoden. Forslaget kodifiserer og presiserer gjeldende praksis.

I høringsnotatet er regler om systematisk observasjon inntatt i lovutkastet § 6-4.

10.7.2 Høringsinstansenes syn

Politiets sikkerhetstjeneste (PST) stiller seg kritiske til forslaget om å lovfeste innhenting gjennom systematisk observasjon. PST viser til risikoen for at forslaget vil ha en smitteeffekt til spørsmålet om å lovfeste politimetoder som per nå er ulovfestede.

10.7.3 Departementets vurdering

Departementet viderefører forslaget i høringsnotatet, som i hovedsak ikke har møtt negative merknader under høringen. Det foreslås enkelte lovtekniske justeringer. For en nærmere beskrivelse av metoden vises det til lovforslaget § 6-4 og merknadene til bestemmelsen.

Selv om systematisk observasjon ikke nødvendigvis vil utgjøre et menneskerettslig inngrep, mener departementet at det er hensiktsmessig å lovregulere rammene for metoden. Det understrekes at det i dette lovarbeidet ikke tas stilling til spørsmålet om lovfesting av ulovfestede politimetoder.

10.8 Teknisk sporing

10.8.1 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 10.5.10 å lovfeste at Etterretningstjenesten kan ta i bruk teknisk sporing for å lokalisere personer og gjenstander. Forslaget kodifiserer og presiserer gjeldende metodebruk. I høringsnotatet er regler om teknisk sporing inntatt i lovutkastet § 6-5.

10.8.2 Høringsinstansenes syn

Ingen høringsinstanser har merknader til forslaget i høringsnotatet.

10.8.3 Departementets vurdering

Departementet viderefører forslaget med enkelte lovtekniske justeringer. Det vises til lovforslaget § 6-5 og merknadene til bestemmelsen for en nærmere beskrivelse av metoden.

10.9 Gjennomsøking, avlytting, bildeovervåkning og annen teknisk innhenting

10.9.1 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 10.5.11 å lovfeste at Etterretningstjenesten kan gjennomføre gjennomsøking, avlytting, skjult bildeovervåkning og annen innhenting med tekniske midler. I høringsnotatet er regler om disse metodene inntatt i lovutkastet § 6-6.

10.9.2 Høringsinstansenes syn

Dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors påpeker at det er tale om svært inngripende metoder, og har merknader knyttet til beslutningsprosessen. Det samme har *Advokatforeningen*. Dette spørsmålet behandles i punkt 10.13. Ingen høringsinstanser har merknader til utformingen av bestemmelsen.

10.9.3 Departementets vurdering

Departementet viderefører i hovedsak forslaget i høringsnotatet. For å gjøre lovforslaget mer oversiktlig splittes bestemmelsen opp i tre paragrafer, slik at gjennomsøking reguleres av § 6-6, avlytting og bildeovervåkning av § 6-7 og annen teknisk innhenting av § 6-8. I § 6-6 presiseres det at Etterretningstjenesten kan tilegne seg etterretningsrelevante gjenstander som finnes under gjennomsøkingen, samt fra personer. Det kan for eksempel være et dokument eller lagringsmedium. I § 6-7 strykes ordet «skjult», da det er overflødig ved siden av regelen i § 6-1 andre ledd om at metodene kan brukes fordekt. For å samordne §§ 6-7 og 6-8 med § 6-4 om systematisk observasjon foreslås det også å endre formuleringen «på eller mot sted» til «på sted». Det vises for øvrig til merknadene til bestemmelsene for en nærmere beskrivelse av metodene.

10.10 Midtpunktinnhenting

10.10.1 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 10.5.12 å lovfeste at Etterretningstjenesten kan gjennomføre midtpunktinnhenting av elektronisk kommunikasjon. Midtpunktinnhenting innebærer å fange opp kommunikasjonssignaler under transport. Forslaget kodifiserer og presiserer gjeldende rammer og praksis. I høringsnotatet er regler om midtpunktinnhenting inntatt i lovutkastet § 6-7.

10.10.2 Høringsinstansenes syn

Datatilsynet mener at all midtpunktinnhenting bør underlegges samme forhåndskontroll som tilrettelagt innhenting, som er en form for midtpunktinnhenting som foreslås særskilt regulert i lovforslaget kapittel 7 og 8. *Norges institusjon for menneskerettigheter (NIM)* gir uttrykk for synspunkter i samme retning. Dette spørsmålet behandles i punkt 10.13. Ingen høringsinstanser har merknader til utformingen av bestemmelsen.

10.10.3 Departementets vurdering

Departementet viderefører forslaget i høringsnotatet med enkelte lovtekniske justeringer. Bestemmelsen inntas i lovforslaget § 6-9. Det vises til merknadene til bestemmelsen for en nærmere beskrivelse av metoden.

10.11 Endepunktinnhenting

10.11.1 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 10.5.13 å lovfeste at Etterretningstjenesten kan gjennomføre endepunktinnhenting av informasjon i systemer og tjenester som etterretningsmål besitter eller antas å ville benytte. Endepunktinnhenting innebærer å avlytte eller avlese informasjon direkte fra en kommunikasjonsenhet, datamaskin eller annet system hvor relevante etterretningsdata ligger lagret eller blir behandlet. Dette til forskjell fra midtpunktinnhenting, hvor informasjonen hentes inn under transport. Forslaget kodifiserer og presiserer gjeldende metodebruk. I høringsnotatet er regler om endepunktinnhenting inntatt i lovutkastet § 6-8.

10.11.2 Høringsinstansenes syn

Ingen høringsinstanser har merknader til forslaget i høringsnotatet.

10.11.3 Departementets vurdering

Departementet viderefører forslaget i høringsnotatet med enkelte lovtekniske justeringer. Bestemmelsen inntas i lovforslaget § 6-10. Det vises til merknadene til bestemmelsen for en nærmere beskrivelse av metoden.

10.12 Forberedende tiltak

10.12.1 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 10.5.3 å lovfeste 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. Det presiseres i høringsnotatet at dette ikke er en selvstendig hjemmel for metodebruk, men kun er ment å synliggjøre i lov at metodebruk krever en rekke forutgående faktiske handlinger. Det heter i høringsnotatet at forslaget kodifiserer og presiserer gjeldende praksis.

10.12.2 Høringsinstansenes syn

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

seg at høringsnotatet ikke inneholder noen vurderinger av hvorvidt, og eventuelt i hvilken utstrekning, forberedende tiltak kan gjennomføres overfor fysiske og juridiske personer og deres eiendeler i Norge. Dermed er heller ikke grensen opp mot den foreslåtte territorielle begrensningen drøftet.

10.12.3 Departementets vurdering

Departementet viderefører forslaget i høringsnotatet. Bestemmelsen inntas i lovforslaget § 6-11.

I lys av høringsuttalelsen til *EOS-utvalget* vil departementet presisere at forbudet etter lovforslaget § 4-1 mot å bruke innhentingsmetoder etter kapittel 6 overfor personer i Norge omfatter forberedende tiltak i den utstrekning tiltaket innebærer et inngrep overfor den enkelte som krever hjemmel i lov. Som følge av dette vil slike forberedende tiltak overfor personer i Norge bare kunne treffes dersom et av unntakene fra § 4-1 får anvendelse, for eksempel ved innhenting om fremmed statsaktivitet i Norge etter § 4-2 eller ved bruk av åpne kilder etter § 4-4.

10.13 Beslutning om metodebruk

10.13.1 Forslaget i høringsnotatet

I høringsnotatet punkt 10.6.2 drøftes hvorvidt det bør etableres en generell mekanisme for forhåndsgodkjennelse av metodebruk av en domstol eller uavhengig administrativt organ, men det konkluderes med at dette verken er mulig, nødvendig eller ønskelig. Det vises til at en slik ordning vil innebære en endring av gjeldende praksis, som vil svekke tjenestens effektivitet og avvike fra hva som gjelder i sammenlignbare land. Det vises dessuten til at mengden beslutninger og sikkerhetsmessige hensyn gjør at det ikke vil være praktisk mulig å legge beslutningsmyndighet i enkeltsaker utenfor tjenesten.

Det understrekes i høringsnotatet at man ikke uten videre kan trekke noen analogi fra forutgående rettslig prøving av straffeforfølgende myndigheters tvangsmiddelbruk, da formålet og den rettslige begrunnelsen for slik virksomhet er vesensforskjellig fra utenlandsetterretning.

Det vises i høringsnotatet til at man alternativt kan se for seg en løsning der en uavhengig instans på overordnet nivå forhåndsgodkjenner metodebruk for hele saksområder. Dette ville være praktisk mulig, men 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 tillagt avgjørende vekt. Bakgrunnen for prinsippet om etterfølgende kontroll var blant annet at EOS-utvalget ikke 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. Det gis i høringsnotatet uttrykk for at de samme argumentene gjør seg gjeldende i dag.

Det vises dessuten til at en ordning med uavhengig forhåndsgodkjennelse ikke vil ivareta behovet for konkrete forholdsmessighetsvurderinger av metodebruk knyttet til spesifikke etterretningsmål eller -operasjoner, hvor omstendighetene kan være i konstant endring.

I høringsnotatet konkluderes det på bakgrunn av de ovennevnte momenter med at det ikke bør innføres en ordning med uavhengig forhåndsgodkjennelse av Etterretningstjenestens bruk av metoder. Det foreslås imidlertid særlige regler for forhåndsgodkjennelse av tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon, som er en spesiell tilgang innenfor rammen av midtpunktinnhenting som metode. Grunnen til dette er at tilgangen medfører lagring av store mengder metadata om norsk innenlandsk kommunikasjon, i motsetning til andre metoder som reguleres av lovutkastet kapittel 6.

10.13.2 Høringsinstansenes syn

Advokatforeningen mener at det må være uavhengig forhåndsgodkjennelse av metoder som nevnt i lovutkastet § 6-5 (teknisk sporing) og § 6-6 (gjennomsøking, avlytting, skjult bildeovervåkning og annen innhenting med tekniske midler). Foreningen fremhever at praksis fra Den europeiske menneskerettsdomstol viser at kravet til rettsgrunnlag omfatter krav til prosessuelle rettssikkerhetsmekanismer for å forebygge myndighetsmisbruk, og er ikke enig med departementet i at EOS-utvalgets tilsyn er tilstrekkelig for å tilfredsstille de menneskerettslige kravene.

Datatilsynet mener at all midtpunktinnhenting må underlegges samme forhåndskontroll som tilrettelagt innhenting etter lovutkastet kapittel 7 og 8.

Dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors bemerker at mange av de

beskrevne metodene er svært inngripende, uten at det legges opp til tilsvarende kontroll som for tilrettelagt innhenting. Som eksempel viser de til innhenting med tekniske midler (lovutkastet § 6-6), og bemerker at PST og det alminnelige politiet må ha domstolens tillatelse for å bruke slike metoder.

Den internasjonale juristkommisjon – norsk avdeling (ICJ-Norge) stiller spørsmål ved hvorfor det ikke er foreslått domstolskontroll ved Etterretningstjenestens overvåking av nordmenn i utlandet. De viser til at en slik ordning blant annet er etablert i Danmark, og etterspør en mer nyansert drøfting av spørsmålet.

Kripos har forståelse for at regelverket må legge til rette for effektiv oppgaveløsning og ivaretakelse av sikkerhetshensyn, og at en domstolskontroll med større deler av innhentingsvirksomheten hverken vil være hensiktsmessig eller mulig, men mener at mulighetene for en bedre legalitetskontroll burde vært vurdert nærmere.

NRK mener at forslaget er i strid med kildevernet fordi det ikke er lagt opp til domstolskontroll eller andre rettssikkerhets- eller kontrollmekanismer som kan ivareta kildevernet. NRK kan ikke se at det er grunn til å forskjellsbehandle de tilfeller der Etterretningstjenesten er avhengig av samarbeid fra eksterne aktører for å få tilgang til informasjon, og de tilfeller der de ikke trenger bistand fra eksterne.

Politiets sikkerhetstjeneste (PST) viser til at domstolskontroll er en etablert og grunnleggende rettssikkerhetsmekanisme i liberale demokratier. PST mener at den delen av Etterretningstjenestens metodebruk som berører personer eller virksomheter innenfor norsk jurisdiksjon, bør underlegges domstolskontroll. Behovet forsterkes ytterligere av at metodebruken ikke synes å ha noen lovpålagt tidsbegrensning utover at den må avsluttes dersom vilkårene ikke lenger er til stede.

Riksadvokaten uttaler:

> «Generelt bemerkes at flere av metodene som er beskrevet i kapittel 6, i sitt innhold likner meget på tvangsmidler som kan brukes av politiet, men da underlagt domstolskontroll. Begrunnelsen for domstolskontrollen er blant annet metodenes inngripende karakter. Beslutningskompetansen etter utkastets § 6-10 første ledd er lagt til Sjef Etterretningstjenesten eller den han eller hun bemyndiger. Dette innebærer i praksis at beslutningskompetansen er lavere når Etterretningstjenesten iverksetter, enn når politiet gjør det. Dette gir grunnlag for atskillig refleksjon, særlig når inngrepets karakter ikke er vesensforskjellig.»

Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget) mener at forhåndskontroll av innhenting i utlandet rettet mot personer med tilknytning til Norge kan utredes, og uttaler:

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

10.13.3 Departementets vurdering

Departementet tar som utgangspunkt at flere av de metodene som foreslås lovregulert, tilsvarer eller ligner på metoder som PST og politiet for øvrig kan bruke med hjemmel i straffeprosessloven og politiloven. Formålet med metodebruken er derimot ikke det samme. PST og politiet for øvrig skal forebygge, avverge og etterforske straffbare handlinger, mens Etterretningstjenesten skal innhente informasjon om utenlandske forhold for å gi myndighetene grunnlag for å fatte riktige beslutninger. Tjenesten rår ikke over fysiske tvangsmidler som pågripelse og fengsling, og har ingen oppgaver knyttet til straffeforfølgning. Innhentingen har i hovedsak en sikkerhetspolitisk karakter, og bærer ikke preg av kriminalitetsbekjempelse. Det kan derfor ikke uten videre trekkes analogier fra reglene om tvangsmidler som gjelder for PST og politiet for øvrig. For eksempel er det etter departementets oppfatning liten grunn til å kreve uavhengig forhåndsgodkjennelse av innhenting av informasjon i utlandet som ikke berører norske personer.

Det kan være sterkere grunner for uavhengig forhåndsgodkjennelse av innhenting på norsk territorium eller mot norske personer i utlandet. Departementet foreslår slik kontroll av tilrettelagt innhenting, som innebærer lagring av store mengder metadata om norsk innenlandsk kommunikasjon. Andre former for innhenting av informasjon som foreslås regulert i loven vil ikke ha slike konsekvenser, og departementet foreslår ikke uavhengig forhåndsgodkjennelse av slik innhenting.

Departementet understreker at Etterretningstjenesten som hovedregel ikke kan bruke inngripende metoder overfor personer i Norge, jf. lovforslaget § 4-1. Metodebruk i Norge er bare tillatt i lovbestemte unntakstilfeller, se nærmere lovforslaget kapittel 4. Innhenting med grunnlag i unntaksbestemmelsen i § 4-2 skal alltid samordnes med PST, og hvis den gjelder forhold som også berører ansvarsområdet til PST, kreves samtykke fra PST, jf. lovforslaget § 4-3.

Departementet viderefører på denne bakgrunn forslaget i høringsnotatet om å legge myndigheten til å fatte beslutning om bruk av metoder for innhenting av informasjon til sjefen for Etterretningstjenesten. Som departementet har redegjort for under punkt 4.4.4, kan det ikke oppstilles noe menneskerettslig krav til forhåndsgodkjennelse av en domstol. Det beror på en samlet vurdering hvorvidt lovgivningen har tilstrekkelige garantier mot misbruk og vilkårlighet. Departementet understreker at all bruk av metoder er underlagt uavhengig etterfølgende kontroll av EOS-utvalget. I tillegg til dette kommer tjenestens internkontroll og departementets forvaltningskontroll. Det foreslås noen endringer på bakgrunn av høringen, herunder at det utelukkende er sjefen for tjenesten som skal kunne fatte beslutning om metodebruk, med mindre beslutningen ligger til departementet i samsvar med lovforslaget § 2-5. Det foreslås også strengere krav til hva beslutningen skal inneholde. Samlet mener departementet at lovforslaget tilfredsstiller de krav som følger av menneskerettighetene.

I lys av høringsuttalelsen til *PST* foreslår departementet å lovfeste at beslutningen ikke skal gis for lenger tid enn nødvendig. Departementet foreslår også en lengstefrist på ett år av gangen. Det vises til lovforslaget §§ 6-12 og 6-13 samt merknadene til disse bestemmelsene for en nærmere beskrivelse.

11 Tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon

11.1 Bakgrunn

11.1.1 Ekspertgruppen for forsvaret av Norge

Ekspertgruppen for forsvaret av Norge, ledet av professor Rolf Tamnes, ble oppnevnt 15. desember 2014 for 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 kapittel 8 drøftes kritiske funksjoner for forsvarsevnen, herunder etterretning og overvåkning. Gruppen redegjør for trusler i det digitale rom, og peker på behovet for å kunne følge med på relevant internettrafikk for å kunne oppdage, varsle og håndtere utenlandske trusler som terror, spionasje og digitale angrep. Dette vil etter gruppens syn utgjøre et slags digitalt grenseforsvar, som må kombineres med gode kontrollordninger som ivaretar hensynet til personvernet (rapporten side 75). Gruppen anbefaler å prioritere etableringen av et digitalt grenseforsvar (rapporten side 85).

11.1.2 Lysne I-utvalgets utredning om digital sårbarhet

Regjeringen nedsatte 20. juni 2014 et utvalg ledet av professor Olav Lysne for å kartlegge samfunnets digitale sårbarheter (Lysne I-utvalget). Utvalget ble bedt om å foreslå tiltak for å styrke beredskapen og redusere den digitale sårbarheten i samfunnet. Utvalget avga 30. november 2015 sin utredning NOU 2015: 13 Digital sårbarhet – sikkert samfunn. Utredningen redegjorde for de 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 å sette ned et eget utvalg for å utrede spørsmålet i større bredde enn det utvalget hadde hatt anledning til å gjøre. Forslaget ble fulgt opp gjennom oppnevningen av Lysne II-utvalget.

11.1.3 Lysne II-utvalgets rapport om digitalt grenseforsvar

Departementet oppnevnte 24. februar 2016 et utvalg ledet av professor Olav Lysne (Lysne II-utvalget). Utvalget fikk 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 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 26. august 2016 sin rapport. 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 et strengt kontrollregime i flere ledd, i tillegg til strenge begrensninger på bruken av informasjonen fra tilgangen.

Departementet sendte 5. oktober 2016 utvalgets rapport på offentlig høring med tre måneders høringsfrist. Departementet mottok nærmere 120 høringsuttalelser. I grove trekk mente høringsinstansene som støttet et digitalt grenseforsvar at tiltaket er nødvendig for at Etterretningstjenesten skal kunne løse sine oppgaver. Høringsinstansene som var kritiske, fremholdt at tiltaket var for inngripende, og at det var risiko for en nedkjølende effekt på ytringsfriheten og fare for formålsutglidning. Dertil mente flere at kryptering vil hindre eller begrense effekten av tiltaket. Noen mente at forslaget ikke var i samsvar med menneskerettslige eller EØS-rettslige krav.

11.1.4 Høringsnotatet 12. november 2018

Departementet har etter høringen av Lysne II-utvalgets rapport utredet hvorvidt det bør foreslås en form for digitalt grenseforsvar. Utredningen med forslag til særregler om tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon ble inntatt i kapittel 11 i høringsnotatet 12. november 2018. Det vises til punkt 2.2 for en nærmere beskrivelse av høringen. Synspunkter som har kommet frem under høringen, vil behandles under de enkelte delene av forslaget.

Noen høringsinstanser har som primærstandpunkt at det ikke bør åpnes for tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon, men kommenterer likevel hvordan reglene i motsatt fall bør utformes. Det understrekes derfor at merknader til deler av forslaget ikke nødvendigvis innebærer at høringsinstansen støtter forslaget i sin helhet.

11.2 Terminologi

11.2.1 Forslaget i høringsnotatet

I høringsnotatet punkt 11.3 drøftes hvilket språklig uttrykk som bør brukes om slik tilgang til grenseoverskridende elektronisk kommunikasjon som skisseres i Lysne II-utvalgets rapport. Det vises til at det har blitt brukt ulike betegnelser om forslaget, herunder digital grensekontroll, digital grenseovervåking og digitalt grenseforsvar. Det gis uttrykk for at det bør velges en annen betegnelse enn disse, blant annet fordi de er lite beskrivende for hva tiltaket faktisk går ut på.

I høringsnotatet vises det til at kabelaksess eller kabeltilgang er mer beskrivende for tiltaket, men at det bør brukes en teknologinøytral betegnelse. Bulkaksess eller bulktilgang er teknologinøytrale betegnelser, men får ikke frem hva som skiller denne formen for bulkinnhenting fra andre former for bulkinnhenting, nemlig at kommersielle tilbydere må tilrettelegge for den. Det fremholdes i høringsnotatet at dette særtrekket bør fremgå av betegnelsen. Betegnelsen bør også få frem at tilgangen gjelder kommunikasjon som passerer den norske grensen, altså at den er grenseoverskridende. På denne bakgrunn foreslås betegnelsen tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon.

11.2.2 Høringsinstansenes syn

Datatilsynet, *Norsk Journalistlag* og *Piratpartiet* er kritiske til at forslaget betegnes som tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon. Datatilsynet mener at betegnelsen er uklar og ikke egnet til å beskrive hva som faktisk skjer, og går inn for betegnelsen digital masseovervåkning.

11.2.3 Departementets vurdering

Departementet tar som utgangspunkt at det bør brukes ord som så presist som mulig gjenspeiler forslagets innhold. I høringsnotatet gikk departementet derfor bort fra termen digitalt grenseforsvar, som i liten grad beskriver forslaget. Termen er godt innarbeidet og vil antakelig fortsatt brukes i den offentlige debatten, men den er for lite presis til å egne seg i et lovforslag.

Termen digital masseovervåkning, som *Datatilsynet* foreslår, er lite presis og egner seg ikke godt i et lovforslag. Departementet mener at forslaget heller ikke kan betegnes som digital masseovervåkning i en mer dagligspråklig mening, gitt formålsbegrensningen til utenlandsetterretning, plikten til utvalg og filtrering, vilkårene for tilgang til lagrede data og tiltakene som skal motvirke misbruk og vilkårlighet. Departementet understreker i denne sammenhengen at Etterretningstjenesten ikke vil kunne søke i lagrede metadata før retten har godkjent det på bakgrunn av lovbestemte vilkår. Når det er sagt, respekterer departementet at det er delte oppfatninger om hvordan forslaget best kan betegnes.

Betegnelsen tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon beskriver etter departementets syn forslagets innhold på en mer presis måte. Den får frem at det er tale om innhenting av elektronisk kommunikasjon, at kommunikasjonen må krysse grensen og at innhentingen forutsetter tilrettelegging. Det sistnevnte momentet får frem hva som skiller denne tilgangen fra andre former for midtpunktinnhenting (innhenting av kommunikasjon i transitt mellom to endepunkter).

Noen høringsinstanser mener at den teknologiske utviklingen gjør det meningsløst å skille mellom grenseoverskridende og ikke-grenseoverskridende kommunikasjon, da svært mye norsk innenlandsk kommunikasjon krysser grensen. Departementet har forståelse for dette synspunktet. I dagens teknologiske situasjon er det en kjensgjerning at norsk innenlandsk kommunikasjon i stor grad krysser grensen, og det vil være

vanskelig å filtrere bort denne før innhenting og lagring, se nærmere punkt 11.8.2. Samtidig finnes det også kommunikasjon som ikke krysser grensen, og som effektivt vil kunne filtreres bort før innhenting og lagring. På denne bakgrunn mener departementet at begrensningen til grenseoverskridende elektronisk kommunikasjon er reell, og bør gjenspeiles i terminologien.

I lys av Datatilsynets standpunkt har departementet vurdert hvorvidt ordet innhenting kan erstattes med masseinnhenting eller bulkinnhenting. Departementet har kommet til at en slik betegnelse ikke er tilstrekkelig presis, da lovforslaget åpner for både innhenting og lagring av metadata i bulk (§ 7-7) og målrettet innhenting av innholdsdata (§ 7-9). For å komme Datatilsynet i møte, har departementet likevel justert lovforslaget § 7-7 for å gjøre det tydelig at metadata vil innhentes og lagres i bulk, det vil si at en vesentlig andel av denne informasjonen antas å være uten relevans for etterretningsformål.

Departementet fastholder etter dette forslaget i høringsnotatet om å bruke betegnelsen tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon. Av språklige grunner vil også kortformen tilrettelagt innhenting brukes i proposisjonen.

11.3 Andre lands rett

11.3.1 Sverige

Sverige vedtok i 2008 lovgivning som åpner for innhenting av grenseoverskridende elektronisk kommunikasjon for etterretningsformål. Det følger av *lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet* at signalspaningsmyndigheten kan innhente signaler i elektronisk form. Innhentingen kan bare ha til formål å kartlegge utenlandske forhold.

Innhentingen skjer etter filtrering basert på søkebegreper. Søkebegrepene skal utformes og anvendes på en måte som medfører minst mulig inngrep i den personlige integriteten. Dette innebærer blant annet at søkebegreper som direkte kan henføres til en konkret person, ikke kan brukes med mindre det er av betydelig viktighet for etterretningen.

Det skal ikke innhentes signaler mellom avsender og mottaker som begge befinner seg i Sverige. Hvis slike signaler ikke kan skilles ut allerede ved innhentingen, skal de slettes når det blir klart at de har blitt innhentet.

Innhentingen krever forhåndsgodkjennelse av *Försvarsunderrättelsedomstolen* etter *lagen (2009:966) om Försvarsunderrättelsedomstol*. Det føres dessuten kontroll av *Statens inspektion för försvarsunderrättelseverksamheten (SIUN)* og *Datainspektionen*.

Regler om tilretteleggingsplikt følger av *lagen (2003:389) om elektronisk kommunikation* 19 a §. Plikten innebærer overføring av signalene til innmeldte punkter.

11.3.2 Danmark

Danmark har ingen lovgivning som uttrykkelig regulerer innhenting av grenseoverskridende elektronisk kommunikasjon for etterretningsformål. Det følger imidlertid av *lov om Forsvarets Efterretningstjeneste (FE)* at FE kan innhente og innsamle opplysninger som kan ha betydning for tjenestens etterretningsmessige virksomhet. Loven er utformet på en teknologi- og metodenøytral måte, og er derfor ikke til hinder for at FE innhenter elektronisk kommunikasjon i bulk.

FE kontrolleres av *Tilsynet med Efterretningstjenesterne (TET)*. Det føres dessuten parlamentarisk kontroll og forvaltningskontroll. Ved innhenting på kontraterrorfeltet som medfører et inngrep i kommunikasjonsvernet til en person i utlandet som er hjemmehørende i Danmark, skal innhentingen godkjennes av en domstol.

11.3.3 Finland

Finland vedtok i 2019 lovgivning som åpner for innhenting av grenseoverskridende elektronisk kommunikasjon for etterretningsformål. Det følger av *lag 590/2019 om militär underrättelseverksamhet* at den militære etterretningstjenesten kan innhente informasjon om datatrafikk som krysser Finlands grenser i kommunikasjonsnett.

Ved innhentingen skal det tas utgangspunkt i søkebegreper. Som søkebegrep kan ikke brukes opplysninger som identifiserer teleterminalutstyr eller teleadresse som innehas av eller antas å brukes av en person som oppholder seg i Finland. Hvis innhentingen gjelder andre enn statlige aktører, får ikke innhentingen innrettes ut fra en meldings innhold, med mindre det brukes informasjon som beskriver innholdet i et sabotasjeprogram.

Innhentingen skal godkjennes av tingretten i Helsingfors. Det føres dessuten ekstern kontroll av *riksdagens underrättelsetillsynsutskott*, *riksdagens justitieombudsman* og *underrättelsetillsynsombudsmannen*.

Etter *lag 582/2019 om civil underrättelseinhämtning avseende datatrafik* kan også sivile etter-

retningsmyndigheter innhente datatrafikk i kommunikasjonsnett som krysser grensen. Den militære etterretningstjenesten står for den tekniske utførelsen av innhentingen.

11.3.4 Andre land

Også andre europeiske land som står Norge nært, har i de senere årene åpnet for innhenting av grenseoverskridende elektronisk kommunikasjon for etterretningsformål. Dette gjelder blant andre *Nederland*, *Frankrike*, *Tyskland* og *Storbritannia*.

11.4 Behov og alternative løsninger

11.4.1 Høringsnotatet

Behovet for tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon drøftes i høringsnotatet punkt 11.6. Det vises til at Norge har blitt et av verdens mest digitaliserte land. Den teknologiske utviklingen gir gevinster, men fører også med seg sårbarheter. Det er naturlig og nødvendig at Etterretningstjenesten tilpasser og moderniserer sin virksomhet i takt med den teknologiske utviklingen.

I høringsnotatet vises det for det første til at både statlige og private aktører bruker det digitale rom til angrep, sabotasje, påvirkningsoperasjoner og spionasje. Aktørene utvikler stadig nye og sofistikerte metoder for slike nettverksoperasjoner. 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 er nødvendig for produksjon av etterretning generelt.

Høringsnotatet understreker betydningen av rettidig informasjon. Myndighetene kan ha et begrenset tidsvindu til å motvirke en trussel. Dersom Etterretningstjenesten er avhengig av å spørre om informasjon fra andre fordi tjenesten mangler egen tilgang, kan ventetiden være skjebnesvanger. Det er heller ikke gitt, og i mange tilfeller lite sannsynlig, at andre besitter den nødvendige informasjonen. Det vurderes som svært viktig at tjenesten har tilgang til relevant informasjon uten unødig opphold.

I høringsnotatet vises det til at Etterretningstjenesten, i fravær av adekvat tilgang til elektronisk kommunikasjon, er avhengig av å motta informasjon fra samarbeidende tjenester. Det pekes på flere svakheter ved denne avhengigheten. Samarbeidende tjenester har ikke norske interesser som prioritet, og uten egen tilgang kan det være vanskelig å kvalitetssikre og verifisere informasjonen som mottas.

Departementet vurderer i høringsnotatet at tilgang på grenseoverskridende elektronisk kommunikasjon vil gi Etterretningstjenesten anledning til selvstendig og formålsrettet å innhente kritisk informasjon fra en helt sentral informasjonskilde som tjenesten i dag ikke har tilgang til. Det vurderes 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, særlig statlig spionasje, forberedelser til cyberangrep og grenseoverskridende terrorplanlegging.

I punkt 11.7 i høringsnotatet drøftes hvorvidt det finnes alternative løsninger som både kan møte behovet og er mindre inngripende enn Lysne II-utvalgets modell. Det utredes ikke modeller som i større grad enn Lysne II-utvalget tar etterretningsfaglige hensyn, og som dermed vil kunne medføre et større menneskerettslig inngrep.

Tre alternativer drøftes i høringsnotatet:

Alternativ 1 er tilrettelagt innhenting utelukkende knyttet til kjente mål («lettversjonen»), se høringsnotatet punkt 11.7.2.

Alternativet bygger på positiv filtrering basert på kjente selektorer, noe som vil føre til at innhenting og lagringen får et vesentlig mindre omfang. Løsningen forutsetter imidlertid at Etterretningstjenesten allerede besitter tilstrekkelig informasjon til å kunne igangsette målrettet innhenting. Denne forutsetningen gjenspeiler ikke virkeligheten. Alternativet åpner ikke for søk i et datagrunnlag for målsøkingsformål, for retrospektiv analyse eller for å finne nye identiteter knyttet til allerede kjente mål.

Det konkluderes med at alternativ 1 vil gi svært lav etterretningsmessig verdi med hensyn til digitale trusler, kontraterror og øvrige oppdrag.

Alternativ 2 er utplassering av sensorer i utvalgte virksomheter, se høringsnotatet punkt 11.7.3.

Alternativet innebærer at det plasseres 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. I motsetning til sikkerhetssensorer, som i Varslingssystemet for digital infrastruktur (VDI), som har til hensikt å øke sikkerheten i et spesifikt nettverk i Norge, vil disse etterretningssensorene ha til hensikt å belyse en utenlandsk trusselaktør, slik at man kan oppdage og

dermed ha mulighet til å stanse trusselaktivitet før trusselaktøren opererer i det spesifikke nettverket.

Alternativet er betraktelig mer spisset enn Lysne II-utvalgets modell, og utgjør dermed ikke et like sterkt menneskerettslig inngrep. Alternativet vil imidlertid ikke gi det nødvendige helhetsbildet av trusselaktørens aktivitet i og mot Norge. Løsningen vil ikke kunne besvare de sentrale spørsmålene som oppstår ved et digitalt angrep, det vil si når aktøren først ble observert, hvem som står båk, hvilke øvrige mål i Norge aktøren går etter, og hva som er hensikten med aktiviteten. Det er også andre svakheter ved forslaget, blant annet at det vil være utfordrende å vite hvor sensorene bør plasseres.

Det konkluderes med at alternativ 2 vil gi lav etterretningsmessig verdi med hensyn til digitale trusler, og ingen verdi med hensyn til kontraterror og øvrige oppdrag.

Alternativ 3 er å opprettholde dagens situasjon uforandret, og ikke åpne for tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon («nullalternativet»), se høringsnotatet punkt 11.7.4.

Alternativet innebærer en fortsatt avhengighet av informasjon fra andre land. For Norge er denne avhengigheten en sårbarhet som i verste fall kan føre til en svekkelse av evnen til å treffe riktige beslutninger i saker som angår vår nasjonale sikkerhet. Alternativet vil også kunne føre til et behov for økt bruk av andre metoder, og mer innenlandsetterretning. På denne bakgrunn anbefales ikke dette alternativet.

Det konkluderes i høringsnotatet med at ingen av de alternative løsningene er egnet til å møte behovet. Det foreslås derfor en løsning som i kjernen er lik Lysne II-utvalgets anbefaling, med innhenting og lagring av metadata i bulk samt målrettet innhenting av innholdsdata. Søk i lagrede metadata og målrettet innhenting av innholdsdata vil kreve rettens kjennelse.

11.4.2 Høringsinstansenes syn

Høringsinstansene viser gjennomgående forståelse for behovet for tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon. Det pekes samtidig på problematiske sider ved forslaget, særlig fra et personvern- og menneskerettighetsperspektiv.

Nasjonal sikkerhetsmyndighet (NSM) slutter seg til beskrivelsen i høringsnotatet av de digitale trusler som samfunnet i dag står overfor. Dette trusselbildet, kombinert med en økende digitalisering, komplekse digitale verdikjeder og at vi legger stadig flere av de viktigste verdiene våre i det digitale rom, medfører nye og betydelige sikkerhetsmessige utfordringer. NSM uttaler:

> «For ivaretakelse av vår nasjonale sikkerhet er det etter NSMs oppfatning av avgjørende betydning at myndighetene disponerer et virkemiddelapparat som gir oss en god nasjonal evne til å håndtere disse utfordringene. Tilgang til tidsriktig og relevant informasjon om trusler og trusselaktører i det digitale rom er i denne sammenheng helt sentralt. NSM ser derfor et behov for, og støtter, at Etterretningstjenesten gis et hjemmelsgrunnlag for tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon som foreslått i lovutkastet kapittel 7.»

NSM slutter seg til departementets vurderinger av de alternative løsningene. NSM kan ikke se at de alternativene som drøftes i høringsnotatet, vil være tilstrekkelig effektive virkemidler for håndtering av de alvorlige trusler vi i dag, og ikke minst i fremtiden, vil stå overfor i det digitale rom. NSM erkjenner at tilrettelagt innhenting er et inngripende virkemiddel, og ser de personvernutfordringer som forslaget reiser, men mener at tiltaket er nødvendig og sentralt for statens samlede evne til å ivareta nasjonens og samfunnets sikkerhet i det digitale rom.

Nasjonal kommunikasjonsmyndighet (Nkom) mener at en regulert tilgang til kommersielle ekomnett vil gi Etterretningstjenesten økt tilgang til etterretningsrelevant informasjon enn det de har i dag, og gi tjenesten økt mulighet til å kartlegge og motvirke ytre trusler mot viktige nasjonale interesser. Etter Nkoms syn er det imidlertid ikke tvilsomt at etablering av tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon er utfordrende i et samfunn som er så digitalisert som Norge, og der kommunikasjonsvernet anses som grunnleggende for tilliten til elektronisk kommunikasjon og digitale tjenester.

Direktoratet for e-helse støtter lovforslagets motivasjon om å sikre og beskytte norsk infrastruktur og systemer mot uønskede angrep og inntrengingsforsøk. Direktoratet viser til at også helsesektoren er utsatt, og har blitt rammet. Direktoratet stiller imidlertid spørsmål ved den reelle nytteverdien av å innhente kryptert kommunikasjon.

Kystverket uttaler at de, som flere andre etater, har merket konsekvenser av det endrede trusselbildet, og har forståelse for Etterretningstje-

nestens behov for metoder som er bedre tilpasset utviklingen på kommunikasjonsområdet.

Justis- og beredskapsdepartementet uttaler:

> «Både PSTs og Etterretningstjenestens trusselvurderinger for 2019 omtaler en rekke trusler mot det norske demokratiet, fra andre land, fra potensielle, politisk motiverte voldsutøvere og personer som ønsker å ramme norske myndighetspersoner på ulike måter. Endrede kommunikasjonsformer innebærer at de etablerte metodene for å innhente nødvendig informasjon for å forebygge disse truslene i stadig mindre grad er relevante for å dekke informasjonsbehovet. Utviklingen i retning av et «hybrid» trusselbilde – som kan bestå av sammensatte hendelser, lovbrudd og påvirkningsoperasjoner både i det digitale rom og i den «analoge» del av virkeligheten – innebærer dessuten et økende behov for tilgang til informasjon også i det digitale rom.
>
> For å kunne gi relevante beslutningsunderlag til politiske myndigheter til riktig tid, er det nødvendig at Etterretningstjenesten får tilstrekkelig tilgang til informasjon også fra digitale formidlingsformer. Dette har vært og er en grunnleggende forutsetning for løsningen av Etterretningstjenestens samfunnsoppdrag.
>
> Som tidligere påpekt i departementets høringsuttalelse 16. januar 2017 til utredningen fra Lysne II-utvalget, er det dessuten «viktig for hensynet til nasjonal selvstendighet og suverenitet – og for å sikre at informasjonsinnhentingen skjer ut fra nasjonale behov og ikke som biprodukt av andre nasjoners informasjonsinnhenting – at mest mulig informasjonsinnhenting skjer av norske organer; i dette tilfelle E-tjenesten. Dette er dessuten avgjørende for at overvåkningen kan kontrolleres av norske domstoler og EOS-utvalget.»»

Det nasjonale statsadvokatembetet viser til sin høringsuttalelse til rapporten til Lysne II-utvalget, hvor de støtter behovet for tiltaket under forutsetning av at det underlegges strenge begrensninger for å være juridisk holdbart og forholdsmessig i et menneskeretts- og personvernperspektiv. *Politidirektoratet* anerkjenner behovet for tilrettelagt innhenting, men mener at de nærmere rammene ikke i tilstrekkelig grad er utredet. *Innlandet politidistrikt* mener at det angis gode grunner for forslaget. *Kripos* uttaler:

> «I høringsnotatet gjøres grundig rede for utfordringer knyttet til eskaleringen av digitale trusler mot Norge og norske interesser. Aktørene bak slike trusler inkluderer etter det opplyste både statlige etterretnings- og sikkerhetstjenester, terrorist- og ekstremistgrupper og organiserte hackergrupper. Per i dag anses etterretningsvirksomhet i statlig regi å utgjøre den mest alvorlige trusselen i det digitale rom, der angrep kan ramme både nasjonale beslutningsprosesser og utfordre samfunns- og statssikkerheten. Digitale kommunikasjonsplattformer brukes også til planlegging og koordinering av terrorhandlinger. Samtidig vises til at det stadig utvikles nye og sofistikerte metoder for nettverksoperasjoner. Departementet anser det alvorlig at norske myndigheter per i dag ikke er rustet til å avdekke og avverge de mest alvorlige truslene mot Norge i det digitale rom. I denne sammenheng vil imidlertid tilrettelagt innhenting gi Etterretningstjenesten mulighet til selvstendig og formålsrettet innhenting av kritisk informasjon, fra en helt sentral informasjonskilde man i dag er avskåret fra.
>
> Etter Kripos' syn viser departementet og tidligere utredninger til tunge hensyn som underbygger behovet for å innføre en tilgang til grenseoverskridende elektronisk kommunikasjon også i Norge. Kripos har ikke noe informasjonsgrunnlag som tilsier en annen vurdering av den underliggende situasjonen som beskrives. Tvert imot er vi gjennom egne ansvarsområder oppmerksom på de utfordringer som utviklingen av kommunikasjonsteknologi medfører, i forhold til å kunne forebygge, avdekke, avverge eller etterforske alvorlig kriminalitet i det digitale rom.
>
> En av statens grunnleggende oppgaver er å sikre landets suverenitet og innbyggernes sikkerhet. Den teknologiske utviklingen har imidlertid gjort både samfunns- og statssikkerheten mer sårbar. At vår etterretningstjeneste ikke er i stand til å avdekke, varsle og motvirke de alvorlige trusler det vises til, fremstår for Kripos som urovekkende, og synes å legge begrensninger på tjenestens evne til å løse sitt samfunnsoppdrag.»

Kripos påpeker samtidig at lovforslaget er utfordrende fra et personvern- og menneskerettighetsperspektiv.

Politiets sikkerhetstjeneste (PST) mener at behovet for tilrettelagt innhenting er grundig drøftet i Lysne II-utvalgets rapport og i høringsnotatet. PST viser særlig til endringen i trusselbildet og behovet for nasjonal kontroll med informasjonen. I en pressemelding 15. februar 2019 i forbin-

delse med oversendelsen av høringsuttalelsen uttaler PST:

> «Når det gjelder forslaget om [Etterretningstjenestens] tilgang til grensekryssende elektronisk kommunikasjon, såkalt tilrettelagt innhenting, er dette et tiltak PST støtter og ønsker velkommen. Gitt dagens trusselbilde og Norges behov for å ha nasjonal kontroll på denne informasjonen, ser PST dette som helt avgjørende for å ivareta den nasjonale sikkerheten. Denne delen av lovforslaget er godt balansert og har vært utredet gjennom flere utvalg, offentlige høringer og samfunnsdebatt.»

Norges institusjon for menneskerettigheter (NIM) uttaler:

> «Forslaget om tilrettelagt innhenting balanserer som et utgangspunkt to viktige interesser, som begge er vanskelige å måle. På den ene siden har staten ved E-tjenesten et behov for virkemidler for å kunne forsvare norske interesser mot blant annet cybertrusler og hybride trusler. Det vises i denne forbindelse til E-tjenestens nylige vurdering av aktuelle sikkerhetsutfordringer, offentliggjort 11. februar 2019. Norge er et av verdens mest digitaliserte samfunn, og hendelser i den senere tid, herunder Helse Sør-Øst-saken, har avdekket sårbarhet for angrep på vesentlig digital infrastruktur. Helse Sør-Øst-saken er et godt eksempel, fordi det viser at også privatlivsvernet vil være under trussel dersom sensitiv helseinformasjon ikke tilstrekkelig beskyttes mot målrettede dataangrep. Gitt at store deler av E-tjenestens virksomhet er hemmelig, er det også vanskelig for utenforstående å overprøve tjenestens behovsvurderinger og effekten av de tiltak som foreslås for å oppnå målet om å bedre beskytte norske interesser, særlig i den digitale sfære. Derfor er det så viktig at E-tjenesten er så åpne som de kan, både om sårbarheter, kapasiteter og udekkede etterretningsbehov, slik at dette så langt det er mulig kan underlegges reell demokratisk kontroll. Samtidig har NIM forståelse for at det er sider ved E-tjenestens virksomhet som ikke kan belyses. Departementet skal berømmes for å gå lenger enn tidligere i å belyse ulike forhold i denne sammenheng i høringsnotatet. NIM viser blant annet her til drøftelsen av alternativer til tilrettelagt innhenting i forslaget under punkt 11.7, som gir en systematisk fremstilling av etterretningsverdien av mindre inngripende alternativer. Dette er i utgangspunktet tillitsvekkende.
>
> På bakgrunn av blant annet disse beskrivelsene, legger NIM som et utgangspunkt til grunn at E-tjenesten har et reelt behov for å innføre et system med tilrettelagt innhenting, primært for å beskytte Norge mot hybride trusler og cyberangrep. NIM har heller ingen forutsetning for å overprøve høringsnotatets premiss om at dette ikke generelt kan gjøres på noen mindre inngripende måte som gir tilsvarende etterretningsverdi. Når det er sagt, er det neppe noen menneskerettslig plikt å innføre et slikt system.
>
> På den andre siden medfører lovforslaget et stort inngrep i nordmenns privatliv og personvern. I denne vektskålen ligger også vernet av ytringsfriheten, herunder pressefriheten og kildevernet, et menneskerettsområde som er avgjørende for et fungerende demokrati, og som forslaget har flere klare sider til.»

Norsk utenrikspolitisk institutt (NUPI) mener at høringsnotatet gir en god beskrivelse av det digitale trusselbildet. NUPI peker på at stater i dag i økende grad bruker digitale våpen til å spionere og kartlegge kritisk infrastruktur. Det har også vært flere tilfeller av digital sabotasje, altså at man lammer store deler av et samfunn gjennom hacking, med store økonomiske og samfunnsmessige konsekvenser. NUPI mener at departementets vurderinger av alternative løsninger er korrekte. De fremholder at det ikke er et reelt alternativ å videreføre dagens situasjon:

> «Det vil gjøre at Norges sikkerhet er prisgitt godviljen hos andre land til å dele essensiell og tidskritisk informasjon. I tillegg til de momenter som departementet legger frem under dette punktet, kan et bevisst valg om ikke å styrke nasjonal etterretning på digital kommunikasjon sende et uheldig signal om at Norge tar lett på slik sikkerhet. Det kan igjen vanskeliggjøre samarbeid med andre land, da de kan bli mindre villige til å dele informasjon. Norge bør ikke bli et «svakt ledd» i det vestlige sikkerhetssamarbeidet.»

Næringslivets sikkerhetsråd (NSR) peker på at Norge er et av verdens mest digitaliserte land. NSR mener at god etterretningskapasitet er ett av flere viktige elementer for å kunne beskytte den digitale infrastrukturen, og det er derfor viktig at Etterretningstjenesten har nødvendige og tidskritiske verktøy for å løse sitt oppdrag. NSR peker på

at Sverige og Storbritannia samler inn grenseoverskridende elektronisk kommunikasjon, og mener at norsk etterretningstjeneste bør ha mulighet til selv å samle data, og ikke være prisgitt samarbeidende nasjoners velvilje.

Tekna mener at tilrettelagt innhenting vil ha nytteverdi, men ser det som usikkert om nytteverdien vil stå i samsvar med de faktiske kostnadene. *SINTEF* uttaler:

> «I forbindelse med forslaget fra Lysne II-utvalget om digitalt grenseforsvar, etterlyste flere instanser, deriblant SINTEF, at mer målrettede og mindre inngripende alternativer til masseovervåkning ble vurdert. Dette er delvis redegjort for i nåværende høringsnotat, men dessverre er analysen av alternativene svært begrenset. Den tar etter vår mening primært utgangspunkt i Etterretningstjenestens behov, fremfor å avveie ulike samfunnsbehov.
>
> For å tilstrekkelig sikre et system er det viktig med tidligst mulig deteksjon av angrep og deling av denne informasjonen mellom relevante aktører for å sikre et godt forsvar. Samtidig er det like viktig at systemene er bygd for å motstå et angrep og håndtere at angrep lykkes. Det vil si at kritisk infrastruktur i Norge må utvikles med sikkerhet i fokus, og at en del av dette er å sørge for tilbakefallsløsninger hvor systemer i ytterste konsekvens kan opereres manuelt.
>
> Regjeringen har nylig bevilget 497 millioner NOK til NSM for, blant annet, videreutvikling av Varslingssystem for Digital Infrastruktur – VDI. I SINTEF har vi ikke gjort noen helhetlig analyse av alternativer til tilrettelagt innhenting, men for samfunnets behov fremstår VDI som en velegnet sensor for tidlig deteksjon av angrep mot kritisk infrastruktur. Etablering av tilrettelagt innhenting er estimert i høringsnotatet til å koste ca. 700 millioner NOK, med årlige driftsutgiftene på ca. 150 millioner NOK. Dette er en betydelig årlig merkostnad for et vidt digitalt barriereforsvar. SINTEF etterlyser en mer helhetlig analyse av hva man ville kunne oppnå av økt samfunnssikkerhet ved å bruke disse midlene på alternative sikringstiltak, som f.eks. å styrke VDI ytterligere, redusere medlemsavgiften for deltagelse i VDI, styrke funksjonen for utveksling av trusselinformasjon og innføre en stor satsning på å bedre sikkerheten i kritisk infrastruktur.»

Amnesty International finner det ikke sannsynliggjort at det ikke finnes andre, mindre inngripende alternativer. I samme retning uttaler *Telia Norge AS* seg.

Befalets fellesorganisasjon (BFO) viser til at digital spionasje stadig øker i omfang og alvorlighet, og at denne typen aktivitet potensielt kan endres til et sabotasjeformål. Fremveksten av internasjonal ekstremisme og terrortrusselen skaper utfordringer på tvers av landegrenser og myndighetsorganer fordi aktivitet skjules i mengden av sivil trafikk. BFO finner det positivt at lovforslaget hjemler metoder som antas å styrke den nasjonale evnen til å detektere og håndtere trusler i det digitale rom. *Norges offisers- og spesialistforbund (NOF)* fremholder at med skiftende internasjonale trender, inkludert overgang fra bruk av papir til elektronisk kommunikasjon, må Etterretningstjenesten ha et rammeverk som er oppdatert og fremtidsrettet.

Fredrik Vingsnes, Marie Anglevik og Marita Haug Haaland, medlemmer av ICJ-Norge, mener at behovet for innsyn i datatrafikk, i en eller annen form, definitivt er til stede. De fremholder samtidig at muligheten til å benytte Internett uten tanke for hvem som følger med, har en stor egenverdi som det er verdt å beskytte.

International Business Machines AS (IBM) viser til at det digitale domenet blir stadig viktigere for så vel offentlig som privat virksomhet både av individuell og samfunnsmessig karakter. IBM mener at Etterretningstjenesten, innenfor akseptable og forsvarlige rammer, må settes i stand til å foreta attribusjon, motivkartlegging, inngående analyser og kategorisering av anslag. IBM påpeker at det av flere grunner er vanskelig å komme bort fra midtpunktinnhenting av rådata som en teknisk konsekvens av digital grensekontroll.

11.4.3 Departementets vurdering

Departementet fastholder vurderingen i høringsnotatet av behovet for tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon. På grunn av den teknologiske utviklingen har myndighetene i dag en begrenset evne til å oppdage, følge, varsle og motvirke utenlandske trusler mot Norge. Etter departementets syn er det nødvendig å styrke denne evnen gjennom tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon. Kombinasjonen av lagring av metadata i bulk og målrettet innhenting av innholdsdata ventes å gi stor etterretningsmessig verdi.

Høringen støtter opp om vurderingen i høringsnotatet. Flere høringsinstanser peker på at

Norge er et av verdens mest digitaliserte land, og at det digitale domenet i dag brukes som en arena for spionasje og sabotasje. Det gis uttrykk for at Etterretningstjenesten må settes i stand til å følge den teknologiske utviklingen. Departementet deler disse synspunktene.

I høringsnotatet ble det vurdert at ingen alternative løsninger kan møte behovet på en mindre inngripende måte enn Lysne II-utvalgets anbefaling. Høringen gir i hovedsak støtte til denne vurderingen. Departementet viser særlig til høringsuttalelsene til *Nasjonal sikkerhetsmyndighet* og *NUPI*. Noen høringsinstanser er ikke overbeviste om at det ikke finnes mindre inngripende alternativer, men disse har i liten grad skissert andre løsninger. Et unntak er *SINTEF*, som særlig peker på en styrking av Varslingssystemet for digital infrastruktur (VDI) som et alternativ. Departementet er enig med SINTEF i at VDI er viktig for å sikre kritisk infrastruktur. VDI har derfor blitt styrket i den senere tid, og det må fortløpende vurderes om systemet bør styrkes ytterligere. Det er samtidig klart at VDI ikke kan møte behovet som ligger til grunn for forslaget om tilrettelagt innhenting. Et sentralt formål med tilrettelagt innhenting er å få oversikt over den samlede aktiviteten til utenlandske trusselaktører i det digitale domenet, og VDI gir ikke tilstrekkelig mulighet til dette. VDI er utelukkende innrettet mot å oppdage skadevare. Det er et viktig bidrag til å trygge nasjonale sikkerhetsinteresser, men vil ikke kunne ivareta Etterretningstjenestens oppgaver knyttet til trusler i det digitale rom. Det vil heller ikke kunne bidra til å løse andre oppgaver, for eksempel å motvirke internasjonal terrorisme eller spredning av masseødeleggelsesvåpen.

Etter departementets vurdering er det ikke et reelt alternativ å videreføre dagens situasjon, hvor Norge i stor grad er avhengig av å motta informasjon fra andre land. Internasjonalt etterretningssamarbeid og informasjonsutveksling er viktig for Norge, men som et fritt og selvstendig land bør vi så langt som mulig søke å unngå å være prisgitt andre nasjoners prioriteringer og velvilje. Selvstendig etterretningsevne er vesentlig for å sikre norske myndigheter et forsvarlig beslutningsgrunnlag i sikkerhets-, forsvars- og utenrikspolitiske saker. Med egen tilgang reduseres risikoen for å bli utsatt for ufullstendig eller villedende informasjon. Som påpekt av *NUPI*, er det dessuten viktig å unngå at Norge blir et svakt ledd i det vestlige sikkerhetssamarbeidet.

Departementet fastholder etter dette at de alternative løsningene som er utredet, vil gi liten eller ingen etterretningsmessig verdi. Departementet kjenner heller ikke til andre løsninger som kan møte behovet på en mindre inngripende måte.

Selv om de fleste høringsinstansene anerkjenner behovet for tilrettelagt innhenting, peker flere på at tiltaket har problematiske sider sett fra et personvern- og menneskerettighetsperspektiv. Departementet er enig i dette. Nytten av tiltaket må veies mot skadevirkningene det kan ha. Spørsmålet er om tiltaket er *nødvendig i et demokratisk samfunn*. Departementet viser til vurderingen i punkt 11.5.3.4, hvor departementet foretar den brede interesseavveiningen som våre menneskerettslige forpliktelser gir anvisning på. Departementet konkluderer der med at tiltaket er nødvendig i et demokratisk samfunn. Det legges avgjørende vekt på de legitime samfunnsmessige behovene som begrunner inngrepet, sammenholdt med summen av kontrollmekanismer og garantier mot misbruk og vilkårlighet.

I lys av høringen understreker departementet at tilrettelagt innhenting ventes å ha stor nytteverdi til tross for at den teknologiske utviklingen går i retning av mer bruk av kryptering. Departementet støtter denne utviklingen, som er viktig for personvernet, kommunikasjonsvernet og informasjonssikkerheten.

11.5 Menneskerettslige rammer

11.5.1 Høringsnotatet

De menneskerettslige rammene for tilrettelagt innhenting drøftes i høringsnotatet punkt 11.8.2. Det vises til at det særlig er retten til respekt for privatliv og kommunikasjon som utgjør rammen for tilrettelagt innhenting, men at også andre menneskerettigheter kan berøres av tiltaket, herunder særlig ytrings- og informasjonsfriheten.

I høringsnotatet vises det til at tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon vil utgjøre et inngrep i retten til respekt for privatliv og kommunikasjon, men at grunnlovsvernet ikke er absolutt. Inngrepet kan tillates dersom det har hjemmel i lov, forfølger et legitimt formål og er forholdsmessig. Det konkluderes med at vilkårene er oppfylt, og 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.

11.5.2 Høringsinstansenes syn

Flere høringsinstanser har merknader knyttet til de menneskerettslige rammene for forslaget. Det gis uttrykk for delte meninger. Noen mener at forslaget ikke er i tråd med Norges menneskerettslige forpliktelser, mens andre reiser spørsmål om dette eller peker på at den rettslige situasjonen er uavklart. Flere høringsinstanser gir innspill til endringer som kan bidra til å imøtekomme menneskerettslige krav.

Norges institusjon for menneskerettigheter (NIM) mener at det i skrivende stund er rettslig uavklart om, og under hvilke betingelser, Den europeiske menneskerettsdomstolen (EMD) vil akseptere bulkinnsamling, og uttaler:

> «I ikke-rettskraftige dommer har domstolen lagt til grunn at det ikke finnes noen absolutte skranker mot innføringen av et system, men at det krever at sterke og effektive kontrollmekanismer er på plass. Det er i så fall grunn til å tro at EMD vil tilkjenne staten en ganske vid skjønnsmargin med hensyn til valg av system. Testen vil trolig bestå i om det er oppstilt mekanismer som i tilstrekkelig grad motvirker misbruksrisikoen. Hvilke mekanismer som er tilstrekkelige kommer an på misbruksrisikoen ved det aktuelle systemet. Hensett til omfanget av overvåkingskapasiteten må den iboende misbruksrisikoen i bulkinnsamlingssystemer anses svært høy. Det vil kunne stille svært strenge krav til sikkerhetsmekanismer, muligens også strengere krav enn EMD har lagt til grunn i tidligere saker.
>
> Som også påpekt av Lysne II-utvalget, er det hårfine avveininger det er snakk om, og selv små justeringer i de aktuelle rettsikkerhetsmekanismene vil kunne få som konsekvens at et slikt system anses menneskerettstridig. Det er derfor grunnleggende i den videre prosessen at alle steiner snus for å sørge for at reelle og operative garantier mot misbruk og at det etableres effektive rettsmidler ved rettsbrudd.
>
> Dette har også vært premissgivende for utformingen av NIMs høringsuttalelse. Vi har tatt utgangspunkt i forslaget slik det foreligger, og bestrebet oss på å komme med konkrete innspill til hvordan forslaget bedre kan ivareta menneskerettslige krav. Vi har lagt stor vekt på den grunnleggende betydningen av å sikre tilstrekkelig kapasitet og kompetanse hos kontrollmekanismene.
>
> Vi har vanskelig for å se at det i denne kompliserte konteksten med raskt endrede rettslige og tekniske premisser er mulig å fremme noen absolutte synspunkter på hvorvidt forslaget (kun basert på hvordan det ser ut på papiret) vil stå seg i en menneskerettslig prøving, men vi mener at forslaget må endres på en rekke punkter for å bedre ivareta menneskerettslige krav.»

Når det gjelder statens menneskerettslige handlingsrom, oppsummerer NIM slik:

> «Generelt sett avtegner praksis et bilde hvor staten har stort handlingsrom i valg av type overvåkingssystem for å ivareta nasjonal sikkerhet, mer begrenset handlingsrom i implementeringen og bruken av overvåkingssystemet. Hvis og i den grad overvåkingssystemet ikke bare rettes mot utenlandske forhold, men også brukes overfor egne borgere, begrenses handlingsrommet ytterligere og krav til sikkerhetsmekanismer skjerpes.
>
> Egenarten ved bulkinnsamling innebærer at det har et betydelig misbrukspotensial overfor egne borgere, selv om det i utgangspunktet er rettet mot utenlandske forhold. NIM mener det er nærliggende at dette vil medføre at EMD vil vurdere kravet til sikkerhetsmekanismer strengt. Det er også en mulighet for at domstolen vil kunne oppstille særegne krav til sikkerhetsmekanismer som adresserer særegenhetene ved bulkinnsamlingssystemer. Dette bør departementet være særlig oppmerksom på i sin videre behandling av saken.»

Dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors mener at det kan reises spørsmål om lovforslaget tilfredsstiller de skranker som EMD har satt. De uttaler at de mange og vage vilkårene som domstolen skal vurdere, kan føre til at en effektiv kontroll ikke lar seg realisere. *Advokatforeningen* gir uttrykk for lignende synspunkter.

Datatilsynet mener at forslaget strider mot Norges menneskerettslige forpliktelser. Etter tilsynets oppfatning tilfredsstiller ikke forslaget kravet til hjemmel i lov på grunn av manglende klarhet og forutberegnelighet, og kontrollsystemet er så svakt at det ikke kan anses å veie opp mot inngrepet i retten til privatliv. Tilsynet mener at den manglende kartleggingen av samfunnsmessige fordeler og ulemper ved forslaget gjør det vanskelig å kunne konkludere med om forslaget er proporsjonalt. *Piratpartiet* slutter seg til tilsynets synspunkter. *Elektronisk Forpost Norge* og flere

privatpersoner mener også at forslaget strider mot Norges menneskerettslige forpliktelser.

Norsk Presseforbund, *Norsk Journalistlag*, *Norsk Redaktørforening* og *NRK* mener at forslaget strider mot menneskerettslige forpliktelser knyttet til kildevernet.

Kripos antar at det foreslåtte tiltaket vil kunne tilfredsstille de ulike sider av lovskravet, men mener at grunnvilkårene for målsøking og målrettet innhenting i lovutkastet kapittel 5 bør angis mer presist.

11.5.3 Departementets vurdering

11.5.3.1 Menneskerettslige utgangspunkter

De menneskerettslige rammene for tilrettelagt innhenting følger i hovedsak av Grunnloven, Den europeiske menneskerettskonvensjon (EMK) og FNs konvensjon om sivile og politiske rettigheter (SP). Dessuten kan enkelte EØS-rettslige forpliktelser ha en side til menneskerettighetene. EØS-retten behandles i punkt 11.6.

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, som ifølge menneskerettsloven §§ 2 og 3 gjelder som norsk lov som ved motstrid går foran bestemmelser i annen lovgivning.

Retten til respekt for privatliv og kommunikasjon utgjør den sentrale menneskerettslige rammen for tilrettelagt innhenting, men også andre menneskerettigheter kan berøres. Dette gjelder særlig ytrings- og informasjonsfriheten, herunder kildevernet. Også forenings- og forsamlingsfriheten og religionsfriheten kan etter omstendighetene berøres. Vilkårene for inngrep i de ulike rettighetene er i grove trekk de samme, og departementet vil derfor i det følgende konsentrere drøftelsen rundt retten til respekt for privatliv og kommunikasjon.

Departementet legger til grunn at tilrettelagt innhenting utgjør et inngrep i retten til respekt for privatliv og kommunikasjon. Det er ikke tvilsomt at både innholdsdata og metadata er kommunikasjon som omfattes av rettighetsvernet. Innsamling, lagring, undersøkelse og bruk vil normalt regnes som selvstendige inngrep. Etter omstendighetene kan lovgivningen i seg selv også regnes som et inngrep.

Grunnlovsvernet av privatliv og kommunikasjon gjelder ikke absolutt. Stortinget valgte formuleringen «rett til respekt for» for å synliggjøre at bestemmelsen ikke står i veien for lovlig etterretning (Innst. 186 (2013–2014) side 27). Heller ikke vernet etter de internasjonale konvensjonene gjelder absolutt. Departementet tar i det følgende utgangspunkt i grunnlovsvernet, men ser også hen til de internasjonale konvensjonene.

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 HR-2015-206-A avsnitt 60. Departementet vil i det følgende drøfte hvorvidt disse tre vilkårene er oppfylt.

11.5.3.2 Legitimt formål

Det følger av EMK artikkel 8 nr. 2 at inngrep kan godtas blant annet av hensyn til den nasjonale sikkerhet eller offentlige trygghet. Et av formålene 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 (lovforslaget § 1-1 bokstav a). Tilrettelagt innhenting vil styrke Etterretningstjenestens evne til å løse sine oppgaver etter lovforslaget kapittel 3. Alle disse oppgavene bidrar til å ivareta nasjonale sikkerhetsinteresser. På denne bakgrunn konkluderer departementet med at kravet til legitimt formål er oppfylt.

Departementet tilføyer at det i den konkrete forholdsmessighetsvurderingen som etter lovforslaget § 5-4 må foretas i hver enkelt sak, vil kunne ha betydning hvilken oppgave innhentingen begrunnes i. I vurderingen skal det blant annet tas hensyn til sakens betydning. Hvis saken gjelder en trussel som nevnt i lovforslaget § 3-1, vil det normalt kunne begrunne et sterkere inngrep enn dersom saken gjelder forhold og utviklingstrekk i andre stater og regioner etter lovforslaget § 3-2. Det vises til punkt 11.8.1.3 for en nærmere drøftelse.

11.5.3.3 Hjemmel i lov

Kravet til hjemmel i lov kan ses i sammenheng med det generelle legalitetsprinsippet som følger av Grunnloven § 113. Prinsippet skal legge til rette for forutberegnelighet for borgerne, motvirke vilkårlighet og usaklig forskjellsbehandling, og sikre at forvaltningen holder seg innenfor rammen av fullmaktene gitt av folkets representanter i Stortinget.

Hjemmelskravets *formelle side* vil være oppfylt gjennom at inngrepet vil ha grunnlag i lov vedtatt

av Stortinget i samsvar med Grunnloven § 75 bokstav a.

Kravet til hjemmel i lov har også en *kvalitativ side*. Det stilles for det første visse krav til lovgivningens klarhet og presisjon. Departementet har søkt å utforme lovforslaget så klart og presist som mulig. Det er samtidig på det rene at hensynet til klarhet og presisjon må veies mot andre legitime hensyn ved utformingen av lovbestemmelser. Det er ikke i strid med menneskerettighetene at lovgivningen bygger på kriterier som er mer eller mindre vage og skjønnsmessige. Det er flere grunner til dette. Lovgivningen må utformes på en måte som gjør at den kan holde takt med utviklingen. Det har for eksempel vært et siktemål å utforme lovforslaget på en teknologinøytral måte. På dette samfunnsområdet er det også et legitimt behov for å skjerme detaljer knyttet til metoder og kapasiteter, blant annet for å unngå at etterretningsmål kan innrette seg slik at de unndrar seg innhentingen.

Departementet tar på alvor at noen høringsinstanser, herunder *Datatilsynet*, mener at forslaget som ble sendt på høring ikke oppfyller menneskerettslige krav til klarhet og presisjon. Departementet har på bakgrunn av høringen gått gjennom lovforslaget med sikte på å gjøre det klarere og mer presist, spesielt der det er reist kritikk mot spesifikke bestemmelser.

Hjemmelskravet tilsier at lovgivningen ikke må være for fragmentarisk. Det er samtidig ikke til å komme fra at lovgivning av et visst omfang i noen grad vil være fragmentarisk. I lovforslaget vil bestemmelsene om tilrettelagt innhenting i kapittel 7 og 8 måtte leses i sammenheng blant annet med reglene om Etterretningstjenestens oppgaver i kapittel 3, innhentingsforbudene i kapittel 4, grunnvilkårene i kapittel 5 og reglene om behandling av personopplysninger i kapittel 9. Etter departementets vurdering har ikke lovforslaget en så fragmentarisk karakter at det er i strid med hjemmelskravet.

Kravet til hjemmel innebærer også et krav til rimelige garantier mot vilkårlighet og misbruk, se for eksempel Høyesteretts flertall i HR-2014-2288-A avsnitt 30 med videre henvisninger til praksis fra EMD. Departementet har lagt vekt på å utforme kontrolltiltak og rettssikkerhetsgarantier som møter de menneskerettslige kravene, og viser til omtalen av disse i punkt 11.9 til 11.11. Lovforslaget følger opp flere forslag fra høringsinstansene som tar sikte på å styrke kontrollen. Rimelige garantier mot vilkårlighet og misbruk har stor betydning også for tiltakets forholdsmessighet, og disse omtales og vurderes derfor nærmere i punkt 11.5.3.4. Departementet legger til grunn at vurderingen av lovskravet og forholdsmessighetsvurderingen i noen grad glir over i hverandre.

Departementet konkluderer etter dette med at forslaget tilfredsstiller kravet til hjemmel i lov.

11.5.3.4 Forholdsmessighet

Det tredje vilkåret som må være oppfylt for at inngrepet skal kunne aksepteres, er kravet til forholdsmessighet. Det skal foretas en sammensatt proporsjonalitetsvurdering, se for eksempel 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 hvorvidt tiltaket er *nødvendig i et demokratisk samfunn*, jf. EMK artikkel 8 nr. 2. Dette vurderingstemaet kan igjen deles opp i spørsmål om hvorvidt tiltaket er egnet, nødvendig og forholdsmessig, se for eksempel HR-2018-104-A avsnitt 23. Departementet legger til grunn at spørsmålene i noen grad glir over i hverandre. Vurderingene bygger på, og må leses i sammenheng med, de beskrivelser og vurderinger som fremgår av proposisjonen for øvrig.

Det første spørsmålet er hvorvidt tiltaket er *egnet*.

Departementet finner det ikke tvilsomt at tiltaket er egnet. Det vises til punkt 11.4.3, hvor det fremgår at tilrettelagt innhenting ventes å gi stor etterretningsmessig verdi selv med økt bruk av kryptering. Uavhengige ekspertutredninger og erfaring fra andre land tilsier også at tiltaket er egnet. Det vises til punkt 11.1 og 11.3.

Det neste spørsmålet er hvorvidt tiltaket er *nødvendig*.

Etter departementets vurdering er det et presserende behov for tilrettelagt innhenting. I dag mangler norske myndigheter tilgang til en vesentlig kilde til informasjon. Tilgangen vil styrke vår evne til å oppdage, følge, varsle og motvirke utenlandske trusler mot Norge, og bidra til å gi myndighetene et forsvarlig beslutningsgrunnlag i sikkerhets-, forsvars- og utenrikspolitiske saker. På grunn av mangelen på tilgang er vi i dag i for stor utstrekning avhengige av informasjon fra andre land, noe som har en rekke uheldige konsekvenser, jf. punkt 11.4.3. Egen tilgang vil styrke Norges selvstendige etterretningsevne, noe som er sentralt for et fritt og selvstendig land.

Det ligger i nødvendighetskravet at det ikke må finnes mindre inngripende tiltak som vil ha samme effekt. Departementet har vurdert alternativer til tilrettelagt innhenting i punkt 11.4.3. Etter

departementets vurdering finnes det ikke mindre inngripende tiltak som vil ha samme nytte som tilrettelagt innhenting.

Departementet mener etter dette at tiltaket er nødvendig.

Det avgjørende spørsmålet blir etter dette hvorvidt tiltaket er *forholdsmessig*. Det skal her foretas en bredere interesseavveining, se for eksempel HR-2015-2016-A 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 tilføyer at de beskyttede individuelle interessene er sentrale ikke bare for enkeltmennesket isolert sett, men også for å bevare et fritt, demokratisk samfunn.

Departementet tar som utgangspunkt at sterke legitime samfunnsbehov begrunner tiltaket. Loven skal 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 Etterretningstjenesten tilgang på informasjon som tjenesten må ha for å kunne utføre sine oppgaver, og slik bidra til å oppfylle lovens formål. Det følger av dette at tiltakets kjerne er vern av vår demokratiske rettsstat og de grunnleggende verdiene, rettighetene og frihetene som denne bygger på og beskytter. Departementet har redegjort for behovet for norsk utenlandsetterretning i kapittel 3. Som drøftet i punkt 11.4.3, er det av flere grunner behov for å styrke Norges selvstendige etterretningsevne.

Dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors fremholder at lovforslaget bryter med rettsstatlig tradisjon fordi innhentingen vil ramme et ukjent antall mennesker som det ikke kan knyttes noen mistanke til. Departementet bemerker at etterretningsvirksomhet som ikke knytter seg til mistanke mot bestemte personer kan være nødvendig for å beskytte samfunnet mot alvorlige trusler. Å oppdage slike trusler og hvem som står bak dem, er en sentral oppgave for myndighetene. Tilrettelagt innhenting vil styrke evnen til å løse denne oppgaven. Etterretningsvirksomhet med tilstrekkelige kontrollmekanismer og garantier mot misbruk og vilkårlighet bryter ikke med rettsstatlig tradisjon, men må snarere regnes som et rettsstatlig svar på alvorlige trusler mot demokratiet og rettsstaten. Som påpekt i punkt 11.3, har en rekke demokratiske rettsstater som står Norge nært, funnet det nødvendig å innføre lignende tiltak.

Det er samtidig ingen tvil om at tilrettelagt innhenting er et inngrep som potensielt kan ha negative virkninger for den demokratiske rettsstaten. *Datatilsynet* og *Norges institusjon for menneskerettigheter (NIM)* viser til at EMD i flere dommer har påpekt risikoen for at «a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it», se for eksempel *Weber og Saravia mot Tyskland* avsnitt 106. Departementet tar denne risikoen alvorlig. Som påpekt i punkt 4.1, skal etterretningsvirksomhet bidra til å beskytte vårt samfunns grunnleggende verdier på en måte som lar seg forene med dem.

Forslaget om innhenting og lagring av metadata i bulk etter lovforslaget § 7-7 er det mest problematiske fra et personvernperspektiv. Inngrepet avhjelpes i noen grad av plikten til å søke å hindre lagring av overskuddsinformasjon gjennom utvalg og filtrering (lovforslaget § 7-6, se nærmere punkt 11.8.2) og den maksimale lagringstiden på 18 måneder (lovforslaget § 7-7 tredje ledd). I dagens teknologiske situasjon vil det imidlertid lagres store mengder metadata om norsk innenlandsk kommunikasjon som ikke er relevant for etterretningsformål. Selv om det ikke er tale om innhenting og lagring av innholdsdata i bulk, vil også analyse og sammenstilling av metadata kunne avsløre sensitive forhold om enkeltpersoner, slik blant andre *Datatilsynet* fremholder i sin høringsuttalelse, se nærmere punkt 11.8.4. Inngrepet må derfor regnes som betydelig.

Innhenting, lagring og analyse av testdata i et korttidslager etter lovforslaget § 7-5 er også inngripende i personvernet, spesielt fordi det er tale om ufiltrert informasjon. Slik virksomhet er likevel avgjørende for drift av systemet, blant annet for å kunne utvikle og oppdatere filtrene som skal hindre lagring av overskuddsinformasjon. Det foreslås strenge og ufravikelige tidsbegrensninger for de ufiltrerte uttrekkene, noe som begrenser misbrukspotensialet. Det foreslås også uttrykkelig lovfestet at informasjonen utelukkende kan brukes til teknisk understøttelse, det vil si at informasjonen aldri kan brukes til etterretningsproduksjon eller til andre formål. For å støtte opp om dette forbudet foreslås det blant annet at testinnhenting og annen teknisk understøttelse bare kan utføres av et begrenset antall tekniske spesialister som har mottatt særskilt opplæring og som ikke har etterretningsanalyse som oppgave. Departementet viser til punkt 11.8.3.

Målrettet innhenting og lagring av innholdsdata etter lovforslaget § 7-9 vil kunne være inngripende for dem det gjelder, men gir etter departe-

mentets vurdering ikke opphav til de samme betenkeligheter med hensyn til personvernet som innhenting og lagring av metadata og testdata. Selv om tilgang til innholdsdata isolert sett normalt må regnes som mer inngripende enn tilgang til metadata, vil ikke innholdsdata innhentes og lagres i bulk, og denne innhentingen er derfor i sin natur mer spisset. Departementet viser til punkt 11.8.6 for en nærmere beskrivelse.

På grunn av inngrepets karakter og omfang foreslår departementet en rekke materielle og prosessuelle vilkår for tilgang til og bruk av informasjonen, samt andre garantier mot misbruk og vilkårlighet. Departementet legger på samme måte som *NIM* til grunn at det ut fra EMDs praksis beror på en helhetlig vurdering hvorvidt et nasjonalt overvåkingssystem i tilstrekkelig grad begrenser risikoen for misbruk. Statene har et visst handlingsrom ved utformingen av systemet. Departementet har ved utformingen av forslagene blant annet sett hen til EMDs praksis og lovgivningen i nærstående land. Departementet har også sett hen til internasjonale anbefalinger, blant annet *Report on the democratic oversight of the Security Services* og *Report on the democratic oversight of signals intelligence agencies* fra Den europeiske kommisjonen for demokrati gjennom lovgivning (Veneziakommisjonen).

Departementet viser for det første til at tilrettelagt innhenting er begrenset til de formål som følger av lovforslaget kapittel 3. Dette innebærer at tilrettelagt innhenting bare kan brukes for utenlandsetterretningsformål. Det oppstilles innhentingsforbud i lovutkastet kapittel 4 som tydeliggjør den strenge formålsbegrensningen, og i kapittel 5 foreslås det grunnvilkår for innhenting som blant annet innebærer krav til forholdsmessighet.

Videre foreslås det blant annet regler om maksimal lagringstid (§ 7-7 tredje ledd), krav til skikkethet og opplæring (§ 7-8 andre ledd), krav til systematiske tiltak for internkontroll og aktivitetslogger (§ 7-10), forbud mot diskriminering (§ 9-4), sletteplikt (§ 9-8), informasjonssikkerhet (§ 9-9) og taushetsplikt (§ 11-2).

Lovforslaget gir et særlig vern for journalistisk og annen fortrolig kommunikasjon (§§ 9-5 og 9-6). Slik kommunikasjon skal som den klare hovedregel ikke behandles. Det vises til drøftelsen i punkt 12.8.

Departementet legger vekt på at forslaget inneholder en rekke kontrollmekanismer og rettssikkerhetsgarantier. Forslaget stiller for det første krav om forhåndsgodkjennelse av en domstol etter reglene i lovforslaget kapittel 8, se nærmere punkt 11.9. 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 generalistdommere som behandler alle typer saker, reduseres risikoen for at dommerne over tid vil identifisere seg med tjenestens virksomhet, samtidig som det ved at sakene samles i Oslo tingrett som førsteinstans legges til rette for at dommerne vil opparbeide seg en erfaring med sakstypen som gir grunnlag for en reell kontroll.

Retten skal foreta en fullstendig legalitetskontroll på bakgrunn av vilkår som er fastsatt i loven, herunder at innhentingen ligger innenfor tjenestens oppgaver, er forholdsmessig og ikke strider mot noen av innhentingsforbudene. Kjennelsen skal begrunnes og kan ankes til en overordnet domstol. Retten skal som hovedregel oppnevne en særskilt advokat som skal målbære den enkeltes rettigheter og samfunnets interesser i saken, for eksempel personvernhensyn, og det kan avholdes muntlige forhandlinger dersom retten ser behov for det. Tillatelser skal ikke gis for lengre tid enn nødvendig, og det foreslås i tillegg absolutte lengstefrister for varighet. Søk og innhenting skal avbrytes dersom lovens vilkår ikke lenger er oppfylt.

Noen høringsinstanser har påpekt at flere av vilkårene er utformet på en måte som kan gjøre det vanskelig for domstolen å føre en reell kontroll, blant annet fordi vilkårene er vage og skjønnsmessige. Departementet har forståelse for synspunktet, og er enig i at det kan være vanskelig for domstolen å overprøve enkelte vurderinger knyttet til vilkår som av ulike grunner må være mer eller mindre vage og skjønnsmessige. Departementet mener like fullt at domstolens forhåndskontroll vil være en reell og viktig garanti mot misbruk og vilkårlighet, særlig på grunn av den disiplinerende virkningen domstolskontrollen må antas å ha. Det vises til drøftelsen i punkt 11.9.1.3.

Domstolens forhåndskontroll må ses i sammenheng med kontrollen som skal utføres av EOS-utvalget. Utvalget skal etter lovforslaget § 7-11 føre løpende kontroll med tilrettelagt innhenting, se nærmere punkt 11.10. Som det fremgår der, er det en forutsetning for forslaget at utvalgets sekretariat styrkes betydelig, spesielt med hensyn til teknologisk kompetanse. I tråd med utvalgets høringsuttalelse foreslås det dessuten å lovfeste en plikt for Etterretningstjenesten til å legge til rette for kontrollen gjennom tekniske løsninger, jf. lovforslaget § 7-11 tredje ledd.

EOS-utvalget skal kontrollere at bestemmelsene i loven etterleves, herunder at søk gjennomføres i tråd med rettens kjennelse og at testdata

utelukkende brukes til teknisk understøttelse. Hvis utvalget mener at en innhentingsaktivitet er ulovlig og må opphøre, og Etterretningstjenesten ikke retter seg etter utvalgets syn, foreslås det at utvalget kan ta saken inn for domstolene, som vil ha myndighet til å pålegge opphør av den ulovlige virksomheten og sletting av ulovlig innhentet informasjon. Departementet viser til lovforslaget § 7-12.

EOS-utvalget vil også føre etterfølgende kontroll med tilrettelagt innhenting i samsvar med EOS-kontrolloven. Etterfølgende domstolskontroll kan også være aktuelt. Som det redegjøres for i punkt 4.4.2, er det en relativt vid klage- og søksmålsadgang for personer som mener seg utsatt for ulovlig overvåkning.

I tillegg til den uavhengige kontrollen ved domstolene og EOS-utvalget vil det også gjelde andre kontrollmekanismer, blant annet tjenestens internkontroll og departementets forvaltningskontroll, se nærmere punkt 11.11. Innenfor sitt tilsynsområde vil dessuten Nasjonal kommunikasjonsmyndighet (Nkom) føre tilsyn med ekomtilbydernes utøvelse av tilretteleggingsplikten, jf. lovforslaget § 2-8 andre ledd andre punktum, se nærmere punkt 11.8.7.3.

Departementet har tatt i betraktning risikoen for formålsutglidning, det vil si risikoen for at tilgangen blir tatt i bruk til andre formål enn tilsiktet. Hvis tilgangen brukes på en måte som strider mot loven, vil det være misbruk. Det vil for eksempel være misbruk hvis en tjenesteperson i Etterretningstjenesten bruker tilgangen for å «snoke». Det vil også være misbruk hvis en tjenesteperson bruker tilgangen for å skaffe informasjon til politiet om lovbrudd som det ligger utenfor Etterretningstjenestens oppgaver å innhente informasjon om (for eksempel narkotikalovbrudd), til skattemyndighetene om skatteunndragelse eller til trygdemyndighetene om trygdesvindel. Bruk i strid med loven vil kunne straffes som tjenestefeil eller misbruk av offentlig myndighet i medhold av straffeloven §§ 171 til 173 eller som brudd på tjenesteplikt etter militær straffelov § 77. Misbruk vil også kunne få arbeidsrettslige og disiplinærrettslige konsekvenser i medhold av statsansatteloven § 25 følgende og disiplinærloven § 1 første ledd.

Faren for misbruk kan aldri helt fjernes, men departementet har søkt å redusere risikoen på flere måter. Kontrollmekanismene som er beskrevet over, står sentralt. Det foreslås i tillegg forbud mot å utlevere overskuddsinformasjon og forbud mot å bruke informasjon fra tilgangen som grunnlag for strafferettslige sanksjoner (lovforslaget §§ 7-13 og 7-14). Det foreslås også forbud mot innhenting med politiformål (lovforslaget § 4-8) og forbud mot å bruke tilgangen i medhold av reglene om Forsvarets bistand til politiet (lovforslaget § 10-7 andre punktum). Alle disse bestemmelsene støtter opp om formålsbegrensningen til utenlandsetterretning, og motvirker risikoen for at tilrettelagt innhenting kan brukes til å overvåke egen befolkning.

Hvis Etterretningstjenesten, til tross for formålsbegrensningen som det er redegjort for over, kommer i besittelse av overskuddsinformasjon som det kan være nødvendig å utlevere for å forhindre alvorlig fare for noens liv, helse eller frihet, kan det være en menneskerettslig plikt å utlevere informasjonen. Det samme gjelder informasjon som kan hindre at noen blir uriktig tiltalt eller domfelt for en straffbar handling. Slik utilsiktet sekundærbruk må etter departementets syn aksepteres, og en adgang til dette følger av lovforslaget § 7-13 andre ledd. Unntaket er meget snevert og skal anvendes med stor varsomhet. Departementet understreker at bruk av tilgangen med sikte på å komme i besittelse av slik informasjon, vil være misbruk. Det vises til nærmere drøftelse i punkt 11.12.3.

Det kan i en viss betydning kalles formålsutglidning også hvis Stortinget på et senere tidspunkt endrer loven for å åpne for bruk av tilgangen til andre formål enn det som var utgangspunktet. Departementet mener at muligheten for senere lovendringer ikke er et argument som med vekt taler mot lovforslaget. Stortingets lovgivende myndighet er et grunnleggende trekk ved vår demokratiske styreform, jf. Grunnloven § 49, som bestemmer at folket utøver den lovgivende makt ved Stortinget. Menneskerettighetene, slik de er vernet av Grunnloven og internasjonale konvensjoner som gjelder som norsk lov etter menneskerettsloven, vil sette grenser for hvilke endringer som kan gjennomføres.

Departementet mener etter dette at risikoen for formålsutglidning ikke er et avgjørende argument mot forslaget.

Noen høringsinstanser peker på risikoen for at systemet kan falle i gale hender ved en udemokratisk maktovertakelse. Det er ingen tvil om at det kan ha alvorlige konsekvenser dersom en fiendtlig aktør får kontroll over systemet. Samtidig er ikke en slik risiko unik for dette systemet, og risikoen må etter departementets syn håndteres med utgangspunkt i alminnelige regler. Departementet viser i den forbindelse til lovforslaget § 11-6, som fastslår at Etterretningstjenesten skal utarbeide og vedlikeholde beredskapsplaner, blant annet

forberede tiltak for å sikre at tjenestens informasjon og systemer ikke kommer under kontroll av uvedkommende i krise eller væpnet konflikt. Departementet mener på denne bakgrunn at risikoen ikke med avgjørende vekt taler mot forslaget.

Risikoen for at tiltaket vil ha en nedkjølende effekt på ytrings- og informasjonsfriheten har vært en sentral del av departementets vurdering. *Datatilsynet* har under høringen kritisert departementet for ikke i tilstrekkelig grad å ta risikoen på alvor. Med en nedkjølende effekt menes i korte trekk at den enkelte vil modifisere eller sensurere ytringene sine, eller helt unnlate å ytre seg, på grunn av frykt for eller kunnskap om at ytringene overvåkes. Departementet tar risikoen for en slik effekt alvorlig. Ytringsfriheten er en forutsetning for demokratiet og for menneskets sannhetssøken, personlige autonomi og frihet. Risikoen for en nedkjølende effekt på ytringsfriheten er derfor en betydelig innvending mot forslaget. Risikoen kan etter departementets syn likevel ikke tillegges avgjørende vekt, gitt de legitime samfunnsbehovene som begrunner inngrepet.

Departementet har sett hen til at tiltaket vil innebære en viss byrde for tilbydere som omfattes av tilretteleggingsplikten etter lovforslaget § 7-2. Byrden vurderes som lav, særlig siden det foreslås at merutgifter knyttet til plikten skal dekkes av staten. Plikten vil heller ikke kreve at tilbyder setter av omfattende tekniske eller andre ressurser. Det lovfestes at tilretteleggingen ikke skal forringe elektroniske kommunikasjonstjenester for brukerne. Departementet viser til drøftelsen i punkt 11.8.7.3.

Etter denne brede interesseavveiningen har departementet kommet til at vilkåret om forholdsmessighet er oppfylt. Departementet har lagt avgjørende vekt på de legitime samfunnsmessige behovene som begrunner inngrepet, sammenholdt med summen av kontrollmekanismer og garantier mot misbruk og vilkårlighet.

11.5.3.5 Forestående avgjørelser fra Den europeiske menneskerettsdomstol

EMDs storkammer har til behandling sakene *Centrum för rättvisa mot Sverige* og *Big Brother Watch mfl. mot Storbritannia*. Sakene ventes å gi avklaringer av de EMK-rettslige rammene for innhenting av data i bulk av hensyn til nasjonal sikkerhet. Begge sakene ble avgjort av EMD i kammer i 2018. I kammerdommene kom domstolen til at det lå innenfor statenes skjønnsmargin å innhente data i bulk av hensyn til nasjonal sikkerhet, men det ble oppstilt krav til garantier mot misbruk og vilkårlighet. Etter departementets vurdering oppfyller lovforslaget de kravene som følger av kammerdommene. Kammerdommene ble anket til EMDs storkammer, og tatt til behandling der. De er derfor ikke rettskraftige.

Norge innga 29. mai 2019 et skriftlig tredjepartsinnlegg til storkammeret, hvor det blant annet ble gitt uttrykk for at statene må ha en vid skjønnsmargin med hensyn til spørsmålet om hvorvidt innhenting av data i bulk av hensyn til nasjonal sikkerhet er nødvendig i et demokratisk samfunn. Det ble avholdt muntlig høring i sakene 10. juli 2019. Avgjørelsene foreligger ikke i skrivende stund. Hvor lang tid storkammeret bruker fra muntlig høring til dom, varierer. Departementet har ikke kjennskap til når avgjørelsene vil bli avsagt. Det er ikke uvanlig at dom fra storkammeret foreligger tidligst ett år etter den muntlige høringen.

Storkammerets avgjørelser kan få betydning for reguleringen av tilrettelagt innhenting, for eksempel dersom storkammeret skulle oppstille strengere krav til garantier mot misbruk og vilkårlighet enn det som følger av kammerdommene. Det vil i så fall måtte vurderes på nytt om lovforslaget er i samsvar med EMK, slik konvensjonen tolkes av EMD. På grunn av dette har departementet vurdert å vente med å fremme proposisjonen til avgjørelsene foreligger. Det er på den andre siden grunner som tilsier at Stortinget bør behandle lovforslaget uten å avvente avgjørelsene. Lovforslaget har høy prioritet, blant annet fordi det som helhet er utformet med sikte på å gi klarere rettslige rammer for Etterretningstjenestens virksomhet, noe som er av sikkerhetspolitisk og menneskerettslig betydning. Departementet viser i den forbindelse til Stortingets anmodningsvedtak 21. februar 2017, se nærmere punkt 2.1 og 10.3. Departementet ønsker på denne bakgrunn å legge til rette for behandling av forslaget i vårsesjonen 2020, og har derfor funnet å burde fremme proposisjonen før storkammerets avgjørelser foreligger.

Når avgjørelsene blir avsagt, må de analyseres for å finne ut om de gjør det påkrevd å endre lovforslaget eller et eventuelt lovvedtak på ett eller flere punkter. Siden det er forskjeller mellom lovforslaget i denne proposisjonen og lovgivningen som er tema i de to sakene, vil det ikke uten videre kunne trekkes slutninger fra resultatet av dommene til spørsmålet om lovforslagets samsvar med EMK. Hvis det blir nødvendig, vil departementet komme tilbake til Stortinget på egnet måte. Fordi tilrettelagt innhenting vil kreve en

anskaffelse, er det ikke grunn til å tro at lovforslaget kapittel 7 og 8 vil bli satt i kraft før storkammerets avgjørelser foreligger.

11.6 EØS-rettslige rammer

Tiltak som tar sikte på å beskytte 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 heller 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 om grunnleggende rettigheter beskytter blant annet retten til respekt for privatliv og kommunikasjon, retten til beskyttelse av personopplysninger og ytringsfriheten. Pakten er etter TEU artikkel 6 nr. 1 bindende for EUs medlemsland. Den er ikke gjort til en del av EØS-avtalen, og er dermed ikke bindende for Norge.

Kommunikasjonsverndirektivet (2002/58/EF) er EØS-relevant og gjennomført i norsk rett i ekomloven. 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 får anvendelse på virksomhet som gjelder offentlig sikkerhet, forsvar, statens sikkerhet eller statens virksomhet på det strafferettslige området.

Personopplysningsloven gjennomfører personvernforordningen i norsk rett. 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 andre 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 unntaket i forordningen artikkel 2 nr. 2 bokstav a foreslås det i proposisjonen her at personopplysningsloven ikke skal gjelde for behandling av personopplysninger for etterretningsformål, jf. punkt 12.4.4.

