NOU Norges offentlige utredninger 2016: 19

Samhandling for sikkerhet

Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid

Norges offentlige utredninger 2016

Seriens redaksjon:
Departementenes sikkerhets- og serviceorganisasjon
Informasjonsforvaltning

---

1. Arbeidstidsutvalget
   Arbeids- og sosialdepartementet
2. Endringer i verdipapirhandelloven – flagging og periodisk rapportering
   Finansdepartementet
3. Ved et vendepunkt: Fra ressursøkonomi til kunnskapsøkonomi
   Finansdepartementet
4. Ny kommunelov
   Kommunal- og moderniseringsdepartementet
5. Omgåelsesregel i skatteretten
   Finansdepartementet
6. Grunnlaget for inntektsoppgjørene 2016
   Arbeids- og sosialdepartementet
7. Norge i omstilling – Karriereveiledning for individ og samfunn
   Kunnskapsdepartementet
8. En god alliert – Norge i Afghanistan 2001–2014
   Utenriksdepartementet og Forsvarsdepartementet
9. Rettferdig og forutsigbar – voldsskadeerstatning
   Justis- og beredskapsdepartementet
10. Evaluering av garantireglene i bustadoppføringslova
    Justis- og beredskapsdepartementet
11. Regnskapslovens bestemmelser om årsberetning mv.
    Finansdepartementet
12. Ideell opprydding
    Kulturdepartementet
13. Samvittighetsfrihet i arbeidslivet
    Arbeids- og sosialdepartementet
14. Mer å hente
    Kunnskapsdepartementet
15. Lønnsdannelsen i lys av nye økonomiske utviklingstrekk
    Finansdepartementet
16. Ny barnevernslov
    Barne- og likestillingsdepartementet
17. På lik linje
    Barne- og likestillingsdepartementet
18. Hjertespråket
    Kommunal- og moderniseringsdepartementet
19. Samhandling for sikkerhet
    Forsvarsdepartementet

Omslagsillustrasjon: Anagramdesign.no

NOU Norges offentlige utredninger 2016: 19

Samhandling for sikkerhet

Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid

Utredning fra utvalg oppnevnt ved kongelig resolusjon 27. mars 2015.
Avgitt til Forsvarsdepartementet 12. oktober 2016.

Departementenes sikkerhets- og serviceorganisasjon
Informasjonsforvaltning

Oslo 2016

ISSN 0333-2306
ISBN 978-82-583-1295-3

07 PrintMedia AS

Til Forsvarsdepartementet

Sikkerhetsutvalget ble oppnevnt ved kongelig resolusjon 27. mars 2015. Utvalget gir med dette sin utredning.

Oslo, 12. oktober 2016

Kim Traavik
(leder)

Brian Bjordal	Olav Fjell	Torgeir Hagen
Gry Dyregrov Hamarsland	Kristin Lian	Hanne Løvstad
Dag Wiese Schartum	Siri Wiig	

Fredrik Irgens
(sekretariatsleder)

Christian F. Mathiessen

Kjetil Longva

Seline Høiseth

Anders G. Romarheim

Innhold

Digitale vedlegg

Elektronisk vedlegg 1 Kartlegging av sektorlovgivning om sikring mot tilsiktede uønskede hendelser (Høgskolen i Oslo og Akershus)
Elektronisk vedlegg 2 Myndighetskontroll med utenlandsk eierskap (Wikborg, Rein & Co)
Elektronisk vedlegg 3 Vurdering av forebyggende sikkerhet innenfor kraft, petroleum og luftfart (Forsvarets Forskningsinstitutt)

Del I
Innledning

Kapittel 1
Oppnevning, mandat og utvalgets arbeid

1.1 Utvalgets sammensetning

Sikkerhetsutvalget ble oppnevnt ved kgl. resolusjon av 27. mars 2015. Utvalget fikk denne sammensetningen:

- Ambassadør Kim Traavik, leder
- Lagmann Espen Bergh
- Administrerende direktør Brian Bjordal
- Styreleder Olav Fjell
- Generalløytnant (p) Torgeir Hagen
- Seksjonsleder Gry Dyregrov Hamarsland
- Konserndirektør Kristin Lian
- Direktør Hanne Løvstad
- Professor dr. juris Dag Wiese Schartum
- Professor Siri Wiig

Utvalgsmedlem Espen Bergh fratrådte utvalget med virkning fra 1. august 2016, grunnet tiltredelse i stilling som høyesterettsdommer.

Utvalgets sekretariat har vært ledet av seniorrådgiver Fredrik Irgens, og har for øvrig bestått av sjefsforsker Kjetil Longva, seniorforsker Anders Romarheim, seniorrådgiver Christian F. Mathiessen og rådgiver Seline Høiseth.

1.2 Utvalgets mandat

Utvalget ble gitt følgende mandat:

1. Innledning og bakgrunn
Sikkerhetsloven trådte i kraft 1. juli 2001. Formålet var å utvikle et nasjonalt lovgrunnlag for sikkerhetstjenestens virksomhet, for derigjennom å motvirke trusler mot rikets selvstendighet og sikkerhet. Virkelighetsbildet har endret seg siden 2001, og risiko- og trusselbildet samfunnet står overfor er bredt og sammensatt. Markante enkelthendelser og mer overordnede tendenser har påvirket utviklingen. Det er behov for en helhetlig vurdering og nytenking med hensyn til lovregulering av forebyggende nasjonal sikkerhet i tråd med de teknologiske, demografiske og sikkerhetsmessige endringene som har funnet sted siden sikkerhetsloven trådte i kraft.

Erfaringer fra hendelser de senere år illustrerer bredden og kompleksiteten i samfunnssikkerhetsarbeidet, og det har blitt vanskeligere å holde oversikt over de avhengigheter som gjør seg gjeldende på tvers av sektorer, virksomheter og infrastrukturer. Den teknologiske utviklingen utfordrer sikkerhetsarbeidet blant annet gjennom nye måter å produsere, dele og lagre samfunnsviktig informasjon på. Den økte risikoen ved, og vår avhengighet av, IKT-baserte informasjonssystemer, stiller krav om tidsriktige og dynamiske verktøy for beskyttelse mot trusler i det digitale rom. I tillegg gjør utviklingen det mulig å installere elektroniske innretninger eller utøve frittstående høyteknologisk virksomhet som kan være en trussel mot grunnleggende nasjonale sikkerhetsinteresser.

2. Nærmere om utvalgets mandat
Utvalget skal vurdere hva som bør reguleres i lov for å sikre nasjonal sikkerhet. Formålet med nytt lovgrunnlag skal være å beskytte kritisk infrastruktur, kritiske samfunnsfunksjoner og sensitiv informasjon mot tilsiktede, uønskede hendelser. Utvalget skal sikre et helhetlig forebyggende lovgrunnlag innen både den militære og sivile sektoren som er relevant og robust med hensyn til dagens og fremtidens risiko- og trusselbilde. Forslaget skal sikre en kostnadseffektiv regulering, som sikrer balanse mellom akseptabel restrisiko, og kostnaden for sikkerhetsnivået. Samfunnsøkonomisk lønnsomhet