Ved lov 15. april 2011 nr. 11 vedtok Stortinget lovendringer for å gjennomføre EUs datalagringsdirektiv i norsk rett. Direktivet ble kjent ugyldig av EU-domstolen i 2014, og loven har ikke trådt i kraft. Hensikten med direktivet var å bidra til å avdekke, etterforske og straffeforfølge alvorlig kriminalitet. Direktivet regulerte ikke datalagring i forbindelse med utenlandsetterretningsvirksomhet. Forslaget i proposisjonen har ingen sammenheng med datalagringsdirektivet.

I *høringsnotatet* punkt 11.8.3.2 drøftes betydningen av EU-domstolens avgjørelse i *Tele2/Watson* (de forente sakene C-203/15 og C-698/15). Det vises til at dommen gjelder nasjonal lovgivning om datalagring med sikte på å bekjempe kriminalitet, mens forslaget i høringsnotatet har beskyttelse av nasjonal sikkerhet som formål. Det konkluderes på denne bakgrunn med at dommen ikke står i veien for nasjonal lovgivning som åpner for tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon når formålet med innhentingen er utenlandsetterretning.

Det konkluderes i høringsnotatet punkt 11.8.5 med at det ikke vil være i strid med Norges EØS-rettslige forpliktelser å vedta lovgivning om tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon for utenlandsetterretningsformål. Ingen *høringsinstanser* har innvendinger mot vurderingen, men noen viser til *Tele2/Watson* som ledd i menneskerettslige innvendinger mot forslaget. Departementet fastholder at Norges EØS-rettslige forpliktelser ikke er til hinder for lovforslaget. Etter departementets syn kan det heller ikke trekkes slutninger fra *Tele2/Watson* med hensyn til de menneskerettslige rammene for tilrettelagt innhenting, all den tid avgjørelsen gjelder nasjonale regler med et annet formål og med en annen innretning. De menneskerettslige rammene for forslaget er drøftet i punkt 11.5.

Departementet bemerker at EU-domstolen har til behandling *Privacy International* (sak C-623/17). Saken gjelder betydningen av kommunikasjonsverndirektivet for lagring av kommunikasjonsdata i bulk for å verne nasjonal sikkerhet, og hvorvidt kravene som domstolen oppstilte i *Tele2/*

Watson gjelder når datalagringen finner sted av hensyn til nasjonal sikkerhet.

Norge innga skriftlig tredjepartsinnlegg til domstolen 14. februar 2018. I likhet med et stort flertall andre stater som innga innlegg, ga Norge uttrykk for at tiltak innen nasjonal sikkerhet ikke omfattes av kommunikasjonsverndirektivets virkeområde. Det ble avholdt muntlig høring i saken 9. til 10. september 2019, i sammenheng med *La Quadrature du Net mfl.* (de forente sakene C-511/18 og C-512/18) og *Ordre des barreaux francophones et germanophone mfl.* (sak C-520/18). Norge holdt innlegg under høringen.

Generaladvokat Manuel Campos Sánchez-Bordona avga 15. januar 2020 sin uttalelse i saken. I motsetning til hva Norge tok til orde for, mener han at direktivet gjelder for lovgivning som pålegger ekomtilbydere å lagre data på vegne av myndighetene for å verne nasjonal sikkerhet. Han mener at nasjonal lovgivning ikke kan pålegge tilbydere en plikt til å gi etterretnings- og sikkerhetstjenester tilgang til kommunikasjonsdata i bulk som innebærer en generell og udifferensiert lagring av slike data i forkant. Subsidiært mener han at etterretnings- og sikkerhetstjenesters tilgang til data fra ekomtilbydere må oppfylle kriteriene som domstolen oppstilte i *Tele2/Watson*. Uttalelsen er ikke bindende for domstolen.

Domstolens avgjørelse foreligger ikke i skrivende stund. Departementet vet ikke når dom vil bli avsagt. Det er ikke klart i hvilken grad avgjørelsen vil få betydning for reguleringen av tilrettelagt innhenting. Siden det er forskjeller mellom lovforslaget i denne proposisjonen og lovgivningen som er tema i *Privacy International*, vil det ikke uten videre kunne trekkes slutninger fra domsresultatet til spørsmålet om lovforslagets samsvar med EØS-retten. I tillegg kommer at EUs pakt om grunnleggende rettigheter, som domstolen i *Tele2/Watson* tolker direktivet i lys av, ikke er en del av EØS-avtalen.

Departementet har vurdert å vente med å fremme proposisjonen til avgjørelsen foreligger, men har av samme grunner som redegjort for under punkt 11.5.3.5 funnet å burde fremme proposisjonen nå. Hvis en analyse av domstolens avgjørelse viser at den gjør det påkrevd å endre lovforslaget eller et eventuelt lovvedtak på ett eller flere punkter, vil departementet komme tilbake til Stortinget på egnet måte. Fordi tilrettelagt innhenting vil kreve en anskaffelse, er det ikke grunn til å tro at lovforslaget kapittel 7 og 8 vil bli satt i kraft før avgjørelsen foreligger.

11.7 Europarådets personvernkonvensjon

Norge har ratifisert Europarådets konvensjon nr. 108 av 28. januar 1981 om personvern i forbindelse med elektronisk databehandling av personopplysninger. 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;
> 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.»

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.»

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. I *høringsnotatet* punkt 11.8.4 legges det til grunn at tiltak som tilfredsstiller kravene som følger av Grunnloven og EMK, heller ikke vil være i strid med konvensjonen. Ingen *høringsinstanser* har innvendinger mot denne tilnærmingen. Departementet mener at inngrepet er i samsvar med kravene som følger av Grunnloven og EMK, og legger etter dette til grunn at det også er i samsvar med Europarådets personvernkonvensjon.

11.8 Reguleringen av tilrettelagt innhenting

11.8.1 Generelle vilkår og virkeområde

11.8.1.1 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 11.14.2 at Etterretningstjenesten skal kunne innhente grenseoverskridende elektronisk kommunikasjon for etterretningsformål, det vil si med formål å ivareta en eller flere av tjenestens oppgaver etter lovutkastet kapittel 3. Etter forslaget gjelder hjemmelen bare kommunikasjon som krysser den norske landegrensen, ikke lagrede data som ikke er i transitt.

Forslaget i høringsnotatet oppstiller tre vilkår i tillegg til formålsbegrensningen. For det første må grunnvilkårene etter kapittel 5 være oppfylt, for det andre må særreglene i kapittel 7 og kapittel 8 følges, og for det tredje må innhentingen ikke stride mot øvrige bestemmelser i loven.

Det vises i høringsnotatet til at tilrettelagt innhenting er en form for midtpunktinnhenting (innhenting av kommunikasjon i transitt mellom to endepunkter) som på grunn av enkelte særtrekk bør reguleres særskilt. Særreglene bør derimot ikke gjelde for annen innhenting av grenseoverskridende elektronisk kommunikasjon. I høringsnotatet foreslås det derfor at særreglene bare skal gjelde for innhenting som ekomtilbydere skal ha plikt til å tilrettelegge for.

11.8.1.2 Høringsinstansenes syn

Noen høringsinstanser mener at tilrettelagt innhenting ikke bør kunne brukes for å løse alle oppgavene som Etterretningstjenesten har etter lovforslaget kapittel 3, eller at dette bør vurderes nærmere. Dette gjelder *Advokatforeningen*, *Borgarting lagmannsrett*, *Den internasjonale juristkommisjon – norsk avdeling (ICJ-Norge), dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors* og *Norges institusjon for menneskerettigheter (NIM)*. NIM uttaler:

> «I høringsnotatet er det lagt opp til at bulkinnsamling og søk i rådata i bulk kun kan skje dersom det er nødvendig og forholdsmessig for å frembringe informasjon som er relevant for «etterretningsformål». Innhentingen har etterretningsformål dersom den tar sikte på å ivareta en eller flere av E-tjenestens oppgaver etter forslaget kapittel 3. Etterretningstjenestens oppgaver etter kapittel 3 er primært rettet mot «utenlandske militære og sivile forhold», jf. forslaget §§ 3-1 og 3-2.
>
> At bulkinnsamling skal brukes for å innhente utenlandsetterretning er i utgangspunktet en sentral avgrensning av virkeområdet, som bidrar til å overholde EMDs krav som er redegjort for over.
>
> Innenfor rammen av hva som kan karakteriseres som «utenlandske militære og sivile forhold» synes det å være få klare avgrensninger. Blant annet fremgår det i forslaget § 3-2, første ledd, bokstav a, at E-tjenesten skal innhente og analysere informasjon for «ivaretakelse av prioriterte utenriks-, forsvars- eller sikkerhetspolitiske interesser knyttet til forhold og utviklingstrekk i andre stater og regioner,». Umiddelbart fremstår det som at dette går videre enn å kun dreie seg om nasjonal sikkerhet.

Ettersom oppgavebeskrivelsen i kapittel 3 danner yttergrensen for adgangen til bulkinnsamling er det også helt sentralt at disse oppgavene fastsettes på en måte som ikke i altfor stor grad overlater til E-tjenesten å definere innholdet.

NIM mener derfor at det innenfor rammen av oppgavebeskrivelsene i kapittel 3, bør fastsettes ytterligere innskrenkninger eller presiseringer av hvilke formål som kan berettige tilrettelagt innhenting. Det på ingen måte gitt at det er nødvendig at virkeområdet korresponderer med E-tjenestens generelle oppgavebeskrivelse.»

Flere høringsinstanser mener at avgrensningen til grenseoverskridende kommunikasjon har liten eller ingen betydning. Det vises til at trafikken normalt vil passere grensen selv om det er tale om kommunikasjon mellom en avsender og en mottaker som begge befinner seg i Norge. Blant høringsinstansene som gir uttrykk for synspunkter i denne retningen, er *Advokatforeningen*, *Datatilsynet*, *Den norske dataforening – IT-politisk råd*, *Elektronisk Forpost Norge* og *SINTEF*.

11.8.1.3 Departementets vurdering

Departementet viderefører forslaget i høringsnotatet. Det fastholdes at hjemmelen bør begrenses til elektronisk kommunikasjon som transporteres over den norske grensen. Det er ingen uenighet om at norsk innenlandsk kommunikasjon normalt krysser grensen, for eksempel fordi den blir rutet via utlandet eller lagres på en server som befinner seg i utlandet. På den andre siden er det heller ingen tvil om at det finnes norsk innenlandsk kommunikasjon som ikke krysser grensen. Slik kommunikasjon bør ikke kunne innhentes, og forslaget gir ikke hjemmel til det. Begrensningen er med andre ord reell. På samme måte som i høringsnotatet, og som påpekt av flere høringsinstanser, er det likevel grunn til å understreke at det i dagens teknologiske situasjon vil innhentes store mengder metadata om norsk innenlandsk kommunikasjon. Det er grunnen til at tilgangen underlegges strengere regler enn andre former for midtpunktinnhenting, som i mindre grad berører norsk innenlandsk kommunikasjon.

I høringsnotatet foreslo departementet å bruke begrepet «landegrensen». Siden begrepet kan tolkes slik at hjemmelen er begrenset til kommunikasjon som transporteres over grensen *på land*, erstattes det i lovforslaget med begrepet «grensen». Endringen er ment å klargjøre at hjemmelen også gjelder kommunikasjon som transporteres inn og ut av Norge sjøveien eller i luften.

Forslaget gir ikke hjemmel til innhenting av lagrede data som ikke er i transitt. Slik data må eventuelt innhentes med hjemmel i lovforslaget § 6-10 om endepunktinnhenting. 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. Dette er nødvendig blant annet for å fange opp digitale angrep som ikke innebærer gjensidig kommunikasjon mellom flere aktører.

Forslaget i høringsnotatet åpner for tilrettelagt innhenting for etterretningsformål, det vil si for å ivareta Etterretningstjenestens oppgaver etter kapittel 3. Felles for oppgavene er at det dreier seg om innhenting av informasjon om utenlandske forhold, det vil si at tilgangen er begrenset til utenlandsetterretning. Departementet har i lys av høringen vurdert hvorvidt formålsangivelsen bør snevres inn ytterligere, for eksempel slik at tilrettelagt innhenting bare skal kunne brukes for å motvirke utenlandske trusler mot Norge, jf. lovforslaget § 3-1. Slike trusler ligger i kjernen av hva forslaget er ment å motvirke, men det er etter departementets syn ikke grunn til å begrense tilgangen til slike trusler. Det kan være glidende overganger mellom utenrikspolitiske, forsvarspolitiske og sikkerhetspolitiske forhold og trusler mot Norge, og for å kunne oppdage en trussel er det av betydning å kunne danne seg et bilde av den utenriks-, forsvars- og sikkerhetspolitiske normalsituasjonen. Alle oppgavene beskrevet i kapittel 3 har til hensikt å ivareta nasjonale sikkerhetsinteresser.

Departementet viser også til at Lysne II-utvalget ikke foreslo å begrense tilrettelagt innhenting til bare enkelte av Etterretningstjenestens oppgaver. En slik begrensning er heller ikke vanlig i land som det er naturlig å sammenligne seg med. For eksempel åpner svensk lovgivning for innhenting om «främmande makts agerande eller avsikter av väsentlig betydelse för svensk utrikes-, säkerhets- eller försvarspolitik» (*lag 2008:717 om signalspaning i försvarsunderrättelseverksamhet* 1 § 2 stk. nr. 8), noe som i grove trekk tilsvarer oppgaven som følger av lovforslaget § 3-2 bokstav a. En i hovedsak tilsvarende oppgave følger av den danske *lov om Forsvarets Efterretningstjeneste (FE)* § 1 stk. 1 nr. 1, som fastsetter at FE skal «tilvejebringe det efterretningsmæssige grundlag for dansk udenrigs-, sikkerheds- og forsvarspolitik».

Departementet understreker at Etterretningstjenesten ikke står fritt med hensyn til hva tje-

nesten skal innhente informasjon om. Virksomheten er styrt av prioriteringene til overordnede myndigheter, se lovforslaget § 2-2 om oppdragsstyring. Det vises også til lovforslaget § 8-2, som fastsetter at det i begjæringen til domstolen må angis hvilket oppdrag søket eller innhentingen knytter seg til.

Det understrekes at det konkrete inngrepet (søket i lagrede metadata eller den målrettede innhentingen og lagringen av innholdsdata) alltid vil måtte tilfredsstille kravet til forholdsmessighet som følger av lovforslaget § 5-4. I forholdsmessighetsvurderingen skal det blant annet tas hensyn til sakens betydning. Hvis saken gjelder en trussel som nevnt i lovforslaget § 3-1, vil det normalt kunne begrunne et sterkere inngrep enn dersom saken gjelder forhold og utviklingstrekk i andre stater og regioner etter lovforslaget § 3-2.

Departementet fastholder at særreglene i kapittel 7 og 8 bare bør gjelde innhenting som krever tilrettelegging fra ekomtilbydere. Andre former for midtpunktinnhenting etter lovforslaget § 6-9 berører ikke norsk innenlandsk kommunikasjon på en måte som begrunner slike særregler. Begrensningen foreslås lovfestet i lovforslaget § 7-1 andre ledd.

11.8.2 Utvalg og filtrering

11.8.2.1 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 11.14.3 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 kommunikasjon mellom en avsender og en mottaker som begge befinner seg i Norge.

I høringsnotatet er regler om utvalg og filtrering inntatt i lovutkastet § 7-5.

11.8.2.2 Høringsinstansenes syn

Tekna anser det i praksis som urealistisk å få til en effektiv og treffende filtrering. I samme retning uttaler *Datatilsynet* seg:

> «Systemet baserer seg på en filtrering som skal frembringe mest mulig etterretningsfaglig relevant informasjon og forsøksvis filtrerer bort informasjon som er sendt mellom avsender og mottaker hvor begge befinner seg i Norge, jf. § 7-5. Dette for å størst mulig grad unnta norske borgere fra etterretningens søkelys.
>
> At det er vanskelig å filtrere bort overskuddsinformasjon er åpenbart. Det vises til høringsnotatets pkt. 8.6.3, hvor det argumenteres med at det ikke finnes «realistiske alternativer for å filtrere ut ikke-relevant informasjon fra datasettene.» fra informasjon som er innhentet gjennom tilrettelagt innhenting.
>
> Metodene for filtrering beskrives ved å vise til et eksempel om å filtrere bort samtaler fra + 47 til + 47. Dette vil trolig få begrenset betydning, sett hen til hvordan kommunikasjon foregår på ulike plattformer i dag.
>
> Lovforslagets bestemmelse om filtrering er uklart formulert, og kan gi et uriktig inntrykk av filtrenes effektivitet. Dette gjør det vanskelig å overskue hvem som i praksis vil kunne bli gjenstand for søk.
>
> I den forbindelse viser vi til Nederlands lov, som ikke skiller mellom innenlandsk eller utenlands data. Dette fordi de mener det ikke er teknisk mulig å gjøre en effektiv filtrering. De har derfor gjort et prinsipielt valg om beskytte all data, som om det var innenlands og har dermed gitt all data høyest mulig vern.»

Norges institusjon for menneskerettigheter (NIM) mener at bestemmelsen legger opp til et svært omfattende skjønn, og at det i praksis er få begrensninger på hvilke bærere som det kan lagres kommunikasjon fra. I utgangspunktet er det heller ikke gitt tidsbegrensninger eller krav om at behovet vurderes fortløpende eller med gitte intervaller.

Direktoratet for e-helse mener at trafikk over Helsenettet, et eget lukket og sikret nett som benyttes av et stort antall helseaktører, bør filtreres bort. Innhenting fra Helsenettet bør kreve særskilt forhåndsgodkjennelse av domstolen.

11.8.2.3 Departementets vurdering

Departementet viderefører forslaget i høringsnotatet, men har i lys av kritikken fra *Datatilsynet* omredigert og omformulert bestemmelsen med sikte på å gjøre den klarere og enklere å forstå. Bestemmelsen inntas i lovforslaget § 7-6.

Forslaget innebærer at Etterretningstjenesten gjennom utvalg og filtrering skal søke å hindre lagring av metadata om kommunikasjon mellom en avsender og en mottaker som begge befinner seg i Norge. I dagens teknologiske situasjon vil det ikke være mulig å hindre lagring av store mengder metadata om norsk innenlandsk kom-

munikasjon. Plikten er derfor utformet som en plikt til å «søke å hindre» lagring av slike data.

Plikten til *utvalg* innebærer at Etterretningstjenesten skal vurdere og beslutte hvilke kommunikasjonsnett, tjenester og linker (kommunikasjonsbærere) som det skal innhentes fra. Etterretningstjenesten skal prioritere innhenting fra de kommunikasjonsbærerne som antas å transportere mest mulig etterretningsrelevant kommunikasjon. Bærere som ikke transporterer kommunikasjon over den norske grensen, skal ikke velges ut. Dette følger av at innhentingshjemmelen er begrenset til grenseoverskridende kommunikasjon. Bærere som utelukkende transporterer kommunikasjon mellom avsendere og mottakere som befinner seg i Norge, skal heller ikke velges ut, selv om det er tale om kommunikasjon som krysser grensen. Her kan det likevel være aktuelt med unntak hvis det er tale om kommunikasjon fra eller til en person som omfattes av lovforslaget § 4-2 første ledd. Det kan for eksempel være tale om en tjeneste som brukes av personer som opptrer på vegne av en fremmed stat eller statsliknende aktør i Norge til å kommunisere seg imellom.

I lys av høringsuttalelsen til *Norges institusjon for menneskerettigheter (NIM)* understreker departementet at plikten til utvalg må ses i sammenheng med lovforslaget for øvrig, blant annet kravet til nødvendighet som følger av lovforslaget § 5-3 og reglene om tilretteleggingsplikt. På bakgrunn av høringen foreslår departementet blant annet at en beslutning om tilrettelegging ikke kan gjelde for mer enn tre år av gangen, se lovforslaget § 7-3 første ledd og punkt 11.8.7.3.

Plikten til *filtrering* innebærer at Etterretningstjenesten skal utvikle og implementere filtre som hindrer lagring av metadata om kommunikasjon mellom en avsender og en mottaker som begge befinner seg i Norge. Som påpekt både i høringsnotatet og i høringsuttalelsen til *Datatilsynet*, er det i dagens situasjon ikke mulig å gjennomføre slik filtrering fullt ut; det er ikke til å komme fra at det vil lagres store mengder metadata om norsk innenlandsk kommunikasjon. 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. Plikten innebærer også en plikt til å sørge for at filtrene holder takt med den teknologiske utviklingen. Hvis utviklingen tillater en mer effektiv filtrering, skal dette følges opp av tjenesten. Filtreringsplikten er i den forstand dynamisk.

Departementet foreslår ingen særregulering for trafikk over Helsenettet, slik *Direktoratet for e-helse* går inn for. De alminnelige reglene er etter departementets syn tilstrekkelige med hensyn til å søke å unngå lagring av metadata om slik kommunikasjon.

11.8.3 Testinnhenting og testanalyser

11.8.3.1 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 11.14.4 å åpne for innhenting og lagring av korte tidsintervaller med ufiltrert kommunikasjon i et korttidslager. Det vises til at slik testinnhenting og testanalyse er nødvendig for teknisk drift av systemet, blant annet med hensyn til utvalg og filtrering.

Etter forslaget skal uttrekkene ikke overstige 30 sekunder, og det kan ikke gjøres mer enn ett uttrekk i timen. Det følger av dette at det maksimalt kan gjøres 24 uttrekk i døgnet. Det foreslås lovfestet at uttrekkene bare kan brukes til teknisk understøttelse. Uttrekkene skal lagres i et eget korttidslager, som skal holdes adskilt fra annen data.

Uttrekkene skal ikke lagres lenger enn det som er nødvendig for de angitte 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 understrekes i høringsnotatet at misbrukspotensialet ved testinnhenting og testanalyse er begrenset, all den tid det vil være tilfeldig hva som fanges opp av uttrekkene. For å styrke tilliten til at adgangen ikke vil misbrukes, foreslås det 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. Det foreslås også at det alltid skal være to tekniske spesialister til stede når uttrekkene settes opp og analyseres.

I høringsnotatet er regler om testinnhenting og testanalyser inntatt i lovutkastet § 7-6.

11.8.3.2 Høringsinstansenes syn

Abelia understreker at det er av særlig viktighet at EOS-utvalget gis full oversikt over arbeid med korttidslageret, og følger opp dette. Høringsinstansen uttaler videre:

> «Vi vil bemerke at det ikke er drøftet hvorvidt det skal tas i bruk maskinlæring eller predika-

tive analyser, og hvilke utfordringer slik teknologibruk vil kunne ha i et kontrollperspektiv. Det bør derfor vurderes om det er mulig og hensiktsmessig at det stilles krav om domstolskjennelse eller lignende forutgående kontroll for innhenting av snapshots og behandlingen av denne dataen. Korttidslageret vil inneholde store mengder informasjon om norske borgere som ligger utenfor Etterretningstjenestens mandat, og risikoen for formålsutglidning syntes derfor å være til stede.»

Den norske dataforening – IT-politisk råd anser at korttidslageret er en nødvendig forutsetning for effektiv bulkinnsamling, men at slik lagring i seg selv utgjør et betydelig inngrep i retten til privatliv.

Elektronisk Forpost Norge uttaler:

«Innhenting av data i bulk vil gi store datamengder selv når det samles inn i korte tidsintervaller. I realiteten kan enhver nettbruker få hele eller deler av sin daglige aktivitet fanget opp i løpet av et døgn. Dette vil være personlig, fortrolig, sensitiv og/eller konfidensiell informasjon som innhentes, og som maskinelt bearbeides og analyseres for videre lagring i et «metadatalager». Over en periode av to uker kan en teoretisk tilrettelegge for profiler/kategorisering av bortimot hele befolkningen via teknikker for indeksering og mining av data.»

NRK uttaler:

«Når det gjelder det såkalte «korttidslageret», vil Etterretningstjenesten ha tilgang til all informasjon den siste 14-dagers perioden. Selv om denne tilgangen begrenses på mange måter – både mht. formål, hvem som kan gjøre søk, antall søk og lengde på søk – vil det forhold at Etterretningstjenestens medarbeidere faktisk har tilgang, i seg selv ha en nedkjølende effekt.»

11.8.3.3 Departementets vurdering

Departementet viderefører forslaget i høringsnotatet. Innhenting, lagring og analyse av korte tidsintervaller med ufiltrert kommunikasjon, både metadata og innholdsdata, er en grunnleggende forutsetning for drift av tilgangen, blant annet med hensyn til utvalg og filtrering som skal søke å hindre innhenting og lagring av overskuddsinformasjon. Det er samtidig ingen tvil om at det fra et personvernperspektiv er problematisk med lagring av ufiltrert kommunikasjon. Det foreslås derfor strenge begrensninger.

Etter forslaget kan ett uttrekk ikke overstige 30 sekunder, og det kan ikke gjøres mer enn ett uttrekk i timen. Dette innebærer at det maksimalt kan gjøres 24 uttrekk i døgnet, og at disse 24 uttrekkene samlet vil kunne omfatte maksimalt 12 minutter med kommunikasjon i løpet av et døgn, brutt opp i 30 sekunders intervaller. Med disse begrensningene mener departementet at misbrukspotensialet er lite. Det vil være tilfeldig hva som fanges opp av uttrekkene, og muligheten til å innrette uttrekk mot bestemt kommunikasjon fremstår som teoretisk.

Departementet understreker at testinnhenting og testanalyse utelukkende skal brukes for teknisk understøttelse. Testdata vil ikke kunne brukes til noen andre formål, slik som etterretningsproduksjon. Testdata kan ikke deles med andre etter reglene i lovforslaget kapittel 10, det være seg norske myndigheter eller samarbeidende tjenester, med mindre det dreier seg om testdata og analyser som ikke kan knyttes til enkeltpersoner. Det bemerkes at ordlyden i lovforslaget er justert fordi teknisk understøttelse også regnes som et etterretningsformål. Justeringen innebærer ingen realitetsendring.

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.

Forbudet mot bruk av testdata til annet enn teknisk understøttelse støttes opp av regelen om at testinnhenting og annen teknisk understøttelse bare skal utføres av et begrenset antall tekniske spesialister som har mottatt særskilt opplæring og som ikke har etterretningsanalyse som oppgave. For ytterligere å motvirke risikoen for misbruk foreslås det dessuten at det alltid skal være to spesialister til stede ved oppsett og analyse av uttrekk. Departementet legger til grunn at det vil etableres prosedyrer for rullering av spesialistene som gjennomfører uttrekkene.

All aktivitet knyttet til korttidslageret vil logges for kontrollformål. Det foreslås lovfestet i lovforslaget § 7-11 at EOS-utvalget skal kontrollere at korttidslageret utelukkende brukes til teknisk understøttelse. Departementet forutsetter at utvalget vil utvikle god kompetanse med hensyn til korttidslageret, og at bruken av dette underlegges omfattende kontroll, slik *Abelia* i sin høringsuttalelse påpeker viktigheten av.

På bakgrunn av høringsuttalelsene til *Elektronisk Forpost Norge* og *NRK* understreker departementet at forslaget på ingen måte innebærer at Etterretningstjenesten har tilgang til all informasjon fra den siste perioden på 14 dager. Forslaget gir utelukkende hjemmel til å innhente uttrekk på maksimalt 30 sekunder, og det kan maksimalt gjøres ett slikt uttrekk hver time. Det kan ikke innhentes og lagres mer informasjon enn dette. Data som hentes inn, vil utelukkende lagres i korttidslageret for teknisk understøttelse.

Departementet presiserer at metadata som lagres i bulk etter lovforslaget § 7-7 også vil være gjenstand for løpende grovutvalg og grovfiltrering av hensyn til å minimere lagring av metadata fra mindre relevante kommunikasjonsstrømmer.

11.8.4 Innhenting og lagring av metadata i bulk

11.8.4.1 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 11.14.5 å gi Etterretningstjenesten adgang til å lagre metadata om kommunikasjon som passerer den norske landegrensen etter at det er foretatt utvalg og filtrering.

Metadata foreslås definert 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». Definisjonen omfatter både trafikkdata og signaleringsdata, jf. ekomforskriften § 7-1 første ledd og § 7-2 første ledd.

For å hindre at det lagres innholdsdata, foreslås det lovfestet at det skal opprettes og vedlikeholdes en liste som spesifiserer hvilke typer data som regnes som metadata. Listen skal være tilgjengelig for kontrollmyndighetene.

I høringsnotatet drøftes særskilt hvor lenge metadata bør kunne lagres. Etter en samlet vurdering av de kryssende hensynene, foreslås det en lagringstid på 18 måneder.

I høringsnotatet er regler om lagring av metadata inntatt i lovutkastet § 7-7.

11.8.4.2 Høringsinstansenes syn

Flere høringsinstanser påpeker at lagring av metadata er svært inngripende, og at metadata er egnet til å avsløre sensitive forhold ved en person. *Datatilsynet* uttaler:

> «Det er i dag ingen prinsipiell eller rettslig forskjell på innholdsdata og metadata. Metadata kan inneholde store mengder personopplysninger. Metadata er lettere å strukturere og analysere enn innholdsdata. På grunn av disse egenskapene er metadata, i minst like stor grad som innholdsdata, egnet til å avsløre intime detaljer om en persons privatliv. Dette betyr at behandling (inkludert lagring) av metadata medfører et stort inngrep i retten til privatliv.
>
> Metadata inneholder blant annet informasjon om tilbyder av kommunikasjonstjeneste, kilden til kommunikasjon og bestemmelsessted, geografisk plassering, dato, klokkeslett, varighet, type kommunikasjonsutstyr, navn, adresse, abonnement, telefonnummer, IP-adresse, brukernavn og gjør det mulig å identifisere hvem som har kommunisert, hvorfra og med hvilken hyppighet. Fra en smarttelefon vil det i dag gå en kontinuerlig strøm av metadata til og fra ulike apper, som vil kunne gi en detaljert kartlegging av en persons liv.»

Amnesty International og *Tekna* gir uttrykk for lignende synspunkter.

Den norske dataforening – IT-politisk råd fremholder at metadatabegrepet som brukes i høringsnotatet er omfattende, og representerer noe annet enn når begrepet har blitt brukt om for eksempel trafikkdata fra telekommunikasjon. Mengden og typene av metadata vil langt overgå hva det var tale om å pålegge lagret gjennom datalagringsdirektivet. Det har i liten grad vært diskutert i den offentlige debatten at et søk kan hente ut 15 måneders livshistorie for målet for etterretningsvirksomheten. *Elektronisk Forpost Norge* gir uttrykk for lignende synspunkter.

Amnesty International støtter forslaget om en liste over hvilke typer metadata som skal lagres, men etterlyser tydeligere rammer for måten lagringen av metadata skal foretas og hvordan det skal sikres på best mulig måte mot at uvedkommende kan skaffe seg adgang til det. *Norsk Presseforbund* mener at sannsynligheten er stor for at listen ikke vil klare å fange opp alt som er innholdsdata. *Tekna* understreker at EOS-utvalget har en viktig funksjon i å etterse at Etterretningstjenesten ikke misbruker retten til å definere hva som skal lagres.

Direktoratet for forvaltning og ikt (Difi) uttaler:

> «Hva som er metadata i kommunikasjon over Internett fremkommer av de tekniske spesifikasjonene for hver enkelt kommunikasjonsprotokoll som er i bruk. Det er viktig å merke seg

at metadata kan omfatte opplysninger som har likhetstrekk med innholdsdata og dermed oppfattes som like sensitive. Et eksempel er at metadata kan inneholde personidentifiserende opplysninger. Det er viktig at dette kommer klart frem av beskrivelsen av begrepet metadata i lovens forarbeider.»

Kripos mener at ordlyden i lovutkastet § 7-7 tredje ledd bør endres fra «etter» til «senest etter».

Abelia, *Norsk Presseforbund* og *Tekna* mener at lagringstiden på 18 måneder er for lang. Abelia mener at lagringstiden bør settes til 12 måneder. Norsk Presseforbund mener at det er grunn til å tro at dataene vil komme til å lagres lenger enn 18 måneder, og viser i den forbindelse til Kontrollutvalget for kommunikasjonskontrolls årsrapport for 2017.

11.8.4.3 Departementets vurdering

Departementet viderefører forslaget i høringsnotatet med enkelte lovtekniske justeringer. Det foreslås presisert at metadata vil innhentes og lagres i bulk, jf. punkt 11.2.3.

Departementet understreker at søk i lagrede metadata bare vil kunne foretas innenfor rammen av rettens tillatelse. Det vises til punkt 11.9. Det er altså på ingen måte slik at Etterretningstjenesten vil ha uhindret tilgang til lageret. All tilgang vil være gjenstand for forhåndskontroll, løpende kontroll og etterfølgende kontroll.

I lys av høringen vil departementet understreke at innhenting og lagring av metadata i bulk, er et sterkt inngrep i personvernet. Som flere høringsinstanser påpeker, kan lagring og analyse av metadata avsløre sensitive forhold knyttet til enkeltpersoner. Departementet mener like fullt at det er grunn til å skille mellom lagring av metadata og innholdsdata. At myndighetene får tilgang til innholdet i kommunikasjonen, må etter departementets syn normalt regnes som mer inngripende enn at de får tilgang til metadata om kommunikasjonen. Innholdsdata bør derfor ikke innhentes og lagres i bulk. Det vises til punkt 11.8.6 om målrettet innhenting og lagring av innholdsdata.

Når det gjelder lagringstiden, tar departementet utgangspunkt i at personvernhensyn taler for en så kort lagringstid som mulig, mens etterretningsfaglige hensyn tilsier en så lang lagringstid som mulig. Tilrettelagt innhenting skal kunne brukes for å løse alle oppgavene til Etterretningstjenesten. Flere av disse oppgavene kan innebære operasjoner som strekker seg over lang tid, noe som tilsier en lagringstid på mer enn 18 måneder. Dette gjelder særlig oppgaver knyttet til statlige aktørers virksomhet. En kortere lagringstid vil derimot i noen tilfeller kunne ha effekt når det gjelder kontraterroroppdraget. Etter en samlet vurdering av de kryssende hensynene kan departementet slutte seg til Lysne II-utvalgets forslag om en lagringstid på 18 måneder.

Departementet er enig med *Kripos* i at det bør presiseres i lovteksten at lagrede metadata skal slettes «senest» etter 18 måneder, og foreslår dette.

På bakgrunn av høringsuttalelsen til *Norsk Presseforbund* vil departementet bemerke at Kontrollutvalget for kommunikasjonskontroll ikke kontrollerer Etterretningstjenesten. Det understrekes for ordens skyld at det vil være et regelbrudd dersom data lagres i strid med bestemmelsen om lagringstid.

11.8.5 Søk i lagrede metadata

11.8.5.1 Forslaget i høringsnotatet

Det vises i høringsnotatet punkt 11.14.6 til at 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.

I tråd med Lysne II-utvalgets forslag foreslås det i høringsnotatet at søk i metadatalageret skal baseres på en personselektor (for eksempel en e-postadresse) eller en modusselektor (et bestemt mønster eller avgrensning). Dette innebærer at det ikke tillates søk hvor både aktør og modus er ukjent.

I høringsnotatet foreslås det at personselektorsøk maksimalt kan inkludere to ledd ut i personenes kommunikasjonskjede, med mindre retten i særskilte tilfeller bestemmer noe annet, jf. lovutkastet § 7-8 første ledd tredje punktum.

Det foreslås i høringsnotatet 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 søke i henhold til søkeprivilegier som er tilpasset oppdragsporteføljen.

I høringsnotatet er regler om søk i lagrede metadata inntatt i lovutkastet § 7-8.

11.8.5.2 Høringsinstansenes syn

Flere høringsinstanser er kritiske til forslaget i høringsnotatet om at personselektorsøk kan inkludere to ledd ut i personenes kommunikasjonskjede. Det vises til at en adgang til søk to ledd ut innebærer at et stort antall personer kan bli gjenstand for søk, og at det dermed kan være vanskelig for domstolen å overskue omfanget av tillatelsen. *Advokatforeningen*, *Borgarting lagmannsrett*, *Norsk Journalistlag*, *Norsk Redaktørforening*, *Norsk Presseforbund*, *NRK* og *dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors* gir uttrykk for synspunkter i denne retningen.

Datatilsynet uttaler:

> «Vi mener at det i lovforslaget og høringsnotatet ikke kommer klart frem hvor omfattende søkene i realiteten vil være. Slik Datatilsynet forstår det, så vil det innsamlede materialet bli utsatt for en kontinuerlig behandling gjennom ulike former for søk basert på de selektorene man til enhver tid benytter. Som et bilde på det kan man si at ved et søk etter et sort får i en saueflokk, så vil en datamaskin måtte vurdere alle sauene og vil ikke kunne identifisere den sorte uten at de andre sauene vurderes.»

Tilsynet mener at det er vanskelig å få tak i hvilken begrensning grunnvilkåret om forholdsmessighet setter for modusselektorsøk, og uttaler videre:

> «Et søk med modusselektor vil gjennomføres i alle data som er lagret. Verktøyene for søk i stor-data blir stadig mer avanserte og mønstergjenkjennelse åpner for å finne sammenhenger som man ikke tidligere klarte. En økt bruk av kunstig intelligens gjør at svart-boks problematikken, hvor programvaren produserer resultater som ikke er kontrollerbare, skaper rom for feil.
>
> Det er uklart hva som kan danne utgangspunkt for et søk. Det som i utgangspunktet kan være et legitimt søk kan få uforutsette virkninger fordi omfanget av opplysninger er så stort og ethvert søk vil kunne ramme alle.»

Tekna og *SINTEF* reiser også spørsmål knyttet til bruk av maskinlæring og kunstig intelligens. Tekna uttaler:

> «Tekna tar det for gitt at etterretningstjenesten ønsker å ta i bruk stordataanalyser og maskinlæring, også omtalt som kunstig intelligens. Vi vil påpeke at disse teknologiene fører med seg mange nye problemstillinger, både etiske og teknologiske. Å introdusere slike teknologier i et miljø som per definisjon har lav transparens, gjør det ekstra vanskelig å adressere og korrigere metodeproblemer og for eksempel skjevheter og innebygde fordommer i datasettene (bias). Noen eksempler på problemstillinger er: Hvilke treningsdata og valideringsdata skal brukes? Hvem skal gis tilgang til disse dataene for å kunne utvikle best mulige algoritmer og modeller? Hva er kravene til treffsikkerhet/feilrate, og hvordan skal dette måles og korrigeres? Hva er kravene til etterprøvbarhet og begrunnelse av resultater?»

11.8.5.3 Departementets vurdering

Departementet fastholder i hovedsak forslaget i høringsnotatet, men med noen endringer som følge av høringen. Bestemmelsen inntas i lovforslaget § 7-8. Det foreslås at søk skal baseres på søkebegreper, som brukes som en fellesbetegnelse for personselektorer og modusselektorer. Denne endringen er rent språklig og innebærer ingen realitetsendring fra forslaget i høringsnotatet. Det vises til merknadene til § 7-8 for en nærmere beskrivelse av personselektorer og modusselektorer. Departementet ser det som overflødig å presisere at kapittel 9 får anvendelse for personopplysninger som Etterretningstjenesten får tilgang til etter søk i lagrede metadata, og viderefører derfor ikke forslaget i høringsnotatet til § 7-8 tredje ledd. Dette medfører ingen realitetsendring.

De konkrete søkebegrepene må ligge innenfor rammen av rettens kjennelse, enten ved at de spesifikt er godkjent av retten eller ved at de er innenfor en kategori av søkebegreper som retten har godkjent. Det vises til reglene om domstolens forhåndsgodkjennelse i lovforslaget kapittel 8.

Departementet viderefører ikke forslaget i høringsnotatet om å oppstille som hovedregel en adgang til personselektorsøk to ledd ut i kommunikasjonskjeden, som har møtt kritikk under høringen. På grunn av forbudet i lovforslaget § 4-1 kan ikke Etterretningstjenesten kartlegge hvilke personer i Norge som den norske kontakten av et utenlandsk etterretningsmål kommuniserer med. En hovedregel om adgang til søk to ledd ut vil av den grunn ha liten betydning når det gjelder tilrettelagt innhenting. Departementet understreker at Etterretningstjenesten vil kunne kartlegge de utenlandske kontaktene til et etterretningsmål så lenge dette er i tråd med lovens vilkår for øvrig.

Informasjon om slike kontakter vil normalt innhentes på andre måter enn gjennom tilrettelagt innhenting.

Datatilsynet, *Tekna* og *SINTEF* peker i sine høringsuttalelser på problemstillinger knyttet til stordata, maskinlæring og kunstig intelligens. Departementet er enig i at utvikling og bruk av kunstig intelligens kan skape utfordringer og reise flere vanskelige spørsmål, se Nasjonal strategi for kunstig intelligens (2020) side 56 følgende. Departementet legger til grunn at Etterretningstjenesten retter oppmerksomhet mot å utvikle søkeverktøy og annen teknologi som bidrar til å motvirke feil og skjevheter i etterretningsvirksomheten, i tråd med likhetsprinsippet og ikke-diskrimineringsprinsippet som følger av Grunnloven § 98 og diskrimineringsforbudet som følger av lovforslaget § 9-4. Departementet understreker at tjenestens bruk av maskinlæring, kunstig intelligens og avanserte søkeverktøy ligger innenfor EOS-utvalgets kontrolloppgave, og legger til grunn at utvalget er bevisst på problematikken.

Departementet bemerker at vilkåret om at søk skal baseres på søkebegreper, innebærer at det ikke er tillatt med søk hvor både aktør og modus er ukjent. Det betyr at det ikke kan søkes etter anomalier uten at søket bygger på søkebegreper eller kategorier av søkebegreper som på forhånd er godkjent av domstolen. Etter departementets vurdering begrenser dette risikoen for slik vilkårlighet som høringsinstansene viser til.

11.8.6 Målrettet innhenting og lagring av innholdsdata

11.8.6.1 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 11.14.7 at Etterretningstjenesten, innenfor rammen av rettens kjennelse, skal kunne innhente og lagre innholdsdata med tilhørende metadata fra elektronisk kommunikasjon som transporteres over den norske landegrensen.

Innholdsdata foreslås legaldefinert som elektronisk kommunikasjon som ikke er metadata. Det er altså innholdet i kommunikasjonen det siktes til, for eksempel innholdet i en e-post, en tekstmelding eller en videosamtale.

Det påpekes i høringsnotatet at en vesentlig forskjell mellom lagring av innholdsdata og lagring av metadata, er at sistnevnte ikke krever rettens kjennelse for selve lagringen, kun for søkene i lagrede data. For lagring av innholdsdata med tilhørende metadata krever allerede lagringen domstolens forhåndsgodkjennelse.

I høringsnotatet heter det at adgangen til innhenting og lagring utelukkende gjelder innenfor rammen av rettens kjennelse etter kapittel 8, eventuelt en ordre som trer i stedet for rettens kjennelse i hastetilfeller. Bestemmelsen må derfor ses i sammenheng med lovutkastet kapittel 8, hvor det er gitt regler om saksbehandlingen for domstolen og hva domstolen skal prøve.

Det understrekes i høringsnotatet at innhenting og lagring av innholdsdata alltid vil være målrettet innhenting. Det presiseres at målrettet innhenting kan finne sted selv om den reelle identiteten til en trusselaktør ikke er kjent.

Av pedagogiske hensyn foreslås det presisert at behandling av personopplysninger som Etterretningstjenesten har fått tilgang til etter bestemmelsen, skal skje i samsvar med bestemmelsene i lovutkastet kapittel 9.

I høringsnotatet er regler om innhenting og lagring av innholdsdata inntatt i lovutkastet § 7-9.

11.8.6.2 Høringsinstansenes syn

Abelia mener at det ikke kommer klart frem hvorfor innhenting og lagring av innholdsdata alltid vil være knyttet til målrettet innhenting, og mener at dette bør presiseres i lov.

11.8.6.3 Departementets vurdering

Departementet viderefører forslaget i høringsnotatet med enkelte justeringer på bakgrunn av høringen. Bestemmelsen inntas i lovforslaget § 7-9.

På bakgrunn av høringsuttalelsen til *Abelia* presiseres det i paragrafoverskriften og i lovteksten at det er tale om målrettet innhenting og lagring av innholdsdata med tilhørende metadata. Dette innebærer at grunnvilkåret i lovforslaget § 5-2 må være oppfylt, det vil si at konkrete holdepunkter må tilsi 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. Som påpekt i høringsnotatet, er det ikke et vilkår at den reelle identiteten til etterretningsmålet er kjent. For eksempel kan det hentes inn innholdsdata fra en IP-adresse som benyttes til cyberoperasjoner mot Norge, selv om angrepet ikke ennå er attribuert en bestemt aktør.

Departementet ser det som overflødig å presisere at kapittel 9 får anvendelse for personopplysninger som Etterretningstjenesten får tilgang til

etter målrettet innhenting og lagring av innholdsdata, og viderefører derfor ikke forslaget i høringsnotatet til § 7-9 tredje ledd. Dette medfører ingen realitetsendring.

11.8.7 Tilretteleggingsplikt for ekomtilbydere

11.8.7.1 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 11.15.1 en tilretteleggingsplikt for aktører i ekomindustrien. Det vises til at 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.

Tilretteleggingsplikten bør gjelde for alle som regnes som tilbydere etter definisjonen i ekomloven § 1-5 nr. 16. Plikten bør også gjelde 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.

I høringsnotatet vises det til at tilretteleggingsplikten på et generelt nivå innebærer 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 hvilket nett eller tjeneste det er snakk om, og vil i takt med den teknologiske utviklingen kunne variere over tid. Det foreslås på denne bakgrunn å lovfeste en generell plikt konkretisert gjennom en ikke-uttømmende opplisting.

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. Etterretningstjenesten vil ha behov for å installere og operere utstyr på steder som kontrolleres av tilbyder. 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 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 testinnhenting og testanalyser av trafikk i nett og tjenester.

Når det gjelder kryptering, vises det i høringsnotatet til uttalelsen i Lysne II-utvalgets rapport punkt 9.5.4 på side 68 til 69:

> «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.»

I høringsnotatet gis det tilslutning til dette, og det foreslås at tilretteleggingsplikten skal inkludere en plikt til å sørge for tilgang til kommunikasjon uten hinder av linkkryptering eller lignende kryptering som tilbyder kontrollerer. Tilretteleggingsplikten skal derimot ikke innebære en plikt til å bidra til annen omgåelse av kryptering, og forslaget 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. Det foreslås også at departementet kan gi regler om tilretteleggingsplikten i forskrift.

Det antas i høringsnotatet 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. Et siste alternativ er å plassere hele bestemmelsen i ekomloven.

I høringsnotatet foreslås det taushetsplikt knyttet til tilretteleggingsplikten. En slik taushetsplikt er etter departementets syn nødvendig for å skjerme Etterretningstjenestens virksomhet. Taushetsplikten skal ikke være til hinder for å gi opplysninger til EOS-utvalget eller Nasjonal kommunikasjonsmyndighet.

11.8.7.2 Høringsinstansenes syn

Flere høringsinstanser har kritiske merknader til forslaget om tilretteleggingsplikt for ekomtilbydere. Noen finner det uklart hvem som omfattes av plikten, mens andre mener det er uklart hva plikten innebærer. Enkelte trekker frem begge deler. Blant høringsinstansene som gir uttrykk at forslaget er uklart, er *Abelia*, *Amnesty International*, *Datatilsynet*, *dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors*, *Nasjonal kommunikasjonsmyndighet (Nkom)*, *Norsk Presseforbund*, *Næringslivets Hovedorganisasjon (NHO)*, *Piratpartiet*, *Tekna* og *Telia Norge AS*.

Noen høringsinstanser peker på at forslaget i høringsnotatet ikke bare omfatter tilbydere etter ekomloven, men også tilbydere av internettbaserte kommunikasjons- eller meldingstjenester, og mener at forslaget med dette går lenger enn Lysne II-utvalgets forslag. Dette gjelder *Abelia, Advokatforeningen*, *Datatilsynet*, *Den norske dataforening – IT-politisk råd (DND)*, *Den internasjonale juristkommisjon – norsk avdeling (ICJ-Norge)*, *Norges institusjon for menneskerettigheter (NIM)* og *Tekna*.

Advokatforeningen fremholder at Lysne II-utvalgets forslag var begrenset til tilgang til datastrømmen i fiberkabler som krysser landegrensene. *Datatilsynet* ser forslaget som en kraftig utvidelse av tilretteleggingsplikten sammenlignet med Lysne II-utvalgets forslag, og mener at det er vanskelig å se rekkevidden av plikten.

Flere høringsinstanser mener at forslaget i høringsnotatet går lenger enn det som ble foreslått av Lysne II-utvalget også med hensyn til kryptering. Det fremholdes at utvalget ville begrense plikten til å omgå kryptering til bare å gjelde linkkryptering, mens forslaget i høringsnotatet også åpner for omgåelse av lignende kryptering som tilbyder kontrollerer.

Amnesty International er kritisk til at tilbydere skal pålegges å bistå med omgåelse av kryptering, men finner det positivt at forslaget ikke går lenger enn Lysne II-utvalgets anbefaling.

Advokatforeningen fremholder at forslaget åpner for at Etterretningstjenesten kan gis tilnærmet fri tilgang til tilbydernes systemer, og at forslaget med dette går lenger enn hva en finner i Sverige. *DND* og *Elektronisk Forpost Norge (EFN)* gir uttrykk for tilsvarende synspunkter.

DND, *EFN* og *Runbox Solutions AS* mener at forslaget åpner for å pålegge tilbydere å stille med bakdører. *Abelia* og *Telia Norge AS* oppfatter dette som uklart. *Dataskydd.net* og *Föreningen för digitala fri- och rättigheter* mener at forslaget åpner for å sabotere nettkryptering og annen kryptering som brukes i vanlige forbrukerprodukter. *Uninett AS* mener at forslaget vil kunne medføre at tjenestetilbydere blir nødt til å avstå fra å benytte krypteringsteknologi som på best måte sikrer brukernes legitime konfidensialitetsbehov, noe som igjen gir ondsinnede aktører økte muligheter til skadelig opptreden.

Flere høringsinstanser har merknader om hvem som skal ha kompetanse til å pålegge tilrettelegging samt om klageadgang og domstolskontroll. *Amnesty International*, *DND*, *EFN*, *ICJ-Norge* og *Nkom* gir uttrykk for at tilretteleggingsplikt ikke bør pålegges av Etterretningstjenesten selv, men av departementet eller en annen høyere instans. Nkom mener at det kan være naturlig å se hen til sikkerhetsloven § 1-3. Blant høringsinstansene som mener at tilbyder bør gis klageadgang, er *Abelia*, *Datatilsynet*, *Norsk Presseforbund* og *ICJ-Norge*. *Datatilsynet* mener dessuten at det bør åpnes for domstolskontroll. *Uninett AS* reiser også spørsmål om klageadgang og rettslig prøving dersom en tilbyder anser en gitt bruk av tilretteleggingsplikten som uforsvarlig.

NIM mener at reglene om tilretteleggingsplikt og utvalg av kommunikasjonsbærere må gjenspeile at Etterretningstjenesten kun har tilgang til bærere og kan kreve tilrettelegging i den grad det er nødvendig ut fra formålet. NIM mener videre at det er grunn til å vurdere om tilretteleggingsplikt skal forutsette rettslig kjennelse. *ICJ-Norge* peker også på dette som et alternativ. NIM fremholder at det kan differensieres mellom tilbydere som er omfattet av ekomloven og andre tilbydere, slik at domstolskontroll kun skal være påkrevd for den siste gruppen.

Norsk rikskringkasting AS (NRK) peker på at lovforslaget kan leses slik at NRK og andre mediehus er omfattet av tilretteleggingsplikten. NRK legger til grunn at dette ikke er tilsiktet, og skriver:

> «Å pålegge en slik plikt ville klart være i strid med det grunnleggende prinsippet om medienes uavhengighet og rolle i et demokratisk samfunn. Det vil etter NRKs syn også være i strid med EMK artikkel 10. Vi ber derfor om at det eksplisitt inntas et unntak for mediene i lovbestemmelsen, alternativt at det uttrykkelig tas inn i forarbeidene at mediene ikke er omfattet av tilretteleggingsplikten.»

Dette synspunktet støttes av *Norsk Journalistlag* og *Norsk Presseforbund*.

Nkom viser til at etablering av tekniske innretninger i tilbydernes infrastruktur potensielt kan påvirke driftssikkerheten i tilbydernes nett og deres plikter etter ekomloven § 2-10 til å tilby elektronisk kommunikasjonsnett og -tjeneste med forsvarlig sikkerhet for brukerne i fred, krise og krig. Nkom understreker at kunnskap om hvordan tilrettelagt innhenting faktisk er implementert ute hos de ulike tilbyderne vil være viktig for arbeidet med å sikre forsvarlig sikkerhet, og foreslår derfor å lovfeste at Etterretningstjenesten skal underrette Nkom når tilbyderne får installert utstyr i egne nett for å tilrettelegge for innhenting, og at Nkom skal føre tilsyn med tilretteleggingen. Nkom påpeker dessuten at tilsynsaktivitet knyttet til tilretteleggingsplikten vil medføre behov for økte ressurser til Nkom.

Direktoratet for forvaltning og ikt (Difi) påpeker at det ikke er gitt at tilbydere av internettbaserte OTT-tjenester bruker slikt utstyr som forutsettes i lovutkastet § 7-2 andre ledd bokstavene b, d og e. Difi fremholder videre at virksomheter som driver datasentre eller tilbyr skytjenester, kan ha egen grenseoverskridende infrastruktur som ikke nødvendigvis omfattes av tilretteleggingsplikten slik den er beskrevet i lovutkastet og høringsnotatet, og at det kan være hensiktsmessig å avklare om slik grenseoverskridende kommunikasjon også skal være underlagt tilretteleggingsplikten.

Noen høringsinstanser etterlyser en regulering av ansvarsspørsmål. *Abelia* reiser spørsmål om hvem som har ansvaret hvis en tilbyder opplever nedetid på sine tjenester som følge av tilretteleggingsplikten, mens *DND* spør hvem som har ansvaret dersom et grensesnitt mellom tilbyder og Etterretningstjenesten skulle lekke informasjon til en tredjepart.

International Business Machines AS (IBM) uttrykker forståelse for behovet for skjerming, men mener at det kan synes noe strengt å oppstille en straffsanksjonert taushetsplikt for personer som blir pålagt å utføre arbeid knyttet til tilrettelegging. IBM peker også på at tilretteleggingsplikten ikke må innebære at tilbyderne selv, eller andre aktører, får innsyn i strid med lovverket disse virksomhetene er underlagt. IBM mener at det er hensiktsmessig at loven utformes på en teknologinøytral måte.

Abelia og *NHO* fremholder at staten må dekke både direkte og indirekte kostnader som følge av tilretteleggingsplikten. *Næringslivets sikkerhetsråd* legger til grunn at tilbydere og andre som får kostnader som følge av tilrettelegging, får disse dekket tilsvarende som i ekomloven. *Telenor Norge AS* forutsetter at alle merkostnader til etablering, utbygging og drift knyttet til tilrettelagt innhenting dekkes. Telenor mener at en regulering i ekomloven kan være hensiktsmessig. *Telia Norge AS* fremholder at tilretteleggingsplikten ikke må resultere i en konkurransevridende eller fordyrende effekt, og mener at det må komme klart frem at det er staten som skal dekke alle utgifter tilretteleggingsplikten resulterer i for tilbyderne.

11.8.7.3 Departementets vurdering

Departementet finner det ikke tvilsomt at det bør lovfestes en plikt for ekomtilbydere til å tilrettelegge for Etterretningstjenestens tilgang til grenseoverskridende elektronisk kommunikasjon. Slik tilrettelegging er en nødvendig betingelse for tilgangen. Det bør fastsettes i lov hvem som omfattes av plikten, og hva den innebærer.

Flere høringsinstanser mener at høringsnotatets forslag om tilretteleggingsplikt fremstår som uklart. Departementet tar denne kritikken alvorlig. Plikten bør formuleres så presist og tydelig som mulig. Det er samtidig klart at ikke alle detaljer kan lovfestes, blant annet fordi loven bør søkes utformet på en teknologinøytral måte, slik *NUPI* og *IBM* fremholder i sine høringsuttalelser. Det er dessuten et legitimt behov for å skjerme detaljer knyttet til tilgangen. Detaljene må uansett i stor utstrekning fastsettes konkret i det enkelte tilfellet, og normalt etter en dialog mellom Etterretningstjenesten og den enkelte tilbyder.

Departementet holder på denne bakgrunn fast ved kjernen i forslaget i høringsnotatet, det vil si en generell plikt til å tilrettelegge for innhentingen som konkretiseres gjennom en ikke-uttømmende opplisting av eksempler. På bakgrunn av de kritiske synspunktene som har kommet frem under høringen, foreslås det noen tilføyelser og presiseringer. Det foreslås blant annet lovfestet at tilretteleggingen ikke skal forringe de elektroniske kommunikasjonstjenestene for brukerne. Departementet har dessuten omredigert og omformulert bestemmelsen med sikte på å gjøre den klarere og mer tilgjengelig.

I lys av høringen har departementet vurdert hvilke tilbydere som skal kunne pålegges å tilrettelegge. Flere høringsinstanser har kritisert at forslaget omfatter ikke bare tilbydere etter ekomloven, men også tilbydere av internettbaserte kommunikasjons- eller meldingstjenester som er tilgjengelige for allmennheten. Noen mener at departementet med dette går betydelig lenger enn hva Lysne II-utvalget gikk inn for.

Departementet bemerker at Lysne II-utvalget ikke utarbeidet noe konkret forslag til regulering av tilretteleggingsplikten. Utvalget forutsatte at utformingen ble utredet nærmere og tydeliggjort i lov (rapporten punkt 9.5.4 side 68). Når det gjelder hvilke tilbydere utvalget så for seg at plikten skulle gjelde for, uttaler utvalget (side 69):

> «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 ha best kontroll over 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 kan ikke se at utvalget med dette mente å stenge for en regulering som etter omstendighetene også kan omfatte andre tilbydere enn dem som omfattes av definisjonen i ekomloven. Dette kan for eksempel være tilbydere av internettbaserte kommunikasjons- eller meldingstjenester («OTT-tilbydere»), slik departementet foreslo i høringsnotatet. Departementet mener at lovgivningen bør åpne for tilrettelegging også fra OTT-tilbydere, spesielt av hensyn til å sikre en teknologinøytral lovgivning i en tid hvor tjenester og produkter er i rask endring. Dersom OTT-tilbydere unntas fra plikten til å tilrettelegge, vil det bli enklere for etterretningsmålene å unngå innhentingen, og loven vil raskt kunne bli teknologisk utdatert. Departementet fastholder derfor forslaget i høringsnotatet på dette punktet.

Forholdet mellom tilretteleggingsplikten og kryptering har fått stor oppmerksomhet under høringen. Utviklingen de senere årene har gått i retning av mer bruk av sterk kryptering. Departementet støtter denne utviklingen, som i stor grad drives av legitime behov for konfidensiell kommunikasjon på alle samfunnsområder, slik *Uninett AS* peker på i sin høringsuttalelse. Regjeringen oppfordrer til bruk av kryptoteknologi i alle samfunnssektorer (Norsk kryptopolitikk (2019) side 15 følgende). Kryptering er viktig for IKT-sikkerheten og for beskyttelse av personopplysninger.

Lysne II-utvalget gikk inn for at tilretteleggingsplikten for teletilbydere burde omfatte leveranse av datastrøm uten linkkryptering på den grensekryssende forbindelsen, men for øvrig ikke inneholde krav om støtte til omgåelse av kryptering (rapporten punkt 8.3 side 49). Utvalget utarbeidet som nevnt ikke noe konkret forslag til regulering, og forutsatte en nærmere utredning av utformingen av tilretteleggingsplikten.

Departementet er enig med utvalget i at tilretteleggingsplikten må omfatte en plikt til å sørge for tilgang til kommunikasjonen uten hinder av linkkryptering. Fordi loven bør søkes utformet på en teknologinøytral måte, mener departementet at det samme må gjelde kryptering som fyller samme funksjon som linkkryptering, men uten å være knyttet til linknivået. Departementet ser dette som avgjørende for å holde tritt med utviklingen av moderne kommunikasjonsteknologi, for eksempel femtegenerasjons mobilnett (5G), som kan innebære kryptering på andre nivåer enn linknivået.

Departementet mener at en tilbyder som har tilgang til en utvalgt kommunikasjonsstrøm i klartekst, det vil si i ukryptert form, bør plikte å speile informasjonen ukryptert. Tilbyder skal dermed ikke selv legge på kryptering på kommunikasjonsstrømmen før speiling. Siden tilbyderen har tilgang i klartekst, mener departementet at det ikke er naturlig å karakterisere dette som *støtte til omgåelse av kryptering*, som Lysne II-utvalget mente at det ikke burde åpnes for. Departementet ser imidlertid at det kan være delte meninger om dette, avhengig av hvilket innhold som legges i ordene. Departementet ønsker derfor å gjøre det klart at plikten til å sørge for tilgang bare bør gjelde kommunikasjonsstrømmer som tilbyderen selv har tilgang til i klartekst. Dette innebærer at loven ikke bør åpne for å pålegge tilbydere å utvikle løsninger for tilgang til ende-til-ende-kryptert kommunikasjon mellom sluttbrukere eller «bakdører» til kryptert informasjon. På bakgrunn av høringen foreslår departementet å markere dette ved å erstatte ordet «lignende» med «tilsvarende» i lovforslaget § 7-2 første ledd bokstav e.

Enkelte høringsinstanser fremholder at tilretteleggingsplikten gir Etterretningstjenesten tilnærmet fri tilgang til tilbydernes systemer. Departementet vil avvise dette. Kjernen er plikten til å speile og gjøre tilgjengelig utvalgte kommunikasjonsstrømmer. Forslaget innebærer ikke en plikt til å gi tjenesten fri tilgang til kjernenett eller annen infrastruktur. Innenfor rammen av legitime skjermingsbehov skal tilbyder gjøres kjent med tiltakene som treffes, og gis anledning til å være til stede når utstyr installeres og vedlikeholdes. Nkom vil føre tilsyn med utøvelsen av tilretteleggingsplikten.

Departementet er enig med de høringsinstansene som påpeker et behov for å regulere hvem som skal treffe beslutning om tilretteleggingsplikt og hvorvidt beslutningen skal kunne påklages. Departementet foreslår en egen bestemmelse om dette i lovforslaget § 7-3. Myndigheten til å fatte beslutning om tilrettelegging bør etter departementets syn legges til sjefen for Etterretningstjenesten. Tilbyderen skal så langt mulig gis anledning til å uttale seg før beslutningen fattes. Departementet forutsetter at det normalt vil finne sted en dialog mellom tjenesten og den enkelte tilbyder om hvilke tiltak som skal treffes og hvilke økonomiske konsekvenser det vil ha for tilbyderen. Tjenesten og den enkelte tilbyder bør tilstrebe å komme til enighet om dette.

Etter forslaget kan beslutningen gjelde for høyst tre år av gangen. Dette sørger for at behovet for tilrettelegging fra den enkelte tilbyder vurderes med jevne mellomrom. Det foreslås videre at tilbyderen kan påklage beslutningen til departementet med en klagefrist på tre uker. Departementet kan på anmodning fra tilbyderen bestemme at beslutningen ikke skal iverksettes før klagen er avgjort.

Departementet har vurdert hvorvidt kompetansen til å beslutte tilrettelegging bør legges til domstolen, slik *Datatilsynet* og *NIM* peker på som et alternativ i sine høringsuttalelser, men ser det ikke som nødvendig eller hensiktsmessig å legge slik myndighet til domstolen på dette stadiet av innhentingsprosessen. Det vises til at Etterretningstjenesten ikke vil kunne søke i lagrede metadata eller innhente innholdsdata uten at dette er godkjent av domstolene i tråd med reglene i lovforslaget kapittel 8.

Departementet er enig med *NIM* i at Etterretningstjenesten bare skal kunne kreve tilrettelegging i den grad det er nødvendig ut fra formålet. Departementet mener at dette kravet er tilstrekkelig regulert gjennom lovforslaget § 5-3 om innhenting av rådata i bulk og plikten til utvalg etter lovforslaget § 7-6.

Beslutninger om tilrettelegging vil på vanlig måte være gjenstand for EOS-utvalgets kontroll. Som nevnt mener departementet dessuten at Nkom bør føre tilsyn med hvordan tilbydere som omfattes av Nkoms tilsynsmyndighet, utøver tilretteleggingsplikten. Som Nkom påpeker i sin høringsuttalelse, arbeider Nkom helhetlig for å sikre forsvarlig sikkerhet i ekomnett og ekomtjenester. Det er derfor viktig at Nkom har kunnskap om hvordan tilrettelagt innhenting er implementert hos den enkelte tilbyder. Nkom vil på denne måten inngå i det samlede kontrollsystemet knyttet til innhentingen, men på samme måte som i dag vil ikke myndigheten ha noen tilsynsfunksjoner direkte overfor Etterretningstjenesten.

Departementet legger til grunn at ekomloven § 10-1 er tilstrekkelig grunnlag for Nkoms tilsynsfunksjon knyttet til tilbyders utøvelse av tilretteleggingsplikten, og ser ikke behov for å særregulere dette i lovforslaget. Lovforslaget § 2-8 andre ledd justeres for å få frem at unntaket fra kapittel 10 i ekomloven for informasjon og områder som vil gi Nkom innsyn i Etterretningstjenestens virksomhet, ikke er til hinder for at Nkom fører tilsyn med tilbydernes utøvelse av tilretteleggingsplikten. Det foreslås dessuten at beslutning om tilrettelegging skal meddeles til både EOS-utvalget og Nkom. Det foreslås også at Nkom på forespørsel har rett til informasjon om tekniske og operasjonelle løsninger som tjener til å oppfylle tilretteleggingsplikten.

Flere presseaktører mener at det bør lovfestes et unntak fra tilretteleggingsplikten for mediene. Departementet understreker at mediene ikke kan pålegges tilrettelegging i den utstrekning det strider med ytrings- og informasjonsfriheten slik den er vernet blant annet av Grunnloven § 100 og EMK artikkel 10. Departementet regner situasjonen som så lite aktuell at det ikke er grunn til å la dette fremgå særskilt av lovteksten.

Noen høringsinstanser etterlyser en nærmere regulering av ansvarsspørsmål som kan oppstå som følge av tilretteleggingsplikten. Departementet ser ikke tilstrekkelig grunn til å foreslå noen slik særregulering. De ansvarsspørsmål som måtte oppstå i praksis, må finne sin løsning med utgangspunkt i alminnelige regler.

Departementet viderefører forslaget i høringsnotatet om å lovfeste at merutgifter som tilbyder har som følge av tilretteleggingsplikten, skal dekkes av staten. Både merutgifter knyttet til investeringer og til drift skal dekkes. Nærmere regler kan gis i forskrift.

I tråd med forslaget i høringsnotatet går departementet inn for å innta en henvisning til tilretteleggingsplikten i ekomloven § 2-8 nytt fjerde ledd.

11.9 Forhåndskontroll

11.9.1 Forhåndsgodkjennelse av en domstol

11.9.1.1 Forslaget i høringsnotatet

I høringsnotatet punkt 11.11.4.1 drøftes 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 gikk i sin rapport inn for domstolskontroll gjennom en ordning med forhåndsgodkjennelser av søk i metadatalageret og innsamling av innholdsdata.

Det vises i høringsnotatet til at rettssikkerhets- og legitimitetshensyn tilsier et krav om forhåndsgodkjennelse fra domstolene. Det vil virke mindre betryggende om Etterretningstjenesten selv skal fatte beslutningen, eller om myndigheten legges til departementet eller en annen del av den utøvende makt. Det er heller ikke ønskelig å legge slik myndighet til EOS-utvalget.

11.9.1.2 Høringsinstansenes syn

Advokatforeningen støtter forslaget om domstolskontroll, men stiller spørsmål ved hvilken reell mulighet domstolen har til å utøve effektiv kontroll. Foreningen mener at domstolens faktiske mulighet til å utøve forhåndskontroll bør styrkes. *Datatilsynet*, *Den internasjonale juristkommisjon – norsk avdeling (ICJ-Norge)* og *NRK* gir uttrykk for synspunkter i samme retning.

Dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors uttaler:

> «En omfattende kontroll med lovligheten av innhentingen og lagringen slik det forutsettes i forslaget, vil kreve betydelig innsikt og forståelse for virksomheten til Etterretningstjenesten, og også til ulike mulige tekniske løsninger. En liten endring i søkekriterier vil kunne få store utslag og gjøre at et søk går fra å være uforholdsmessig til forholdsmessig. Dommeren må kunne se og forstå hvilke endringer som er mulige og ønskelige.
>
> Samlet sett vil vi peke på at det er svært mange vilkår i loven som skal vurderes ved hver eneste kjennelse. Når vilkårene hver for seg er vage og uklare, mener vi at det ikke ligger til rette for en reell kontroll.»

Domstoladministrasjonen støtter synspunktet om at krav om forhåndstillatelse fra domstolene utgjør en viktig og reell rettssikkerhetsgaranti. Samtidig kan det være vanskelig for domstolen å etterprøve enkelte av vilkårene i lovforslaget, slik at de øvrige foreslåtte tilsyns- og kontrollmekanismene vil fylle en viktig funksjon.

Oslo tingrett uttaler:

> «Tingretten er enig med departementet i at et krav om forhåndstillatelse fra domstolene vil utgjøre en rettssikkerhetsgaranti, både ved at det utføres legalitetskontroll, og ved at en slik ordning sannsynligvis [vil] ha en disiplinerende virkning for Etterretningstjenesten. Den forutgående domstolskontrollen må dessuten sees i sammenheng med tilsyns- og kontrollsystemet for øvrig.»

Flere høringsinstanser er kritiske til at retten skal være avhengig av Etterretningstjenesten for sakens opplysning, spesielt med hensyn til tekniske forhold. Det tas derfor til orde for å styrke rettens mulighet til å få uavhengig faglig bistand, for eksempel ved å åpne for at retten kan oppnevne sakkyndig. *Advokatforeningen*, *Borgarting lagmannsrett*, *Den norske dataforening – IT-politisk råd*, *ICJ-Norge*, *dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors*, *Elektronisk Forpost Norge* og *Norges institusjon for menneskerettigheter (NIM)* gir uttrykk for synspunkter i denne retningen. NIM uttaler:

> «Behovet for særskilt kompetanse er fremhevet av EMD. Ettersom det er lagt opp til at avgjørelsene skal treffes av ordinære dommere, er det nærliggende at retten gis fagkyndig bistand. Av hensyn til domstolens uavhengighet er NIM i utgangspunktet lite positive til forslaget om at dette alene ivaretas ved at E-tjenesten selv medbringer fagkyndig. Etter NIMs oppfatning bør det legges opp til et spor hvor domstolen kan innhente uavhengig faglig bistand, og på den måten også sikre at domstolens kontroll oppleves som reell, effektiv og uavhengig.»

11.9.1.3 Departementets vurdering

Departementet har i punkt 10.13 drøftet hvorvidt det bør oppstilles et generelt krav om domstolens forhåndsgodkjennelse av Etterretningstjenestens metodebruk. Spørsmålet ble besvart benektende. Det er imidlertid grunn til å vurdere spørsmålet særskilt når det gjelder tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon, på grunn av det særpreget tilgangen har som følge av at det vil lagres store mengder metadata om norsk innenlandsk kommunikasjon. Særpreget tilsier etter departementets syn at det oppstilles et krav om uavhengig forhåndsgodkjennelse. Departementet viser også til at Lysne II-utvalget gikk inn for å oppstille et krav om forhåndsgodkjennelse av en domstol.

Et alternativ kunne være å legge oppgaven til EOS-utvalget eller til et nytt, uavhengig forvalt-

ningsorgan. Departementet mener imidlertid at hensyn til legitimitet, tillit og rettssikkerhet taler for å legge oppgaven til domstolene. Departementet mener, på samme måte som *Domstoladministrasjonen* og *Oslo tingrett*, at kravet om forhåndstillatelse vil være en viktig rettssikkerhetsgaranti. Domstolen vil føre kontroll med lovligheten av Etterretningstjenestens begjæringer om bruk av tilgangen, og det må antas at slik kontroll vil ha en disiplinerende effekt på tjenesten.

Flere høringsinstanser mener at det kan være vanskelig for domstolene å gjennomføre en reell kontroll, blant annet på grunn av skjønnsmessige vilkår. Departementet har forståelse for synspunktet. Effektiviteten av domstolskontrollen må ses i sammenheng med hvordan vilkårene er utformet, og noen vilkår kan være vanskelige å overprøve. For eksempel kan ikke grunnvilkårene for innhenting være for strenge. Det er heller ikke til å komme fra at enkelte vilkår må bygge på skjønn, her som på andre rettsområder. På samme måte som i høringsnotatet kan det derfor være grunn til å advare mot urealistiske forestillinger om hvor høy grad av rettssikkerhet og hvor godt personvern som kan oppnås ved å kreve domstolens forhåndsgodkjennelse. Departementet mener like fullt at domstolens forhåndskontroll vil være reell, og fylle en viktig funksjon i det samlede kontrollsystemet.

Flere høringsinstanser, som *Advokatforeningen* og *Datatilsynet*, tar til orde for at domstolens faktiske mulighet til å utøve en reell kontroll må styrkes. Departementet tar disse tilbakemeldingene på alvor, og foreslår på bakgrunn av dem flere tiltak som skal styrke kontrollfunksjonen. Etter høringen foreslås det lovfestet at retten som hovedregel skal oppnevne særskilt advokat (punkt 11.9.5), og det stilles strengere krav til spesifisering av begjæringen (punkt 11.9.4). Dessuten gis domstolen myndighet til å pålegge stansing av pågående innhenting etter begjæring fra EOS-utvalget (punkt 11.10.4).

Departementet har vurdert hvorvidt det bør åpnes for at retten kan oppnevne en uavhengig sakkyndig, slik flere høringsinstanser tar til orde for, men foreslår ikke dette. Det bør etter departementets syn holdes fast ved at det er Etterretningstjenesten som skal sørge for sakens opplysning. Teknisk innhenting innenfor utenlandsetterretning er en høyt spesialisert disiplin som av legitime grunner er skjermet, og det vil derfor være vanskelig å finne egnet sakkyndighet. Sikkerhetshensyn taler også mot å involvere flere aktører i saksbehandlingen. Det vises til at retten ikke har adgang til å oppnevne sakkyndig i saker etter politiloven § 17 d, hvor tilsvarende hensyn gjør seg gjeldende. Departementet legger til grunn at retten vil få et forsvarlig faktisk avgjørelsesgrunnlag gjennom den skriftlige begjæringen og uttalelsen fra den særskilte advokaten, eventuelt i kombinasjon med den supplerende informasjon fra tjenesten som retten måtte be om, som kan gis både skriftlig og i rettsmøte.

Departementet vil understreke at domstolskontrollen må ses i sammenheng med tilsyns- og kontrollsystemet for øvrig, slik også *Domstoladministrasjonen* og *Oslo tingrett* trekker frem i sine høringsuttalelser. Sammen med domstolens forhåndskontroll vil EOS-utvalgets løpende kontroll og etterfølgende kontroll være sentrale elementer i systemet. I tillegg til denne uavhengige kontrollen kommer Etterretningstjenestens internkontroll og departementets forvaltningskontroll. Nasjonal kommunikasjonsmyndighet (Nkom) vil dessuten føre kontroll med hvordan tilbydere som omfattes av Nkoms tilsynsmyndighet utøver tilretteleggingsplikten.

11.9.2 Plassering av domstolskontrollen

11.9.2.1 Forslaget i høringsnotatet

I høringsnotatet punkt 11.11.4.2 drøftes hvorvidt domstolskontrollen bør legges til de alminnelige domstoler eller til en særdomstol. Lysne II-utvalget tok ikke stilling til dette spørsmålet.

Det vises i høringsnotatet til grunner som taler for en form for dommerspesialisering. Et alternativ er å opprette en spesialdomstol, som i Sverige. Hensynet til legitimitet og tillit i befolkningen taler imidlertid for å legge kontrollen til de alminnelige domstolene. For å legge til rette for en viss form for dommerspesialisering foreslås det å legge sakene til Oslo tingrett.

11.9.2.2 Høringsinstansenes syn

De fleste høringsinstansene som uttaler seg om spørsmålet, støtter forslaget om å legge sakene til de alminnelige domstolene med Oslo tingrett som førsteinstans. Dette gjelder *Advokatforeningen*, *Amnesty International*, *Borgarting lagmannsrett*, *Det nasjonale statsadvokatembetet*, *dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors*, *Domstoladministrasjonen*, *Kripos* og *Oslo tingrett*. *Domstoladministrasjonen* ser samtidig behovet for at dommere som skal jobbe innenfor feltet må få opparbeide seg kompetanse, og uttaler:

«I forbindelse med kompetansebygging i forhold til kjennskap til Etterretningstjenesten må man være oppmerksom på faren for identifikasjon dersom slik kompetanse skal formidles av Etterretningstjenesten selv. På grunn av kravet til sikkerhetsklarering vil det uansett være et mindre antall dommere som skal behandle slike saker, og de vil på sikt opparbeide seg erfaring med sakstypen.»

Dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors uttaler:

«Vi mener ikke det er behov for å opprette en egen domstol, slik de har i Sverige. Det ville stride mot vår tradisjon med dommere som er generalister, dog slik at det skjer en moderat spesialisering. På området her er det naturlig at det skjer en spesialisering, i og med at dommerne må sikkerhetsklareres. Dette vil i så fall bli en parallell til hvordan begjæringene fra PST behandles. Det kan også være at dommerne bør ha særskilt kompetanse på persongrupper som kan bli særlig utsatt for etterretningen, eller lignende.»

Datatilsynet uttaler:

«Siden vilkårene er vidt formulert vil det kreve høy kompetanse hos dommerne for å kunne etterprøve nødvendighet og forholdsmessighet av tiltaket som det bes om godkjenning til. Dette krever igjen grundig innsikt og kunnskap i den etterretningsfaglige verdien som søkes oppnådd ved søk i informasjon og/eller lagring av innholdsdata.

Videre vil domstolen måtte foreta en vurdering av forholdsmessighet som innebærer at dommere må kunne overskue konsekvensene av det aktuelle tiltaket. Dette krever god kunnskap om de tekniske løsninger for å vite hvordan og hvem som vil bli rammet av tiltaket. Med de tekniske innretninger som er foreslått i høringsnotatet er vi bekymret for at kompleksiteten overstiger kompetansen til den jevnlige dommer i Oslo tingrett, selv om det blir en slik spesialisering som departementet foreslår.

Vi stiller spørsmål ved hvor realistisk disse kompetansekrav til dommerne er, og er bekymret for at de fleste dommere ikke vil ha de kunnskaper som kreves for å foreta en [reell] avveiing av disse momentene. Dette vil i realiteten innebære en uthuling av domstolskontrollen.»

11.9.2.3 Departementets vurdering

Departementet opprettholder forslaget i høringsnotatet om å legge domstolskontrollen til de alminnelige domstoler, med Oslo tingrett som førsteinstans. Hensynet til legitimitet og tillit i befolkningen tilsier en slik løsning, som har fått bred støtte av høringsinstansene.

Som flere høringsinstanser påpeker, er tilstrekkelig fagkompetanse en forutsetning for at retten skal kunne foreta en reell kontroll. Dette kunne isolert sett tilsi å legge sakene til en uavhengig særdomstol med spesialiserte dommere. Å opprette en særdomstol ville gitt virksomheten en tydelig egen identitet, og lagt til rette for utviklingen av et spesialisert fagmiljø. På den andre siden er risikoen for at dommerne i for stor grad vil identifisere seg med sitt eget fagområde større i en særdomstol enn i de alminnelige domstolene, hvor dommerne er generalister som behandler alle sakstyper. Departementet stiller seg dessuten tvilende til hvorvidt saksmengden vil være av en størrelse som kan forsvare opprettelsen av en særdomstol. På denne bakgrunn mener departementet at forhåndskontrollen bør legges til de alminnelige domstoler.

Den generelle kompetansen til dommerne i de alminnelige domstolene er høy. Det er nok slik at etterretningsfaget til å begynne med vil være ukjent for de fleste dommerne, både med hensyn til rettslige og faktiske forhold. At dommere må sette seg inn i nye fagfelt, er likevel ikke en uvanlig situasjon; det kan snarere regnes som et trekk ved den norske tradisjonen med alminnelige domstoler. Etter departementets syn er det like fullt viktig at de aktuelle dommerne har en viss innsikt i etterretningsfaget, sikkerhetspolitiske forhold og tekniske forhold ved innhentingen. Dette har betydning for muligheten til å foreta en reell prøving av begjæringene. En konsekvens av at domstolskontrollen blir lagt til de alminnelige domstolene, er at spesialiseringen blir mer begrenset enn hvis det opprettes en særdomstol. Domstolen bør like fullt sørge for en viss form for spesialisering. Dette kan skje gjennom at domstolen setter en begrenset gruppe dommere til å behandle de aktuelle sakene, slik at disse dommerne over tid opparbeider seg erfaring med sakstypen. Dette er naturlig også på grunn av at behandling av sakene vil kreve sikkerhetsklarering og autorisasjon etter reglene i sikkerhetsloven og klareringsforskriften kapittel 5.

Det bør legges til rette for at dommerne får bygget kompetanse gjennom kursdeltakelse, studiepermisjoner eller lignende. Slike tiltak må gjen-

nomføres på en måte som ivaretar domstolenes uavhengighet. Etterretningstjenesten og andre deler av forvaltningen kan være sentrale kilder til relevant kunnskap og kompetanse om fagfeltet, men som påpekt av *Domstoladministrasjonen* må man i denne sammenhengen være oppmerksom på faren for identifikasjon. Kompetansetiltakene bør derfor gjennomføres på domstolens initiativ og på den måten som domstolen ønsker det.

11.9.3 Hva domstolen skal prøve

11.9.3.1 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 11.11.4.3 at retten skal foreta en forutgående legalitetskontroll av bruken av tilrettelagt innhenting. Dette innebærer at retten 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.

I høringsnotatet er regler om hva retten skal prøve inntatt i lovutkastet § 8-4.

11.9.3.2 Høringsinstansenes syn

Det synes ikke å være noen uenighet blant høringsinstansene om at retten skal prøve om lovens vilkår er oppfylt, men som omtalt under punkt 11.9.1.2 påpeker flere at det kan være vanskelig å føre en reell kontroll med enkelte av vilkårene.

Amnesty International mener at forslaget vil sikre en grundig rettslig prøving, og at en klar angivelse i loven av hva retten skal prøve må anses å være en avgjørende rettssikkerhetsmessig garanti.

Norsk Journalistlag, *Norsk Presseforbund*, *Norsk Redaktørforening* og *NRK* er kritiske til at lovutkastet § 9-6, som fastsetter en særskilt terskel for behandling av fortrolig kommunikasjon med særlige yrkesutøvere, ikke er blant bestemmelsene som er oppregnet i lovutkastet § 8-4.

Datatilsynet viser til at domstolens prøving av saker om kommunikasjonskontroll har blitt kritisert for å fremstå som lite reell. Tilsynet viser til statistikk fra 2016 som viser at det ble brukt kommunikasjonskontroll i 135 saker. Tingretten avslo politiets begjæring i to av sakene, men det ble gitt tillatelse i begge sakene etter anke.

11.9.3.3 Departementets vurdering

Departementet viderefører forslaget i høringsnotatet om at retten skal prøve hvorvidt lovens vilkår er oppfylt.

Flere presseaktører stiller seg kritiske til at § 9-6 i høringsnotatet, som blant annet oppstiller et særskilt vern for journalistisk materiale, ikke er regnet opp i § 8-4 som en av bestemmelsene retten skal prøve. Departementet bemerker at § 9-6 i høringsnotatet ikke gjelder for behandling i form av innhenting, noe som videreføres i proposisjonen. Den høye terskelen for inngrep i kildevernet vil likevel være gjenstand for prøving av domstolen som et ledd i forholdsmessighetsvurderingen etter § 5-4. Dette innebærer for eksempel et tilnærmet absolutt forbud mot målrettet innhenting etter lovforslaget § 7-9 av kommunikasjon mellom en journalist mv. som er vernet av lovforslaget § 9-6 og en kilde, og dette vil prøves av retten. Det vises for øvrig til punkt 12.8.6.

Datatilsynet viser til statistikk fra 2016 som gjelder det alminnelige politiets bruk av kommunikasjonskontroll. Statistikken viser at politiet fikk rettens tillatelse i alle sakene som ble behandlet. Departementet tilføyer at statistikken for 2017 viser at retten avslo seks saker av et totalt antall på 160. I to av disse sakene ble det gitt tillatelse etter anke. For 2018 ble det gitt helt eller delvis avslag i fire av 130 saker. I én av sakene ble tillatelse gitt etter anke. Statistikken viser at det blir gitt tillatelse i en stor andel av sakene. Det er grunn til å tro at det samme vil gjelde for saker etter lovforslaget i denne proposisjonen, fordi Etterretningstjenesten, blant annet på grunn av kontrollens disiplinerende virkning, neppe vil fremme begjæringer med dårlige utsikter til å føre frem. Det kan derfor ikke uten videre sluttes fra en høy andel tillatelser til at kontrollen ikke er reell.

11.9.4 Saksbehandlingen

11.9.4.1 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 11.11.4.4 at saksbehandlingen ved domstolen skal 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. Forslaget oppstiller ikke krav om at begjæringene må individualiseres. Det vil derfor kunne fremmes begjæringer som består av et sakskompleks. Kompetansen til å

fremsette begjæring bør i utgangspunktet ligge til sjefen for Etterretningstjenesten, men bør kunne delegeres. Hensyn til notoritet og forsvarlig saksbehandling tilsier at begjæringen må være skriftlig.

Det vises i høringsnotatet til at begjæringen må inneholde den informasjonen som er nødvendig for at domstolen skal kunne prøve om lovens vilkår er oppfylt. Omfanget vil kunne variere fra sak til sak, men det må påvises 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. Hvis retten mener at begjæringen ikke gir tilstrekkelig grunnlag for avgjørelsen, kan den kreve ytterligere opplysninger.

Etter forslaget i høringsnotatet kan retten beslutte muntlige forhandlinger for å opplyse saken ytterligere, og Etterretningstjenesten kan i så fall stille med tjenestepersoner eller andre som kan opplyse saken. Retten avgjør saken i form av en skriftlig kjennelse som skal begrunnes.

I høringsnotatet er det inntatt regler om rettens kjennelser i § 8-1, krav til begjæringen i § 8-2 og rettsmøte i § 8-3.

11.9.4.2 Høringsinstansenes syn

Flere høringsinstanser mener at det bør stilles strengere krav til begjæringens innhold, herunder *Datatilsynet* og *Norges institusjon for menneskerettigheter (NIM)*. NIM uttaler:

> «I høringsnotatet på side 238 fremgår det at det er tilstrekkelig at E-tjenestens begjæringer «består av et sakskompleks». Det fremstår uklart hvilken grad av spesifisering det her er snakk om. Videre på samme sted i høringsnotatet fremgår det at det ikke er lagt opp til et krav om at begjæringene må «individualiseres». Her må det klargjøres nærmere hvor omfattende eller avgrensede E-tjenestens begjæringer må være, noe som igjen spiller inn på omfanget av rettens kjennelser. Som det fremgår over, har EMD lagt vekt på i hvilken grad kjennelser som autoriserer overvåking er spesifiserte. For å sikre en kvalitativt forsvarlig domstolkontroll, mener NIM det er viktig at det fastsettes kriterier som avgrenser omfanget av begjæringene på en måte [som] gjør at rettens vurdering ikke bare knytter an til generelle behov i et overordnet sakskompleks, men heller de konkrete stadiene i saken som gjør søk og innhenting nødvendig. Det fremgår for eksempel av lovforslaget § 8-6 at rettens tillatelse ikke skal gis lenger enn nødvendig. For at domstolene skal kunne vurdere dette på en forsvarlig måte, er det nødvendig at begjæringen inneholder informasjon om begrunnelse for foreslått tidsramme slik at domstolen også har mulighet til å begrense denne etter en selvstendig vurdering. Retten skal dessuten kontrollere at E-tjenesten ikke behandler 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.» For å kunne foreta en meningsfull kontroll av dette, kreves også mer konkretisert innsikt i hvilke vurderinger som ligger bak E-tjenestens begjæring.»

NIM viser til at Etterretningstjenesten i sin begjæring skal angi hva eller hvem søkene rettes mot, men at den ikke må angi hvilke søkebegreper som skal benyttes:

> «Søkebegrepene vil være direkte avgjørende for hva E-tjenesten får tilgang på og omfanget av tilgangen. Følgelig er det vanskelig å se annet enn at søkebegrepene nødvendigvis utgjør den direkte og avgjørende faktoren for om søk og innhenting er forholdsmessig i konkrete saker. En ordning der retten kun tar stilling til abstraherte person- og moduselektorer og E-tjenesten utarbeider konkrete søkekriterier på grunnlag av disse, vil potensielt gi E-tjenesten et betydelig skjønn ved påfølgende innhenting og søk, noe som skaper en ganske klar risiko for misbruk. Videre kommer det at EOS-utvalget ikke er bemyndiget til å stanse søk eller slette informasjon fra søk som ikke omfattes av kjennelsen eller som er uforholdsmessige.
>
> For at rettens prøving skal anses fullstendig, mener NIM at E-tjenestens begjæring bør inneholde søkebegreper og at E-tjenesten med rettens kjennelse ikke kan gå ut over disse. Dette medfører også at retten kan ekskludere enkelte søkekriterier, f.eks. hvis det er stor risiko for at disse vil frembringe særlig beskyt-

tet kommunikasjon eller i for stor grad ramme personer i Norge. Hvis det viser seg at de aktuelle søkebegrepene ikke er tilstrekkelige og at andre søkebegreper kan frembringe relevante resultater, kan E-tjenesten fremme en ny begjæring for retten. Dette kan medføre at E-tjenesten i en operasjon må begjære flere tillatelser, noe som igjen bidrar til minimalisering og ivaretakelse av at søk og innhenting begrenses til hva som er nødvendig og forholdsmessig.»

NIM fremholder videre at det bør fremgå eksplisitt at retten skal ha tilgang på alle relevante opplysninger i saken, og at retten helt generelt kan kreve fremlagt ytterligere opplysninger.

Borgarting lagmannsrett uttaler:

«For at domstolsprøvingen skal bli reell og effektiv må det stilles ganske store krav til begjæringene. Disse må være konkrete, beskrive det aktuelle formålet og redegjøre for hvorfor det foreligger «grunn til å undersøke». Videre må begjæringen gi retten alle opplysninger som trengs for å kunne vurdere forholdsmessigheten.»

Dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors gir uttrykk for synspunkter i samme retning. De peker også på muligheten til å avholde muntlige forhandlinger som viktig, og uttaler:

«Vi mener at det vil være nødvendig med utstrakt bruk av muntlige forhandlinger, særlig i startfasen før det foreligger rettspraksis. Det er tale om svært inngripende innhenting av informasjon som rammer potensielt svært mange personer og virksomheter. I startfasen vil det være nødvendig å stille spørsmål for å forstå hva saken gjelder.»

Advokatforeningen mener at det bør oppstilles som hovedregel at domstolens prøving skal skje på grunnlag av muntlige forhandlinger:

«Domstolenes metode for å komme frem til det materielt riktige resultat er i alminnelighet tuftet på kontradiksjon mellom sakens parter. I saker etter utkastet kapittel 8 er domstolens forutsetning for å komme frem til det riktige resultat derfor dårligere enn i andre saker for domstolene. Dette skyldes at den ene part ikke er til stede. Denne kan ikke uttale seg, og det kontradiktoriske prinsipp er satt til side. Oppnevning av særskilt advokat som et minstekrav vil riktignok avhjelpe et stykke på vei. Den særskilte advokaten kan imidlertid ikke tilegne seg kunnskap om sakens faktum utover det som følger av utk. § 8-5. Det er med andre ord Etterretningstjenesten som alene fremlegger faktum i saken for retten.

Når dette er utgangspunktet er det et paradoks at både dommerens og den særskilte advokatens rammevilkår ytterligere skal svekkes ved at hovedregelen skal være at det ikke er muntlige forhandlinger. Muntlige forhandlinger vil bedre både dommerens og advokatens muligheter til å sette seg inn i saken og få uklare punkter avklart. Kontradiksjonen vil styrkes, dommeren vil få et bedre grunnlag for sin avgjørelse, og den intenderte kontrollen i utkastet kapittel 8 vil lettere bli oppnådd. Den best mulige domstolskontroll vil dessuten styrke tilliten til at systemet fungerer.

Det er Advokatforeningens mening at et krav om muntlige forhandlinger ikke vil medføre nevneverdige forsinkelser. Løsningene for å ivareta hensynet til hurtig avvikling av sakene kan være flere, hvorav vaktturnuser blant de særskilte advokatene er én.»

EOS-utvalget foreslår at både kjennelsen og den underliggende begjæringen skal meddeles til utvalget. Utvalget peker på at de må kjenne forutsetningene som kjennelsen bygger på for å være i stand til å føre en dekkende kontroll med hvorvidt tjenestens søk er i samsvar med kjennelsens innhold.

11.9.4.3 Departementets vurdering

Departementet viderefører i hovedsak forslaget i høringsnotatet, men med noen endringer som følge av høringen. Departementet er enig med høringsinstansene som mener at loven bør angi mer presise krav til hva begjæringen skal inneholde, herunder *Datatilsynet* og *Norges institusjon for menneskerettigheter (NIM)*. Det foreslås i tråd med dette å liste opp krav til begjæringens innhold i lovforslaget § 8-2.

Forslaget innebærer blant annet at det i begjæringen skal angis hvilke søkebegreper eller kategorier av søkebegreper som skal brukes til å søke i lagrede metadata. Søkebegrepene kan knytte seg til en person (personselektor) eller et bestemt mønster eller avgrensning (modusselektor). At det kan angis kategorier av søkebegreper, innebærer at de konkrete søkebegrepene ikke nødvendigvis vil prøves av retten. Kategorier kan for

eksempel gjelde alle selektorer (som telefonnumre og e-postadresser) knyttet til en bestemt person, eller alle personer som har en nærmere kvalifisert tilknytning til en bestemt organisasjon, for eksempel en fremmed sikkerhets- og etterretningstjeneste. *NIM* går i sin høringsuttalelse inn for et krav om prøving av konkrete søkebegreper. Departementet mener at en slik løsning ikke vil la seg gjennomføre i praksis, fordi relevante nettidentiteter og handlingsmønstre vil være i rask og hyppig endring. Departementet viser til at både svensk og finsk lovgivning åpner for at begjæringene kan angi kategorier av søkebegreper. Det vises dessuten til at EOS-utvalget vil kunne begjære stansing hvis utvalget mener at det brukes søkebegreper som ikke ligger innenfor rammen av rettens tillatelse, jf. punkt 11.10.4. Dette minimerer den risikoen for misbruk som NIM peker på i sin høringsuttalelse.

Departementet understreker at retten vil kunne kreve mer informasjon dersom den mener at begjæringen ikke gir et tilstrekkelig grunnlag for avgjørelsen, både skriftlig og i form av muntlige forhandlinger etter lovforslaget § 8-3. Departementet er enig med *Advokatforeningen* og *dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors* i at muntlige forhandlinger kan være et viktig virkemiddel for å opplyse saken. Muntlige forhandlinger vil antakelig brukes hyppig spesielt i den første tiden, men kan være aktuelt også i en senere fase, avhengig av sakens karakter og rettens behov for avklaringer. I lys av høringsuttalelsen til *Advokatforeningen* vil departementet bemerke at lovforslaget ikke oppstiller som hovedregel at det ikke skal avholdes muntlige forhandlinger, men lar dette være opp til retten å vurdere i den enkelte sak.

EOS-utvalget går inn for at utvalget bør gjøres kjent med både kjennelsen og begjæringen som ligger til grunn for den. Departementet slutter seg til dette, og foreslår en slik regel i lovforslaget § 8-1 tredje ledd.

11.9.5 Særskilt advokat

11.9.5.1 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 11.11.4.4 en ordning med oppnevnelse av særskilt advokat for den som berøres av en begjæring om tilrettelagt innhenting. Det vises til at det er viktig for balansen i domstolsprosessen at en av aktørene har som oppgave å stille kritiske spørsmål til begjæringen og sørge for å belyse personvernhensyn som grunnlag for rettens forholdsmessighetsvurdering i den enkelte sak.

Det foreslås i høringsnotatet at advokaten skal ivareta interessene både til den eller de som innhentingen retter seg mot og interessene til eventuelle tredjepersoner. Det bør være opp til retten å beslutte oppnevning. Hvis innhentingen retter seg mot en eller flere bestemte personer, bør advokat som hovedregel oppnevnes. I noen saker vil ikke innhentingen rette seg mot bestemte personer eller grupper. Retten bør likevel kunne oppnevne advokat, for eksempel for å belyse mer allmenne personverninteresser som gjør seg gjeldende.

Etter forslaget skal 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.

I høringsnotatet er oppnevnelse av særskilt advokat regulert i lovutkastet § 8-5.

11.9.5.2 Høringsinstansenes syn

Ingen høringsinstanser har hatt innvendinger mot forslaget om oppnevnelse av særskilt advokat i saker om tilrettelagt innhenting. *Advokatforeningen*, *Amnesty International*, *Borgarting lagmannsrett*, *dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors*, *Kripos* og *Norges institusjon for menneskerettigheter* mener at det bør være obligatorisk å oppnevne særskilt advokat. *Norsk Journalistlag* fremholder at terskelen for å oppnevne advokat bør være lav, og at det alltid bør oppnevnes advokat når man står overfor behandling av opplysninger som kan omfatte kildemateriale.

Oslo tingrett uttaler:

> «I forslagets § 8-5 er det lagt opp til at retten kan oppnevne en særskilt advokat for å ivareta rettighetene til den eller de som innhentingen retter seg mot. Til forskjell fra den obligatoriske ordningen med særskilt advokat ved behandling av saker om skjulte tvangsmidler i dag, jf. straffeprosessloven § 100a og politiloven § 17e, er den foreslåtte lovbestemmelsen i utformet som en kan-regel. Oslo tingrett støtter at dette bør være hovedregelen. Etter forslaget kan særskilt advokat oppnevnes også for å ivareta mer allmenne personverninteresser, noe som er naturlig siden begjæringene må antas å ikke alltid rette seg mot bestemte per-

soner. Det bør vurderes å gjøre dette til en skalregel.»

11.9.5.3 Departementets vurdering

Departementet viderefører forslaget i høringsnotatet om en ordning med oppnevnelse av særskilt advokat i saker om forhåndskontroll av tilrettelagt innhenting, men med noen endringer som følge av høringen.

Departementet tar som utgangspunkt at tilrettelagt innhenting må skje i det skjulte overfor aktører som innhentingen berører. Noe annet ville undergrave formålet med innhentingen. Det følger av dette at de berørte ikke kan underrettes om eller ta del i en sak om forhåndsgodkjennelse av innhentingen. En kontradiktorisk domstolsbehandling lar seg derfor ikke gjennomføre på vanlig måte. Når dette er situasjonen, mener departementet at det må legges til rette for en saksbehandling som kan ivareta rettssikkerhetshensyn og andre samfunnsinteresser så langt det er mulig.

En kontradiktorisk saksbehandling kan i en viss utstrekning ivaretas gjennom at retten oppnevner en særskilt advokat. I straffeprosessen ble en slik ordning innført i 1999 gjennom vedtakelsen av straffeprosessloven § 100 a. Bestemmelsen ble vedtatt etter forslag fra Metodeutvalget, som omtalte advokatens rolle slik (NOU 1997: 15 punkt 6.2.10 side 152 til 153):

> «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.
>
> 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 disse betraktningene knytter seg til straffeprosessen, har de etter departementets syn relevans også for domstolens forhåndskontroll av tilrettelagt innhenting. Det er viktig for balansen i domstolsprosessen at en av aktørene har som oppgave å målbære allmenne interesser i saken, stille kritiske spørsmål til Etterretningstjenestens begjæring og belyse personvernhensyn og andre samfunnsinteresser som potensielt kan lide utilbørlig skade av innhentingen, som ytrings- og informasjonsfriheten og religionsfriheten. Ved å gi den særskilte advokaten rett til å anke, åpnes det også for at en sak kan prøves i flere instanser.

Forslaget i høringsnotatet er utformet som en «kan»-regel som lar det være opp til retten å beslutte om det skal oppnevnes særskilt advokat. Flere *høringsinstanser* tar til orde for at oppnevning bør være obligatorisk. Departementet mener etter høringen at oppnevning bør være den store hovedregelen, og foreslår derfor at retten «skal» oppnevne særskilt advokat. Retten bør imidlertid kunne unnlate å oppnevne særskilt advokat hvis det anses ubetenkelig. Hvorvidt oppnevnelse kan unnlates, må avgjøres konkret. Det kan for eksempel være aktuelt hvis søket eller innhentingen i liten grad vil gripe inn i vernede interesser, typisk i saker som gjelder statlige aktørers spionasje- eller sabotasjevirksomhet mot Norge.

Det presiseres i forslaget at den særskilte advokaten skal oppnevnes etter at retten har mottatt begjæringen om tillatelse, og at advokaten skal ha godtgjørelse av staten.

Lovforslaget gir departementet hjemmel til å gi forskrift om oppnevning av særskilt advokat, for eksempel om godtgjørelse.

11.9.6 Tillatelsens varighet

11.9.6.1 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 11.11.4.4 at retten i den enkelte sak skal vurdere og ta stilling til varigheten av tillatelsen. Hovedregelen bør være at tillatelsen ikke skal vare lenger enn nødvendig. Dessuten tilsier personvernhensyn en yttergrense for tillatelsens varighet. Det foreslås en maksimal varighet på ett år når søket gjelder målsøking og seks måneder når søket gjelder målrettet innhenting.

Det foreslås av pedagogiske grunner å lovfeste at Etterretningstjenesten skal avslutte pågående søk av eget tiltak dersom vilkårene ikke lenger er til stede, for eksempel hvis nye faktiske omsten-

digheter gjør at inngrepet ikke lenger kan regnes som forholdsmessig.

I høringsnotatet er regler om tillatelsens varighet inntatt i lovutkastet § 8-6.

11.9.6.2 Høringsinstansenes syn

Amnesty International uttaler:

> «Vi støtter forslaget om at retten skal avgjøre varighet for tillatelsen slik at varighet begrenses til det strengt nødvendige. Vi støtter også forslaget om å lovfeste at Etterretningstjenesten skal avslutte søk av eget tiltak dersom vilkårene etter loven ikke lenger er oppfylt. Denne presiseringen vil tydeliggjøre etterretningstjenestens til enhver tid selvstendige ansvar for å vurdere om vilkårene for lovlig inngrep er oppfylt. En forutgående rettslig kjennelse skal ikke kunne legitimere inngrep der forutsetningene for kjennelsen er endret.»

NRK uttaler at det kan spørres hvor reell domstolskontrollen blir når tillatelsene kan gis for lang tid. *Norsk Presseforbund* mener at domstolskontrollen må skje oftere når det er snakk om så alvorlige inngrep som her. *Kripos* gir uttrykk for lignende synspunkter.

11.9.6.3 Departementets vurdering

Departementet opprettholder forslaget i høringsnotatet om å lovfeste at tillatelsen ikke skal vare lenger enn nødvendig. Forslaget innebærer at retten i den enkelte sak skal vurdere og ta stilling til hvor lenge tillatelsen bør vare. Departementet mener dessuten at loven bør oppstille en lengstefrist, og opprettholder forslaget i høringsnotatet om at denne bør være ett år ved målsøking og seks måneder ved målrettet innhenting. Når en tillatelse har løpt ut eller er i ferd med å løpe ut, må Etterretningstjenesten fremme ny begjæring hvis den ønsker å gjenoppta eller fortsette søket eller innhentingen.

I lys av høringsuttalelsene til *Kripos*, *Norsk Presseforbund* og *NRK* vil departementet understreke at fristene på seks måneder og ett år er lengstefrister. Retten kan sette en kortere frist hvis det i en konkret sak er grunn til hyppigere domstolskontroll, for eksempel fordi det er grunn til å tro at faktiske forhold av betydning for lovligheten vil kunne endre seg i løpet av et kortere tidsrom.

Departementet viderefører også forslaget om å lovfeste at Etterretningstjenesten skal avslutte pågående søk av eget tiltak dersom vilkårene ikke lenger er til stede, for eksempel fordi nye faktiske omstendigheter gjør at inngrepet blir uforholdsmessig. En slik plikt må sies å følge allerede av lovens system, men som påpekt av *Amnesty International* kan det være grunn til å tydeliggjøre den i loven.

11.9.7 Offentlighet

11.9.7.1 Forslaget i høringsnotatet

I høringsnotatet punkt 11.11.4.4 vises det til at offentlighetsprinsippet er et grunnleggende prinsipp i norsk domstolsprosess, men at det ligger i sakens natur at tilrettelagt innhenting må skje i det skjulte overfor personer som den berører og offentligheten for øvrig. Noe annet vil undergrave formålet med innhentingen. Det foreslås derfor i høringsnotatet at rettsmøtene skal holdes for lukkede dører og at rettens avgjørelser ikke kan gjengis offentlig.

11.9.7.2 Høringsinstansenes syn

Datatilsynet uttaler:

> «Slik domstolskontrollen er utformet i forslaget vil den innebære en hemmelig forhåndskontroll ved Oslo tingrett. Behandlingen i sakene og kjennelsene vil ikke bli offentliggjort. Dette innebærer store utfordringer med hensyn til offentlighetens tillit til at det faktisk skjer en kontroll. Det må derfor stilles ekstra store krav til de prosessuelle og materielle reglene som skal gjelde for domstolskontrollen.»

Tekna innser at det er nødvendig å holde rettsmøter bak lukkede dører, men bemerker at lukket rett med kun advokater som er spesielt klarert, potensielt kan svekke tilliten til kontrollregimet. Tekna peker på at EOS-utvalget er viktig for å skape tillit til prosesser som i utgangspunktet mangler transparens.

Norsk Presseforbund mener at det er en stor svakhet at forhåndskontrollen er hemmelig, og at behandlingen av sakene og kjennelsene ikke offentliggjøres. Forbundet mener at dette i seg selv svekker tilliten til kontrollen, og skaper en uvisshet som i seg selv kan virke nedkjølende på ytringsfriheten.

Norges institusjon for menneskerettigheter (NIM), *Norsk Journalistlag* og *dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors* rei-

ser spørsmål om tilgang til rettspraksis og offentliggjøring av kjennelser. NIM skriver:

> «Den enkelte dommer som skal avgjøre saken alene, må ha tilgang til tidligere rettspraksis, slik at det blir en enhetlig tolkning av loven. Tilgangen bør være elektronisk og søkbar.
>
> NIM mener også at avgjørelsene bør offentliggjøres i anonym form i den grad hensynet til hemmelighold ikke gjør seg gjeldende.»

11.9.7.3 Departementets vurdering

Departementet tar som utgangspunkt at offentlighetsprinsippet er et grunnleggende prinsipp i norsk domstolsprosess. Prinsippet 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 i lov fastsettes begrensninger i denne retten ut fra hensyn til personvern og av andre tungtveiende grunner. Det følger av domstolloven § 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 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.

Noen *høringsinstanser* påpeker at manglende åpenhet kan utfordre tilliten til domstolskontrollen. Samtidig er det ikke til å komme fra at det er nødvendig å gjøre unntak fra offentlighetsprinsippet i disse sakene. Reglene om særskilt advokat med ankerett er blant tiltakene som skal bidra til å styrke tilliten til at domstolens kontroll er uavhengig og reell. Departementet understreker også i denne sammenhengen at forhåndskontrollen ved domstolene må ses i sammenheng med kontrollsystemet for øvrig.

Etter dette opprettholder departementet forslaget om at rettsmøtene skal holdes for lukkede dører. Det vises til lovforslaget § 8-3 andre ledd.

Flere *høringsinstanser* reiser spørsmål om tilgang til rettspraksis og offentliggjøring av kjennelser. Departementet mener at dommere som skal behandle saker etter lovforslaget bør ha tilgang til tidligere avgjørelser, og antar at dette kan la seg gjøre innenfor rammen av reglene gitt i og i medhold av sikkerhetsloven. Det foreslås at departementet kan gi nærmere regler om dommernes tilgang til rettspraksis. Det foreslås derimot ikke å gi regler om offentliggjøring av kjennelsene for allmennheten. Kjennelsene vil omhandle informasjon som må skjermes av hensyn til nasjonal sikkerhet, og som alle involverte plikter å bevare taushet om både etter sikkerhetsloven og lovforslaget her.

11.9.8 Ankeadgang

11.9.8.1 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 11.11.4.4 at Etterretningstjenesten og den særskilte advokaten skal ha rett til å anke kjennelser de er uenige i. Reglene i straffeprosessloven kapittel 26 om anke over kjennelser og beslutninger skal anvendes så langt de passer. Det bes om høringsinstansenes syn på hvorvidt det bør presiseres nærmere hvilke regler som passer, eventuelt ikke passer, og i så fall hvilke regler dette gjelder.

I høringsnotatet er regler om anke inntatt i lovutkastet § 8-9.

11.9.8.2 Høringsinstansenes syn

Ingen høringsinstanser har hatt negative merknader til forslaget i høringsnotatet om å gi Etterretningstjenesten og den særskilte advokaten rett til å anke. *Amnesty International* påpeker at adgang til å anke utgjør en viktig rettssikkerhetsgaranti.

Domstoladministrasjonen skriver:

> «Når det gjelder anke i forslaget § 8-9 antar Domstoladministrasjonen at det er tilstrekkelig å vise til at straffeprosessloven kapittel 26 gjelder så langt reglene passer. En presisering av hvilke bestemmelser i straffeprosessloven kapittel 26 som er aktuelle vil gjøre bestemmelsen uoversiktlig. Ankekompetansen er lagt til Etterretningstjenesten og den særskilte advokaten. Det vil dermed være forholdsvis få personer som har ankekompetanse og Domstoladministrasjonen antar at disse ikke vil [ha] behov for en nærmere presisering i loven av hvilke regler som passer. Hensynet til andre som leser loven kan heller ikke medføre et behov for ytterligere presisering.»

Oslo tingrett antar at det er hensiktsmessig å anvende straffeprosessloven kapittel 26 i ankesakene, men har ingen særlige synspunkter på om

det bør presiseres nærmere hvilke regler som passer, eventuelt ikke passer.

Borgarting lagmannsrett skriver:

> «Vi antar at i lagmannsretten som ankeinstans kan de fleste sakene behandles skriftlig, slik regelen ellers er ved anke over kjennelser, jf. straffeprosessloven § 385 første ledd. Men også her vil det nok, særlig de første par årene etter ikrafttredelsen, bli holdt muntlig forhandling i en ikke ubetydelig andel av sakene.»

Kripos gir uttrykk for at domstolen bør kunne bestemme oppsettende virkning.

11.9.8.3 Departementets vurdering

Departementet opprettholder forslaget i høringsnotatet om å gi Etterretningstjenesten og den særskilte advokaten rett til å anke kjennelser de er uenige i. Adgangen til å anke er en rettssikkerhetsgaranti som må antas å virke skjerpende for underinstansens avgjørelse.

Det foreslås å gi reglene i straffeprosessloven kapittel 26 om anke over kjennelser og beslutninger anvendelse så langt de passer. Dette kan være reglene om ankefrist (§ 379 første ledd), innledende saksbehandling ved tingretten (§ 381 første og andre ledd), oppsettende virkning (§ 382 første ledd), innhenting av ytterligere opplysninger (§ 384), ankedomstolens avgjørelse (§ 385), muntlige forhandlinger (§ 387 første ledd) og anke til Høyesterett (§§ 387 a og 388).

I høringsnotatet foreslo departementet at anke fra den særskilte advokaten ikke skulle ha oppsettende virkning. *Kripos* mener at retten bør kunne bestemme oppsettende virkning. Departementet er enig i dette, og viderefører ikke forslaget i høringsnotatet på dette punktet. Anken vil dermed som hovedregel ikke ha oppsettende virkning, men retten kan bestemme det motsatte.

11.9.9 Hastekompetanse

11.9.9.1 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 11.11.4.4 å gi sjefen for Etterretningstjenesten myndighet til å beslutte søk eller innhenting i kvalifiserte hastetilfeller. Bestemmelsen er ment som en meget snever unntaksregel som bare skal kunne brukes når det ved opphold vil være «stor fare» for at etterretningsinformasjon «av vesentlig betydning» kan gå tapt.

I høringsnotatet er regler om hastekompetanse inntatt i lovutkastet § 8-10.

11.9.9.2 Høringsinstansenes syn

Norsk Journalistlag fremholder at bestemmelsen mangler den rettssikkerhetsgarantien som kreves i saker som kan omfatte kildemateriale.

11.9.9.3 Departementets vurdering

Departementet tar utgangspunkt i at kravet til domstolens forhåndsgodkjennelse 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 det oppstilles 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 fra 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 alvorlig cyberangrep som finner sted på en helligdag, hvor tjenesten har behov for å søke i lagrede metadata for å kunne bidra til å motvirke angrepet.

Hastekompetansen bærer i seg en fare for misbruk. Departementet mener likevel at denne er begrenset, all den tid beslutningen vil være gjenstand for domstolskontroll kort tid etter at den ble fattet, samt løpende og etterfølgende kontroll av EOS-utvalget. Når det gjelder forholdet til kildevernet, viser departementet til punkt 12.8.

Departementet mener på denne bakgrunn at loven 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 Politiets sikkerhetstjeneste 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», se Prop. 68 L (2015–2016) punkt 13.5.4 side 209. 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. Kompetansen kan ikke delegeres, det vil si at det bare er sjefen eller den som fungerer som sjef i dennes fravær som kan fatte slik beslutning.

11.10 Løpende kontroll

11.10.1 Forslaget i høringsnotatet

I høringsnotatet punkt 11.12 drøftes behovet for løpende kontroll av tilrettelagt innhenting (i høringsnotatet benevnt styrket kontroll).

Det tas i høringsnotatet utgangspunkt i Lysne II-utvalgets anbefaling om å opprette et eget tilsyn under Samferdselsdepartementet til å foreta en uavhengig og løpende kontroll i nær sanntid. Det kunne ifølge utvalgets forslag vurderes å delegere forvaltningsansvaret for tilsynets virksomhet til Nasjonal kommunikasjonsmyndighet (Nkom). I høringsnotatet vises det til at EOS-utvalget og Nasjonal sikkerhetsmyndighet i sine høringsuttalelser til Lysne II-utvalgets rapport stilte seg kritiske til forslaget om å opprette et eget tilsyn, mens Nkom mente at de kunne ta på seg en slik oppgave.

Det redegjøres i høringsnotatet for menneskerettslige krav, kontrolloppgaven og sentrale hensyn i vurderingen. Deretter vurderes de ulike alternativene. Det første alternativet er et eget tilsyn i tråd med Lysne II-utvalgets forslag. Det andre alternativet er et særskilt kontrollorgan etter modell av Kontrollutvalget for kommunikasjonskontroll. Det tredje alternativet er å legge kontrollen til EOS-utvalget.

I høringsnotatet konkluderes det med at kontrolloppgaven bør legges til EOS-utvalget. Det legges særlig vekt på at EOS-utvalget har de beste forutsetningene for en god kontroll med Etterretningstjenestens virksomhet. Det legges dessuten vekt på sikkerhetshensyn, uavhengighetshensyn og hensynet til å opprettholde den norske kontrollmodellen.

På denne bakgrunn foreslås det i høringsnotatet å gi EOS-utvalget i oppgave å føre løpende kontroll med Etterretningstjenestens etterlevelse av bestemmelsene i lovforslaget kapittel 7 og 8. Kontrollen skal komme i tillegg til utvalgets alminnelige kontroll. Den bør foretas relativt hyppig og på EOS-utvalgets eget initiativ. Det vises til at mye av den utøvende rutinekontrollen i praksis vil utføres av EOS-utvalgets sekretariat, som bør forsterkes ytterligere i tillegg til den styrkingen som allerede er gjennomført.

Det fremholdes i høringsnotatet at EOS-utvalget bør ha full innsikt i begjæringene til domstolen og rettens kjennelser. 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. Ellers bør utvalget følge normale kontrollrutiner.

I samsvar med gjeldende regler bør EOS-utvalget ha uhindret adgang til nødvendig informasjon, og på forespørsel få innsyn i interne retningslinjer og prosedyrer, lokaler, utstyr, programvare, filteroppdateringer, aktivitetslogger og annet som benyttes for tilrettelagt innhenting.

I høringsnotatet er regler om løpende kontroll av tilrettelagt innhenting inntatt i lovutkastet § 7-11.

11.10.2 Høringsinstansenes syn

Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget) forstår forslaget slik at det skal føres en mer intensiv kontroll enn den som utvalget regelmessig fører med Etterretningstjenestens øvrige etterretningsvirksomhet, men at det for øvrig vil være opp til utvalget å vurdere kontrollintensiteten. Utvalget uttaler videre:

> «EOS-utvalgets kontroll med EOS-tjenestene, inkludert E-tjenesten, er ikke innrettet slik at den innebærer en full kontroll av alle sider av tjenestenes EOS-virksomhet. En fullstendig kontroll ville være for omfattende for utvalget, og det er et spørsmål om en slik kontroll overhodet er mulig eller ønskelig. Utvalget velger hvilke av tjenestens aktiviteter som skal undersøkes nærmere, blant annet basert på kriterier i EOS-kontrolloven og utvalgets vurderinger av hvor risikoen for rettighetskrenkelser og regelbrudd med alvorlige konsekvenser er størst. Selv om utvalget har full innsynsrett i E-tjenesten, med unntak for særlig sensitiv informasjon, vil ikke alle tjenestens aktiviteter bli kontrollert.
>
> Evalueringen av EOS-utvalget i 2016 viste at utvalgets kapasitet allerede da var presset. Utvalgsmodellen begrenser utvalgets kapasitet og dermed omfanget av kontrollvirksomheten. En utvidelse av kontrolloppgaven til å omfatte en styrket kontroll med tilrettelagt innhenting vil føre til flere oppgaver for utvalget. Det vil redusere utvalgets kapasitet til å kontrollere de andre EOS-tjenestene og andre sider ved E-tjenestens virksomhet.»

Utvalget mener at det vil være essensielt å bygge inn kontrollmekanismer i systemene for innhenting allerede under utviklingen av disse. I tillegg er det en nødvendig forutsetning for kontrollen at det settes av tilstrekkelig datakraft og andre ressurser til kontrollfunksjonalitet i systemene som tjenesten utvikler. Tilrettelegging bidrar til å underlette kontrollen, og sikrer at kontrollen kan foretas på en så hensiktsmessig måte som mulig.

De fleste høringsinstanser har ingen innvendinger mot at den løpende kontrollen føres av EOS-utvalget. Noen mener imidlertid at kontrollen bør føres av et eget tilsyn, i tråd med Lysne II-utvalgets anbefaling. Blant disse er *Nasjonal kommunikasjonsmyndighet (Nkom)*, som uttaler at departementets forslag innebærer en redusering av kontrollmekanismene som utvalget satt som forutsetning for å anbefale tilrettelagt innhenting. Nkom mener at de som tilsynsmyndighet har nødvendig kompetanse til å påta seg en tilsynsoppgave for tilrettelagt innhenting. Nkoms samarbeid med Etterretningstjenesten og mulighet til å gi innspill til tjenestens oppdrag er etter Nkoms syn ikke problematisk. Sikkerhetsmessige forhold må veies opp mot en tilsynsfunksjon som styrker tilliten til tjenesten. Etter Nkoms mening er risikoen ved å legge funksjonen til et kompetent tilsyn som allerede har rutiner og erfaring med å behandle høygradert informasjon, svært liten.

Den internasjonale juristkommisjon – norsk avdeling (ICJ-Norge) og *Norsk Journalistlag* støtter også opprettelsen av et eget tilsyn. *Kripos* og *Nasjonal sikkerhetsmyndighet* støtter derimot å legge den løpende kontrollen til EOS-utvalget.

Norges institusjon for menneskerettigheter (NIM) fremholder at den løpende kontrollen skaper noen utfordringer i lys av EOS-utvalgets arbeidsform:

> «Som konsekvens av en intensivert løpende kontroll er det f.eks. nærliggende at det kan oppstå saker eller problemstillinger som er tidssensitive. Det kan være vanskelig å forene med at utvalget ikke er permanent samlet og at utvalget bare er beslutningsdyktig med fem medlemmer til stede. Dette skaper en treghet i arbeidsformen som klart innvirker på effektiviteten av den løpende kontrollen. NIM mener derfor at det bør vurderes om sekretariatet, eventuelt ved sekretariatsleder bør ha hastekompetanse til å treffe beslutninger, som senere behandles av utvalget. Mer generelt kan man tenke seg at de funksjonene som knytter seg til den styrkede kontrollen operasjonaliseres på en mer selvstendig måte, uavhengig av den mer tradisjonelle kontrollen som EOS-utvalget forøvrig foretar, og som er tilpasset at dette er en kontroll som skal utføres i sanntid og som ikke nødvendigvis så lett lar seg forene med en utvalgsmodell.»

NIM mener at det bør vurderes om EOS-utvalget kan gis myndighet til å treffe bindende avgjørelser. En slik kompetanse kan fremstå som utradisjonell, men NIM kan vanskelig se at det skulle foreligge noen absolutte konstitusjonelle hindre for en slik ordning. Hvis konklusjonen skulle være at en slik ordning ikke er konstitusjonelt mulig, mener NIM at kontrollsystemet for tilrettelagt innhenting bør revurderes mer helhetlig, eventuelt slik at departementet følger opp noe i retning av Lysne II-utvalgets forslag om et eget tilsyn, som EOS-utvalget igjen vil føre kontroll med.

NIM fremholder videre at en form for merking av dataene vil bedre forutsetningene for utvalgets mulighet til å kontrollere at de behandles på riktig måte, og for eksempel ikke deles i større utstrekning enn hva loven tillater.

Datatilsynet mener at det er avgjørende for å opprettholde tillit at det føres et kontinuerlig tilsyn og en tilstrekkelig kontroll, og at forslaget ikke gir den nødvendige kompetansen til dette. Tilsynet fremholder at forslaget i realiteten kun innebærer etterkontroll, og at forslaget fra Lysne II-utvalget om at informasjonen skal mottas «i nær sanntid» ikke er fulgt opp. Tilsynet uttaler videre:

> «Etter vårt syn ivaretar ikke loven kravet til løpende kontroll og selv med en betydelig personellmessig styrking av EOS-utvalget, vil ikke dette være tilstrekkelig. Kontrollen bør innrettes ved at Etterretningstjenesten pålegges en plikt til å opprette systemer og rutiner for kontinuerlig rapportering. Dette vil kunne bidra til å forhindre misbruk, og rapporteringsplikten vil fremme kravet til åpenhet og kontroll kontinuerlig i arbeidet. Dette er spesielt viktig når kontrollrutinene og resultat ikke er tilgjengelig for offentligheten.
>
> Vi anbefaler videre at det gjøres en grundigere vurdering av muligheten for tekniske løsninger som tilrettelegger for mer effektiv løpende kontroll, gjennom en kombinasjon av manuell og automatisert maskinell kontroll.»

Tilsynet mener at det i denne sammenhengen bør tas hensyn til personvernprinsippet om innebygd personvern, og foreslår en lovfestet plikt til å tilrettelegge for kontrollen gjennom tekniske løsninger.

Det er bred enighet blant høringsinstansene om at EOS-utvalget må sikres tilstrekkelige ressurser. Flere reiser spørsmål om fire nye stillinger vil være tilstrekkelig for å ivareta den nye funksjonen knyttet til tilrettelagt innhenting. *EOS-utvalget* skriver:

> «Departementet anslår at 4 årsverk vil være tilstrekkelig for å ivareta kontrollfunksjonen. Det er vanskelig å gi et konkret overslag over hvilke økonomiske og administrative konsekvenser innføring av metoden vil få for utvalget. Høringsnotatet gir ikke en konkret beskrivelse av omfanget av bruken av den nye innhentingskapasiteten. Omfanget av den virksomheten som skal kontrolleres er dermed ukjent.
>
> Beskrivelsen av ressursbehovet i forhåndskontrollen gir en pekepinn. Departementet anslår at retten vil behandle 1–2 saker i uken. Anslaget er basert på at tjenestens begjæringer til retten kan omfatte et sakskompleks fremfor å individualiseres, samt at søk etter personselektorer reguleres på en måte som vil «bidra til at antall rettsavgjørelser kan holdes på et håndterlig nivå». Utvalget legger derfor til grunn at antallet søk mv. som kan kontrolleres, kan bli omfangsrikt. I tillegg kommer at utvalgets kontroll også vil omfatte andre sider av systemet for tilrettelagt innhenting, for eksempel bruken av korttidslageret, aktivitetslogger og hvordan filtrene settes opp.
>
> Utvalget mener på denne bakgrunn at departementets anslag på 4 årsverk er for beskjedent. Utvalget anser at en kontroll av tilrettelagt innhenting kan ivaretas ved at utvalgets sekretariat så raskt som mulig tilføres minst 6 årsverk dersom tilrettelagt innhenting vedtas. Deretter må behovet for ressurser i sekretariatet vurderes løpende. Utvalget kan ikke se bort fra at det er nødvendig med en betydelig styrking også utover de nevnte 6 årsverkene, for å styrke kompetansen og kapasiteten til denne kontrollen. Utvalget ser for seg at hovedtyngden ligger i personer med teknologisk kompetanse. Men det vil også være behov for å styrke sekretariatets juridiske kompetanse og noe på administrativ side. De ekstra ressursene må på plass så tidlig som mulig etter en eventuell vedtakelse av ny e-lov med hjemmel til tilrettelagt innhenting.»

EOS-utvalget peker også på at den teknologiske kompetansen til medlemmene i utvalget bør styrkes. Utvalget legger til grunn at utviklingskostnadene knyttet til å bygge inn kontrollmekanismer i systemer for datainnhenting vil ligge hos tjenesten. Utvalget foreslår også at det legges til rette for at den løpende kontrollen i størst mulig grad kan utføres fra utvalgets egne lokaler, og fremholder at kostnaden ved å tilrettelegge for systemtilgang fra utvalgets lokaler må ligge hos tjenesten.

11.10.3 Anbefaling fra Norges institusjon for menneskerettigheter

I etterkant av høringen har departementet avholdt flere møter med *Norges institusjon for menneskerettigheter (NIM)* hvor kontrollen med tilrettelagt innhenting har vært tema. I brev 30. april 2019 til departementet har NIM blant annet gitt følgende anbefaling:

> «Departementet bør utrede muligheten for at EOS-utvalget kan fremme begjæringer til retten om hel eller delvis stansing av pågående overvåkingstiltak eller sletting av innhentet informasjon, i tilfeller der E-tjenesten ikke tar EOS-utvalgets syn til følge. Rettens avgjørelse blir bindende for E-tjenesten.»

NIM uttaler at en slik adgang vil kunne bidra til å effektivisere utvalgets kontrollfunksjon, gjennom å initiere at det treffes bindende avgjørelser. Adgangen vil kunne fungere som en sikkerhetsventil, som igjen vil kunne ha en disiplinerende effekt. Den vil også kunne bidra til rettsavklaring. NIM mener at løsningen vil styrke den menneskerettslige innrammingen av forslaget.

Departementet har drøftet anbefalingen med medlemmer av EOS-utvalgets sekretariat.

11.10.4 Departementets vurdering

Departementet konstaterer at det er bred enighet blant høringsinstansene om at det må etableres en mekanisme for løpende kontroll av tilrettelagt innhenting, og viderefører i hovedsak forslaget i høringsnotatet. På bakgrunn av høringen foreslår departementet noen endringer som har til hensikt å styrke kontrollfunksjonen ytterligere. Reglene om løpende kontroll inntas i lovforslaget §§ 7-11 og 7-12.

Den løpende kontrollen med tilrettelagt innhenting bør etter departementets syn føres av EOS-utvalget, ikke et eget tilsyn. For å kunne føre en effektiv kontroll må kontrollorganet se tilrettelagt innhenting i sammenheng med Etterretningstjenestens andre metoder og kapasiteter. Tjenes-

tens virksomhet må dessuten ses i sammenheng med virksomheten til de andre EOS-tjenestene. Et tilsyn som bare skal kontrollere tilrettelagt innhenting, vil i motsetning til EOS-utvalget ikke ha denne muligheten.

Et sterkt fagmiljø er også en forutsetning for effektiv kontroll. Etter departementets syn vil det være lite formålstjenlig å bygge opp et separat fagmiljø i et eget tilsyn, som på grunn av den begrensede kontrolloppgaven vil være lite. Fra et kontrollperspektiv vil det være bedre å samle kompetansen i EOS-utvalget. Utvalgets sekretariat har i de senere årene blitt styrket, blant annet med en egen teknologisk enhet, og departementet ser det som naturlig å bygge videre på dette.

På denne bakgrunn finner departementet det klart at hensynet til effektiv kontroll taler for å legge den løpende kontrollen til EOS-utvalget. Departementet har dessuten lagt vekt på to andre hensyn. For det første taler hensyn til informasjonssikkerhet imot å opprette et nytt organ med tilgang til skjermingsverdig informasjon hos Etterretningstjenesten. For det andre tilsier legitimitets- og tillitshensyn at kontrollfunksjonen legges til et organ som ikke er en del av forvaltningen.

Noen høringsinstanser mener at departementets forslag innebærer en svekkelse i forhold til Lysne II-utvalgets forslag. Av de nevnte grunner er ikke departementet enig i dette. Det må like fullt tas på alvor at sentrale aktører ser behov for å styrke den løpende kontrollen av tilrettelagt innhenting. Etter høringen har departementet derfor vurdert om det kan gjøres endringer som kan styrke kontrollfunksjonen. Departementet har i den forbindelse ført en dialog med *Norges institusjon for menneskerettigheter (NIM)*, jf. punkt 11.10.3. På bakgrunn av denne dialogen foreslår departementet – i tråd med en anbefaling fra NIM – at Oslo tingrett, på begjæring fra EOS-utvalget, skal ha myndighet til å stanse pågående innhenting og pålegge sletting av lagrede data. Departementet er enig med NIM i at en slik ordning vil kunne fungere som en sikkerhetsventil som vil ha en disiplinerende effekt, og som vil styrke det menneskerettslige grunnlaget for tiltaket.

Å fremme begjæring om stansing vil være aktuelt i tilfeller hvor Etterretningstjenesten ikke retter seg etter utvalgets syn om lovligheten av pågående innhenting. Ordningen skal fungere som en sikkerhetsventil, og ikke erstatte vanlige prosedyrer for å løse uenigheter mellom utvalget og tjenesten. Tjenesten skal derfor få anledning til å vurdere og ta stilling til utvalgets syn, og eventuelt løfte saken til departementet for avgjørelse, før utvalget kan fremme begjæring om stansing.

Det vil etter departementets syn være uheldig om Etterretningstjenesten og EOS-utvalget kommer i formelle motpartsroller til hverandre i en domstolsprosess. Utvalget skal derfor ikke ha noen annen rolle enn å fremme begjæringen. Utvalget skal ikke møte i retten, og vil heller ikke ha rett til å anke. Retten skal imidlertid normalt oppnevne en særskilt advokat som skal målbære allmenne interesser i saken. Advokaten vil ha rett til å anke.

NIM har i sin anbefaling tatt til orde for at det bør etableres en form for hastekompetanse til å fremme begjæring, for eksempel for lederen av utvalgets sekretariat. Det kan være grunner som taler for en slik ordning. EOS-utvalget er etter EOS-kontrolloven § 13 første ledd beslutningsdyktig når fem medlemmer er til stede. Med utvalgets arbeidsform vil saksbehandlingen normalt ta noe tid, og det kan etter omstendighetene være behov for rettslig prøving av lovligheten av en innhentingsaktivitet raskere enn det utvalgets normale arbeidsform tillater. På den andre siden er utvalgets brede sammensetning viktig for kontrollens legitimitet, og ved bruk av en hastekompetanse vil ikke beslutningen få den brede forankringen som en behandling av det samlede utvalget gir. Departementet går derfor i denne omgangen ikke inn for en hastekompetanse. Departementet legger til grunn at utvalget, innenfor rammen av gjeldende regelverk, kan etablere prosedyrer som legger til rette for en raskere behandling av hastesaker enn det utvalgets normale arbeidsform åpner for.

Både *Datatilsynet* og *EOS-utvalget* påpeker at det bør bygges inn kontrollmekanismer i systemene allerede under utviklingen av disse. Departementet er enig i dette, og legger til grunn at Etterretningstjenesten retter oppmerksomhet mot kontrollfunksjonalitet under utviklingen og implementeringen av de tekniske løsningene. Som påpekt av Datatilsynet, bør den løpende kontrollen bestå av en kombinasjon av manuell og automatisert maskinell kontroll.

I tråd med Datatilsynets anbefaling foreslår departementet å lovfeste en plikt for Etterretningstjenesten til å tilrettelegge for den løpende kontrollen gjennom tekniske løsninger. Hvilke tiltak som skal treffes, må avgjøres konkret og i dialog mellom tjenesten og EOS-utvalget. Det kan for eksempel være tale om merking av data, slik *NIM* trekker fram i sin høringsuttalelse. Departementet forutsetter at tjenesten vil strekke seg langt for å imøtekomme utvalgets behov innenfor de øko-

nomiske, tekniske og praktiske rammer som gjelder til enhver tid.

Høringen har vist bred enighet om at EOS-utvalget må ha tilstrekkelige ressurser. Utvalget gir i sin høringsuttalelse uttrykk for at kontrollen kan ivaretas ved at sekretariatet så raskt som mulig tilføres seks nye årsverk, og at det ikke kan ses bort fra at det vil være behov for en betydelig styrking også utover dette. Departementet legger dette til grunn.

EOS-utvalget mener at den løpende kontrollen i størst mulig grad bør utføres fra utvalgets egne lokaler. Departementet er enig i at hensynet til utvalgets uavhengighet kan tilsi at kontrollen i størst mulig utstrekning utføres fra egne lokaler, på samme måte som domstolens forhåndskontroll vil foretas fra domstolens egne lokaler. På den andre siden har den løpende kontrollen en annen karakter enn forhåndskontrollen, og informasjonssikkerhetshensyn taler med tyngde for at den løpende kontrollen utføres fra Etterretningstjenestens lokaler. I tillegg vil sentrale kontrollpunkter i praksis ikke la seg utføre fra utvalgets lokaler. Departementet legger derfor til grunn at løpende kontroll i all hovedsak vil måtte føres fra tjenestens lokaler. Departementet forutsetter at tjenesten og utvalget vil være seg bevisste betydningen av å ivareta hensynet til utvalgets uavhengighet ved den praktiske gjennomføringen av den løpende kontrollen.

Departementet vil i lys av høringsuttalelsen til *Nasjonal kommunikasjonsmyndighet (Nkom)* understreke at Nkom har relevant kompetanse innen elektronisk kommunikasjon og erfaring med å beskytte skjermingsverdig informasjon. Selv om løpende kontroll bør føres av EOS-utvalget, vil utvalget kunne nyttiggjøre seg Nkoms ekomfaglige kompetanse i samsvar med EOS-kontrolloven § 19. Nkom vil dessuten føre tilsyn med tilbydernes utøvelse av tilretteleggingsplikten, jf. punkt 11.8.7.3.

11.11 Etterfølgende kontroll og andre kontrollfunksjoner

Tilrettelagt innhenting vil på vanlig måte omfattes av EOS-utvalgets etterfølgende kontroll. Det vises til punkt 6.2.2 for en nærmere beskrivelse av denne kontrollfunksjonen.

Tilrettelagt innhenting vil dessuten på vanlig måte omfattes av Etterretningstjenestens internkontroll og av departementets forvaltningskontroll. Det vises til punkt 6.2 for en nærmere beskrivelse av disse kontrollfunksjonene.

Av pedagogiske grunner foreslås det presisert i lovforslaget § 7-10 første ledd at Etterretningstjenesten skal iverksette systematiske tiltak for å sikre at tilrettelagt innhenting gjennomføres i samsvar med loven.

11.12 Forbud mot utlevering av overskuddsinformasjon

11.12.1 Forslaget i høringsnotatet

I høringsnotatet punkt 11.13.2 drøftes hvorvidt det bør gjelde et forbud mot å utlevere overskuddsinformasjon som stammer fra tilrettelagt innhenting. Overskuddsinformasjon er informasjon som ikke har relevans for Etterretningstjenestens oppgaver etter kapittel 3 og som dermed skal slettes. Den alminnelige hovedregelen er at overskuddsinformasjon kan utleveres til andre myndigheter før den slettes hos tjenesten dersom det er nødvendig og forholdsmessig. Et forbud mot utlevering av overskuddsinformasjon fra tilrettelagt innhenting vil utgjøre et unntak fra hovedregelen. Spørsmålet aktualiseres fordi tilrettelagt innhenting innebærer lagring av store mengder overskuddsinformasjon om norsk innenlandsk kommunikasjon.

Det tas utgangspunkt i at det bør gjelde et forbud mot deling av overskuddsinformasjon av hensyn til å motvirke et press i retning av å tillate at informasjonen brukes til andre formål enn etterretningsformål. Samtidig utfordres et ubetinget forbud av fire forhold:

For det første gjelder det en avvergingsplikt etter straffeloven § 196. Bestemmelsen setter straff for den som unnlater å forsøke å hindre visse alvorlige straffbare handlinger eller følgene av disse. Avvergingsplikten gjelder for enhver og uten hensyn av taushetsplikt.

For det andre gjelder det en plikt etter straffeloven § 226 til å gi opplysninger som kan forhindre at uskyldige blir dømt. Også denne plikten gjelder for enhver og uten hensyn av taushetsplikt.

For det tredje er staten forpliktet til å sikre menneskerettighetene. Plikten kan innebære at staten må treffe tiltak for å hindre krenkelser av menneskerettighetene, inkludert privates krenkelser av andre private, se for eksempel Høyesteretts dom i HR-2013-881-A. Plikten til å beskytte menneskerettighetene gjelder særlig retten til liv, vernet mot tortur og annen umenneskelig eller nedverdigende behandling eller straff.

For det fjerde følger det av nødretten at en handling som ellers er straffbar vil kunne være

lovlig dersom den er foretatt for å for eksempel redde noens liv fra en fare for skade som ikke kan avverges på en annen rimelig måte.

Etter en drøftelse av de rettslige rammene og hensynene som gjør seg gjeldende, foreslås det i høringsnotatet et forbud mot utlevering av overskuddsinformasjon. Etter forslaget skal straffeloven §§ 196 og 226 ikke gjelde for Etterretningstjenestens personell i den utstrekning de får kunnskap om forholdet gjennom tilrettelagt innhenting.

Det foreslås unntak fra forbudet for overskuddsinformasjon om straffbare handlinger som kan avverges og som omfattes av straffeloven kapittel 17 om vern av Norges selvstendighet og andre grunnleggende nasjonale interesser eller kapittel 18 om terrorhandlinger og terrorrelaterte handlinger.

11.12.2 Høringsinstansenes syn

Abelia støtter det generelle forbudet mot deling av overskuddsinformasjon, men er kritiske til at det åpnes for deling under kapittel 17 og 18 i straffeloven. *International Business Machines AS* synes også å støtte et absolutt forbud. *Tekna* er positive til et forbud, men mener at det fort vil oppstå et politisk press om å ta i bruk innhentede data til nye formål. *Amnesty International* uttaler:

> «Ulike former for bruk og deling av informasjon og overskuddsmateriale innebærer potensielt en rekke inngrep i rettighetsvernet. Vi støtter departementets syn at det bør gjelde et strengt forbud mot deling av overskuddsmateriale fra tilrettelagt innhenting. Det vil av personvernhensyn være viktig at slikt overskuddsmateriale ikke er gjenstand for hverken deling eller bruk. Dersom man ønsker å gjøre unntak fra forbudet mot deling så må dette være unntak som er nøye spesifisert. Unntakene må være formulert slik at de er uttømmende. Skjønnsmessige begrensninger kan, som nevnt i høringsnotatet, være vanskelig å praktisere og kontrollere. Vi har forståelse for at det kan være nødvendig å gjøre unntak på bakgrunn av våre folkerettslige forpliktelser, herunder plikten til å treffe tiltak dersom privatlivets fred og andre menneskerettigheter trues.
>
> I lovforslagets § 7-12 andre ledd første setning heter det at «Forbudet etter første ledd gjelder ikke overskuddsinformasjon om en straffbar handling som omfattes av straffeloven kapittel 17 eller 18 og som kan avverges.» Det forstås slik at dette er kumulative vilkår. Hvorvidt noe *kan avverges* formodes å bero på en konkret helhetsvurdering i hvert enkelt tilfelle. Her kan det være behov for nærmere presisering av hvordan en slik vurdering skal gjennomføres. Det er uklart hvordan dette i praksis vil vurderes og håndteres.»

Datatilsynet er kritiske til at det skal gjelde egne regler for deling av overskuddsinformasjon fra tilrettelagt innhenting. Tilsynet tror at det i praksis vil bli vanskelig å til enhver tid vite hvor informasjonen i en konkret sak kommer fra, noe som gjør kontroll med utlevering vanskelig. Tilsynet uttaler videre:

> «Disse foreslåtte bestemmelsene er på ingen måte en garanti for at opplysningene som er innhentet ikke vil bli brukt til nye formål. Vi mener det ikke kan være noen tvil om at spørsmål omkring videre bruk til nye formål før eller senere vil komme opp. Som det også fremgår av høringsnotatet, var politiet ute med en gang Lysne II-rapporten ble sendt på høring og krevde at opplysningene også måtte kunne brukes til kriminalitetsbekjempelse.
>
> Avgjørelsen om å ikke benytte slik overskuddsinformasjon til å forhindre kriminalitet eller andre skadelige hendelser vil bli et etisk dilemma. Både for lovgiver generelt og den enkelte medarbeider i konkrete situasjoner. For eksempel der en medarbeider kommer over informasjon om et planlagt ran. I høringsnotatet er det drøftet hvorvidt nødrettsbetraktninger og eventuelle positive forpliktelser etter Grunnloven og EMK innebærer at staten får en handlingsplikt som går foran begrensningen i § 7-12. Dette viser at det er grunnlag for reelle bekymringer og at erfaring viser at det vil komme situasjoner hvor forbudet vil bli utfordret. På samme måte vil politikere komme under press til å endre loven, dersom det i forbindelse med en konkret hendelse kommer frem at etterretningstjenesten hadde tilgang til informasjon som kunne forhindret forbrytelsen.
>
> For at Stortinget skal bestemme at overskuddsinformasjon innhentet gjennom tilrettelagt innhenting skal brukes til andre formål, og deles på en måte som avviker fra den vedtatte loven, må det foretas en ny forholdsmessighetsvurdering og vurdering opp mot de menneskerettslige skrankene som ligger til grunn for lovligheten. En endring vil helt klart kunne forrykke denne balansen. Det vil i så fall være

nødvendig å vurdere hele systemet og kontrollmekanismene på nytt.

Det kan for øvrig stilles spørsmål ved forholdet til lov om straff (straffeloven) § 287, om forsømmelse av hjelpeplikt. Dette bør avklares mer presist.

Forbudet gjelder ikke straffbar handling som omfattes av straffeloven kapittel 17 om vern av Norges selvstendighet og andre grunnleggende nasjonale interesser eller kapittel 18 om terrorhandlinger og terrorrelaterte handlinger og som kan avverges. Det ligger et potensiale for formålsutglidning i denne avvergingsplikten.

Kombinasjonen av den enorme mengden av data, en stadig utvikling av søkemetoder og kunstig intelligens gjør potensialet for formålsutglidning stort. Det vil alltid være gode formål som vil tale for å bruke opplysningene på nye måter. En slik utglidning vil kunne bringe oss stadig nærmere et totalt overvåkingssamfunn.

Den overhengende muligheten for formålsutglidning gjør det vanskelig å forutberegne konsekvensene av tiltaket og anslå omfanget av inngrepet. Det beste vernet mot formålsutgliding er å ikke samle inn opplysningene i første omgang, eller begrense innsamlingen til mer målrettede tiltak.»

Den internasjonale juristkommisjon – norsk avdeling (ICJ-Norge) er kritiske til at alle straffbare handlinger etter straffeloven kapittel 17 og 18 skal omfattes av unntaket fra forbudet mot deling av overskuddsinformasjon. I samme retning uttaler *Norges institusjon for menneskerettigheter (NIM)* seg. NIM mener dessuten at det bør klargjøres hva som menes med «avverges», og at det bør stilles kvalifikasjonskrav til hvilken betydning overskuddsinformasjonen kan ha.

På den andre siden er en rekke høringsinstanser kritiske til forslaget om å oppstille unntak fra straffeloven §§ 196 og 226. *Det nasjonale statsadvokatembetet* mener at departementet legger for liten vekt på statens menneskerettslige sikrings- og beskyttelsesplikter og hensynene bak §§ 196 og 226:

> «Hensynet til potensielle ofre for alvorlig kriminalitet tilsier med styrke at det må gjøres ytterligere unntak fra et delingsforbud. Det vil være svært problematisk om ansatte i Etterretningstjenesten som kommer til kjennskap om eksempelvis planlegging av drap eller seksuelt misbruk av barn skal kunne slette opplysningene uten videre oppfølgning.»

Etisk råd for forsvarssektoren (ERF) deler departementets syn om at faren for formålsglidning bør tas på alvor, og at eventuelle unntak fra forbudet bør presiseres så tydelig som mulig og kun gjelde forhold som fortsatt kan avverges. ERF mener likevel at unntakene er for snevre. ERF fremholder at de etiske utfordringene lovforslaget innebærer for Etterretningstjenestens personell ikke er tilstrekkelig belyst, og uttaler:

> «Lovforslaget innebærer, som høringsuttalelsen påpeker, at det kan oppstå situasjoner der personell i Etterretningstjenesten kan få kjennskap til alvorlig forbrytelser, som drap eller seksuelt misbruk av mindreårige, som kan avverges. Personellet kan ikke dele denne informasjonen uten å bryte loven. Dette vil innebære å sette personellet i en etisk og psykologisk svært belastende situasjon, der vedkomne må leve med at han eller hun kunne ha avverget f.eks. grove overgrep mot barn eller tap av liv. ERF stiller spørsmål om hvorvidt dette er en moralsk byrde Etterretningstjenesten skal kunne pålegge sine ansatte.»

ERF mener at høringsnotatet gjør en god jobb med å identifisere vektige hensyn som taler mot et ubetinget forbud, men mener det er noe uklart hvordan selve avveiningen som ledet til lovforslaget er blitt gjort. ERF påpeker at det er grunn til å tro at straffeloven i dette tilfellet speiler en grunnleggende etisk norm om at avverging av visse grove forbrytelser er så viktig at andre tungtveiende hensyn må settes til side. ERF mener at det ikke gis tilstrekkelige argumenter for hvorfor faren for formålsglidning nødvendiggjør at forbudet mot deling av overskuddsinformasjon gjøres såpass uinnskrenket.

Kripos går sterkt imot forslaget, og peker på at straffeloven §§ 196 og 226 bygger på helt sentrale hensyn i et samfunn. Kripos finner det rettslig og etisk uholdbart at myndighetene skal kunne komme til kunnskap om eksempelvis pågående seksuelt misbruk av barn, for så å slette informasjonen uten videre oppfølgning. Kripos fremholder at strenge rettssikkerhets- og kontrollmekanismer vil sikre at det utelukkende innhentes informasjon med etterretningsformål. Politiet vil ikke ha noen innvirkning på hvilken informasjon som innhentes. På denne bakgrunn mener Kripos at hensynet til å motvirke formålsutglidning trekkes for langt. *Innlandet politidistrikt* gir uttrykk for synspunkter i samme retning, og mener at overskuddsinformasjon fra tilrettelagt innhenting bør følge hovedregelen i lovutkastet § 10-8. *Politi-*

direktoratet tiltrer merknadene til Kripos og Innlandet politidistrikt, og mener at hensynet til formålsglidning trekkes for langt i lovforslaget. Den aktuelle overskuddsinformasjonen vil allerede være innhentet, og det praktiske omfanget vil etter det opplyste i høringsnotatet bli svært lite. Etter direktoratets oppfatning må hensynet til statens aktivitetsplikt ved kunnskap om øvrig alvorlig kriminalitet veie tungt. På vanlig måte vil fare for misbruk kunne minimaliseres ved et klart hjemmelsgrunnlag for adgang til å dele overskuddsinformasjon og med etablering av kontrollordninger.

Professor Morten Holmboe mener at forslaget i lovutkastet § 7-12 om begrensning av pliktene etter straffeloven § 196 og § 226 ikke bør vedtas. Han fremholder at forslaget har flere svakheter:

> «For det første har vi *andre viktige regler om varslingsplikt og handleplikt* som også gjelder etterretningstjenesten. Lovforslaget gjør ikke unntak for hjelpeplikt etter straffeloven § 287 eller varslingsplikt etter barnevernloven § 6-4. Tar man forslaget på ordet, har etterretningstjenesten plikt til å varsle barnevernet om at en 16-åring blir utsatt for mishandling i hjemmet, men ikke plikt til å varsle politiet om at noen utenfor familien planlegger å påføre den samme 16-åringen en grov kroppsskade.
>
> For det andre gir forarbeidenes drøftelser av en mulig handleplikt for myndighetene *liten veiledning* for når en slik handleplikt vil inntre. I en akutt situasjon er det unødig komplisert å henvise etterretningstjenesten til vanskelige juridiske avveininger av om det forestående lovbruddet er alvorlig nok til å utløse en handleplikt på grunnlag av menneskerettighetene og Grunnloven.
>
> Begrensningene som foreslås, er begrunnet i personvern og i tilliten til ordningen med innhenting av grenseoverskridende elektronisk informasjon. Samtidig kan tilliten til etterretningstjenesten ta skade dersom tjenesten forholder seg passiv, til tross for at den har troverdig informasjon som ville gi andre en straffsanksjonert plikt til å handle. Til sammenligning må selv politiets strenge taushetsplikt ved kommunikasjonskontroll vike for straffeloven § 196 og § 226, og retten til å dele informasjon går lengre når man kan forebygge at en uskyldig blir straffet, eller avverge en straffbar handling som «kan medføre frihetsstraff» (straffeprosessloven § 216 i) – det vil si de aller fleste straffebud.»

Professor Holmboe påpeker at straffeloven § 196 omfatter handlinger som er særlig samfunnsskadelige eller krenkende for enkeltmennesker. Vedtas forslaget i sin nåværende form, vil Etterretningstjenesten ikke uten videre ha rett eller plikt til å varsle om en forestående voldtekt, systematisk seksuelt misbruk av små barn, grove frihetsberøvelser eller mishandling i nære relasjoner – så lenge det ikke foreligger terrorhensikt. Professor Holmboe fremholder at hensynet til uskyldige kriminalitetsofre og uskyldige tiltalte – og tilliten til tjenesten – med tyngde taler for at tjenesten bør være underlagt de samme avvergings- og varslingsplikter som andre forvaltningsorganer og borgerne ellers. Forslaget kan også ha uheldige konsekvenser i form av et mer fragmentert lovverk med forskjellige regler om avvergings- og varslingsplikter for forskjellige yrkesgrupper.

Riksadvokaten mener at det er meget problematisk om Etterretningstjenesten skal unntas fra avvergingsplikten etter straffeloven § 196. Det pekes på statens ansvar for at ulike myndighetsorganer samhandler best mulig for å ivareta stats- og samfunnssikkerheten, og at forslaget ikke legger til rette for dette. Riksadvokaten er dessuten kritisk til at plikten etter straffeloven § 226 til å gi opplysninger som kan hindre at uskyldige blir dømt, ikke skal gjelde. Det påpekes at det er en sentral forpliktelse i en rettsstat å unngå justismord. Noe annet er både en alvorlig krenkelse av rettssikkerheten og menneskerettighetene til den som rammes, men også en generell og alvorlig svekkelse av rettssystemet og tilliten til det.

Telenor Norge AS har enkelte merknader knyttet til bruk av overskuddsinformasjon og formålsutglidning.

11.12.3 Departementets vurdering

Utgangspunktet etter lovforslaget § 10-4, som viderefører gjeldende rett, er at det ikke gjelder noe forbud mot å utlevere overskuddsinformasjon. Spørsmålet er hvorvidt det bør oppstilles et forbud mot å utlevere overskuddsinformasjon fra tilrettelagt innhenting, og i så fall om det bør fastsettes unntak fra forbudet.

Det er bred enighet blant høringsinstansene om å formålsbegrense tilrettelagt innhenting til utenlandsetterretning, det vil si at tilgangen bare skal kunne brukes for å løse oppgaver etter lovforslaget kapittel 3. Tilgangen kan ikke brukes til andre formål, for eksempel for å innhente informasjon som kan brukes for å bekjempe alminnelig kriminalitet. Slik bruk vil være misbruk som

kan få strafferettslige og andre konsekvenser for de involverte.

Tilrettelagt innhenting skiller seg fra andre tilganger til informasjon fordi det i dagens teknologiske situasjon innebærer lagring av store mengder metadata om norsk innenlandsk kommunikasjon. Slik informasjon er uten relevans for Etterretningstjenesten, og regnes dermed som overskuddsinformasjon. Tjenesten vil bare få tilgang til å søke i lagrede metadata hvis nærmere vilkår er oppfylt, noe som prøves av domstolen på forhånd. Et grunnleggende vilkår er formålsbegrensningen til utenlandsetterretning. På grunn av det teoretiske overvåkningspotensialet overfor egne borgere som lagringen innebærer, er det likevel av stor betydning å hindre formålsutglidning, det vil si at data tas i bruk til andre formål enn tilsiktet. En rekke høringsinstanser ser dette som sentralt. Departementet mener at det i første rekke er de ulike kontrollmekanismene som oppstilles i lovforslaget som vil hindre formålsutglidning. Et forbud mot utlevering av overskuddsinformasjon vil like fullt ha symbolsk betydning gjennom tydelig å markere formålsbegrensningen, og på denne måten bidra til å redusere risikoen for formålsutglidning. Departementet fastholder derfor forslaget i høringsnotatet om å forby utlevering av overskuddsinformasjon fra tilrettelagt innhenting. Forbudet inntas i lovforslaget § 7-13.

Departementet presiserer at forbudet bare gjelder *overskuddsinformasjon*, det vil si informasjon som er uten interesse for etterretningsformål. Informasjon om utenlandske trusler mot Norge, for eksempel fremmede staters etterretningsvirksomhet, angrep i det digitale rom som stammer fra utlandet og internasjonal terrorisme, er ikke overskuddsinformasjon. Slik informasjon skal deles med Politiets sikkerhetstjeneste, Nasjonal sikkerhetsmyndighet og andre relevante myndigheter innenfor rammen av reglene om samarbeid og deling av informasjon i lovforslaget kapittel 10. Deling av slik informasjon er et sentralt formål med lovforslaget, da Etterretningstjenesten bare har som oppgave å innhente informasjon om de fremmede truslene, mens det er andre myndigheter som har til oppgave å håndtere dem i Norge.

Hensynet til å motvirke risikoen for formålsutglidning tilsier etter departementets syn at forbudet mot å utlevere overskuddsinformasjon fra tilrettelagt innhenting bør gå foran avvergings- og opplysningsplikter som følger av annen lovgivning. Forslaget i høringsnotatet videreføres på dette punktet, men det gjøres mer generelt, slik at det også omfatter hjelpeplikten etter straffeloven § 287 og plikten etter barnevernloven § 6-4 til å melde fra til barneverntjenesten om blant annet alvorlig omsorgssvikt.

Flere høringsinstanser har fremholdt at Etterretningstjenesten ikke kan unnlate å handle i en situasjon hvor de får kjennskap til et forestående drap, pågående seksuelt misbruk av barn eller et justismord. Departementet er enig i dette. Som påpekt i høringsnotatet kan nødretten samt menneskerettslige sikrings- og beskyttelsesplikter gi grunnlag for å handle i slike tilfeller. På bakgrunn av høringen mener departementet at det bør lovfestes et unntak fra forbudet mot utlevering av overskuddsinformasjon. Pedagogiske hensyn tilsier en slik tydeliggjøring av det som følger av nødretten og menneskerettighetene.

Departementet understreker at det svært sjelden vil være aktuelt å gjøre unntak fra forbudet mot å utlevere overskuddsinformasjon. Det er flere grunner til dette. For det første innebærer formålsbegrensningen til utenlandsetterretning at det er lite trolig at Etterretningstjenesten vil komme i besittelse av overskuddsinformasjon som aktualiserer unntaket. Departementet anser situasjonen som helt usannsynlig ved analyse av testdata etter lovforslaget § 7-5 og søk i lagrede metadata etter § 7-8, selv om den teoretisk ikke helt kan utelukkes. Testdata hentes inn over korte tidsintervaller med sikte på teknisk understøttelse, og det er derfor ikke grunn til å tro at de tekniske spesialistene vil få kunnskap om en situasjon som kan sette spørsmålet om utlevering på spissen. Det er heller ikke grunn til å tro at søk i lagrede metadata, som sier noe om hvem som kommuniserer med hvem, tidspunkt for kommunikasjonen og lignende, er egnet til å gi slik kunnskap. Situasjonen er dermed først og fremst tenkelig ved målrettet innhenting av *innholdsdata* fra identifiserte etterretningsmål etter lovforslaget § 7-9, som kan innebære overvåkning av innholdet i målets kommunikasjon over tid. Selv her er det lite sannsynlig at tjenesten vil få kjennskap til for eksempel pågående seksuelt misbruk av barn eller et justismord, fordi Etterretningstjenestens informasjonsinnhenting knytter seg til utenlandske trusler mv., ikke straffesaker. Hvis en slik situasjon likevel skulle oppstå, mener departementet at forbudet mot å utlevere overskuddsinformasjon ikke kan stå i veien for å handle.

Etter dette foreslår departementet å lovfeste at overskuddsinformasjon kan utleveres i den utstrekning det er nødvendig for å forhindre alvorlig fare for noens liv, helse eller frihet eller at noen blir uriktig tiltalt eller domfelt for en straffbar handling. Unntaket er ment som en meget snever

unntaksregel som forutsettes anvendt med stor varsomhet. Det må være tale om en konkret fare av kvalifisert art. Det presiseres at unntaket ikke gir grunnlag for innhenting med sikte på å komme i besittelse av overskuddsinformasjon som kan utleveres. Dette vil være en ulovlig omgåelse.

Flere høringsinstanser har fremhevet betydningen av kontrollmekanismer. Departementet er enig i dette, og understreker at det faller innenfor EOS-utvalgets kontrolloppgave å føre kontroll med etterlevelsen av forbudet mot deling av overskuddsinformasjon fra tilrettelagt innhenting. Departementet foreslår å lovfeste en plikt for Etterretningstjenesten til å varsle utvalget ved utlevering av overskuddsinformasjon fra tilrettelagt innhenting med grunnlag i unntaksbestemmelsen. Hensikten med denne plikten er å sikre muligheten for å kontrollere at unntaksbestemmelsen ikke brukes for å omgå formålsbegrensningen til utenlandsetterretning.

Departementet er enig med *Datatilsynet* i at det kan oppstå krevende dilemmaer knyttet til overskuddsinformasjon og formålsutglidning. Departementet deler likevel ikke tilsynets konklusjon om at man derfor bør unngå å samle inn opplysningene i første omgang. Det er som nevnt grunn til å tro at problemstillingen sjelden vil aktualisere seg, på grunn av formålsbegrensningen og øvrige vilkår for tilgang til data. Gitt behovet for å styrke norske myndigheters selvstendige etterretningsevne finner departementet derfor at risikoen for formålsutglidning ikke med avgjørende vekt taler mot forslaget.

Datatilsynet og *Tekna* peker på risikoen for at det kan oppstå et politisk press om å endre loven slik at overskuddsinformasjon kan brukes til andre formål. Departementet kan ikke se at muligheten for senere lovendringer er et argument som med vekt taler mot å åpne for tilrettelagt innhenting. Stortingets lovgivende myndighet er et grunnleggende trekk ved vår styreform. Som Datatilsynet viser til, vil menneskerettslige skranker være førende for hvilke endringer som kan vedtas.

11.13 Bevisforbud i straffesaker

11.13.1 Forslaget i høringsnotatet

Det vurderes i høringsnotatet punkt 11.13.3 hvorvidt det bør lovfestes et bevisforbud i straffesaker for informasjon som stammer fra tilrettelagt innhenting. Det vises til at Lysne II-utvalget i sin rapport gikk inn for et slikt forbud.

Høringsnotatet tar utgangspunkt i at norsk straffeprosess bygger på prinsippet om fri bevisføring. Spørsmålet er om det finnes tilstrekkelig tungtveiende grunner til å gjøre unntak fra prinsippet.

I høringsnotatet vises det til at det spesielt er hensynet til å motvirke formålsutglidning som kan tilsi et bevisforbud i straffesaker. Selv om et bevisforbud kan virke urimelig i enkeltsaker, foreslås derfor et slikt forbud.

Det bes i høringsnotatet om høringsinstansenes syn på hvorvidt det bør gjøres et unntak fra bevisforbudet i saker som gjelder terrorhandlinger.

11.13.2 Høringsinstansenes syn

Abelia, *Advokatforeningen* og *Amnesty International* støtter forslaget i høringsnotatet. Det samme gjør *Justis- og beredskapsdepartementet*, som mener at en slik formålsbegrensning er egnet til å styrke tilliten til bruken av tilrettelagt innhenting.

Det nasjonale statsadvokatembetet mener at det bør gjøres unntak fra bevisforbudet for de alvorligste forbrytelsene mot liv, helse og frihet. Etter embetets syn er det under enhver omstendighet vanskelig å se at det ikke skal gjøres unntak fra bevisforbudet i saker som gjelder terrorhandlinger. *Kripos* er også kritiske til forslaget i høringsnotatet, og uttaler:

> «Kripos kan ikke se at en adgang til å bruke opplysninger som bevis medfører særlig økt fare for formålsglidning, dersom vilkårene for deling først er oppfylt. Tilsvarende anses ikke en slik begrensning nødvendig for å styrke tilliten til at metoden og informasjonen ikke misbrukes. Igjen forutsettes at de foreslåtte kontrollmekanismer vil kunne ivareta dette. Således fremstår et bevisforbud heller ikke nødvendig for at ordningen med tilrettelagt innhenting kan anses forholdsmessig og innføres.
>
> Det foreslåtte bevisforbudet har en klar side til kriminalitetsbekjempelse. Kripos' prinsipielle utgangspunkt er at delt informasjon fra tilrettelagt innhenting også bør kunne benyttes som bevis i straffesaker. Manglende oppklaring og iretteføring av alvorlig kriminalitet som følge av begrensninger i bruken av opplysninger, er også egnet til å svekke tilliten til både politiet, domstolen og myndighetsapparatet. Prinsippet om fri bevisføring og hensynet til sakens opplysning, innebærer at påtalemyndigheten bør kunne føre de bevis man har. Dette

vil bidra til en riktig avgjørelse og straffereaksjon.

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

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

Politiets sikkerhetstjeneste mener at det bør gjøres unntak fra bevisforbudet i saker som gjelder terrorhandlinger, og viser til det tilsvarende unntaket for opplysninger innhentet ved bruk av forebyggende tvangsmidler etter politiloven § 17 d.

Riksadvokaten viser til det grunnleggende prinsippet om fri bevisbedømmelse i straffeprosessen, og fremholder at det må kunne begrunnes i svært tungtveiende hensyn dersom dette skal fravikes. *Innlandet politidistrikt* mener at det ikke er gode nok grunner til å gå bort fra prinsippet, og peker blant annet på iretteføringens preventive virkning. *Politidirektoratet* gir uttrykk for tilsvarende synspunkter.

Telenor Norge AS finner det uklart hva det siktes til i høringsnotatets omtale av strenge begrensninger på å dele informasjon, og anbefaler å etablere kontrollmekanismer.

11.13.3 Departementets vurdering

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, se for eksempel Rt. 1990 side 1008. 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 (NOU 2016: 24 Ny straffeprosesslov punkt 13.2.3 side 257). Spørsmålet er om det finnes tilstrekkelig tungtveiende grunner til å gjøre unntak fra prinsippet gjennom å oppstille et bevisforbud for informasjon som stammer fra tilrettelagt innhenting.

Det har vært delte meninger om spørsmålet under høringen. Departementet er ikke uenig med høringsinstansene som påpeker at straffeforfølgning etter omstendighetene kan være et relevant virkemiddel for å motvirke trusler som Etterretningstjenesten har som oppgave å innhente informasjon om. Et bevisforbud vil kunne vanskeliggjøre straffeforfølgning, og kan virke urimelig i enkeltsaker. Dette taler imot å oppstille et bevisforbud. På samme måte som Lysne II-utvalget mener departementet likevel at hensynet til å motvirke risikoen for formålsutglidning bør tillegges avgjørende vekt, og viderefører derfor forslaget i høringsnotatet. Bevisforbudet inntas i lovforslaget § 7-14. Departementet mener at det ikke er nødvendig å innta en egen bestemmelse i straffeprosessloven.

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 skal avskjære slik bevisføring. Bevisforbudet innebærer også at påtalemyndigheten ikke kan bruke slik informasjon som grunnlag for egen ileggelse av straff eller andre strafferettslige reaksjoner, 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 å beslutte bruk av tvangsmidler.

I høringsnotatet ba departementet om høringsinstansenes syn på hvorvidt det burde gjøres et unntak fra bevisforbudet for terrorhandlinger, på samme måte som i politiloven § 17 f andre ledd bokstav c. Et slikt unntak støttes av de fleste høringsinstansene som har uttalt seg særskilt om det. Departementet er enig i at terrorhandlinger står i en særstilling. Det foreslås derfor unntak fra bevisforbudet i saker som gjelder overtredelse av straffeloven § 131. Politiloven § 17 f andre ledd bokstav c gjør unntak også i saker om overtredelse av straffeloven § 133 (terrorforbund) og § 134 (terrortrusler), men departementet finner ikke tilstrekkelig grunn til å foreslå tilsvarende unntak i lovforslaget § 7-15.

I lys av høringsuttalelsen til *Telenor Norge AS* vil departementet bemerke at det følger av lovfor-

slaget § 7-13 at overskuddsinformasjon som stammer fra tilrettelagt innhenting, ikke kan utleveres. Bruk av informasjon som stammer fra tilrettelagt innhenting som grunnlag for bruk av tvangsmidler vil dermed i alminnelighet bare være aktuelt på områder som Etterretningstjenesten samarbeider om å motvirke med Politiets sikkerhetstjeneste, Nasjonal sikkerhetsmyndighet og andre relevante myndigheter, for eksempel fremmed etterretningsvirksomhet mot Norge, internasjonal terrorisme og digitale angrep som stammer fra utlandet.

11.14 Informasjonssikkerhet

11.14.1 Forslaget i høringsnotatet

Det ble i høringsnotatet punkt 11.13.6 foreslått å lovfeste at Etterretningstjenesten plikter å hindre at uvedkommende får tilgang til informasjon som lagres og behandles etter kapittelet om tilrettelagt innhenting.

I høringsnotatet vises det til at generelle bestemmelser om informasjonssikkerhet er inntatt i lovutkastet § 9-11 og § 11-4. Pliktene som følger av disse bestemmelsene vil gjelde også for så vidt gjelder tilrettelagt innhenting, men dette bør av pedagogiske grunner presiseres i lovutkastet § 7-14.

11.14.2 Høringsinstansenes syn

Abelia uttaler at det som sikkerhet ved en eventuell ikke-demokratisk maktovertakelse bør finnes raske metoder for å avvikle systemet, og at det bør legges føringer for dette i lov og forskrift.

11.14.3 Departementets vurdering

Departementet viderefører forslaget i høringsnotatet. Bestemmelsen inntas i lovforslaget § 7-15.

Etter første punktum plikter Etterretningstjenesten å hindre at uvedkommende får tilgang til informasjon som lagres og behandles etter bestemmelsene i kapittel 7 om tilrettelagt innhenting. Av pedagogiske grunner fastslås det i andre punktum at Etterretningstjenesten skal gjennomføre sikkerhetstiltak etter §§ 9-9 og 11-5 for å sikre at informasjonen bare er tilgjengelig for de som har lovmessig tilgang til den.

Det er etter departementets syn ikke grunn til å særregulere i lovforslaget de spørsmål som reiser seg i forbindelse med en eventuell ikke-demokratisk maktovertakelse, slik *Abelia* tar til orde for. Det bemerkes at det gjeldende beredskapssystemet inneholder tiltak for å hindre at sensitive systemer og registre faller i hendene til fiendtlige aktører. Det vises til lovforslaget § 11-6.

11.15 Økonomiske og administrative konsekvenser

11.15.1 Beskrivelse i høringsnotatet

I høringsnotatet punkt 11.16 redegjøres det for hvilke aktører som antas å bli direkte berørt av forslaget og hvordan disse forventes å bli berørt. Aktørene som løftes frem er Etterretningstjenesten, domstolene ved Oslo tingrett og Borgarting lagmannsrett, EOS-utvalget og teletilbydere som omfattes av tilretteleggingsplikten.

11.15.2 Høringsinstansenes syn

Borgarting lagmannsrett mener at de økonomiske og administrative konsekvensene for domstolene er summarisk behandlet. Det påpekes at for Borgarting lagmannsrett vil merbelastningen avhenge av antallet begjæringer, ankesaker og hvorvidt det blir muntlig behandling av ankesakene. Usikkerheten gjelder både dommerbehov og dommernes behov for teknisk og administrativ støtte. Lagmannsretten legger til grunn at flere saker vil ankes i starten, og at flere ankesaker vil foregå som muntlig forhandling. Det vil også påløpe utgifter til salær.

Domstoladministrasjonen (DA) understreker behovet for midler til å etablere en gradert rettssal i Oslo tingrett ut over de midlene som ble bevilget i statsbudsjettet for 2019:

> «I statsbudsjettet for 2019 er det bevilget 2,1 millioner kroner for å etablere en gradert rettssal i Oslo tingrett. Domstoladministrasjonen mener det er en viktig forutsetning for domstolskontrollen at det bygges en rettsal i Oslo tingrett som tilfredsstiller kravene til strengt hemmelig etter sikkerhetsloven. Bevilgningene som er gitt over statsbudsjettet er etter beregninger av kostnader til et rom som tilfredsstiller kravene til hemmelig etter sikkerhetsloven. Det er blant annet behov for en gradert rettssal for å kunne gjennomføre muntlige forhandlinger, jf. lovforslaget § 8-3. Domstoladministrasjonen anser det som uaktuelt at dommere, i mangel av en gradert rettssal, må benytte seg eksempelvis av Etterretningstjenestens lokaler for å gjennomføre muntlige forhandlinger. Dette blant annet på bakgrunn av faren for identifikasjon med Etterretningstje-

nesten. Den særskilte advokaten må videre ha tilgang til et leserom som tilfredsstiller samme nivå for å kunne sette seg inn i sakens dokumenter forut for rettsmøtet.»

DA understreker at det må etableres nødvendig infrastruktur for å legge til rette for elektronisk kommunikasjon inn til rettssalen, samt etablering av et eget teknisk rom i tilknytning til denne. Det estimeres at det vil koste omkring 6 mill. kroner for prosjektering og bygging av gradert rettssal, leserom og teknisk rom.

Videre understreker DA at det i forbindelse med bevilgningene til Oslo tingrett må tas tilstrekkelig høyde for at begjæringene kan bli arbeidskrevende, særlig i en oppstartsfase. Dommerne som tillegges oppgaven må i starten bruke tid på å skaffe seg kompetanse om fagfeltet. DA anslår i høringsnotatet at årlige økte driftsutgifter knyttet til å behandle disse sakene er på 2,4 millioner kroner. Det baserte seg på behov for ett dommerårsverk og et halvt saksbehandlerårsverk i Oslo tingrett, og noe arbeid i Borgarting lagmannsrett. Det understrekes at uten tilførsel av friske midler vil saksbehandlingstiden for domstolens andre saker øke.

Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget) er enig med departementet i at lovforslaget vil medføre behov for å utvide den tekniske og juridiske kompetansen i EOS-utvalgets sekretariat, og at sekretariatet styrkes med dedikert kapasitet allerede på utviklingsstadiet. Det presiseres at behov for styrking av sekretariatets tekniske kompetanse som følge av en innføring av tilrettelagt innhenting vil komme i tillegg til styrkingen av utvalgets ordinære kontroll som skjedde og som bør skje i 2020. EOS-utvalget mener at anslaget i høringsnotatet på 4 årsverk er for beskjedent, og uttaler at:

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

EOS-utvalget fremmer også behov for en styrking av den samlede teknologiske kompetansen i utvalget, og at dette kan skje ved valg av nye medlemmer eller ved at medlemmene tilbys kompetansehevende tiltak. Videre uttaler utvalget:

> «Ved vurderingen av økonomiske og administrative kostnader for E-tjenesten vises det til at forslaget medfører behov for administrative rutiner knyttet til EOS-utvalgets styrkede kontroll av tilrettelagt innhenting. Utvalget legger til grunn at utviklingskostnader knyttet til å bygge inn kontrollmekanismer i systemer for datainnhenting også vil ligge hos tjenesten.
>
> For i størst mulig grad å ivareta utvalgets uavhengighet til tjenesten, foreslår utvalget at det legges til rette for at den løpende (styrkede) kontrollen i størst mulig grad kan utføres fra utvalgets egne lokaler. Det vil etter utvalgets vurdering være mulig å få til i utvalgets nye lokale fra 2019, sett ut fra tilgjengelig grad av plass, sikkerhet og tekniske forhold. Også kostnaden ved å tilrettelegge for systemtilgang fra utvalgets lokale, må ligge hos tjenesten.»

Oslo tingrett viser til at tingretten i dag ikke har tilfredsstillende lokaler for behandling av informasjon og dokumenter med høyeste sikkerhetsgrad. Siden lokalene skal benyttes av dommere og advokater om hverandre, i tillegg til at det skal være mulig med muntlige forhandlinger, bør det være minst to rom som tilfredsstiller sikkerhetskravene etter sikkerhetsloven. Rommet for muntlige forhandlinger bør dimensjoneres slik at det også kan benyttes av lagmannsretten ved behov. Rommene må utstyres med nødvendig og sikkert digitalt utstyr. I tillegg til lokaler for aktivt arbeid med sakene, bør det samtidig legges til rette for sikker digital kommunikasjon av dokumenter opp til HEMMELIG. Behovet for nyinvesteringer må ses i sammenheng med den allerede pågående prosessen med å etablere en ny sikker rettssal i Oslo tingrett. Oslo tingrett anslås skjønnsmessig at årlige driftsutgifter vil tilsvare ett nytt dommerårsverk og et halvt saksbehandlerårsverk.

Telenor viser til høringsnotatet side 215 der det understrekes at «det må foreslås lovfestet at merutgifter knyttet til tilretteleggingsplikten skal dekkes av staten», og uttaler:

«Telenor mener en eventuell innføring av tilrettelagt innhenting bør skje på en måte som sikrer forutberegnelighet, og der dokumenterte og direkte påløpte utgifter til tilretteleggingsplikten fullt ut kan søkes kompensert av staten. Etter Telenors vurdering kan regulering i ekomloven med tilhørende forskrifter være hensiktsmessig her, for å sikre rettsenhet og forutsigbarhet i dialog med relevant sektormyndighet.

Telenor forutsetter at alle merkostnader til etablering, utbygging og drift knyttet til tilrettelagt innhenting dekkes av norske myndigheter, og at det ikke hersker tvil om hvilke kostnader kan tilordnes kategorien «merkostnader». Telenor anser at kostnader til eventuelt økte sikringsbehov av blant annet lokasjoner, økt ressursbruk og økt reservedelslager som følge av innføring av tilrettelagt innhenting dekkes av myndighetene, og at dette blir presisert i den endelige lovteksten.

Ved eventuell videreutvikling av løsning eller fremtidig utvidelse av antall transportveier for datatrafikk ut/inn av Norge må kostnader knyttet til utvidelse av løsningen for tilrettelagt innhenting på nye lokasjoner dekkes av myndighetene.»

Telia uttaler seg også om dekningen av merutgifter som følge av tilretteleggingsplikten:

«Telia synes det er viktig at tilretteleggingsplikten ikke resulterer i en konkurransevridende eller fordyrende effekt. Det må derfor komme klart frem at det er staten som skal dekke alle utgifter tilretteleggingsplikten resulterer i for tilbyderne. Eksempler på utgifter som må dekkes er utgifter knyttet direkte til innkjøp eller omlegging av utstyr, utgifter knyttet til personell og fysiske lokaler som stilles til disposisjon for Etterretningstjenestens arbeid. Herunder lønnskostnader, kostnader til husleie, strøm og annen infrastruktur. Ekstrautgifter ved medvirking av teknisk drift og vedlikehold av etablerte løsninger som tilhører etterretningstjenesten, og ekstrautgifter for sikkerhets/adgangsklarering. Dette til en fastsatt timepris.

Telia vurderer det som hensiktsmessig at det etableres en beredskapsavtale/sikkerhetsavtale tilsvarende den beredskapsavtalen Telia har med Nkom (jf. ekomloven §2-10 annet ledd). En slik avtale spesifiserer den tilretteleggingen som Telia skal gjennomføre på vegne av Etterretningstjenesten og kostnadene dette medfører, herunder investeringer, operasjonelle- og administrative kostnader. Hensikten med inngåelse av en slik avtale vil være å sikre at tilbyderene som blir truffet av tilretteleggingsplikten ikke blir belastet mer enn de tilbyderne som ikke treffes av tilretteleggingsplikten.»

11.15.3 Rapport om virkninger for berørte aktører

Rådgivnings- og revisjonsselskapet BDO har på oppdrag fra Forsvarsdepartementet utarbeidet en rapport om virkninger for berørte aktører ved innføring av tilrettelagt innhenting sammenlignet med nullalternativet. Nullalternativet innebærer at dagens situasjon videreføres. Rapporten omfatter en analyse av økonomiske og administrative virkninger, samt hvilke virkninger tilrettelagt innhenting vil ha for nasjonale sikkerhetsinteresser.

Det lå utenfor BDOs mandat å vurdere virkninger knyttet til personvern. Videre lå det utenfor mandatet å vurdere andre alternativer enn nullalternativet og innføring av tilrettelagt innhenting. Disse avgrensningene er begrunnet i at spørsmål knyttet til personvern og alternativer er grundig vurdert av departementet i arbeidet med høringsnotatet og proposisjonen, se spesielt punkt 11.4.og 11.5.

Analysen er skrevet på bakgrunn av intervjuer og dialog i annen form med Etterretningstjenesten, EOS-utvalget, Politiets sikkerhetstjeneste (PST), Oslo tingrett, Nasjonal sikkerhetsmyndighet (NSM), Abelia og utvalgte teletilbydere. På bakgrunn av denne informasjonen har BDO prissatt de økonomiske og administrative virkningene for Etterretningstjenesten, EOS-utvalget, Oslo tingrett og NSM. For PST ble det ikke identifisert signifikante økonomiske og administrative virkninger.

BDO innhentet også informasjon om hvilke virkninger tilrettelagt innhenting vil kunne ha for nasjonale sikkerhetsinteresser, og ga følgende samlede vurdering av om tilrettelagt innhenting bør innføres:

«Våre analyser viser at innføring av tilrettelagt innhenting for Etterretningstjenesten vil innebære en estimert neddiskontert kostnad lik 3,2 milliarder kroner over 20 år. Til tross for dette er det vår vurdering at alternativet som innebærer en innføring av tilrettelagt innhenting, er fordelaktig sammenlignet med nullalternativet, gitt de forutsetninger og avgrensninger som ligger til grunn for vår rapport.»

BDO begrunner sin vurdering med fire forhold:

1. Tilrettelagt innhenting vil ha en sterk positiv påvirkning på evnen til å avdekke og avverge fremmed etterretningsvirksomhet, alvorlige hendelser og angrep mot Norge og norske interesser.
2. En positiv (men også begrenset) sideeffekt av tilrettelagt innhenting er at tiltaket vil kunne styrke evnen til nasjonal kriminalitetsbekjempelse på enkelte områder der Etterretningstjenesten har hjemmel til å dele informasjon med nasjonale samarbeidspartnere (fortrinnsvis der Etterretningstjenesten og PST har overlappende oppgaver).
3. Tilrettelagt innhenting vil sannsynligvis styrke Norges evne til å bidra i internasjonale etterretningssamarbeid, samt Norges status som en relevant og troverdig aktør i slike samarbeidssituasjoner.
4. Norge vil kunne bli mindre attraktivt som transittland for rettsstridig datatrafikk, som elektronisk kommunikasjon mellom terroraktører, digitale angrep på andre gjennom norske servere eller lignende forhold.

Samlet mener BDO at disse virkningene vil ha positiv innvirkning på norske sikkerhetstjenesters evne til å utføre sine samfunnsoppdrag, og at den samlede nytten av de ikke-prissatte virkningene overstiger de beregnede kostnadene.

11.15.4 Departementets vurdering

Departementet har etter høringen fortsatt arbeidet med å utrede de økonomiske og administrative konsekvensene av forslaget om tilrettelagt innhenting. Det er etablert et prosjekt i departementet som skal ivareta behovet for nødvendige utredninger og kostnadsberegninger for en eventuell implementering i Etterretningstjenesten av tilrettelagt innhenting. Prosjektet skal videre gjennomføre en anskaffelse forutsatt at lovforslaget om tilrettelagt innhenting blir vedtatt. Prosjektet følger de etablerte prosesser for store, statlige investeringsprosjekter, og sørger blant annet for at påkrevde økonomiske analyser og andre kost/nytte-vurderinger foretas for å gi det nødvendige grunnlag for beslutninger i departementet, regjeringen og Stortinget. Arbeidet ledes av departementet og gjennomføres i samarbeid med Etterretningstjenesten.

Departementet har mottatt innspill til kostnadsberegningene i høringsnotatet fra *Borgarting lagmannsrett, Domstoladministrasjonen, EOS-utvalget* og *Oslo tingrett.* I etterkant av høringen har enkelte estimater blitt oppdaterte. Dette gjelder kostnadene for etablering av graderte rom i Oslo tingrett og behovet for årsverk i EOS-utvalgets sekretariat. De oppdaterte tallgrunnlagene fremgår også av BDOs rapport. I de følgende kostnadsberegningene er de oppdaterte estimatene lagt til grunn for disse aktørene.

De økonomiske og administrative konsekvensene av tilrettelagt innhenting vil naturlig nok være størst for Etterretningstjenesten. Det anslås at den totale investeringskostnaden vil være om lag 1 000 millioner kroner inkludert mva., fordelt over de fire første årene. Investeringskostnaden omfatter anskaffelse og oppbygning av kapasiteten, herunder personellutgifter knyttet til gjennomføring av prosjektet og ulike bygningsmessige tiltak. Departementet gjør oppmerksom på at anslaget er basert på en teknisk løsning som vurderes å ville gi tilgang til grenseoverskridende kommunikasjon på en troverdig måte ut fra dagens situasjon hva gjelder volum på relevant datatrafikk. Konsekvensen av et eventuelt økt volum på relevant datatrafikk vil på sikt kunne medføre et behov for ytterligere investeringer. Driftsutgiftene for Etterretningstjenesten anslås til 140 millioner kroner årlig til dekning av personellutgifter og drift av materiell og eiendom, bygg og anlegg. Merutgifter for teletilbyderne er inkludert i anslaget for Etterretningstjenesten.

EOS-utvalget har anslått at tilrettelagt innhenting vil medføre investeringskostnader totalt pålydende 4,8 millioner kroner fordelt over to år. I tillegg viser utvalget til at det vil være behov for oppgradering av det tekniske utstyret estimert til 21 millioner kroner hvert femte år. Driftsutgiftene per år anslås å være om lag 11 millioner kroner.

Investeringskostnadene for domstolen er beregnet til om lag 9,1 millioner kroner til etablering av rettssal, teknisk rom og leserom som tilfredsstiller kravene til graderingsnivå STRENGT HEMMELIG. Kompetanseheving vil medføre utgifter beregnet til 0,1 millioner kroner i oppstartsåret, og deretter 20 000 kroner årlig. De anslåtte årlige økte utgiftene knyttet til domstolsbehandling er om lag 0,5 millioner kroner. Beregningen er basert på dagens ressursbruk knyttet til behandling av PST-saker med gradering HEMMELIG. Utgiftene består av økte driftsutgifter for domstolene på om lag 200 000 kroner årlig, og utgifter for staten til salær til advokater, estimert til om lag 250 000 kroner årlig. Tilrettelagt innhenting vil kunne medføre behov for flere ansatte i NSM. Etter hva NSM har opplyst, vil de totale driftsutgiftene være 13,5 millioner kroner fra og med 2024, når alle ansettelser er gjennomført.

Kostnadsbildet kan oppsummeres slik:

mill. kroner

Departement/organ	Aktør/prosess	Investering	Drift
Forsvarsdepartementet	Etterretningstjenesten	1 000	140
Justis- og beredskapsdepartementet	Domstolsbehandling	9,2	0,5
Stortingets underliggende organer	EOS-utvalget	4,8	11
Justis- og beredskapsdepartementet	NSM	0	13,5
Sum		1 014	165

I denne proposisjonen bes det om Stortingets tilslutning til det rettslige grunnlaget som muliggjør tilrettelagt innhenting. Alle de økonomiske og administrative konsekvensene av tilrettelagt innhenting er ikke endelig avklart. Eventuelle forslag om anskaffelse og drift av tilrettelagt innhenting vil vurderes i de årlige budsjettfremleggene for de respektive departementene.

12 Behandling av personopplysninger etter innhenting

12.1 Innledning

Den enkeltes rett til personvern og respekt for sitt privatliv er forankret i Grunnloven og menneskerettskonvensjoner som gjelder som norsk lov etter menneskerettsloven. Begrepene «personvern», «personopplysningsvern» og «privatliv» brukes gjerne om hverandre i dagligtalen, men begrepene har selvstendig innhold og betydning. Personvernkommisjonen la til grunn følgende definisjoner i sin rapport (NOU 2009: 1 punkt 4.1.5), som Menneskerettighetsutvalget senere sluttet seg til (Dokument 16 (2011–2012), punkt 30.6.2 side 172):

> «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. […]»

Reglene i lovforslaget kapittel 9 om behandling av personopplysninger ivaretar i første rekke personopplysningsvernet. Formålet med personopplysningsvernet er blant annet å ivareta balansen mellom borger og stat, og forhindre at staten får for stor makt over egne borgere. I takt med den teknologiske utviklingen har personopplysningsvernet fått en mer selvstendig betydning ved siden av personvernet. Begrunnelsen er at tiltak som griper inn i personvernet, i stadig større utstrekning gjennomføres slik at de også medfører behandling av personopplysninger i form av innhenting, registrering, bearbeiding og analysering.

12.2 Andre lands rett

12.2.1 Sverige

Lag (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst regulerer svensk etterretningsvirksomhets behandling av personopplysninger. Loven åpner for behandling av personopplysninger når det er nødvendig for å drive virksomhet som angis i *lag (2000:130) om försvarsunderrättelseverksamhet*. Det presiseres at opplysninger om en person bare kan behandles så lenge det er relatert til et oppdrag for etterretningsvirksomheten og behandlingen er nødvendig for å fullføre oppdraget.

Det fremgår av *lag (2018:218) med kompletterande bestämmelser til EU:s dataskyddsförordning* at personvernforordningen ikke kommer til anvendelse for behandling av personopplysninger etter *lag (2007:258)*.

12.2.2 Danmark

Lov om Forsvarets Efterretningstjeneste (FE) har særskilte bestemmelser om behandling av personopplysninger om fysiske personer som er hjemmehørende i Danmark. I korte trekk følger det av § 4 at slike personopplysninger kan behandles hvis behandlingen skjer med samtykke, må antas å ha betydning for å ivareta tjenestens oppgaver som utenlandsetterretningstjeneste, eller er nødvendig for å ivareta tjenestens oppgaver som militær sikkerhetstjeneste og nasjonal sikkerhetsmyndighet for forsvarssektoren.

FE er unntatt *lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven)* og personvernforordningen.

12.2.3 Finland

Lag (332/2019) om behandling av personuppgifter inom Försvarsmakten regulerer behandling av personopplysninger i det finske forsvaret. Loven

gjelder også for behandling av personopplysninger i den militære etterretningstjenesten. Personopplysningene kan behandles for formål som følger av *lag (551/2007) om försvarsmakten* 2 §. Loven åpner blant annet for å etablere et eget register for den militære etterretningstjenesten, som kan brukes til militære etterretningsoppdrag. Loven angir en uttømmende liste over hvilke personopplysninger som kan registreres. For behandling av personopplysninger til andre formål kommer personvernforordningen til anvendelse.

12.3 Personopplysningsvernets rettslige forankring

Retten til respekt for privatlivet er grunnlovsfestet i Grunnloven § 102:

> «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.»

Personopplysningsvernet omfattes av bestemmelsen, se Innst. 186 S (2013–2014) punkt 2.1.9 side 27, hvor Stortingets kontroll- og konstitusjonskomité uttaler:

> «K o m i t e e n understreker at forslaget skal leses som at systematisk innhenting, oppbevaring og bruk av opplysninger om andres personlige forhold bare kan finne sted i henhold til lov, benyttes i henhold til lov eller informert samtykke og slettes når formålet ikke lenger er til stede.»

Det følger av HR-2014-2288-A avsnitt 28 og HR-2015-206-A avsnitt 60 at myndighetene ikke kan gripe inn i personopplysningsvernet med mindre det er forankret i lov, ivaretar et legitimt formål og møter de alminnelige kravene til nødvendighet og forholdsmessighet, se nærmere punkt 4.3.

De sentrale internasjonale menneskerettighetsinstrumentene som omfatter personopplysningsvernet er Den europeiske menneskerettskonvensjon (EMK) og FNs konvensjon om sivile og politiske rettigheter (SP). Det følger av menneskerettsloven at disse konvensjonene gjelder som norsk lov.

Det følger av EMK artikkel 8 nr. 1 at enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse. Etter praksis fra Den europeiske menneskerettsdomstol (EMD) vil personopplysningsvernet etter omstendighetene innfortolkes i begrepet «privatliv», men likevel ikke slik at alle former for personlig informasjon omfattes, se for eksempel *S. og Marper mot Storbritannia* (4. desember 2008) avsnitt 66 og 67. Ved vurderingen må det ses hen til den spesifikke konteksten rundt innsamlingen og lagringen, personopplysningenes art, med hvilket formål opplysningene brukes og prosesseres, og resultatene som kan oppnås. Der det er sikkerhets- og etterretningstjenester som innhenter og tar i bruk personopplysninger, er formodningen at det er tale om et inngrep etter EMK artikkel 8, se for eksempel *Rotaru mot Romania* (4. mai 2000). Likevel kan det tenkes tilfeller der personopplysninger som innhentes i forbindelse med strategisk etterretning, slik som lister over deltakere på åpne møter, ikke vernes etter denne bestemmelsen.

Hvor fritt myndighetene står ved utformingen av regler om behandling av personopplysninger, varierer etter hvilke omstendigheter opplysningene er innhentet og lagret i, samt opplysningenes art. EMD har for eksempel fremholdt at statene har en videre skjønnsmargin i saker som involverer mistenkte terrorister, særlig der det er tale om lagring av informasjon om individer som har tatt del i terroraktiviteter tidligere, se for eksempel *Segerstedt-Wiberg mfl. mot Sverige* (6. juni 2006) avsnitt 88 til 89. På den andre siden vil skjønnsmarginen være snevrere der inngrepet kan vanskeliggjøre realiseringen av sentrale og intime rettigheter, se *G.S.B. mot Sveits* (22. desember 2015) avsnitt 93.

Norge har ratifisert Europarådets konvensjon nr. 108 av 28. januar 1981 om personvern i forbindelse med elektronisk databehandling av personopplysninger (Europarådets personvernkonvensjon). Konvensjonens formål er:

> «[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 («datavern»).»

Personvernkonvensjonen forplikter konvensjonspartene til å treffe nødvendige tiltak i sin interne lovgivning for å gjennomføre hovedprinsippene for datavern. Disse prinsippene går særlig ut på å sikre datakvalitet, herunder at personopplysningene innsamles og bearbeides på lovlig måte;

lagres for bestemte og lovlige formål og ikke nyttes på en måte som er uforenlig med disse formålene; er adekvate, relevante og ikke for omfattende i relasjon til formålet de lagres for; er nøyaktige og ajourførte; og at de oppbevares på en måte som begrenser identifikasjon til det som er formålsmessig, jf. artikkel 5. Det følger av artikkel 9 nr. 2 at det kan gjøres unntak fra enkelte av konvensjonsrettighetene der dette følger av lov og er et nødvendig tiltak i et demokratisk samfunn blant annet av hensyn til statens sikkerhet.

Personopplysningsvernet er regulert i EUs personvernforordning 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger, som erstattet EUs personverndirektiv 95/46. Forordningens overordnede mål er å verne fysiske personer i forbindelse med behandling av personopplysninger, og sikre ensartede regler og fri utveksling av personopplysninger i EØS-området. De generelle prinsippene som forordningen bygger på, er i stor grad sammenfallende med personverndirektivet.

EUs personvernforordning ble inkorporert i Norge gjennom personopplysningsloven 2018, som på de fleste områder erstatter personopplysningsloven 2000. Virksomhet innen nasjonal sikkerhet omfattes ikke av EØS-avtalens saklige virkeområde. EØS-relevante forordninger og direktiver har derfor begrenset relevans for utformingen av nasjonal lovgivning knyttet til nasjonal sikkerhet. Personopplysningsloven 2018 gjelder ikke for Etterretningstjenestens behandling av personopplysninger for etterretningsformål, se punkt 12.4.

12.4 Særregler om behandling av personopplysninger hos Etterretningstjenesten

12.4.1 Gjeldende rett

Etterretningstjenesten behandler personopplysninger innenfor rammen av etterretningstjenesteloven, personopplysningsloven 2000 og personopplysningsforskriften 2000. Personopplysningsloven 2000 implementerer personverndirektivet, som er erstattet av personvernforordningen. I en overgangsperiode fortsetter personopplysningsloven 2000 å gjelde for Etterretningstjenesten, jf. forskrift av 15. juni 2018 nr. 877 om overgangsregler om behandling av personopplysninger § 1 bokstav c.

12.4.2 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 12.3 at Etterretningstjenestens behandling av personopplysninger for etterretningsformål skal skje innenfor rammen av særregler som fremgår av ny etterretningstjenestelov. Det vises til at prinsippene og verdiene som den alminnelige personvernlovgivningen bygger på, bør være retningsgivende ved utformingen av regelverket.

Videre fremgår det at personopplysningsloven 2018 bør få anvendelse på behandling av personopplysninger for andre formål enn etterretningsformål i tjenestens alminnelige forvaltningsvirksomhet, for eksempel ved behandling av opplysninger om Etterretningstjenestens personell for arbeidsgiverformål.

Det fremgår av høringsnotatet punkt 12.5.2 at behandling i form av innhenting er gjenstand for særskilt regulering i lovutkastet kapittel 3 til kapittel 8, og derfor unntatt behandlingsreglene som foreslås i kapittel 9.

12.4.3 Høringsinstansenes syn

Flere høringsinstanser, herunder *Datatilsynet*, *Den norske dataforening – IT-politisk råd* og *Den internasjonale juristkommisjon – norsk avdeling*, er positive til at det foreslås egne regler om Etterretningstjenestens behandling av personopplysninger.

Advokatforeningen viser til at det i høringsnotatet pekes på viktige rettslige utgangspunkter for vern av personopplysninger, men stiller spørsmål ved om de foreslåtte behandlingsreglene reflekterer personopplysningsloven 2018 og EUs personvernforordning. Blant annet påpeker Advokatforeningen at de skjerpede kravene i det nye regelverket ikke er reflektert i lovutkastet, og at man ikke i tilstrekkelig grad hensyntar at personopplysningsvernet er en selvstendig grunnrettighet ved siden av retten til privatliv, jf. EUs pakt om grunnleggende rettigheter artikkel 7 og 8. Advokatforeningen mener at det må angis hvem som er behandlingsansvarlig for behandlingen av personopplysningene, samt at det bør inntas krav om innebygget personvern i regelverket.

Også *Datatilsynet* mener at personvernprinsipper må bygges ytterligere inn i loven, og at det bør stilles krav til kontinuerlig vurdering av personvernkonsekvenser. Tilsynet understreker i den sammenheng at den nye loven i størst mulig grad bør følge personopplysningsprinsippene som reflekteres i EUs personvernforordning, og uttaler:

> «Lov om etterretningen er ment å uttømmende regulere behandling av personopplysninger på dette området og bør gi føringer utover behandling i de enkelte sakene. Vi kan ikke se hvorfor det skal være lavere krav til slike vurderinger på dette området enn på forordningens virkeområde. Det kan her nevnes at politiregisterforskriften § 41-1 oppstiller krav til personvernkonsekvensvurderinger ved ny type behandling av personopplysninger på [politiregisterlovens] virkeområde. Dette kom inn i forskriften som en konsekvens av nytt EU-regelverk.
>
> Vi mener departementet må vurdere å ta inn bestemmelser om krav til innebygget personvern og krav til konsekvensutredninger, for eksempel ved innføring av ny teknologi i lov om Etterretningstjenesten, for å sikre at det ved innføring av nye tiltak gjøres gode personvernkonsekvensutredninger og at hensynet til personvernet vektlegges allerede når man starter planleggingen av et tiltak eller en tjeneste eller et produkt skal utvikles. Personvernhensyn skal ikke være noe man utkvitterer etter at en tjeneste er ferdig utviklet og alle valg er tatt.»

Datatilsynet mener at artikkel 23 i personvernforordningen bør være det naturlige utgangspunktet for vurderingen av personopplysningsreglene. Videre mener Datatilsynet at reglene for behandling av personopplysninger bør gis anvendelse for registre som omhandler innhenting av opplysninger fra åpne kilder.

Næringslivets sikkerhetsråd forutsetter at balansegangen mellom personvernet og samfunnssikkerheten ivaretas av de foreslåtte kontrollmekanismene i høringsforslaget.

12.4.4 Departementets vurdering

Departementet opprettholder forslaget i høringsnotatet om å gi tilpassede regler for Etterretningstjenestens behandling av personopplysninger i lovforslaget kapittel 9.

Advokatforeningen og *Datatilsynet* tar til orde for at reglene og prinsippene i personopplysningsloven 2018 og EUs personvernforordning bør reflekteres i større grad, herunder at departementet i større grad bør hensynta EUs pakt om grunnleggende rettigheter artikkel 7 og 8, og at EUs personvernforordning artikkel 23 bør danne et utgangspunkt for regelverket. Til dette vil departementet bemerke at forordningen artikkel 23 angir at det i nasjonal lovgivning er anledning til å fastsette unntak fra forpliktelsene og rettighetene fastsatt i artikkel 12 til 22, altså reglene som gir registrerte personer konkrete rettigheter. Slike unntak må være nødvendige og proporsjonale. I tillegg kreves at begrensningen overholder det vesentligste innholdet i de grunnleggende rettigheter og friheter. Forordningens fortalepunkt 73 slår fast at de fastsatte begrensningene må være i overensstemmelse med EUs pakt om grunnleggende rettigheter og EMK. Pakten er ikke en del av EØS-avtalen, og er dermed ikke bindende for Norge.

Personvernforordningen gjelder ikke tiltak for å ivareta nasjonal sikkerhet. Slik departementet ser det, er det primært Grunnloven § 102, EMK artikkel 8 og Europarådets personvernkonvensjon som må danne rammen for lovforslaget. De prinsipper som den generelle personopplysningslovgivningen bygger på, blant annet lovlighet, formålsbegrensning, riktighet, lagringsbegrensning, integritet og konfidensialitet, er etter departementets vurdering i stor grad ivaretatt i lovforslaget. De foreslåtte behandlingsreglene forutsetter at Etterretningstjenesten jevnlig må vurdere hvorvidt den konkrete behandlingen er innenfor lovens rammer. Ved innføring av ny teknologi eller andre tiltak som påvirker behandlingen av personopplysninger, må det gjøres nye vurderinger.

Behandling i form av innhenting omfattes som utgangspunkt av behandlingsbegrepet, jf. legaldefinisjonen i lovforslaget § 1-3 bokstav b. Departementet anser det imidlertid som hensiktsmessig at det i loven skilles mellom regler om innhenting og regler om behandling av personopplysninger *etter* innhenting. Dette skyldes at innhenting av informasjon er utførlig regulert i lovforslaget kapittel 3 til 8, se nærmere blant annet proposisjonens omtale av grunnvilkårene (kapittel 9), metodebruk for innhenting av informasjon (kapittel 10) og tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon (kapittel 11). På denne bakgrunn videreføres forslaget i høringsnotatet om å unnta behandling i form av innhenting fra lovforslaget kapittel 9. Departementet foreslår å tydeliggjøre dette i kapitteloverskriften.

12.5 Legaldefinisjon av begrepet «personopplysninger«

12.5.1 Gjeldende rett

I personopplysningsloven 2000 defineres «personopplysning» som «opplysninger og vurderinger

som kan knyttes til en enkeltperson», jf. § 2 nr. 1. Bestemmelsen reflekterer EUs personverndirektiv artikkel 2 bokstav a, som definerer en personopplysning som:

> «[Enhver] opplysning om en identifisert eller identifiserbar person («den registrerte»); en identifiserbar person er en som direkte eller indirekte kan identifiseres, særlig ved hjelp av et identifikasjonsnummer eller ett eller flere elementer som er særegne for personens fysiske, fysiologiske, psykiske, økonomiske, kulturelle eller sosiale identitet.»

Definisjonen er omtalt nærmere i Ot.prp. nr. 92 (1998–99) punkt 16 side 101 til 102.

12.5.2 Forslaget i høringsnotatet

I høringsnotatet punkt 12.4 foreslås det at «personopplysninger» skal forstås som «enhver opplysning og vurdering som med enkle midler kan knyttes til en identifisert eller identifiserbar fysisk person». Det vises til at forslaget materielt sett tilsvarer legaldefinisjonen i EUs personvernforordning artikkel 4 nr. 1.

Det redegjøres i høringsnotatet for at alle opplysninger som direkte eller indirekte kan knyttes til en person, skal regnes som personopplysninger i lovens forstand. Også opplysninger som bare kan knyttes til en person gjennom identifiserende kjennetegn, faller inn under begrepet. At opplysningen må kunne «knyttes til» en person, innebærer et krav om identifikasjon. I dette identifikasjonskravet ligger en forutsetning om at en opplysning med stor grad av sikkerhet må kunne knyttes til en spesifikk person, slik at et IP-nummer som tilhører en datamaskin med mange brukere ikke vil kunne regnes som en personopplysning fordi IP-nummeret ikke kan knyttes til en konkret enkeltperson. Imidlertid må ikke *selve identifiseringen* ha skjedd. Det fremgår videre av høringsnotatet at det er tilstrekkelig at identifisering kan skje, men da med «enkle midler», slik at ikke enhver fjern mulighet for identifisering er tilstrekkelig for å kategorisere en opplysning som en personopplysning. Jo mer alvorlige de mulige følgene for personvernet antas å kunne bli, desto mindre skal til for at noe regnes som en personopplysning.

12.5.3 Høringsinstansenes syn

Advokatforeningen, *Datatilsynet*, *Den internasjonale juristkommisjon – norsk avdeling*, *Den norske dataforening – IT-politisk råd* og *Kripos* er kritiske til at departementet foreslår en legaldefinisjon av «personopplysninger» som avviker fra definisjonen i EUs personvernforordning. Datatilsynet mener at det ikke er riktig at forslaget materielt sett tilsvarer legaldefinisjonen i personvernforordningen, og uttaler:

> «For [det] første avviker definisjonen språklig fra personvernforordningens, noe som i seg selv åpner for uklarheter, men den er også innholdsmessig forskjellig på et vesentlig punkt: I forslaget snevres definisjonen inn ved at det kun er opplysninger som med *enkle midler* kan knyttes til en person som er omfattet av definisjonen. Dette endrer altså kravet til hvor mye som skal til for å si at en opplysning er å regne som en personopplysning.»

Kripos mener at definisjonen av «personopplysninger» bør komme før definisjonen av «behandling av personopplysninger».

Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget) har i etterkant av høringen bedt departementet om å vurdere hvorvidt døde personer bør gis samme personopplysningsvern som levende personer.

12.5.4 Departementets vurdering

Flere høringsinstanser, blant andre *Advokatforeningen* og *Datatilsynet*, er kritiske til at det foreslås en definisjon av begrepet «personopplysninger» som avviker fra definisjonen i EUs personvernforordning. Departementet er enig med høringsinstansene i at personvernforordningens definisjon bør legges til grunn. Selv om personvernforordningen ikke er bindende på dette området, er det i dette tilfellet hensiktsmessig å benytte samme definisjon, da dette bidrar til klarhet og forutberegnelighet for rettsanvenderen. Det vises til merknadene til § 1-3 bokstav a for en nærmere redegjørelse for innholdet i begrepet.

EOS-utvalget har i brev 22. oktober 2019 bedt departementet om å vurdere å inkludere døde personer i personopplysningsbegrepet. Personopplysninger om døde personer er ikke direkte regulert i personopplysningsloven 2000, men det følger av Ot.prp. nr. 92 (1998–99) punkt 16 side 102 at slike opplysninger ikke omfattes av begrepet. Utvalget trekker paralleller til politiregisterloven og PSTs behandling av personopplysninger, og viser til at opplysningene som Etterretningstjenesten behandler, er så sensitive at personens død

ikke bør ha noen betydning for beskyttelsen. Utvalget viser til hensynet til avdødes ettermæle. Problemstillingen ble ikke reist i høringsnotatet eller i høringen, men departementet har vurdert spørsmålet på bakgrunn av EOS-utvalgets henvendelse.

Etter departementets vurdering gjør de hensyn som begrunner vernet av døde personers personopplysninger i politiregisterloven, særlig hensynet til avdødes ettermæle, seg ikke i like stor grad gjeldende for Etterretningstjenestens virksomhet. Departementet viser til at tjenesten ikke har oppgaver knyttet til straffeforfølgning. Det vil være en svært begrenset krets med personer som kjenner til at opplysningene om den avdøde blir behandlet. I motsetning til hva som gjelder for politiet, vil det i tillegg i all hovedsak dreie seg om utenlandske borgere. På bakgrunn av dette mener departementet at gjeldende rett bør videreføres, og foreslår ikke å la døde personer inkluderes i personopplysningsbegrepet i lovforslaget.

Departementet understreker at det gjelder en presumpsjon for at personen lever frem til det foreligger konkrete holdepunkter for noe annet. Dersom tjenesten ikke med en viss grad av sikkerhet kan slå fast at personen er død, vil behandlingsreglene etter kapittel 9 gjelde.

12.6 Behandlingsgrunnlag, behandlingsformål og nødvendighet

12.6.1 Gjeldende rett

12.6.1.1 Behandlingsgrunnlag

I personopplysningsloven 2000 fremgår de alminnelige reglene om behandlingsgrunnlag av § 8. Etter denne bestemmelsen kan behandling av personopplysninger bare finne sted dersom den registrerte har samtykket, dersom det er en lovfestet adgang til behandling, eller dersom behandlingen er nødvendig for et av formålene i bokstav a til f. For behandling av sensitive opplysninger må i tillegg et av vilkårene i § 9 første ledd være oppfylt.

Etterretningstjenestens behandlingsgrunnlag følger av personopplysningsloven 2000 sammenholdt med etterretningstjenesteloven § 3 første ledd. Etterretningstjenesten kan bare behandle personopplysninger dersom behandlingen antas å ha betydning for ivaretakelsen av tjenestens oppgaver etter § 3. Etterretningstjenesteloven § 3 første ledd gir tjenesten adgang til å innhente, bearbeide og analysere informasjon i den utstrekning det kan bidra til å sikre viktige nasjonale interesser, som er nærmere beskrevet i bokstav a til j. Etterretningstjenesten må vurdere om det er nødvendig å behandle den aktuelle informasjonen. Vurderingen er av etterretningsfaglig karakter, og kan variere etter fagområde, tema og andre omstendigheter. Det er tilstrekkelig at informasjonen *kan* være egnet, alene eller sett i sammenheng med annen informasjon, til å bidra til å sikre viktige nasjonale interesser.

Etterretningstjenesteloven § 4 andre 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. Det følger av bestemmelsen at innhentingsforbudet etter første ledd ikke skal tolkes dit hen at Etterretningstjenesten er avskåret fra å behandle opplysninger om norske fysiske og juridiske personer.

12.6.1.2 Behandlingsformål

Personopplysninger kan bare benyttes for uttrykkelig angitte formål som er saklig begrunnet i den behandlingsansvarliges virksomhet, jf. personopplysningsloven 2000 § 11 første ledd bokstav b. Dette innebærer at den behandlingsansvarlige forut for behandlingen må fastsette et formål som er tilstrekkelig konkret og avgrenset til at det skaper åpenhet og klarhet om hva behandlingen skal tjene til. Generelle og vage beskrivelser som «administrative oppgaver» eller «kommersiell bruk» vil ikke være tilstrekkelig presise. Jo større fare behandlingen kan medføre for personvernet, desto viktigere er det at formålet er presist definert (Ot.prp. nr. 92 (1998–99) punkt 16 side 114).

Personopplysninger skal ikke brukes senere til formål som er uforenlig med det opprinnelige formålet med innsamlingen, jf. personopplysningsloven 2000 § 11 første ledd bokstav c. Bokstav c må leses i sammenheng med § 11 første ledd bokstav a, som krever at behandlingen må oppfylle kravene til lovlig behandling i § 8, og eventuelt § 9 dersom det dreier seg om sensitive opplysninger. Hva som skal til før det nye behandlingsformålet er uforenlig med det opprinnelige formålet, må vurderes konkret og individuelt.

Det følger av etterretningstjenesteloven § 3 at tjenesten bare kan behandle personopplysninger for *etterretningsformål*. Skal tjenesten behandle

opplysninger med andre formål, må det etter personopplysningsloven § 11 foreligge et eget behandlingsgrunnlag for dette etter §§ 8 eller 9.

12.6.1.3 Nødvendighet

Kravet til nødvendighet 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*. 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.

12.6.2 Forslaget i høringsnotatet

I høringsnotatet punkt 12.5 foreslås det å regulere Etterretningstjenestens behandlingsgrunnlag i en bestemmelse om «formålsbestemthet» i lovutkastet § 9-2. Det følger av forslaget at tjenesten kan behandle personopplysninger for etterretningsformål. Etterretningsformål defineres som «formål å ivareta en eller flere av tjenestens oppgaver etter lovforslagets kapittel 3», jf. lovutkastet § 1-4 nr. 3.

Etterretningstjenesten skal etter lovutkastet kapittel 3 innhente og analysere informasjon om utenlandske militære og sivile forhold som kan bidra til å avdekke og motvirke forhold som nevnt i lovutkastet § 3-1 bokstav a til i. I tillegg skal tjenesten innhente informasjon om andre utenlandske forhold (§ 3-2), opprettholde okkupasjonsberedskap (§ 3-3), og drive internasjonalt samarbeid (§ 3-4). Det vises til at tjenesten også skal kunne innhente evneinformasjon som utgjør nødvendige forutsetninger for å kunne gjennomføre oppgavene (§ 3-5). Lovutkastet kapittel 3 danner altså rammen for hva slags personopplysninger som kan behandles til hvilke formål.

På samme måte som PSTs virksomhet anses som ett behandlingsformål, jf. Ot.prp. nr. 108 (2008–2009) punkt 9.2 side 74 til 76, vurderes det i høringsnotatet at også oppgavene etter lovutkastet kapittel 3 bør regnes som ett behandlingsformål. Dette særlig med hensyn til at oppgavene angitt i kapittel 3 anses for å ha en nær og naturlig sammenheng, og sjelden vil være uforenlige med hverandre.

I lovutkastet § 9-5 foreslås et uttrykkelig krav om at Etterretningstjenesten skal vurdere om personopplysningene er nødvendige å behandle for etterretningsformål. Det foreslås at nødvendighetsvurderingen skal foretas første gang opplysningen vurderes brukt for etterretningsformål, herunder når opplysningene inntas i et produkt som planlegges distribuert utenfor tjenesten, og ellers dersom ny informasjon eller andre omstendigheter tilsier det. For personopplysninger som er rådata i bulk, foreslås en særregel om at nødvendighetsvurderingen skal gjennomføres samlet når rådata innhentes etter reglene i lovutkastet § 5-3, og ellers når ny informasjon eller andre omstendigheter tilsier det.

I lovutkastet § 9-5 tredje ledd foreslås det behandlingsgrunnlag for personopplysninger om kilder som ikke ønsker å samarbeide med tjenesten, for å hindre at vedkommende kontaktes igjen. Behandling om slike kilder skal begrenses til det som er strengt nødvendig for dette formålet. Regelen foreslås av hensyn til den registrerte selv.

I lovutkastet § 9-7 foreslås et unntak fra kravene til formålsbestemthet og nødvendighet, som skal sikre at Etterretningstjenesten har hjemmel til å behandle personopplysninger som samles inn, men som ikke ennå er vurdert for etterretningsrelevans (rådata).

I høringsnotatet punkt 12.4.2 vurderes det at det ikke er nødvendig å skille mellom behandling av alminnelige personopplysninger og behandling av sensitive personopplysninger. Dette begrunnes i at Etterretningstjenestens regelverk og forslaget i høringsnotatet bærer preg av at tjenesten nettopp behandler sensitive opplysninger. Personopplysningenes grad av sensitivitet vil imidlertid være et sentralt moment i forholdsmessighetsvurderingen. Det foreslås en egen bestemmelse om diskrimineringsforbud, se punkt 12.7 under.

12.6.3 Høringsinstansenes syn

Kripos mener at det bør ses hen til det alminnelige nødvendighetsprinsippet i personvernlovgivningen ved utformingen av § 9-5, det vil si at opplysninger kun kan behandles når det er nødvendig for å oppnå formålet med behandlingen. Kripos mener også at begrepet «distribuert» i § 9-5 andre ledd bør erstattes med begrepet «utlevert».

Kripos mener videre at lovutkastet § 9-7, som gir Etterretningstjenesten hjemmel til å behandle personopplysninger for å avklare om grunnkrav til behandling er oppfylt, ikke gir føringer for behandlingen, og at bestemmelsen fremstår som et generelt unntak fra formålsbestemthet og nødvendighet. Kripos mener det bør gjelde en viss tidsfrist for denne avklaringen.

12.6.4 Departementets vurdering

12.6.4.1 Innledning

Departementet viderefører i hovedsak det materielle innholdet i forslaget i høringsnotatet, men foreslår en omstrukturering av bestemmelsene og flere lovtekniske justeringer. Etter departementets vurdering bør Etterretningstjenestens behandlingsgrunnlag komme klart frem i en egen bestemmelse, og paragrafoverskriften til lovforslaget § 9-2 foreslås derfor endret fra «formålsbestemthet» til «behandlingsgrunnlag». Departementet foreslår å ta inn kravet til vurdering av nødvendighet i bestemmelsen. Denne endringen gjør lovutkastet § 9-5 om nødvendighet overflødig, og departementet viderefører heller ikke forslaget om unntak fra kravet til formålsbestemthet og nødvendighet i lovutkastet § 9-7.

12.6.4.2 Behandling av personopplysninger

Behandling av personopplysninger er definert i lovforslaget § 1-3 bokstav b. Med behandling menes «enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke». Definisjonen tilsvarer definisjonen i personvernforordningen, og er ment å omfatte de samme behandlingsformene. Definisjonen er ikke uttømmende, så andre operasjoner eller aktiviteter enn de som er nevnt i bestemmelsen kan etter omstendighetene omfattes. Det skal svært lite til før en aktivitet er omfattet av definisjonen, slik at mer eller mindre enhver befatning som Etterretningstjenesten har med personopplysninger, vil regnes som behandling.

Det følger av lovforslaget § 4-1 at Etterretningstjenesten som hovedregel ikke kan benytte innhentingsmetoder overfor personer i Norge. Personopplysningene som tjenesten behandler, vil dermed i hovedsak gjelde personer som befinner seg utenfor norsk territorium. Det er imidlertid ikke forbudt for tjenesten å behandle personopplysninger om norske borgere, så lenge det er nødvendig for etterretningsformål og opplysningene ikke er innhentet i strid med forbudet mot innhenting i Norge. Dette er en videreføring av gjeldende etterretningstjenestelov § 4 andre ledd. Behandling av personopplysninger om norske borgere kan aktualiseres på ulike måter, for eksempel ved innhenting fra åpne kilder som berører personer i Norge, eller ved innhenting av rådata i bulk, se nærmere proposisjonen kapittel 8.

Etterretningstjenesten behandler forskjellige typer personopplysninger i sin etterretningsvirksomhet. Enkelte av opplysningene kan være «sensitive personopplysninger» etter personopplysningsloven 2000 § 2 nr. 8, for eksempel opplysninger om etnisk bakgrunn eller politisk oppfatning. I motsetning til reguleringen i personopplysningsloven 2000, foreslår ikke departementet at det oppstilles krav om et særskilt behandlingsgrunnlag utover det som følger av lovforslaget kapittel 9. Det anses ikke hensiktsmessig å skille mellom vanlige og sensitive personopplysninger når det gjelder behandlingsgrunnlaget, da det ligger i sakens natur at tjenesten vil måtte behandle sensitive personopplysninger. Departementet mener derfor at det samme kravet til nødvendighet bør gjelde for all behandling av personopplysninger, uavhengig av personopplysningens art. Forholdsmessighetsvurderingen vil imidlertid kunne tilsi at én personopplysning er nødvendig å behandle, mens en annen, av mer sensitiv karakter, ikke vil være det.

12.6.4.3 Behandlingsformål

Departementet viderefører forslaget om å knytte det rettslige grunnlaget for behandling av personopplysninger til formålet med behandlingen. Ingen høringsinstanser har gitt uttrykk for innvendinger mot å anse Etterretningstjenestens oppgaver etter kapittel 3 som ett behandlingsformål.

Departementet presiserer at behandling av personopplysninger for andre formål enn etterretningsformål, må følge de alminnelige reglene i personopplysningsloven 2018 og personvernforordningen. I den sammenheng vil det særlig være personvernforordningen artikkel 6 nr. 4 som vil være avgjørende for om personopplysningene kan viderebehandles til nye formål. Dette vil blant annet gjelde ved viderebehandling for historiske, statistiske eller vitenskapelige formål. Etterretningstjenesten avleverer ikke arkiver til Riksarkivet, og har derfor et eget ansvar for å dokumentere og lagre materiale for historiske formål. Det presiseres at behandling av personopplysninger for å oppfylle lovens krav, for eksempel for å sikre at tjenesten overholder forbudet mot innhenting i Norge etter lovforslaget § 4-1, vil regnes som etterretningsformål.

Hva som til enhver tid vil være etterretningsformål, beror på oppgavebeskrivelsen i lovforslaget kapittel 3. Dette er nærmere omtalt i kapittel 7 i proposisjonen og i merknadene til lovforslaget kapittel 3.

12.6.4.4 Nødvendighet

Nødvendighetskravet er et sentralt personvernrettslig prinsipp, som gjelder for enhver behandling av personopplysninger hos Etterretningstjenesten. Selv om tjenesten har hjemmel til å behandle opplysninger for etterretningsformål, utgjør nødvendighetskravet en begrensning, da opplysninger bare kan behandles når det er nødvendig ut fra formålet.

Hvilke opplysninger det er nødvendig å behandle for etterretningsformål, beror på en konkret etterretningsfaglig vurdering. Sentrale momenter er omfanget av behandlingen, inngrepets karakter, og hvor relevant informasjonen er for formålet. Kravet kan ikke tolkes så strengt at behandlingen må være den eneste mulige løsningen, men det er heller ikke tilstrekkelig at behandlingen bare er hensiktsmessig. Et bærende synspunkt i den sammenheng, er at Etterretningstjenestens tilgang til informasjon skal sette tjenesten i stand til å løse oppgavene sine 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. I det praktiske etterretningsarbeidet er det avgjørende å kunne bearbeide store mengder opplysninger over tid.

En særskilt problemstilling er *når* nødvendighetsvurderingen skal finne sted. Kravet til nødvendighet i forbindelse med behandling av personopplysninger etter kapittel 9 gjelder først etter at opplysningene er samlet inn, jf. lovforslaget § 9-3, som fastsetter at reglene i kapittel 9 ikke gjelder for behandling i form av innhenting.

I høringsnotatet punkt 12.6.2.3 ble det vurdert om det var behov for å regulere tidspunktet for når nødvendighetsvurderingen etter kapittel 9 om behandling av personopplysninger skal foretas. Det ble vist til at politiregisterloven gir politiet adgang til å behandle personopplysninger i fire måneder for å avklare om kravene til behandling er oppfylt. Det ble imidlertid vurdert som uhensiktsmessig å oppstille en tilsvarende frist for Etterretningstjenesten. *Kripos* fremholder i sin høringsuttalelse at det bør tas inn en tidsfrist for å avklare om kravene til behandling er oppfylt.

Departementet foreslår å sløyfe angivelsen av når nødvendighetsvurderingen skal foretas. Etter departementets syn vil det gi en bedre og mer sammenhengende regulering dersom nødvendighetskravet for behandling av personopplysninger i prinsippet gjelder straks opplysningene er samlet inn. Kravet må imidlertid ses i sammenheng med bestemmelsene om Etterretningstjenestens adgang til å innhente informasjon. For innhenting gjelder det nærmere regler i lovforslaget kapittel 3 til kapittel 8. Det oppstilles blant annet et krav om forholdsmessighet etter lovforslaget § 5-4. I den forbindelse må nødvendigheten av å samle inn opplysningene vurderes. I enkelte av bestemmelsene oppstilles det strengere nødvendighetskrav, for eksempel lovforslaget §§ 6-6 og 6-7.

Nødvendighetsvurderingen som foretas ved innhentingen, knytter seg naturlig nok ikke bare til selve innhentingen, men også til om det er behov for å beholde opplysningene en viss tid for å vurdere nærmere den konkrete relevansen. Når det er vurdert at innhentingen er nødvendig, jf. kapittel 3 til 8, må det også etter lovforslaget § 9-2 kunne legges til grunn at det er nødvendig å beholde opplysningene en viss tid for å vurdere dem nærmere. På denne bakgrunn er departementet kommet til at det ikke er behov for en bestemmelse som gjør unntak fra kravet til formålsbestemthet og nødvendighet som foreslått i lovutkastet § 9-7, og forslaget videreføres ikke.

Departementet vil samtidig bemerke at selv om det er gjort en nødvendighetsvurdering ved innhentingen, må det foretas nye nødvendighetsvurderinger for å oppfylle kravet i § 9-2. Dette må i alle tilfeller gjøres når opplysninger som er innhentet og lagret, vurderes brukt i etterretningsprodukter. Dersom det viser seg at innhentede opplysninger ikke brukes i etterretningsprodukter, må det vurderes om fortsatt lagring er nødvendig for etterretningsformål. Det lar seg imidlertid ikke angi generelt på hvilke tidspunkter dette må gjøres. I hvilken grad større mengder av opplysninger kan vurderes samlet, beror på omstendighetene, på samme måte som etter personopplysningsloven. Det vises til merknadene til § 9-2 for en nærmere omtale. Kravet til nødvendighet må for øvrig ses i sammenheng med sletteplikten etter lovforslaget § 9-8, som blant annet inneholder konkrete slettefrister for rådata innhentet i bulk.

Departementet bemerker at Etterretningstjenesten i sine systemer vil kunne ha personopplysninger som på et tidspunkt var vurdert som nødvendig å behandle for etterretningsformål, men som med tiden har fått mer historisk karakter. *Når* en personopplysning mister sin relevans og blir mer av historisk karakter, vil ofte være vanskelig å tidfeste konkret. Sett hen til arbeidsmetodikk og at et sakskompleks kan gjøre det nødvendig å behandle enkelte opplysninger over lang tid,

blir en konkret tidsfrist for fornyet vurdering av nødvendighet uhensiktsmessig.

Det understrekes at nødvendighetskravet gjelder for alle deler av en behandling, blant annet med hensyn til hvilke opplysninger som kan lagres, hvem som skal få tilgang til opplysningene, og hvor lenge de skal oppbevares.

12.6.4.5 Særlig om behandling av rådata

Rådata defineres i lovforslaget § 1-3 bokstav h som ubearbeidet eller automatisk bearbeidet informasjon i enhver form hvis etterretningsverdi ikke er vurdert. Av tekniske og praktiske årsaker er det umulig å foreta rutinemessige gjennomgåelser av samtlige lagrede rådata på Etterretningstjenestens innhentingsplattformer for å vurdere om hver enkelt informasjonsbit er nødvendig å behandle for etterretningsformål eller ikke. Dette gjelder uavhengig av omfanget til den konkrete innhentede dataen, og uavhengig av om det skjer ved bulkinnhenting eller ikke.

Rådata kan hentes inn på forskjellige måter. Når Etterretningstjenesten mottar informasjon fra andre norske myndigheter, virksomheter eller internasjonale samarbeidende tjenester, er det under forutsetning av at avgiver av informasjonen vurderer opplysningene som nødvendige for Etterretningstjenestens oppdrag. Det er imidlertid tjenesten selv som må vurdere om opplysningene er nødvendig å behandle for etterretningsformål, eller om de må slettes.

Når Etterretningstjenesten selv innhenter informasjon, gjøres dette basert på holdepunkter og etterretningsfaglige hypoteser, slik at en viss nødvendighetsvurdering allerede er foretatt på innhentingstidspunktet. I tillegg er innhentingen formålsstyrt. Målet er å fremskaffe etterretningsrelevant informasjon. Departementet viser til lovforslaget §§ 5-1 og 5-2, som er nærmere omtalt i kapittel 9.

Det rettslige grunnlaget for innhenting av rådata foreligger i de ulike innhentingshjemlene i lovforslaget, og i nødvendighetsvurderingen som skal foretas etter § 5-3 første ledd om innhenting av rådata i bulk. Etter at rådataene er innhentet, vil nødvendighetskravet og kravet til behandlingsformål gjøre at Etterretningstjenesten må ta stilling til om de har behandlingsgrunnlag for videre behandling av de konkrete personopplysningene.

12.7 Forbudet mot diskriminering

12.7.1 Gjeldende rett

Forbudet mot diskriminering ved behandling av personopplysninger følger forutsetningsvis av Grunnloven § 98, som lyder:

> «Alle er like for loven.
>
> Intet menneske må utsettes for usaklig eller uforholdsmessig forskjellsbehandling.»

EMK artikkel 14 lyder i norsk oversettelse:

> «Utøvelsen av de rettigheter og friheter som er fastlagt i denne konvensjon skal bli sikret uten diskriminering på noe grunnlag slik som kjønn, rase, farge, språk, religion, politisk eller annen oppfatning, nasjonal eller sosial opprinnelse, tilknytning til en nasjonal minoritet, eiendom, fødsel eller annen status.»

Bestemmelsen må leses i lys av EMK artikkel 8 om retten til respekt for privatliv, herunder personopplysningsvernet.

12.7.2 Forslaget i høringsnotatet

I høringsnotatet punkt 12.4.2 foreslås det et forbud mot å behandle personopplysninger utelukkende basert på hva som er kjent om en persons etnisitet eller nasjonale bakgrunn, politiske, religiøse eller filosofiske overbevisning, språk, politiske virksomhet, fagforeningstilhørighet, helsemessige eller seksuelle forhold. Diskrimineringsforbudet, som i høringsnotatet er inntatt i lovutkastet § 9-4, skal sikre at Etterretningstjenesten ikke baserer behandlingen av personopplysninger kun på et av de ovennevnte forholdene.

12.7.3 Høringsinstansenes syn

Dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors mener at det bør beskrives hvordan diskrimineringsforbudet i lovutkastet § 9-4 skal vurderes opp mot grunnvilkåret i § 5-1 om at det må være «grunn til å undersøke».

Kripos påpeker at det synes som om man i høringsnotatet har tatt utgangspunkt i den tidligere definisjonen av sensitive opplysninger i personopplysningsloven 2000 § 2 nr. 8. Kripos bemerker at personvernlovgivningen nå bruker formuleringen «særlige kategorier personopplysninger», som blant annet også omfatter genetiske og biometriske opplysninger. Kripos viser til person-

vernforordningen artikkel 9 og politiregisterloven § 7 for veiledning ved utformingen av diskrimineringsforbudet.

12.7.4 Departementets vurdering

Departementet viderefører forslaget i høringsnotatet om å lovfeste et diskrimineringsforbud. Selv om et slikt forbud allerede følger av Grunnloven og EMK, mener departementet at hensyn til klarhet og forutberegnelighet tilsier å lovfeste det i etterretningstjenesteloven. Når det gjelder høringsuttalelsen til *Kripos*, vil departementet påpeke at forslaget til diskrimineringsforbud ikke er en bestemmelse som stiller krav om behandlingsgrunnlag for denne typen opplysninger. Det er derfor heller ikke naturlig å se hen til de bestemmelsene Kripos viser til for utformingen av diskrimineringsforbudet i etterretningstjenesteloven. Det vises for øvrig til punkt 12.6.4.2, hvor det redegjøres nærmere for behandlingsgrunnlaget knyttet til sensitive personopplysninger.

Departementet understreker at diskrimineringsforbudet ikke forbyr Etterretningstjenesten å behandle opplysninger om en persons etnisitet eller nasjonale bakgrunn, politiske, religiøse eller filosofiske overbevisning, språk, politiske virksomhet, fagforeningstilhørighet eller helsemessige eller seksuelle forhold. Behandlingen av slike personopplysninger må imidlertid suppleres med andre opplysninger som er av en annen karakter. Etterretningstjenesten vil for eksempel kunne behandle opplysninger om en persons religiøse tilhørighet hvis tjenesten følger med på et ekstremistisk miljø i utlandet som baserer seg på rekruttering av personer med en spesiell trosretning, og vedkommende har en tilknytning til dette miljøet. Likeledes vil det kunne være grunnlag for å behandle opplysninger om et etterretningsmåls etniske bakgrunn fordi opplysningene kan være av betydning for identifikasjon. Forbudet innebærer imidlertid et forbud mot behandling utelukkende på bakgrunn av hva de nevnte forhold. Det innebærer for eksempel at det ikke kan brukes digitale verktøy som registrerer, selekterer eller på annen måte behandler opplysninger om personer kun basert på slike kjennetegn.

Dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors savner en beskrivelse av forholdet mellom diskrimineringsforbudet i lovforslaget § 9-4 og grunnvilkåret i lovforslaget § 5-1. Departementet bemerker at diskrimineringsforbudet, som ifølge lovforslaget § 9-3 gjelder for behandling i form av innhenting, har som konsekvens at det ikke kan være «grunn til å undersøke» alene på grunn av informasjon om forhold som omfattes av diskrimineringsforbudet. For eksempel vil informasjon om den religiøse eller politiske tilhørigheten til en person ikke alene gi «grunn til å undersøke». Informasjon om andre omstendigheter må komme i tillegg. Forbudet mot diskriminering kan på den måten ses som en presisering av grunnvilkåret i § 5-1. Det samme gjelder grunnvilkåret for målrettet innhenting i lovforslaget § 5-2.

12.8 Behandling av kildeidentifiserende opplysninger og fortrolig kommunikasjon

12.8.1 Innledning

Opplysninger som er egnet til å avsløre kilden til en journalist, samt enkelte former for taushetsbelagt kommunikasjon, er særlig vernet etter henholdsvis Grunnloven § 100 og EMK artikkel 10 om ytringsfriheten og Grunnloven § 102 og EMK artikkel 8 om retten til privatliv. Inngrep i vernet kan bare finne sted dersom det er forankret i lov, forfølger et legitimt formål og oppfyller krav til nødvendighet og forholdsmessighet.

I høringsnotatet foreslås særregler for Etterretningstjenestens behandling av kommunikasjon og opplysninger som nevnt over. Flere høringsinstanser kritiserer forslaget. Departementet har i lys av disse høringsinnspillene foretatt en grundig vurdering av forslagets utforming, rekkevidde og innhold.

12.8.2 Kildevernet. Gjeldende rett

Ytringsfriheten er vernet av Grunnloven § 100, EMK artikkel 10 og SP artikkel 19. Den omfatter frihet til å ha meninger og til å motta og meddele opplysninger og ideer uten inngrep av offentlig myndighet og uten hensyn til grenser. Retten til å bestemme om en opplysning overhodet skal avgis, altså retten til å forholde seg taus, omfattes også. Denne siden av ytringsfriheten forankrer pressens rett til å forholde seg tause om sine kilder. Det følger av flere avgjørelser i EMD at kildevernet omfattes av EMKs ytringsfrihetsbegrep, se for eksempel *Goodwin mot Storbritannia* (27. mars 1996) avsnitt 39.

Kildevernet kommer også til uttrykk i norsk prosesslovgivning, se særlig straffeprosessloven § 125 og tvisteloven § 22-11. Reglene gir blant andre redaktører av et trykt skrift rett til å nekte å svare på spørsmål eller legge frem bevis om hvem

som er kilde for opplysninger som er betrodd dem i deres journalistiske virksomhet.

Kildevernet omfatter journalistisk materiale som direkte eller indirekte kan avsløre identiteten til en kilde som journalisten har benyttet. Vernet omfatter opplysninger som kan identifisere kilden ved navn, bilde eller annen personidentifikasjon, samt uredigert og upublisert materiale såfremt informasjonen kan avsløre journalistens kilder, se for eksempel HR-2015-2308-A avsnitt 53 og 54. Kildevernet kan også omfatte kilder som har stått frem som sådanne i det offentlige, slik at journalister kan nekte å forklare seg om kontakten med vedkommende, se EMDs avgjørelse i *Becker mot Norge* (5. oktober 2017).

Ytringsfriheten kan innskrenkes ved lov dersom det er nødvendig i et demokratisk samfunn blant annet av hensyn til den nasjonale sikkerhet, territoriale integritet eller offentlige trygghet, jf. EMK artikkel 10 nr. 2. I lys av kildevernets betydning for et velfungerende og informert demokrati, har EMD lagt til grunn en høy terskel for når inngripende myndighetsutøvelse kan aksepteres. Et inngrep må la seg forsvare «by an overriding requirement in the public interest», se *Goodwin mot Storbritannia* avsnitt 39 og senere praksis fra EMD. Dette innebærer at kildevernet kun vil vike dersom andre og tilsvarende tungtveiende samfunnsinteresser etter omstendighetene gjør inngrepet nødvendig og forholdsmessig. For eksempel kan det være grunn til å gjøre unntak dersom den aktuelle saken gjelder alvorlig kriminalitet, se HR-2015-2308-A avsnitt 67 med henvisning til HR-2013-2170-A avsnitt 32. Tilsvarende må antas å gjelde der det er tale om inngrep for å avverge eller oppklare forhold som er av vesentlig betydning for rikets sikkerhet. Den potensielt dempende og derved skadelige effekten et inngrep i vernet kan ha på pressens tilgang til kilder, vil være et tungtveiende moment i forholdsmessighetsvurderingen.

12.8.3 Retten til privatliv og vern om fortrolig kommunikasjon. Gjeldende rett

Enhver har rett til respekt for sitt privatliv, herunder sin korrespondanse og kommunikasjon, jf. Grunnloven § 102 og EMK artikkel 8. Myndighetene kan gripe inn i retten dersom inngrepet har grunnlag i lov, forfølger et legitimt formål og er nødvendig og forholdsmessig. Enkelte former for kommunikasjon nyter etter omstendighetene et sterkere menneskerettslig vern enn andre, slik som advokaters korrespondanse med sine klienter og særlig sensitive helsedata. Dette vernet kjennetegnes ved at det stilles strengere krav til nødvendigheten av inngrepet og til sikkerhetsgarantiene som skal forhindre misbruk.

EMD har i flere saker uttalt at advokaters klientkorrespondanse er særlig vernet etter EMK artikkel 8, se for eksempel *Kopp mot Sveits* (25. mars 1998), *Erdem mot Tyskland* (5. juli 2001) og *Helander mot Finland* (10. september 2013). Advokaters vern etter EMK artikkel 8 kan også ha en side til EMK artikkel 6 om retten til en rettferdig rettergang. *Erdem mot Tyskland* gjaldt spørsmålet om innsamling av korrespondansen mellom en innsatt og dennes advokat var et ulovlig inngrep i EMK artikkel 8. Domstolen uttalte i avsnitt 65:

> «[...] the privilege that attaches to correspondence between prisoners and their lawyers constitutes a fundamental right of the individual and directly affects the rights of the defence.»

Domstolen uttalte dernest at korrespondansevernet bare kunne fravikes «in exceptional cases and on condition that adequate and sufficient safeguards against abuse are in place». I *Kopp mot Sveits* ble Sveits felt for krenkelse av EMK artikkel 8 som følge av at det sveitsiske postvesenet på påtalemyndighetens anmodning hadde avlyttet telefonlinjene til et sveitsisk advokatkontor. Det ble lagt særlig vekt på at avlyttingen var basert på en administrativ beslutning uten «supervision by an independent judge» (avsnitt 74). På samme måte som i *Erdem mot Tyskland*, viste EMD til at den aktuelle korrespondansen direkte angikk «the rights of the defence».

Respekt for konfidensialiteten til helsedata er et grunnleggende prinsipp som hensyntar både den enkelte pasients privatliv og befolkningens tillit til helsetjenestene. For å unngå at det oppstår en nedkjølende effekt på befolkningens bruk av helsetjenester, kreves sikkerhetsmekanismer som forhindrer bruk av helsedata på en måte som er i strid med EMK artikkel 8. Helsedataenes karakter, herunder hvor sensitive opplysninger det er tale om, vil spille inn i forholdsmessighetsvurderingen. Der det er tale om å avdekke opplysninger som kan ha en ødeleggende effekt for privatlivet til et individ, må det være «justified by an overriding requirement in the public interest» (*Z mot Finland* 25. februar 1997, avsnitt 96).

12.8.4 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 12.10 å lovfeste særlige regler for Etterretningstjenestens behandling av «fortrolig kommunikasjon med særlige yrkesutøvere». Etter forslaget omfattes både yrkesutøvere som er underlagt lovbestemt eller yrkesetisk taushetsplikt (kallsmessig taushetsplikt) og journalister mv. som har rett til å forholde seg tause om identiteten til kilder for opplysninger (kildevernet) av betegnelsen «særlige yrkesutøvere». Personkretsen med kallsmessig taushetsplikt tilsvarer de yrkesgrupper som omfattes av straffeprosessloven § 119 og tvisteloven § 22-5.

Det vises til at vernet er funksjonelt, og således vil bero på en konkret vurdering av om den enkeltes yrkestittel er reell eller et skalkeskjul for virksomhet som ikke gir grunnlag for vern. I vurderingen vil det ha stor betydning om den aktuelle yrkesutøveren utfører sitt arbeide i tråd med profesjonelle og yrkesetiske krav. En person vil ikke være å regne som en særlig yrkesutøver dersom det sannsynliggjøres at yrkestittelen misbrukes. Det kan også tenkes at en person som fungerer som særlig yrkesutøver, også bedriver illegal virksomhet i arbeidstiden. I slike tilfeller vises det til at det må vurderes konkret hvilke opplysninger som må regnes som «fortrolige».

I høringsnotatet vernes opplysninger som etter en konkret vurdering anses som «fortrolig kommunikasjon». Vernets rekkevidde skal forstås på samme måte som i prosesslovgivningen. Kommunikasjonens karakter er avgjørende, herunder om opplysningene er *betrodd* yrkesutøveren som ledd i utførelsen av dennes yrke. Det skilles mellom profesjonell og privat kommunikasjon.

Hovedregelen som foreslås i høringsnotatet, er at fortrolig kommunikasjon med særlige yrkesutøvere ikke skal behandles. Det gjøres unntak fra behandlingsforbudet dersom «vektige samfunnshensyn gjør behandlingen strengt nødvendig». Unntaket begrunnes i at det kan tenkes tilfeller hvor hensynet til nasjonal sikkerhet vil veie tyngre enn hensynet til å verne den fortrolige kommunikasjonen, og hvor Etterretningstjenesten har et strengt begrunnet behov for å behandle slik informasjon. Kravet til streng nødvendighet vil i praksis innebære at opplysningene må være av vesentlig betydning for utførelsen av et konkret oppdrag, og at informasjonen må være umulig å tilveiebringe på noen annen praktikabel og mindre inngripende måte. Den høye terskelen begrunnes i at en uthuling av det særlige vernet av fortrolig kommunikasjon kan påvirke samfunnet så vel som den enkelte på en negativ måte, herunder at en slik uthuling kan medføre en fare for en nedkjølende effekt knyttet til pressens kildetilfang og bruk av tjenester der yrkesutøveren er underlagt kallsmessig taushetsplikt. Det understrekes at terskelen må tolkes og anvendes i lys av Norges menneskerettslige forpliktelser.

Som garanti mot misbruk og tiltak mot potensielle negative konsekvenser, foreslås det at opplysninger som er fortrolig kommunikasjon som ikke kan behandles av Etterretningstjenesten, heller ikke skal kunne utleveres. Det samme foreslås for fortrolig kommunikasjon som er overskuddsinformasjon. Som en ytterligere sikkerhetsgaranti foreslås det at beslutningen om å behandle fortrolig kommunikasjon bør fattes av sjefen for Etterretningstjenesten, og i enkelte tilfeller av departementet selv. Videre foreslås at opplysninger som er fortrolig kommunikasjon, skal merkes særskilt, for på den måten å legge til rette for EOS-utvalgets kontroll.

12.8.5 Høringsinstansenes syn

Flere høringsinstanser er kritiske til forslaget, blant annet *Advokatforeningen, Datatilsynet*, *Norges institusjon for menneskerettigheter (NIM)* og en rekke presse- og medieaktører. Kritikken går i stor grad ut på at forslaget ikke oppfyller menneskerettslige krav. Flere av høringsinnspillene knytter seg til forslaget om tilrettelagt innhenting, som behandles i kapittel 11 i proposisjonen.

De fleste høringsinnspillene angår forslagets betydning for pressens kildevern. Enkelte instanser omtaler også annen fortrolig kommunikasjon. *Advokatforeningen* peker på at forslaget ikke ivaretar konfidensialiteten mellom en advokat og dennes klient, og viser blant annet til EMDs praksis på området i sin uttalelse:

> «De konfidensialitetsprivilegier som vi står overfor her, slik som kommunikasjon mellom advokat og klient, er grunnleggende. De håndheves strengt, både av våre nasjonale domstoler og av de internasjonale domstolene som EMD og EU-domstolen. EMD har i flere saker understreket at i den grad det er innrettet systemer for informasjonsinnsamling som fanger opp slik konfidensiell kommunikasjon, eller slik informasjon rent faktisk kommer med, så må det finnes en form for uavhengig konkret kontroll. Advokatforeningen viser blant annet til saken *Kopp mot Sveits* (1998), der det sveitsiske postvesen hadde på påtalemyndighetens anmodning avlyttet telefonlin-

jene til et sveitsisk advokatkontor. EMD fant at dette utgjorde en krenkelse av artikkel 8 som ikke kunne legitimeres i tvingende nødvendige hensyn. EMD påpekte videre som oppsiktsvekkende at avlyttingen var basert på en ren administrativ beslutning uten noen form for uavhengig konkret kontroll ved domstolene.»

NIM konsentrerer seg om kildevernet i sin høringsuttalelse, men påpeker at flere av kommentarene kan ha generell verdi også overfor andre typer fortrolig kommunikasjon som nyter et særlig menneskerettslig vern, slik som kommunikasjonen mellom advokat og klient. NIM uttaler at de anser det som positivt at man i høringsnotatet søker å sette opp særskilte skranker for behandlingen av fortrolig kommunikasjon, men har en rekke innspill til hvordan lovutkastet kan forbedres. Om hvilke opplysninger som faller inn under kildevernet og hvordan dette bør fremgå av loven, uttaler NIM:

«Etter EMDs praksis er det ikke avgjørende for vurderingen av om opplysningene omfattes av kildevernet, hvor de stammer fra eller mellom hvem de utveksles (for eksempel mellom journalist og kilde, selv om det naturligvis ofte kan være tilfellet). Det avgjørende kan heller sammenfattes som hvorvidt opplysningene er *egnet til å avsløre* en kildes identitet. [...]

Det er uklart for NIM om forslaget i § 9-6 er ment å innebære noen begrensning med hensyn til hvilket format opplysningene kan stamme fra – om det må være fra selve «kommunikasjonen» (eposter etc.) mellom journalist og kilde. Dette vil i tilfellet være en avsporing sammenlignet med hva som er relevant å vurdere i henhold til EMDs praksis. Kildevernet har ikke nødvendigvis for øye å verne kommunikasjonen som sådan, men å verne den generelle tilliten til at kilders identitet forblir anonym (uavhengig av hvordan identiteten eventuelt kan avsløres). Det vil også være en avsporing om det her legges opp til en eventuell vurdering av hvorvidt vedkommende er «journalist» i tradisjonell forstand eller lignende. Når lovforslaget viser til «tilsvarende fortrolig kommunikasjon» er det uklart om dette sikter på andre kategorier av personer enn de som er listet opp i § 9-6 første ledd, eller om det siktes til kommunikasjon som sådan.

NIM anbefaler at vilkåret for hvilken informasjon som gis et særlig vern gjøres mer fleksibel og i større grad knyttes opp mot hvorvidt opplysninger (uansett format, mellom hvem etc.) er egnet til å avsløre kilder.»

Andre høringsinstanser uttaler seg i samme retning.

Flere høringsinstanser kommenterer forslaget til unntak fra hovedregelen om behandlingsforbud. *Datatilsynet* mener at bestemmelsen ikke gir tilstrekkelig vern for de aktuelle yrkesgruppene, og at terskelen «strengt nødvendig» er for lav. NIM finner det positivt at departementet har sett hen til den menneskerettslige terskelen, og at det slås fast at unntaksbestemmelsen må tolkes og anvendes i lys av menneskerettslige forpliktelser. NIM stiller imidlertid spørsmål ved om terskelen kan formuleres på en måte som bedre gjenspeiler EMDs praksis, og foreslår å se hen til eventuelle endringer av kildevernbestemmelsene innen straffeprosessen. NIM mener at «vektige samfunnshensyn» i hvert fall bør kvalifiseres til «meget vektige» eller lignende, eventuelt at man benytter formuleringen «kun i ekstraordinære tilfeller og dersom det er strengt nødvendig». NIM peker også på at vurderingskriteriene bør fremgå av ordlyden, og at hvilke formål som kan være tungtveiende nok til å fravike kildevernet med fordel kan konkretiseres i bestemmelsen eller i forarbeidene. *Norsk Journalistlag, Norsk Presseforbund, Norsk Redaktørforening* og *NRK* har lignende uttalelser om terskelen i lovutkastet § 9-6.

Noen høringsinstanser kritiserer at det ikke foreslås domstolskontroll eller tilsvarende uavhengig forhåndskontroll av unntak fra behandlingsforbudet. *Datatilsynet* mener at det ikke er tillitvekkende at Etterretningstjenesten skal foreta avveiningen av de motstridende hensyn selv, og fremholder at beslutningen bør fattes av domstolen eller en annen uavhengig instans. *Dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors* er kritiske til at det er sjefen for Etterretningstjenesten som skal vurdere om tjenesten skal kunne behandle fortrolig kommunikasjon, og mener det bør vurderes om ikke dette er noe retten bør ta stilling til. *NIM* stiller spørsmål ved om de foreslåtte kontrollmekanismene for kildesensitiv informasjon er tilstrekkelige, og mener at det er en svakhet ved høringsnotatet at det ikke foretas en vurdering i lys av EMDs praksis av på hvilket nivå beslutningen om å behandle kildeopplysninger bør ligge:

«Forslaget, slik NIM forstår det, innebærer at den *uavhengige* kontrollen vil være etterfølgende (av EOS-utvalget). Kontrollen i forkant

vil være intern, av sjefen for E-tjenesten (eventuelt departementet), jf. § 9-6 andre ledd.

EMDs praksis viser imidlertid at det er den forutgående uavhengige kontrollen som er viktigst for å sikre ivaretakelse av kildevernet. Dersom eventuelle ulovlige inngrep eller feil først blir avdekket i ettertid, er de langsiktige skadene på kildevernet langt på vei allerede inntruffet, slik EMD understreker i *Sanoma Uitgevers B.V. v. Nederland*. Nederland ble da dømt for krenkelse av EMK artikkel 10 siden kildeverninngrep ble foretatt uten en forutgående kontroll og avgjørelse fra en domstol eller et annet uavhengig organ. Selv om denne dommen gjaldt straffeprosessuelle inngrep, vil begrunnelsen og de bakenforliggende hensynene som kildevernet hviler på (om blant annet å sikre tilliten til at kilders konfidensialitet generelt blir ivaretatt) gjøre seg gjeldende også på etterretningsområdet. Nylige *Big Brother Watch v. Storbritannia*, som skal behandles i EMDs storkammer og følgelig ikke har rettslig relevans som sådan, bidrar til å illustrere at kontrollmekanismer vil kunne ha betydning på etterretningsområdet. Følgelig er ikke EMDs vurderinger i Sanoma-saken enkle å forene med lovforslaget i sin nåværende form (da også i lys av mangelen på nærmere begrunnelser i høringsnotatet).»

NIM anbefaler at den forutgående kontrollen for kildevernet vurderes og begrunnes nærmere, at kontrollen som et utgangspunkt bør legges til en domstol eller lignende uavhengig organ, og at man bør vurdere en differensiert tilnærming med personell eller territoriell avgrensning. Av hensyn til helheten i kontrollmekanismene foreslår NIM at man kan se hen til virkeområdet for EOS-utvalgets kontroll.

Norsk Journalistlag mener at forslaget i høringsnotatet bryter med kravene som oppstilles i henhold til EMDs praksis, og uttaler:

«[Forslaget til § 9-6 andre ledd] er etter NJs syn et graverende brudd på kravene som oppstilles i storkammeravgjørelsen EMD Sanoma Uitgevers-saken 2010. Disse kravene gjelder selvfølgelig også for E-tjenesten, jf. igjen EMD Big Brother Watch (avsnitt 488). Det sentrale i denne avgjørelsen kan oppsummeres i fire punkter:

- Kildesensitivt materiale må gjennomgås av en dommer eller annen uavhengig og upartisk beslutningstaker, jf. avsnitt 90 første setning.
- Kontrollen skal utføres av et organ adskilt fra virksomheten som kontrolleres, jf. avsnitt 90 tredje setning.
- Den uavhengige kontrollen må finne sted senest før myndighetene får overlevert materialet, jf. avsnitt 91 andre setning.
- Kontrollen skal ha en forebyggende karakter, jf. avsnitt 92 første setning.

Etterretningssjefen selv har militær kommando over tjenesten. Forsvarsdepartementet ivaretar politisk styring og forvaltningskontroll med tjenesten. Forslaget går med andre ord ut på at de som har *direkte* kontrollen av tjenesten, skal utføre den såkalte *ekstra* rettssikkerhetsgarantien som EMD pålegger norsk lovgiver i kildevernsaker. I realiteten skal altså «Bukken passe havresekken».»

Norsk Presseforbund anser forslaget i høringsnotatet som «totalt uforenlig» med EMK artikkel 10, og gjengir *NRKs* uttalelse om at EMD ser metoder som gir myndighetene direkte tilgang til journalisters materiale som mer inngripende enn pålegg om å oppgi en kilde. Både Norsk Presseforbund og NRK mener at det i lys av EMDs praksis kreves at alle inngrep i kildemateriale må vurderes av en uavhengig og objektiv instans før Etterretningstjenesten kan få tilgang til materialet. I likhet med NIM, påpeker NRK at forslaget forutsetter at Etterretningstjenesten vet at det er tale om fortrolig kommunikasjon, og at skaden for kildevernet således har skjedd når bestemmelsen får anvendelse. NRK mener på denne bakgrunn at det må innføres særskilte mekanismer for å ivareta kildevernet, og det må lovfestes en prosess som sikrer at Etterretningstjenesten eller andre myndigheter ikke får tilgang til eller kan bruke materialet før det er godkjent av en uavhengig instans. *Norsk Redaktørforening* er av samme oppfatning.

NIM anser det som positivt at man ønsker å legge til rette for EOS-utvalgets etterfølgende kontroll, jf. forslaget om merking i lovutkastet § 9-6 tredje ledd, men understreker samtidig at slike opplysninger må oppbevares så forsvarlig og fortrolig som forholdene og menneskerettslige krav tilsier. *Norsk Journalistlag* har samme oppfatning, og mener at det må foreligge klare regler for hvordan kildesensitive opplysninger skal skilles ut fra den øvrige mengden data, samt hvordan de skal behandles. Journalistlaget uttaler videre at det i størst mulig grad må settes inn barrierer mellom de som samler inn og de som behandler data.

NIM understreker at EOS-utvalget må tilføres tilstrekkelige ressurser, personell og kompetanse til å foreta kontrollen av hvordan kildevernet prak-

tiseres. NIM mener videre at det vil være en fordel å opprette ytterligere uavhengige kontrollmekanismer, for slik å redusere faren for systemsvikt. På denne bakgrunn foreslår NIM at det opprettes en variant av «DGF-tilsynet» som foreslått i Lysne II-utvalgets rapport fra 2016, eller at det ses nærmere på mulighetene for klage- og innsynsmuligheter for enkelte bestemte aktører, eksempelvis pressen. Videre fremholder NIM at loven og praktiseringen av den bør evalueres. Etterretningstjenesten bør legge til rette for slik evaluering gjennom notoritet, sporbarhet og skriftlighet.

Flere høringsinstanser forstår forslaget om rettens prøving av begjæringer om tilrettelagt innhenting etter kapittel 8 dit hen at retten ikke skal prøve kravene til nødvendighet og forholdsmessighet dersom Etterretningstjenesten begjærer søk mot en journalist eller en annen med en vernet funksjon.

12.8.6 Departementets vurdering

Departementet opprettholder forslaget i høringsnotatet om at Etterretningstjenesten som hovedregel ikke skal behandle fortrolig kommunikasjon med særlige yrkesutøvere, for eksempel journalister og advokater. På bakgrunn av høringen foreslår departementet en rekke endringer, blant annet for å tydeliggjøre hvem som vernes av behandlingsreglene, hvilke opplysninger som omfattes, hvilken terskel som må være nådd for at unntaket skal komme til anvendelse, og hvilke krav som stilles til beslutningen.

Departementet presiserer at reglene i lovforslaget §§ 9-5 og 9-6 gjelder behandling etter innhenting. Regler om innhentingen følger av lovforslaget kapittel 3 til 8. Departementet understreker at yrkesgruppene som vernes av lovforslaget §§ 9-5 og 9-6, også vernes av forbudet etter lovforslaget § 4-1 mot å bruke innhentingsmetoder overfor personer i Norge. Det ytterligere vernet etter lovforslaget §§ 9-5 og 9-6 er begrunnet i hensynet til å motvirke risikoen for å skade de aktuelle yrkesgruppenes mulighet til å utføre sine samfunnsoppdrag. Det er for eksempel av stor betydning å hindre en nedkjølende effekt på pressens kildetilfang, da en slik effekt kan ha sterke skadevirkninger på demokratiet. På den andre siden er det klart at det ikke kan oppstilles et absolutt forbud. Forslaget tar sikte på å treffe den riktige balansen mellom de legitime interessene som gjør seg gjeldende.

En rekke høringsinstanser viser til praksis fra Høyesterett og EMD som gjelder politiets adgang til å ta beslag i fortrolig kommunikasjon. Til dette vil departementet bemerke at det er forskjeller mellom Etterretningstjenestens og politiets oppgaver og metoder som gjør at det må utvises varsomhet med å trekke slutninger fra det ene området til det andre. Etterretningstjenestens informasjonsinnhenting er utelukkende rettet mot utenlandske forhold, og har i hovedsak en sikkerhetspolitisk karakter. Tjenesten har ingen oppgaver knyttet til straffeforfølgning, og rår ikke over maktmidler som pågripelse og fengsling.

NIM tar i sin høringsuttalelse til orde for å dele opp bestemmelsene og formulere mer differensierte og konkrete terskler. Departementet er enig i dette, og foreslår å splitte opp bestemmelsen. Lovforslaget § 9-5 gjelder behandling av fortrolig kommunikasjon med særlige yrkesutøvere, mens lovforslaget § 9-6 gjelder behandling av kildeidentifiserende opplysninger. På denne måten vil det bli klarere hvilke yrkesutøvere og hvilke typer opplysninger som vernes, samt hvilke bestemmelser i Grunnloven og EMK som danner utgangspunktet for den konkrete nødvendighets- og forholdsmessighetsvurderingen som må foretas i det enkelte tilfellet. Bestemmelsene foreslås dessuten omredigert for å gjøre dem klarere og enklere å forstå.

Departementet foreslår på bakgrunn av høringen å formulere unntaksbestemmelsen på en måte som bedre gjenspeiler den høye terskelen som følger av våre menneskerettslige forpliktelser. I vurderingen av om det kan gjøres unntak fra behandlingsforbudet, må det stilles strenge krav til *nødvendighet* og *forholdsmessighet.* For det første må det vurderes om det er nødvendig å behandle de aktuelle opplysningene for å oppnå det aktuelle formålet. Kravet til *streng nødvendighet* innebærer at det må noe mer til enn at opplysningene kan bidra til å oppnå et legitimt, men vidt angitt formål. Opplysningene må være sentrale for å oppnå en konkretisert oppgave, og de må ikke kunne skaffes til veie gjennom mindre inngripende tiltak. Videre må behandlingen være *forholdsmessig*. Dette innebærer at formålet med behandlingen etter omstendighetene må vurderes som mer tungtveiende enn inngrepet i den aktuelle vernede interessen.

Unntaksbestemmelsen formuleres likt i lovforslaget §§ 9-5 og 9-6, men praktiseringen vil variere ut fra hvilken fortrolig relasjon eller hvilke opplysninger det er tale om. Utgangspunktet vil normalt enten være Grunnloven § 102 og EMK artikkel 8 (§ 9-5) eller Grunnloven § 100 og EMK artikkel 10 (§ 9-6). Der det er relevant, må det ses hen til de samfunnsmessige konsekvensene av å tillate

behandling, for eksempel risikoen for en nedkjølende effekt. For enkelte typer kommunikasjon og opplysninger vil vernet være tilnærmet absolutt. I slike tilfeller vil behandlingen normalt bare kunne vurderes som forholdsmessig dersom formålet er å avdekke eller motvirke en trussel som nevnt i lovforslaget § 3-1.

Departementet mener etter høringen at den vernede personkretsen som utgangspunkt bør ha en form for tilknytning til Norge. Norske statsborgere og personer som oppholder seg i Norge, er underlagt norsk jurisdiksjon, og som følge av det eksponert for inngrep fra norske myndigheter. Utlendinger i utlandet er som utgangspunkt ikke eksponert på denne måten. Lovforslaget §§ 9-5 og 9-6 første ledd oppstiller derfor et vilkår om tilknytning til Norge. Det kan likevel ikke utelukkes at Norge etter omstendighetene kan ha jurisdiksjon etter menneskerettighetene også overfor utlendinger i utlandet. I slike tilfeller må Etterretningstjenesten vurdere hvorvidt behandlingen av opplysningene vil være i tråd med våre menneskerettslige forpliktelser, jf. menneskerettsloven §§ 2 og 3.

Flere høringsinstanser kritiserer forslaget om å gi sjefen for Etterretningstjenesten kompetanse til å beslutte unntak fra behandlingsforbudet for opplysninger som kan identifisere en kilde, blant annet under henvisning til EMDs avgjørelse i *Sanoma Uitgevers B.V. mot Nederland* (14. september 2010). Departementet bemerker at avgjørelsen gjelder politiets beslag av journalistisk informasjon i en straffesak. Avgjørelsen kan etter departementets vurdering ikke tas til inntekt for et krav om forutgående domstolskontroll på utenlandsetterretningsområdet. En slik ordning er etter departementets syn ikke nødvendig eller hensiktsmessig, gitt den strenge formålsbegrensningen til utenlandsetterretning og de øvrige kontrollmekanismene som vil gjelde. I lys av den kritikken som er satt fram under høringen, mener departementet likevel at beslutningen om å gjøre unntak fra behandlingsforbudet for kildeidentifiserende opplysninger ikke bør ligge til sjefen for Etterretningstjenesten. Det foreslås å legge myndigheten til å gjøre unntak fra forbudet etter lovforslaget § 9-6 til departementet. Etter departementets vurdering oppfyller lovforslaget de krav som EMD oppstiller i den ikke-rettskraftige kammerdommen *Big Brother Watch mfl. mot Storbritannia* (13. september 2018), som NIM og flere presseaktører viser til. Det vises for øvrig til punkt 11.5.3.5.

Den etterfølgende kontrollen av hvordan behandlingsreglene praktiseres, vil være en sentral garanti mot misbruk. På grunn av opplysningenes karakter bør det tilrettelegges særskilt for at EOS-utvalget får informasjon om praktiseringen av bestemmelsene, slik at utvalget kan iverksette kontrolltiltak. Departementet foreslår på denne bakgrunn at alle beslutninger om unntak skal meddeles utvalget. Beslutningen skal redegjøre for det rettslige og faktiske grunnlaget for behandlingen, herunder formålet med behandlingen, hvorfor opplysningene vurderes som strengt nødvendige å behandle, og hvilke momenter som har inngått i interesseavveiningen. En slik meddelelsesplikt innebærer at utvalgets kontroll knyttet til disse bestemmelsene ligger nærmere en løpende kontroll enn den alminnelige, etterfølgende kontrollen. Prinsippet om etterfølgende kontroll, jf. EOS-kontrolloven § 2 tredje ledd andre punktum, er ikke til hinder for dette. Når det gjelder tilrettelagt innhenting, følger det av lovforslaget § 7-11 at EOS-utvalget skal føre løpende kontroll, se nærmere punkt 11.10. Departementet mener etter en samlet vurdering at kontrollordningen tilfredsstiller de menneskerettslige kravene som kan oppstilles på dette området.

Departementet understreker at søk i lagrede metadata og innhenting av innholdsdata etter lovforslaget kapittel 7 (tilrettelagt innhenting) bare kan gjennomføres etter forutgående domstolskontroll i samsvar med reglene i lovforslaget kapittel 8. Retten skal i den forbindelse prøve om søket eller innhentingen er nødvendig og forholdsmessig etter lovforslaget § 5-4, blant annet om den høye terskelen for å gripe inn i kildevernet eller andre særlig vernede opplysninger er nådd. Det vises til punkt 11.9.3.3.

Departementet har vurdert om det bør stilles ytterligere krav til sikring av opplysningene som er vernet av behandlingsforbudene. Etterretningstjenesten er etter gjeldende rett underlagt strenge krav til informasjonssikkerhet og informasjonssystemsikkerhet etter sikkerhetsloven. I tillegg gjelder prinsippet om «need to know» og tjenstlig behov. Dette innebærer at opplysningene vil oppbevares sikkert, uten at uvedkommende, herunder andre ansatte i Etterretningstjenesten, får kjennskap til dem. Departementet anser det derfor ikke som nødvendig å foreslå særlige regler om informasjonssikkerhet for vernede opplysninger.

12.9 Kravet til at personopplysningene skal være korrekte og oppdaterte

12.9.1 Gjeldende rett

Kravet til at personopplysningene skal være korrekte og oppdaterte følger av personopplysningsloven 2000 § 11 bokstav e. I Ot.prp. nr. 92 (1998–99) punkt 16 side 114 heter det om kravet:

> «*Bokstav e* krever at den behandlingsansvarlige skal rette eller slette uriktige, ufullstendige eller overflødige personopplysninger. Bestemmelsen presiserer at disse pliktene ikke bare er rettigheter som tilkommer den registrerte, jf §§ 27 og 28 i lovforslaget som det henvises til, men selvstendige plikter som påhviler den behandlingsansvarlige uavhengig av om den registrerte krever det, jf EU-direktivet art 6 nr 1 bokstav d og nr 2.»

Av personverndirektivet artikkel 6 nr. 1 bokstav d følger det at opplysningene «skal være nøyaktige og om nødvendig ajourført».

Kravet innebærer at opplysningene så langt som mulig skal være fullstendige og korrekte. Opplysninger som ikke lenger er nødvendige å behandle eller som ikke lar seg korrigere, skal slettes.

12.9.2 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 12.7 at kvalitetskravet som følger av den alminnelige personvernlovgivningen, også skal gjelde for Etterretningstjenesten. Dette innebærer at opplysningene som behandles, og som ikke er rådata i bulk, skal være korrekte og oppdaterte. Opplysninger som ikke er korrekte, skal rettes eller slettes. Det foreslås en egen hjemmel for behandling av ikke-verifiserte opplysninger, og krav om at disse må merkes særskilt.

12.9.3 Høringsinstansenes syn

Kripos mener at definisjonen av begrepet «kvalitet» i lovutkastet § 9-8 ikke er dekkende. Kvalitetskravet omfatter som hovedregel mer, herunder at opplysningene skal være tilstrekkelige og relevante for formålet med behandlingen, og ikke lagres lenger enn nødvendig ut fra formålet med behandlingen. Kripos bemerker videre at det bør fremgå av Etterretningstjenestens produkter dersom opplysninger som utleveres er ikke-verifiserte.

12.9.4 Departementets vurdering

Departementet viderefører forslaget om at personopplysningene som behandles så langt som mulig skal være korrekte og oppdaterte, men med enkelte lovtekniske justeringer.

Kripos gir i sitt høringssvar uttrykk for at begrepet «kvalitet», som inngår i overskriften i høringsnotatets forslag til § 9-8, også omfatter at opplysningene skal være tilstrekkelige og relevante for formålet og ikke lagres lenger enn nødvendig. Departementet er enig i at kvalitetsbegrepet benyttes i en bredere sammenheng i personvernlovgivningen for øvrig. I personvernforordningen er kravet til korrekte og oppdaterte opplysninger omtalt som prinsippet om «riktighet». Departementet foreslår derfor å justere overskriften på bestemmelsen, og benytte begrepene korrekte og oppdaterte opplysninger.

Kravet om korrekte og oppdaterte opplysninger må ses i sammenheng med muligheten til å behandle ikke-verifiserte opplysninger. I høringsnotatet ble det foreslått en særskilt hjemmel for behandling av denne typen opplysninger. Departementet har imidlertid vurdert det slik at ordlyden i første ledd også dekker behandling av ikke-verifiserte opplysninger, og har derfor sløyfet den særskilte hjemmelen for dette i andre ledd.

Det fremgår av lovforslaget § 9-7 første ledd at Etterretningstjenesten så langt det er mulig skal påse at personopplysningene er korrekte og oppdaterte. Tjenesten innhenter en rekke opplysninger som de i første omgang ikke vet hvorvidt er korrekte. Den videre behandlingen av disse vil nettopp ta sikte på å finne ut av om opplysningene er korrekte eller ikke. Det er ikke omtvistet at registrering av uriktige opplysninger i seg selv er et inngrep i personvernet. Likevel er muligheten til å behandle ikke-verifiserte opplysninger en forutsetning for etterretningsvirksomheten. Det er departementets syn at det må være adgang til å behandle ikke-verifiserte opplysninger dersom det er nødvendig ut fra formålet med behandlingen. Ettersom etterretningsvirksomhet dreier seg om å kartlegge korrekt faktum blant annet på bakgrunn av en vurdering av kildens troverdighet, vil det at en opplysning er ikke-verifisert måtte fremgå i beskrivelsen eller konteksten opplysningen blir brukt i.

Dersom Etterretningstjenesten kommer i besittelse av opplysninger som ikke er korrekte, skal de rettes hvis det er mulig. Dersom det ikke er mulig å rette opplysningene, vil ikke tjenesten lenger ha hjemmel for behandlingen, og de må følgelig slettes. Departementet understreker imid-

lertid at det vil kunne forekomme tilfeller hvor Etterretningstjenesten må behandle opplysninger som ikke er korrekte. Det vil for eksempel kunne dreie seg om avdekking av en påvirkningsoperasjon mot Norge i regi av en fremmed stat, hvor det fremsettes uriktige opplysninger om navngitte personer. I tjenestens behandling av opplysningene vil det av konteksten klart fremgå at opplysningen ikke er korrekte. Kravet til sletting eller retting av opplysningene vil ikke gjelde i disse tilfellene, selv om de er åpenbart feilaktige.

12.10 Kravet til sletting

12.10.1 Gjeldende rett

Kravet til sletting følger av personopplysningsloven 2000 § 11 bokstav e, jf. § 28 om forbud mot å lagre unødvendige personopplysninger. 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. § 28 første ledd andre punktum.

Det følger av § 28 andre ledd at den behandlingsansvarlige uten hinder av første ledd kan lagre personopplysninger for historiske, statistiske eller vitenskapelige formål. Den behandlingsansvarlige skal i så fall sørge for at opplysningene ikke oppbevares på måter som gjør det mulig å identifisere den registrerte lenger enn nødvendig.

Sletteplikten innebærer at Etterretningstjenesten må vurdere konkret hvorvidt personopplysningene er nødvendige for å oppnå formålet med behandlingen. Plikten til å slette må vurderes i lys av arkivloven eller annen lovgivning som medfører en plikt til videre lagring av personopplysningene.

12.10.2 Forslaget i høringsnotatet

12.10.2.1 Generelt

Det foreslås i høringsnotatet punkt 12.6.4 en bestemmelse om sletting i § 9-9, som i hovedsak viderefører gjeldende rett. Sletteplikten knyttes opp mot vurderingen av om det er nødvendig med fortsatt behandling.

Sletteplikten innebærer en plikt til å slette personopplysningene fra operative systemer og registre som er tilgjengelig for etterretningsproduksjon. Denne plikten må imidlertid ses i lys av arkivplikten, som vil medføre videre lagring av personopplysningene.

12.10.2.2 Sletting av rådata i bulk

I høringsnotatet punkt 12.6.5 foreslås det at rådata i bulk skal slettes senest 15 år fra lagringstidspunktet, med mindre vesentlige hensyn tilsier at sletting utsettes. Beslutning om utsatt sletting skal treffes av sjefen for Etterretningstjenesten, og ikke vare mer enn fem år av gangen. Rådata er data hvis etterretningsverdi ikke er vurdert, og bulk er informasjonssamlinger og datasett hvorav en vesentlig del av informasjonen antas å være irrelevant for etterretningsformål. Dette tilsier en praktisk tilnærming til spørsmålet om sletting. I høringsnotatet legges det til grunn at denne typen data etter et gitt antall år hovedsakelig vil ha historisk verdi. Det kan imidlertid være tilfeller hvor rådataene har åpenbar interesse utover 15 år, noe som taler for at det inntas en sikkerhetsventil som i unntakstilfeller gir Etterretningstjenesten mulighet til å lagre rådata utover 15-årsfristen.

12.10.3 Høringsinstansenes syn

Kripos stiller spørsmål ved begrunnelsen for en lagringstid på 15 år for rådata i bulk, ettersom slike data primært inneholder opplysninger som antas å være irrelevante for etterretningsformål. Videre påpekes at det i andre ledd bør defineres hva sletting er, ikke hva det ikke er.

Tekna oppfordrer til at lovutkastet § 9-9 strammes inn:

> «§ 9-9 tillater at «rådata i bulk» (informasjon der etterretningsverdien ikke er vurdert av mennesker) kan lagres i så mye som 15 år før de må slettes – men at sjefen for etterretningstjenesten kan treffe beslutning om å utsette slettingen i fem år om gangen. Det gjøres også unntak for sletting for «historiske, statistiske eller vitenskapelige formål». For øvrig fremstår det lite tillitvekkende at data ikke må slettes endelig, men kun slik at det kreves «avansert teknisk gjenfinningsverktøy» for å rekonstruere de slettede dataene. Hvis lovutkastet skulle vedtas, ber vi om en innstramming av denne paragrafen.»

12.10.4 Departementets vurdering

12.10.4.1 Generelt

Departementet viderefører i det vesentlige forslaget i høringsnotatet, med enkelte lovtekniske justeringer. Bestemmelsen inntas i lovforslaget § 9-8.

Tekna gir i sin høringsuttalelse uttrykk for at forslaget bør strammes inn, og departementet har på denne bakgrunn vurdert utformingen av bestemmelsen på nytt. Departementet peker i denne forbindelse på at en side av nødvendighetskravet er at personopplysninger som ikke lenger er nødvendige å behandle for etterretningsformål, skal slettes, med mindre opplysningene skal oppbevares i medhold av annen lov, for eksempel arkivloven (se punkt 12.6.4.4). Nødvendighetskravet innebærer at det som utgangspunkt må foretas en individuell og konkret vurdering av om det i hvert enkelt tilfelle er nødvendig å fortsette behandlingen av den enkelte personopplysningen. Dette prinsippet lar seg på grunn av etterretningsvirksomhetens natur ikke gjennomføre fullt ut. Fremgangsmåten dreier seg i hovedsak om å sammenstille og analysere en større informasjonsmengde for å danne seg et helhetlig bilde av situasjonen. Dette vil ofte være et møysommelig puslespill som krever oppbevaring av opplysninger over tid. Tatt i betraktning at tjenesten i enkelte sammenhenger samler inn store mengder opplysninger, herunder personopplysninger, vil det være svært krevende og lite hensiktsmessig å foreta individuelle vurderinger av hver enkelt opplysning. Det er ikke dermed sagt at tjenesten aldri trenger å gjøre individuelle vurderinger. I praksis vil det imidlertid i stor grad gjennomføres samlede vurderinger av hvorvidt større datasett, som også vil inneholde personopplysninger, skal slettes eller ikke. Departementet understreker at dersom tjenesten gjennom søk eller på annen måte blir klar over at en personopplysning som ligger lagret, ikke er nødvendig å behandle for etterretningsformål, skal opplysningen slettes etter de alminnelige reglene om sletting.

Departementet viderefører ikke forslaget i høringsnotatet § 9-9 første ledd andre punktum om sletting av fortrolig kommunikasjon, da en slik regel er overflødig ved siden av den alminnelige sletteregelen. Dette innebærer ingen realitetsendring.

Etter departementets vurdering bør det ikke oppstilles konkrete tidsfrister for sletting utover det som følger av lovforslaget § 9-8 andre ledd om rådata i bulk, da dette vil kunne medføre at tjenesten må slette opplysninger som det fortsatt er nødvendig å behandle for etterretningsformål. Å knytte sletting til en nødvendighetsvurdering er vanlig også i annen lovgivning, se for eksempel personopplysningsloven 2000 § 28, personvernforordningen artikkel 17 og helseregisterloven § 25. Dette innebærer ikke at Etterretningstjenesten kan lagre opplysningene så lenge den ønsker. Tjenesten må etablere rutiner som sørger for at det gjennomføres vurderinger av hvorvidt personopplysningene fortsatt er nødvendige å behandle for formålet. Departementet understreker at tjenesten ikke kan unnlate å vurdere nødvendighetsvilkåret ut fra bekvemmelighetshensyn.

Tekna mener videre at det fremstår lite tillitvekkende at personopplysninger ikke må slettes endelig. I høringsnotatets forslag til § 9-9 siste ledd ble det fastslått at sletteplikten skulle anses gjennomført dersom opplysningene kun kan rekonstrueres med «avansert teknisk gjenfinningsverktøy». I lys av høringsuttalelsen viderefører ikke departementet forslaget i høringsnotatet på dette punktet. Departementet understreker likevel at data vil kunne anses som slettet selv om det i teorien er mulig å rekonstruere dem. At en slik teoretisk mulighet eksisterer, betyr selvsagt ikke at det vil være tillatt å forsøke å benytte seg av den. Det sentrale ved sletting er etter departementets syn at opplysningene ikke lenger skal være tilgjengelige for Etterretningstjenesten.

Sletteplikten er ikke til hinder for at personopplysningene fortsatt kan lagres i medhold av annen lov, for eksempel for å bli brukt som ledd i historisk, statistisk eller vitenskapelig virksomhet, jf. personopplysningsloven § 8.

12.10.4.2 Sletting av rådata i bulk

Kripos stiller spørsmål ved begrunnelsen for at rådata bør kunne lagres i opptil 15 år, ettersom slike datasett inneholder data som ikke er relevante for etterretningsformål. *Tekna* tar til orde for at lagringsadgangen bør strammes inn. Departementet har i lys av høringsinnspillene vurdert hvorvidt lagringstiden på opptil 15 år er nødvendig og lar seg forsvare ut fra hensynet til personopplysningsvernet.

Det er en viktig oppgave for Etterretningstjenesten å følge med på og analysere relevante utenlandske forhold over tid. Dette forutsetter tilgang til historiske data. Det er derfor nødvendig for tjenesten å oppbevare rådata om utenlandske forhold innhentet i bulk i lang tid. I lys av dette mener departementet som utgangspunkt at fristen bør være 15 år, på samme måte som i dansk rett, se *lov om Forsvarets Efterretningstjeneste (FE)* § 6, stk. 2.

Departementet presiserer at så snart personopplysninger fra et rådatasett hentes ut og behandles med sikte på etterretningsproduksjon, må det vurderes hvorvidt det foreligger et behandlingsgrunnlag. Dersom opplysningene som hentes ut ikke er nødvendige å behandle for etterretningsformål, skal opplysningene slettes. Departementet presiserer også at ordet «senest» innebærer at Etterretningstjenesten etter omstendighetene kan være forpliktet til å slette rådata i bulk før det har gått 15 år. Man kunne sett for seg en bestemmelse som tok sikte på å differensiere ulike former for rådata i bulk, slik at tidsangivelsen for eksempel ble knyttet til innhentingsmetode eller hvilken oppgave man ved innhentingen hadde som formål å utføre. Departementet vil imidlertid ikke foreslå en slik løsning, ettersom det ikke lar seg besvare generelt når rådata i bulk mister sin etterretningsverdi.

På denne bakgrunn viderefører departementet forslaget om at rådata i bulk skal slettes senest 15 år fra lagringstidspunktet, med mulighet for forlengelse for fem år av gangen dersom sjefen for Etterretningstjenesten finner at vesentlige hensyn tilsier det.

12.11 Informasjonssikkerhet

12.11.1 Gjeldende rett

Kravet til informasjonssikkerhet følger i dag både av personopplysningsloven 2000 og sikkerhetsloven.

Det følger av personopplysningsloven 2000 § 13 at den behandlingsansvarlige og databehandleren gjennom planlagte og systematiske tiltak skal sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger. Bestemmelsen er utdypet i personopplysningsforskriften kapittel 2.

Sikkerhetsloven regulerer beskyttelse av skjermingsverdig informasjon og stiller krav om at en virksomhet som har skjermingsverdig informasjon, må ha et forsvarlig sikkerhetsnivå. Den utfylles av virksomhetsikkerhetsforskriften, som stiller krav til styringssystemet for sikkerhet, administrative krav til håndtering og beskyttelse av informasjon og særlige krav til sikkerhetsgradert informasjon. Det vises til Prop. 153 L (2016–2017) kapittel 9 og 10 for en nærmere beskrivelse.

Kravene til informasjonssikkerhet innebærer at Etterretningstjenesten må foreta en risikovurdering og vurdere egnede tiltak for å sørge for konfidensialiteten, integriteten og tilgjengeligheten til personopplysningene som behandles.

12.11.2 Forslaget i høringsnotatet

I høringsnotatet punkt 12.8 foreslås en særskilt bestemmelse i § 9-11 om krav til informasjonssikkerhet ved behandling av personopplysninger. Selv om sikkerhetslovens regler vil komme til anvendelse for Etterretningstjenestens behandling av personopplysninger, vurderes det likevel ut fra personvernhensyn som hensiktsmessig med en egen bestemmelse om informasjonssikkerhet ved behandling av personopplysninger. Det vises til at den foreslåtte informasjonssikkerhetsbestemmelsen har til formål å gi en særskilt forankring i ny etterretningstjenestelov av både sikkerhetslovens krav om informasjonssikkerhet og det grunnleggende personvernprinsippet om informasjonssikkerhet. Dette vil medføre at det stilles strenge krav til beskyttelse av personopplysningenes konfidensialitet, integritet og tilgjengelighet for Etterretningstjenesten.

12.11.3 Høringsinstansenes syn

Ingen høringsinstanser har merknader til forslaget.

12.11.4 Departementets vurdering

Departementet viderefører forslaget i høringsnotatet med enkelte lovtekniske justeringer i lovforslaget § 9-9. Det vises til merknadene til bestemmelsen for en nærmere beskrivelse.

12.12 Personvernrådgiver

12.12.1 Gjeldende rett

Personvernombudsordningen i personopplysningsloven 2000 er basert på frivillighet for den behandlingsansvarlige. Det eksisterer ingen plikt til å ha personvernombud. Oppnevning av et personvernombud medfører imidlertid at det kan gjøres unntak fra meldeplikten til Datatilsynet, jf. personopplysningsforskriften 2000 § 7-12, og unntak fra konsesjonsplikten ved behandling av personopplysninger i forbindelse med et forskningsprosjekt, jf. § 7-27.

Selv om det ikke har vært et lovfestet krav, har Etterretningstjenesten siden 2014 hatt en personvernrådgiver. Personvernrådgiveren har i oppgave å påse at tjenesten behandler personopplysninger i overensstemmelse med personvernlov-

givningen. Rådgiveren har ansvar for å utarbeide rutiner og drive opplæring om behandling av personopplysninger internt i Etterretningstjenesten.

12.12.2 Forslaget i høringsnotatet

I høringsnotatet punkt 12.11 foreslås det å lovfeste en plikt for Etterretningstjenesten til å ha én eller flere personvernrådgivere. Personvernrådgiveren skal bidra til intern legalitetskontroll, notoritet, og at behandling av personopplysninger i Etterretningstjenesten skjer i overensstemmelse med lovgivningen og folkerettslige forpliktelser.

12.12.3 Høringsinstansenes syn

Datatilsynet mener at begrepet «personvernrådgiver» bør byttes ut med «personvernombud», og at det bør lovfestes krav til ressurser på samme måte som i personvernforordningen artikkel 38 nr. 2. Tilsynet etterspør også en lovfesting av en varslingskanal til EOS-utvalget og prosedyrer for personvernrådgiveren dersom vedkommende mottar et varsel, og uttaler:

> «Slik varslingsmekanismen er utformet i forslaget, er det tvilsomt om den i tilstrekkelig grad ivaretar hensynene til varslerens rettigheter. Den innebærer også utfordringer for personvernrådgiverens uavhengighet. En sentral del av personvernombudenes oppgaver under personvernforordningen er å være kontaktpunkter for tilsynsmyndighet, noe som vil trenge en avklaring av rollen i regelverket.»

Kripos foreslår at ordlyden forenkles, samtidig som det stilles spørsmål ved om det er hensiktsmessig å begrense kretsen som kan kontakte personvernrådgiveren til kun interne i Etterretningstjenesten.

12.12.4 Departementets vurdering

Departementet viderefører forslaget i høringsnotatet med enkelte lovtekniske justeringer.

Begrepet «personvernombud» er godt innarbeidet i personopplysningsretten, og er etter personvernforordningen et lovfestet krav for alle offentlige myndigheter som behandler personopplysninger. Etterretningstjenesten er unntatt personvernforordningen når det gjelder behandling av personopplysninger for etterretningsformål, noe som kan tilsi ulik begrepsbruk. Ved å bruke et annet begrep tydeliggjør man at det er forskjell på et personvernombud etter personvernforordningen og en personvernrådgiver etter etterretningstjenesteloven. Forsvaret, som Etterretningstjenesten er en del av, har et personvernombud som ivaretar rollen i tråd med personvernforordningen. Dette ombudet vil også være ombud for Etterretningstjenestens behandling av personopplysninger etter personvernforordningen.

Datatilsynet etterspør en lovfesting av krav til ressurser, på samme måte som i personvernforordningen. Departementet vurderer at pliktene som foreslås lovfestet for personvernrådgiveren, herunder opplæring, rådgivning, veiledning og internkontroll for etterlevelse av reglene om behandling av personopplysninger, forutsetter at det må settes av ressurser til personvernrådgiveren. Det samme gjelder for andre plikter som foreslås pålagt Etterretningstjenesten. Det forutsettes at tjenesten avsetter tilstrekkelige ressurser til å oppfylle lovens plikter. Funksjonen har en mer integrert rolle i organisasjonen enn det et personvernombud etter personvernforordningen har, slik at det etter departementets syn ikke vil være naturlig å lovfeste et krav om ressurser. Det legges imidlertid til grunn at personen som utpekes som personvernrådgiver skal ha reell mulighet til å gjennomføre opplæring av ansatte og bidra med rådgivning og veiledning i konkrete saker, i tillegg til å få tilgang til nødvendig dokumentasjon i forbindelse med internkontroll.

Når det gjelder Datatilsynets innspill om lovfesting av en varslingskanal til EOS-utvalget og prosedyrer knyttet til personvernrådgiverens håndtering av varsler, er departementet av den oppfatning at dette er tilstrekkelig ivaretatt gjennom dagens ordning. Enhver kan varsle EOS-utvalget dersom man mener at Etterretningstjenesten opererer i strid med etterretningstjenesteloven. Utvalget kan, basert på en klage eller av eget tiltak, ta opp alle saker som det ut fra formålet med EOS-kontrolloven er riktig å behandle, jf. loven § 5. Av samme grunn følger ikke departementet opp forslaget fra *Kripos* om at andre enn ansatte i tjenesten skal kunne varsle personvernrådgiveren. Departementet foreslår av informasjonshensyn å henvise til klageretten til EOS-utvalget i lovforslaget § 11-7.

13 Nasjonalt og internasjonalt samarbeid og informasjonsutveksling

13.1 Innledning

Nasjonalt og internasjonalt samarbeid er viktig for å nå formålene med Etterretningstjenestens virksomhet. Samarbeid vil normalt innebære informasjonsutveksling. Internasjonalt samarbeid øker tilgangen til relevant informasjon, og styrker slik norske myndigheters evne til å treffe rettidige og korrekte beslutninger som angår rikets sikkerhet. Nasjonale samarbeidsmekanismer bidrar til at norske myndigheter arbeider koordinert og utfyller hverandre. Utlevering av informasjon som Etterretningstjenesten besitter, kan utgjøre et nytt menneskerettslig inngrep i retten til respekt for privatliv etter Grunnloven § 102 og EMK artikkel 8, og må derfor reguleres i lov. Kontrollhensyn taler også for at reglene om utlevering av informasjon kommer klart frem av loven. Det foreslås at bestemmelser som regulerer nasjonalt og internasjonalt samarbeid og informasjonsutveksling samles i et eget kapittel i loven.

13.2 Nasjonalt og internasjonalt samarbeid

13.2.1 Gjeldende rett

13.2.1.1 Nasjonalt samarbeid

Etterretningstjenesteloven regulerer ikke tjenestens samarbeid med nasjonale aktører direkte. Det er likevel ikke tvilsomt at slikt samarbeid kan etableres og opprettholdes. Samarbeidets omfang og karakter begrenses av de samarbeidende partenes rettsgrunnlag, samt av sikkerhetsmessige hensyn. For eksempel medfører territorialforbudet i etterretningstjenesteloven § 4 første ledd en viktig begrensning for Etterretningstjenesten.

Instruks 13. oktober 2006 om samarbeidet mellom Etterretningstjenesten og Politiets sikkerhetstjeneste (samarbeidsinstruksen) regulerer samarbeidet mellom nevnte tjenester på områder av felles interesse. Tjenestene skal – innenfor rammen av sine respektive rettsgrunnlag – prioritere å samarbeide om grenseoverskridende trusler som terrorisme, spredning av masseødeleggelsesvåpen og fremmed etterretningsvirksomhet. Etter omstendighetene skal tjenestene også samarbeide om andre prioriterte forhold som berører viktige nasjonale interesser. Tjenestene skal også bistå hverandre i konkrete saker, blant annet gjennom innhenting, analyse og utveksling av informasjon, samt gjennom utlån av utstyr eller annen teknisk bistand (denne formen for bistand må ikke forveksles med bistand etter politiloven § 27 a, som omtales nærmere under).

13.2.1.2 Internasjonalt samarbeid

Det fremgår av etterretningstjenesteloven § 3 andre ledd at tjenesten kan etablere og opprettholde etterretningssamarbeid med andre land. I Ot.prp. nr. 50 (1996–97) punkt 2 side 4 omtales dette som en av tjenestens hovedoppgaver. Videre har tjenesten et særlig ansvar for å ivareta samarbeidet med forsvarsallianser som Norge deltar i, se instruks om Etterretningstjenesten § 7 tredje ledd og Ot.prp. nr. 50 (1996–97) punkt 8 side 10.

På enkelte områder er Norge folkerettslig forpliktet til internasjonalt samarbeid. Blant annet har FN vedtatt en rekke kontraterrorkonvensjoner og sikkerhetsrådsresolusjoner som pålegger statene å bidra i kampen mot internasjonal terrorisme. Det samme gjelder i arbeidet mot spredning av masseødeleggelsesvåpen. Utveksling av informasjon kan inngå som del i, eller være en forutsetning for, slikt internasjonalt samarbeid.

13.2.2 Forslaget i høringsnotatet

Det understrekes i høringsnotatet punkt 13.1 at Etterretningstjenesten har behov for å samarbeide både nasjonalt og internasjonalt. Samtidig fremheves det at samarbeid kan reise rettslige problemstillinger, særlig knyttet til forholdet mellom informasjonsdeling og den enkeltes personvern og rettssikkerhet.

I høringsnotatet fremheves viktigheten av at det foreligger mekanismer for samarbeid og informasjonsdeling mellom Etterretningstjenesten og andre norske offentlige myndigheter. Det foreslås i lovutkastet § 10-1 å lovfeste at 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. Utenfor disse saksfeltene foreslås det at Etterretningstjenesten *kan* samarbeide med andre norske myndigheter, herunder gjennom informasjonsutveksling og felles operasjoner.

Det fremheves i høringsnotatet at fordelene ved internasjonalt etterretningssamarbeid er av avgjørende betydning for et lite land som Norge, som har begrensede ressurser. En sentral del av samarbeidet består av informasjonsdeling, som kan gi felles situasjonsforståelse og bidra til forbedret og mer effektiv etterretningsproduksjon. Det vises til at det på enkelte områder foreligger en folkerettslig samarbeidsplikt.

Det foreslås en bestemmelse i lovutkastet § 10-4 om at Etterretningstjenesten skal etablere og opprettholde bi- og multilateralt etterretningssamarbeid med andre land, forsvarsallianser som Norge deltar i og andre relevante internasjonale organisasjoner. Ordlyden er noe skjerpet sammenlignet med gjeldende regulering, men dette forventes ikke å innebære endringer i praksis.

13.2.3 Høringsinstansenes syn

Nasjonal sikkerhetsmyndighet (NSM) uttaler at de støtter forslagene til regulering i kapittel 10. Etter NSMs syn er det sentralt at det etableres et klart rettslig grunnlag som tilrettelegger for, og pålegger, formålsbestemt samarbeid og informasjonsdeling mellom Etterretningstjenesten og andre aktører med et ansvar for håndtering av alvorlige angrep i det digitale rom. *Politiets sikkerhetstjeneste (PST)* viser på sin side til instruks 13. oktober 2006 om samarbeidet mellom Etterretningstjenesten og Politiets sikkerhetstjeneste (samarbeidsinstruksen), som danner grunnlaget for disse tjenestenes samarbeid. Det heter i instruksen at tjenestene samarbeider innenfor rammene av sine overordnede rettsgrunnlag. PST kommenterer lovforslaget § 10-1 i lys av dette:

> «Bestemmelsen løfter reguleringen av samarbeidet mellom Etterretningstjenesten og Politiets sikkerhetstjeneste fra instruks til lovs form, uten at det er kommentert i høringsnotatet hvilke implikasjoner dette eventuelt vil ha for det praktiske samarbeidet tjenestene imellom, eller hvilken virkning bestemmelsen skal ha i relasjon til begrensninger i tjenestenes ulike lovverk.»

PST uttaler videre at bestemmelsen i § 10-1 andre ledd, i motsetning til første ledd, er utformet som en pliktregel. Etter PSTs syn bør bestemmelsens formål og tiltenkte virkning kommenteres i lovforarbeidene.

Abelia, NSM og *Næringslivets sikkerhetsråd (NSR)* peker på behovet for trusselvurderinger og annen sikkerhetsinformasjon fra Etterretningstjenesten i forbindelse med andre aktørers håndtering av digitale trusler mot norske interesser. Abelia påpeker at det i stor grad er private aktører som eier, utvikler og opererer infrastrukturen for håndtering av digitale angrep, og at det derfor er essensielt med partnerskap på dette feltet. Abelia fremhever at mange bedrifter – særlig små og mellomstore – faller utenfor eksisterende ordninger for varsling og håndtering av IKT-hendelser. NSR viser til Abelias høringssvar om samarbeid mellom offentlig og privat sektor, og mener at norsk næringsliv har behov for tidlig varsling om potensielle alvorlige angrep både i Norge og i utlandet. NSR forutsetter at myndighetene legger til rette for en bedre informasjonsdeling mellom myndigheter og relevant næringsliv. *Datatilsynet* savner en nærmere redegjørelse av hvem det er aktuelt å utlevere til, og etterspør konkrete eksempler. Særlig gjelder dette hvem som er «andre offentlige myndigheter.»

Amnesty International mener at det er for lite fokus på Etterretningstjenestens samarbeid med andre lands tjenester. Det fremheves at etterretningsinformasjon er en handelsvare, at Norge i liten grad effektivt kan kontrollere hvordan andre land bruker informasjonen som deles med dem, og at det på grunn av hemmelighold er umulig å vite i hvilken grad norsk etterretningsinformasjon bidrar til alliertes folkerettsbrudd. *Piratpartiet* mener at reglene om deling av informasjon gjennom internasjonalt samarbeid ikke er tilfredsstillende.

13.2.4 Departementets vurdering

Departementet viderefører forslaget i høringsnotatet, men med enkelte endringer som følge av høringen. Departementet foreslår å forenkle og slå sammen bestemmelsene om nasjonalt og internasjonalt samarbeid. Bestemmelsen inntas i lovforslaget § 10-1.

I lys av høringsuttalelsen til *PST*, vil departementet bemerke at forslaget ikke innebærer noen endringer i det etablerte samarbeidet mellom Etterretningstjenesten og PST. Det foreslås ingen endringer i samarbeidsinstruksen. Departementet mener likevel at det er hensiktsmessig å lovfeste Etterretningstjenestens plikt til å samarbeide med nasjonale myndigheter innenfor prioriterte saksfelt, på samme måte som man lovfester en plikt for tjenesten til å etablere og opprettholde internasjonalt etterretningssamarbeid. Slik deltakelse i internasjonalt samarbeid er en videreføring av gjeldende praksis, selv om det nå foreslås oppstilt som en «skal»-regel og ikke en «kan»-regel.

Enkelte høringsinstanser peker på at reglene må legge til rette for samarbeid og rettidig informasjonsdeling med nasjonale private aktører. Departementet er enig i at det er viktig med et godt offentlig-privat samarbeid for å verne nasjonale interesser, men foreslår ingen endringer i de samarbeidsstrukturene som allerede eksisterer. Når det gjelder Etterretningstjenestens evne til å avdekke trusler mot norske interesser, vil denne styrkes med tilrettelagt innhenting. Informasjon fra tilrettelagt innhenting som er relevant for den nasjonale trusselhåndteringen i det digitale rom, vil for eksempel tilflyte NSM gjennom Felles cyberkoordineringssenter, og vil dermed komme private aktører til gode gjennom NSMs eksisterende varslingsmekanismer. Det vises også til reglene om varsling og rapportering i lovforslaget § 2-4. Departementet vil dessuten vise til at NSM er tillagt et særskilt ansvar etter sikkerhetsloven § 2-3 for å legge til rette for at virksomheter som er omfattet av loven, får tilgang til informasjon om trusselvurderinger og andre opplysninger av relevans for virksomhetenes sikkerhetsarbeid. NSM skal også, i samråd med sektormyndigheter og andre relevante myndigheter, sikre at det etableres nødvendige fora for informasjons- og erfaringsutveksling. Etterretningstjenesten vil være en naturlig bidragsyter i denne sammenheng. Departementet er derfor av den oppfatning at de foreslåtte bestemmelsene, sammenholdt med annen relevant lovgivning, legger til rette for et hensiktsmessig sikkerhetssamarbeid mellom offentlig og privat sektor.

Amnesty International uttrykker i sin høringsuttalelse bekymring for at Norge i internasjonalt etterretningssamarbeid mister kontrollen over hvordan informasjon håndteres av mottaker etter at den er delt. Departementet vil bemerke at selv om man aldri kan garantere for hvordan utlevert informasjon blir håndtert av andre aktører, så utleveres informasjon i henhold til prinsipper som skal sikre forsvarlig håndtering. Disse vilkårene for utlevering omtales nærmere under punkt 13.3.

13.3 Utlevering av informasjon som ledd i nasjonalt og internasjonalt samarbeid

13.3.1 Gjeldende rett

Utlevering av informasjon reguleres ikke uttrykkelig av etterretningstjenesteloven, men det er ikke tvilsomt at Etterretningstjenesten kan utlevere informasjon som ledd i nasjonalt og internasjonalt samarbeid. Utlevering av personopplysninger reguleres av personopplysningsloven 2000 § 8.

Særregler om utlevering av informasjon til utenlandske samarbeidspartnere er gitt i instruks om Etterretningstjenesten § 4. Det kreves at utlevering er i norsk interesse og underlagt nasjonal kontroll, jf. § 4 første ledd andre punktum. Kontrollen sikres blant annet ved at Forsvarsdepartementet skal forelegges saker om etablering av samarbeid og avtaler med utenlandske tjenester og internasjonale organisasjoner, jf. instruksen § 13 bokstav a. Etterretningstjenesten kan innhente informasjon om forhold som er av betydning for samarbeidende lands tjenester, selv om forholdene ikke er direkte relatert til Norges selvstendighet, sikkerhet eller viktige nasjonale interesser, se Ot.prp. nr. 50 (1996–97) punkt 12 side 15.

Videre følger en rekke særvilkår for utlevering av personopplysninger om norske personer til utenlandske tjenester av Forsvarsdepartementets utfyllende bestemmelser av 24. juni 2013 for Etterretningstjenestens innsamling mot norske personer i utlandet samt for utlevering av personopplysninger til utenlandske samarbeidende tjenester. Blant annet må det knyttes forbehold til utleveringen om at opplysningene ikke kan benyttes som grunnlag for overvåkning eller annen fordekt innsamling rettet mot personer som oppholder seg på norsk territorium, jf. § 4 nr. 5. Videre kreves at utleveringen må vurderes som forsvarlig i lys av opplysningenes kvalitet, hvem som er omhandlet, hvem som er mottaker og antatt handlemåte fra mottaker, jf. § 4 nr. 6.

I instruks 26. november 2012 er det gitt regler om etterretningssamarbeid med stater hvor det foreligger risiko for tortur eller annen grusom, umenneskelig eller nedverdigende behandling

eller straff. Formålet med instruksen er å søke å redusere risikoen for at Etterretningstjenestens personell, i forbindelse med internasjonalt samarbeid, direkte eller indirekte medvirker til grove menneskerettighetsbrudd i de aktuelle samarbeidslandene. Det skal blant annet foretas aktsomhetsvurderinger knyttet til et mulig samarbeidslands menneskerettighets- og fengslingspraksis, og risikovurderinger knyttet til konkrete samarbeidsoperasjoner eller -tiltak. Videre skal det foretas en risikoanalyse forut for utlevering av informasjon om enkeltpersoner, og etter omstendighetene avtales risikoreduserende tiltak med vedkommende samarbeidende tjeneste.

13.3.2 Forslaget i høringsnotatet

I høringsnotatet redegjøres det for gjeldende bestemmelser og prinsipper for utlevering av informasjon. Det vises til at gjeldende rett balanserer behovet for effektivt samarbeid med personvern- og menneskerettslige hensyn på en god måte. Det anbefales at hovedtrekkene videreføres, men at utleveringsadgangen bør fremgå tydeligere. En slik lovfesting vurderes også å legge godt til rette for EOS-utvalgets kontroll.

Det foreslås en bestemmelse i lovforslaget § 10-5 med et sett av kumulative vilkår for utlevering av informasjon til nasjonale så vel som internasjonale aktører. Dessuten foreslås det en egen bestemmelse med tilleggsvilkår for utlevering til internasjonale aktører i lovutkastet § 10-6.

De kumulative vilkårene i § 10-5 krever for det første at utleveringen enten skjer for etterretningsformål, for å fremme mottakerens oppgaver eller for å hindre at virksomhet utøves på en uforsvarlig måte. Videre kreves det at Etterretningstjenesten ikke kan utlevere opplysninger den har mottatt fra en tredjepart uten dennes samtykke. For det tredje foreslås det at utlevering av personopplysninger bare kan skje dersom Etterretningstjenesten selv kan behandle opplysningene etter reglene i kapittel 9. Dersom behandlingsvilkåret er oppfylt, må Etterretningstjenesten i tillegg vurdere om utleveringen er forholdsmessig etter § 5-4. Videre må utleveringen vurderes som forsvarlig i lys av opplysningenes kvalitet, hvem som er mottaker av opplysningene og hvordan mottakeren antas å bruke dem. I dette kravet ligger at tjenesten ikke kan dele opplysninger uten henblikk på hvordan mottakeren behandler eller antas å behandle opplysningene og dem som opplysningene omhandler. Det foreslås også et krav om at tjenesten må kunne forvente at mottakeren behandler opplysningene på en forsvarlig sikkerhetsmessig måte. Av hensyn til kontroll og etterprøvbarhet foreslås det et krav om at utleveringen dokumenteres. Av pedagogiske hensyn foreslås det presisert at utlevering med sikte på innhenting eller andre tiltak hos mottaker på vegne av og i Etterretningstjenestens interesse, bare kan skje dersom tjenesten selv kunne gjennomført innhentingen eller tiltaket på lovlig måte. Det presiseres også at de nevnte vilkårene ikke skal gjelde for utlevering av informasjon til EOS-utvalget eller andre tilsyns- eller kontrollinstanser.

For utlevering av informasjon til internasjonale samarbeidspartnere foreslås det ytterligere vilkår for utlevering i § 10-6. Vilkårene er en kodifisering av gjeldende rett og praksis. For det første kreves at utleveringen er under nasjonal kontroll og i norsk interesse. Videre pålegges Etterretningstjenesten å oppstille som vilkår for deling at opplysningene ikke kan benyttes som grunnlag for innhenting av opplysninger om personer som oppholder seg på norsk territorium, med mindre det er tale om personer som opptrer på vegne av fremmed makt etter § 4-2 første ledd og som det er i norsk interesse at mottakeren gjennomfører innhenting mot. For det tredje må utleveringen skje i overensstemmelse med særskilte prosessuelle og materielle bestemmelser som skal sikre overholdelse av forbudet i lovforslaget § 1-3 andre ledd, som forbyr medvirkning til virksomhet som innebærer en reell risiko for at ufravikelige og andre grunnleggende menneskerettigheter krenkes.

13.3.3 Høringsinstansenes syn

Høringsinstansene er i hovedsak positive til at vilkårene for utlevering av informasjon foreslås lovfestet, men enkelte har kommentarer til utformingen av reglene.

Kripos foreslår at det ses hen til politiregisterforskriften § 11-4 ved utarbeidelsen av de generelle vilkårene for utlevering. *Politiets sikkerhetstjeneste (PST)* understreker at et godt samarbeid mellom tjenestene forutsetter korrelasjon mellom tjenestenes lovgrunnlag, slik at begge tjenestene like enkelt kan utlevere informasjon til og motta informasjon fra hverandre. PST understreker at uklarheter i loven og rom for skjønnsmessige vurderinger kan forsinke utveksling av informasjon.

Amnesty International anser det som urealistisk at Norge skal kunne utøve effektiv kontroll av andre lands bruk av delt informasjon, herunder hvilke tredjeparter som mottar informasjonen. *Datatilsynet* påpeker at det er viktig med klare

regler for å unngå en omgåelse ved at stater overvåker hverandres innbyggere for så å bytte informasjonen. Tilsynet mener at loven bør liste opp en rekke vurderinger som må foretas ved inngåelse av samarbeidsavtaler, herunder hvorvidt tjenesten er en del av en demokratisk rettsstat, etterlevelsen av menneskerettigheter i det landet det skal samarbeides med, tjenestens profesjonalitet og pålitelighet, og lovpålagte oppgaver og kompetanse, inkludert kontrollmekanismer og måten personopplysninger behandles og beskyttes på.

Norges institusjon for menneskerettigheter (NIM) viser til lovutkastet § 10-6 bokstav c om at utlevering skal skje i overensstemmelse med særskilte bestemmelser som skal sikre overholdelse av forbudet i lovutkastet § 1-3 andre ledd. NIM uttaler at utkastet til § 1-3 er dels en henvisning til jus cogens (ufravikelig folkerett) og torturforbudet, og dels en henvisning til andre former for folkerettsbrudd. NIM påpeker at mens det første alternativet er svært snevert, er det andre vagt, og at rekkevidden av disse reglene er usikker.

13.3.4 Departementets vurdering

Departementet opprettholder forslaget i høringsnotatet om å lovfeste adgangen til å utlevere informasjon som ledd i nasjonalt og internasjonalt samarbeid. Departementet foreslår i hovedsak å videreføre bestemmelsene slik de er utformet i høringsnotatet, men med enkelte lovtekniske justeringer.

Departementet har vurdert innspillene fra høringen, men finner ikke grunn til å foreslå endringer i hovedregelen som oppstiller vilkår for utlevering av etterretningsinformasjon som følge av dette. Etter en omstrukturering av kapittelet foreslås hovedregelen inntatt i § 10-2. Bestemmelsen ivaretar etter departementets oppfatning behovet for klare regler som legger til rette for forsvarlige og effektive prosedyrer i forbindelse med utlevering av informasjon.

Bestemmelsene er utformet innenfor rammen av menneskerettslige og personvernmessige krav. I denne sammenhengen peker departementet på vilkårene om at Etterretningstjenesten selv må kunne behandle opplysningene, at utleveringen må vurderes som forholdsmessig, og at Etterretningstjenesten må vurdere hvem som er mottaker av opplysningene og hvordan vedkommende forventes å behandle dem. Utlevering som ledd i internasjonalt samarbeid skal ikke skje dersom det foreligger reell risiko for at noen utsettes for tortur eller annen umenneskelig eller nedverdigende behandling eller straff. Denne regelen inntas i lovforslaget § 10-3 som følge av at forslaget i høringsnotatet til § 1-3 ikke videreføres.

Departementet vurderer at lovforslaget i tilstrekkelig grad tar høyde for og reduserer faren for omgåelse i form av at samarbeidende stater innhenter og bytter opplysninger om hverandres innbyggere. Det understrekes at slik virksomhet vil være en ulovlig omgåelse av lovforslaget § 4-1.

13.4 Utlevering av overskuddsinformasjon

13.4.1 Gjeldende rett

Overskuddsinformasjon er informasjon som er uten interesse for ivaretakelsen av Etterretningstjenestens oppgaver, men som tjenesten likevel kommer i besittelse av som følge av etterretningsvirksomhet. Etterretningstjenesteloven inneholder ingen bestemmelser om utlevering av overskuddsinformasjon. Slik utlevering er imidlertid omtalt i lovens forarbeider (Ot.prp. nr. 50 (1996–97) punkt 9 side 11):

> «[Etterretningstjenesteloven § 4 første ledd] gjelder *innhenting* av informasjon om norske borgere og norske juridiske personer. Dersom Etterretningstjenesten som ledd i utførelsen av oppgavene passivt mottar overskuddsinformasjon av overvåkingsmessig eller annen interesse, vil det ikke være noe til hinder for at slik informasjon overbringes rette myndigheter. Det vil f.eks. være helt i orden å melde mulige straffbare forhold til politiet.»

Av instruks om Etterretningstjenesten § 5 første ledd følger det at dersom tjenesten som ledd i løsningen av sine oppgaver mottar overskuddsinformasjon av overvåkingsmessig eller annen interesse, og som ikke kan oppbevares av tjenesten etter loven § 4 andre ledd, kan slik informasjon overbringes rette norske offentlige myndighet i overensstemmelse med reglene om rapportering i instruksen kapittel 4.

Utlevering av overskuddsinformasjon er også regulert i instruks 13. oktober 2006 om samarbeidet mellom Etterretningstjenesten og Politiets sikkerhetstjeneste (samarbeidsinstruksen) § 10 første ledd andre punktum, jf. første punktum. Det fremgår der at tjenestene, innenfor rammen av «need to know»-prinsippet og hensynet til å beskytte sensitive kilder og metoder, så langt mulig skal utveksle overskuddsinformasjon som den ene tjenesten besitter og som åpenbart er av interesse for den andre tjenesten. Med over-

skuddsinformasjon menes informasjon om forhold som ligger utenfor vedkommende tjenestes ansvarsområde, men som tjenesten likevel kommer i besittelse av som følge av dens virksomhet rettet mot forhold innenfor ansvarsområdet, jf. instruksen § 10 første ledd tredje punktum.

13.4.2 Forslaget i høringsnotatet

I høringsnotatet foreslås det å lovfeste adgangen til å utlevere overskuddsinformasjon. Det foreslås at overskuddsinformasjon bare skal kunne utleveres når vilkårene for utlevering etter § 10-5 er oppfylt, se punkt 13.3 over, med unntak av kravet om at utlevering av personopplysninger bare skal kunne skje dersom Etterretningstjenesten selv kan behandle opplysningene etter lovutkastet kapittel 9. Det foreslås at overskuddsinformasjon bare kan utleveres til andre norske offentlige myndigheter, og ikke til andre aktører.

Det foreslås to unntak fra hovedregelen om utlevering. For det første foreslås det at overskuddsinformasjon som Etterretningstjenesten kommer i besittelse av gjennom tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon, ikke skal kunne deles, med mindre informasjonen gjelder et forhold som faller inn under straffeloven kapittel 17 og 18 og som kan avverges. Videre foreslås det et delingsforbud knyttet til overskuddsinformasjon som er fortrolig kommunikasjon etter lovutkastet § 9-6.

13.4.3 Høringsinstansenes syn

Ingen høringsinstanser har kommentert forslaget om å lovfeste adgangen til å utlevere overskuddsinformasjon. En rekke høringsinstanser har imidlertid merknader til forslaget i lovutkastet § 7-12 om et forbud mot deling av overskuddsinformasjon fra tilrettelagt innhenting. Dette forslaget behandles i punkt 11.12.

Enkelte høringsinstanser har kommentert forslaget om å forby utlevering av overskuddsinformasjon som er fortrolig kommunikasjon. *Norges institusjon for menneskerettigheter (NIM)* understreker at det er positivt med et forbud mot å dele kildesensitiv informasjon, og at dette er et tiltak som kan forebygge en nedkjølende effekt. Samtidig mener NIM at delingsreglene i lovforslaget § 10-5 er vide og vage, og at dette gjør det vanskelig å overskue hvilken *de facto* mulighet som eksisterer for deling av kildeinformasjon. NIM anbefaler at man oppstiller så tydelige og snevre vilkår som mulig for deling av kildeinformasjon. NIM stiller også spørsmål ved hvor beslutning om deling av slik informasjon bør ligge, herunder om den kan, og bør, ligge til et uavhengig organ, slik som en domstol.

Norsk Journalistlag mener at delingsforbudet ikke er tilstrekkelig i lys av Norges internasjonale forpliktelser på området, og at kildesensitivt materiale som ikke er overskuddsinformasjon heller ikke kan utleveres til andre myndigheter uten forhåndsgodkjenning av en uavhengig kontrollinstans. *Norsk rikskringkasting (NRK)* uttaler seg kritisk til at det ikke er lagt opp til rettssikkerhets- eller kontrollmekanismer i form av domstolskontroll eller andre tiltak for å sikre ivaretakelse av kildevernet eller forhindre misbruk ved nasjonal eller internasjonal informasjonsdeling, og at man bør innføre særskilte mekanismer for å ivareta kildevernet. NRK anfører at problemstillingen knyttet til kildevernet forsterkes av den vide angivelsen av hva som er etterretningsformål.

13.4.4 Departementets vurdering

Departementet opprettholder forslaget i høringsnotatet om å lovfeste adgangen til å utlevere overskuddsinformasjon til andre norske myndigheter. Dette er en videreføring av gjeldende rett. Utlevering innebærer behandling av personopplysninger og krever behandlingsgrunnlag. Departementet understreker i den sammenheng at utlevering av overskuddsinformasjon vil skje for andre formål enn etterretningsformål, noe som medfører at personopplysningloven 2018 og personvernforordningen kommer til anvendelse.

Lovforslaget § 7-13 oppstiller forbud mot utlevering av overskuddsinformasjon som stammer fra tilrettelagt innhenting etter lovforslaget kapittel 7. Regelen utgjør en viktig begrensning av hovedregelen etter § 10-4 første ledd. Av pedagogiske hensyn inntas en henvisning til lovforslaget § 7-13 i § 10-4 andre ledd. Den nærmere utformingen av forbudet i § 7-13 drøftes i punkt 11.12.

Departementet vurderer at det foreslåtte forbudet i tredje ledd bidrar til å oppfylle Norges internasjonale forpliktelser. Det vises til punkt 12.8. I tråd med de strukturelle endringene som etter høringen er gjort i lovforslaget kapittel 9, er henvisningen oppdatert til å gjelde både bestemmelsen som gjelder fortrolig kommunikasjon i § 9-5 og til kildeidentifiserende materiale i § 9-6.

Enkelte høringsinstanser, herunder *NIM, Norsk Journalistlag* og *NRK*, oppfatter adgangen til å utlevere kildeidentifiserende materiale som vid og uklar. Departementet deler ikke dette synet. For det første foreslås det i § 10-4 tredje ledd et forbud mot utlevering av overskuddsinformasjon

som er kildeinformasjon etter lovforslaget § 9-6. Det betyr at informasjonen må være etterretningsrelevant etter lovforslaget kapittel 3 for å kunne utleveres. At informasjonen er etterretningsrelevant, er imidlertid ikke tilstrekkelig. Utleveringsreglene etter § 10-2 må også være oppfylt. Lovforslaget § 10-2 første ledd bokstav c oppstiller som vilkår for utlevering at tjenesten selv kan behandle informasjonen etter lovforslaget kapittel 9. Lovforslaget § 9-6 andre ledd oppstiller en meget høy terskel for at Etterretningstjenesten kan behandle kildeidentifiserende informasjon. I tillegg krever lovutkastet § 10-2 første ledd bokstav d at utleveringen er forholdsmessig etter lovforslaget § 5-4. Også dette må bero på en selvstendig vurdering. Jo større inngrep utlevering av informasjon vil innebære, jo mer skal til for at utleveringen er forholdsmessig. Departementet legger til grunn at det skal svært mye til for at det skal kunne anses forholdsmessig å utlevere kildeidentifiserende materiale til andre norske myndigheter, og vurderer adgangen som en snever sikkerhetsventil. I sum mener departementet at adgangen til å utlevere kildeidentifiserende materiale er svært begrenset, og at dette fremgår klart av loven. Det tilføyes at de samme vurderinger vil måtte gjøres for fortrolig kommunikasjon etter lovforslaget § 9-5.

Departementet finner det ikke naturlig å foreslå at en domstol skal ta stilling til om informasjon kan deles mellom norske myndigheter, slik enkelte høringsinstanser har reist spørsmål om. EOS-tjenestenes utlevering av informasjon er en sentral del av EOS-utvalgets kontrolloppgave.

13.5 Utlevering av informasjon fra andre offentlige myndigheter til Etterretningstjenesten

13.5.1 Gjeldende rett

Etterretningstjenesten kan etter gjeldende rett motta og behandle etterretningsrelevant informasjon som andre aktører deler med tjenesten, men tilgangen til slik informasjon kan i mange tilfeller hindres av lovbestemt taushetsplikt. I tillegg er norske myndigheter som hovedregel underlagt personvernforordningens virkeområde, slik at det gjelder særlige krav til behandlingsgrunnlaget for personopplysninger som er innsamlet for de aktuelle myndighetenes respektive formål.

Hovedregelen om taushetsplikt i forvaltningsloven § 13 første ledd slår fast at enhver som utfører tjeneste eller arbeid for et forvaltningsorgan, plikter å hindre at andre får adgang eller kjennskap til det han i forbindelse med tjenesten eller arbeidet får vite om noens personlige forhold. Taushetspliktens rekkevidde begrenses i forvaltningsloven §§ 13 a og 13 b. Blant annet er ikke taushetsplikt til hinder for at et forvaltningsorgan gir andre forvaltningsorganer opplysninger som det er nødvendig å gi for å fremme *avgiverorganets* oppgaver etter lov, instruks eller oppnevningsgrunnlag, jf. § 13 b første ledd nr. 5. Det gjelder videre en rekke andre delingsmuligheter etter § 13 b, men det finnes ikke et renskåret unntak fra taushetsplikten for å dele opplysninger som det er nødvendig å gi for å fremme *mottakerorganets* oppgaveløsning.

Særlovgivningen inneholder også en rekke bestemmelser om taushetsplikt.

13.5.2 Forslag i høringsnotatet

Det redegjøres i høringsnotatet punkt 13.4 for situasjoner der lovbestemt taushetsplikt utgjør en skranke for utlevering av etterretningsrelevant informasjon til Etterretningstjenesten. Det vises til at taushetspliktbestemmelser medfører at tjenesten ikke mottar viktig informasjon av betydning for rikets sikkerhet. Det vises også til at behovet for informasjonsdeling i enkelte saker har vært så påtrengende at utlevering likevel har skjedd, selv om taushetspliktreglene har voldt betydelig tvil.

Det foreslås i høringsnotatet en bestemmelse i lovutkastet § 10-2 om at lovbestemt taushetsplikt ikke er til hinder for at offentlige myndigheter utleverer informasjon til Etterretningstjenesten dersom det innenfor rammen av Etterretningstjenestens oppgaver etter kapittel 3 er nødvendig for forebyggelses- og sikkerhetsformål.

Forslaget oppstiller ingen plikt til å dele opplysninger, kun en rett. Vurderingen må foretas av virksomheten, ikke den enkelte saksbehandler. Det må foretas en konkret vurdering av inngrepets karakter og om utlevering er nødvendig og forholdsmessig, herunder omfanget og arten av de relevante opplysningene sett i forhold til de hensyn som begrunner taushetsplikten og hensynet til den opplysningene gjelder.

13.5.3 Høringsinstansenes syn

Datatilsynet mener at tilnærmingen til spørsmålet om andre offentlige myndigheter skal kunne utlevere taushetsbelagt informasjon til Etterretningstjenesten, er for passiv, og uttaler:

> «Datatilsynet støtter ikke dette forslaget. Vi mener regler om opphevelse av taushetsplikt i størst mulig grad bør fremgå av lovgivningen som regulerer den aktuelle offentlige myndigheten. Dette for å skape forutberegnelighet og klarhet. Det bør gjøres konkrete avveininger knyttet til de konkrete myndighetenes taushetsplikt og ikke i form av en generell opphevelse av taushetsplikt slik det er foreslått.
>
> Vår erfaring er at offentlige etater enkelte ganger tror opphevelse av taushetsplikt er det samme som behandlingsgrunnlag for utlevering av opplysninger etter personopplysningsregelverket. Vi frykter derfor at den foreslåtte bestemmelse vil kunne bli oppfattet som en generell bestemmelse om rettslig grunnlag for utlevering, uten at det foretas en nærmere vurdering i det enkelte tilfelle.»

Dersom forslaget fastholdes, mener Datatilsynet at det bør inntas en henvisning til lovutkastet § 9-6 om særskilte yrkesutøvere.

Kripos bemerker at en utlevering av opplysninger fra en behandlingsansvarlig etter personopplysningsloven må oppfylle kravene i personvernforordningen artikkel 6, og eventuelt også artikkel 9 ved utlevering av særlige kategorier personopplysninger.

Riksadvokaten uttaler:

> «En lov som gjelder Etterretningstjenesten og for personell og enheter som er under kommando eller instruksjon av sjef Etterretningstjenesten, jf. utkastet § 1-2 første og annet ledd, kan ikke ha en bestemmelse som generelt opphever lovpålagt taushetsplikt for andre virksomheter, eller for personell tilknyttet disse. Slik sett vil utkastet § 10-2 mer være veiledende ved skjønnsutøvelsen om betydningen av Etterretningstjenestens sentrale rolle i stats- og samfunnssikkerhetsarbeidet når det skal vurderes om reglene om egen taushetsplikt åpner for formidling av informasjon til tjenesten.»

På denne bakgrunn stiller riksadvokaten seg spørrende til behovet for bestemmelsen.

13.5.4 Forvaltningslovutvalgets utredning

Forvaltningslovutvalget avga 14. mars 2019 sin utredning om ny forvaltningslov (NOU 2019: 5). Utvalget hadde i oppgave å revidere forvaltningsloven, og legge fram forslag til lovverk som legger bedre til rette for en god og effektiv saksbehandling tilpasset vår tids forvaltningsoppgaver.

Utvalget vurderer i punkt 19.12.6 spørsmålet om ny forvaltningslov bør legge til rette for deling av taushetsbelagte opplysninger i tilfeller hvor deling er i *mottakerorganets* interesse. Det påpekes at reglene om deling av taushetsbelagte opplysninger oppfattes som vanskelig tilgjengelige, og at dette, sammenholdt med straffansvaret for brudd på taushetsplikten, utgjør et hinder for å dele opplysninger. Utvalget anser dette som uheldig gitt tendensene til spesialisering og rendyrking av funksjoner i forvaltningen, som gjør informasjonsutveksling i forvaltningen viktigere nå enn før. Utvalget vektlegger videre at de gjeldende reglene om taushetsplikt kan vanskeliggjøre en hensiktsmessig organisering av forvaltningsapparatet, og at en vid adgang til å dele taushetsbelagte opplysninger vil kunne bidra til at forvaltningen får et bedre avgjørelsesgrunnlag enn den ellers ville ha fått. Det foreslås blant annet på denne bakgrunn at det som hovedregel bør være adgang til å dele taushetsbelagte opplysninger med andre forvaltningsorganer som har «saklig behov» for dem i sin virksomhet. Om dette vilkåret uttaler utvalget følgende:

> «Et slikt krav – som svarer til vilkåret for deling i avgiverorganets interesse – vil innebære at det er adgang til å dele opplysninger som har saklig sammenheng med den avgjørelse som skal treffes, eller det tiltak som skal gjennomføres. Det vil bety en viss utvidelse av delingsadgangen sammenliknet med i dag. Selv om loven åpner for deling i mange situasjoner, gir den ingen alminnelig adgang til å dele taushetsbelagte opplysninger med andre organer som har behov for dem. En slik endring vil bidra til at forvaltningen oftere får et korrekt avgjørelsesgrunnlag, og det vil kunne lede til effektivisering av saksbehandlingen, især innenfor masseforvaltningen. I tillegg vil endringen åpne for større grad av automatisert saksbehandling.»

Utvalget omtaler også de hensyn som taler mot en vid delingsadgang:

> «En adgang til å dele taushetsbelagte opplysninger utgjør et innhugg i behovet for konfidensialitet og kan på sikt lede til at andre parter og andre blir mer tilbakeholdne med å gi fra seg opplysninger. En vid adgang til deling kan dessuten i noen tilfeller være vanskelig å forene med de hensyn som annen lovgivning byg-

ger på. Dette kan være tilfelle der vedkommende organ er avskåret fra å innhente opplysningene, eller iallfall ikke har fått hjemmel til å gjøre det selv. Endelig kan også hensynet til et korrekt avgjørelsesgrunnlag i noen tilfeller tale mot deling. Det er ikke gitt at en opplysning som er innhentet ved en tidligere anledning, og kanskje i en helt annen sammenheng, fremdeles er dekkende.»

Utvalget vurderer ikke at mothensynene gir tilstrekkelig grunn til å holde fast ved dagens ordning.

13.5.5 Departementets vurdering

Departementet har på bakgrunn av forslaget til Forvaltningslovutvalget vurdert hvorvidt det er nødvendig å videreføre forslaget i høringsnotatet. Departementet har kommet til at forslaget i høringsnotatet bør videreføres. Bestemmelser om taushetsplikt i særlovgivningen utgjør et hinder for deling av etterretningsrelevant informasjon, og det er behov for å bygge ned hindrene som vanskeliggjør det samlede offentlige arbeidet med å forebygge, avdekke og motvirke utenlandske trusler mot Norge.

Bestemmelsens formål er dels å tydeliggjøre at informasjon kan utleveres til Etterretningstjenesten uten hinder av lovbestemt taushetsplikt, og dels å danne grunnlag for at norske myndigheter kan utlevere informasjon til Etterretningstjenesten på en måte som oppfyller kravene i den alminnelige personvernlovgivningen. Bestemmelsen utgjør følgelig et supplerende rettsgrunnlag etter personvernforordningen artikkel 6 nr. 3, grunnlag for viderebehandling i samsvar med forordningen artikkel 6 nr. 4, samt grunnlag for å utlevere særlige kategorier personopplysninger etter forordningen artikkel 9 nr. 2 bokstav g.

Departementet er enig med *riksadvokaten* i at bestemmelsen ikke opphever lovpålagt taushetsplikt for andre virksomheter eller for personell tilknyttet disse. Det er den enkelte utleverende myndighet som må vurdere konkret i det enkelte tilfellet om bestemmelsen gir tilstrekkelig grunnlag for den enkelte utleveringen. Den utleverende myndigheten vil måtte ta utgangspunkt i kravene i personvernforordningen ved vurderingen av om utlevering kan finne sted.

I lys av det ovennevnte opprettholder departementet forslaget i høringsnotatet om å lovfeste at lovbestemt taushetsplikt ikke er til hinder for at offentlige myndigheter utleverer informasjon til Etterretningstjenesten. En slik utvidet utleveringsadgang bør begrenses til informasjon som Etterretningstjenesten trenger for forebyggelses- og sikkerhetsmessige formål. Videre mener departementet at en utvidet utleveringsadgang bør avgrenses mot profesjonsbasert taushetsplikt. De yrkesgrupper som omfattes av en slik taushetsplikt, fremgår av straffeprosessloven § 119 og tvisteloven § 22-5. I tillegg vil departementet understreke at bestemmelsen ikke åpner for utlevering av opplysninger om at det er begjært eller besluttet kommunikasjonskontroll, eller opplysninger som fremkommer ved kontrollen, i større utstrekning enn det som følger av straffeprosessloven § 216 i.

Bestemmelsen gir en adgang til å utlevere informasjon uten hinder av lovbestemt taushetsplikt, men oppstiller ingen plikt til dette. Det vises til forholdsmessighetsvurderingen som må foretas i forbindelse med utlevering av personopplysninger fordi utlevering innebærer en nytt menneskerettslig inngrep. I tillegg vil den enkelte utleverende myndighet måtte vurdere hvilke skranker som gjelder etter Grunnloven § 102 og EMK artikkel 8, herunder hvor strenge krav som stilles til nødvendigheten og forholdsmessigheten av inngrepet.

13.6 Formidling av opplysninger på vegne av andre norske myndigheter

13.6.1 Gjeldende rett

Dagens regelverk regulerer ikke Etterretningstjenestens videreformidling av opplysninger på vegne av andre norske myndigheter. Slik videreformidling forekommer i praksis, og reguleres av interne prosedyrer. Bakgrunnen for praksisen er at Etterretningstjenesten i enkelte situasjoner har bedre forutsetninger enn vedkommende myndighet til å formidle informasjon til utenlandske tjenester og myndigheter. Det er et vilkår at Etterretningstjenesten ikke er opphav til informasjonen som formidles, og at tjenesten ikke ellers har egeninteresser i saken.

13.6.2 Forslag i høringsnotatet

Det foreslås i høringsnotatet punkt 13.3.4 å lovfeste i lovutkastet § 10-7 at Etterretningstjenesten skal kunne videreformidle opplysninger til og fra en utenlandsk samarbeidende tjeneste på vegne av en annen norsk myndighet. Det foreslås fem kumulative vilkår for slik videreformidling. For det første må den aktuelle norske myndigheten ha

anmodet Etterretningstjenesten om å videreformidle informasjonen. Videre må det fremstå klart overfor mottakeren at formidlingen skjer på vegne av en annen norsk myndighet, og ikke er utlevering av informasjon fra Etterretningstjenesten. Tjenesten skal ikke endre opplysningene som videreformidles, legge til egen informasjon eller be mottakeren om å handle på en bestemt måte i lys av opplysningene. Tjenesten må sørge for at mottakeren har kunnskap om at det kreves samtykke fra den norske myndigheten før informasjonen videreformidles til en tredjepart. Videreformidlingen må skje med notoritet fra tjenestens side. Kravet om notoritet bidrar til å legge til rette for EOS-utvalgets kontroll med etterlevelsen av de nevnte vilkårene.

13.6.3 Høringsinstansenes syn

Ingen høringsinstanser har uttalt seg om forslaget.

13.6.4 Departementets vurdering

Departementet opprettholder forslaget i høringsnotatet med enkelte justeringer. I samsvar med gjeldende praksis og behov bør utlevering på vegne av andre norske myndigheter kunne skje ikke bare til utenlandske samarbeidende *tjenester*, men også til andre lands *myndigheter* som den norske offentlige myndigheten vil utlevere informasjon til som ledd i et samarbeid. Etter oppdateringen av kapittel 10 fremgår bestemmelsen av lovforslaget § 10-6.

13.7 Bistand til politiet

13.7.1 Gjeldende rett

Etterretningstjenesten kan gi bistand til politiet etter reglene i politiloven § 27 a og instruks om Forsvarets bistand til politiet av 16. juni 2017 nr. 789 (bistandsinstruksen). Politiloven § 27 a første ledd lister opp hvilke situasjoner som åpner for bistand. I de tilfeller som faller utenfor første ledd, kan Etterretningstjenesten bistå politiet med materiell, spesialkyndig operatørpersonell og annet, jf. tredje ledd. Bistanden gjennomføres etter politiets rettsgrunnlag og for å løse politiets oppdrag, og personellet som yter bistand vil være under politiets ledelse og instruksjonsmyndighet.

Bistand etter politiloven § 27 a må ikke sammenblandes med bistand etter instruks 13. oktober 2006 om samarbeidet mellom Etterretningstjenesten og Politiets sikkerhetstjeneste (samarbeidsinstruksen). Sistnevnte form for bistand er et samarbeid hvor Etterretningstjenesten og PST bistår hverandre innenfor rammen av sine respektive regelverk.

13.7.2 Forslag i høringsnotatet

I høringsnotatet foreslås det at Etterretningstjenesten kan gi bistand til politiet etter politiloven § 27 a, med unntak av bistand i form av informasjonsinnhenting etter reglene i kapittel 7 og utlevering av informasjon etter lovutkastet § 7-12 andre ledd. Begrensningen begrunnes med at det vil være en teoretisk mulighet for formålsglidning dersom loven åpner for at politiet kan anmode om bistand fra Etterretningstjenesten i form av direkte bruk av tilrettelagt innhenting eller utlevering av opplysninger fremskaffet gjennom denne tilgangen.

13.7.3 Høringsinstansenes syn

Ingen høringsinstanser har uttalt seg om forslaget.

13.7.4 Departementets vurdering

Departementet opprettholder forslaget i høringsnotatet om at Etterretningstjenesten kan gi bistand til politiet etter politiloven § 27 a, med unntak av bistand i form av informasjonsinnhenting etter reglene i kapittel 7. Henvisningen til lovutkastet § 7-12 andre ledd videreføres ikke, da dette dekkes av den generelle henvisningen til kapittel 7.

14 Avsluttende bestemmelser

14.1 Forholdet til annen lovgivning

14.1.1 Forvaltningsloven

14.1.1.1 Gjeldende rett

Forvaltningsloven gjelder for «virksomhet som drives av forvaltningsorganer», jf. forvaltningsloven § 1 første punktum. Med «forvaltningsorgan» menes «ethvert organ for stat eller kommune», jf. andre punktum.

Etterretningstjenesten er organisatorisk en del av Forsvaret, og følgelig et organ for staten. Dette innebærer at forvaltningsloven i utgangspunktet kommer til anvendelse for Etterretningstjenestens virksomhet, med mindre annet følger av lov, jf. forvaltningsloven § 1 første punktum.

Etterretningstjenesten treffer i sin informasjonsinnhentingsvirksomhet ikke avgjørelser som er bestemmende for noens rettigheter eller plikter. Dette innebærer at forvaltningsloven i liten grad får anvendelse når Etterretningstjenesten løser sine oppgaver etter etterretningstjenesteloven § 3. De mest relevante bestemmelsene i forvaltningsloven er reglene om taushetsplikt i §§ 13 til 13 f. Disse bestemmelsene får anvendelse ved enhver form for behandling av opplysninger hos Etterretningstjenesten, med mindre taushetsplikten er særregulert i annen lov eller i medhold av annen lov.

I den daglige virksomheten driver Etterretningstjenesten også alminnelig forvaltningsvirksomhet som reguleres av forvaltningsloven.

14.1.1.2 Forslaget i høringsnotatet

Det pekes i høringsnotatet punkt 14.2 på at forvaltningsloven i liten grad er relevant for Etterretningstjenestens oppgaveløsning etter lovforslaget. Det foreslås derfor å slå uttrykkelig fast i § 11-7 at forvaltningsloven ikke får anvendelse på saksbehandling som knytter seg til utførelsen av Etterretningstjenestens oppgaver etter loven. Til sammenligning vises det til at det gjelder egne bestemmelser om forvaltningslovens anvendelse for PSTs saksbehandling tilknyttet tvangsmidler i forebyggende øyemed, jf. politiloven § 17 e tredje ledd.

Det vurderes i høringsnotatet at forvaltningslovens regler om taushetsplikt i §§ 13 til 13 f fortsatt bør gjelde for Etterretningstjenesten, da disse vil utfylle den særlige taushetspliktbestemmelsen som foreslås i lov om Etterretningstjenesten § 11-2, og at dette bør fremgå av loven.

Det presiseres at bestemmelsen ikke regulerer den øvrige forvaltningsmessige virksomheten til Etterretningstjenesten, som fortsatt vil reguleres av forvaltningsloven.

14.1.1.3 Høringsinstansenes syn

Ingen høringsinstanser har uttalt seg om forslaget.

14.1.1.4 Departementets vurdering

Departementet opprettholder forslaget i høringsnotatet. Bestemmelsen om forholdet til forvaltningsloven inntas i lovforslaget § 11-1.

14.1.2 Offentleglova

14.1.2.1 Gjeldende rett

Offentleglova gjelder for statlige organer, jf. § 2 første ledd bokstav a. Hovedregelen er innsyn, jf. § 3, men det er adgang til å gjøre unntak fra innsynsretten etter reglene i kapittel 3.

Taushetsbelagte, herunder sikkerhetsgraderte, opplysninger er unntatt fra innsyn etter offentleglova § 13 første ledd og sikkerhetsloven §§ 5-3 og 5-4. Det fremgår motsetningsvis av offentleglova § 11 at meroffentlighet ikke skal vurderes når opplysningene er underlagt taushetsplikt. Ved krav om innsyn i graderte dokumenter må utsteder på nærmere vilkår vurdere avgradering etter offentlegforskrifta § 10 og virksomhetsikkerhetsforskriften § 33.

Opplysninger som Etterretningstjenesten besitter som ikke er underlagt taushetsplikt, vil i mange tilfeller være unntatt offentlighet etter offentleglova § 20 første ledd bokstav b og § 21 av

hensyn til utenrikspolitiske interesser eller av hensyn til nasjonal sikkerhet eller forsvaret av landet. Offentlegforskrifta § 9 tredje ledd gir adgang til å gjøre unntak fra innsyn i Etterretningstjenestens journaler og saksdokumenter.

14.1.2.2 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 14.8 å innta en bestemmelse i § 11-6 som gjør unntak fra offentleglovas regler om innsyn for opplysninger som behandles av Etterretningstjenesten etter loven.

Det presiseres i forslag til § 11-6 andre ledd at den enkelte av sikkerhetsmessige grunner hverken har rett til innsyn i etterretningsinformasjon som Etterretningstjenesten behandler eller har behandlet om vedkommende, eller i om Etterretningstjenesten behandler eller har behandlet etterretningsinformasjon om vedkommende. Det foreslås i andre ledd at begjæringer om slikt innsyn skal kunne avvises uten realitetsbehandling. Forslaget innebærer at det gjøres unntak fra meroffentlighetsprinsippet. Det slås i forslaget tredje ledd siste punktum fast at enhver som mener at Etterretningstjenesten har begått urett mot seg, kan klage til EOS-utvalget i tråd med EOS-kontrollovens bestemmelser.

Forslaget om å gjøre unntak fra offentleglova begrunnes med at informasjonen Etterretningstjenesten behandler, som hovedregel er sikkerhetsgradert etter sikkerhetsloven og dermed unntatt innsyn etter offentleglova § 13. Øvrig informasjon vil svært ofte unntas offentlighet etter samme lov §§ 20 første ledd bokstav b og 21. Det påpekes at en innsynsordning dermed fremstår som lite reell. Videre uttrykkes bekymring for at dersom det i enkeltsaker unntaksvis skulle gis innsyn, vil sammenholdte opplysninger fra flere saker kunne røpe sikkerhetsgradert informasjon.

Det vises til at tilsvarende vurdering er gjort for Politiets sikkerhetstjeneste (PST). PSTs arkiver og registre er unntatt fra innsyn og informasjonsplikt etter offentleglova, jf. politiregisterloven § 66. Det understrekes at begrunnelsen for en slik unntaksbestemmelse også gjør seg gjeldende for Etterretningstjenesten.

14.1.2.3 Høringsinstansenes syn

Norsk Journalistlag og *Norsk Presseforbund* er kritiske til forslaget om å unnta Etterretningstjenesten fra offentleglovas regler om innsyn. Journalistlaget uttaler:

> «For å skape legitimitet og tillit hos befolkningen, må tjenesten vise åpenhet rundt det som er mulig å være åpen om. Hemmelighold svekker forutsetningene for en kunnskapsbasert offentlig debatt om hvilke handlingsrom tjenesten bør ha. Dette demokratiske underskuddet må kompenseres med større åpenhet om de sidene ved tjenestens virksomhet som det kan snakkes om.
>
> Vi mener forslaget fra departementet om unntak fra offentlighet og innsyn, går utover de reelle grunnene som taler for dette, og vil ikke skape den tilliten som Etterretningstjenesten er avhengig av fra samfunnet. Departementet foreslår at offentlighetsloven ikke skal gjelde. Å begrunne en slik begrensning med «regelharmonisering og kostnadseffektivitet», som departementet gjør på s. 363, viser en misforstått hemmelighold og manglende forståelse for offentlighetsprinsippet. Skal hemmeligholdet kunne forsvares, må det være av hensyn til å trygge Norges suverenitet, territorielle integritet og andre nasjonale sikkerhetsinteresser.»

Journalistlaget tilføyer at lovforslaget ikke gjelder for all virksomhet som Etterretningstjenesten bedriver. Dette tilsier etter journalistlagets vurdering at offentleglova fortsatt vil gjelde for administrativ, forvaltningsmessig eller annen virksomhet som utøves av Etterretningstjenesten, og at meroffentlighet her må vurderes på vanlig måte. Det etterspørres en nærmere presisering av dette i forarbeidene. Journalistlaget oppsummerer sitt syn slik:

> «Generelt bør det i større grad enn i dag, være bedre balanse mellom det nasjonale behovet for hemmelighold, og samfunnets behov for informasjon. Sikkerhet og trygghet er selvfølgelig helt avgjørende for den grunnleggende samfunnsfriheten vår. Men lukkethetskulturen må utfordres. Som Godahl-utredningen understreket i 2016: «Åpenhet er viktig, også om mindre heldige forhold, for å sikre en informert offentlig debatt og en politisk forankring av engasjementene.»»

Også *Norsk Presseforbund* er kritiske til forslaget, og uttaler:

> «Vi støtter ikke forslaget om at offentlighetsloven ikke skal gjelde, og mener dette er et område der det er særdeles viktig at man tilstreber [så] mye åpenhet som mulig. Dette for

å kompensere for en prosess som er helt lukket fram til EOS-kontrollen, også i domstolen.»

Presseforbundet uttaler videre at det ikke kan være noen tvil om at «opplysninger om overvåking av det norske folk» er av betydelig allmenn interesse, og at dette ligger innenfor kjerneområdet av hva mediene skal kontrollere. Presseforbundet mener at tilbakeholdelse av informasjon må vurderes etter EMK artikkel 10. Når Etterretningstjenesten får et innsynskrav, må det gjøres en konkret vurdering i det enkelte tilfellet av om innsyn skal gis, eller om det foreligger sterke hensyn som berettiger hemmelighold.

14.1.2.4 Departementets vurdering

Departementet har i lys av høringen vurdert hvorvidt forslaget om å gjøre unntak fra offentleglova bør videreføres. Hensynet til en åpen og offentlig forvaltning tilsier som utgangspunkt at offentleglova bør gjelde. Det skal tungtveiende grunner til for å gjøre unntak fra innsynsretten, jf. offentlighetsprinsippet i Grunnloven § 100 femte ledd. Retten til innsyn i statens dokumenter er begrunnet i rettssikkerhetshensyn og i hensynet til å sikre befolkningens tillit til forvaltningen. Departementet er enig med *Norsk Journalistlag* i at hensyn til regelharmonisering og kostnadseffektivitet ikke er tilstrekkelig til å gjøre unntak fra innsynsretten.

På den andre siden er det av hensyn til nasjonale sikkerhetsinteresser et legitimt behov for å skjerme informasjon om etterretningsmål, metoder, personell, kilder og internasjonale samarbeidspartnere. Departementet viser i denne sammenhengen til politiregisterloven § 66, som gjør unntak fra offentleglovas regler om innsyn for Politiets sikkerhetstjeneste (PST). Unntaket er begrunnet med de skadevirkningene en innsynsrett ville ha for PSTs arbeid, se Ot.prp. nr. 108 (2008–2009) punkt 17.4.3 side 278 og NOU 2003: 21 punkt 23.6.2.2 side 337 følgende. Innsynsretten ville dessuten ikke være reell, idet unntakene fra innsyn på grunn av hensynet til blant annet rikets sikkerhet, kildevern og metodebruk ville komme til anvendelse i nærmest samtlige tilfeller. Departementet finner det ikke tvilsomt at de samme hensyn gjør seg gjeldende når det gjelder spørsmålet om innsyn i saker hos Etterretningstjenesten.

Departementet understreker i lys av høringen at Etterretningstjenestens adgang til å samle inn informasjon om personer i Norge, er begrenset etter lovforslaget kapittel 4. Informasjon som tjenesten besitter om norske rettssubjekter, er dessuten et viktig område for EOS-utvalgets kontroll. Departementet anerkjenner pressens kontrollfunksjon i samfunnet. På grunn av de legitime skjermingsbehovene på utenlandsetterretningens område, vil offentlighetens ønske om informasjon likevel ikke kunne tilfredsstilles fullt ut. Det var denne erkjennelsen som lå bak opprettelsen av EOS-utvalget, se rapporten til Stortinget fra Evalueringsutvalget for EOS-utvalget (Dokument 16 (2015–2016)) side 165.

Etter dette har departementet kommet til at forslaget i høringsnotatet opprettholdes. Det foreslås enkelte justeringer. Lovutkastet § 11-6 andre ledd fremstår som overflødig ved siden av regelen i første ledd. Departementet foreslår videre å plassere unntaket i offentleglova selv, heller enn i etterretningstjenesteloven. Det vises til forslaget til nytt fjerde punktum i offentleglova § 2 fjerde ledd. Bestemmelsen som viser til klageretten til EOS-utvalget foreslås plassert i § 11-7 første ledd.

Departementet presiserer at unntaket fra offentleglova ikke gjelder for virksomhet som ligger utenfor lovforslaget, som påpekt av *Norsk Journalistlag*. Unntaket innebærer heller ikke et forbud mot å gi innsyn i informasjon hos Etterretningstjenesten, så fremt ikke regler om taushetsplikt eller andre regler er til hinder for dette. Departementet legger til grunn at tjenesten utviser åpenhet i den utstrekning det er forsvarlig.

14.2 Særregulering av taushetsplikten

14.2.1 Gjeldende rett

Etterretningstjenesteloven har ingen bestemmelse om taushetsplikt. Etterretningstjenestens personell er underlagt taushetsplikt etter annet lovverk, blant annet forvaltningsloven §§ 13 til 13 f. Videre er enhver som får tilgang til sikkerhetsgradert informasjon som ledd i sitt arbeide eller tjeneste for en virksomhet som faller inn under sikkerhetslovens virkeområde, underlagt livsvarig taushetsplikt etter sikkerhetsloven § 5-4. Etterretningstjenesten faller klart innenfor sikkerhetslovens virkeområde. Formuleringen «arbeidet eller tjenesten» skal forstås vidt, og omfatter både oppdrag, verv eller aktivitet for, og andre formaliserte relasjoner til, virksomheten, se Prop. 153 L (2016–2017) side 177.

14.2.2 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 14.3 at reglene om taushetsplikt etter forvaltningsloven og sik-

kerhetsloven suppleres av en egen bestemmelse i etterretningstjenesteloven § 11-1.

Etter forslaget pålegges enhver som gjør arbeid eller tjeneste for Etterretningstjenesten plikt til å bevare livsvarig taushet om skjermingsverdig informasjon som de blir kjent med gjennom arbeidet eller tjenesten. Det samme foreslås å gjelde for kilder og oppdragstakere som har signert taushetserklæring.

«Skjermingsverdig informasjon» defineres i høringsnotatet som «informasjon som kan skade nasjonale sikkerhetsinteresser dersom informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig». Definisjonen reflekterer ordlyden i sikkerhetsloven § 5-1, og det fremgår av høringsnotatet at begrepet er ment å forstås på samme måte.

Videre foreslås det lovfestet at skjermingsverdig informasjon som en person som gjør arbeid eller tjeneste for Etterretningstjenesten får kjennskap til, ikke kan utnyttes i virksomhet utenfor tjenesten. Formålet med bestemmelsen er å gjøre det klart at kunnskap som stammer fra informasjon som vedkommende har fått i forbindelse med arbeidet eller tjenesten, ikke kan benyttes i kommersiell eller annen virksomhet uten at dette er klarert med Etterretningstjenesten.

Det presiseres at taushetsplikten ikke vil være til hinder for at opplysningene kan utleveres i medhold av lov, som for eksempel ved utlevering til de myndigheter som har som oppgave å kontrollere eller føre tilsyn med Etterretningstjenesten. Taushetsplikten vil heller ikke være til hinder for at opplysningene gjøres kjent for andre i Etterretningstjenesten, i samsvar med reglene om autorisasjon og tjenstlig behov.

14.2.3 Høringsinstansenes syn

Ingen høringsinstanser har uttalt seg om forslaget til en særbestemmelse om taushetsplikt i lovforslaget. Enkelte har imidlertid stilt seg kritiske til behovet for en egen bestemmelse om straff for brudd på denne taushetsplikten, se nedenfor i punkt 14.8.

14.2.4 Departementets vurdering

Departementet opprettholder forslaget i høringsnotatet om en egen taushetspliktbestemmelse for personer som gjør arbeid eller tjeneste for Etterretningstjenesten. Det foreslås enkelte endringer og lovtekniske justeringer. Bestemmelsen foreslås i tråd med omstruktureringen av kapittel 11 plassert i § 11-2.

Departementet foreslår at formuleringen «arbeid eller tjeneste for» skal forstås på samme måte som etter sikkerhetsloven. Dermed vil også personer med en løsere tilknytning til Etterretningstjenesten enn formelt ansatte og tjenestegjørende, for eksempel kilder og oppdragstakere, omfattes. En slik forståelse av begrepet «arbeidet eller tjenesten for» gjør at behovet for særskilte taushetserklæringer for nevnte grupper faller bort. Forslaget til § 11-1 første ledd andre punktum er dermed overflødig og videreføres ikke.

Forslaget i høringsnotatet bruker begrepet «skjermingsverdig informasjon». Begrepet omfatter informasjon som er sikkerhetsgradert etter en ren konfidensialitetsvurdering og informasjon som må beskyttes av integritets- og tilgjengelighetshensyn. Departementet viderefører etter en nærmere vurdering ikke begrepet «skjermingsverdig informasjon» i bestemmelsen om taushetsplikt. Begrunnelsen er at taushetsplikt er forbundet med opplysningers *konfidensielle karakter*, enten på grunn av opplysningenes innhold eller av hensyn til hvem som har avgitt eller mottatt dem. Det gir etter departementets syn mindre mening å pålegge noen taushetsplikt begrunnet i behovet for integritet eller tilgjengelighet. Departementet foreslår på denne bakgrunn at taushetsplikten knyttes til brudd på konfidensialiteten der dette kan skade «nasjonale sikkerhetsinteresser». Begrepet «nasjonale sikkerhetsinteresser» reflekterer legaldefinisjonen i sikkerhetsloven § 1-5 nr. 1.

Informasjon som kan skade nasjonale sikkerhetsinteresser dersom den blir kjent for uvedkommende, skal etter sikkerhetsloven § 5-3 sikkerhetsgraderes og merkes med riktig graderingsnivå. Det kan tenkes tilfeller hvor merking ikke er påført eller der graderingsnivået er feil. Departementet vil understreke at taushetsplikten etter lovforslaget i alle tilfeller må vurderes på et selvstendig grunnlag, og at manglende eller feilaktig merking ikke fritar den enkelte for taushetsplikt, dersom man burde forstå at informasjonen kan skade nasjonale sikkerhetsinteresser hvis den blir kjent for uvedkommende.

Departementet viderefører forslaget om at informasjon som nevnt i første ledd ikke kan utnyttes i virksomhet utenfor Etterretningstjenesten. Departementet viderefører også forslaget om å presisere i femte ledd at taushetsplikten ikke er til hinder for at opplysninger utleveres der det er fastsatt i loven eller etter regler i annen lov, eller at de gjøres kjent for andre i Etterretningstjenesten i samsvar med gjeldende autorisasjonsre-

gler og prinsippet om tjenstlig behov, med enkelte språklige endringer.

14.3 Informasjons- og personellsikkerhet

14.3.1 Gjeldende rett

Virksomheter som tilvirker informasjon, skal sikkerhetsgradere og merke denne dersom det kan skade nasjonale sikkerhetsinteresser om den blir kjent for uvedkommende, jf. sikkerhetsloven § 5-3. De fire graderingsnivåene etter loven er «BEGRENSET», «KONFIDENSIELT», «HEMMELIG» og «STRENGT HEMMELIG». Graderingsnivået avhenger av i hvilken grad det kan oppstå skadefølger dersom uvedkommende får kjennskap til informasjonen, og hvor alvorlige disse skadefølgene kan bli.

Personer som skal ha tilgang til informasjon gradert «KONFIDENSIELT» eller høyere, må sikkerhetsklareres, jf. sikkerhetsloven § 8-2 første ledd. Det samme gjelder som hovedregel personer som gjennom arbeidet sitt vil kunne få tilgang til slik informasjon, med mindre risikoen for tilgang kan fjernes gjennom andre og enklere tiltak, jf. sikkerhetsloven § 8-2 andre ledd.

Instruks om Etterretningstjenesten (e-instruksen) § 4 andre ledd fastsetter at Etterretningstjenestens personell som hovedregel skal være sikkerhetsklarert for «STRENGT HEMMELIG», men at sjefen for Etterretningstjenesten kan bestemme at personell i stillinger med lavere klareringsbehov heller skal klareres for «HEMMELIG».

14.3.2 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 14.5 at bestemmelsen om sikkerhetsklarering i e-instruksen § 4 andre ledd lovfestes i utkast til § 11-2. I tillegg foreslås lovfestet at enhver som gjør arbeid eller tjeneste i Etterretningstjenesten skal være norsk statsborger. Dersom en person har dobbelt statsborgerskap, må spørsmålet om ansettelse i Etterretningstjenesten tas opp til særskilt vurdering. Kretsen av personer som «gjør arbeid eller tjeneste i» Etterretningstjenesten, omfatter etter forslaget ikke oppdragstakere og kilder.

Kravet om statsborgerskap begrunnes av hensyn til Etterretningstjenestens hovedoppgave, som er å innhente informasjon om forhold i utlandet, herunder informasjon som direkte angår andre lands anliggender. Videre behandler Etterretningstjenesten høyt gradert informasjon i et stort omfang. Det vises til at informasjonens art og karakter, sammenholdt med sensitiviteten og skadepotensialet ved spredning til uvedkommende, gjør at Etterretningstjenesten er avhengig av personell som utviser full lojalitet til tjenestens samfunnsoppdrag.

Det heter i høringsnotatet at dobbelt statsborgerskap som den klare hovedregel vil utelukke ansettelse i Etterretningstjenesten. Likevel åpner forslaget for at ansettelse av personer med dobbelt statsborgerskap kan aksepteres i spesielle unntakssituasjoner, etter en særskilt vurdering og forutsatt at kravet om sikkerhetsklarering og øvrige vilkår er oppfylt.

14.3.3 Høringsinstansenes syn

Abelia påpeker at ny lov om Etterretningstjenesten, i kombinasjon med ny sikkerhetslov og annet arbeid, vil utvide behovet for sikkerhetsklarert personell i både sivil og militær sektor. Abelia oppfordrer til forutsigbarhet, økt transparens i vurderingskriteriene og betydelig kortere saksbehandlingstider, og mener at personell- og systemkapasiteten til behandling av sikkerhetsklareringer bør utbedres umiddelbart.

STAFO Etatsforeningen anbefaler å ikke lovfeste et krav om sikkerhetsklarering for «STRENGT HEMMELIG», fordi det som følge av globaliseringen blir stadig mer utfordrende å foreta personkontroll av personellets ektefelle, partner eller samboer. Foreningen mener at reguleringen som følger av sikkerhetsloven, er tilstrekkelig.

14.3.4 Departementets vurdering

Departementet opprettholder i hovedsak forslaget i høringsnotatet, men med enkelte språklige endringer. Det følger av drøftelsen i punkt 14.2.4 over at begrepet «arbeid eller tjeneste for» bør forstås på samme måte som i sikkerhetsloven, slik at også kilder og oppdragstakere omfattes. Kravet om statsborgerskap og sikkerhetsklarering bør imidlertid etter departementets syn bare gjelde for personer som er ansatt i eller tjenestegjør i Etterretningstjenesten, og ikke omfatte kilder, oppdragstakere og andre med en løsere tilknytning til tjenesten. Departementet foreslår derfor å sløyfe formuleringen «arbeid eller tjeneste for», og heller presisere i bestemmelsen at plikten gjelder «militært personell og sivilt ansatte».

Departementet har merket seg at *STAFO Etatsforeningen* stiller seg kritiske til å lovfeste et krav om sikkerhetsklarering for «STRENGT

HEMMELIG», men har kommet til at forslaget i høringsnotatet bør videreføres. Departementet har forståelse for at kravet kan oppfattes som strengt, men mener at det er nødvendig av hensyn til nasjonal sikkerhet. Bestemmelsen er en videreføring av gjeldende rett, jf. e-instruksen § 4 andre ledd. Sjefen for Etterretningstjenesten kan for særskilte stillinger med lavere klareringsbehov bestemme at personellet skal være sikkerhetsklarert for «HEMMELIG». Også dette er en videreføring av e-instruksen § 4 andre ledd.

14.4 Beredskap

14.4.1 Gjeldende rett

Forsvaret har egne beredskapsplaner som skal ivareta installasjoner, personell og evne til oppgaveløsning i alvorlige krisesituasjoner eller under væpnet konflikt. Beredskapsplanene er basert på Nasjonalt beredskapssystem og Forsvarets operative planverk.

E-instruksen § 6 fastsetter særlige krav til tjenestens beredskap. Generelt gjelder at tjenesten skal utarbeide og vedlikeholde sine beredskapsplaner basert på Forsvarets beredskapsplanverk, jf. første ledd. Videre skal tjenesten 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, jf. e-instruksen § 6 andre ledd. Kravene til sikkerhet og konfidensialitet etter instruksen oppfylles gjennom implementeringen av særskilte sikkerhetstiltak.

14.4.2 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 14.6 å lovfeste i § 11-3 kravet om at Etterretningstjenesten skal ivareta egen beredskap, og at lovteksten synliggjør krav om informasjons- og systemsikkerhetstiltak som er egnet til å forhindre at uvedkommende får kontroll over Etterretningstjenestens informasjon og systemer. Beredskapsplanene skal baseres på Nasjonalt beredskapssystem og Forsvarets operative planverk.

14.4.3 Høringsinstansenes syn

Ingen høringsinstanser har uttalt seg om forslaget.

14.4.4 Departementets vurdering

Departementet opprettholder forslaget i høringsnotatet. Etter oppdateringen av kapittelet fremgår bestemmelsen av lovforslaget § 11-6.

14.5 Arkiver, informasjonssystemer og etterretningsregistre

14.5.1 Gjeldende rett

Sikkerhetsloven oppstiller krav til informasjonssikkerhet i kapittel 5 og informasjonssystemsikkerhet i kapittel 6. For å oppfylle lovens krav må Etterretningstjenesten sørge for et forsvarlig sikkerhetsnivå, slik at skjermingsverdig informasjon, herunder sikkerhetsgradert informasjon, ikke blir kjent for uvedkommende, ikke går tapt eller blir endret, er tilgjengelig for personer med tjenstlig behov, samt at informasjonssystemene fungerer slik de skal, jf. sikkerhetsloven §§ 5-2 og 6-2.

Personopplysningsloven 2000 § 13 og personopplysningsforskriften 2000 kapittel 2 gir regler om informasjonssikkerhet ved behandling av personopplysninger. Personopplysningsloven 2000 med tilhørende forskrifter gjelder i en overgangsperiode for Etterretningstjenestens virksomhet frem til særregler om tjenestens behandling av personopplysninger trer i kraft, se nærmere om dette i kapittel 12.3.

Arkivlova fastsetter hovedregelen om at statlige arkiver skal avleveres til Arkivverket, jf. § 10 første ledd. Imidlertid kan Riksarkivaren gi samtykke til at statlige arkiv oppbevares av det arkivskapende organet, jf. andre ledd. Det følger av etterretningstjenesteloven § 5 første ledd at Etterretningstjenesten systematisk skal ordne informasjon som innhentes eller utarbeides i arkiv som er betryggende sikret og utilgjengelig for andre enn tjenestens eget personell og personer som fører kontroll eller tilsyn med Etterretningstjenestens virksomhet. På denne bakgrunn bortsettes ikke Etterretningstjenestens arkivalier til Arkivverket, men oppbevares i tjenestens egne lokaler som er sikret i tråd med sikkerhetslovens krav om informasjons- og informasjonssystemsikkerhet.

14.5.2 Forslaget i høringsnotatet

I høringsnotatet punkt 14.7 foreslås lovfestet i § 11-4 krav om at Etterretningstjenestens arkiver, informasjonssystemer og etterretningsregistre skal være betryggende sikret og utilgjengelig for andre enn eget autorisert personell med tjenstlig behov og personer som er satt til å føre kontroll

og tilsyn med Etterretningstjenesten. Forslaget viderefører gjeldende regler etter etterretningstjenesteloven § 5 første ledd.

14.5.3 Høringsinstansenes syn

Kripos ber departementet vurdere om det er hensiktsmessig å definere begrepet «tjenstlig behov».

Nasjonal sikkerhetsmyndighet (NSM) støtter tilnærmingen i høringsforslaget, og legger til grunn at NSM også under ny lov vil samarbeide med Etterretningstjenesten for å sikre et høyt nivå av informasjonssikkerhet i tjenesten, herunder at den etablerte ordningen for overordnet tilsyn med forebyggende sikkerhet i tjenesten videreføres.

14.5.4 Departementets vurdering

Departementet opprettholder forslaget i høringsnotatet, som i det oppdaterte lovforslaget er plassert i § 11-5. Det vises til merknaden til bestemmelsen for en nærmere omtale av begrepet «tjenstlig behov». Samarbeidet mellom NSM og Etterretningstjenesten omtales i punkt 13 om nasjonalt samarbeid.

14.6 Krav til underretning

14.6.1 Gjeldende rett

Den europeiske menneskerettskonvensjon (EMK) artikkel 13 om retten til et effektivt rettsmiddel lyder i norsk oversettelse:

> «Enhver hvis rettigheter og friheter fastlagt i denne konvensjon blir krenket, skal ha en effektiv prøvningsrett ved en nasjonal myndighet uansett om krenkelsen er begått av personer som handler i offisiell egenskap.»

Den europeiske menneskerettsdomstol (EMD) har lagt til grunn at den nasjonale lovgivningen må være tilstrekkelig klar til å gi borgerne en adekvat indikasjon på under hvilke omstendigheter myndighetene kan anvende hemmelige overvåkningstiltak, men at det ikke kan kreves at den enkelte skal varsles eller på annen måte kunne forutse når overvåkingen vil bli gjennomført (*Roman Zakharov mot Russland* 4. desember 2015, avsnitt 229). EMD har lagt til grunn at hvis, og så snart, det kan skje uten å undergrave formålet med overvåkingstiltaket eller den overvåkende tjenestens virksomhet, bør i utgangspunktet den overvåkede personen underrettes om overvåkningen i etterkant. Fordi overvåkning normalt skjer i skjul, vil en underrettelse bidra til å gi den enkelte en reell klageadgang (*Roman Zakharov mot Russland* avsnitt 287). I denne saken kom EMD 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 (avsnitt 298). Slik underretning er imidlertid ikke et absolutt krav dersom det foreligger en generell klageadgang etter nasjonal rett, altså et klagesystem som ikke beror på at klager er gjort kjent med overvåkningen eller av at klager kan godtgjøre at overvåkning har funnet sted (*Roman Zakharov mot Russland* avsnitt 234 og 288 med henvisning til *Kennedy mot Storbritannia* 18. mai 2010, avsnitt 167).

14.6.2 Forslaget i høringsnotatet

Spørsmålet om informasjonsplikt og underretning drøftes i høringsnotatet punkt 14.9. Det understrekes at det ligger i sakens natur at Etterretningstjenesten ikke kan informere etterretningsmål eller andre om at informasjonsinnhenting skal finne eller finner sted. Også etterhåndsunderretning 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, men adgang til å unnlate underretning er hjemlet i personopplysningsloven 2000 § 23. I tillegg vises det til at Etterretningstjenestens ansatte er bundet av taushetsplikt, og en underrettelse vil innebære brudd på denne. I høringsnotatet anbefales at det bør fremgå klart av loven at den som har vært gjenstand for informasjonsinnhenting som kan innebære inngrep i dennes menneskerettigheter, ikke har krav på underretning om inngrepet. Bestemmelsen foreslås inntatt i § 11-8.

Kravet til effektivt rettsmiddel drøftes i høringsnotatet punkt 4.3. Det vises til at det ikke gjelder noe absolutt krav om underretning etter menneskerettighetene.

14.6.3 Høringsinstansenes syn

Norges institusjon for menneskerettigheter (NIM) uttaler at det prinsipielt sett blir feil å oppstille en kategorisk regel om at den som har blitt overvåket, ikke skal notifiseres. NIM peker på at hoved-

regelen er at den som har vært gjenstand for informasjonsinnhenting, har krav på notifikasjon, men at det fra denne hovedregelen er adgang til å fastsette til dels omfattende unntak som ivaretar behovet for hemmelighold. NIM understreker at forutsetningen for en regel om at det ikke skal gis underretning, må være at den enkelte har tilgang på et effektivt rettsmiddel uten at det er nødvendig å påvise at man har blitt utsatt for overvåking.

Norsk Journalistlag, *Norsk Presseforbund* og *Datatilsynet* mener at det bør innføres en plikt til å underrette registrerte som har vært gjenstand for informasjonsinnhenting i strid med loven, men med nødvendige unntak.

14.6.4 Departementets vurdering

Det kan ikke oppstilles noe krav om at underretning skal skje i forkant av eller mens fordekt informasjonsinnhenting finner sted. Dette ville vesentlig forfeile formålet med innhentingen. Spørsmålet er om det skal oppstilles en plikt til underretning etter at informasjonsinnhentingen er avsluttet.

Justis- og beredskapsdepartementet vurderte spørsmålet i forbindelse med PSTs bruk av skjulte tvangsmidler i forebyggende øyemed i Prop. 68 L (2015–2016) punkt 13.5.8 side 222 til 223. Justis- og beredskapsdepartementet kom til at særtrekkene ved PSTs forebyggende virksomhet som regel ville gjøre det nødvendig å holde opplysninger om bruken av tvangsmiddelet og opplysningene som bruken resulterte i hemmelig for den som ble utsatt for inngrepet. Det ble vektlagt at det var snakk om handlinger som truer sikkerheten i samfunnet, og som ofte blir begått av lukkede og profesjonelle miljøer, og at det å oppdage og avverge slike mulige trusler tidligst mulig utgjør kjernevirksomheten til sikkerhetstjenestene. På denne bakgrunn ble det i politiloven § 17 e lovfestet at den som inngrepet retter seg mot, ikke har krav på underretning etter at bruken av tvangsmidlet har opphørt, eller rett til innsyn i opplysningene som har blitt innhentet ved bruk av tvangsmidlene.

Departementet finner det klart at en tilsvarende regel bør oppstilles i forbindelse med Etterretningstjenestens informasjonsinnhenting. Departementet kan vanskelig se hvordan underretning kan finne sted uten å røpe skjermingsverdig informasjon om prioriteringer, metoder og kapasiteter. Det ville være misvisende å lovfeste underretning som hovedregel når dette av legitime grunner i praksis ikke lar seg gjennomføre. På denne bakgrunn mener departementet at det bør lovfestes at den som har vært gjenstand for inngrepet, ikke har krav på underretning.

Departementet understreker at Etterretningstjenesten innhenter informasjon om utenlandske forhold. Tjenesten kan etter hovedregelen i lovforslaget § 4-1 ikke bruke metoder som utgjør et menneskerettslig inngrep overfor personer i Norge. Unntak gjelder i hovedsak for utenlandske statsborgere som opptrer på vegne av fremmed stat, jf. lovforslaget § 4-2. Disse har, på samme måte som etterretningsmål i utlandet, ingen berettiget forventning om underretning fra norske myndigheter om innhentingen.

Kravet til effektive rettsmidler etter EMK artikkel 13 oppfylles etter departementets syn av klageadgangen til EOS-utvalget. Utvalget kan behandle alle klager som faller inn under kontrollområdet, jf. EOS-kontrolloven § 5 andre ledd, og det oppstilles ikke noe krav til dokumentasjon. Enhver kan dessuten anlegge søksmål mot staten ved domstolene. Det vises til drøftelsen i punkt 4.4.

På denne bakgrunn opprettholder departementet forslaget i høringsnotatet. Bestemmelsen inntas i lovforslaget § 11-7 andre punktum. Departementet presiserer at bestemmelsen ikke innebærer noe forbud mot underretning. Underretning kan derfor etter forholdene finne sted dersom lovbestemt taushetsplikt eller andre regler ikke er til hinder for det, og underretning er sikkerhetsmessig forsvarlig.

14.7 Skjerming av etterretningsoperasjoner mv.

14.7.1 Gjeldende rett

Virksomheter som er underlagt sikkerhetsloven, skal gjennomføre de forebyggende sikkerhetstiltak som må til for å gi et forsvarlig sikkerhetsnivå og redusere risikoen knyttet til sikkerhetstruende virksomhet som kan skade nasjonale sikkerhetsinteresser, jf. sikkerhetsloven § 4-3. Sikkerhetstiltakene skal både omfatte tiltak som reduserer risikoen for at slik virksomhet inntreffer, og tiltak som reduserer konsekvensene av slik virksomhet ved å redusere skadeomfanget, jf. Prop. 153 L (2016–2017) side 173. For Etterretningstjenestens del vil effektive forebyggende sikkerhetstiltak blant annet innebære skjerming av ansatte, kilder, oppdragstakere, kapasiteter, metoder og operasjoner mot offentlig eksponering og kompromittering.

14.7.2 Forslag i høringsnotatet

I høringsnotatet punkt 14.10 understrekes det at skjerming mot eksponering av Etterretningstjenestens innhentingsvirksomhet er en avgjørende forutsetning for å kunne drive etterretning. Det vises til at dette i praksis skjer ved at man søker å unngå å vise tilknytningen til Etterretningstjenesten, norske myndigheter og Norge.

Skjerming kan skje ved bruk av dekkstrukturer og uriktige, falske eller villedende identiteter, dokumenter og opplysninger, samt ved at tjenesten tar kontroll over, modifiserer eller utplasserer elektronisk utstyr, for å hemmeligholde og gjennomføre sine operasjoner. Det foreslås at en slik adgang lovfestes i lovutkastet § 11-5. Det understrekes at bestemmelsen ikke er en innhentingshjemmel.

Det foreslås i lovutkastet § 11-5 tredje ledd at rapporteringsplikter i annen lov ikke gjelder for vederlag som Etterretningstjenesten yter til kilder og oppdragstakere som ikke er ansatt i Etterretningstjenesten. Slike vederlag og betalinger skal etter forslaget heller ikke regnes som skattepliktig inntekt eller inngå i grunnlag for beregning eller avkortning av sosiale ytelser eller lignende. Fritaket fra rapporteringsplikter er begrunnet i at offentlige rapporteringsplikter kan si noe om hvor Etterretningstjenesten utøver sine aktiviteter, samt om tjenestens kapasiteter og ressurser. Det understrekes i høringsnotatet at Etterretningstjenesten må forholde seg til gjeldende regler om skatt av lønn til ansatte og andre offentligrettslige krav.

Det vises i høringsnotatet til at behovet for skjerming også utfordres av en rekke andre rapporteringsplikter. Det foreslås derfor at Kongen i statsråd skal kunne gi bestemmelser som fraviker bestemmelser i annen lov, herunder 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. Forslaget begrunnes i behovet for særlige regler som unntar tjenesten fra ulike rapporteringsplikter og behovet for fleksibilitet til å følge fremtidige teknologiske og samfunnsmessige utviklingstrekk. Det presiseres at kompetansen ikke kan delegeres videre.

14.7.3 Høringsinstansenes syn

Befalets Fellesorganisasjon er positive til forslaget om å lovfeste egne regler om skjerming av Etterretningstjenestens personell mot offentlig eksponering. Det påpekes at det for personellet er en belastning å utføre oppdrag som innebærer personlig risiko, og at forslaget om bedre skjerming gir ekstra trygghet. BFO vektlegger videre at eksponering av Etterretningstjenestens ansatte i mediene vil virke hemmende for rekruttering.

Skattedirektoratet viser til forslaget i høringsnotatet om unntak fra skatte- og rapporteringsplikt for vederlag til kilder og oppdragstakere som ikke er ansatt i Etterretningstjenesten. Direktoratet mener det bør vurderes om det bør inntas korresponderende endringer i skattelovgivningen for å tydeliggjøre unntaket fra skatte- og rapporteringsplikt. Direktoratet opplyser at en eventuell endring antas å ikke medføre praktiske konsekvenser for Skatteetaten.

14.7.4 Departementets vurdering

Departementet opprettholder forslaget i høringsnotatet med enkelte lovtekniske justeringer. I tråd med omstruktureringen av bestemmelsene i lovforslaget kapittel 11 etter høringen foreslås bestemmelsen inntatt i § 11-4. Departementet har vurdert innspillet fra Skattedirektoratet om å innta korresponderende endringer i skattelovgivningen, men ser ikke dette som nødvendig.

14.8 Straff for brudd på taushetsplikt mv.

14.8.1 Gjeldende rett

Brudd på taushetsplikten kan etter gjeldende rett straffes etter ulike bestemmelser. Etter straffeloven § 209 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, med bot eller fengsel inntil 1 år. Samme straffansvar gjelder etter andre ledd ved brudd på taushetsplikt som følger av gyldig instruks for tjeneste eller arbeid for statlig eller kommunalt organ, jf. andre ledd. Etter tredje ledd gjelder straffansvaret også brudd på taushetsplikt etter at tjenesten eller arbeidet er avsluttet. Det følger av fjerde ledd at grovt uaktsom overtredelse straffes på samme måte. Medvirkning er ikke straffbar, jf. femte ledd.

Grovt brudd på taushetsplikt straffes med fengsel inntil 3 år, jf. straffeloven § 210. Ved avgjørelsen av om taushetsbruddet er grovt, skal det særlig legges vekt på om gjerningspersonen har

hatt forsett om uberettiget vinning og om handlingen har ført til tap eller fare for tap for noen.

Dersom brudd på taushetsplikt innebærer avsløring av statshemmeligheter, rammes det av straffeloven § 123. Bestemmelsen setter straff for 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. Strafferammen er fengsel inntil 3 år. Grov avsløring av en statshemmelighet straffes med fengsel inntil 15 år, jf. § 124. Ved avgjørelsen av om avsløringen er grov, skal det blant annet særlig legges vekt på om hemmeligheten er betrodd gjerningspersonen i tjeneste eller arbeid, om hemmeligheten er avslørt til en fremmed stat eller en terrororganisasjon og om betydelig skade er voldt.

Uaktsom avsløring av statshemmeligheter straffes etter straffeloven § 125 med fengsel inntil 2 år.

Militær straffelov § 69 første ledd setter straff for den som «uden skjellig Grund aabenbarer, hvad der i den militære Tjenestes Medfør er blevet ham betroet eller ved Lov eller anden gyldig Bestemmelse er betegnet som Tjenestehemmelighed». Etter andre ledd gjelder straffansvaret også etter fratrådt tjeneste. Overtredelser kan straffes med fengsel inntil 6 år. Militær straffelov gjelder etter § 9 nr. 1 for «alle ved rikets vebnede makt ansatte eller dertil hørende personer». Etterretningstjenesten er en del av Forsvaret, og ansatte i tjenesten omfattes dermed av virkeområdet til militær straffelov.

Etter sikkerhetsloven § 11-4 andre ledd straffes den som forsettlig eller grovt uaktsomt bryter taushetsplikt etter § 5-4 andre ledd med bot eller fengsel inntil 1 år eller begge deler, hvis ikke forholdet går inn under en strengere straffebestemmelse. Det følger av § 5-4 andre ledd at alle som får tilgang til sikkerhetsgradert informasjon som ledd i arbeidet eller tjenesten for en virksomhet som omfattes av loven, har taushetsplikt om innholdet. Taushetsplikten gjelder også etter at arbeidet eller tjenesten er avsluttet.

14.8.2 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 15.1 å sette straff for brudd på taushetsplikten og ødeleggelse eller manipulasjon av aktivitetslogger. Straffeprosessloven foreslås endret for å åpne for bruk av skjulte tvangsmidler i etterforskningen av saker om grove brudd på taushetsplikten. Det foreslås også straff for brudd på plikten til å tilrettelegge for innhenting av grenseoverskridende elektronisk kommunikasjon samt brudd på taushetsplikten i forbindelse med tilretteleggingen. I høringsnotatet er forslaget til straffebestemmelse inntatt i lovutkastet § 12-1. Forslag til endringer i straffeprosessloven er inntatt i lovutkastet § 13-3 nr. 1.

14.8.3 Høringsinstansenes syn

Kripos kan ikke se at forslaget til straffebestemmelse er nødvendig, idet forholdene allerede er belagt med straff. *Riksadvokaten* gir uttrykk for lignende synspunkter. *Generaladvokaten* peker på at Etterretningstjenesten er en del av Forsvaret, og at militær straffelov § 69 derfor vil være anvendelig i en rekke tilfeller. *Riksadvokaten* og *Politiets sikkerhetstjeneste (PST)* støtter ikke endringene i straffeprosessloven. *International Business Machines AS (IBM)* har forståelse for behovet for skjerming i forbindelse med tilretteleggingsplikten etter lovutkastet § 7-2, men fremholder at det kan synes strengt å oppstille en relativt tungt straffeklausulert taushetsplikt.

14.8.4 Departementets vurdering

Departementet har etter høringen kommet til at straffansvaret for brudd på taushetsplikten er tilfredsstillende regulert i straffeloven og militær straffelov. Det vises til redegjørelsen for gjeldende rett i punkt 14.8.1. Det er etter departementets syn heller ikke nødvendig å oppstille et særskilt straffebud om ødeleggelse og manipulasjon av aktivitetslogger, da dette kan straffes etter alminnelige straffebestemmelser om tjenestefeil mv. På denne bakgrunn videreføres ikke forslaget til straffebestemmelse i lovutkastet § 12-1 første til tredje ledd. Som en konsekvens av dette videreføres heller ikke forslaget til endringer i straffeprosessloven. Departementet viderefører med enkelte justeringer forslaget i lovutkastet § 12-1 fjerde ledd om straff for brudd på tilretteleggingsplikten og taushetsplikten knyttet til denne. Straffebestemmelsen plasseres i lovforslaget § 11-8. Det understrekes at brudd på taushetsplikten etter omstendighetene kan rammes av strengere straffebestemmelser i straffeloven kapittel 17.

14.9 Straffrihet for lovlige tjeneste- og oppdragshandlinger

14.9.1 Gjeldende rett

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. Slike *lovlige tjenestehandlinger* kan ikke straffes etter norsk rett. Dette antas etter gjeldende rett å følge av innhentingshjemmelen i etterretningstjenesteloven § 3. 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 (Ot.prp. nr. 90 (2003–2004) punkt 14.3.5.3 side 214).

14.9.2 Forslaget i høringsnotatet

Det drøftes i høringsnotatet punkt 15.2 hvorvidt det bør lovfestes at ansatte i og kilder eller oppdragstakere for Etterretningstjenesten ikke kan straffes for lovlige tjeneste- eller oppdragshandlinger. Det vises til at pedagogiske grunner kan tilsi en slik lovfesting, som blant annet kan antas å virke positivt for Etterretningstjenestens evne til å rekruttere ansatte, kilder og oppdragstakere. På den andre siden vises det til at bestemmelsen vanskelig vil kunne gi noe svar på hva som er en lovlig tjeneste- eller oppdragshandling. Straffriheten vil derfor avhenge av en nærmere vurdering av handlingens lovlighet med grunnlag i normer utenfor bestemmelsen selv, på samme måte som etter gjeldende rett. Formålet med bestemmelsen må derfor være å minne rettsanvenderen om at straffebud tidvis må tolkes innskrenkende. Det bes i høringsnotatet særskilt om høringsinstansenes syn på hvorvidt en bestemmelse om straffrihet bør tas inn i loven. I høringsnotatet er et forslag til bestemmelse inntatt i lovutkastet § 12-2.

14.9.3 Høringsinstansenes syn

Befalets Fellesorganisasjon (BFO) støtter forslaget i høringsnotatet, som de mener vil gi en ekstra trygghet for personell som blir pålagt å utføre denne typen arbeidsoppgaver.

Justis- og beredskapsdepartementet mener at det ikke bør inntas en bestemmelse om straffrihet for lovlige tjeneste- og oppdragshandlinger. De viser til at det følger av alminnelig juridisk metodelære at straffebestemmelser må tolkes i lys av andre lovbestemmelser, og uttaler:

> «Det vil etter vårt syn være en uheldig utvikling om det inntas bestemmelser i lovgivningen som skal minne rettsanvenderen om å benytte grunnleggende tolkningsprinsipper. I alle tilfelle kan vi ikke se at en bestemmelse som kun gir uttrykk for at handlinger ikke er straffbare når de er «lovlige», vil ha noen pedagogisk betydning i denne forbindelse. Tvert imot vil det være en risiko for at bestemmelsen feiloppfattes, slik at det gis inntrykk av at handlefriheten er større enn det som er ment.»

Riksadvokaten og *Kripos* gir uttrykk for lignende synspunkter.

14.9.4 Departementets vurdering

Departementet har på bakgrunn av høringen kommet til at forslaget i høringsnotatet ikke bør videreføres. Departementet legger til grunn at de spørsmål som måtte oppstå i praksis, må løses med utgangspunkt i en tolkning av den enkelte straffebestemmelse. Det vises i den sammenheng særlig til den alminnelige rettsstridsreservasjonen. Det vises til redegjørelsen under punkt 14.9.1.

15 Endringer i andre lover

15.1 Endringer i EOS-kontrolloven § 5

15.1.1 Gjeldende rett

EOS-kontrolloven § 5 gjelder utvalgets behandling av klager fra enkeltpersoner og organisasjoner. 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, jf. femte ledd første punktum. Utvalget kan likevel utøve slik kontroll dersom særlige grunner tilsier det, jf. andre punktum.

15.1.2 Forslaget i høringsnotatet

I høringsnotatet punkt 4.3.4.1 vurderes om den enkeltes klageadgang overfor EOS-utvalget er tilstrekkelig vid, særlig med henblikk på dagens begrensning som gjelder «personer som ikke er bosatt i riket og organisasjoner som ikke har tilhold her». Det foreslås at EOS-kontrolloven § 5 endres slik at kontrolloppgaven omfatter enhver person, uavhengig av bosted eller statsborgerskap, som er underlagt norsk jurisdiksjon.

15.1.3 Høringsinstansenes syn

Stortingets kontrollutvalg for etterretnings-, overvåkings, og sikkerhetstjeneste (EOS-utvalget) mener de foreslåtte endringene utløser behov for avklaringer av konsekvensene for utvalgets virksomhet. Utvalget viser til høringsnotatet punkt 4.3.4.1, hvor det foreslås at den någjeldende territorielle begrensningen for utvalgets kontrolloppgaver erstattes med en jurisdiksjonsbegrensning. Videre uttaler utvalget:

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

På bakgrunn av den rettslige usikkerheten som knytter seg til EMKs rekkevidde for utenlandsetterretningstjenestens overvåking av personer i utlandet, ber EOS-utvalget om følgende avklaringer knyttet til følgene av forslaget om jurisdiksjon som vilkår for utvalgets kontrollvirksomhet i EOS-kontrolloven § 5:

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

Videre påpeker utvalget:

> «Dersom EOS-utvalget er tiltenkt kontroll av E-tjenestens overvåking av alle personer i utlandet vil det innebære en betydelig utvidelse av kontrolloppgaven. Dette vil igjen legge press på kontrollmodellen [...]«

EOS-utvalget redegjør for jurisdiksjonsvilkårets betydning for utvalgets klagesaksbehandling. Det fremheves at forslaget om at utvalget kan ta klager til behandling *dersom* personen faller inn under norsk jurisdiksjon, synes å bryte med dagens kontrollmodell etter EOS-kontrolloven og forutsetningene om sikkerhetsgradering som loven hviler på.

Utvalget ber departementet avklare hvorvidt en konklusjon fra utvalget om at en person i utlandet faller under norsk jurisdiksjon (hvorpå det meddeles til vedkommende at klagen dermed tas til behandling), vil kunne anses som en bekreftelse av en skjermingsverdig opplysning. En slik konklusjon kan etter utvalgets syn vanskelig forstås som annet enn en bekreftelse av norsk etterretningstjenestes tilstedeværelse eller interesse for et område, land eller person. Utvalget uttaler:

> «Dersom departementet mener at resultatet av utvalgets jurisdiksjonsvurdering i en klagesak kan blottlegge skjermingsverdig informasjon, mener utvalget at et jurisdiksjonsvilkår ikke bør inntas i EOS-kontrolloven som vilkår for utvalgets mandat, eller at klageadgangen må sikres på annen måte.»

EOS-utvalget mener på denne bakgrunn at departementet må avklare konsekvensen av jurisdiksjonsvilkåret for utvalgets klagesaksbehandling.

Politiets sikkerhetstjeneste (PST) viser til at spørsmålet om klageadgang ble vurdert av Solbakkenutvalget som avga sin rapport til Stortinget 29. februar 2016. Solbakkenutvalget konkluderte med at det ikke kunne utledes forpliktelser etter EMD for at disse delene av EOS-tjenestenes virksomhet skulle vies en større del av EOS-utvalgets oppmerksomhet enn det som er tilfellet i dag, og at det derfor ikke ble anbefalt lovendringer. PST viser til at Solbakkenutvalget vurderte at unntaket der «særlige grunner tilsier det» i EOS-kontrolloven § 5 femte ledd siste setning i tilstrekkelig grad ivaretar klageadgangen, og uttaler:

> «Slik PST leser gjeldende bestemmelse, er klageadgangen tilstrekkelig ivaretatt i dagens lovgivning, og vi kan ikke se at rettstilstanden er endret siden Solbakken avga sin utredning. Gjeldende rett synes derfor å gi tilstrekkelig klageadgang.»

15.1.4 Departementets vurdering

På bakgrunn av høringen har departementet kommet til at forslaget i høringsnotatet ikke videreføres.

15.2 Endring i EOS-kontrolloven § 15

15.2.1 Gjeldende rett

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

15.2.2 Forslaget i høringsnotatet

I høringsnotatet punkt 4.3.6 vurderes 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. Det vises til at kravet etter EMK artikkel 13 og relevant rettspraksis fra EMD til «appropriate relief», tilsier at EOS-utvalget bør kunne uttale seg om erstatningsansvar i klagesaker mot tjenestene. Dette anses i vesentlig grad å styrke klagernes mulighet til å søke om erstatning fra det offentlige der det er konstatert at tjenestenes overvåkingsmessige virksomhet har medført kritikk. Det vises til at EOS-utvalget i dag neppe er fullstendig forhindret fra å ytre seg overfor forvaltningen om erstatningsspørsmålet, og at en formalisering av adgangen ikke vurderes å ha vesentlige konsekvenser for verken Etterretningstjenesten eller de øvrige EOS-tjenestene.

15.2.3 Høringsinstansenes syn

Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget ser i utgangspunktet positivt på å få mulighet til å uttale seg om erstatningsansvar i overvåkingsklager, men understreker at en slik ordning må utredes grundig og antakeligvis regelfestes mer i detalj. Utvalget uttaler:

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

Politiets sikkerhetstjeneste (PST) viser til at PST ikke har blitt konferert i dette spørsmålet om lovendring, og ikke på nåværende tidspunkt er beredt til å kommentere forslaget. PST fraråder på denne bakgrunn en slik lovendring nå.

15.2.4 Departementets vurdering

På bakgrunn av høringen viderefører ikke departementet forslaget i høringsnotatet. Som påpekt av

EOS-utvalget, reiser forslaget spørsmål som krever nærmere utredning, blant annet med hensyn til erstatning i klareringssaker og i klagesaker som gjelder de øvrige EOS-tjenestene.

15.3 Endringer i ekomloven § 6-2 a første ledd og andre ledd

15.3.1 Gjeldende rett

Politiet kan med hjemmel i ekomloven § 6-2 a første ledd første punktum på nærmere vilkår uten tillatelse fra myndigheten ta i bruk frekvenser som er tildelt andre. Myndigheten er i disse tilfellene lagt til Nasjonal kommunikasjonsmyndighet (Nkom), jf. § 1-4. Etter § 6-2 a første ledd annet punktum kan Nasjonal sikkerhetsmyndighet i særskilte tilfeller og i korte tidsrom uten tillatelse fra myndigheten ta i bruk frekvenser som er tildelt andre når dette er et nødvendig tiltak for forsvarlig sikring av konferanserom. Etterretningstjenesten har ingen tilsvarende adgang til å ta i bruk frekvenser.

15.3.2 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 16.1.3 å tilføye et tredje punktum i ekomloven § 6-2 a første ledd. Det følger av forslaget at Etterretningstjenesten i særskilte tilfeller og i korte tidsrom uten tillatelse fra eller varsel til myndigheten kan 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 lovutkastet § 4-2 første ledd.

Det foreslås at varsling til Nkom bør kunne unnlates av tungtveiende sikkerhetsmessige grunner. Det fremheves at tjenestens inngrep med stor sannsynlighet ikke vil forårsake noen form for skadelig interferens for øvrige brukere av mobilnettet, og at konsekvensene for personvernet vil vurderes ved all bruk av mobilregulert sone. Hensynet til å sikre samfunnets behov for uavbrutt elektronisk kommunikasjon vil være tungtveiende. Det vises til at grunnvilkårene i lovutkastet kapittel 5 må være oppfylt, og at aktiviteten vil være underlagt EOS-utvalgets kontroll.

15.3.3 Høringsinstansenes syn

Nasjonal kommunikasjonsmyndighet (Nkom) mener at det vil være problematisk dersom Etterretningstjenesten gis adgang til å ta i bruk frekvensene uten å varsle om dette. Nkom påpeker at det i forarbeidene til § 6-2 a ble presisert at myndigheten etter ekomloven til enhver tid må være oppdatert om den faktiske etableringen av mobilregulerte soner, og at det derfor stilles krav om varsling så snart som mulig etter at frekvensen er tatt i bruk. Nkom mener at de samme hensynene gjør seg gjeldende for Etterretningstjenestens bruk av frekvensene som for politiet, og at dette tilsier at varslingsplikten må gjelde. Dersom Etterretningstjenesten unntas fra varslingsplikten, vil det bli vanskelig for å Nkom å ivareta sitt kontrollansvar etter ekomloven. Videre foreslår Nkom å begrense frekvensbruken til metoden *lovlig identitetsfanging,* jf. ekomloven § 1-5 nr. 20, og at ekomloven § 6-2 a første ledd første punktum får følgende ordlyd:

> «Etterretningstjenesten kan i særskilte tilfeller og i korte tidsrom uten tillatelse fra myndigheten ta i bruk frekvenser som er tildelt andre til identitetsfanging 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.»

Videre foreslår Nkom følgende ordlyd i ekomloven § 6-2 a andre ledd første punktum:

> «Politiet, Etterretningstjenesten og Nasjonal sikkerhetsmyndighet skal varsle myndigheten uten ugrunnet opphold etter at frekvenser som er tildelt andre, er tatt i bruk.»

15.3.4 Departementets vurdering

Departementet fastholder forslaget i høringsnotatet, men med de justeringer som foreslås av Nkom, blant annet at Etterretningstjenesten pålegges varslingsplikt etter at frekvenser som er tildelt andre, er tatt i bruk. Varslingsplikten må gjennomføres på en måte som ivaretar Etterretningstjenestens behov for skjerming. Vedkommende som håndterer varslingen, må derfor inneha klareringsnivå STRENGT HEMMELIG etter sikkerhetsloven med forskrifter.

15.4 Endringer i ekomloven § 6-2 a tredje ledd

15.4.1 Gjeldende rett

Ekomloven § 6-2 a tredje ledd gir myndigheten etter ekomloven hjemmel til, i særskilte tilfeller og etter søknad, å gi Forsvaret og politiet tillatelse til å bruke frekvenser som er tildelt andre for å eta-

blere mobilregulert sone for øvingsformål. Tillatelsene kan bare gis til Forsvaret innenfor Forsvarets permanente øvingsområder, jf. tredje punktum. Frekvensenes rettighetshavere skal underrettes i god tid før frekvenser som er tildelt andre, tas i bruk.

15.4.2 Forslaget i høringsnotatet

I høringsnotatet foreslås at ekomloven § 6-2 a tredje ledd tredje punktum oppheves, slik at Etterretningstjenesten får en generell adgang til å etablere mobilregulerte soner uten dagens begrensning til permanente øvingsområder. Forslaget begrunnes med at Etterretningstjenesten har behov for å øve med teknisk utstyr i Norge, og at begrensningen etter gjeldende rett hindrer tjenestens mulighet til å gjennomføre hensiktsmessig og teknisk øving. Det presiseres at øvingen vil foregå innenfor klart definerte og avgrensede områder, der sannsynligheten for å interferere med sivile brukere av mobilnettet er minimal, og hvor øvingen er godkjent av Nkom.

15.4.3 Høringsinstansenes syn

Nasjonal kommunikasjonsmyndighet (Nkom) uttrykker forståelse for Etterretningstjenestens behov for å gjennomføre øvelser som er mest mulig lik en reell situasjon, men er skeptiske til forslaget om å oppheve § 6-2 a tredje ledd tredje punktum fordi mobilregulert sone kan opprettes både for lovlig identitetsfanging og jamming. Nkom fremhever at det særlig for jamming er viktig å foreta konsekvensanalyser, samt å kunne varsle frekvensinnehaverne for å forhindre unødvendige mottiltak. Nkom påpeker at selv om det er mest aktuelt for Etterretningstjenesten å opprette mobilregulert sone for identitetsfanging, så kan det være at Forsvaret for øvrig har behov for å gjennomføre øvelser på andre måter og at dette taler for at tredje ledd tredje punktum opprettholdes. For å ivareta Etterretningstjenestens behov og samtidig opprettholde begrensningen i dagens ordlyd, foreslår Nkom følgende ordlyd i ekomloven § 6-2 a tredje ledd tredje punktum:

> «Tillatelser til Forsvaret, med unntak for Etterretningstjenesten, kan bare gis til øvelser innenfor Forsvarets permanente øvingsområder.»

15.4.4 Departementets vurdering

Departementet er enig i Nkoms vurdering av behovet for å opprettholde begrensningen i ekomloven § 6-2 a tredje ledd tredje punktum for Forsvaret generelt, men at det i bestemmelsen gjøres unntak for Etterretningstjenesten. Departementet viderefører dermed forslaget i høringsnotatet, med de justeringer som foreslås av Nkom.

15.5 Endringer i straffeloven § 123

15.5.1 Gjeldende rett

Straffeloven § 123 setter straff for 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. Det følger av andre punktum at den som avslører en slik opplysning til en fremmed stat eller terrororganisasjon, ikke anses for å ha en aktverdig grunn.

15.5.2 Forslaget i høringsnotatet

Det foreslås i høringsnotatet punkt 16.1.2 en endring i straffeloven § 123 andre punktum som fastslår at den som offentliggjør en hemmelig opplysning om identiteten til operativt personell i og operative kilder for Etterretningstjenesten eller Politiets sikkerhetstjeneste, ikke anses for å ha aktverdig grunn. Det vises til at forslaget vil styrke vernet mot offentliggjøring eller annen avsløring av identiteten til Etterretningstjenestens og PSTs personell og kilder. Det presiseres at dersom en offentliggjøring helt unntaksvis skulle være vernet av ytringsfriheten, vil forholdet ikke kunne straffes.

15.5.3 Høringsinstansenes syn

Befalets Fellesorganisasjon (BFO) støtter forslaget i høringsnotatet:

> «Fra et arbeidstakerperspektiv er det svært positivt at E-tjenestens personell får et ekstra vern mot offentlig eksponering. For personellet som tar belastningen i å utføre oppdrag som innebærer personlig risiko er det en ekstra trygghet at lovforslaget legger opp til en bedre skjerming. Dersom E-tjenestens ansatte blir eksponert i mediene vil dette også virke hemmende for rekruttering.»

Riksadvokaten mener at ordlyden i forslaget er misvisende, da det ikke kan utelukkes at en offentliggjøring etter omstendighetene kan være vernet av ytringsfriheten. *Justis- og beredskapsdepartementet* gir uttrykk for samme synspunkt:

> «Når det forutsettes at offentliggjøringen unntaksvis kan være vernet av ytringsfriheten, vil det være misvisende om ordlyden gir uttrykk for at dette aldri kan anses å ha en aktverdig grunn. Skal det strafferettslige vernet mot offentliggjøring av identitet styrkes, bør dette etter vårt syn ikke skje ved tilføyelse i någjeldende § 123 annet punktum. Det kan eksempelvis vurderes å utforme et nytt punktum for disse tilfellene, slik at det ved utformingen kan tas høyde for at slik offentliggjøring ikke alltid vil være sammenlignbart med avsløring av opplysninger direkte til fremmede stater og terrororganisasjoner.»

Også *Politiets sikkerhetstjeneste (PST)* fraråder lovendringen.

15.5.4 Departementets vurdering

Departementet har på bakgrunn av høringen kommet til at forslaget i høringsnotatet ikke bør videreføres. Det er vanskelig å se for seg tilfeller der offentliggjøring av en hemmelig opplysning om identiteten til operativt personell i Etterretningstjenesten vil ha aktverdig grunn. Siden det likevel ikke helt kan utelukkes, bør ikke ordlyden utformes slik som i høringsnotatet. Det kan på et senere tidspunkt være aktuelt å utrede en styrking av det strafferettslige vernet mot offentliggjøring av identiteten til operativt personell på annen måte, slik *Justis- og beredskapsdepartementet* skisserer i sin høringsuttalelse.

16 Økonomiske og administrative konsekvenser

Bakgrunnen for revideringen av gjeldende lov om Etterretningstjenesten er behovet for å oppdatere regelverket i lys av den samfunnsmessige, rettslige og teknologiske utviklingen som har funnet sted siden gjeldende lov ble vedtatt i 1998. Departementets siktemål har særlig vært å ajourføre lovgrunnlaget med de krav som følger av rettsutviklingen på særlig menneskerettighets- og personvernområdet. Med unntak av tilrettelagt innhenting forventes ikke lovforslaget å få administrative eller økonomiske konsekvenser av større betydning, selv om 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 (punkt 10.13) og behandling av fortrolig kommunikasjon og kildeidentifiserende opplysninger (punkt 12.8). Det kan imidlertid ikke utelukkes at tilrettelagt innhenting og allerede eksisterende informasjonskilder vil kunne få betydning for Etterretningstjenestens virksomhet for øvrig. Dette er imidlertid vanskelig å forutsi.

Departementet mener på denne bakgrunn at lovforslaget ikke medfører vesentlige økonomiske eller administrative konsekvenser utover de som kan knyttes til tilrettelagt innhenting. Det redegjøres særskilt for de økonomiske og administrative konsekvensene knyttet til dette i lovproposisjonen punkt 11.15.

17 Merknader til de enkelte bestemmelsene

Til kapittel 1

Til § 1-1

Bestemmelsen fastsetter etterretningstjenestelovens formål.

Det følger av *bokstav a* at loven skal 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. Begrepene *Norges suverenitet, territorielle integritet, demokratiske styreform og andre nasjonale sikkerhetsinteresser* og *forebygge, avdekke og motvirke* skal forstås på samme måte som i sikkerhetsloven § 1-1. For en nærmere beskrivelse vises det til merknadene til sikkerhetsloven § 1-1 i Prop. 153 L (2016–2017) punkt 19.1 side 163.

Til forskjell fra sikkerhetsloven er etterretningstjenesteloven kun rettet mot *utenlandske trusler*. Med *trusler* menes forhold som er eller har potensial til å bli av en viss alvorlighetsgrad. Det kan for eksempel være sabotasje eller terrorvirksomhet fra utenlandske aktører der målet er å påføre en eller annen form for skade på våre nasjonale sikkerhetsinteresser. Det kan også dreie seg om spionasje fra andre stater eller utenlandske organisasjoner.

Bokstav b slår fast at loven skal bidra til å trygge tilliten til og sikre grunnlaget for kontroll med Etterretningstjenestens virksomhet. Etterretningstjenesten kan bruke inngripende metoder for å løse oppgavene som følger av lovforslaget kapittel 3. Tillit til at tjenesten utfører sin virksomhet innenfor fastsatte rettslige rammer, er sentralt. For å sikre dette foreslås et kontrollregime som består av internkontroll, forvaltningsmessig kontroll av overordnet departement, revisjon av Riksrevisjonen, kontroll av EOS-utvalget og domstolskontroll i saker om tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon.

Av *bokstav c* følger det at loven skal sikre at Etterretningstjenestens virksomhet utøves i samsvar med menneskerettighetene og øvrige grunnleggende verdier i et demokratisk samfunn. Formålsbestemmelsen må leses i sammenheng med Grunnloven § 2, som fastslår grunnleggende verdier for vår statsform, og Grunnloven § 92, som fastslår at statens myndigheter skal respektere og sikre menneskerettighetene slik de er nedfelt i Grunnloven og i for Norge bindende traktater om menneskerettigheter.

Til § 1-2

Bestemmelsen fastsetter lovens virkeområde.

Det fremgår av *første ledd* at loven gjelder for Etterretningstjenesten. Begrepet «Etterretningstjenesten» skal forstås organisatorisk, ikke funksjonelt. Loven gjelder for Etterretningstjenesten i den utstrekning tjenesten innhenter og behandler informasjon for etterretningsformål. Oppgavene til Etterretningstjenesten er nærmere beskrevet i merknadene til §§ 3-1 og 3-2. Avgrensningen innebærer at loven ikke kommer til anvendelse for tjenestens forvaltningsmessige og administrative aktivitet. I den grad Etterretningstjenesten, som en del av Forsvaret, blir satt til å løse andre oppgaver enn informasjonsinnhenting, må dette ha et annet rettslig grunnlag.

Loven regulerer ikke informasjonsinnhenting utført av andre enheter i Forsvaret, med mindre det er personell og enheter som er underlagt sjefen for Etterretningstjenestens kommando eller instruksjonsmyndighet. Kommandooverføringen kan være midlertidig eller gjentagende, men det skal være et tydelig skille for når en person eller enhet er underlagt kommando av sjefen for Etterretningstjenesten, og når personen eller enheten ikke er det. Loven kommer også til anvendelse for andre i den utstrekning det følger av den enkelte bestemmelse, for eksempel tilretteleggingsplikten som pålegges ekomtilbydere etter § 7-2. Det vises til punkt 5.2.4.1.

Andre ledd fastsetter unntak fra hovedregelen i første ledd ved innhenting og behandling av informasjon for etterretningsformål som skjer som ledd i en internasjonal operasjon med folkerettslig mandat. Mandatet kan eksempelvis være en sikkerhetsrådsresolusjon, myndighet til å utøve statlig selvforsvar eller samtykke fra vertsnasjonen. I tillegg må informasjonen innhentes og behandles

for operasjonens formål. Dersom informasjonen behandles for andre formål enn den konkrete operasjonen, vil loven få anvendelse for den aktuelle behandlingen. Det innebærer at innhentingen og behandlingen må ligge innenfor Etterretningstjenestens oppgaver i kapittel 3, i tillegg til at lovens vilkår for øvrig må være oppfylt.

Til § 1-3

Bestemmelsen definerer enkelte sentrale begreper i loven.

I *bokstav a* defineres *personopplysninger*. Definisjonen tilsvarer definisjonen i personvernforordningen, og er ment å ha det samme materielle innholdet.

En personopplysning er enhver opplysning om en identifisert eller identifiserbar fysisk person. *Enhver opplysning* favner svært vidt, og betyr i alminnelighet all tenkelig informasjon uavhengig av art, innhold eller form. Uttrykket omfatter både opplysninger som er objektivt og subjektivt verifiserbare. Dette innebærer at informasjon som alder og bosted er omfattet, så vel som en persons vurderinger eller karakteristikker av en annen. Begrepet omfatter all informasjon uavhengig av format. Eksempler på personopplysninger kan være et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for en fysisk persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet.

Opplysningen må relatere seg til en fysisk person. Dette innebærer at opplysningene må handle om, eller angå, et enkeltindivid. Det er i den sammenheng tilstrekkelig at tilknytningen mellom informasjon og person er indirekte.

Enkeltpersonen opplysningen knytter seg til, må være *identifiserbar*. At en fysisk person kan identifiseres, vil si at han eller hun kan skilles ut fra en gruppe av personer. Identifisering av en person er normalt enkelt å konstatere, men det er imidlertid ikke gitt at vedkommende kan identifiseres samtidig som opplysningene samles inn eller lagres. Det er i den sammenheng tilstrekkelig at identifikasjon kan tenkes å finne sted på et eller annet tidspunkt i fremtiden. Opplysninger som fremstår anonyme, kan vise seg å være personopplysninger fordi det er mulig å identifisere en eller flere personer indirekte.

I *bokstav b* defineres *behandling av personopplysninger*. Definisjonen tilsvarer definisjonen i personvernforordningen, og er ment å ha det samme materielle innholdet.

Behandling kan skje i form av 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. Det understrekes at eksemplene ikke er ment å være uttømmende, slik at behandlingsbegrepet også vil kunne omfatte andre operasjoner eller aktiviteter enn dem som er nevnt.

I *bokstav c* defineres *etterretningsformål* som «formål om å ivareta en eller flere av Etterretningstjenestens oppgaver etter kapittel 3». Oppgavebeskrivelsen i kapittel 3 er altså førende for hva som er etterretningsformål.

I *bokstav d* defineres *etterretningsmål* som «objekt, person, virksomhet eller annet som informasjonsinnhentingen retter seg mot». Det ligger ikke i denne definisjonen noen begrensning i hva som kan være et mål for Etterretningstjenesten. Det kan eksempelvis være en person, en bygning, en organisasjon eller en virksomhet. Det avgjørende for om noe skal regnes for å være et etterretningsmål, er om tjenesten retter innhentingen mot det aktuelle målet. Det innebærer at dersom tjenesten iverksetter målrettet innhenting mot en person, og det følger med informasjon om andre personer, vil ikke det i seg selv gjøre dem til etterretningsmål.

I *bokstav e* defineres *målsøking* som «systematisk arbeid for å identifisere nye etterretningsmål». Mål er «nye» hvis de er ukjente for Etterretningstjenesten. Formålet med prosessen er å identifisere personer, miljøer og organisasjoner som kan være i besittelse av etterretningsrelevant informasjon. Det følger av § 5-1 at målsøking kan iverksettes når det foreligger grunn til å undersøke om søket kan bidra til å frembringe informasjon som er relevant for etterretningsformål.

Målrettet innhenting defineres i *bokstav f* som «systematisk arbeid for å finne informasjon knyttet til identifiserte etterretningsmål». Det følger av § 5-2 at Etterretningstjenesten kan iverksette målrettet innhenting når konkrete holdepunkter gir grunn til å undersøke om innhenting kan frembringe informasjon som er relevant for etterretningsformål.

I *bokstav g* defineres *overskuddsinformasjon* som «informasjon som er uten interesse for etterretningsformål». Formuleringen «uten interesse» innebærer at informasjonen ikke kan bidra til å løse Etterretningstjenestens oppgaver etter kapittel 3, eller at informasjon som har vært relevant for etterretningsformål ikke lenger kan behand-

les. Et illustrerende eksempel er innsamling av metadata fra satellittkommunikasjon. Det er uunngåelig at det følger med metadata som ikke er av interesse for etterretningsformål. Dette regnes som overskuddsinformasjon. Overskuddsinformasjon kan være av interesse for andre myndigheter, og kan utleveres på visse vilkår, jf. § 10-4. Overskuddsinformasjon som stammer fra tilrettelagt innhenting etter kapittel 7, kan ikke deles, jf. § 7-13.

I *bokstav h* defineres *rådata* som «ubearbeidet eller automatisk bearbeidet informasjon i enhver form hvis etterretningsverdi ikke er vurdert». Når informasjon er vurdert for etterretningsverdi av en analytiker eller annen tjenesteperson, vil informasjonen ikke lenger være å regne som rådata. Informasjon med etterretningsverdi kan behandles i tråd med reglene i kapittel 9. Hvis informasjonen vurderes ikke å være relevant for etterretningsformål, regnes den som overskuddsinformasjon som skal slettes.

Bulk defineres i *bokstav i* som «informasjonssamlinger og datasett hvorav en vesentlig andel av informasjonen antas å være irrelevant for etterretningsformål». Hva som skal til før en «vesentlig andel» av informasjonen er irrelevant, må vurderes konkret, men det legges til grunn at det normalt vil kreves at minimum 40 % av informasjonen må antas å være irrelevant før det er snakk om innhenting i bulk. I tillegg må det dreie seg om datamengder i større omfang. Det kan ikke angis presist hvor stort omfang som må til for at noe skal kvalifisere som bulk. Omfanget må imidlertid være så stort at det ikke vil være mulig for Etterretningstjenesten å gjennomgå datamengden manuelt med sikte på å vurdere informasjonens relevans for etterretningsformål.

Innhenting av informasjon i bulk kan gjøres gjennom enhver innhentingsmetode, men er særlig aktuelt ved midtpunktinnhenting (innhenting av elektronisk kommunikasjon i transitt) etter § 6-9, for eksempel via fiberkabler eller satellitt.

I *bokstav j* defineres *utlevering* som «enhver formidling av opplysninger, både skriftlig og muntlig, til mottaker utenfor Etterretningstjenesten som ikke utfører tjeneste eller oppdrag for tjenesten». Alle former for deling av informasjon med eksterne vil være å regne som utlevering etter denne bestemmelsen.

Til kapittel 2

Til § 2-1

Bestemmelsen fastsetter at Etterretningstjenesten er Norges utenlandsetterretningstjeneste, jf. *første ledd første punktum*. Tjenesten bistår både sivile og militære myndigheter, og har dermed et sektoroverskridende oppdrag. Tjenestens oppgaver er regulert i kapittel 3, som er nærmere beskrevet i kapittel 7 i proposisjonen. Det følger av første ledd *andre punktum* at tjenesten er en del av Forsvaret og underlagt forsvarssjefens kommando. Det følger av dette at tjenesten ikke er en egen etat eller et selvstendig forvaltningsorgan, selv om tjenestens virksomhet i stor utstrekning er underlagt særlig regulering i loven.

Andre ledd første punktum lovfester det grunnleggende prinsippet om nasjonal kontroll med Etterretningstjenesten. Dette innebærer blant annet at kommandoen for tjenesten ikke kan overføres til en annen stat. En annen følge av prinsippet er at det skal sikres nasjonal kontroll med hvilken informasjon som gjøres kjent for utenlandske samarbeidspartnere, noe som fastsettes uttrykkelig i andre ledd *andre punktum*.

Til § 2-2

Bestemmelsen er en lovfesting av instruks om Etterretningstjenesten § 12, og er ment å videreføre gjeldende praksis. Det følger av *første ledd* at det er Forsvarsdepartementet som koordinerer og prioriterer norske myndigheters etterretningsbehov. Dette gjøres primært gjennom den årlige fastsettelsen av et gradert prioriteringsdokument for nasjonale etterretningsbehov (PNEB).

Bestemmelsen innebærer at andre departementer må melde sine og sine underordnede virksomheters etterretningsbehov til Forsvarsdepartementet, som må vurdere og prioritere dem sett i sammenheng med andre behov. Andre departementer og myndigheter har ikke anledning til å formulere oppdrag eller prioritere ressurser hos tjenesten på selvstendig grunnlag. Bestemmelsen er derimot ikke til hinder for at Forsvarsdepartementet kan fastsette rutiner for etterretningsdialog og koordinering mellom tjenesten og øvrige departementer og myndigheter.

Andre ledd fastsetter at departementet bestemmer prosedyrer for sivile etterretningsbehov som ikke dekkes av PNEB. For slike etterretningsbehov i Forsvaret bestemmes prosedyrene av Forsvarssjefen. Bestemmelsen åpner for at det kan gjøres andre prioriteringer enn det som følger av PNEB. Trusselbildet er dynamisk, og kan endres på svært kort tid. Bestemmelsen legger til rette for en fleksibel tilnærming til bruken av tjenestens ressurser, slik at de til enhver tid viktigste sakene kan prioriteres.

Til § 2-3

Det følger av *første ledd første punktum* at departementet ivaretar styring og kontroll med Etterretningstjenesten gjennom forsvarssjefen dersom annet ikke er fastsatt i loven. Regler om departementets styring og kontroll som ikke utøves gjennom forsvarssjefen, følger blant annet av § 2-2 (oppdragsstyring) og § 2-5 (foreleggelse av visse saker). Økonomi- og virksomhetsstyring ivaretas gjennom Koordineringsutvalget for Etterretningstjenesten (K-utvalget), jf. første ledd *andre punktum*. Det vises til punkt 6.1 for en nærmere beskrivelse.

Det følger av *andre ledd* at departementet kan fastsette særlige ordninger og rapporteringsrutiner for ivaretakelse av styring og kontroll.

Til § 2-4

Bestemmelsen lovfester Etterretningstjenestens plikt til å varsle og rapportere hendelser til norske myndigheter. Varslingsplikten fremgår av *første ledd bokstav a*, og inntrer dersom tjenesten oppdager trusler eller andre forhold som krever umiddelbar handling. Første ledd *bokstav b* fastsetter rapporteringsplikten. Dersom tjenesten oppdager utenlandske forhold som kan ha betydning for norske interesser, skal forholdene rapporteres inn. Kapittel 3 om Etterretningstjenestens oppgaver fastsetter rammen for varslings- og rapporteringsplikten. Det er bare forhold som faller innenfor tjenestens oppgaver det skal varsles og rapporteres om.

Andre ledd fastsetter at varslingen og rapporteringen etter første ledd skal skje i tråd med henholdsvis forsvarssjefens og departementets bestemmelser. Dette forutsetter at det utarbeides nærmere prosedyrer for hvordan varslings- og rapporteringsplikten skal gjennomføres.

Tredje ledd første punktum åpner for at Etterretningstjenesten kan varsle og rådgi andre enn norske myndigheter. Det kan være norske eller utenlandske personer og virksomheter. Et eksempel kan være en norsk virksomhet i utlandet som er utsatt for en terrortrussel. Varsling og rådgivning til andre enn norske myndigheter må skje innenfor rammen av departementets bestemmelser. Fordi det ved slik varsling og rådgivning etter omstendighetene kan være nødvendig å dele sikkerhetsgradert informasjon, åpner tredje ledd *andre punktum* for et snevert unntak fra kravet til autorisasjon og sikkerhetsklarering i sikkerhetsloven § 8-1. Vilkårene for unntak er for det første at det er *strengt nødvendig* å gi tilgang til informasjonen, og for det andre at dette er *sikkerhetsmessig forsvarlig*. Det må vurderes konkret i hvert enkelt tilfelle om det er anledning til å utlevere informasjonen. Personer og virksomheter som mottar sikkerhetsgraderte opplysninger med grunnlag i unntaksbestemmelsen, har taushetsplikt etter § 11-2.

Til § 2-5

Bestemmelsen fastsetter hvilke saker Etterretningstjenesten skal forelegge departementet for beslutning. Bestemmelsen er en lovfesting av instruks om Etterretningstjenesten § 13.

Det er tre kategorier av saker som skal forelegges departementet for beslutning. Det gjelder for det første etablering av samarbeid og avtaler med utenlandske tjenester eller internasjonale organisasjoner, jf. *bokstav a*. Etter *bokstav b* skal iverksettelse av særskilte etterretningsoperasjoner som kan reise politiske problemstillinger, forelegges. For det tredje skal *andre særlig viktige saker* forelegges, jf. *bokstav c*. Bokstav c er ment som en sikkerhetsventil for å sikre at Etterretningstjenesten ikke fatter beslutning i saker av stor betydning uten å involvere departementet.

Til § 2-6

Bestemmelsen fastslår at Etterretningstjenesten er underlagt EOS-utvalgets kontroll etter EOS-kontrolloven, jf. *første ledd første punktum*. Rammene for utvalgets kontroll endres ikke som følge av ny etterretningstjenestelov. Det etableres imidlertid en løpende kontroll med tjenestens etterlevelse av reglene i kapittel 7 om tilrettelagt innhenting, jf. første ledd *andre punktum*, som kommer i tillegg til den alminnelige etterfølgende kontrollen etter EOS-kontrolloven. Det vises til merknadene til § 7-11 for en nærmere beskrivelse.

Det fremgår av *andre ledd første punktum* at Etterretningstjenesten er underlagt revisjon og kontroll av Riksrevisjonen. Riksrevisjonen skal utpeke bestemte tjenestepersoner til å utføre revisjonen og kontrollen. Disse skal ha norsk statsborgerskap og være sikkerhetsklarert for STRENGT HEMMELIG, jf. andre ledd *andre og tredje punktum*. Etter andre ledd *fjerde punktum* skal Riksrevisjonen være representert i Koordineringsutvalget for Etterretningstjenesten (K-utvalget), se § 2-3 første ledd andre punktum.

Til § 2-7

Paragrafen etablerer en plikt for statsråden til å orientere stortingspresidenten årlig om Etterretningstjenestens virksomhet, jf. *første ledd*. Av hensyn til skjerming er det ikke mulig å orientere et åpent storting om tjenestens virksomhet. Stortingspresidenten mottar derfor en orientering på vegne av Stortinget. Det følger av *andre ledd første punktum* at sjefen for Etterretningstjenesten skal delta under orienteringen. For øvrig bestemmer stortingspresidenten hvem som skal delta, jf. andre ledd *andre punktum*.

Til § 2-8

Første ledd viderefører gjeldende rett om at det kun er EOS-utvalget som fører tilsyn med Etterretningstjenestens behandling av personopplysninger for etterretningsformål. Dette innebærer at tjenesten er unntatt kontroll og tilsyn av Datatilsynet og Personvernnemnda.

Av *andre ledd første punktum* følger det at kapittel 10 om tilsyn i ekomloven ikke gjelder for informasjon og områder som vil gi Nasjonal kommunikasjonsmyndighet innsyn i Etterretningstjenestens virksomhet. Det presiseres imidlertid i andre ledd *andre punktum* at unntaket ikke er til hinder for at Nasjonal kommunikasjonsmyndighet fører tilsyn med hvordan tilretteleggingsplikten etter § 7-2 utøves.

Det framgår av *tredje ledd* at domstolene fører kontroll med tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon i samsvar med reglene i kapittel 8. Det vises til nærmere redegjørelse under punkt 11.9.

Til kapittel 3

Til § 3-1

Bestemmelsen angir en av Etterretningstjenestens hovedoppgaver, som er å innhente og analysere informasjon om utenlandske forhold som kan bidra til at utenlandske trusler som nevnt i *bokstavene a til i* avdekkes og motvirkes. Bestemmelsen gir en uttømmende regulering av hvilke *utenlandske trusler* som er å regne som *etterretningsformål* og som kan danne grunnlag for innhenting og analyse av informasjon. Hva som ligger i *trusler* i denne sammenheng, er omtalt i punkt 7.3. Det innebærer i hovedsak at forholdet må være, eller ha potensiale til å bli, av en viss alvorlighetsgrad.

Med *utenlandske forhold* menes militære og sivile forhold utenfor Norges territorium som har betydning for å avdekke eller forstå de trusler som følger av bestemmelsen. Det kan eksempelvis dreie seg om å kartlegge andre staters militære kapasiteter, identifisere organisasjoner eller enkeltpersoner i utlandet som er på vei til Norge for å utføre en terrorhandling, avdekke digitale angrep eller påvirkningsoperasjoner mot Norge fra utlandet, eller lete etter (finne) trusler mot norske styrker i utlandet.

Det følger av bestemmelsen at Etterretningstjenesten «skal» innhente og analysere informasjon, men dette innebærer ikke at tjenesten til enhver tid har plikt til å innhente informasjon om alle truslene som regnes opp i bestemmelsen. Bestemmelsen må for det første forstås i lys av § 2-2 om oppdragsstyring. Det er departementet som fastsetter hvilke prioriteringer Etterretningstjenesten til enhver tid skal arbeide etter. Dette gjøres gjennom prioriteringsdokumentet for nasjonale etterretningsbehov (PNEB). Se punkt 6.1 for mer om dette. For det andre har Etterretningstjenesten begrensede ressurser og må gjøre nødvendige prioriteringer for å løse sine oppgaver på best mulig måte.

At informasjonen skal *bidra* til at trusler avdekkes og motvirkes, innebærer at Etterretningstjenesten må sørge for at informasjon de innhenter antas å ha en viss relevans for oppgavene. Terskelen for informasjonsinnhenting er ment å være lav når det gjelder sannsynligheten for at innhentingen vil frembringe faktisk relevant informasjon. Begrepet må leses i lys av grunnvilkårene for innhenting av informasjon i lovens kapittel 5.

Med *avdekke* siktes det til informasjon som er egnet til å oppdage og kartlegge trusler, mens det med *motvirke* siktes til informasjon som er egnet til sette beslutningstakere i stand til å treffe nødvendige tiltak ved behov.

I *bokstav a* slås det fast at informasjonen skal bidra til å avdekke og motvirke *trusler mot Norges selvstendighet og sikkerhet, territorielle integritet og politiske og økonomiske handlefrihet.* Dette omtales gjerne som trusler mot statssikkerheten. Norges selvstendighet og territorielle integritet knytter seg til Norges råderett over egne politiske og økonomiske anliggender. Landets øverste statsorganer må herunder ha kontroll over norsk territorium for å blant annet opprettholde statens konstitusjonelle funksjoner. Med *sikkerhet* menes blant annet vår evne til å avdekke og motvirke sikkerhetstruende virksomhet, jf. sikkerhetsloven § 1-1. Trusler mot statssikkerheten kan eksempelvis fremkomme gjennom mer begrensede væpnede angrep eller andre anslag på norske interesser,

gjennom manipulering av valg eller angrep på våre grunnleggende nasjonale funksjoner.

Bokstav b fastsetter at informasjonen skal bidra til å avdekke og motvirke *alvorlige trusler mot samfunnssikkerheten i Norge*. Samfunnssikkerheten dreier seg blant annet om å ivareta befolkningens liv og helse, sørge for at sentrale samfunnsfunksjoner opprettholdes og at viktig infrastruktur ikke går tapt. Det er imidlertid ikke informasjon om enhver trussel mot samfunnssikkerheten som ligger innenfor Etterretningstjenestens oppgaver. Det er bare *alvorlige* trusler, det vil si trusler som utfordrer samfunnets grunnleggende funksjonalitet, stabilitet eller befolkningens sikkerhet, som tjenesten skal innhente informasjon om, og kun trusler som har sitt utspring i utlandet.

Etter *bokstav c* skal informasjonen bidra til å avdekke og motvirke *alvorlige trusler mot norske interesser i utlandet*. Dette kan dreie seg om trusler mot norske borgere i utlandet, for eksempel gisselsituasjoner som anslaget mot gasskraftverket ved In Amenas i januar 2013.

Det følger av *bokstav d* at informasjonen skal bidra til å avdekke og motvirke *fremmed etterretningsvirksomhet*. Etterretningsaktivitet mot Norge dreier seg blant annet om å avdekke norske og allierte sikkerhets-, forsvars- og utenrikspolitiske posisjoner, sikre tilgang til viktig teknologi og avdekke sårbarheter og muligheter ved eventuelle krise- og krigssituasjoner. Det er viktig at Etterretningstjenesten innhenter informasjon som kan bidra til å avdekke hvilke aktører som opererer, motivene deres og hvilke metoder som benyttes.

Etter *bokstav e* skal informasjonen bidra til å avdekke og motvirke *fremmede sabotasje- og påvirkningsoperasjoner*. Med *fremmede sabotasjeoperasjoner* menes blant annet ødeleggelser og lignende som utføres av eller på vegne av en fremmed makt, organisasjon eller gruppering. Det forutsettes at virksomheten er grenseoverskridende og representerer en *ytre* trussel. Sabotasjebegrepet er ikke helt presist, og vil delvis kunne overlappe med begrepet «terrorisme». Det kan også falle innenfor hva som anses som en alvorlig trussel mot samfunnssikkerheten. *Påvirkningsoperasjoner* kan blant annet skje gjennom illegitim påvirkning av samfunnsopinionen eller valgresultater, for på den måten å påvirke våre demokratiske prosesser. Begrepet vil også kunne dekke utenlandske oppkjøp og eierskapsutøvelse som har til hensikt å undergrave nasjonale sikkerhetsinteresser. Begrepet vil i enkelte tilfeller overlappe med trusler mot statssikkerheten, jf. merknadene til bokstav a.

I *bokstav f* slås det fast at informasjonen skal bidra til å avdekke og motvirke *grenseoverskridende terrorisme*. Det finnes ingen allment anerkjent definisjon av terrorisme, verken i Norge eller internasjonalt. Bakgrunnen for det er blant annet uenigheter om innholdet i et slikt begrep. Det avgjørende for om Etterretningstjenesten kan innhente informasjon for formålet i bestemmelsen her, er imidlertid om trusselen faller innenfor det *norske myndigheter* anser for å være terrorisme. Det finnes ingen nasjonale terrorlister, men allment kjente organisasjoner og grupperinger som ISIL og Al-Qaida vil åpenbart falle innenfor begrepet. Det har videre formodningen for seg at organisasjoner og grupper som er vurdert som terrororganisasjoner av FN og EU vil falle inn under bokstav f, men det må likevel foretas en selvstendig nasjonal vurdering av spørsmålet.

Veiledning om hva norske myndigheter anser for å være terrorisme, finnes i straffeloven § 131. Der straffes nærmere bestemte handlinger (for eksempel drap) som terrorhandling dersom den er utført med terrorhensikt. Handlinger med terrorhensikt er handlinger som begås i den hensikt å forstyrre alvorlig en funksjon av grunnleggende betydning for samfunnet, å skape alvorlig frykt i befolkningen eller urettmessig å tvinge offentlige myndigheter eller en mellomstatlig organisasjon til å gjøre, tåle eller unnlate noe av vesentlig betydning for landet eller organisasjonen, eller for et annet land eller mellomstatlig organisasjon. Øvrige bestemmelser i straffeloven kapittel 18 kan fungere som eksempler på handlinger som anses som terrorrelaterte. Det må altså legges til grunn at det vil være innenfor bokstav f å innhente informasjon som kan bidra til å avdekke og motvirke trusler som dekkes av gjerningsbeskrivelsene i disse bestemmelsene.

For at Etterretningstjenesten skal kunne innhente informasjon om terrorisme, må den være *grenseoverskridende*. Begrepet indikerer at terroren må utgjøre en trussel som er styrt fra eller på annen måte har forbindelse til utenlandsk person, gruppe, organisasjon, stat eller forhold. Det ligger utenfor tjenestens oppgaver å bidra til å avdekke og motvirke terrorisme som foregår i de ulike statene. Dersom terrorismen kan utgjøre en trussel mot Norge eller norske interesser i utlandet, vil det imidlertid falle innenfor bestemmelsen her.

Av *bokstav g* følger det at informasjonen skal bidra til å avdekke og motvirke *spredning av masseødeleggelsesvåpen og utstyr og materiale for fremstilling av slike våpen*. Masseødeleggelsesvåpen (MØV) er en betegnelse på atomvåpen, radiologiske, biologiske og kjemiske våpen, gjerne kalt

ARBC-våpen. Hva som til enhver tid skal være å regne som MØV, må ses i lys av internasjonale konvensjoner og ikke-spredningsregimer.

Etter *bokstav h* skal informasjonen bidra til å avdekke og motvirke *internasjonal våpenhandel som kan utgjøre en alvorlig sikkerhetstrussel.* Begrepet *internasjonal våpenhandel* må forstås bredt. All handel med ethvert våpen, forutsatt at det er mellom organisasjoner eller stater, faller som utgangspunkt innenfor begrepet. Etterretningstjenesten skal imidlertid ikke innhente informasjon om enhver våpenhandel, det er et krav at våpenhandelen kan utgjøre en *alvorlig* sikkerhetstrussel mot Norge eller norske interesser. Det betyr at mer ordinær våpenhandel, for eksempel salg av håndvåpen til en kriminell organisasjon, ikke faller innenfor Etterretningstjenestens oppgaver.

Forhold som kan regnes for å utgjøre en alvorlig sikkerhetstrussel, kan være våpenhandel med en særskilt våpentype (for eksempel MØV) som i seg selv kan utgjøre en alvorlig trussel, salg av store mengder våpen til internasjonale terrororganisasjoner som utgjør en trussel mot Norge eller norske interesser i utlandet, eller våpenhandel mellom stater som gir indikasjoner på at det innføres nye kapasiteter som kan påvirke maktbalansen i en region.

I *bokstav i* slås det fast at informasjonen skal bidra til å avdekke og motvirke *eksport av sanksjonerte, listeførte eller sensitive varer og tjenester*. Det dreier seg først og fremst om varer og tjenester som er regulert av eksportkontrolloven eller i sanksjonsforskrifter i medhold av annen lovgivning, herunder lov om vedtak i FNs sikkerhetsråd og sanksjonslova.

De ulike utenlandske truslene som følger av bokstav a til i, vil i enkelte tilfeller gli over i hverandre. Våpenhandel som involverer MØV eller utstyr og materiale for fremstilling av slike våpen, vil falle innenfor bokstav g og h. Grenseoverskridende terrorisme kan være en trussel mot samfunnssikkerheten, og påvirkningsoperasjoner har en side til statssikkerheten. Det viktige er ikke hvilken bokstav trusselen faller inn under, men at trusselen ligger innenfor rammene til bestemmelsen. Det vil bero på en konkret vurdering i det enkelte tilfelle om den innhentede informasjonen faller innenfor en av de opplistede kategoriene i bokstav a til i.

Til § 3-2

Det følger av bestemmelsen at Etterretningstjenesten, i tillegg til informasjon om trusler som beskrevet i § 3-1, også skal innhente og analysere informasjon om andre utenlandske militære og sivile forhold. Hva som ligger i at tjenesten *skal* innhente og analysere informasjonen, er beskrevet nærmere i merknadene til § 3-1.

Bokstav a fastsetter at Etterretningstjenesten skal innhente og analysere informasjon om utenlandske forhold som kan bidra til *ivaretakelse av prioriterte utenriks-, forsvars- eller sikkerhetspolitiske interesser knyttet til forhold og utviklingstrekk i andre stater og regioner*. Bestemmelsen har to hovedelementer. For det første må informasjonen knytte seg til forhold eller utviklingstrekk i andre stater og regioner. For det andre må den antas å ha relevans for Norges utenriks-, forsvars- eller sikkerhetspolitiske interesser. Det følger av dette at informasjonen for eksempel må kunne bidra til å gi situasjonsforståelse i land og regioner som er viktige for Norge. Det kan være nordområdene, sentrale konfliktområder eller områder som Norge har større økonomiske interesser i. Informasjonen vil blant annet kunne dreie seg om de politiske forholdene, migrasjonsutfordringer eller utvikling av militære eller andre kapasiteter som ikke har manifestert seg som en trussel.

At informasjonen må kunne bidra til *ivaretakelse* av disse interessene, innebærer at den må ha en viss relevans for interessene, men likevel ikke slik at det stilles høyere krav enn det som følger av grunnvilkårene for innhenting i kapittel 5.

Det er kun *prioriterte* interesser som faller innenfor Etterretningstjenestens oppgaver. Dette innebærer en begrensning i *hva* tjenesten kan innhente informasjon om. Kravet må, i likhet med § 3-1, ses i lys av § 2-2 om oppdragsstyring og prioriteringsdokumentet for nasjonale etterretningsbehov. Det er departementet som koordinerer norske myndigheters etterretningsbehov og styrer hva tjenesten skal innhente informasjon om.

Etter *bokstav b* skal Etterretningstjenesten innhente informasjon som kan bidra til *nasjonal beredskapsplanlegging*. Dette omfatter informasjon som bidrar til at den nasjonale beredskapen til enhver tid kan tilpasses det gjeldende trussel- og risikobildet. Det vil blant annet være informasjon som bidrar til utforming av nasjonalt og alliert operativt planverk, og informasjon for å gjøre nødvendige tilpasninger i styrkeoppbyggingssystemet og nasjonalt beredskapssystem.

Det følger av *bokstav c* at Etterretningstjenesten skal innhente informasjon som kan bidra til *episode- og krisehåndtering*. I den lavere enden av krisespekteret kan det for eksempel være tale om informasjon om grensekrenkelser eller lignende som kan kreve diplomatisk håndtering. Det

vil også være nødvendig å innhente informasjon som bidrar til å danne et normalbilde i norske interesseområder.

Det følger av *bokstav d* at informasjonen skal bidra til *planlegging og gjennomføring av nasjonale eller internasjonale militære operasjoner*. Det vil først og fremst være informasjon som gir norske styrker et oppdatert bilde av de faktiske forhold der operasjonen finner sted, enten det er nasjonalt eller internasjonalt. Videre vil det være snakk om informasjon som danner utgangspunkt for etterretningsvurderinger av kapasiteter og metoder som de militære styrkene kan stå overfor. Lovens virkeområde er i § 1-2 andre ledd avgrenset mot informasjonsinnhenting som ledd i en internasjonal operasjon med folkerettslig mandat, men bestemmelsen kan være relevant i planleggingsfasen.

Til § 3-3

Første ledd viderefører gjeldende lov § 3 tredje ledd. Bestemmelsen fastslår at tjenesten skal ivareta evne til å *innhente og formidle* informasjon i tilfeller hvor hele eller deler av Norge okkuperes. Det innebærer at Etterretningstjenesten utarbeider og vedlikeholder beredskapsplanverk og trener og øver på dette oppdraget.

Etter *andre ledd* skal Etterretningstjenesten holde departementet *generelt orientert* om organisering og planlegging av okkupasjonsberedskapen. Det er tilstrekkelig at tjenesten gir en overordnet orientering om temaet, slik at departementet kan kontrollere at oppgaven gjennomføres uten at det går på bekostning av de spesielt strenge kravene til skjerming som okkupasjonsberedskapen forutsetter.

Til § 3-4

Bestemmelsen åpner for at Etterretningstjenesten kan innhente og analysere informasjon om forhold som nevnt i §§ 3-1 og 3-2 dersom det antas å være av vesentlig betydning for det bi- eller multilaterale etterretningssamarbeidet og er i norsk interesse. Dette innebærer at Etterretningstjenesten kan innhente informasjon som vil være relevant for andre land, uten at det har direkte etterretningsrelevans for Norge. Forutsetningen er at det bidrar til å etablere og opprettholde etterretningssamarbeid som er viktig for Norge.

Bestemmelsen må ses i sammenheng med vilkårene for å dele opplysninger med andre lands samarbeidende tjenester i lovforslaget kapittel 10.

Til § 3-5

Bestemmelsen gir hjemmel for å innhente informasjon som utgjør et nødvendig grunnlag for å kunne innhente relevant informasjon (evneinformasjon). Det kan for eksempel være nødvendig å innhente informasjon om sikkerhetssituasjonen 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 tjenestens evne til å innhente informasjon på en trygg, målrettet og sikkerhetsmessig forsvarlig måte. Et annet eksempel kan være innhenting av informasjon om hvordan et informasjonssystem er bygget opp eller om signalmiljøet i et område, for å forstå hvordan man kan få tilgang 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.

Til kapittel 4

Til § 4-1

Bestemmelsen fastsetter i *første ledd* et forbud for Etterretningstjenesten mot å benytte metoder for innhenting av informasjon etter kapittel 6 overfor personer i Norge. Med «personer» forstås både fysiske og juridiske personer.

Formålet med forbudet er å begrense Etterretningstjenestens adgang til å innhente informasjon om personer i Norge (den territorielle begrensningen). Det vises til punkt 8.3 for en nærmere redegjørelse for behovet for en slik begrensning. Forbudet viderefører gjeldende rett, men oppstiller et klarere avgrensningskriterium. Det oppstilles ingen skjønnsmessige vilkår som krav om overvåkningshensikt eller lignende.

At forbudet er knyttet til bruk av innhentingsmetoder etter kapittel 6, innebærer at det avgjørende for om bestemmelsen kommer til anvendelse, er om innhentingen skjer med en metode som nevnt i kapittel 6. Kapittel 6 regulerer Etterretningstjenestens systematiske innhentingsvirksomhet ved bruk av menneskebaserte og tekniske fremgangsmåter. Metodene er nærmere omtalt i merknadene til den enkelte bestemmelse.

Innhentingsmetodene i kapittel 6 omfatter ikke alle måter Etterretningstjenesten kan komme i besittelse av informasjon på. Tjenesten kan for det første motta informasjon fra andre i form av tips og lignende. Tips fra publikum kan være en viktig informasjonskilde. Mottak av slik informasjon kan ikke med rimelighet omtales som en «innhentingsmetode», og er derfor ikke regulert i kapittel 6. Denne måten å komme i besittelse av informasjon på dekkes følgelig ikke av forbudet i første ledd mot innhenting i Norge. Informasjon som mottas innenfor rammen av et kildeforhold, regnes derimot som menneskebasert innhenting etter § 6-3, slik at forbudet i første ledd får anvendelse.

Forbudet i første ledd er heller ikke til hinder for at Etterretningstjenesten mottar informasjon om norske personer innenfor rammen av informasjonsutveksling med nasjonale og internasjonale partnere, slik dette er regulert i kapittel 10.

Informasjonsinnhenting fra åpne kilder reguleres av §§ 6-2 og 4-4. I henhold til den territorielle begrensningen er det – med noen unntak – PST som har ansvar for og adgang til innhenting av informasjon om personer i Norge. Unntaket etter § 4-4, som gir Etterretningstjenesten adgang til å innhente informasjon om utenlandske forhold fra åpne kilder selv om informasjonen er publisert av eller på annen måte berører personer i Norge, skal forstås i lys av dette.

Det presiseres at tilrettelagt innhenting, som reguleres i kapittel 7 og 8, regnes som en form for midtpunktinnhenting etter § 6-9. Tilrettelagt innhenting omfattes derfor som et utgangspunkt av innhentingsforbudet. Presiseringen i § 4-7 kommer imidlertid til anvendelse, slik at tilrettelagt innhenting overfor utenlandske etterretningsmål kan gjennomføres selv om den innhentede informasjonen vil omfatte overskuddsinformasjon om personer i Norge.

Bestemmelsen er ikke til hinder for at innhenting rettet mot mål i utlandet, gjennomføres fra Norge. For eksempel kan tekniske innhentingskapasiteter, som å følge fremmede undervannsbåter til havs, opereres fra installasjoner på norsk territorium. Det understrekes også for ordens skyld at innhentet informasjon kan bearbeides og analyseres i Norge.

Med *Norge* menes norsk territorium, som omfatter Fastlands-Norge, Svalbard, Jan Mayen og bilandene. Begrepet inkluderer territorialfarvannet (sjøterritoriet og de indre farvann) og luftterritoriet.

Regler om behandling av informasjon som Etterretningstjenesten kommer i besittelse av, følger av kapittel 9. Kapittel 9 regulerer behandling av personopplysninger *etter innhenting*. Opplysninger om norske personer som Etterretningstjenesten lovlig besitter, kan behandles etter kapittel 9 så fremt behandlingsvilkårene i det kapittelet er oppfylt.

Det kan i enkelte tilfeller være uklart om en person er i Norge eller i utlandet. I slike tilfeller følger det av *andre ledd* at Etterretningstjenesten skal søke å avklare forholdet. Til dette formålet kan det bare brukes informasjon fra norske myndigheter eller utenlandske samarbeidspartnere, åpne kilder eller egen innhenting i utlandet. Informasjonen kan være informasjon som Etterretningstjenesten allerede besitter, eller informasjon som hentes inn fra nevnte kilder for dette formålet.

Tjenesten må legge til grunn det faktum som fremstår som mest sannsynlig. Det er ikke tilstrekkelig at tjenesten har *søkt* å avklare om personen er i Norge uten å lykkes i å etablere en sannsynlighetsovervekt i den ene eller andre retningen. Tjenesten må avstå fra innhenting dersom man ikke lykkes i å etablere sannsynlighetsovervekt for at personen er i utlandet.

Det fastsettes enkelte unntak fra innhentingsforbudet i §§ 4-2, 4-4, 4-5 og 4-6.

Til § 4-2

Bestemmelsen fastsetter et unntak fra § 4-1 for fremmed statsaktivitet i Norge.

Etter *første ledd* kan Etterretningstjenesten uten hinder av forbudet etter § 4-1 benytte innhentingsmetoder etter kapittel 6 overfor utenlandske og statsløse personer i Norge som opptrer på vegne av fremmed stat eller statslignende aktør.

Bestemmelsen skiller ikke mellom de ulike metodene i kapittel 6, men metodens karakter vil være et viktig moment i forholdsmessighetsvurderingen som må foretas etter lovforslaget § 5-4. Etter § 5-4 skal det vurderes om mindre inngripende tiltak i tilstrekkelig grad kan ivareta formålet, inngrepets virkning for den som rammes, sakens betydning og forholdene ellers. Ved informasjonsinnhenting i Norge må det særlig legges vekt på hvorvidt og hvordan innhentingen vil kunne berøre tredjepart.

Med *statslignende aktør* menes en entitet som rettslig sett ikke oppfyller alle de fire folkerettslige kravene til å være en stat, men som i praksis utøver statslignende funksjoner i en slik grad at det er naturlig å sammenligne den med en stat. Terskelen for å være en statslignende aktør vil følgelig ligge høyt.

Unntaket gjelder bare for utenlandske og statsløse personer. Dette innebærer at det ikke kan innhentes informasjon om norske statsborgere som handler på vegne av en fremmed stat eller statslignende aktør, selv om personen også har utenlandsk statsborgerskap.

Med *personer* forstås både fysiske og juridiske personer. Det må avgjøres konkret hvorvidt en virksomhet skal anses som norsk eller utenlandsk. Hvis virksomheten er registrert i Norge eller utøver virksomhet fra forretningssted i Norge, må den normalt regnes som norsk.

I vurderingen av hvorvidt personen opptrer *på vegne av* fremmed stat eller statslignende aktør, må det ses hen til folkerettslige regler om statsansvar. En handling vil normalt regnes som utført på vegne av en stat når den er utført av personer som handlet på bakgrunn av direkte instruksjoner fra eller under ledelse eller effektiv kontroll av staten.

Dersom det er tvil om en person opptrer på vegne av en fremmed stat eller statslignende aktør, følger det av *andre ledd* at Etterretningstjenesten skal søke å avklare forholdet. For dette formålet skal det kun brukes informasjon fra norske myndigheter, utenlandske samarbeidspartnere, åpne kilder eller egen innhenting i utlandet. Informasjonen kan være informasjon som Etterretningstjenesten allerede besitter, eller informasjon som hentes inn fra nevnte kilder for dette formålet. Tjenesten må legge til grunn det faktum som fremstår som mest sannsynlig. Det må etableres sannsynlighetsovervekt for at personen handler på vegne av en stat eller statslignende aktør for at innhenting etter første ledd kan finne sted. Etableres det ikke sannsynlighetsovervekt, må tjenesten avstå fra innhentingen.

Tredje ledd fastsetter at når riket er i krig eller krig truer eller rikets selvstendighet eller sikkerhet er i fare, kan Kongen bestemme at Etterretningstjenesten uten hinder av § 4-1 kan innhente enhver opplysning som har betydning for Forsvarets evne til å håndtere fiendtlig militær aktivitet.

Terskelkriteriene *i krig eller når krig truer eller når rikets selvstendighet eller sikkerhet står i fare* tilsvarer kriteriene i beredskapsloven § 3 og annen beredskapslovgivning. Det vises til NOU 1995: 31 punkt 4.5.5 side 50 følgende. På samme måte som i beredskapsloven § 3, er terskelkriteriene knyttet til fiendtlig aktivitet på norsk territorium. At Norge deltar med militære kapasiteter i en væpnet konflikt utenfor norsk territorium, er ikke tilstrekkelig til å oppfylle kriteriene.

Gitt vurderingens viktighet er det Kongen som avgjør når terskelkriteriene er oppfylt, på samme måte som i annen beredskapslovgivning.

Med *enhver opplysning* menes også opplysninger om norske personer og virksomheter. Det oppstilles en materiell begrensning ved at opplysningene som innhentes må ha betydning for å håndtere fiendtlig militær aktivitet.

Til § 4-3

Bestemmelsen regulerer samordning med Politiets sikkerhetstjeneste ved innhenting på norsk territorium etter § 4-2 første ledd.

Både Etterretningstjenesten og Politiets sikkerhetstjeneste (PST) har oppgaver knyttet til å motvirke utenlandske trusler mot Norge. Innenfor rammen av politiloven § 17 b har PST hovedansvaret for å innhente informasjon om slike trusler på norsk territorium, men i de tilfellene som er nevnt i § 4-2 (fremmed statsaktivitet i Norge) kan også Etterretningstjenesten innhente informasjon på norsk territorium. De to tjenestene må i slike tilfeller samordne virksomheten for å unngå etterretningssvikt, ivareta operasjonssikkerhet og legge til rette for hensiktsmessig bruk av samfunnets ressurser.

Det følger av *første punktum* at Etterretningstjenesten, når den skal innhente informasjon om fremmed statsaktivitet i Norge i samsvar med § 4-2 første ledd, må be PST om samtykke til innhentingen dersom den gjelder forhold som også dekkes av oppgavebeskrivelsen i politiloven § 17 b første ledd. Avslag vil normalt bare være aktuelt dersom PST allerede innhenter informasjon om det aktuelle etterretningsmålet, og det kan virke forstyrrende på operasjonen med Etterretningstjenestens inntreden. PST skal derimot ikke overprøve Etterretningstjenestens vurdering av det rettslige grunnlaget for innhentingen og hvorvidt innhenting er nødvendig og hensiktsmessig for å løse Etterretningstjenestens oppgaver. Departementet legger til grunn at tjenestene etablerer prosedyrer som sikrer en hurtig avklaring av samtykkeanmodninger. Hvis tjenestene i en konkret sak ikke skulle bli enige, må uenigheten løses av de overordnede departementene på vanlig måte.

Samtykkekravet gjelder i alle saker hvor Etterretningstjenesten, i samsvar med unntaket i § 4-2 første ledd, kan bruke metoder etter kapittel 6 overfor personer i Norge som opptrer på vegne av fremmed stat eller statslignende aktør, og den aktuelle statsaktiviteten er av en karakter som gjør at forholdet også omfattes av beskrivelsen av oppgavene til PST i politiloven § 17 b første ledd. Kravet antas å være mest praktisk med hensyn til fremmede staters ulovlige etterretningsvirksomhet i Norge, jf. politiloven § 17 b første ledd nr. 2,

men innhenting om fremmed statsaktivitet som dekkes av andre alternativer i bestemmelsen kan også være aktuelt. Forutsetningen er i alle tilfeller at det er tale om et forhold som dekkes av Etterretningstjenestens oppgavebeskrivelse i kapittel 3, det vil si at det må være tale om utenlandske forhold.

Hvis innhentingen gjelder forhold som ikke faller inn under en av oppgavene til PST etter politiloven § 17 b første ledd, kreves det ikke samtykke. Etterretningstjenesten skal like fullt informere PST om innhentingen, jf. *andre punktum*. Formålet med denne plikten er å sikre samordning av virksomheten på norsk territorium og ivareta operasjonssikkerhet. Informasjonen bør normalt gis skriftlig og i så god tid som mulig før operasjonen, slik at PST gis anledning til å gjøre gjeldende at det dreier seg om en sak som krever samtykke etter første ledd. Uenighet mellom tjenestene på dette punktet må løses av de overordnede departementene på vanlig måte. I hastetilfeller kan informasjonen gis muntlig, men av hensyn til notoritet skal den i så fall snarest mulig nedtegnes.

Samordningsplikten er begrenset til innhenting etter § 4-2 første ledd. Av hensyn til det folkerettslige distinksjonsprinsippet oppstilles det ingen lovpålagt samordningsplikt for innhenting i beredskapssituasjoner etter § 4-2 tredje ledd. Det presiseres at det også gjelder en plikt til samordning etter instruks om samarbeidet mellom Etterretningstjenesten og Politiets sikkerhetstjeneste § 8. Plikten i instruksen vil i en beredskapssituasjon fremdeles gjelde, men folkerettslige regler vil kunne ha betydning for hvor langt plikten rekker.

Til § 4-4

Bestemmelsen utgjør et unntak fra § 4-1 gjennom å fastslå at Etterretningstjenesten kan innhente informasjon om utenlandske forhold fra åpne kilder etter § 6-2 selv om informasjonen er publisert av eller på annen måte berører personer i Norge. Det vises til merknadene til § 6-2 når det gjelder åpne kilder som metode og grensedragningen mot andre metoder. Paragraf 4-4 er ikke en hjemmel for innhenting av informasjon, men et unntak fra forbudet i § 4-1. Uten et slikt unntak ville Etterretningstjenesten ikke kunne ha befatning med åpent tilgjengelig informasjon som er publisert av eller berører personer i Norge, fordi innhenting fra åpne kilder er en metode etter kapittel 6, og dermed omfattet av forbudet i § 4-1.

Det kan innhentes informasjon fra åpne kilder i en målsøkingsfase, der inngangsverdier knyttet til personer eller virksomheter i Norge benyttes for å frembringe informasjon om etterretningsrelevante utenlandske forhold. For eksempel vil det være behov for å gjøre søk i åpne kilder, slik som i selskapsregistre, for å avdekke utenlandske eierskapskjeder knyttet til et selskap i Norge for å avdekke om fremmede trusselaktører driver strategiske oppkjøp eller investeringer.

Det presiseres at innhenting av informasjon fra åpne kilder, som all annen innhenting av informasjon, må være begrunnet i Etterretningstjenestens oppgaver etter lovforslaget kapittel 3, det vil si at det må dreie seg om utenlandske forhold. Det vil imidlertid ikke være i strid med bestemmelsene at Etterretningstjenesten registrerer hvilket nettsted den relevante informasjonen fremgår av eller hvilken norsk person som har publisert informasjonen, dersom dette er nødvendig for å kunne vurdere informasjonens kvalitet eller av andre grunner vurderes som relevant og nødvendig kontekstinformasjon.

Til § 4-5

Bestemmelsen regulerer kilderekruttering og kildeverifikasjon i Norge.

Etter *første ledd* kan Etterretningstjenesten uten hinder av § 4-1 innhente informasjon om personer i Norge for å finne, rekruttere og verifisere kilder. En *kilde* er en fysisk person som kultiveres, rekrutteres og føres av Etterretningstjenesten for å gjennomføre eller tilrettelegge for menneskebasert innhenting. En organisasjon eller et miljø kan regnes som kilde inntil relevante fysiske enkeltpersoner innenfor organisasjonen eller miljøet er identifisert. Det vises til merknadene til § 6-3 for en nærmere beskrivelse.

Kilder kan være norske eller utenlandske statsborgere, som kan oppholde seg på norsk eller utenlandsk territorium.

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 for å fastslå motivasjon, troverdighet og egnethet.

Hvilke innhentingsmetoder som kan benyttes i Norge, reguleres i *andre ledd*. Som hovedregel skal informasjonen innhentes fra åpne kilder eller ved utlevering fra norske myndigheter, jf. andre ledd *første punktum*. Det kan imidlertid brukes metoder som nevnt i § 6-3 (menneskebasert innhenting) og § 6-4 (systematisk observasjon) hvis det foreligger tungtveiende sikkerhetsmessige grunner. Andre metoder som nevnt i kapittel 6

kan ikke brukes for kilderekruttering og kildeverifikasjon i Norge.

Med *tungtveiende sikkerhetsmessige grunner* siktes det særlig til situasjoner hvor Etterretningstjenesten tilnærmer seg en person eller et miljø som kan utgjøre en trussel mot tjenestepersoners eller oppdragstakeres liv og helse, hvor en åpen tilnærming kan kompromittere tjenestepersoner eller oppdragstakere på en måte som kan vanskeliggjøre tjenestens arbeid i fremtiden, eller der det kan være grunn til å undersøke om kilden i realiteten opptrer på vegne av annen stats etterretnings- eller sikkerhetstjeneste eller på annen måte ikke er den som personen utgir seg for å være.

Som ved all annen metodebruk må det foretas en forholdsmessighetsvurdering i tråd med § 5-4. Det vises til merknadene til den bestemmelsen. Det følger dessuten av *tredje ledd første punktum* at det ikke skal innhentes mer informasjon enn *strengt nødvendig*. Dette innebærer et skjerpet krav med hensyn til hvor lenge innhentingen kan pågå og hvor omfattende undersøkelsene kan være. Det er ikke mulig å oppstille presise grenser, men det legges til grunn at innhenting kun skal foregå i en begrenset innledende fase forut for eventuell åpen kontakt. For verifikasjon av etablerte (rekrutterte) kilder skal innhenting skje kun så lenge sikkerhetsmessige forhold åpenbart krever det, og ellers bare dersom omstendighetene konkret og klart krever det.

Det fremgår av tredje ledd *andre punktum* at innhentede opplysninger *utelukkende* skal brukes for å finne, rekruttere og verifisere kilder. Opplysninger som er innhentet for disse formål, kan ikke behandles for andre formål, og personopplysninger skal slettes når det ikke er nødvendig å behandle opplysningene, jf. § 9-8 første ledd. Utlevering som ledd i kildesamarbeid med samarbeidende tjenester anses som samme formål. For det tilfelle at en kilde ikke ønsker å samarbeide med Etterretningstjenesten, kan opplysninger om kilden behandles for å hindre at vedkommende kontaktes igjen. Det skal i så fall ikke registreres flere opplysninger enn det som er strengt nødvendig for dette formålet.

Til § 4-6

Bestemmelsen gir i en viss utstrekning hjemmel for innhenting i Norge i forbindelse med trening, øving og testing av utstyr.

Trening foregår normalt på enkeltpersonnivå eller i mindre grupper, mens øving innebærer større simulerte operasjoner. Det kan ikke trekkes noe klart skille mellom begrepene. Med *utstyr* menes alt utstyr som Etterretningstjenesten benytter i forbindelse med gjennomføring av etterretningsvirksomhet. Det er ikke avgjørende hvorvidt utstyret kan karakteriseres som innhentingsutstyr.

Innhentingen må være *strengt nødvendig* for å trene, øve og teste utstyr. I prinsippet vil enhver innhentingsmetode kunne benyttes, men på grunn av det strenge nødvendighetskravet går det en grense for hvilke inngripende metoder som kan brukes mot uvitende tredjepersoner i Norge. Departementet legger for eksempel til grunn at testing av utstyr for endepunktinnhenting mot uvitende tredjepersoner i Norge neppe kan regnes som strengt nødvendig. Det må vurderes nøye hvorvidt formålet kan oppnås på en annen måte enn ved innhenting i Norge. Det bør sikres at innhentingen berører minst mulig antall personer, og det bør unngås å innhente sensitive personopplysninger.

Det følger av *andre ledd* at informasjonen *utelukkende* skal brukes til å trene, øve og teste utstyr. Dette innebærer at informasjonen ikke kan brukes til etterretningsproduksjon eller til andre formål, eller deles med andre. Med mindre den som opplysningene gjelder, samtykker til at opplysningene behandles videre for trenings-, øvings- og testformål, skal de slettes snarest mulig, og senest når treningen, øvingen eller testingen avsluttes. Dette er et strengere krav enn det som ellers ville ha fulgt av § 9-8 om sletting av personopplysninger. Informasjonen skal heller ikke arkiveres etter arkivlova.

Til § 4-7

Bestemmelsen er en presisering av hovedregelen i § 4-1. Innhenting av informasjon om etterretningsmål i utlandet vil kunne medføre at det også avdekkes informasjon om personer i Norge. Informasjon som følger med annen innhenting, betegnes *aksessorisk informasjon*. Hensikten med bestemmelsen er å slå fast at dersom det følger med informasjon om personer i Norge, gjør ikke dette ellers lovlig innhenting i utlandet ulovlig. Bestemmelsen er ikke i seg selv en innhentingshjemmel, men forutsetter at lovens vilkår for øvrig er oppfylt. Det presiseres for ordens skyld at Etterretningstjenesten også vil kunne få befatning med informasjon om personer i Norge i tilfeller hvor tjenesten unntaksvis kan bruke innhentingsmetoder overfor personer i Norge, for eksempel etter § 4-2.

At aksessorisk informasjon kommer Etterretningstjenesten i hende, kan være tilsiktet eller

utilsiktet. For eksempel vil det være tilsiktet å avdekke informasjon om fremmede etterretningstjenesters kommunikasjon med operatører og agenter i Norge, eller et internasjonalt terrornettverks kommunikasjon med medlemmer i Norge. Det vil også være tilsiktet å avdekke hvilke norske virksomheter en fremmed aktør planlegger å gjennomføre cybersabotasje mot. Slik informasjon er etterretningsrelevant, og vil kunne behandles av Etterretningstjenesten i tråd med reglene i kapittel 9 og deles med andre norske myndigheter i tråd med reglene i kapittel 10. Departementet presiserer at innhentingen alltid må være rettet mot den utenlandske enden av den grenseoverskridende kommunikasjonen, med mindre en av unntaksbestemmelsene i kapittel 4 kommer til anvendelse, slik som § 4-2 første ledd om fremmed statsaktivitet i Norge.

Informasjon om norske personer kan også være informasjon som er uten interesse for etterretningsformål (overskuddsinformasjon). Innhenting av slik informasjon vil være en utilsiktet konsekvens av informasjonsinnhenting om etterretningsmål i utlandet, typisk ved innhenting av rådata i bulk. For eksempel innebærer innhenting av metadata i bulk etter § 7-7 innhenting av store mengder metadata om norsk innenlandsk kommunikasjon. Det foreslås derfor strenge regler om tilgang til og behandling av slik informasjon i kapittel 7. Det presiseres i *andre ledd* at rådata i bulk kan innhentes selv om informasjon om personer i Norge vil kunne følge med i rådatagrunnlaget.

Til § 4-8

Etter *første ledd* skal Etterretningstjenesten ikke innhente eller medvirke til å innhente informasjon med formål å utføre oppgaver som tilligger politiet eller andre rettshåndhevende myndigheter. Politiets oppgaver følger særlig av politiloven, men kan også være regulert i spesiallovgivning. Med «andre rettshåndhevende myndigheter» menes andre norske eller utenlandske offentlige myndigheter som har til oppgave å håndheve lovgivning overfor befolkningen, og som har håndhevelsesmyndighet, ofte med maktmidler, til rådighet.

Bestemmelsen er utelukkende ment å ha en pedagogisk funksjon ved siden av den positive angivelsen av Etterretningstjenestens oppgaver i kapittel 3. Den innebærer ingen endringer i gjeldende oppgavefordeling eller samarbeidsformer mellom Etterretningstjenesten, Politiets sikkerhetstjeneste, det øvrige politi og andre myndigheter.

Andre ledd presiserer at regelen i første ledd ikke er til hinder for utveksling av informasjon etter kapittel 10 eller bistand til politiet i medhold av § 10-7, jf. politiloven § 27 a.

Til § 4-9

Det følger av bestemmelsen at Etterretningstjenesten ikke skal innhente eller medvirke til å innhente, bearbeide eller utlevere informasjon med formål å gi selskaper eller andre kommersielle virksomheter eller sektorer konkurransemessige fortrinn. Ordlyden bygger på tilsvarende ordlyd i bilaterale avtaler og internasjonale uttalelser om forbud mot industrispionasje. Begrepet *konkurransemessige fortrinn* må forstås i en kommersiell kontekst, og ikke for eksempel i en statsvitenskapelig kontekst.

Bestemmelsen vil ikke hindre at det innhentes informasjon i den hensikt å avdekke og motvirke cyberangrep eller lignende trusler mot kommersielle virksomheter som for eksempel besitter kritisk infrastruktur, selv om innhentingen indirekte skulle føre til at virksomheten sparer ressurser eller på annen måte unngår kostnader som rammer andre kommersielle virksomheter.

Til § 5-1

Bestemmelsen regulerer grunnvilkåret for målsøking.

Målsøking er «systematisk arbeid for å identifisere nye etterretningsmål», jf. definisjonen i § 1-3 bokstav e. Målsøking kan gjennomføres ved innhenting av informasjon gjennom for eksempel åpne kilder, avlytting, bildeovervåking eller teknisk sporing, eller ved søk i informasjon som allerede er samlet inn, for eksempel rådata i bulk. Søk i lagrede metadata som er innhentet i tråd med reglene i kapittel 7 om tilrettelagt innhenting, krever rettens godkjennelse etter reglene i kapittel 8.

Målsøking skal ikke være vilkårlig eller basert på ren magefølelse. Samtidig kan det på dette stadiet ikke oppstilles en for høy terskel. Bestemmelsen oppstiller derfor som vilkår at det må være *grunn til å undersøke* om innhenting kan frembringe informasjon som er relevant for etterretningsformål. Vilkåret innebærer at Etterretningstjenesten må kunne vise til et holdepunkt eller en erfaringsbasert hypotese som tilsier at målsøkingsprosessen kan frembringe informasjon som er relevant for etterretningsformål. Det følger av dette at målsøket er *formålsbegrenset*. Det vises i denne forbindelse til angivelsen av Etterretningstjenestens oppgaver i kapittel 3.

Hva som gir «grunn til å undersøke», vil variere fra sak til sak. På kontraterrorområdet kan det for eksempel være kontaktlisten til et medlem av et terrornettverk. Kontaktlisten kan brukes som utgangspunkt for å identifisere andre, ukjente medlemmer av samme nettverk. På cyberområdet kan det for eksempel være informasjon om utstyr som brukes til angrep i det digitale rom, som kan brukes som utgangspunkt for å identifisere personer eller organisasjoner som bruker utstyret. I motsetning til målrettet innhenting stilles det derimot ikke krav til at det foreligger konkrete holdepunkter som underbygger søket. På målsøkingsstadiet vil det kunne være «grunn til å undersøke» på bakgrunn av en begrunnet hypotese, for eksempel med bakgrunn i erfaring om handlingsmønstre som typisk kan knyttes til en trusselaktør.

Vilkåret «grunn til å undersøke» innebærer også at det må være en viss sannsynlighet for at innhentingen vil kunne frembringe relevant informasjon. Det er tilstrekkelig at sannsynligheten for å finne etterretningsrelevant informasjon er i området 10 til 40 %. Det bemerkes at graden av sannsynlighet også vil kunne ha betydning i vurderingen av innhentingens forholdsmessighet, jf. § 5-4, i den forstand at det kan aksepteres sterkere inngrep jo større sannsynligheten er for å finne relevant informasjon.

Bestemmelsen må leses i sammenheng med *diskrimineringsforbudet* som følger av § 9-4. Dette innebærer at målsøking ikke kan iverksettes utelukkende på bakgrunn av en persons etnisitet eller nasjonale bakgrunn, politiske, religiøse eller filosofiske overbevisning, språk, politiske virksomhet, fagforeningstilhørighet eller helsemessige eller seksuelle forhold.

Selv om grunnvilkåret for målsøking er oppfylt, kan innhenting ikke finne sted dersom det vil være et *uforholdsmessig inngrep* overfor den enkelte. Dette følger av § 5-4. Enkelte metoder kan bare brukes dersom det er «strengt nødvendig», noe som innebærer en strengere forholdsmessighetsvurdering. Innhenting kan heller ikke finne sted dersom det strider mot forbud som følger av kapittel 4, for eksempel forbudet mot å bruke inngripende metoder overfor personer i Norge.

Til § 5-2

Bestemmelsen regulerer grunnvilkåret for målrettet innhenting.

Målrettet innhenting er «systematisk arbeid for å finne informasjon knyttet til identifiserte etterretningsmål», jf. definisjonen i § 1-3 bokstav f. Arbeidet gjennomføres ofte på samme måte som målsøking, det vil si ved bruk av metoder for innhenting av informasjon eller søk i innhentet informasjon, for eksempel rådata i bulk. Prosessen er imidlertid som regel vesentlig mer spisset, da innhentingen er rettet mot et spesifikt mål, typisk en bestemt person eller objekt.

I likhet med det som gjelder for målsøking, er det et grunnvilkår for målrettet innhenting at det er *grunn til å undersøke* om innhenting kan frembringe informasjon som er relevant for etterretningsformål. I motsetning til det som gjelder for målsøking, oppstilles det også et krav om «konkrete holdepunkter». Dette innebærer et strengere krav til sannsynlighet for at innhentingen kan frembringe etterretningsrelevant informasjon enn det som gjelder for målsøking, men likevel ikke slik at det kreves sannsynlighetsovervekt.

Bestemmelsen må leses i sammenheng med *diskrimineringsforbudet* som følger av § 9-4. Dette innebærer at målrettet innhenting ikke kan iverksettes utelukkende på bakgrunn av en persons etnisitet eller nasjonale bakgrunn, politiske, religiøse eller filosofiske overbevisning, språk, politiske virksomhet, fagforeningstilhørighet eller helsemessige eller seksuelle forhold.

Selv om grunnvilkåret for målrettet innhenting er oppfylt, kan innhenting ikke finne sted dersom det vil være et *uforholdsmessig inngrep* overfor den enkelte. Dette følger av § 5-4. Enkelte metoder kan bare brukes dersom det er «strengt nødvendig», noe som innebærer en strengere forholdsmessighetsvurdering. Innhenting kan heller ikke finne sted dersom det strider mot forbud som følger av kapittel 4, for eksempel forbudet mot å bruke inngripende metoder overfor personer i Norge.

Til § 5-3

Bestemmelsen regulerer grunnvilkår for innhenting av og søk i rådata i bulk.

Første ledd gir Etterretningstjenesten hjemmel til å innhente rådata i bulk. Begrepene «rådata» og «bulk» er definert i § 1-3 bokstav h og i. Det vises til merknadene til § 1-3 for en nærmere beskrivelse. Rådata i bulk kan bare innhentes når det er *nødvendig* for å få tilgang til et tilstrekkelig og relevant informasjonsgrunnlag. Det innebærer at rådata i bulk ikke kan hentes inn dersom mindre inngripende alternativer vil gi tilgang til et adekvat informasjonsgrunnlag.

Det følger av *andre ledd første punktum* at søk i rådata i bulk må oppfylle grunnvilkårene som føl-

ger av §§ 5-1 og 5-2. I tillegg oppstilles det et krav til logging. Hensikten med kravet er å forhindre misbruk og legge til rette for effektiv kontroll. Andre ledd *andre punktum* fastsetter at søket ikke skal gjennomføres dersom det vil være et uforholdsmessig inngrep overfor den enkelte, jf. § 5-4.

Tredje ledd første punktum åpner for at Etterretningstjenesten unntaksvis kan benytte søkebegreper tilknyttet en person i Norge når tjenesten gjennomfører søk i rådata. Bestemmelsen forutsetter at informasjonen allerede er lovlig innhentet av tjenesten. Det avgjørende for om bestemmelsen kommer til anvendelse, er om personen befinner seg i Norge. Det vises til § 4-1 andre ledd. Det er uten betydning hvorvidt vedkommende er norsk eller utenlandsk statsborger. Med søkebegrep menes i denne sammenhengen en personselektor, det vil si en identifikator knyttet til en bestemt person eller virksomhet, for eksempel et telefonnummer, en e-postadresse eller et brukernavn på en tjeneste. At søkebegrepet må være *tilknyttet* personen, innebærer at det må være registrert på personen eller at Etterretningstjenesten på annen måte er kjent med at det brukes av vedkommende.

Søket kan bare gjennomføres dersom det er *strengt nødvendig* for å ivareta en av oppgavene nevnt i § 3-1. I henhold til § 3-1 skal tjenesten bidra til å avdekke og motvirke utenlandske trusler mot Norge. Formålet med et slikt søk vil være å finne forbindelsen mellom et utenlandsk etterretningsmål og Norge. Det er altså ikke tillatt for Etterretningstjenesten å søke med sikte på å finne informasjon om de norske kontaktene til personen i Norge eller andre innenlandske forhold. Det er de utenlandske forholdene som søket skal ta sikte på å avdekke. Hvis Etterretningstjenesten er kjent med at en person i Norge planlegger et terrorangrep i Norge, vil bestemmelsen for eksempel kunne gi tjenesten anledning til å finne ut av hvem vedkommende har kommunisert med for å identifisere trusselaktører i utlandet.

Det følger av tredje ledd *andre punktum* at begrensningen i første punktum ikke gjelder dersom personen er en utenlandsk eller statsløs person som opptrer på vegne av en fremmed stat eller statslignende aktør, jf. § 4-2 første ledd. Det vises til merknadene til § 4-2 for en nærmere beskrivelse av hvem som omfattes av unntaket.

Kravet til streng nødvendighet innebærer at det ikke vil være anledning til å benytte et søkebegrep tilknyttet en person i Norge dersom det vil være mulig å få det samme resultatet med utgangspunkt i et søkebegrep tilknyttet en person i utlandet.

Til § 5-4

Bestemmelsen fastsetter et grunnleggende forholdsmessighetsprinsipp. Den må tolkes i lys av kravet til forholdsmessighet ved inngrep i menneskerettighetene etter Grunnloven og internasjonale konvensjoner som gjelder som norsk rett etter menneskerettsloven. Det er særlig Grunnloven § 102 og EMK artikkel 8, som verner retten til respekt for privatliv, familieliv, hjem og kommunikasjon, som aktualiseres av innhenting og utlevering av etterretningsinformasjon. Etter omstendighetene kan også andre rettigheter berøres, for eksempel ytrings- og informasjonsfriheten (Grunnloven § 100 og EMK artikkel 10), religionsfriheten (Grunnloven § 16 og EMK artikkel 9) og foreningsfriheten (Grunnloven § 101 og EMK artikkel 11).

Forholdsmessighetskravet gjelder ved både innhenting og utlevering av informasjon, jf. *første punktum*. Bestemmelsen fastslår at innhenting og utlevering ikke kan gjennomføres dersom det vil være et uforholdsmessig inngrep overfor den enkelte. Dette innebærer for det første at tiltaket må være *egnet* og *nødvendig*. For det andre må det foretas en *samlet interesseavveining* av de beskyttede individuelle interessene på den ene siden, og de legitime samfunnsbehovene som begrunner inngrepet på den andre siden. Vurderingene kan i noen grad gli over i hverandre.

Andre punktum regner opp hensyn som skal tas i betraktning ved vurderingen. Det skal for det første tas hensyn til hvorvidt *mindre inngripende tiltak i tilstrekkelig grad kan ivareta formålet*. Ved innhenting av informasjon innebærer dette særlig at det må vurderes om det er mulig å benytte mindre inngripende innhentingsmetoder. For eksempel vil det være uforholdsmessig å bruke midt- eller endepunktinnhenting hvis innhenting fra åpne kilder vil være tilstrekkelig for å dekke et konkret informasjonsbehov.

Det skal for det andre tas hensyn til *inngrepets virkning for den som rammes*, med andre ord styrken av inngrepet i den beskyttede rettigheten, som retten til respekt for privatliv eller ytrings- og informasjonsfriheten. Ved innhenting av informasjon vil det ofte være sentralt hvilken metode som det er aktuelt å benytte. For enkelte spesielt inngripende metoder oppstilles det krav om at metoden i visse situasjoner bare kan benyttes dersom det er *strengt nødvendig*, se §§ 6-6 tredje punktum (gjennomsøking), 6-7 andre punktum (avlytting og bildeovervåking), 6-8 andre ledd (annen teknisk innhenting) og 6-10 andre ledd (endepunktinnhenting).

For det tredje skal det tas hensyn til *sakens betydning*. Jo mer alvorlig saken er, jo større inngrep kan aksepteres. Inngripende metodebruk vil for eksempel lettere kunne aksepteres hvis informasjonsbehovet gjelder en utenlandsk trussel mot Norge, jf. § 3-1 (for eksempel en militær trussel, et angrep i det digitale rom eller en terrorhandling) enn hvis det gjelder andre utenlandske forhold, jf. § 3-2 (for eksempel generelle utviklingstrekk i en annen stat eller region). Det vil også kunne ha betydning hvor tidskritisk saken er. Hvis det er tale om å innhente informasjon om et angrep som pågår eller antas å være nært forestående, vil dette kunne forsvare et større inngrep enn dersom det er tale om en mer langsiktig operasjon, hvor tjenesten har tid til å innrette innhentingen på minst mulig inngripende måte.

For det fjerde skal det tas hensyn til *forholdene ellers*. Dette innebærer at alle relevante hensyn i den konkrete saken kan tas i betraktning. Det kan være forhold som knytter seg til den som inngrepet retter seg mot, for eksempel hvorvidt det er en profesjonell eller organisert aktør eller ikke, og i hvilken utstrekning inngrepet vil berøre tredjepersoner. Det kan også være aktuelt å se hen til hvorvidt det kan treffes andre tiltak som reduserer negative konsekvenser av inngrepet.

Kravet til forholdsmessighet ved innhenting av informasjon må ses i sammenheng med § 6-13 første ledd bokstav c, som fastslår at en beslutning om metodebruk skal angi det faktiske og rettslige grunnlaget for innhentingen. Denne bestemmelsen innebærer et krav til å redegjøre for vurderingen av tiltakets forholdsmessighet. Et tilsvarende krav gjelder for begjæring om tilrettelagt innhenting etter § 8-2 bokstav b.

Til kapittel 6

Til § 6-1

Det følger av *første ledd* at Etterretningstjenesten kan benytte metoder for innhenting av informasjon i samsvar med bestemmelsene i kapittel 6. Metodene kan bare brukes «for etterretningsformål», det vil si at innhentingen må begrunnes i en av tjenestens oppgaver etter kapittel 3. Regler om oppdragsstyring er gitt i § 2-2. Se også § 4-8, som fastsetter et uttrykkelig forbud mot å innhente informasjon med formål å utføre oppgaver som tilligger politiet eller andre rettshåndhevende myndigheter.

Av pedagogiske grunner fremgår det av bestemmelsen at metodene bare kan brukes når grunnvilkårene etter kapittel 5 er oppfylt og innhenting ikke strider mot loven for øvrig. En sentral begrensning følger av forbudet i § 4-1 mot å bruke innhentingsmetoder etter kapittel 6 overfor personer i Norge. Dette innebærer at metodene i kapittel 6 bare kan brukes overfor personer i utlandet, med mindre et av unntakene i kapittel 4 kommer til anvendelse, for eksempel ved fremmed statsaktivitet i Norge.

Etter *andre ledd* kan metoder etter kapittel 6 brukes fordekt overfor personer som er gjenstand for eller på annen måte berøres av dem. At metoden brukes fordekt, innebærer at det treffes tiltak for å skjule den overfor målet. Fordekt metodebruk er en sentral forutsetning for Etterretningstjenestens virksomhet. Regler om virkemidler for å skjerme ansatte, kilder, kapasiteter, metoder og operasjoner er gitt i § 11-4.

Tredje ledd fastsetter av pedagogiske grunner at bruk av en metode skal avsluttes dersom det blir klart at vilkårene ikke lenger er til stede. Det kan for eksempel være fordi endrede faktiske omstendigheter gjør at bruk av metoden ikke lenger er forholdsmessig.

Til § 6-2

Bestemmelsen fastslår i *første punktum* at Etterretningstjenesten kan innhente åpent tilgjengelig informasjon (informasjon fra åpne kilder). Innhenting av informasjon fra åpne kilder faller normalt innenfor den alminnelige handlefriheten, og krever ikke hjemmel i lov. Etter omstendighetene kan innhenting fra åpne kilder om en bestemt person likevel få et slikt omfang at det kan reises spørsmål om den utgjør et inngrep overfor vedkommende. For å unngå tvil om lovligheten av metoden foreslås det derfor å lovfeste den.

Det er ikke avgjørende hvor eller på hvilken måte informasjonen er gjort åpent tilgjengelig. Det kan typisk være informasjon som er publisert på Internett, for eksempel på et sosialt medium eller et annet nettsted. Andre eksempler er informasjon som er publisert i kringkastingsmedier, åpne registre eller i trykte bøker, aviser og tidsskrifter.

Andre punktum fastsetter i hvilke tilfeller informasjon *ikke* regnes som åpent tilgjengelig. For det første regnes informasjon ikke som åpent tilgjengelig hvis tilgang til den krever aktiv fordekt opptreden, for eksempel ved at en tjenesteperson utgir seg for å være en annen, ikke-fiktiv person og gjennom samhandling med mennesker oppnår tilgang til for eksempel et forum på Internett. I så fall vil det være menneskebasert innhenting etter § 6-3. Det regnes derimot ikke som aktiv fordekt

opptreden hvis Etterretningstjenesten, gjennom en fiktiv bruker, opptrer med normal aktivitet for å få eller opprettholde tilgang til for eksempel et forum eller gruppe på et nettsamfunn. Hvis slik aktivitet antar karakter av manipulasjon, vil det derimot være menneskebasert innhenting etter § 6-3. Det er ikke aktiv fordekt opptreden å betale vederlag for tilgang til informasjon som tilbys til allmennheten.

Informasjon regnes heller ikke som åpent tilgjengelig hvis tilgang til den krever forsering av passord eller lignende beskyttelsesmekanismer. Hvis slik forsering er nødvendig, vil det være endepunktinnhenting etter § 6-10. Det presiseres at informasjon regnes som åpent tilgjengelig selv om den er publisert på «det mørke nettet» og ikke er tilgjengelig gjennom vanlige søkemotorer, med mindre det er etablert spesielle mekanismer for å beskytte innholdet. Kryptert informasjon kan være åpent tilgjengelig hvis enhver kan laste den ned fra Internett, for eksempel hvis en bruker på et åpent forum laster opp en kryptert fil som andre brukere fritt kan laste ned.

Til § 6-3

Bestemmelsen gir Etterretningstjenesten hjemmel til å gjennomføre menneskebasert innhenting, det vil si innhenting av informasjon gjennom systematisk samhandling med mennesker, jf. *første punktum*. Menneskebasert innhenting vil ofte innebære å finne, verifisere, kultivere, rekruttere, trene og føre kilder i den hensikt å innhente ikke åpent tilgjengelig informasjon eller legge til rette for slik innhenting, jf. *andre punktum*. Menneskebasert innhenting behøver imidlertid ikke å innebære kontakt med kilder. Det presiseres i bestemmelsen at menneskebasert innhenting kan gjennomføres både i det fysiske og i det digitale rom.

Det følger av bestemmelsen at menneskebasert innhenting innebærer «systematisk samhandling» med andre. Dette innebærer for eksempel at det ikke regnes som menneskebasert innhenting hvis Etterretningstjenesten mottar tips fra publikum. Det vil derimot være menneskebasert innhenting dersom det inngås en kilderelasjon mellom tjenesten og en kilde som selv har tatt kontakt med tjenesten.

Menneskebasert innhenting vil ofte innledes ved at Etterretningstjenesten selv finner en kilde. Det vil normalt finne sted en kultivering av kilden, det vil si at en tjenesteperson bygger opp en relasjon med kilden med sikte på å rekruttere vedkommende. Det kan ikke trekkes en skarp grense mellom kultivering og rekruttering. Etter at kilden er rekruttert, vil tjenesten føre kilden med sikte på innhenting av informasjon eller tilrettelegging for innhenting.

Det kan være aktuelt å trene kilden, typisk for å ivareta operasjonssikkerhet. Tjenesten vil også fortløpende verifisere kilden, det vil si å vurdere hvorvidt kilden besitter eller kan skaffe tilgang til etterretningsrelevant informasjon, samt kildens motivasjon, troverdighet og egnethet. Kildeverifikasjon vil gjennomføres på alle stadier av innhentingsoperasjonen, fra før kontakten blir etablert og helt frem til kilderelasjonen avsluttes.

Forholdet mellom tjenesten og kilden kan være deklarert, og dermed kjent for kilden, eller ikke. For norske rekrutterte kilder vil relasjonen alltid være deklarert. For å skjerme innhentingsoperasjonen kan det brukes dekkstrukturer og uriktige, falske eller villedende identiteter, dokumenter og opplysninger, jf. § 11-4 første ledd. Slike virkemidler kan også tas i bruk for å infiltrere relevante miljøer og organisasjoner.

Hensikten med kildeaktiviteten kan for det første være å innhente ikke åpent tilgjengelig informasjon som kilden besitter eller kan få tilgang til. Hensikten kan også være at kilden skal legge til rette for innhenting av slik informasjon, for eksempel ved å gi tilgang til et bestemt sted eller miljø, eller ved å yte annen bistand til tjenesten.

Det er gitt særregler for kildevirksomhet i Norge i § 4-5.

Det ligger i menneskebasert innhenting at tjenesten kan påvirke handlingene til andre personer, for eksempel gjennom å anspore dem til å utlevere informasjon. Slike handlinger kan være straffbare i andre land. I hvilken utstrekning en tjenesteperson eller kilde straffritt kan utføre handlinger som i utgangspunktet rammes av gjerningsbeskrivelsen i et norsk straffebud, må vurderes konkret. For eksempel vil det straffritt kunne brukes virkemidler for å skjerme innhentingsoperasjonen i tråd med § 11-4 første ledd. Det presiseres for ordens skyld at handlinger foretatt i nødrett eller nødverge vil være straffrie hvis vilkårene for dette er oppfylt, jf. straffeloven §§ 17 og 18.

Det gjelder et absolutt forbud mot å medvirke til virksomhet som innebærer en reell risiko for brudd på ufravikelige menneskerettigheter, for eksempel i form av tortur eller annen umenneskelig eller nedverdigende behandling.

Til § 6-4

Etter *første ledd første punktum* kan Etterretningstjenesten foreta systematisk observasjon på

offentlig sted hvor det er sannsynlig at etterretningsmål vil befinne seg. «Offentlig sted» skal forstås på samme måte som i straffeloven § 10 første ledd, det vil si sted bestemt for alminnelig ferdsel eller sted der allmennheten ferdes.

Det kan også foretas systematisk observasjon mot privat lukket sted, jf. første ledd *andre punktum*. Forutsetningen er at den som observerer, befinner seg utenfor det private stedet.

Det følger av første ledd *tredje punktum* at det kan tas i bruk hjelpemidler for observasjon, opptak og annen dokumentasjon. Dette kan for eksempel være kikkerter og kameraer.

Systematisk observasjon er definert i *andre ledd*. Det trekkes en nedre grense mot ikke-planlagte visuelle iakttakelser. Definisjonen omfatter bare visuelle iakttakelser i det fysiske rom.

Til § 6-5

Bestemmelsen fastslår at Etterretningstjenesten kan plassere teknisk peileutstyr i det fysiske rom på eller ved et etterretningsmål for å kartlegge målets posisjon og bevegelser (teknisk sporing). Bestemmelsen er nøytral med hensyn til hva slags peileteknologi som kan tas i bruk.

Peileutstyret må plasseres «i det fysiske rom på eller ved et etterretningsmål». Det kan for eksempel plasseres utstyr på et kjøretøy eller i klær eller gjenstander som målet bærer med seg.

Bestemmelsen gir ikke hjemmel for sporing som gjennomføres ved å avlese posisjon fra etterretningsmålets elektroniske utstyr, som for eksempel en mobiltelefon eller datamaskin. Slik sporing vil kunne gjennomføres som midtpunktinnhenting (§ 6-9) eller endepunktinnhenting (§ 6-10), avhengig av hvor informasjonen kan observeres.

Til § 6-6

Det følger av *første ledd første punktum* at Etterretningstjenesten kan gjennomsøke bolig, rom eller annet oppbevaringssted for å finne informasjon eller gjenstander. Metoden vil ofte kunne kombineres med endepunktinnhenting (§ 6-10) eller annen innhenting med tekniske midler, for eksempel kopiering eller avfotografering (§ 6-8). Etter første ledd *andre punktum* kan tjenesten tilegne seg gjenstander som finnes under gjennomsøkingen og som har relevans for etterretningsformål, for eksempel et dokument eller en lagringsenhet.

Første ledd *tredje punktum* fastslår at gjennomsøking av sted som etter sin art ikke er tilgjengelig for alle, bare kan gjennomføres dersom det er strengt nødvendig. Vilkåret «tilgjengelig for alle» skal forstås på samme måte som etter straffeprosessloven § 193. En bolig er det fremste eksempelet på et sted som etter sin art ikke er tilgjengelig for alle, men også for eksempel et kontor kan omfattes. Kravet til streng nødvendighet innebærer at det kreves en sterkere interesseovervekt for å bruke metoden enn det som ellers følger av § 5-4.

Andre ledd fastsetter at Etterretningstjenesten kan tilegne seg etterretningsrelevante gjenstander fra personer.

Til § 6-7

Første punktum gir Etterretningstjenesten hjemmel til å innhente lyd og bilde fra kamera eller mikrofon som plasseres på eller i nærheten av sted hvor det er rimelig å anta at et etterretningsmål vil oppholde seg. Det ligger i formuleringen «plasseres» at bestemmelsen gjelder tiltak i det fysiske rom. Bestemmelsen gir derfor ikke hjemmel for overvåkning som gjennomføres ved å avlese etterretningsmålets elektroniske utstyr, som for eksempel en mobiltelefon eller datamaskin. Slik overvåkning vil kunne gjennomføres som midtpunktinnhenting (§ 6-9) eller endepunktinnhenting (§ 6-10), avhengig av hvor informasjonen kan observeres.

Det følger av *andre punktum* at innhentingen ikke kan gjennomføres på sted som etter sin art ikke er tilgjengelig for alle, med mindre det er strengt nødvendig. Vilkåret «tilgjengelig for alle» skal forstås på samme måte som etter straffeprosessloven § 193. En bolig er det fremste eksempelet på et sted som etter sin art ikke er tilgjengelig for alle, men også for eksempel et kontor kan omfattes. Kravet til streng nødvendighet innebærer at det kreves en sterkere interesseovervekt for å bruke metoden enn det som ellers følger av § 5-4.

Til § 6-8

Bestemmelsen gir Etterretningstjenesten hjemmel til å gjennomføre annen teknisk innhenting, jf. *første ledd første punktum*. Annen teknisk innhenting er innhenting av informasjon ved bruk av tekniske sensorer eller metoder som ikke reguleres av § 6-5 (teknisk sporing), § 6-7 (avlytting og bildeovervåkning), § 6-9 (midtpunktinnhenting) eller § 6-10 (endepunktinnhenting). Dette vil typisk være innhenting med andre typer sensorer enn kamera og mikrofon, men som på samme måte

plasseres i fysisk nærhet til målet. Det kan også være fjerninnhenting som ikke krever fysisk nærhet til målet. Det fremgår uttrykkelig av definisjonen at bildeovervåking av enkeltpersoner fra rombaserte sensorer (typisk satellitter) eller luftbårne sensorer (typisk droner), omfattes. For øvrig er definisjonen nøytral med hensyn til hvilken teknologi som kan brukes.

Det følger av *andre ledd* at innhentingen ikke kan gjennomføres på sted som etter sin art ikke er tilgjengelig for alle, med mindre det er strengt nødvendig. Vilkåret «tilgjengelig for alle» skal forstås på samme måte som etter straffeprosessloven § 193. En bolig er det fremste eksempelet på et sted som etter sin art ikke er tilgjengelig for alle, men også for eksempel et kontor kan omfattes. Kravet til streng nødvendighet innebærer at det kreves en sterkere interesseovervekt for å bruke metoden enn det som ellers følger av § 5-4.

Til § 6-9

Bestemmelsen gir Etterretningstjenesten hjemmel til å gjennomføre midtpunktinnhenting, jf. *første punktum*. Midtpunktinnhenting er innhenting av elektronisk kommunikasjon i transitt og kartlegging av kommunikasjonsinfrastruktur. Bestemmelsen åpner ikke for innhenting av lagrede data som ikke er i transitt mellom to endepunkter. Slik innhenting vil være endepunktinnhenting etter § 6-10.

Midtpunktinnhenting innebærer å fange opp kommunikasjonssignaler under transport, for eksempel via radio, satellitt eller Internett. Bestemmelsen er søkt utformet på en måte som er teknologinøytral. Dette innebærer at den også kan omfatte systemer for transport av kommunikasjonssignaler som for tiden ikke eksisterer eller ikke er i bruk, så fremt det er tale om elektronisk kommunikasjon. 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.

«Kartlegging av kommunikasjonsinfrastruktur» innebærer innhenting av signaler som ikke er kommunikasjon, for eksempel for å kartlegge basestasjoner i et bestemt geografisk område.

I motsetning til endepunktinnhenting er midtpunktinnhenting en *passiv* metode i den forstand at tjenesten kan avlese kommunikasjonen uten å bryte sikkerhetsmekanismer. Eventuell dekryptering av innhentet informasjon som er kryptert, finner sted i etterkant av innhentingen. Midtpunktinnhenting vil ofte innebære innhenting av rådata i bulk.

Det understrekes at bestemmelsen ikke åpner for å pålegge tilbydere å legge til rette for innhentingen. Bestemmelser om midtpunktinnhenting som forutsetter slik tilrettelegging (tilrettelagt innhenting), er gitt i kapittel 7 og 8. Dette presiseres i *andre punktum*.

Til § 6-10

Bestemmelsen gir Etterretningstjenesten hjemmel til å gjennomføre endepunktinnhenting av informasjon i systemer og tjenester som etterretningsmål besitter eller antas å ville benytte, jf. *første ledd*. Endepunktinnhenting er innhenting av ikke åpent tilgjengelig elektronisk informasjon i datasystem eller lignende system eller tjeneste. Bestemmelsen gir også hjemmel til å observere slik informasjon uten å innhente den.

I motsetning til midtpunktinnhenting etter § 6-9, retter endepunktinnhenting seg ikke mot informasjon som er *i transitt*, men mot informasjon som er tilgjengelig *fra selve endepunktet*. Det kan for eksempel være tale om en lagret melding. Et typisk endepunkt er en datamaskin eller en mobiltelefon, men bestemmelsen er søkt utformet på en teknologinøytral måte, slik at det er uten betydning hvilken teknologi som benyttes.

Endepunktinnhenting skiller seg fra midtpunktinnhenting også ved å være en *aktiv* metode i den forstand at den normalt innebærer forsering av sikkerhetsmekanismer for å få tilgang til endepunktet. Innhentingen kan blant annet skje over Internett, telenettet eller ved fysisk (varig eller midlertidig) tilgang til endepunktet. Fysisk tilgang kan for eksempel oppnås ved bruk av gjennomsøking etter § 6-6. Endepunktinnhenting kan innebære innhenting av rådata i bulk.

Innhentingen skal så langt mulig gjennomføres slik at det ikke unødig voldes fare for driftshindring eller skade på utrustning eller data, eller fare for at utenforstående får uberettiget tilgang til datasystemet eller lignende system eller tjeneste.

Det understrekes at bestemmelsen ikke åpner for å pålegge tilbydere å legge til rette for innhentingen.

Det følger av *andre ledd* at innhentingen ikke skal gjennomføres dersom det er grunn til å tro at den vil omfatte informasjon som ikke er ment for kommunikasjon, med mindre det er strengt nødvendig. Dette skyldes at innhenting av slik informasjon normalt må regnes som mer inngripende. Eksempler på data som ikke er ment for kommunikasjon, kan være kontaktlister og notatkladder. Kravet til streng nødvendighet innebærer at det

kreves en sterkere interesseovervekt for å bruke metoden enn det som ellers følger av § 5-4.

Til § 6-11

Bestemmelsen fastslår at Etterretningstjenesten kan treffe forberedende tiltak som er nødvendige for å gjennomføre metoder etter kapittelet. Den har primært en pedagogisk funksjon gjennom å synliggjøre at gjennomføringen av innhentingsmetodene normalt forutsetter en rekke forutgående faktiske handlinger.

En rekke eksempler på forberedende tiltak oppregnes i bestemmelsen, men den er ikke uttømmende, jf. ordet «herunder». Det avgjørende er hvorvidt tiltaket er nødvendig for å gjennomføre en metode etter kapittelet. I dette ligger det også at det forberedende tiltaket må være forholdsmessig. En forutsetning for å treffe forberedende tiltak er at det er fattet beslutning om bruk av en innhentingsmetode i samsvar med § 6-12.

Til § 6-12

Sjefen for Etterretningstjenesten har myndigheten til å beslutte bruk av en metode etter kapittelet, jf. *første ledd*. Kompetansen kan ikke delegeres til andre. Saker som omfattes av § 2-5, skal forelegges departementet for beslutning. Det følger av *andre ledd første punktum* at beslutningen ikke skal gis for lengre tid enn nødvendig, og ikke for mer enn ett år av gangen. Etter andre ledd *andre punktum* skal beslutningen snarest mulig revurderes dersom forutsetningene for den vesentlig endres.

Til § 6-13

Det følger av *første ledd* at beslutningen etter § 6-12 skal være skriftlig. Bestemmelsen oppstiller ingen andre formkrav, og er derfor ikke til hinder for at beslutningen kan ta form av en operasjonsordre, innhentingsplan eller lignende, så fremt kravene i *bokstav a til d* oppfylles.

Etter *bokstav a* skal beslutningen angi oppdraget som innhentingen knytter seg til. Det skal vises til hvilken lovbestemt oppgave som begrunner innhentingen, jf. kapittel 3. Det bør normalt også vises til den aktuelle prioriteringen i prioriteringsdokumentet for nasjonale etterretningsbehov (PNEB), den mer detaljerte operasjonaliseringen av PNEB eller den aktuelle informasjonsforespørselen (RFI). Det vises til § 2-2 om oppdragsstyring.

Bokstav b fastsetter at beslutningen skal angi hva eller hvem innhentingen gjelder.

Det følger av *bokstav c* at beslutningen skal angi det faktiske og rettslige grunnlaget for innhentingen. Hvor omfattende redegjørelsen skal være, må avgjøres konkret, og vil kunne variere fra sak til sak. Det skal redegjøres for vurderingen av tiltakets forholdsmessighet etter § 5-4. Hvis en metode bare kan brukes når det er strengt nødvendig, skal det angis hvorfor dette vilkåret er oppfylt.

Etter *bokstav d* skal beslutningens varighet angis, jf. § 6-12 andre ledd.

Andre ledd første punktum åpner for muntlige beslutninger i hastetilfeller. Regelen er ment som en meget snever unntaksregel som bør utøves med stor varsomhet. Det følger av andre ledd *andre punktum* at en muntlig beslutning snarest mulig skal nedtegnes.

Til kapittel 7

Til § 7-1

Bestemmelsen fastsetter i *første ledd* at Etterretningstjenesten for etterretningsformål kan innhente elektronisk kommunikasjon som transporteres over den norske grensen.

Kommunikasjonen kan utelukkende innhentes «for etterretningsformål». Dette innebærer at innhentingen må begrunnes i en av Etterretningstjenestens oppgaver etter kapittel 3, se § 1-3 bokstav c. Regler om oppdragsstyring er gitt i § 2-2. Det vises dessuten til § 4-8, som fastsetter et uttrykkelig forbud mot å innhente informasjon med formål å utføre oppgaver som tilligger politiet eller andre rettshåndhevende myndigheter. Det vises også til § 10-7, som fastsetter at bistand til politiet etter politiloven § 27 a ikke kan ta form av innhenting etter kapittel 7.

Bestemmelsen gjelder «elektronisk kommunikasjon som transporteres over den norske grensen». Dette innebærer for det første at det ikke kan innhentes kommunikasjon som utelukkende transporteres internt i et norsk nettverk. Kommunikasjonen må krysse den norske grensen. Det er uten betydning hvorvidt kommunikasjonen transporteres inn og ut av Norge på land, sjøveien eller i luften. For det andre gir bestemmelsen ikke hjemmel til innhenting av lagrede data som ikke er i transitt. Slik data må eventuelt innhentes med hjemmel i lovforslaget § 6-10 om endepunktinnhenting. Innhentingen er altså en form for midtpunktinnhenting, jf. § 6-9, som reguleres særskilt i kapittel 7 og 8. Begrunnelsen for særreguleringen er at innhentingen i stor grad vil berøre norsk

innenlandsk kommunikasjon, som av ulike grunner normalt vil krysse den norske grensen. Det vises til nærmere redegjørelse under punkt 11.8.1.3.

I dagens situasjon vil det i praksis normalt være tale om å innhente kommunikasjon som transporteres i fiberoptiske kabler, men bestemmelsen er søkt utformet på en måte som er teknologinøytral. Dette innebærer at den også kan omfatte transportsystemer for eksempel i luften eller som for tiden ikke eksisterer eller ikke er i bruk. Hvor speilingen finner sted, er ikke avgjørende. Det vises til merknadene til § 7-2.

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.

Av pedagogiske grunner slås det fast i bestemmelsen at innhentingen bare kan finne sted når grunnvilkårene etter kapittel 5 er oppfylt, bestemmelsene i kapittel 7 og 8 følges og innhenting ikke strider mot loven for øvrig.

Det følger av *andre ledd* at bestemmelsene i kapittel 7 og 8 bare kommer til anvendelse der det er nødvendig at tilbydere som nevnt i § 7-2 legger til rette for tilgangen. Midtpunktinnhenting som ikke forutsetter slik tilrettelegging, reguleres av § 6-9.

Til § 7-2

Bestemmelsen fastsetter i *første ledd* en plikt for ekomtilbydere til å legge til rette for innhenting av elektronisk kommunikasjon som transporteres over den norske grensen. Tilretteleggingsplikten skiller innhentingen regulert i kapittel 7 og 8 fra andre former for midtpunktinnhenting, som reguleres av § 6-9.

Tilretteleggingsplikten gjelder for tilbydere som omfattes av ekomloven § 1-5, det vil si tilbydere av elektronisk kommunikasjonsnett eller -tjeneste. Plikten gjelder også for tilbydere av internettbaserte kommunikasjons- eller meldingstjenester som er tilgjengelige for allmennheten. Slike tjenester omtales med et faguttrykk gjerne som *over the top*-tjenester (OTT-tjenester). For at en tjeneste skal regnes som en kommunikasjons- eller meldingstjeneste, må den ha en kommunikasjons- eller meldingsfunksjonalitet, men det er ikke et krav at dette er hovedformålet med tjenesten.

Kjernen i tilretteleggingsplikten er plikten til å *speile og gjøre tilgjengelig* utvalgte kommunikasjonsstrømmer for Etterretningstjenesten. Tjenesten skal velge ut de mest etterretningsrelevante kommunikasjonsstrømmene, se nærmere § 7-6 og punkt 11.8.2.3. At plikten er å speile og tilgjengeliggjøre, innebærer at tilbyderne ikke kan pålegges å lagre informasjonen selv.

Kommunikasjonsstrømmene vil ikke nødvendigvis speiles og tilgjengeliggjøres på det bestemte punktet hvor de krysser grensen. Speilingspunktet vil avhenge av tekniske og praktiske forhold knyttet til de utvalgte kommunikasjonsstrømmene. Det kan for eksempel være aktuelt å speile på tjenere knyttet til 5G (IMS-tjenere m.m.) eller Internett (DNS-tjenere m.m.). Avhengig av den teknologiske utviklingen kan det ikke ses bort fra at speilingen også vil kunne omfatte norsk innenlandsk kommunikasjon som ikke krysser grensen, men slik informasjon skal ikke innhentes og lagres. Det understrekes at Etterretningstjenesten i samsvar med lovforslaget § 7-6 plikter å søke å forhindre lagring av norsk innenlandsk kommunikasjon gjennom utvalg og filtrering.

Tilbyderne pålegges også plikt til å tilrettelegge for Etterretningstjenestens virksomhet etter kapittelet på annen måte, herunder på de måtene som er listet opp i *bokstavene a til f.*

Bokstav a fastsetter en informasjonsplikt om signalmiljøet og tekniske forhold. Formålet med plikten er å sette Etterretningstjenesten i stand til å etablere og drifte tilgangen.

Etterretningstjenesten vil kunne ha behov for å installere utstyr og etablere midlertidig eller permanent tilstedeværelse for å drifte utstyr på steder som kontrolleres av tilbyder. Det følger av *bokstav b* at tilbyder plikter å tillate dette. Plikten innebærer ikke en plikt til å gi Etterretningstjenesten fri tilgang til tilbyders infrastruktur og systemer uten tilbyders kjennskap. Tilbyder skal gjøres kjent med tiltakene som treffes, og skal så langt som mulig gis anledning til å være til stede ved installasjon og vedlikehold av utstyr.

Det fremgår av *bokstav c* at tilbyder plikter å medvirke til teknisk drift og vedlikehold av etablerte løsninger.

Etter *bokstav d* plikter tilbyder å bidra til testinnhenting og testanalyser av trafikk i nett og tjenester. Se nærmere punkt 11.8.3.3 og § 7-5 om slik testvirksomhet.

Bokstav e fastslår at tilbyder plikter å sørge for tilgang til kommunikasjon uten hinder av linkkryptering eller tilsvarende kryptering som tilbyder kontrollerer. Dette innebærer at en tilbyder som har tilgang til en utvalgt kommunikasjonsstrøm i klartekst, plikter å speile og tilgjengeliggjøre denne for Etterretningstjenesten uten å legge på kryptering. Det kan være kryptering på linknivå («linkkryptering») eller på andre nivåer

(«tilsvarende kryptering»), men vilkåret «som tilbyder kontrollerer» innebærer at tilbyder ikke kan pålegges å utvikle løsninger for tilgang til ende-til-ende-kryptert informasjon mellom sluttbrukere.

Bokstav f fastsetter at tilbyder skal medvirke til sikkerhetsmessig forsvarlige løsninger. Det vil for eksempel være behov for å skjerme Etterretningstjenestens personell og utstyr i størst mulig utstrekning, slik at dette blir kjent for færrest mulig personer hos tilbyder og bare for de som har tjenstlig behov for det. I tillegg til pliktene etter dette punktet, kan det påhvile tilbyder plikter som følger av regler gitt i eller i medhold av sikkerhetsloven, i den utstrekning disse reglene gjelder for vedkommende tilbyder.

Det følger av *andre ledd første punktum* at tilretteleggingen ikke skal forringe de elektroniske kommunikasjonstjenestene for brukerne. Dette innebærer at de tekniske løsningene ikke skal føre til forsinkelse, redusert kapasitet eller brudd i kommunikasjonen. Det ligger i forringelsesvilkåret at en teoretisk eller neglisjerbar forsinkelse eller kapasitetsreduksjon må aksepteres.

Andre ledd *andre punktum* fastslår at merutgifter for tilbyder som følge av tilretteleggingen skal dekkes av staten. Merutgiftene kan knytte seg til både investeringer og drift.

Etter *tredje ledd* kan departementet gi forskrift om tilretteleggingsplikten etter første ledd og prinsipper for utregning av merutgifter etter andre ledd.

Til § 7-3

Bestemmelsen regulerer beslutning om tilrettelegging. *Første ledd første punktum* gir sjefen for Etterretningstjenesten myndighet til å fatte beslutning om tilrettelegging. Myndigheten kan ikke delegeres. Den som handler i strid med beslutning om tilrettelegging, kan straffes etter § 11-8.

Det følger av første ledd *andre punktum* at tilbyderen så langt mulig skal gis anledning til å uttale seg før beslutningen fattes. Departementet forutsetter at det normalt vil finne sted en dialog med tilbyderen før det blir aktuelt å treffe beslutning. Tjenesten og tilbyderen bør tilstrebe å komme til en omforent forståelse om tiltakene som skal treffes og de økonomiske konsekvensene av dem.

Første ledd *tredje punktum* fastslår at beslutningen maksimalt kan gjelde for tre år av gangen. Hensikten med regelen er å sikre at behovet for tilrettelegging fra den aktuelle tilbyderen blir vurdert med jevne mellomrom.

Regler om klage er gitt i *andre ledd*. Etter andre ledd *første punktum* har tilbyderen rett til å klage på beslutningen. Departementet er klageinstans. Klagefristen er i henhold til andre ledd *andre punktum* tre uker. Hvis tilbyderen ber om det, kan departementet bestemme at beslutningen ikke skal iverksettes før klagen er avgjort, det vil si at klagen gis oppsettende virkning, jf. andre ledd *tredje punktum*.

Etter *tredje ledd første punktum* skal beslutning om tilrettelegging meddeles EOS-utvalget og Nasjonal kommunikasjonsmyndighet (Nkom). Dette gjelder både beslutning etter første ledd og beslutning i klagesak etter andre ledd. Tredje ledd *andre punktum* gir Nkom rett til informasjon om de tekniske og operasjonelle løsningene som tjener til å oppfylle tilretteleggingsplikten. For EOS-utvalget følger en slik rett av EOS-kontrolloven § 8.

Fjerde ledd gir departementet myndighet til å gi forskrift om beslutning om tilrettelegging etter første ledd og klagebehandling etter andre ledd.

Til § 7-4

Bestemmelsen fastsetter i *første ledd første punktum* taushetsplikt for tilbydere som har tilretteleggingsplikt etter § 7-2. Taushetsplikten gjelder alle forhold i forbindelse med tilretteleggingen. I kjernen er opplysninger om tekniske løsninger, men taushetsplikten rekker videre enn dette, og omfatter for eksempel også opplysninger om prosessen knyttet til tilrettelegging, inkludert dialog mellom Etterretningstjenesten og tilbyder, beslutning om tilrettelegging og eventuell klagebehandling. Etter første ledd *andre punktum* gjelder taushetsplikten tilsvarende for enhver som utfører arbeid eller tjeneste for tilbyderen eller på annen måte bistår i å gjennomføre tilrettelegging. Det følger av første ledd *tredje punktum* at taushetsplikten fortsetter å gjelde også etter at vedkommende har avsluttet arbeidet eller tjenesten.

Andre ledd fastslår et unntak fra taushetsplikten for så vidt gjelder å gi opplysninger til EOS-utvalget eller Nasjonal kommunikasjonsmyndighet (Nkom). Unntaket sikrer at disse organene kan motta fra tilbyder den informasjonen om tekniske og operasjonelle løsninger som de trenger for å løse sine kontroll- og tilsynsoppgaver.

Brudd på taushetsplikten kan straffes etter § 11-8.

Til § 7-5

Bestemmelsen regulerer testinnhenting og testanalyser.

Første ledd første punktum fastslår at Etterretningstjenesten kan gjennomføre testinnhenting og testanalyser av trafikk og nett som omfattes av kapittelet. Det følger av første ledd *andre punktum* at testinnhenting og testanalyser utelukkende skal brukes til de formål som er listet opp der, det vil si til teknisk understøttelse av systemet. Dette innebærer et forbud mot å bruke testdata og testanalyser til andre formål, slik som produksjon av etterretning. Testdata og testanalyser kan heller ikke deles med andre.

Gjennomføringen av testinnhentingen er regulert i *andre ledd*. Det følger av andre ledd *første punktum* at testinnhenting gjennomføres ved å trekke ut ufiltrert kommunikasjon fra en eller flere kommunikasjonsstrømmer. Ett uttrekk skal ikke overstige 30 sekunder, jf. andre ledd *andre punktum*. Det kan maksimalt gjøres ett uttrekk per time, jf. andre ledd *tredje punktum*. Det følger av dette at det i høyden kan gjøres 24 uttrekk i døgnet.

Uttrekkene skal lagres i et korttidslager, jf. *tredje ledd*. Dette lageret skal holdes adskilt fra data som lagres etter §§ 7-7 og 7-9. At testdata skal lagres adskilt fra annen data, har til hensikt å støtte opp om forbudet mot bruk av testdata til andre formål enn teknisk understøttelse, jf. første ledd andre punktum.

Regler om oppbevaring følger av *fjerde ledd*. Hovedregelen etter fjerde ledd *første punktum* er at uttrekkene ikke skal oppbevares lenger enn nødvendig. Den absolutte lengstefristen er 14 dager. Etter fjerde ledd *andre punktum* kan tekniske parametere og bearbeidede analyser som ikke kan knyttes til enkeltpersoner, oppbevares så lenge det er nødvendig for de tekniske formålene som er oppregnet i første ledd andre punktum.

Femte ledd fastsetter enkelte særregler for testinnhenting, testanalyser og annen teknisk understøttelse. Etter femte ledd *første punktum* skal slik understøttelse bare utføres av et begrenset antall tekniske spesialister som har mottatt særskilt opplæring og som ikke har etterretningsanalyse som oppgave. Regelen støtter opp om forbudet mot bruk av testdata til andre formål enn teknisk understøttelse, jf. første ledd andre punktum. Det samme gjør regelen i femte ledd *andre punktum* om at det alltid skal være to spesialister til stede når uttrekkene settes opp og analyseres. Det legges til grunn at Etterretningstjenesten vil etablere prosedyrer for rullering av spesialistene som gjennomfører uttrekkene.

Til § 7-6

Bestemmelsen fastslår en plikt for Etterretningstjenesten til gjennom utvalg og filtrering å søke å hindre lagring av metadata om kommunikasjon mellom en avsender og en mottaker som begge befinner seg i Norge.

Plikten til *utvalg* innebærer at Etterretningstjenesten skal vurdere og beslutte hvilke kommunikasjonsnett, tjenester og linker som det skal innhentes fra. Tjenesten skal prioritere innhenting fra de kommunikasjonsstrømmene som antas å transportere mest mulig etterretningsrelevant kommunikasjon. Kommunikasjonsstrømmer som ikke transporterer kommunikasjon over den norske grensen, skal ikke velges ut. Dette følger av at innhentingshjemmelen er begrenset til grenseoverskridende kommunikasjon. Kommunikasjonsstrømmer som utelukkende transporterer kommunikasjon mellom avsendere og mottakere som befinner seg i Norge, skal så langt mulig heller ikke velges ut, selv om det er tale om kommunikasjon som krysser grensen. Det presiseres at det uansett ikke kan søkes i kommunikasjon med begge ender i Norge. Her kan det likevel være aktuelt med unntak hvis det er tale om kommunikasjon fra eller til en person som omfattes av lovforslaget § 4-2 første ledd. Det kan for eksempel være tale om en tjeneste som brukes av personer som opptrer på vegne av en fremmed stat i Norge til å kommunisere seg imellom.

Plikten til *filtrering* innebærer at Etterretningstjenesten skal utvikle og implementere filtre som skal søke å hindre lagring av metadata om kommunikasjon mellom en avsender og en mottaker som begge befinner seg i Norge. At tjenesten skal «søke å» hindre lagring, synliggjør at det ikke alltid vil være mulig å filtrere bort irrelevant data. Det vil ofte måtte lagres store mengder irrelevante data fra enkelte kommunikasjonsstrømmer, fordi det ikke er mulig å filtrere bort informasjonen som er uten interesse. I den utstrekning det er mulig å filtrere bort irrelevante data, for eksempel ved hjelp av geografiske kjennetegn, skal dette like fullt gjøres. Etterretningstjenesten skal sørge for at filtrene oppdateres i tråd med den teknologiske utviklingen.

Bestemmelsen fastsetter et unntak fra utvalgs- og filtreringsplikten i den utstrekning enten avsender eller mottaker er en utenlandsk eller statsløs person i Norge som opptrer på vegne av en fremmed stat eller statslignende aktør, jf. § 4-2 første ledd.

Til § 7-7

Bestemmelsen regulerer innhenting og lagring av metadata i bulk.

Det følger av *første ledd første punktum* at Etterretningstjenesten kan innhente og lagre metadata i bulk om elektronisk kommunikasjon som transporteres over den norske grensen etter at det er foretatt utvalg og filtrering i samsvar med § 7-6. Metadata defineres i første ledd *andre punktum*.

Etter *andre ledd første punktum* plikter Etterretningstjenesten å opprette og vedlikeholde en liste over hvilke typer metadata som kan lagres, for å hindre at det lagres innholdsdata. Denne listen skal være tilgjengelig for EOS-utvalget og Nasjonal kommunikasjonsmyndighet, jf. andre ledd *andre punktum*.

Tredje ledd fastslår at lagrede metadata skal slettes senest etter 18 måneder. Dette utgjør et unntak fra den alminnelige maksimale lagringstiden for rådata i bulk, som etter § 9-8 andre ledd første punktum er 15 år. Det er ikke adgang til å forlenge lagringstiden etter § 9-8 andre ledd andre punktum. Når det i bestemmelsen fremgår at opplysninger skal slettes *senest* etter 18 måneder, innebærer dette at det også kan bli aktuelt å slette data på et tidligere tidspunkt. Data som tjenesten blir klar over ikke er nødvendige, skal slettes selv om de ikke har nådd 18-månedersgrensen.

Fjerde ledd gir § 7-5 femte ledd første punktum tilsvarende anvendelse for teknisk analyse, feilsøking og oppdatering av lagrede metadata i den hensikt å muliggjøre søk. Dette innebærer at slike oppgaver bare kan utføres av et begrenset antall tekniske spesialister som har mottatt særskilt opplæring og som ikke har etterretningsanalyse som oppgave.

Til § 7-8

Bestemmelsen regulerer Etterretningstjenestens søk i metadata som er lagret i samsvar med § 7-7.

Det følger av *første ledd første punktum* at søk kan foretas innenfor rammen av rettens kjennelse etter kapittel 8. Etter første ledd *andre punktum* skal søk baseres på søkebegreper.

Søkebegreper kan knytte seg til en person (personselektor) eller til et bestemt mønster eller avgrensning (modusselektor).

En personselektor er en identifikator knyttet til en bestemt person eller virksomhet, for eksempel et telefonnummer, en e-postadresse eller et brukernavn på en tjeneste. Hvis rettens kjennelse identifiserer en bestemt person det skal kunne søkes på, vil det kunne søkes på alle kjente identifikatorer knyttet til personen.

En modusselektor beskriver et bestemt mønster eller avgrensning. Modusselektoren vil ofte bestå av en kombinasjon av søkebegreper. Den vil normalt være mindre finmasket enn en personselektor. På den andre siden ligger det i grunnvilkåret om forholdsmessighet etter § 5-4 en begrensning i hvor grovkornet den kan være. Det vil for eksempel kunne være uforholdsmessig hvis søkebegrepet alene er et større geografisk område, slik som en by. I slike tilfeller vil det normalt være nødvendig å spisse søket ved bruk av flere søkebegreper, for eksempel bestemte kjennetegn som kan knyttes til en trusselaktør.

En konsekvens av regelen om at søk skal baseres på søkebegreper, er at det ikke er tillatt med søk hvor hverken aktør eller modus er kjent. Hensikten med dette forbudet er å hindre vilkårlighet.

I *andre ledd* fastsettes flere personelle og materielle begrensninger med hensyn til søk etter første ledd. Det følger av andre ledd *første punktum* at søk bare kan utføres av personell som er vurdert skikket til det og som utpekes av sjefen for Etterretningstjenesten. Kompetansen kan ikke delegeres. Det vil si at det bare er sjefen, eventuelt den som fungerer som sjef i sjefens fravær, som kan utpeke personell med myndighet til å søke i metadatalageret. Etter andre ledd *andre punktum* må personellet ha gjennomgått særskilt opplæring. I tillegg til etterretningsfaglige og tekniske aspekter, vil rettslige og etiske rammer stå sentralt i opplæringen.

Etter andre ledd *tredje punktum* skal den enkelte bare ha anledning til å utføre søk i henhold til søkeprivilegier som er tilpasset dennes oppdragsportefølje.

Til § 7-9

Bestemmelsen regulerer målrettet innhenting og lagring av innholdsdata med tilhørende metadata fra elektronisk kommunikasjon som transporteres over den norske grensen.

I motsetning til lagring av metadata etter § 7-7, er det her ikke tale om innhenting og lagring i bulk, men om målrettet innhenting og lagring. Bestemmelsen gir altså ikke hjemmel til lagring av innholdsdata med tilhørende metadata i bulk.

I første ledd *andre punktum* er innholdsdata definert som data som ikke er metadata. Det vil si at all data som ikke regnes som metadata, regnes som innholdsdata. Det vises til definisjonen av metadata i § 7-7 første ledd andre punktum.

Til § 7-10

Bestemmelsen regulerer internkontroll og aktivitetslogger.

Etter *første ledd* skal Etterretningstjenesten iverksette systematiske tiltak for å sikre at virksomhet etter kapittelet gjennomføres i samsvar med loven.

Andre ledd første punktum fastsetter at Etterretningstjenestens informasjonssystemer skal ha en funksjonalitet som sikrer at alle søk skal kunne kontrolleres i ettertid gjennom aktivitetslogger. Etter andre ledd *andre punktum* skal loggene oppbevares i 10 år, og de skal til enhver tid være tilgjengelige for EOS-utvalgets kontroll.

Til § 7-11

Bestemmelsen gjelder løpende kontroll av tilrettelagt innhenting. Det vises til nærmere redegjørelse under punkt 11.10.4. Det presiseres for ordens skyld at prinsippet om etterfølgende kontroll, jf. EOS-kontrolloven § 2 tredje ledd andre punktum, ikke er til hinder for den løpende kontrollen.

Kontrolloppgaven fremgår av *første ledd*, som fastsetter at EOS-utvalget skal føre kontroll med Etterretningstjenestens etterlevelse av bestemmelsene i kapittel 7. Kontrolloppgaven gjelder alle bestemmelsene i kapittelet, men to forhold nevnes særskilt: For det første skal utvalget kontrollere at Etterretningstjenesten bare gjennomfører søk i henhold til rettens kjennelser. Utvalget vil få tilgang til rettens kjennelser og begjæringene som ligger til grunn for dem i henhold til § 8-1 tredje ledd. Utvalget skal for det andre føre kontroll med at korttidslageret og testdata bare brukes til teknisk understøttelse, jf. § 7-5 første ledd andre punktum, som innebærer et forbud mot å bruke slike data til andre formål, herunder til etterretningsproduksjon.

Et eksempel på et annet forhold som faller innenfor kontrolloppgaven er etterlevelse av plikten til utvalg og filtrering etter § 7-6 for å søke å hindre at det lagres metadata om kommunikasjon mellom en avsender og en mottaker som begge befinner seg i Norge.

Andre ledd første punktum fastslår at 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 tilrettelagt innhenting. Det forutsettes at unntaket etter gjeldende rett for «særlig sensitiv informasjon» ikke vil få betydning for informasjon som nevnt i bestemmelsen.

Etter *tredje ledd* skal Etterretningstjenesten tilrettelegge for kontrollen gjennom tekniske løsninger. Dette innebærer blant annet at Etterretningstjenesten skal ta hensyn til kontrollfunksjonalitet når den utvikler og implementerer de tekniske løsningene for innhenting og analyse.

Omfanget av tilretteleggingen må avgjøres konkret og i dialog mellom tjenesten og utvalget. Det forutsettes at tjenesten strekker seg langt for å imøtekomme utvalgets behov innenfor de økonomiske, tekniske, sikkerhetsmessige og praktiske rammer som gjelder til enhver tid. Det bemerkes at det følger av EOS-kontrolloven § 2 andre ledd andre punktum at kontrollen bør innrettes slik at den er til minst mulig ulempe for tjenestens løpende virksomhet.

Til § 7-12

Paragrafen gir regler om rettslig prøving som ledd i den løpende kontrollen av tilrettelagt innhenting.

Etter *første ledd første punktum* kan EOS-utvalget fremme begjæring for Oslo tingrett hvis utvalget mener at Etterretningstjenesten gjennomfører virksomhet etter kapittel 7 i strid med loven. Det kan for eksempel være tale om bruk av søkebegreper som etter utvalgets syn er utenfor rammen av rettens kjennelse etter kapittel 8. Retten kan pålegge tjenesten å stanse den ulovlige virksomheten og slette informasjon som har blitt hentet inn i strid med loven. Tjenesten plikter å rette seg etter rettens avgjørelse.

Etter EOS-kontrolloven § 5 femte ledd omfatter ikke kontrolloppgaven virksomhet som angår personer som ikke er bosatt i Norge 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 slike tilfeller når særlige grunner tilsier det.

Ordningen med rettslig prøving er ment som en sikkerhetsventil, og skal ikke erstatte vanlige prosedyrer for å løse uenigheter mellom tjenesten og utvalget. Tjenesten skal derfor gis anledning til å vurdere og ta stilling til utvalgets syn, og eventuelt bringe saken inn for departementet for avgjørelse, før det blir aktuelt for utvalget å fremme begjæring til tingretten. I tråd med dette fastsettes det i første ledd *andre punktum* at tjenesten skal gjøres kjent med utvalgets syn og gis mulighet til å rette seg etter det før begjæringen fremmes.

Etter *andre ledd* gjelder reglene i kapittel 8 tilsvarende så langt de passer. Det bemerkes at

EOS-utvalget ikke møter som part for retten, og ikke har ankerett. Retten skal imidlertid normalt oppnevne særskilt advokat i tråd med § 8-5. Advokaten vil kunne anke rettens kjennelse. Etterretningstjenesten vil også ha rett til å anke kjennelsen.

Til § 7-13

Første ledd første punktum fastsetter et forbud mot å utlevere overskuddsinformasjon fra tilrettelagt innhenting, se nærmere punkt 11.12.3. Forbudet utgjør et unntak fra det alminnelige utgangspunktet etter § 10-4 om at overskuddsinformasjon kan deles med offentlige myndigheter. Begrunnelsen for forbudet er det særpreget tilrettelagt innhenting har som følge av at det i dagens teknologiske situasjon vil lagres store mengder metadata om norsk innenlandsk kommunikasjon. Lagringen innebærer i teorien et stort overvåkningspotensiale overfor egne borgere. Forbudet har symbolsk betydning gjennom tydelig å markere formålsbegrensningen til utenlandsetterretning. Det bidrar på denne måten til å motvirke formålsutglidning, det vil si at lagrede data tas i bruk til andre formål enn tilsiktet.

Departementet understreker at tilrettelagt innhenting utelukkende kan finne sted «for etterretningsformål», jf. § 7-1 første ledd. Dette innebærer at innhentingen må begrunnes i en av Etterretningstjenestens oppgaver etter kapittel 3. Med «overskuddsinformasjon» forstås informasjon som er uten interesse for etterretningsformål. Det kan for eksempel være informasjon om alminnelig kriminalitet. Informasjon som har relevans både for Etterretningstjenesten og for andre myndigheter, er ikke overskuddsinformasjon. Det kan for eksempel være informasjon om fremmede staters etterretningsvirksomhet mot Norge, internasjonal terrorisme eller digitale angrep som stammer fra utlandet. Deling av slik informasjon med Politiets sikkerhetstjeneste, Nasjonal sikkerhetsmyndighet og andre relevante myndigheter er et sentralt formål med tilrettelagt innhenting.

Det følger av første ledd *andre punktum* at forbudet mot å utlevere overskuddsinformasjon går foran avvergings- og opplysningsplikter som følger av annen lovgivning. Et eksempel kan være at innhenting av innholdsdata fra et godkjent etterretningsmål viser at etterretningsmålet vil begå en handling som omfattes av avvergingsplikten i straffeloven § 196. Det følger av andre punktum at avvergingsplikten ikke gjelder i et slikt tilfelle. Andre eksempler på avvergings- og opplysningsplikter som ikke vil gjelde dersom plikten oppstår som følge av overskuddsinformasjon fra tilrettelagt innhenting, er straffeloven §§ 226 og 287 samt barnevernloven § 6-4.

Bestemmelsen i første ledd andre punktum må ses i sammenheng med *andre ledd første punktum*, som fastslår at overskuddsinformasjon likevel kan utleveres i den utstrekning det er nødvendig for å forhindre alvorlig fare for noens liv, helse eller frihet eller at noen blir uriktig tiltalt eller domfelt for en straffbar handling. Unntaket er ment som en meget snever unntaksregel som skal anvendes med stor varsomhet. Det må være tale om en konkret fare som kan forhindres, og faren må være av en kvalifisert art. Unntaket kan for eksempel komme til anvendelse dersom målrettet innhenting av innholdsdata fra et godkjent etterretningsmål viser at etterretningsmålet utsetter sine nærstående for alvorlig vold eller seksuelt misbruker et barn. Denne informasjonen regnes som overskuddsinformasjon fordi den er uten interesse for etterretningsformål, men i en slik situasjon kan det være nødvendig å utlevere informasjonen til andre myndigheter for å forhindre alvorlig fare for liv og helse. I teorien kan det også tenkes at Etterretningstjenesten gjennom målrettet innhenting av innholdsdata får kjennskap til et justismord, og unntaksbestemmelsen vil da komme til anvendelse.

Etter andre ledd *andre punktum* plikter Etterretningstjenesten å varsle EOS-utvalget om utlevering etter unntaksbestemmelsen i andre ledd første punktum. Hensikten med denne plikten er å sikre muligheten for kontroll av at unntaksadgangen ikke brukes for å omgå formålsbegrensningen til utenlandsetterretning.

Departementet understreker at forbudet etter § 7-14 mot å bruke informasjon som stammer fra tilrettelagt innhenting som bevis i en straffesak gjelder for overskuddsinformasjon som har blitt utlevert med grunnlag i unntaksbestemmelsen i første ledd andre punktum.

Det foreslås av pedagogiske grunner presisert i *tredje ledd* at informasjon som ikke er overskuddsinformasjon, kan utleveres i samsvar med reglene i kapittel 10.

Til § 7-14

Bestemmelsen fastsetter et bevisforbud i straffesaker for informasjon som stammer fra tilrettelagt innhenting, se nærmere punkt 11.13.3.

Forbudet etter *første punktum* innebærer at påtalemyndigheten ikke kan legge frem informasjon som stammer fra tilrettelagt innhenting som grunnlag for krav om straff eller andre straffe-

rettslige reaksjoner, jf. straffeloven §§ 29 og 30. Retten skal avskjære slik bevisføring.

Påtalemyndigheten kan heller ikke bruke slik informasjon som grunnlag for egen ileggelse av straff eller andre strafferettslige reaksjoner, for eksempel forelegg på bot etter straffeprosessloven § 255 eller påtaleunnlatelse etter straffeprosessloven § 69.

Bevisforbudet er ikke til hinder for at informasjon som stammer fra tilrettelagt innhenting danner grunnlag for bruk av tvangsmidler. Slik informasjon kan for eksempel gi skjellig grunn til mistanke om lovbrudd. På grunn av formålsbegrensningen til utenlandsetterretning og forbudet mot å innhente informasjon med politiformål, vil dette normalt bare være aktuelt på områder som Etterretningstjenesten samarbeider med Politiets sikkerhetstjeneste og andre norske myndigheter om å motvirke, slik som fremmed etterretningsvirksomhet mot Norge, internasjonal terrorisme og digitale angrep som stammer fra utlandet. For eksempel kan informasjon fra tilrettelagt innhenting vise at en person i utlandet planlegger en terrorhandling i Norge. Denne informasjonen skal Etterretningstjenesten dele med Politiets sikkerhetstjeneste, som kan bruke den som grunnlag for bruk av tvangsmidler mot personen med grunnlag i straffeprosessloven eller politiloven. Informasjon som Politiets sikkerhetstjeneste innhenter ved bruk av tvangsmidler, kan normalt brukes som bevis i en straffesak. Se imidlertid politiloven § 17 f for tvangsmidler brukt i forebyggende øyemed.

Andre punktum fastsetter et unntak fra bevisforbudet i saker som gjelder overtredelse av straffeloven § 131 (terrorhandlinger).

Til kapittel 8

Til § 8-1

Bestemmelsen regulerer rettens myndighet til å gi tillatelse til tilrettelagt innhenting.

Det følger av *første ledd første punktum* at retten kan gi Etterretningstjenesten tillatelse til søk i lagrede metadata etter § 7-8. Det er her tale om metadata som er allerede er innhentet og lagret i bulk i medhold av § 7-7. Retten kan også gi tillatelse til målrettet innhenting og lagring av innholdsdata med tilhørende metadata etter § 7-9. I dette tilfellet kan det bare innhentes og lagres informasjon fra det tidspunktet retten gir tillatelse til det. Tillatelse forutsetter i begge tilfeller at Etterretningstjenesten har fremmet en begjæring etter § 8-2.

Det følger av første ledd *andre punktum* at retten kan oppstille vilkår i kjennelsen. Det kan for eksempel være tiltak for å minimere risikoen for tilgang til irrelevant informasjon, eller andre vilkår som retten mener bør oppstilles, for eksempel av hensyn til kravet om forholdsmessighet etter § 5-4.

Etter første ledd *tredje punktum* skal kjennelsen begrunnes. Kravet til begrunnelse skal sikre en reell og samvittighetsfull vurdering, og motvirke risikoen for urettmessige og vilkårlige avgjørelser. Begrunnelsen skal også gi Etterretningstjenesten og den særskilte advokaten grunnlag for å vurdere om kjennelsen bør ankes, og, hvis kjennelsen ankes, gi grunnlag for ankedomstolens behandling av anken. Hvor omfattende begrunnelsen skal være, må avgjøres konkret, og vil kunne variere fra sak til sak.

Første ledd *fjerde punktum* fastsetter at retten kan omgjøre kjennelsen. Omgjøring kan for eksempel bli aktuelt hvis EOS-utvalget med grunnlag i § 7-12 fremmer begjæring om stansing og sletting.

Etter *andre ledd første punktum* skal rettens avgjørelse treffes så raskt som mulig. Det vil ofte være tale om tidssensitive saker som må prioriteres høyt. Andre ledd *andre punktum* fastsetter at den som avgjørelsen retter seg mot eller ellers rammer, ikke gis adgang til å uttale seg, og meddeles ikke kjennelsen. Det følger av dette at prosessen ikke er en partsprosess. Hensikten med reglene er å hindre at formålet med innhentingen forfeiles ved at etterretningsmålet blir kjent med innhentingen. I enkelte sakstyper vil innhentingen uansett ikke rette seg mot bestemte personer. For å skape balanse i domstolsprosessen skal retten normalt oppnevne en særskilt advokat som skal målbære samfunnets interesser i et bredere perspektiv, for eksempel personvernhensyn, jf. § 8-5. Det vises til merknadene til den bestemmelsen.

Retten skal meddele kjennelsen til Etterretningstjenesten, jf. *tredje ledd første punktum*. I sin tur skal Etterretningstjenesten gjøre både kjennelsen og begjæringen som ligger til grunn for den tilgjengelig for EOS-utvalget, jf. tredje ledd *andre punktum*.

Til § 8-2

Bestemmelsen stiller krav til Etterretningstjenestens begjæringer om tillatelse etter § 8-1.

Det følger av *første punktum* at begjæringen fremmes for Oslo tingrett av sjefen for Etterretningstjenesten eller den som sjefen gir fullmakt. Etter *andre punktum* skal begjæringen være

skriftlig og inneholde opplysninger som nevnt i *bokstavene a til e*.

Begjæringen skal for det første angi oppdraget som søket eller innhentingen knytter seg til, jf. *bokstav a*. Det skal vises til hvilken lovbestemt oppgave som begrunner søket eller innhentingen, jf. kapittel 3. Det bør normalt også vises til den aktuelle prioriteringen i prioriteringsdokumentet for nasjonale etterretningsbehov (PNEB), den mer detaljerte operasjonaliseringen av PNEB eller den aktuelle informasjonsforespørselen (RFI). Det vises til § 2-2 om oppdragsstyring.

For det andre skal begjæringen angi det faktiske og rettslige grunnlaget for søket eller innhentingen, jf. *bokstav b*. Hensikten med kravet er å sette retten i stand til å vurdere om lovens vilkår er oppfylt, jf. § 8-4. Etterretningstjenesten må legge frem alle opplysninger som er nødvendige for dette formålet. Hvor omfattende redegjørelsen skal være, må avgjøres konkret, og vil kunne variere fra sak til sak. Retten vil alltid kunne be om ytterligere opplysninger dersom den ser behov for det.

Bokstav c gjelder begjæringer om søk i lagrede metadata etter § 7-8. Slike begjæringer skal angi hvilke søkebegreper eller kategorier av søkebegreper som skal brukes. Disse kan knytte seg til en bestemt person eller virksomhet (personselektor) eller et bestemt mønster eller avgrensning (modusselektor). Det vises til merknadene til § 7-8 for en nærmere beskrivelse. At det kan angis kategorier av søkebegreper, innebærer at det ikke oppstilles noe krav om at begjæringen må angi ett eller flere spesifikke søkebegreper. En kategori kan for eksempel være alle identifikatorer som kan knyttes til en bestemt person eller gruppe personer, eller all skadelig programvare som kan knyttes til en trusselaktør på cyberområdet. Ved utformingen av søkebegreper eller kategorier av søkebegreper må det ses hen til kravet til forholdsmessighet etter § 5-4.

Bokstav d gjelder begjæringer om innhenting og lagring av innholdsdata med tilhørende metadata etter § 7-9. I slike begjæringer skal det angis hva eller hvem innhentingen retter seg mot (etterretningsmålet).

Bokstav e fastslår at begjæringen skal angi hvor lenge tillatelsen bør vare. Det vises til § 8-6 om tillatelsens varighet.

Opplistingen i bokstavene a til e er ikke uttømmende, det vil si at det også kan medtas andre opplysninger som Etterretningstjenesten mener er relevante for rettens avgjørelse.

Til § 8-3

Bestemmelsen gir regler om muntlige forhandlinger.

Det følger av *første ledd første punktum* at retten kan beslutte å avholde muntlige forhandlinger. Muntlige forhandlinger vil kunne bidra til å opplyse saken gjennom å gi dommeren mulighet til å stille spørsmål til sakens aktører.

Det er opp til rettens skjønn hvorvidt det bør avholdes muntlige forhandlinger. Hvis retten mener at skriftlig behandling vil gi det beste avgjørelsesgrunnlaget, eller for øvrig ikke ser behov for muntlige forhandlinger, trenger den ikke å fatte beslutning om det.

Etter første ledd *andre punktum* skal Etterretningstjenesten møte ved sjefen for tjenesten eller den som sjefen bemyndiger. Det følger dessuten av første ledd *tredje punktum* at tjenesten kan møte med tjenestepersoner eller andre som kan opplyse saken.

Det ligger i sakens natur at tilrettelagt innhenting må skje i det skjulte overfor berørte personer og offentligheten for øvrig. Noe annet ville undergrave formålet med innhentingen. Det følger derfor av *andre ledd* at rettsmøtene skal holdes for lukkede dører.

Dersom det er oppnevnt særskilt advokat etter § 8-5, skal advokaten varsles om rettsmøtet og har rett til å være til stede der, jf. § 8-5 tredje ledd andre punktum.

Til § 8-4

Bestemmelsen regulerer hva retten skal prøve i saker om forhåndskontroll av tilrettelagt innhenting.

Rettens oppgave er å føre forhåndskontroll av lovligheten av søk etter § 7-8 og innhenting og lagring etter § 7-9. De sentrale vilkårene er uttrykkelig listet opp i bestemmelsen, men opplistingen er ikke uttømmende.

Retten skal prøve om søk og innhenting er innenfor Etterretningstjenestens oppgaver etter kapittel 3. Etterretningstjenesten har et bredt oppgavesett knyttet til utenlandske trusler og forhold, og det er derfor ikke grunn til å tro at retten ofte vil overprøve tjenestens vurdering på dette punktet.

Loven oppstiller enkelte særskilte innhentingsforbud. Noen av disse har i hovedsak en pedagogisk funksjon gjennom å tydeliggjøre og presisere hva som følger av den positive angivelsen av Etterretningstjenestens oppgaver i kapittel 3. Dette gjelder forbudet mot å innhente informa-

sjon med politiformål (§ 4-8) og forbudet mot industrispionasje (§ 4-9). Forbudet i § 4-1 mot å benytte innhentingsmetoder etter kapittel 6 overfor fysiske eller juridiske personer i Norge, har derimot selvstendig betydning. Tilrettelagt innhenting er en form for midtpunktinnhenting etter § 6-9, og forbudet kommer dermed til anvendelse. Det følger av dette at tilrettelagt innhenting ikke kan benyttes overfor personer i Norge, med mindre unntaksbestemmelsen i § 4-2 er aktuell.

I tråd med § 4-7 kan tilrettelagt innhenting benyttes overfor personer i utlandet selv om informasjon om personer i Norge vil kunne følge med. Søk og innhenting vil for eksempel kunne ha til hensikt å avdekke hvilke mål i Norge en utenlandsk trusselaktør gjennomfører digitale angrep mot, eller hvilke personer i Norge som er i kontakt med en fremmed etterretningstjeneste eller et internasjonalt terrornettverk.

Retten skal ikke gi tillatelse til søk eller innhenting som strider med forbudet mot diskriminering i § 9-4, for eksempel fordi det foreslås søkebegreper som utelukkende knytter seg til etnisitet eller nasjonal bakgrunn, politisk, religiøs eller filosofisk overbevisning, språk, politisk virksomhet, fagforeningstilhørighet eller helsemessige eller seksuelle forhold.

Søk i lagrede metadata etter § 7-8 og innhenting og lagring av innholdsdata etter § 7-9 må tilfredsstille grunnvilkårene etter kapittel 5. Hvis begjæringen gjelder målsøking, må det foreligge grunn til å undersøke om søket kan bidra til å frembringe informasjon som er relevant for etterretningsformål. Dette er en relativt lav terskel. Det vises til merknadene til § 5-1. Hvis begjæringen gjelder målrettet innhenting, må det være konkrete holdepunkter som tilsier at det foreligger grunn til å undersøke om etterretningsmålet besitter, kommuniserer eller vil motta, eller om søket på annen måte kan frembringe, informasjon som er relevant for etterretningsformål. Det vises til merknadene til § 5-2.

Retten skal ikke prøve hvorvidt metadata i det hele tatt skal lagres i bulk. At slike data skal lagres, følger av § 7-7. Det er bare spørsmålet om søk i allerede lagrede metadata som skal prøves av retten, jf. § 7-8. Innholdsdata lagres derimot ikke i bulk. Slik informasjon kan bare innhentes og lagres hvis retten tillater det, jf. § 7-9.

Et sentralt vilkår både for søk i lagrede metadata etter § 7-8 og innhenting og lagring av innholdsdata etter § 7-9, er forholdsmessighetskravet som følger av § 5-4. Det må vurderes konkret i den enkelte sak hvorvidt vilkåret er oppfylt. Det vises til merknadene til § 5-4 for en gjennomgåelse av de ulike momentene som skal tas i betraktning. Når det gjelder hvorvidt mindre inngripende tiltak i tilstrekkelig grad kan ivareta formålet, bemerkes at de fleste av metodene som er regulert i kapittel 6 normalt må regnes som større inngrep overfor den enkelte enn søk etter § 7-8 og innhenting og lagring etter § 7-9. Det bør imidlertid vurderes hvorvidt informasjon fra åpne kilder i tilstrekkelig grad kan ivareta formålet.

Til § 8-5

Bestemmelsen gjelder oppnevning av særskilt advokat.

Det følger av *første ledd første punktum* at retten skal oppnevne en advokat etter å ha mottatt begjæring om søk eller innhenting etter § 8-2. Advokaten skal ivareta den enkeltes rettigheter og samfunnets interesser i saken. Oppnevnelse kan bare unnlates dersom retten finner det ubetenkelig, jf. første ledd *andre punktum*. Det ligger i dette at lovens utgangspunkt og hovedregel er oppnevning. Det må avgjøres konkret i hvilke situasjoner det er ubetenkelig å unnlate oppnevning. En sak kan for eksempel ligge slik an hvis den fremstår som oversiktlig, og i mindre utstrekning griper inn i vernede interesser, typisk ved søk eller innhenting om statlige aktører.

Advokaten skal fremføre faktiske og rettslige argumenter som advokaten mener bør være del av domstolens vurdering. Advokaten kan peke på svakheter ved begjæringen, og imøtegå anførsler i den. Advokaten vil ikke ha noen klient i tradisjonell forstand, men skal fungere som en representant for allmennheten, og bidra til balanse i domstolsprosessen. Søket eller innhentingen vil ofte ikke rette seg mot bestemte personer, men advokaten har likevel en viktig rolle i å belyse samfunnets interesser i et bredere perspektiv, for eksempel med hensyn til ytrings- og informasjonsfriheten og diskrimineringsforbudet. I saker som retter seg mot bestemte personer, for eksempel på kontraterrorområdet, skal advokaten også ivareta den enkeltes rettigheter.

Første ledd *tredje punktum* fastsetter at advokaten skal oppnevnes fra en særlig krets av sikkerhetsklarerte advokater. Advokatene som inngår i kretsen bør ha kompetanse innen personvern, menneskerettigheter, etterretnings- og sikkerhetstjeneste, utenriks-, forsvars- og sikkerhetspolitikk, informasjons- og kommunikasjonsteknologi eller andre relevante områder. Det følger også av tredje punktum at oppdraget er strengt personlig. Advokaten kan ikke la seg representere eller møte ved annen advokat eller fullmektig.

Advokaten skal ha godtgjørelse av staten, jf. første ledd *fjerde punktum*.

Etter *andre ledd første punktum* skal advokaten gjøres kjent med begjæringen og annen informasjon som legges frem for retten, men har utover dette ingen innsynsrett. Det følger av andre ledd *andre punktum* at advokaten ikke må sette seg i forbindelse med personer som berøres av saken. Se også § 8-8 om taushetsplikt.

Tredje ledd første punktum fastslår at advokaten har rett til å uttale seg før retten treffer avgjørelse. Slik uttalelse kan gis skriftlig eller muntlig, avhengig av om det avholdes rettsmøte i saken eller ikke. Etter tredje ledd *andre punktum* skal advokaten varsles om rettsmøter og har rett til å delta i dem.

Med grunnlag i *fjerde ledd* kan departementet gi forskrift om oppnevning av advokat etter første ledd, for eksempel om godtgjørelse.

Til § 8-6

Bestemmelsen regulerer tillatelsens varighet.

Hovedregelen etter *første ledd første punktum* er at rettens tillatelse ikke skal gis for lengre tid enn nødvendig. Første ledd *andre punktum* fastsetter at tillatelsen ikke kan overstige ett år hvis den gjelder målsøking etter § 7-8. Etter første ledd *tredje punktum* kan tillatelsen ikke overstige seks måneder hvis den gjelder målrettet innhenting etter §§ 7-8 eller 7-9.

Innenfor rammen av lengstefristene må retten avgjøre tillatelsens varighet konkret i den enkelte sak. Varighet til lengstefristen kan være aktuelt når de faktiske forholdene som har betydning for innhentingen, antas å være stabile i denne perioden. Det kan for eksempel være tilfelle hvis det er tale om søk eller innhenting som gjelder statlige aktører. Hvis det er grunn til å anta at faktiske forhold av betydning vil kunne endre seg i løpet av et kortere tidsrom, bør det gis en kortere tillatelse.

Det følger av *andre ledd* at Etterretningstjenesten skal avslutte pågående søk og innhenting dersom vilkårene etter loven ikke lenger er til stede. Det kan for eksempel være tilfelle hvis nye faktiske omstendigheter gjør fortsatt innhenting uforholdsmessig. Regelen har primært en pedagogisk funksjon, siden en plikt til å avbryte innhentingen hvis vilkårene ikke lenger er oppfylt må sies å følge allerede av lovens system.

Til § 8-7

Bestemmelsen gir regler om informasjonssikkerhet. Av pedagogiske grunner fastsetter *første ledd* at rettens kjennelse skal sikkerhetsgraderes etter reglene gitt i og i medhold av sikkerhetsloven. Det vises til sikkerhetsloven § 5-3 og virksomhetsikkerhetsforskriften.

Etter *andre ledd første punktum* skal domstolen sørge for at informasjon og dokumenter med høyeste sikkerhetsgrad kan behandles i henhold til sikkerhetsloven hos domstolen som ledd i skriftlige eller muntlige forhandlinger. Bestemmelsen er en presisering av sikkerhetsloven § 5-2, som fastsetter at virksomheten skal sørge for et forsvarlig sikkerhetsnivå for skjermingsverdig informasjon. Andre ledd *andre punktum* fastslår at domstolen skal legge til rette for at advokater oppnevnt etter § 8-5 kan gjøres kjent med sikkerhetsgradert informasjon i domstolens lokaler.

Det er ønskelig at rettspraksis gjøres tilgjengelig for dommere som skal behandle saker etter kapittel 8 i den utstrekning det lar seg gjøre innenfor rammen av reglene gitt i og i medhold av sikkerhetsloven. Etter *tredje ledd* kan departementet gi regler om dette i forskrift.

Til § 8-8

Bestemmelsen regulerer taushetsplikt for rettens aktører.

Første ledd første punktum fastslår at dommere og andre som utfører tjeneste eller arbeid for domstolene, har taushetsplikt om begjæringer, rettsmøter, kjennelser og andre opplysninger de får kjennskap til i saker etter kapittel 8. Foruten dommere og domstolens tjenestepersoner, for eksempel saksbehandlere og utredere, omfattes også advokater oppnevnt etter § 8-5 av bestemmelsen.

Etter første ledd *andre punktum* gjelder taushetsplikten også etter at arbeidet eller tjenesten er avsluttet.

Det følger av *andre ledd* at taushetsplikten ikke er til hinder for å gi opplysninger til EOS-utvalget.

For sikkerhetsgradert informasjon gjelder også sikkerhetsloven § 5-4.

Til § 8-9

Bestemmelsen regulerer adgangen til å anke rettens kjennelse.

Første ledd fastsetter at både Etterretningstjenesten og den særskilte advokaten har rett til å anke rettens kjennelse. Ankekompetansen til Etterretningstjenesten utøves av sjefen for tjenesten eller den sjefen gir fullmakt.

Etter *andre ledd første punktum* gjelder reglene i straffeprosessloven kapittel 26 tilsvarende så langt de passer. Det må avgjøres konkret hvilke regler som passer. Det kan være regler om ankefrist (straffeprosessloven § 379 første ledd), den innledende saksbehandlingen ved tingretten (straffeprosessloven § 381 første og andre ledd), at anken som hovedregel ikke har oppsettende virkning (straffeprosessloven § 382 første ledd), at ankedomstolen kan innhente ytterligere opplysninger (straffeprosessloven § 384), ankedomstolens avgjørelse (straffeprosessloven § 385), muntlige forhandlinger når særlige grunner taler for det (straffeprosessloven § 387 første ledd) og anke til Høyesterett (straffeprosessloven §§ 387 a og 388).

Andre ledd *andre punktum* gir § 8-7 om informasjonssikkerhet tilsvarende anvendelse for ankedomstolen.

Til § 8-10

Bestemmelsen regulerer sjefen for Etterretningstjenestens kompetanse til å gi ordre som trer i stedet for rettens kjennelse i kvalifiserte hastetilfeller.

Grunnvilkårene for hastekompetansen følger av *første ledd første punktum*. Regelen er ment som en meget snever unntaksregel som skal brukes med stor varsomhet. Hastekompetansen er derfor begrenset til tilfeller hvor det ved opphold er «stor fare» for at informasjon «av vesentlig betydning» for utførelsen av Etterretningstjenestens oppgaver etter kapittel 3, kan gå tapt. Kompetansen ligger til sjefen for Etterretningstjenesten, og kan ikke delegeres.

Saken skal straks, og senest innen 24 timer, forelegges for retten, jf. første ledd *andre punktum*. Retten skal på vanlig måte prøve lovligheten av søket eller innhentingen, og avgjør ved kjennelse om den kan tillates, jf. *andre ledd første punktum*. Hvis retten kommer til at søket eller innhentingen var ulovlig, skal retten meddele dette til EOS-utvalget. Retten kan dessuten pålegge Etterretningstjenesten å slette innhentet informasjon.

Til kapittel 9

Til § 9-1

Første ledd fastsetter at kapittel 9 gjelder for Etterretningstjenestens behandling av personopplysninger for etterretningsformål. Det er utelukkende behandling for etterretningsformål som er unntatt fra personopplysningsloven. Det er en forutsetning at personopplysningene behandles helt eller delvis automatisert eller behandles ikke-automatisert og inngår i eller skal inngå i et register, jf. personopplysningsloven § 2 første ledd første punktum og personvernforordningen artikkel 2 nr. 1.

I *andre ledd* presiseres det at personopplysningsloven 2018 og personvernforordningen gjelder for de tilfellene hvor Etterretningstjenesten behandler personopplysninger for andre formål. Dette kan for eksempel være der tjenesten behandler personopplysninger om sine ansatte for å ivareta sine plikter som arbeidsgiver. Et annet eksempel er opplysninger som i første omgang er lagret for etterretningsformål, men som man ønsker å behandle for andre formål senere, for eksempel viderebehandling for historiske, statistiske eller vitenskapelige formål. Dersom tjenesten skal behandle personopplysninger til disse formålene, må de oppfylle kravene til viderebehandling i personvernforordningen.

Til § 9-2

Paragrafen fastsetter behandlingsgrunnlaget for Etterretningstjenestens behandling av personopplysninger. Tjenesten kan behandle personopplysninger når det er nødvendig for etterretningsformål.

Etterretningsformål er formål om å ivareta en eller flere av tjenestens oppgaver etter kapittel 3, se § 1-3 bokstav c. Det vil altså være oppgavene i kapittel 3 som danner rammen for hva Etterretningstjenesten kan behandle personopplysninger for. Behandling av personopplysninger for å oppfylle lovens krav ligger innenfor hva som er å anse som etterretningsformål. Dette innebærer for eksempel at personopplysninger om kilder som ikke ønsker å samarbeide med Etterretningstjenesten, kan behandles for å hindre at vedkommende kontaktes igjen. Det samme gjelder personopplysninger som er nødvendig å behandle for å hindre innhenting i strid med innhentingsforbudet i § 4-1. Dersom Etterretningstjenesten skal behandle personopplysninger til *andre formål* enn etterretningsformål, kommer personopplysningsloven 2018 og personvernforordningen til anvendelse, jf. § 9-1 andre ledd.

I tillegg til krav om etterretningsformål, oppstiller bestemmelsen et vilkår om at tjenesten bare kan behandle personopplysninger til etterretningsformål dersom det er *nødvendig*. Både opplysningene og behandlingsformen må være nødvendig for å oppnå formålet. I dette ligger samtidig et krav om at opplysningene må være adekvate og relevante for formålet. Kravene til ade-

kvans og relevans innebærer at opplysningene skal ha nær og naturlig sammenheng med behandlingsformålet, og være egnet til å oppnå formålet.

Etterretningstjenesten har behov for å samle inn og lagre store mengder informasjon, noe som får betydning for *når* tjenesten har mulighet til å gjøre en vurdering av nødvendighet.

Vurderingen av nødvendighet vil falle ulikt ut for opplysninger som er samlet inn i bulk og andre opplysninger. For personopplysninger som er rådata i bulk, ligger det i metodens natur at nødvendighetsvurderingen må gjennomføres overordnet etter at rådata er innhentet etter § 5-3, og ellers når ny informasjon eller andre omstendigheter tilsier det. At det foretas en vurdering av om det er nødvendig å innhente rådata i bulk, innebærer ikke at Etterretningstjenesten har evaluert de aktuelle dataenes etterretningsmessige verdi.

For andre personopplysninger skal nødvendighetsvurderingen alltid gjennomføres når personopplysningene vurderes brukt for etterretningsformål. Så lenge informasjonen ikke benyttes til etterretningsprodukter, må Etterretningstjenesten gjennomføre en vurdering av om fortsatt lagring er nødvendig hvis ny informasjon eller andre omstendigheter tilsier det.

Det er som utgangspunkt ingen begrensninger i *hvem* Etterretningstjenesten kan behandle personopplysninger om. Reglene i kapittel 4 begrenser tjenestens adgang til å innhente informasjon om personer i Norge. Det medfører imidlertid ikke et forbud mot å behandle personopplysninger om personer i Norge.

Bestemmelsen må leses i sammenheng med § 9-8 om sletting, som stiller krav til at opplysningene skal slettes dersom de ikke lenger er nødvendig å behandle for formålet.

Til § 9-3

Bestemmelsen fastsetter unntak fra behandlingsreglene i kapittel 9 for behandling i form av *innhenting* av personopplysninger. Innhenting av personopplysninger er regulert i kapitlene 3 til 8. Det anses derfor som mest hensiktsmessig å skille ut denne formen for behandling fra behandlingsreglene i kapittel 9. Diskrimineringsforbudet som følger av § 9-4, gjelder imidlertid også for behandling i form av innhenting.

Til § 9-4

Paragrafen lovfester et diskrimineringsforbud i relasjon til behandling av personopplysninger for etterretningsformål. Bestemmelsen må tolkes i lys av likhetsprinsippet og ikke-diskrimineringsprinsippet som følger av Grunnloven § 98.

Diskrimineringsforbudet innebærer at Etterretningstjenesten ikke kan basere sin behandling av personopplysninger *utelukkende* på bakgrunn av det som er kjent om en persons etnisitet, nasjonale bakgrunn, politiske, religiøse eller filosofiske overbevisning, språk, politiske virksomhet, fagforeningstilhørighet eller helsemessige eller seksuelle forhold. Forbudet innebærer for eksempel at det ikke kan lages en liste over alle personer som tilhører en bestemt trosretning, eller iverksettes målrettet innhenting mot en person bare på grunn av personens politiske virksomhet.

Diskrimineringsforbudet spiller sammen med grunnvilkårene for informasjonsinnhenting etter §§ 5-1 og 5-2 på den måten at en opplysning om forhold som nevnt i diskrimineringsforbudet, ikke alene kan gi «grunn til å undersøke» om innhenting kan frembringe informasjon som er relevant for etterretningsformål.

Til § 9-5

Bestemmelsen gjelder behandling av enkelte typer fortrolig kommunikasjon. Det vises til punkt 12.8.6.

Første ledd forbyr Etterretningstjenesten å behandle informasjon som er betrodd en yrkesutøver som er nevnt i straffeprosessloven § 119 og tvisteloven § 22-5 i kraft av stillingen. Forbudet gjelder bare dersom yrkesutøveren, den som betror seg eller begge er bosatt i Norge eller norsk statsborger på tidspunktet betroelsen gis. Bakgrunnen er den spesielle relasjonen mellom partene, som er tuftet på en forutsetning om konfidensialitet. Brudd på denne konfidensialiteten kan medføre en risiko for at borgerne vegrer seg for å benytte tilbud som er sentrale for deres helse, velferd og rettssikkerhet, slik som bistand fra advokat eller helsehjelp.

Andre ledd slår fast at det kan gjøres unntak fra hovedregelen dersom de hensyn som begrunner vernet av den fortrolige kommunikasjonen, må vike for nasjonale sikkerhetsinteresser. Nødvendighets- og forholdsmessighetsvurderingen som må foretas i det enkelte tilfellet, vil avhenge av hvilken type taushetsbelagt kommunikasjon det er tale om. For eksempel stilles det strengere krav til nødvendigheten og forholdsmessigheten av behandlingen dersom den taushetsbelagte kommunikasjonen er mellom advokat og klient. Terskelen må vurderes konkret i den enkelte sak, og vil avhenge av vernets utstrekning etter Grunnlo-

ven § 102, EMK artikkel 8 og andre relevante menneskerettslige regler.

Det ligger i kravet til streng nødvendighet at det må være strengt nødvendig å behandle informasjonen for å bidra til å løse en eller flere av Etterretningstjenestens oppgaver etter lovforslaget kapittel 3. Formålet med behandlingen må etter en konkret vurdering regnes som mer tungtveiende enn de hensyn som begrunner vernet. Der det er tale om kommunikasjon som nyter et sterkt menneskerettslig vern, må formålet med behandlingen normalt være knyttet til forhold av alvorlig karakter som ligger innenfor rammen av oppgavene i § 3-1 (utenlandske trusler mot Norge). For at kravet om streng nødvendighet skal anses oppfylt, må det være umulig eller uforholdsmessig vanskelig å skaffe opplysninger som kan bidra til å løse den aktuelle oppgaven på en mindre inngripende måte. Det presiseres at Etterretningstjenesten plikter å slette opplysningene uten unødig opphold dersom de ikke lenger er nødvendig å behandle for formålet, jf. § 9-8.

Beslutningen om å behandle fortrolig kommunikasjon skal fattes av sjefen for Etterretningstjenesten, jf. *tredje ledd første punktum*. Kompetansen kan ikke delegeres. Beslutningen skal være skriftlig og redegjøre for det faktiske og rettslige grunnlaget for behandlingen, jf. tredje ledd *andre punktum*. Etter tredje ledd *tredje punktum* skal beslutningen om å behandle fortrolig kommunikasjon meddeles EOS-utvalget.

Til § 9-6

Bestemmelsen gjelder behandling av journalistisk materiale som er egnet til å avsløre identiteten til en kilde. Den må tolkes og anvendes i samsvar med kildevernet som følger av Grunnloven § 100, EMK artikkel 10 og SP artikkel 19. Det vises til punkt 12.8.6.

Første ledd første punktum forbyr Etterretningstjenesten å behandle opplysninger som er betrodd noen i deres journalistiske virke, dersom opplysningene kan avsløre hvem som har avgitt dem. Det er for det første et vilkår at opplysningene er gitt under forutsetning om anonymitet, jf. begrepet «betrodd». I tillegg må den aktuelle opplysningen være *egnet til* å avsløre identiteten til den som har avgitt den. I vurderingen må det ses hen til om opplysningen kan bidra til å «sirkle inn» kilden, for eksempel dersom den sammenstilles med andre opplysninger og hvor kildens identitet fremgår av sammenhengen.

I kjernen av begrepet «journalistisk virke» er samfunnsrelatert journalistikk i en medievirksomhet ledet av en person med oppgaver tilsvarende en ansvarlig redaktør, og som er tilsluttet pressens selvdømmeordning med tilhørende etiske retningslinjer. Også annen medievirksomhet kan regnes som «journalistisk virke», herunder virksomheten til frilansere, dokumentarfilmskapere, forfattere og journaliststudenter. I vurderingen må det ses hen til om virksomheten ivaretar en samfunnsfunksjon og har et journalistisk formål, herunder om den har til formål å legge til rette for en åpen og opplyst offentlig debatt, avsløre kritikkverdige forhold eller lignende. Begrepet må for øvrig forstås i samsvar med utviklingen etter Grunnloven § 100 og EMK artikkel 10.

Aktører som ikke driver reell journalistisk virksomhet, for eksempel produksjon av propaganda for en terrororganisasjon, vernes ikke av bestemmelsen. I spesielle tilfeller kan det tenkes at en person driver legitim journalistisk virksomhet samtidig som vedkommende er et relevant etterretningsmål, for eksempel fordi personen arbeider på vegne av en fremmed stats etterretningstjeneste. Behandlingsforbudet må som et utgangspunkt respekteres i et slikt tilfelle, men det må antas at terskelen for å behandle opplysningene stort sett vil være oppfylt dersom overholdelse av forbudet vil gagne virksomheten som gjør personen til et legitimt etterretningsmål.

Behandlingsforbudet får ikke anvendelse før det foreligger konkrete holdepunkter for at det aktuelle informasjonsgrunnlaget med sannsynlighet inneholder betrodde opplysninger som kan avsløre en kilde. Det oppstilles ingen aktivitetsplikt før slike holdepunkter foreligger. Tidspunktet for når Etterretningstjenesten må anses å ha konkrete holdepunkter, vil variere etter omstendighetene. Dersom det er tale om målrettet innhenting mot kjente selektorer, vil det være mer nærliggende at tjenesten har kunnskap om at opplysningene som innhentes, kan være vernet. I slike tilfeller gjelder forbudet fra innhentingstidspunktet. På den andre siden vil det ikke være mulig for tjenesten å vite om rådata i bulk inneholder slike opplysninger før disse dataene evalueres på et senere tidspunkt. Det er ikke før en slik evaluering skjer, at bestemmelsen får anvendelse.

Det følger videre av første punktum at forbudet kun gjelder dersom personen som driver journalistisk virke, eller som betror seg til denne, er bosatt i Norge, er norsk statsborger eller arbeider på oppdrag for en virksomhet i Norge som er omfattet av mediefridomslova § 2. Det sistnevnte alternativet tar sikte på utenlandske journalister mv. som har en form for formalisert relasjon til den norske virksomheten, for eksempel i form av

en arbeidskontrakt eller ved at den aktuelle virksomheten kjøper artikler eller reportasjer fra en utenlandsk frilanser.

Etter første ledd *andre punktum* gjelder forbudet tilsvarende for personer som på betroelsestidspunktet oppfylte vilkårene etter første punktum.

Andre ledd åpner for at det kan gjøres unntak fra forbudet i første ledd. Unntaket er formulert likt som i § 9-5, men vil trolig praktiseres strengere som følge av den høye terskelen som gjelder for behandling av kildeidentifiserende opplysninger etter gjeldende rett. Det må være strengt nødvendig for Etterretningstjenestens oppgaveløsning å behandle de vernede opplysningene. I kravet ligger for det første at de aktuelle opplysningene må være av vesentlig betydning for utførelsen av et konkret etterretningsformål, og at informasjonen er tilnærmet umulig å tilveiebringe på en annen, mindre inngripende måte. For det andre vil kildevernet kun vike dersom formålet med behandlingen veier tyngre enn hensynet til kildevernet. Dette vil i hovedsak utelukkende være aktuelt der formålet med behandlingen er å løse oppgaver etter lovforslaget § 3-1 (utenlandske trusler mot Norge). I forholdsmessighetsvurderingen vil risikoen for at kilder vil unnlate å gi informasjon til personer som driver journalistisk virksomhet som følge av frykt for å bli identifisert, det vil si risikoen for en nedkjølende effekt på pressens kildetilfang, stå sentralt.

Det presiseres at Etterretningstjenesten plikter å slette opplysningene uten unødig opphold dersom de ikke lenger er nødvendig å behandle for formålet, jf. § 9-8.

Tredje ledd første punktum slår fast at beslutningsmyndigheten er lagt til departementet etter reglene om foreleggelse i § 2-5. Beslutningen skal være skriftlig og inneholde en redegjørelse for det rettslige og faktiske grunnlaget for behandlingen, jf. tredje ledd *andre punktum*. Det følger av tredje ledd *tredje punktum* at beslutningen skal meddeles EOS-utvalget.

Til § 9-7

Bestemmelsens *første ledd* stiller krav til at personopplysningene som behandles så langt som mulig skal være korrekte og oppdaterte. At de *så langt det er mulig* skal være korrekte og oppdaterte, innebærer at Etterretningstjenesten nødvendigvis må kunne behandle ikke-verifiserte personopplysninger. Samtidig plikter tjenesten å forsøke å verifisere personopplysningene i den grad det er mulig. Personopplysninger som det ikke er mulig å verifisere, kan behandles så lenge det er nødvendig ut fra formålet med behandlingen.

Etterretningstjenesten skal sørge for at personopplysningene oppdateres, slik at informasjonen de gir, stemmer med virkeligheten. Bakgrunnen for dette er at opplysninger som ikke er oppdaterte, kan gi et misvisende eller uriktig bilde av personen de omhandler.

Personopplysninger som viser seg å ikke være korrekte, skal i utgangspunktet slettes eller rettes. Dette har sammenheng med kravet om nødvendighet og formålsbestemthet. Hvis opplysningene som er samlet inn ikke viser seg å være riktige, vil det normalt heller ikke være nødvendig å behandle personopplysningene. Sletteplikten fremgår i utgangspunktet av § 9-8, men er presisert i bestemmelsen her for å understreke sammenhengen. Det gjelder som utgangspunkt et tilsvarende krav for opplysninger som ikke er oppdaterte, med mindre det fremgår uttrykkelig eller av sammenhengen at opplysningen likevel er relevant, for eksempel fordi den sier noe om en persons historikk. For ordens skyld vil departementet understreke at det vil forekomme tilfeller hvor Etterretningstjenesten må kunne behandle ukorrekte opplysninger. Det vil for eksempel kunne dreie seg om avdekking av en fremmed stats påvirkningsoperasjon, hvor det fremsettes uriktige opplysninger om navngitte personer. I tjenestens behandling av opplysningene vil det av konteksten imidlertid klart fremgå at opplysningene ikke er korrekte. Kravet om sletting eller retting av opplysningene vil ikke gjelde for disse tilfellene, selv om opplysningene er åpenbart feilaktige.

Andre ledd fastsetter en plikt til å gjøre eksterne mottakere av etterretningsinformasjon oppmerksomme på personopplysninger som ikke er verifiserte. Det innebærer blant annet at det må fremgå av Etterretningstjenestens produkter dersom de inneholder ubekreftede personopplysninger. Kravet skal sørge for at mottakeren av opplysningene skal kunne ta hensyn til dette.

Til § 9-8

Etter *første ledd* skal Etterretningstjenesten slette personopplysninger når de ikke lenger er nødvendige for formålet med behandlingen. Det vises til merknadene til § 9-2 om nødvendighetsvurderingen.

I *andre ledd første punktum* er det fastsatt en sletteplikt senest etter 15 år for rådata i bulk, se § 1-3 bokstavene h og i. Begrepet «senest» skal forstås slik at dataene skal slettes på et tidligere

tidspunkt dersom Etterretningstjenesten vurderer at datasettet som sådan ikke lenger har etterretningsmessig verdi, basert på at ny informasjon eller andre omstendigheter tilsier at Etterretningstjenesten er pålagt å foreta en nødvendighetsvurdering.

Dersom vesentlige etterretningsfaglige hensyn krever det, kan sletting utsettes i inntil fem år av gangen. Det vil blant annet kunne være tilfelle dersom opplysninger i datasett som fortsatt anses viktig for etterretningsformål, ikke kan innhentes med andre, mindre inngripende virkemidler. Dette formodes kun å være tilfelle unntaksvis. Beslutning om forlengelse skal fattes av sjefen for Etterretningstjenesten, jf. andre ledd *andre punktum*. Det presiseres i andre ledd *tredje punktum* at metadata som er innhentet og lagret i bulk i samsvar med lovforslaget § 7-7, skal slettes senest etter 18 måneder, jf. § 7-7 tredje ledd.

Tredje ledd åpner for at personopplysningene kan lagres i medhold av annen lov, for eksempel arkivlova.

Til § 9-9

Paragrafen regulerer krav til informasjonssikkerhet ved behandling av personopplysninger. Den er utformet etter mønster av personopplysningsloven 2000 § 13, og er nærmere omtalt i punkt 12.11.

Første ledd innebærer at Etterretningstjenesten skal ha en systematisk og planmessig tilnærming til arbeidet med informasjonssikkerhet. Dette skal sikre at opplysningene til enhver tid er underlagt tilfredsstillende sikkerhet, og at etablerte tekniske og organisatoriske tiltak fungerer som forutsatt.

Kravet til *konfidensialitet* skal sikre at opplysninger er utilgjengelige for uvedkommende, også for egne medarbeidere som ikke er autorisert for tilgang til opplysningene. Konfidensialiteten skal sikres under lagring, overføring og behandling på annen måte. Kravet til *integritet* skal sikre at opplysningene ikke endres eller ødelegges utilsiktet, samt at uvedkommende forhindres fra å gjøre dette. Kravet til *tilgjengelighet* innebærer at opplysningene skal være tilgjengelig for autoriserte brukere når opplysningene behandles i samsvar med det formål de er samlet inn for.

Dersom sikkerhetslovens krav til informasjonssikkerhet er oppfylt, vil også informasjonssikkerhetskravet som alminnelig personvernprinsipp være oppfylt, jf. første ledd *andre punktum*. Bestemmelsen må altså i første rekke ses i lys av sikkerhetslovens regler om informasjonssikkerhet.

Andre ledd fastsetter krav om tilgangsstyring knyttet til personopplysningene. For sikkerhetsgradert informasjon følger dette kravet også av sikkerhetsloven. Det er kun personell med tjenstlig behov som skal ha tilgang til personopplysningene.

Til § 9-10

Paragrafen fastsetter krav om at Etterretningstjenesten skal ha minimum én personvernrådgiver. Begrepet skiller seg fra personvernombud etter personvernforordningen for å synliggjøre forskjellen mellom de to rollene. Det vises til punkt 12.12.4 for en nærmere beskrivelse.

Det legges til grunn at personen som utpekes som personvernrådgiver, må ha en reell mulighet til å gjennomføre opplæring av ansatte og bidra med rådgivning og veiledning i konkrete saker, i tillegg til å få tilgang til nødvendig dokumentasjon i forbindelse med internkontroll.

Personvernrådgiveren skal i tillegg til å bidra til etterlevelse av reglene om behandling av personopplysninger, kunne motta varsler fra ansatte i Etterretningstjenesten om avvik og brudd på kravene til behandling av personopplysninger etter loven. Bestemmelsen forutsetter at det fastsettes interne rutiner for personvernrådgiverens håndtering av varsler.

Til kapittel 10

Til § 10-1

Første ledd fastsetter at Etterretningstjenesten skal samarbeide med andre norske myndigheter om grenseoverskridende trusler, forsvar mot og håndtering av alvorlige hendelser i det digitale rom samt andre prioriterte saksområder.

Med «grenseoverskridende trusler» menes trusler fra fremmede aktører mot Norges stats- og samfunnssikkerhet ved hjelp av en eller flere aktører i Norge, eller trusler som krysser grensen på annen måte. Slike trusler kan for eksempel være terrorisme, etterretningsvirksomhet og spredning av masseødeleggelsesvåpen.

Med «alvorlige hendelser i det digitale rom» menes reelle og potensielle uønskede hendelser i det digitale rom rettet mot samfunnskritisk infrastruktur, informasjon eller funksjoner. Det kan for eksempel være hendelser som direkte eller potensielt ødelegger fysiske eller logiske sammenkoblinger av informasjonssystemer, herunder nettverksenheter, kommunikasjonsinfrastruktur, lagringsmedier og data. Ødeleggelsene kan materialisere seg ved at digitale komponenter tar fysisk

skade eller omprogrammeres, eller ved at hendelsen kan medføre personell, materiell, samfunnsmessig eller økonomisk skade av et betydelig omfang. Eksempler på alvorlige hendelser i det digitale rom kan være bruk av det digitale domenet for å stjele sensitiv informasjon, sabotere kritisk infrastruktur eller påvirke demokratiske prosesser.

Formuleringen «andre prioriterte saksområder» innebærer at Etterretningstjenesten kan pålegges å samarbeide med andre norske myndigheter dersom saksområdet er prioritert på linje med arbeidet for å motvirke grenseoverskridende trusler og alvorlige hendelser i det digitale rom.

Bestemmelsen skal ikke leses motsetningsvis. Selv om det ikke fremgår direkte av bestemmelsen, kan Etterretningstjenesten fortsatt samarbeide med andre norske offentlige myndigheter, herunder gjennom utlevering av informasjon og felles operasjoner.

Andre ledd første punktum slår fast at Etterretningstjenesten skal etablere og opprettholde etterretningssamarbeid med andre land, forsvarsallianser som Norge deltar i, og andre internasjonale organisasjoner. Samarbeidet kan være bi- eller multilateralt. Prioriterte samarbeidspartnere kan endre seg over tid og i lys av endringer i trusselbildet, og bestemmelsen innebærer ingen plikt til å inngå forpliktende samarbeid med enhver mulig relevant tjeneste eller organisasjon. Bestemmelsen må leses i sammenheng med § 3-4, som gir Etterretningstjenesten hjemmel til å innhente og analysere informasjon for internasjonale samarbeidspartnere dersom dette er i Norges interesse.

Andre ledd *andre punktum* henviser til § 2-5, som sier at Etterretningstjenesten skal forelegge saker om etablering av samarbeid og avtaler med utenlandske tjenester eller internasjonale organisasjoner (inkludert forsvarsallianser som NATO) for departementet.

Til § 10-2

Bestemmelsen oppstiller i *første ledd* en rekke kumulative vilkår som må være oppfylt før etterretningsinformasjon kan utleveres til norske myndigheter. Vilkårene gjelder også for utlevering som ledd i internasjonalt samarbeid, jf. § 10-3, som også oppstiller ytterligere vilkår ved slik utlevering.

Bokstav a oppstiller tre alternative formål med utleveringen. Utleveringen kan for det første skje for etterretningsformål. Det innebærer at formålet med utleveringen er å ivareta en eller flere av Etterretningstjenestens oppgaver etter lovens kapittel 3, jf. legaldefinisjonen i § 1-3 bokstav c. For det andre kan utlevering skje dersom det er nødvendig for å fremme mottakerens oppgaver. For det tredje kan utlevering skje for å hindre at virksomhet blir utøvd på en uforsvarlig måte. En tilsvarende bestemmelse finnes i politiregisterloven § 30 første ledd. Det presiseres at overskuddsinformasjon som stammer fra tilrettelagt innhenting, ikke kan utleveres, jf. § 7-13.

Bokstav b slår fast at utlevering av informasjon som Etterretningstjenesten har mottatt fra en tredjepart, skal skje med tredjepartens samtykke. Bestemmelsen reflekterer tredjepartsprinsippet og informasjonseierskapsprinsippet.

Etter *bokstav c* kan utlevering av *personopplysninger* bare skje dersom Etterretningstjenesten kan behandle opplysningene etter loven kapittel 9. Det presiseres i den sammenheng at utlevering utelukkende for å fremme mottakers interesser eller for å hindre at virksomhet blir utøvd på en uforsvarlig måte i første ledd bokstav a, vil være et annet formål enn etterretningsformål. Utlevering for disse formålene må skje i tråd med personopplysningsloven 2018 og personvernforordningen, jf. § 9-1 andre ledd.

Etter *bokstav d* må utleveringen være forholdsmessig, jf. § 5-4. Det skal blant annet tas hensyn til om det finnes mindre inngripende tiltak enn utlevering av personopplysninger som i tilstrekkelig grad kan ivareta det samme formålet, hvordan utleveringen virker inn på den som personopplysningene gjelder, og sakens betydning, herunder om det er tale om en konkret etterretningsoperasjon eller innhentingsvirksomhet av mer generell art.

Bokstav e fastslår at utleveringen må være forsvarlig i lys av opplysningenes kvalitet, hvem som er mottaker av opplysningene og hvordan mottaker antas å bruke dem. Bestemmelsen må leses i sammenheng med § 9-7, som pålegger Etterretningstjenesten å påse, så langt det er mulig, at personopplysninger som behandles, er oppdaterte og korrekte. Bestemmelsen innebærer videre at Etterretningstjenesten ikke kan dele opplysninger uten henblikk til hvordan mottakeren behandler eller antas å behandle opplysningene og dem som opplysningene omhandler. Selv om Etterretningstjenesten aldri vil kunne garantere at mottakeren behandler opplysningene på en forsvarlig måte, vil denne aktsomhet- og risikovurderingen bidra til å redusere misbruksrisikoen, herunder risikoen for at enkeltpersoner utsettes for overgrep.

Bokstav f fastsetter krav om at utleverte opplysninger må forventes å bli forsvarlig sikkerhetsmessig behandlet hos mottakeren. Vilkåret inne-

bærer at mottakeren må ha tilstrekkelig sikre systemer og prosedyrer for lagring og behandling av informasjonen som utleveres, og at mottakeren ivaretar grunnleggende krav til sikkerhet og konfidensialitet.

Andre ledd slår fast at utlevering med sikte på innhenting eller andre tiltak hos mottaker på vegne av Etterretningstjenesten, bare kan skje dersom tjenesten selv kunne ha innhentet informasjonen eller gjennomført det aktuelle tiltaket. Bestemmelsen er inntatt av pedagogiske hensyn, og understreker det allerede gjeldende forbudet mot å omgå blant annet forbudet mot å innhente informasjon i Norge i § 4-1.

Tredje ledd oppstiller krav om at utleveringen skal skje med notoritet. Notoritetskravet har som formål å sikre sporbarhet om hvem som har behandlet opplysningene, hvordan behandlingen har skjedd og hvilke vurderinger som ligger bak behandlingen. Kravet gjør det mulig å ettergå hvilke opplysninger som er utlevert og til hvem, samt eventuelle vilkår som Etterretningstjenesten har stilt overfor mottakeren for behandling av opplysningene og adgang til å dele opplysningene med tredjepart. Notoritet er særlig viktig av hensyn til EOS-utvalgets kontroll.

Fjerde ledd fastsetter at vilkårene ikke gjelder for utlevering av informasjon til EOS-utvalget og andre tilsyns- og kontrollinstanser.

Til § 10-3

Bestemmelsen fastsetter hvilke vilkår som må være oppfylt for at Etterretningstjenesten skal kunne utlevere etterretningsinformasjon som ledd i internasjonalt samarbeid, for eksempel til en samarbeidende tjeneste eller en internasjonal organisasjon.

Det følger av *bokstav a* at vilkårene som følger av § 10-2 må være oppfylt. Det vises til merknadene til den bestemmelsen.

Bokstav b oppstiller som vilkår at utleveringen er under nasjonal kontroll og i Norges interesse. Med *nasjonal kontroll* menes at Etterretningstjenesten skal ha kontroll på hvem opplysningene utleveres til, herunder kunne oppstille vilkår vedrørende utlevering til tredjeparter, samt kontroll på hva slags type data det er tale om å utlevere og fra hvilken innhentingskapasitet disse stammer fra. Formålet med dette vilkåret er å sikre Etterretningstjenestens selvstendighet og integritet overfor utenlandske samarbeidspartnere, samt å legge til rette for etterhåndskontroll. At utleveringen må være i *norsk interesse* innebærer at Norge må dra en fordel ut av utleveringen, for eksempel i form av at utleveringen bidrar til å frembringe ytterligere relevant informasjon, eller ved at innhenting i en utenlandsk samarbeidspartners interesse vil bidra til et styrket samarbeid som kommer Norge til gode. Som ved all annen innhenting, må innhenting i samarbeidende tjenesters interesse skje innenfor Etterretningstjenestens rettslige rammer.

Bokstav c krever at Etterretningstjenesten må oppstille som vilkår for utleveringen 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 Norges interesse at mottakeren gjennomfører innhenting mot. Bestemmelsen i § 4-2 første ledd omfatter utenlandske og statsløse personer som opptrer i Norge på vegne av en fremmed stat eller statslignende aktør. Med *personer* refereres det i bestemmelsen både til fysiske og juridiske personer.

Andre ledd oppstiller et forbud mot utlevering hvis det er en reell risiko for at det kan medvirke til at noen utsettes for tortur eller annen umenneskelig eller nedverdigende behandling eller straff. Det vises til Grunnloven § 93 andre ledd, EMK artikkel 3, SP artikkel 7 og FNs torturkonvensjon. Med *reell risiko* menes omstendigheter der det foreligger konkrete holdepunkter for å tro at de nevnte handlingene har funnet sted eller kan finne sted overfor en eller flere personer. Det er ikke tilstrekkelig at det foreligger en hypotetisk eller teoretisk mulighet for dette. Det er heller ikke tilstrekkelig at den aktuelle utenlandske myndigheten på et tidligere tidspunkt har utført slike handlinger, selv om dette kan inngå et som et moment i vurderingen. Andre momenter i vurderingen kan være hva det aktuelle etterretningssamarbeidet dreier seg om, den samarbeidende parts antatte handlemåte, erfarings- eller etterretningsbasert informasjon, samt annen troverdig informasjon om den samarbeidende partens evne og vilje til å utsette noen for tortur eller annen umenneskelig eller nedverdigende behandling.

Til § 10-4

Bestemmelsen gjelder utlevering av overskuddsinformasjon til andre norske myndigheter. Overskuddsinformasjon defineres som «informasjon som er uten interesse for etterretningsformål», jf. § 1-3 bokstav g. Formuleringen «uten interesse» innebærer at informasjonen ikke kan bidra til å løse Etterretningstjenestens oppgavesett etter kapittel 3, eller at informasjon som har vært rele-

vant for etterretningsformål, ikke lenger kan behandles. Det vises for øvrig til merknadene til § 1-3.

Første ledd fastslår hovedregelen om at overskuddsinformasjon kan deles med norske myndigheter når vilkårene etter § 10-2 er oppfylt. Det presiseres i den forbindelse at utlevering av overskuddsinformasjon skjer for andre formål enn etterretningsformål, noe som medfører at personopplysningsloven 2018 og personvernforordningen kommer til anvendelse, jf. § 9-1 andre ledd.

Andre ledd henviser til forbudet mot utlevering av overskuddsinformasjon som stammer fra tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon. Det vises til § 7-13.

Tredje ledd slår fast at overskuddsinformasjon som er fortrolig kommunikasjon etter § 9-5 eller som er kildeidentifiserende journalistisk materiale etter § 9-6, ikke kan utleveres.

Til § 10-5

Bestemmelsen slår i *første punktum* fast at norske myndigheter kan utlevere informasjon til Etterretningstjenesten uten hinder av lovbestemt taushetsplikt. Utlevering i kraft av bestemmelsen kan bare skje dersom det er nødvendig for forebyggelses- eller sikkerhetsmessige formål innenfor rammen av Etterretningstjenestens oppgaver etter kapittel 3. Begrensningen tilsvarer ordlyden i politiregisterforskriften § 9-6 første ledd nr. 6 og politiloven § 17 f andre ledd bokstav f, og skal forstås på samme måte som etter disse bestemmelsene.

Bestemmelsen er formulert som en adgang, og skal ikke leses som en plikt til å utlevere informasjon selv om vilkårene er oppfylt. Det er opp til avgivende myndighet å avgjøre om utlevering skal finne sted. Avgivende myndighet må bedømme om det er tilstrekkelig grunnlag for utlevering etter den alminnelige personvernlovgivningen, om utlevering vil utgjøre et menneskerettslig inngrep, og i så fall om utleveringen er nødvendig og forholdsmessig. I forholdsmessighetsvurderingen skal hensynet til nasjonale sikkerhetsinteresser veie tungt. Den konkrete avveiningen vil blant annet avhenge av hvem personopplysningene gjelder. Der det er tale om å utlevere sensitive personopplysninger om i Norge tilhørende personer, må formålet med utleveringen normalt være å bidra til å utføre en oppgave etter lovforslaget § 3-1 om utenlandske trusler mot Norge. På den andre siden må det antas at utlevering alltid vil være forholdsmessig der det er tale om opplysninger om en utenlandsk person med fast tilhørighet utenfor norsk territorium. Et annet moment i forholdsmessighetsvurderingen vil være om utleveringen kan bidra til å løse en prekær sak eller en sak der utfallet kan bli alvorlig for norsk stats- eller samfunnssikkerhet. Eksempelvis vil det veie tungt i vurderingen dersom opplysningene gir informasjon som kan bidra til å avdekke eller kartlegge et terrornettverk i utlandet som kan utgjøre en trussel mot Norge, eller der informasjonen omhandler eksport eller innførsel av ulovlig og farlig materiale. For å avhjelpe inngrepets intensitet kan det oppstilles behandlingsvilkår knyttet til de utleverte opplysningene, for eksempel krav om sletting eller at opplysningene ikke kan videreformidles. Andre tiltak vil også kunne redusere styrken i inngrepet, for eksempel anonymisering der personlige opplysninger vil være overskuddsinformasjon.

Det følger av *andre punktum* at første punktum ikke gjelder for taushetsplikt som nevnt i straffeprosessloven § 119 og tvisteloven § 22-5 (profesjonsbasert taushetsplikt) eller taushetsplikt etter straffeprosessloven § 216 i (opplysninger fra kommunikasjonskontroll). Det presiseres at unntaket i andre punktum er ikke til hinder for utlevering av opplysninger i medhold av straffeprosessloven § 216 i første ledd bokstav i, som fastsetter at Politiets sikkerhetstjeneste kan utlevere opplysninger til Etterretningstjenesten dersom det er nødvendig for forebyggelses- og sikkerhetsmessige formål.

Til § 10-6

Bestemmelsen gjelder Etterretningstjenestens adgang til å formidle opplysninger til og fra andre staters myndigheter, typisk en samarbeidende tjeneste, på vegne av andre norske myndigheter.

Første ledd bokstav a oppstiller krav om at den aktuelle norske myndigheten har anmodet Etterretningstjenesten om å formidle opplysningene. *Bokstav b* krever at mottakeren må opplyses om at formidlingen skjer på vegne av vedkommende norske myndighet, og at det ikke er utlevering av informasjon fra Etterretningstjenesten. *Bokstav c* setter krav om at Etterretningstjenesten ikke kan endre opplysningene som skal formidles, legge til egen informasjon eller be mottakeren om å handle på en bestemt måte i lys av opplysningene.

Andre ledd fastslår at mottakeren må opplyses om at videreformidling til tredjepart krever samtykke fra den norske myndigheten, og eventuelt om at slikt samtykke allerede er gitt.

Tredje ledd oppstiller krav om at formidlingen skal skje med notoritet.

Til § 10-7

Første punktum slår fast utgangspunktet om at Etterretningstjenesten kan yte bistand til politiet etter politiloven § 27 a. Det vises til instruks 16. juni 2017 nr. 789 om Forsvarets bistand til politiet. *Andre punktum* fastsetter at bistanden ikke kan ta form av søk eller innhenting etter reglene i kapittel 7 om tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon.

Til kapittel 11

Til § 11-1

Bestemmelsen unntar saksbehandlingen som knytter seg til utførelsen av Etterretningstjenestens oppgaver etter loven fra forvaltningslovens virkeområde, med unntak av forvaltningsloven §§ 13 til 13 f om taushetsplikt.

Til § 11-2

Bestemmelsen fastsetter en særlig taushetsplikt for personer som gjør arbeid eller tjeneste for Etterretningstjenesten.

Første ledd fastsetter at enhver i Etterretningstjenesten har livsvarig taushetsplikt om den informasjonen som de blir kjent med gjennom arbeidet eller tjenesten dersom det kan skade nasjonale sikkerhetsinteresser om den blir kjent for uvedkommende. Begrepet «gjør arbeid eller tjeneste for» skal forstås på samme måte som etter sikkerhetsloven § 5-4 andre ledd. Dermed omfattes oppdrag, verv eller aktivitet for, og andre formaliserte relasjoner til, Etterretningstjenesten, herunder kilder og oppdragstakere. «Nasjonale sikkerhetsinteresser» skal forstås på samme måte som etter sikkerhetsloven § 1-5 nr. 1. Følgelig er taushetsplikten brutt dersom informasjonen som kommer uvedkommende til kjennskap, kan skade landets suverenitet, territorielle integritet og demokratiske styreform, eller overordnede sikkerhetspolitiske interesser knyttet til de øverste statsorganers virksomhet, sikkerhet og handlefrihet; forsvar, sikkerhet og beredskap; forholdet til andre stater og internasjonale organisasjoner; økonomisk stabilitet og handlefrihet; og samfunnets grunnleggende funksjonalitet eller befolkningens grunnleggende sikkerhet.

Andre ledd fastsetter taushetsplikt for opplysninger om tilsettingsforhold i Etterretningstjenesten. Som hovedregel vil slike opplysninger være sikkerhetsgradert, og således omfattes av taushetsplikten i første ledd. For opplysninger om tilsettingsforhold for enkelte personellkategorier, vil det, selv om opplysningene ikke er gradert etter sikkerhetsloven, fortsatt foreligge et skjermingsbehov. Dette både av hensyn til den enkelte selv og av hensyn til tjenestens sensitive virksomhet. Opplysninger om tilsettingsforhold vil derfor, uavhengig av sikkerhetsgradering, være forbundet med lovbestemt taushetsplikt, med mindre taushetsplikten eksplisitt er opphevet for enkelte personellkategorier eller for konkrete ansatte, for eksempel ved at Etterretningstjenesten samtykker til at opplysningene deles, jf. forvaltningsloven § 13 a nr. 1. Taushetsplikten innebærer blant annet at opplysninger om tilsettingsforhold vil være underlagt bevisforbudsreglene i tvisteloven kapittel 22. For sikkerhetsgraderte opplysninger som må holdes hemmelig av hensyn til rikets sikkerhet eller forholdet til fremmed stat, gjelder bevisforbudet i tvisteloven § 22-1. For andre taushetsbelagte opplysninger om tilsettingsforhold, gjelder bevisforbudet i tvisteloven § 22-3 om opplysninger undergitt lovbestemt taushetsplikt.

Tredje ledd fastsetter taushetsplikt for enhver som blir kjent med sikkerhetsgradert informasjon etter § 2-4 tredje ledd. Bestemmelsen sikrer at personer og virksomheter som mottar sikkerhetsgradert informasjon uten å ha nødvendig autorisasjon og klarering, og dermed heller ikke er underlagt sikkerhetsloven, har taushetsplikt om informasjonen.

Fjerde ledd slår fast at informasjon som nevnt i første til tredje ledd ikke kan utnyttes i virksomhet utenfor Etterretningstjenesten. Bestemmelsen tar her sikte på at personer som har avsluttet sitt arbeid i, eller i den aktuelle sammenhengen ikke opptrer på vegne av, Etterretningstjenesten, ikke kan dra fordel av eller på annen måte benytte informasjonen i forbindelse med annen privat eller offentlig virksomhet.

Femte ledd presiserer at taushetsplikten ikke er til hinder for at opplysninger utleveres etter bestemmelsene i etterretningstjenesteloven eller i medhold av annen lov, som for eksempel utlevering til EOS-utvalget etter EOS-kontrolloven. Taushetsplikten er heller ikke til hinder for at opplysningene gjøres kjent for andre i Etterretningstjenesten i samsvar med gjeldende autorisasjonsregler og prinsippet om tjenstlig behov. Med «tjenstlig behov» menes det informasjonsbehovet vedkommende personell har for å kunne utføre sine oppgaver. Etterretningstjenestens personell skal ikke få kjennskap til mer informasjon enn det som er nødvendig av tjenstlige grunner. Hva som er nødvendig, vil måtte vurderes konkret. Taushetsplikten er ikke til hinder for at Etterretnings-

tjenestens personell rapporterer eller lignende til sine oppdragsgivere.

Til § 11-3

Første ledd slår fast at militært personell og sivilt ansatte i Etterretningstjenesten skal ha norsk statsborgerskap og være sikkerhetsklarert for STRENGT HEMMELIG. Med «militært personell» menes vernepliktige, militært tilsatte og andre som har inngått kontrakt om tjeneste med Forsvaret (tjenestepliktige), jf. forsvarsloven § 2. Med «sivilt ansatte» menes personer med fast eller midlertidig ansettelse i Etterretningstjenesten.

Andre ledd gir sjefen for Etterretningstjenesten kompetanse til å bestemme at det er tilstrekkelig med sikkerhetsklarering for HEMMELIG dersom den aktuelle stillingen har et lavere klareringsbehov enn det som kreves ellers i Etterretningstjenesten. Kravet til norsk statsborgerskap gjelder også for disse stillingene.

Til § 11-4

Bestemmelsens formål er å skjerme Etterretningstjenestens ansatte, kilder, kapasiteter, metoder og operasjoner mot offentlig eksponering. Skjerming er i stor utstrekning en nødvendig forutsetning for etterretningsvirksomheten.

Første ledd regner opp hvilke tiltak Etterretningstjenesten kan benytte for å skjerme sine operasjoner. Tiltakene innebærer bruk av dekkstrukturer og uriktige, falske eller villedende identiteter, dokumenter og opplysninger. Det kan i tillegg tas kontroll over, modifiseres eller utplasseres elektronisk utstyr. Formålet med tiltaket må være å skjerme operasjonen. Bestemmelsen er ikke en hjemmel for innhenting av informasjon.

Andre ledd første punktum unntar Etterretningstjenesten fra rapporteringsplikter etter bestemmelser i annen lov når disse ellers ville omfattet vederlag som ytes til kilder og oppdragstakere som ikke er ansatt i tjenesten. Det følger av andre ledd *andre punktum* at slike vederlag ikke skal regnes som skattepliktig inntekt eller inngå i grunnlag for beregning eller avkortning av sosiale ytelser eller lignende som tilkommer mottakeren.

Tredje ledd gir Kongen i statsråd myndighet til å gi bestemmelser som fraviker annen lov dersom dette er nødvendig av skjermingshensyn.

Til § 11-5

Bestemmelsen slår fast den generelle plikten som påligger Etterretningstjenesten til enhver tid å sikre sine arkiver, informasjonssystemer og etterretningsregistre på en slik måte at disse er utilgjengelige for uvedkommende og sikret mot ytre påvirkning. Det er kun autorisert personell med tjenstlig behov og personer som er satt til å føre kontroll og tilsyn med Etterretningstjenesten, som skal ha tilgang til informasjonen som tjenesten besitter.

Til § 11-6

Bestemmelsen slår fast at Etterretningstjenesten skal utarbeide og vedlikeholde beredskapsplaner basert på Nasjonalt beredskapssystem og Forsvarets operative planverk. Formålet med bestemmelsen er å tydeliggjøre plikten til å sørge for at Etterretningstjenestens planverk til enhver tid er oppdatert og i samsvar med det overordnede planverket, og at tjenesten til enhver tid skal være i stand til å opprettholde de spesielle krav til sikkerhet og konfidensialitet som er en forutsetning for oppgaveløsningen. Av pedagogiske hensyn fremheves Etterretningstjenestens plikt til, i fredstid, å forberede tiltak som skal sikre informasjons- og informasjonssystemsikkerhet i tilfelle krise eller væpnet konflikt.

Til § 11-7

Av informasjonshensyn synliggjøres i *første punktum* den klageadgangen som enhver har i samsvar med bestemmelsene i EOS-kontrolloven.

Andre punktum slår fast at Etterretningstjenesten ikke plikter å gi underretning til personer som har vært gjenstand for informasjonsinnhenting som kan innebære et menneskerettslig inngrep. Det understrekes at bestemmelsen ikke innebærer noe forbud mot å gi slik underretning. Dette innebærer at Etterretningstjenesten eller overordnet myndighet etter forholdene kan gi underretning dersom lovbestemt taushetsplikt eller andre regler ikke er til hinder for det, og det for øvrig regnes som sikkerhetsmessig forsvarlig. På grunn av behovet for å skjerme informasjon om Etterretningstjenestens virksomhet, vil underretning likevel sjelden være aktuelt. Det vises til drøftelsen i punkt 14.6.4. Bestemmelsen må ses i sammenheng med den vide klageadgangen som følger av EOS-kontrolloven § 5. Det er ikke et vilkår for å klage til EOS-utvalget at klager kan godtgjøre at han eller hun har vært utsatt for et inn-

grep, og det er derfor ikke nødvendig med underretning for å oppfylle kravet til effektive rettsmidler etter EMK artikkel 13.

Til § 11-8

Bestemmelsen setter for det første straff for den som handler i strid med beslutning om tilrettelegging etter § 7-3, for eksempel ved å unnlate å treffe de nødvendige tiltak for å gjøre utvalgte kommunikasjonsstrømmer tilgjengelig for Etterretningstjenesten. For det andre setter bestemmelsen straff for den som bryter taushetsplikt etter § 7-4. Straffen er i begge tilfeller bot eller fengsel inntil 6 måneder. Medvirkning kan straffes etter straffeloven § 15. Strafferammen innebærer at forsøk ikke kan straffes, jf. straffeloven § 16. Ved brudd på bestemmelsen vil det kunne være aktuelt med foretaksstraff etter straffeloven § 27. Brudd på taushetsplikten kan etter omstendighetene rammes av strengere straffebestemmelser i straffeloven kapittel 17.

Til kapittel 12

Til § 12-1

Bestemmelsen gjelder lovens ikrafttredelse. *Første punktum* fastsetter at loven trer i kraft fra det tidspunktet Kongen bestemmer. *Andre punktum* åpner for at de ulike bestemmelsene i loven kan settes i kraft til ulik tid.

Til § 12-2

Når den nye etterretningstjenesteloven trer i kraft, oppheves lov 20. mars 1998 nr. 11 om Etterretningstjenesten.

Til § 12-3

Bestemmelsen fastsetter endringer i andre lover fra det tidspunktet ny etterretningstjenestelov trer i kraft.

Til endringer i ekomloven

Til § 2-8 nytt fjerde ledd

Av pedagogiske grunner inntas det et nytt *fjerde ledd* som informerer om at det er gitt bestemmelser om tilrettelegging for innhenting av grenseoverskridende elektronisk kommunikasjon i etterretningstjenesteloven kapittel 7. Se nærmere punkt 11.8.7.

Til § 6-2 a første ledd nytt tredje punktum

Paragrafen gjelder opprettelse og bruk av mobilregulerte soner. Tilføyelsen av et nytt *tredje punktum* i første ledd gir Etterretningstjenesten hjemmel til å ta i bruk frekvenser som er tildelt andre for identitetsfanging dersom dette er strengt nødvendig for å innhente informasjon om person som omfattes av etterretningstjenesteloven § 4-2 første ledd (fremmed statsrepresentant). Etterretningstjenesten kan gjøre dette uten forutgående tillatelse fra Nkom, men bare i særskilte tilfeller og i korte tidsrom. Det vises til merknadene til § 4-2 for en nærmere beskrivelse av personkretsen som omfattes av unntaket.

Til § 6-2 a annet ledd

Endringen i *første punktum* innebærer at Etterretningstjenesten, på samme måte som Politiets sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet, skal varsle myndigheten uten ugrunnet opphold etter at frekvenser som er tildelt andre, er tatt i bruk. Varslingen skal skje på en måte som ivaretar Etterretningstjenestens behov for skjerming. Dette innebærer blant annet at vedkommende som håndterer varslingen, må være klarert for STRENGT HEMMELIG etter sikkerhetsloven.

Endringen i *tredje punktum* innebærer at myndigheten i samråd med Etterretningstjenesten skal bestemme om og i tilfelle når rettighetshaverne skal underrettes.

Til § 6-2 a tredje ledd tredje punktum

Myndigheten kan i særskilte tilfeller etter søknad gi tillatelse til Forsvaret til å bruke frekvenser som er tildelt andre for å etablere mobilregulert sone for øvingsformål innenfor Forsvarets permanente øvingsområder. Endringen innebærer at Etterretningstjenesten er unntatt fra denne geografiske begrensningen, slik at tjenesten kan bruke frekvenser til identitetsfanging for øvingsformål også utenfor permanente øvingsområder.

Til endringer i offentleglova

Til § 2 fjerde ledd nytt fjerde punktum

Det tilføyes et nytt *fjerde punktum* i § 2 fjerde ledd som fastsetter at offentleglova ikke gjelder for dokumenter som blir behandlet av Etterretningstjenesten etter etterretningstjenesteloven. Nåværende fjerde punktum videreføres i nytt femte punktum.

Forsvarsdepartementet

t i l r å r :

At Deres Majestet godkjenner og skriver under et framlagt forslag til proposisjon til Stortinget om lov om Etterretningstjenesten (etterretningstjenesteloven).

- - - - - - - - - - - - -

Tilstedeværende statsråder fra Venstre vil uttale:

«Vi har etter en samlet vurdering kommet til at vi ikke kan gi vår tilslutning til lovforslagets kapittel 7 og 8 om tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon. Norske borgeres elektroniske kommunikasjon krysser i stor grad grensen, og forslaget vil føre til at staten lagrer store mengder data om denne kommunikasjonen. Selv om vi anerkjenner de legitime samfunnsbehovene som begrunner forslaget, mener vi at inngrepet i personvernet blir for sterkt. Vi peker særlig på risikoen for formålsutglidning og en nedkjølende virkning på ytringsfriheten. For øvrig gir vi vår tilslutning til lovforslaget.»

Vi HARALD, Norges Konge,

s t a d f e s t e r :

Stortinget blir bedt om å gjøre vedtak til lov om Etterretningstjenesten (etterretningstjenesteloven) i samsvar med et vedlagt forslag.

Forslag
til lov om Etterretningstjenesten (etterretningstjenesteloven)

Kapittel 1. Formål og virkeområde

§ 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
c) sikre at Etterretningstjenestens virksomhet utøves i samsvar med menneskerettighetene og andre grunnleggende verdier i et demokratisk samfunn.

§ 1-2 *Virkeområde*

Loven gjelder for Etterretningstjenesten og for andre enheter og personer underlagt sjefen for Etterretningstjenestens kommando eller instruksjonsmyndighet.

Loven gjelder ikke innhenting og annen behandling av informasjon som utelukkende gjennomføres av Etterretningstjenesten som ledd i en internasjonal operasjon med folkerettslig mandat.

§ 1-3 *Definisjoner*

I denne loven menes med:

a) personopplysning: enhver opplysning om en identifisert eller identifiserbar fysisk person
b) behandling av personopplysninger: enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke
c) etterretningsformål: formål om å ivareta en eller flere av Etterretningstjenestens oppgaver etter kapittel 3
d) etterretningsmål: objekt, person, virksomhet eller annet som informasjonsinnhentingen retter seg mot
e) målsøking: systematisk arbeid for å identifisere nye etterretningsmål
f) målrettet innhenting: systematisk arbeid for å finne informasjon knyttet til identifiserte etterretningsmål
g) overskuddsinformasjon: informasjon som er uten interesse for etterretningsformål
h) rådata: ubearbeidet eller automatisk bearbeidet informasjon i enhver form hvis etterretningsverdi ikke er vurdert
i) bulk: informasjonssamlinger og datasett hvorav en vesentlig andel av informasjonen antas å være irrelevant for etterretningsformål
j) utlevering: enhver formidling av opplysninger, både skriftlig og muntlig, til mottaker utenfor Etterretningstjenesten som ikke utfører tjeneste eller oppdrag for tjenesten.

Kapittel 2. Organisering, styring og kontroll

§ 2-1 *Nasjonal tjeneste*

Etterretningstjenesten er Norges nasjonale utenlandsetterretningstjeneste. Tjenesten er en del av Forsvaret og underlagt forsvarssjefens kommando.

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

§ 2-2 *Oppdragsstyring*

Departementet koordinerer og prioriterer myndighetenes etterretningsbehov, og fastsetter årlig et prioriteringsdokument for nasjonale etterretningsbehov.

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

§ 2-3 *Departementets styring og kontroll*

Departementet ivaretar styring og kontroll med Etterretningstjenesten gjennom forsvarssjefen hvis ikke annet er fastsatt i denne loven. Økonomi- og virksomhetsstyring ivaretas gjennom Koordineringsutvalget for Etterretningstjenesten.

Departementet kan fastsette andre særlige ordninger og rapporteringsrutiner for ivaretakelse av styring og kontroll.

§ 2-4 *Varsling og rapportering*

Etterretningstjenesten skal innenfor rammen av oppgavene etter kapittel 3

a) 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, og
b) 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 bestemmelser kan Etterretningstjenesten varsle og rådgi personer og virksomheter om trusler innenfor rammen av oppgavene etter kapittel 3. Utlevering av sikkerhetsgradert informasjon kan skje uten hensyn til kravene om autorisasjon og sikkerhetsklarering i sikkerhetsloven § 8-1 når dette er strengt nødvendig og sikkerhetsmessig forsvarlig.

§ 2-5 *Saker som skal forelegges departementet for beslutning*

Etterretningstjenesten skal forelegge følgende saker for departementet for 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 særlig viktige saker.

§ 2-6 *EOS-utvalgets og Riksrevisjonens kontroll*

Etterretningstjenesten er underlagt kontroll etter EOS-kontrolloven. I samsvar med § 7-11 fører EOS-utvalget løpende kontroll med tjenestens etterlevelse av bestemmelsene i kapittel 7.

Etterretningstjenesten er underlagt revisjon og kontroll av Riksrevisjonen etter riksrevisjonsloven. Riksrevisjonen skal utpeke bestemte tjenestepersoner til å ivareta revisjon og kontroll av tjenesten. Utpekte tjenestepersoner skal være norske statsborgere og sikkerhetsklarert for STRENGT HEMMELIG. Riksrevisjonen skal være representert i Koordineringsutvalget for Etterretningstjenesten.

§ 2-7 *Orientering til Stortingets president*

Statsråden som er ansvarlig for Etterretningstjenesten, skal årlig orientere Stortingets president om tjenestens virksomhet.

Sjefen for Etterretningstjenesten skal delta ved orienteringen. Stortingets president bestemmer hvem som deltar for øvrig.

§ 2-8 *Andre bestemmelser om tilsyn og kontroll*

Bestemmelsene i personopplysningsloven kapittel 6 og 7 og personvernforordningen kapittel VI til VIII om tilsyn, klage og sanksjoner mv. gjelder ikke overfor Etterretningstjenesten.

Bestemmelsene i ekomloven kapittel 10 gjelder ikke i den utstrekning de vil gi myndigheten innsyn i Etterretningstjenestens virksomhet. Første punktum er ikke til hinder for at myndigheten fører tilsyn med hvordan tilbydere som omfattes av § 7-2, utøver tilretteleggingsplikten.

Domstolene fører kontroll med tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon i samsvar med kapittel 8.

Kapittel 3. Oppgaver

§ 3-1 *Informasjonsinnhenting om utenlandske trusler*

Etterretningstjenesten skal innhente og analysere informasjon om utenlandske 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
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 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
d) planlegging og gjennomføring av nasjonale eller internasjonale militære operasjoner.

§ 3-3 *Okkupasjonsberedskap*

Etterretningstjenesten skal ivareta nasjonal evne til å innhente og formidle informasjon til norske myndigheter dersom Norge helt eller delvis okkuperes.

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

§ 3-4 *Internasjonalt etterretningssamarbeid*

Når det er i Norges interesse, kan Etterretningstjenesten innhente og analysere informasjon om utenlandske trusler og andre forhold som nevnt i dette kapittelet 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 dette kapittelet, 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
d) opprettholde og videreutvikle Etterretningstjenestens informasjonstilganger og metodiske, teknologiske og øvrige evne til å utføre pålagte oppgaver.

Kapittel 4. Forbud mot innhenting i Norge og andre særskilte forbud

§ 4-1 *Forbud mot innhenting i Norge*

Etterretningstjenesten skal ikke benytte innhentingsmetoder etter kapittel 6 overfor personer i Norge.

Ved tvil om en person befinner seg i Norge eller utlandet, skal Etterretningstjenesten søke å avklare forholdet. For dette formålet skal det kun brukes informasjon fra norske myndigheter, utenlandske samarbeidspartnere, åpne kilder eller egen innhenting i utlandet.

§ 4-2 *Fremmed statsaktivitet i Norge*

Etterretningstjenesten kan uten hinder av § 4-1 benytte innhentingsmetoder etter kapittel 6 overfor utenlandske og statsløse personer i Norge som opptrer på vegne av en fremmed stat eller statslignende aktør.

Ved tvil om en person befinner seg i Norge eller utlandet, skal Etterretningstjenesten søke å avklare forholdet. For dette formålet skal det kun brukes informasjon fra norske myndigheter, utenlandske samarbeidspartnere, åpne kilder eller egen innhenting i utlandet.

Når riket er i krig, krig truer eller rikets selvstendighet eller sikkerhet er i fare, kan Kongen bestemme at Etterretningstjenesten uten hinder av § 4-1 kan innhente enhver opplysning som har betydning for Forsvarets evne til å håndtere fiendtlig militær aktivitet.

§ 4-3 *Samordning med Politiets sikkerhetstjeneste*

Etterretningstjenesten skal be Politiets sikkerhetstjeneste om samtykke til innhenting etter § 4-2 første ledd om forhold som også faller inn under beskrivelsen av oppgavene til Politiets sikkerhetstjeneste i politiloven § 17 b første ledd. Ved annen innhenting etter § 4-2 første ledd skal Politiets sikkerhetstjeneste informeres.

§ 4-4 *Åpne kilder som berører personer i Norge*

Etterretningstjenesten kan uten hinder av § 4-1 innhente informasjon om utenlandske forhold fra åpne kilder etter § 6-2 selv om informasjonen er publisert av eller på annen måte berører personer i Norge.

§ 4-5 *Kilderekruttering og kildeverifikasjon i Norge*

Etterretningstjenesten kan uten hinder av § 4-1 innhente informasjon om personer i Norge for å finne, rekruttere og verifisere kilder.

Informasjonen skal innhentes fra åpne kilder eller ved utlevering fra norske myndigheter. Hvis det foreligger tungtveiende sikkerhetsmessige grunner, kan det brukes metoder som nevnt i §§ 6-3 og 6-4.

Det skal ikke innhentes mer informasjon enn strengt nødvendig. Opplysningene skal utelukkende brukes for å finne, rekruttere og verifisere kilder.

§ 4-6 *Trening, øving og testing av utstyr i Norge*

Etterretningstjenesten kan uten hinder av § 4-1 innhente informasjon om personer i Norge når det er strengt nødvendig for å trene, øve eller teste utstyr.

Informasjonen skal utelukkende brukes til å trene, øve og teste utstyr, og skal ikke behandles sammen med annen informasjon. Med mindre den som informasjonen gjelder, samtykker til at den behandles videre, skal informasjonen slettes snarest mulig, og senest når treningen, øvingen eller testingen avsluttes. Arkivlova gjelder ikke for informasjon etter denne paragrafen.

§ 4-7 *Aksessorisk informasjon om personer i Norge*

Etterretningstjenesten kan benytte innhentingsmetoder etter kapittel 6 overfor personer i utlandet selv om informasjon om personer i Norge vil kunne følge med.

Etterretningstjenesten kan innhente rådata i bulk selv om informasjon om personer i Norge vil kunne følge med.

§ 4-8 *Forbud mot å innhente informasjon for politiformål*

Etterretningstjenesten skal ikke innhente eller medvirke til å innhente informasjon for å utføre oppgaver som tilligger politiet eller andre rettshåndhevende myndigheter.

Første ledd er ikke til hinder for utveksling av informasjon etter kapittel 10 eller bistand til politiet i medhold av § 10-7, jf. politiloven § 27 a.

§ 4-9 *Forbud mot industrispionasje*

Etterretningstjenesten skal ikke innhente eller medvirke til å innhente, bearbeide eller utlevere informasjon for å gi selskaper eller andre kommersielle virksomheter eller sektorer konkurransemessige fortrinn.

Kapittel 5. Grunnvilkår for innhenting og utlevering av informasjon

§ 5-1 *Grunnvilkår for målsøking*

Etterretningstjenesten kan iverksette målsøking når det er grunn til å undersøke om innhenting kan frembringe informasjon som er relevant for etterretningsformål.

§ 5-2 *Grunnvilkår for målrettet innhenting*

Etterretningstjenesten kan iverksette målrettet innhenting når konkrete holdepunkter gir grunn til å undersøke om innhenting kan frembringe informasjon som er relevant for etterretningsformål.

§ 5-3 *Grunnvilkår for innhenting av og søk i rådata i bulk*

Etterretningstjenesten kan innhente rådata i bulk når det er nødvendig for å få tilgang til et relevant og tilstrekkelig informasjonsgrunnlag.

Søk i rådata i bulk skal tilfredsstille grunnvilkårene for målsøking eller målrettet innhenting og logges for kontrollformål. Søket skal ikke gjennomføres dersom det vil være et uforholdsmessig inngrep overfor den enkelte.

Søk i rådata med utgangspunkt i et søkebegrep tilknyttet en person som oppholder seg i Norge, kan bare gjennomføres dersom det er strengt nødvendig for å ivareta en oppgave som nevnt i § 3-1. Første punktum gjelder ikke dersom personen er en utenlandsk eller statsløs person som opptrer på vegne av en fremmed stat eller statslignende aktør.

§ 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. Metoder for innhenting av informasjon som kan medføre inngrep overfor den enkelte

§ 6-1 *Generelle vilkår*

Etterretningstjenesten kan for etterretningsformål bruke metoder for innhenting av informasjon i samsvar med bestemmelsene i dette kapittelet når grunnvilkårene etter kapittel 5 er oppfylt, og innhentingen ikke strider mot loven for øvrig.

Metodene kan brukes fordekt overfor personer som er gjenstand for eller på annen måte berøres av dem.

Bruken skal avsluttes dersom lovens vilkår ikke lenger er til stede.

§ 6-2 *Åpne kilder*

Etterretningstjenesten kan innhente åpent tilgjengelig informasjon. Informasjon er ikke åpent tilgjengelig dersom tilgang krever aktiv fordekt opptreden eller forsering av passord eller lignende beskyttelsesmekanismer.

§ 6-3 *Menneskebasert innhenting*

Etterretningstjenesten kan innhente informasjon gjennom systematisk samhandling med mennesker i det fysiske eller digitale rom. Tjenesten kan finne, verifisere, kultivere, rekruttere, trene og føre kilder i den hensikt å innhente ikke åpent tilgjengelig informasjon eller legge til rette for slik innhenting.

§ 6-4 *Systematisk observasjon*

Etterretningstjenesten kan foreta systematisk observasjon på offentlig sted hvor det er sannsynlig at etterretningsmål vil befinne seg. Det samme gjelder mot privat lukket sted dersom den som observerer, befinner seg utenfor. Det kan tas i bruk hjelpemidler for observasjon samt 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 etterretningsmål.

§ 6-5 *Teknisk sporing*

Etterretningstjenesten kan plassere teknisk peileutstyr i det fysiske rom på eller ved et etterretningsmål for å kartlegge målets posisjon og bevegelser.

§ 6-6 *Gjennomsøking mv.*

Etterretningstjenesten kan gjennomsøke bolig, rom eller annet oppbevaringssted for å finne informasjon eller gjenstander. Tjenesten kan tilegne seg etterretningsrelevante gjenstander som finnes under gjennomsøkingen. Gjennomsøking av sted som etter sin art ikke er tilgjengelig for alle, kan bare gjennomføres dersom det er strengt nødvendig.

Etterretningstjenesten kan tilegne seg etterretningsrelevante gjenstander fra personer.

§ 6-7 *Avlytting og bildeovervåkning*

Etterretningstjenesten kan innhente lyd og bilde fra kamera eller mikrofon som plasseres på eller i nærheten av sted hvor det er rimelig å anta at et etterretningsmål vil oppholde seg. Innhentingen kan ikke gjennomføres på sted som etter sin art ikke er tilgjengelig for alle, med mindre det er strengt nødvendig.

§ 6-8 *Annen teknisk innhenting*

Etterretningstjenesten kan innhente informasjon ved bruk av tekniske sensorer eller andre tekniske metoder som ikke reguleres av §§ 6-5, 6-7, 6-9 eller 6-10, blant annet bildeovervåkning av enkeltpersoner fra rombaserte eller luftbårne sensorer.

Innhentingen kan ikke gjennomføres på sted som etter sin art ikke er tilgjengelig for alle, med mindre det er strengt nødvendig.

§ 6-9 *Midtpunktinnhenting*

Etterretningstjenesten kan innhente elektronisk kommunikasjon i transitt og kartlegge kommunikasjonsinfrastruktur. Bestemmelser om tilrettelagt innhenting av elektronisk kommunikasjon som transporteres over den norske grensen, er gitt i kapittel 7 og 8.

§ 6-10 *Endepunktinnhenting*

Etterretningstjenesten kan observere og innhente ikke åpent tilgjengelig elektronisk informasjon i datasystemer eller lignende systemer eller tjenester som etterretningsmål besitter eller antas å ville benytte.

Dersom det er grunn til å tro at innhentingen vil omfatte informasjon som ikke er ment for kommunikasjon, skal den ikke gjennomføres med mindre det er strengt nødvendig.

§ 6-11 *Forberedende tiltak*

Etterretningstjenesten kan treffe forberedende tiltak som er nødvendige for å bruke metoder etter dette kapittelet, blant annet 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.

§ 6-12 *Beslutning om bruk av en innhentingsmetode*

Sjefen for Etterretningstjenesten kan treffe beslutning om bruk av metoder etter dette kapittelet, med mindre beslutningen ligger til departementet etter § 2-5.

Beslutningen skal ikke gis for lengre tid enn nødvendig, og ikke for mer enn ett år av gangen. Dersom forutsetningene for beslutningen endres vesentlig, skal den snarest mulig vurderes på nytt.

§ 6-13 *Krav til beslutningen*

Beslutningen etter § 6-12 skal være skriftlig og angi

a) oppdraget som innhentingen knytter seg til
b) hva eller hvem innhentingen gjelder
c) det faktiske og rettslige grunnlaget for innhentingen
d) beslutningens varighet.

I hastetilfeller kan beslutningen treffes muntlig. Den skal i så fall snarest mulig nedtegnes.

Kapittel 7. Tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon

§ 7-1 *Generelle vilkår og virkeområde*

Etterretningstjenesten kan for etterretningsformål innhente elektronisk kommunikasjon som transporteres over den norske grensen når grunnvilkårene etter kapittel 5 er oppfylt, bestemmel-

sene i kapittel 7 og 8 følges, og innhenting ikke strider mot loven for øvrig.

Bestemmelsene i kapittel 7 og 8 kommer bare til anvendelse der det er nødvendig at tilbydere som nevnt i § 7-2 legger til rette for innhentingen.

§ 7-2 *Tilretteleggingsplikt for ekomtilbydere*

Tilbydere som omfattes av ekomloven § 1-5 og tilbydere av internettbaserte kommunikasjons- eller meldingstjenester som er tilgjengelige for allmennheten, skal speile og gjøre tilgjengelig for Etterretningstjenesten utvalgte kommunikasjonsstrømmer og på annen måte tilrettelegge for utvalg, filtrering, testing, innhenting, lagring og søk som beskrevet i dette kapittelet, blant annet ved å

a) gi informasjon om signalmiljø, dataformater, tekniske innretninger og fremgangsmåter
b) tillate at tjenesten installerer utstyr og etablerer midlertidig eller permanent tilstedeværelse for å drifte utstyr på steder som kontrolleres av tilbyder
c) medvirke til teknisk drift og vedlikehold av etablerte løsninger
d) bidra til at tjenesten kan gjennomføre testinnhenting og testanalyser av trafikk i nett og tjenester
e) sørge for tilgang til kommunikasjon uten hinder av linkkryptering eller tilsvarende kryptering som tilbyder kontrollerer
f) medvirke til sikkerhetsmessig forsvarlige løsninger.

Tilretteleggingen skal ikke forringe elektroniske kommunikasjonstjenester for brukerne. Merutgifter for tilbyder som følge av tilretteleggingen skal dekkes av staten.

Departementet kan gi forskrift om tilretteleggingsplikten etter første ledd og prinsipper for utregning av merutgifter etter andre ledd.

§ 7-3 *Beslutning om tilrettelegging*

Sjefen for Etterretningstjenesten fatter beslutning om tilrettelegging. Tilbyderen skal så langt som mulig gis anledning til å uttale seg før beslutningen fattes. Beslutningen kan gjelde for inntil tre år av gangen.

Tilbyderen kan påklage beslutningen til departementet. Fristen for å klage er tre uker fra beslutningen ble meddelt tilbyderen. Departementet kan på anmodning fra tilbyderen bestemme at beslutningen ikke skal iverksettes før klagen er avgjort.

Beslutning om tilrettelegging skal meddeles EOS-utvalget og Nasjonal kommunikasjonsmyndighet. Nasjonal kommunikasjonsmyndighet har ved forespørsel rett til informasjon fra Etterretningstjenesten om tekniske og operasjonelle løsninger som tjener til å oppfylle tilretteleggingsplikten.

Departementet kan gi forskrift om beslutning om tilrettelegging etter første ledd og klagebehandling etter andre ledd.

§ 7-4 *Taushetsplikt*

Den som er underlagt tilretteleggingsplikt etter § 7-2, plikter å bevare taushet om Etterretningstjenestens tilgang, tekniske og operasjonelle løsninger og andre forhold knyttet til tilretteleggingen. Taushetsplikten gjelder tilsvarende for enhver som utfører arbeid eller tjeneste for den som er underlagt tilretteleggingsplikt, eller som på annen måte bistår med tilrettelegging. Taushetsplikten gjelder også etter at vedkommende har avsluttet arbeidet eller tjenesten.

Taushetsplikten er ikke til hinder for å gi opplysninger til EOS-utvalget eller Nasjonal kommunikasjonsmyndighet.

§ 7-5 *Testinnhenting og testanalyser*

Etterretningstjenesten kan gjennomføre testinnhenting og testanalyser av trafikk og nett som omfattes av dette kapittelet. Testinnhenting og testanalyser skal utelukkende brukes for å muliggjøre utvalg, filtrering, lagring, søk, reprosessering, forståelse av signalmiljø og gjenkjenning av tjenester og dataformater, samt annen teknisk understøttelse.

Testinnhenting gjennomføres ved uttrekk av ufiltrert kommunikasjon fra én eller flere kommunikasjonsstrømmer. Ett uttrekk skal ikke overstige 30 sekunder. Det kan ikke gjøres mer enn ett uttrekk hver time.

Uttrekkene skal lagres i et korttidslager som skal holdes adskilt fra data som lagres etter §§ 7-7 og 7-9.

Uttrekkene skal ikke oppbevares lenger enn nødvendig, og de 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 andre punktum.

Testinnhenting, testanalyser og annen teknisk understøttelse skal bare utføres av tekniske spesialister med særskilt opplæring og som ikke har etterretningsanalyse som oppgave. Det skal alltid være to spesialister til stede ved oppsett og analyse av uttrekk etter andre ledd.

§ 7-6 *Utvalg og filtrering*

Etterretningstjenesten skal gjennom utvalg og filtrering søke å hindre lagring etter § 7-7 av metadata om kommunikasjon mellom avsender og mottaker som begge befinner seg i Norge, hvis ikke en av dem omfattes av § 4-2 første ledd.

§ 7-7 *Innhenting og lagring av metadata i bulk*

Etter utvalg og filtrering i samsvar med § 7-6 kan Etterretningstjenesten innhente og lagre metadata i bulk om elektronisk kommunikasjon som transporteres over den norske grensen. Med metadata menes data som beskriver annen data eller som inneholder ekstra informasjon knyttet til data, blant annet data som beskriver formatet på innholdet, hvem som er avsender og mottaker, eller kommunikasjonens størrelse, posisjon, tidspunkt eller varighet.

For å hindre lagring av innholdsdata skal Etterretningstjenesten opprette og vedlikeholde en liste over hvilke typer metadata som kan lagres. Listen skal være tilgjengelig for EOS-utvalget og Nasjonal kommunikasjonsmyndighet.

Lagrede metadata skal slettes senest etter 18 måneder.

For teknisk analyse, feilsøking og oppdatering av lagrede metadata i den hensikt å muliggjøre søk gjelder § 7-5 femte ledd første punktum tilsvarende.

§ 7-8 *Søk i lagrede metadata*

Etterretningstjenesten kan innenfor rammen av rettens kjennelse etter kapittel 8 foreta søk i metadata lagret i samsvar med § 7-7. Søkene skal baseres på søkebegreper.

Søk i lagrede metadata kan bare utføres av personell i Etterretningstjenesten som er vurdert som skikket til det og som utpekes av sjefen for tjenesten. Personellet må ha gjennomgått særskilt opplæring. Den enkelte skal bare kunne utføre søk i henhold til søkeprivilegier som er tilpasset vedkommendes oppdragsportefølje.

§ 7-9 *Målrettet innhenting og lagring av innholdsdata*

Etterretningstjenesten kan innenfor rammen av rettens kjennelse etter kapittel 8 målrettet innhente og lagre innholdsdata med tilhørende metadata fra elektronisk kommunikasjon som transporteres over den norske grensen. Innholdsdata er data som ikke er metadata.

§ 7-10 *Internkontroll og aktivitetslogger*

Etterretningstjenesten skal iverksette systematiske tiltak for å sikre at virksomhet etter dette kapittelet gjennomføres i samsvar med loven.

Alle søk skal kunne kontrolleres i ettertid gjennom aktivitetslogger. Loggene skal oppbevares i 10 år, og skal være tilgjengelige for EOS-utvalgets kontroll til enhver tid.

§ 7-11 *Løpende kontroll*

EOS-utvalget skal føre løpende kontroll med Etterretningstjenestens etterlevelse av bestemmelsene i dette kapittelet, blant annet med at søk bare gjennomføres i tråd med rettens kjennelser og at korttidslageret og testdata utelukkende brukes til teknisk understøttelse.

EOS-utvalget skal ha uhindret tilgang til all informasjon, interne retningslinjer og prosedyrer, lokaler, utstyr, programvare, filteroppdateringer, aktivitetslogger og annet som benyttes ved virksomhet etter dette kapittelet.

Etterretningstjenesten skal tilrettelegge for kontrollen gjennom tekniske løsninger.

§ 7-12 *Begjæring om stansing og sletting*

Hvis EOS-utvalget mener at virksomhet etter dette kapittelet gjennomføres i strid med loven, kan utvalget fremme begjæring for Oslo tingrett med krav om at ulovlig virksomhet opphører, og at ulovlig innhentet informasjon slettes. Før begjæringen fremmes, skal Etterretningstjenesten gjøres kjent med utvalgets syn og gis mulighet til å rette seg etter det.

Reglene i kapittel 8 gjelder tilsvarende så langt de passer.

§ 7-13 *Forbud mot utlevering av overskuddsinformasjon*

Etterretningstjenesten skal ikke utlevere overskuddsinformasjon fra innhenting etter dette kapittelet. Slik informasjon utløser ikke avvergings- eller opplysningsplikter etter annen lov.

Overskuddsinformasjon som nevnt i første ledd kan likevel utleveres i den utstrekning det er nødvendig for å forhindre alvorlig fare for noens liv, helse eller frihet eller at noen blir uriktig tiltalt eller domfelt for en straffbar handling. EOS-utvalget skal varsles om utleveringen.

Informasjon som ikke er overskuddsinformasjon, kan utleveres dersom vilkårene i kapittel 10 er oppfylt.

§ 7-14 *Bevisforbud i straffesaker*

Informasjon fremkommet gjennom innhenting etter dette kapittelet kan ikke brukes som grunnlag for ileggelse av straff eller andre strafferettslige reaksjoner. Første punktum gjelder ikke i saker om overtredelse av straffeloven § 131.

§ 7-15 *Informasjonssikkerhet*

Etterretningstjenesten plikter å hindre at uvedkommende får tilgang til informasjon som lagres og behandles etter bestemmelsene i dette kapittelet. Tjenesten skal gjennomføre sikkerhetstiltak etter §§ 9-9 og 11-5 for å sikre at informasjonen bare er tilgjengelig for de som har lovlig 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. Det kan oppstilles vilkår i kjennelsen. Kjennelsen skal begrunnes. Retten kan omgjøre kjennelsen.

Rettens avgjørelse skal treffes så raskt som mulig. Den som avgjørelsen retter seg mot eller ellers rammer, skal ikke gis adgang til å uttale seg og meddeles ikke kjennelsen.

Kjennelsen skal meddeles Etterretningstjenesten. Tjenesten skal gjøre kjennelsen og begjæringen tilgjengelig for EOS-utvalget.

§ 8-2 *Krav til begjæringen*

Begjæring om tillatelse etter § 8-1 fremmes for Oslo tingrett av sjefen for Etterretningstjenesten eller den som sjefen gir fullmakt. Begjæringen skal være skriftlig og angi

a) oppdraget som søket eller innhentingen knytter seg til
b) det faktiske og rettslige grunnlaget for søket eller innhentingen
c) hvilke søkebegreper eller kategorier av søkebegreper som skal brukes, hvis begjæringen gjelder søk i lagrede metadata etter § 7-8
d) hva eller hvem innhentingen retter seg mot, hvis begjæringen gjelder målrettet innhenting og lagring av innholdsdata etter § 7-9
e) hvor lenge tillatelsen bør vare, jf. § 8-6.

§ 8-3 *Muntlige forhandlinger*

Retten kan beslutte å avholde muntlige forhandlinger. Etterretningstjenesten møter ved sjefen for tjenesten eller den som sjefen gir fullmakt. Tjenesten kan også møte med tjenestepersoner eller andre som kan opplyse saken.

Rettsmøtene holdes for lukkede dører.

§ 8-4 *Hva retten skal prøve*

Retten skal prøve om vilkårene etter denne loven er oppfylt. Dette omfatter blant annet

a) om søket eller innhentingen ligger innenfor Etterretningstjenestens oppgaver etter kapittel 3
b) om noen av forbudene i §§ 4-1, 4-8, 4-9 eller 9-4 er til hinder for søket eller innhentingen
c) om grunnvilkårene etter kapittel 5 er oppfylt.

§ 8-5 *Særskilt advokat*

Retten skal etter å ha mottatt begjæring som nevnt i § 8-2 oppnevne en advokat som skal ivareta den enkeltes rettigheter og samfunnets interesser i saken. Oppnevnelse kan unnlates dersom retten finner det ubetenkelig. Advokaten oppnevnes fra en særlig krets av sikkerhetsklarerte advokater, og kan ikke la seg representere eller møte ved annen advokat eller fullmektig. Advokaten skal ha godtgjørelse av staten.

Advokaten skal gjøres kjent med begjæringen og annen informasjon som legges frem for retten, men har ellers ingen innsynsrett. Advokaten må ikke sette seg i forbindelse med personer som berøres av saken.

Advokaten har rett til å uttale seg før retten treffer avgjørelse. Advokaten skal varsles om rettsmøter i saken og har rett til å delta i dem.

Departementet kan gi forskrift om oppnevning av advokat etter første ledd.

§ 8-6 *Varighet*

Rettens tillatelse etter § 8-1 skal ikke gis for lengre tid enn nødvendig. Gjelder tillatelsen målsøking etter § 7-8, kan den ikke overstige ett år. Gjelder tillatelsen målrettet innhenting etter §§ 7-8 eller 7-9, kan den ikke overstige seks måneder.

Etterretningstjenesten skal avslutte pågående søk etter § 7-8 og innhenting og lagring etter § 7-9 dersom lovens vilkår ikke lenger er til stede.

§ 8-7 *Informasjonssikkerhet*

Rettens kjennelse skal sikkerhetsgraderes etter reglene gitt i og i medhold av sikkerhetsloven.

Domstolen skal sørge for at informasjon og dokumenter med høyeste sikkerhetsgrad kan behandles i henhold til reglene gitt i og i medhold av 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.

Departementet kan gi forskrift om rettens tilgang til rettspraksis i saker etter dette kapittelet.

§ 8-8 *Taushetsplikt*

Dommere og andre som utfører tjeneste eller arbeid for domstolene, har taushetsplikt om begjæringer, rettsmøter, kjennelser og annet de får kjennskap til i saker etter dette kapittelet. Taushetsplikten gjelder også etter at arbeidet eller tjenesten er avsluttet.

Taushetsplikten er ikke til hinder for å gi opplysninger til EOS-utvalget.

§ 8-9 *Anke*

Etterretningstjenesten og den særskilte advokaten kan anke rettens kjennelse.

Reglene i straffeprosessloven kapittel 26 gjelder tilsvarende så langt de passer. § 8-7 gjelder tilsvarende for ankedomstolen.

§ 8-10 *Hastekompetanse*

Dersom det ved opphold er stor fare for at informasjon av vesentlig betydning for utførelsen av Etterretningstjenestens oppgaver etter kapittel 3 kan gå tapt, kan ordre fra sjefen for tjenesten tre i stedet for rettens kjennelse. Tjenesten skal straks og senest innen 24 timer etter at innhentingen ble påbegynt, forelegge saken for retten.

Retten avgjør ved kjennelse om søket eller innhentingen kan tillates, jf. § 8-1. Kommer retten til at søket eller innhentingen var ulovlig, skal retten meddele dette til EOS-utvalget. Retten kan pålegge Etterretningstjenesten å slette innhentet informasjon.

Kapittel 9. Behandling av personopplysninger etter innhenting

§ 9-1 *Forholdet til personopplysningsloven*

Dette kapittelet gjelder for Etterretningstjenestens behandling av personopplysninger for etterretningsformål når personopplysninger behandles helt eller delvis automatisert eller behandles ikke-automatisert og inngår i eller skal inngå i et register.

For behandling av personopplysninger for andre formål enn etterretningsformål gjelder bestemmelsene i personopplysningsloven, med de unntak som følger av § 2-8 første ledd og eventuelle tilpassede skjermingsregler i medhold av § 11-4 tredje ledd.

§ 9-2 *Behandlingsgrunnlag*

Etterretningstjenesten kan behandle personopplysninger når det er nødvendig for etterretningsformål.

§ 9-3 *Unntak for innhenting av personopplysninger*

Med unntak av § 9-4 gjelder ikke bestemmelsene i dette kapittelet for behandling i form av innhenting. Behandling i form av innhenting reguleres i kapittel 3 til kapittel 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 *Behandling av fortrolig kommunikasjon med særlige yrkesutøvere*

Etterretningstjenesten skal ikke behandle fortrolig kommunikasjon med særlige yrkesutøvere som nevnt i straffeprosessloven § 119 og tvisteloven § 22-5 når yrkesutøveren eller den som betror seg, er bosatt i Norge eller norsk statsborger.

Dersom det er strengt nødvendig at de hensyn som begrunner vernet av den fortrolige kommunikasjonen, viker for nasjonale sikkerhetsinteresser, kan slik fortrolig kommunikasjon likevel behandles.

Beslutning om å behandle fortrolig kommunikasjon etter andre ledd skal treffes av sjefen for Etterretningstjenesten. Beslutningen skal være skriftlig og redegjøre for det faktiske og rettslige grunnlaget for behandlingen. Beslutningen skal meddeles EOS-utvalget.

§ 9-6 *Behandling av opplysninger som kan identifisere en kilde*

Etterretningstjenesten skal ikke behandle opplysninger som er betrodd noen i deres journalistiske virke og som kan avsløre hvem som er kilde for opplysningen, dersom den som betror seg eller som er betrodd opplysningen, er bosatt i Norge, norsk statsborger eller arbeider på oppdrag for virksomhet i Norge som omfattes av mediefridomslova § 2. Forbudet gjelder også dersom vedkommende ikke lenger bor i Norge eller arbeider for virksomheten, men gjorde dette da opplysningen ble gitt.

Dersom det er strengt nødvendig at de hensyn som begrunner kildevernet, viker for nasjonale

sikkerhetsinteresser, kan opplysninger som nevnt i første ledd likevel behandles.

Beslutning om å behandle opplysninger etter andre ledd skal treffes av departementet etter foreleggelse etter § 2-5. Beslutningen skal være skriftlig og redegjøre for det faktiske og rettslige grunnlaget for behandlingen. Beslutningen skal meddeles EOS-utvalget.

§ 9-7 *Korrekte og oppdaterte personopplysninger*

Etterretningstjenesten skal, så langt det er mulig, påse at personopplysninger som behandles og som ikke er rådata i bulk, er korrekte og oppdaterte. Uriktige personopplysninger skal rettes eller slettes uten unødig opphold. Tjenesten skal, så langt det er mulig, sørge for at feilen ikke får betydning for den personopplysningene gjelder.

Dersom ikke-verifiserte personopplysninger utleveres etter kapittel 10, skal mottakeren gjøres oppmerksom på dette.

§ 9-8 *Sletting*

Personopplysninger skal slettes når de ikke lenger er nødvendige for formålet med behandlingen.

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. Metadata som er innhentet og lagret i bulk i samsvar med § 7-7, skal likevel slettes senest etter 18 måneder, jf. § 7-7 tredje ledd.

Sletting av personopplysninger i operative systemer og registre som er tilgjengelige for etterretningsproduksjon, er ikke til hinder for lagring av opplysningene etter annen lov.

§ 9-9 *Informasjonssikkerhet*

Etterretningstjenesten skal gjennom systematiske tiltak sikre konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger. Tiltakene skal utformes i samsvar med bestemmelsene i sikkerhetsloven.

Personopplysninger skal ikke gjøres tilgjengelige for flere personer enn det som er nødvendig for formålet med behandlingen.

§ 9-10 *Personvernrådgiver*

Etterretningstjenesten skal ha minst én personvernrådgiver.

Personvernrådgiveren skal bidra til etterlevelse av denne loven gjennom opplæring, rådgivning, veiledning og internkontroll. Personvernrådgiveren skal kunne motta varsler fra ansatte i Etterretningstjenesten om brudd og avvik knyttet til behandling av personopplysninger.

Kapittel 10. Nasjonalt og internasjonalt samarbeid og informasjonsutveksling

§ 10-1 *Nasjonalt og internasjonalt samarbeid*

Etterretningstjenesten skal samarbeide med andre norske myndigheter om grenseoverskridende trusler, forsvar mot og håndtering av alvorlige hendelser i det digitale rom samt andre prioriterte saksområder.

Etterretningstjenesten skal etablere og opprettholde etterretningssamarbeid med andre land, forsvarsallianser som Norge deltar i, og andre internasjonale organisasjoner. Departementets beslutning skal innhentes i saker som nevnt i § 2-5.

§ 10-2 *Utlevering av etterretningsinformasjon som ledd i nasjonalt samarbeid*

Etterretningstjenesten kan utlevere etterretningsinformasjon til andre norske myndigheter dersom

a) utleveringen skjer for etterretningsformål eller er nødvendig for å fremme mottakerens oppgaver eller 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 er i samsvar med kapittel 9
d) utleveringen er forholdsmessig etter § 5-4
e) utleveringen er forsvarlig i lys av opplysningenes kvalitet, hvem som er mottaker av opplysningene, og hvordan mottakeren antas å bruke dem
f) utleverte opplysninger forventes å bli forsvarlig sikkerhetsmessig behandlet.

Utlevering med sikte på innhenting eller andre tiltak hos mottaker på vegne av Etterretningstjenesten kan bare skje dersom tjenesten selv ville hatt adgang til å gjennomføre innhentingen eller tiltaket.

Utlevering skal skje med notoritet.

Denne paragrafen gjelder ikke for utlevering av informasjon til EOS-utvalget og andre tilsyns- og kontrollinstanser.

§ 10-3 *Utlevering av etterretningsinformasjon som ledd i internasjonalt samarbeid*

Etterretningstjenesten kan utlevere etterretningsinformasjon til andre staters myndigheter eller internasjonale organisasjoner dersom

a) vilkårene etter § 10-2 er oppfylt

b) utleveringen er under nasjonal kontroll og i Norges interesse
c) det settes som vilkår at informasjonen ikke kan brukes som grunnlag for innhenting rettet mot personer i Norge, med unntak for personer som omfattes av § 4-2 første ledd og som det er i Norges interesse at mottakeren innhenter opplysninger om.

Etterretningstjenesten skal ikke utlevere etterretningsinformasjon hvis det er en reell risiko for at informasjonen kan medvirke til at noen utsettes for tortur eller annen umenneskelig eller nedverdigende behandling eller straff.

§ 10-4 *Utlevering av overskuddsinformasjon*

Etterretningstjenesten kan utlevere overskuddsinformasjon til andre norske myndigheter når vilkårene etter § 10-2 er oppfylt.

Overskuddsinformasjon som stammer fra innhenting etter kapittel 7, reguleres av § 7-13.

Overskuddsinformasjon som er fortrolig kommunikasjon etter § 9-5 eller kildeinformasjon etter § 9-6, kan ikke utleveres.

§ 10-5 *Utlevering av informasjon til Etterretningstjenesten fra norske myndigheter*

Norske myndigheter kan uten hinder av lovbestemt taushetsplikt utlevere informasjon til Etterretningstjenesten dersom det er nødvendig for forebyggelses- og sikkerhetsmessige formål innenfor rammen av Etterretningstjenestens oppgaver etter kapittel 3. Første punktum gjelder ikke for taushetsplikt som nevnt i straffeprosessloven § 119 og tvisteloven § 22-5 eller taushetsplikt etter straffeprosessloven § 216 i.

§ 10-6 *Formidling av opplysninger på vegne av norske myndigheter*

Etterretningstjenesten kan på vegne av andre norske myndigheter formidle opplysninger til og fra andre staters myndigheter dersom

a) den norske myndigheten har anmodet Etterretningstjenesten om å formidle opplysningene
b) mottakeren opplyses om at formidlingen skjer på vegne av den norske myndigheten
c) Etterretningstjenesten ikke endrer opplysningene, legger til egen informasjon eller ber mottakeren om å handle på en bestemt måte i lys av opplysningene.

Mottakeren skal opplyses om at videreformidling til tredjeparter krever samtykke fra den norske myndigheten, og eventuelt om at slikt samtykke allerede er gitt.

Formidlingen skal skje med notoritet.

§ 10-7 *Bistand til politiet*

Etterretningstjenesten kan bistå politiet i samsvar med politiloven § 27 a. Bistand i form av søk eller innhenting etter kapittel 7 kan ikke finne sted.

Kapittel 11. Avsluttende bestemmelser

§ 11-1 *Forholdet til forvaltningsloven*

Med unntak av forvaltningsloven §§ 13 til 13 f om taushetsplikt kommer forvaltningsloven ikke til anvendelse for saksbehandling som knytter seg til utførelsen av Etterretningstjenestens oppgaver etter denne loven.

§ 11-2 *Taushetsplikt*

Enhver som gjør arbeid eller tjeneste for Etterretningstjenesten, skal bevare livsvarig taushet om informasjon som vedkommende blir kjent med gjennom arbeidet eller tjenesten, dersom det kan skade nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.

Ansatte i Etterretningstjenesten skal bevare livsvarig taushet om eget eller andres tilsettingsforhold.

Taushetsplikten etter første ledd gjelder også for enhver som blir kjent med sikkerhetsgradert informasjon etter § 2-4 tredje ledd.

Informasjon som nevnt i første til tredje ledd kan ikke utnyttes i virksomhet utenfor Etterretningstjenesten.

Taushetsplikten er ikke til hinder for at opplysninger utleveres etter bestemmelsene i denne loven eller etter regler fastsatt i annen lov, eller at opplysninger gjøres kjent for andre i Etterretningstjenesten i samsvar med gjeldende autorisasjonsregler og prinsippet om tjenstlig behov.

§ 11-3 *Krav til statsborgerskap og sikkerhetsklarering*

Militært personell og sivilt ansatte i Etterretningstjenesten skal ha norsk statsborgerskap og være sikkerhetsklarert for STRENGT HEMMELIG.

Sjefen for Etterretningstjenesten kan for særskilte stillinger med lavere klareringsbehov bestemme at personellet kan være sikkerhetsklarert for HEMMELIG.

§ 11-4 *Skjerming av etterretningsoperasjoner mv.*

Etterretningstjenesten kan for å skjerme sine operasjoner benytte dekkstrukturer og uriktige, falske eller villedende identiteter, dokumenter og opplysninger, samt ta kontroll over, modifisere eller utplassere elektronisk utstyr.

Bestemmelser om opplysningsplikt i annen lov gjelder ikke for opplysninger om vederlag som Etterretningstjenesten yter til kilder og oppdragstakere som ikke er ansatt i tjenesten. Slike vederlag og betalinger skal ikke regnes som skattepliktig inntekt for mottakeren eller inngå i grunnlag for beregning eller avkortning av sosiale ytelser eller lignende.

Kongen i statsråd kan gi bestemmelser som fraviker annen lov, blant annet krav om rapportering av informasjon til offentlige registre, i den utstrekning det er nødvendig for å skjerme Etterretningstjenestens ansatte, kilder, kapasiteter, metoder eller operasjoner mot offentlig eksponering eller kompromittering overfor andre stater.

§ 11-5 *Arkiver, informasjonssystemer og etterretningsregistre*

Etterretningstjenestens arkiver, informasjonssystemer og etterretningsregistre skal være betryggende sikret og utilgjengelige for andre enn eget autorisert personell med tjenstlig behov for tilgang og personer som er satt til å føre kontroll og tilsyn med Etterretningstjenesten.

§ 11-6 *Beredskap*

Etterretningstjenesten skal utarbeide og vedlikeholde beredskapsplaner, blant annet forberedte tiltak for å sikre at tjenestens informasjon og systemer ikke kommer under kontroll av uvedkommende i krise eller væpnet konflikt, basert på Nasjonalt beredskapssystem og Forsvarets operative planverk.

§ 11-7 *Klage og underretning*

Enhver kan klage til EOS-utvalget etter EOS-kontrolloven. Etterretningstjenesten plikter ikke å gi underretning til den som har vært gjenstand for informasjonsinnhenting som kan innebære et menneskerettslig inngrep.

§ 11-8 *Straff*

Den som handler i strid med beslutning om tilrettelegging etter § 7-3 eller bryter taushetsplikt etter § 7-4, straffes med bot eller fengsel inntil 6 måneder.

Kapittel 12. Ikrafttredelse og endringer i andre lover

§ 12-1 *Ikrafttredelse*

Loven trer i kraft fra det tidspunktet Kongen bestemmer. De ulike bestemmelsene kan settes i kraft til ulik tid.

§ 12-2 *Opphevelse*

Fra det tidspunktet loven trer i kraft, oppheves lov 20. mars 1998 nr. 11 om Etterretningstjenesten.

§ 12-3 *Endringer i andre lover*

Fra det tidspunktet loven trer i kraft, gjøres følgende endringer i andre lover:

1. I lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon gjøres følgende endringer:

§ 2-8 nytt fjerde ledd skal lyde:

Bestemmelser om tilrettelegging for innhenting av elektronisk kommunikasjon som transporteres over den norske grensen, er gitt i etterretningstjenesteloven kapittel 7.

§ 6-2 a første ledd nytt tredje punktum skal lyde:
Etterretningstjenesten kan i særskilte tilfeller og i korte tidsrom uten tillatelse fra myndigheten ta i bruk frekvenser som er tildelt andre til identitetsfanging, når dette er strengt nødvendig for å innhente informasjon om en person som omfattes av etterretningstjenesteloven § 4-2 første ledd.

§ 6-2 a annet ledd skal lyde:

Politiet*, Etterretningstjenesten* og Nasjonal sikkerhetsmyndighet skal varsle myndigheten uten ugrunnet opphold etter at frekvenser som er tildelt andre, er tatt i bruk. Varsel skal angi frekvensområde, tidsrom og sted. Myndigheten avgjør i samråd med politiet, *Etterretningstjenesten* eller Nasjonal sikkerhetsmyndighet om og i tilfelle når rettighetshaverne skal underrettes.

§ 6-2 a tredje ledd tredje punktum skal lyde:
Tillatelser til Forsvaret, *med unntak for Etterretningstjenesten,* kan bare gis til øvelser innenfor Forsvarets permanente øvingsområder.

2. I lov 19. mai 2006 nr. 16 om rett til innsyn i offentleg verksemd skal § 2 fjerde ledd nytt fjerde punktum lyde:

Lova gjeld ikkje for dokument som blir behandla av Etterretningstenesta etter etterretningstjenesteloven.

Nåværende fjerde punktum blir nytt femte punktum.

Bestilling av publikasjoner

Departementenes sikkerhets- og serviceorganisasjon
www.publikasjoner.dep.no
Telefon: 22 24 00 00

Publikasjonene er også tilgjengelige på
www.regjeringen.no

Trykk: 07 Media AS – 04/2020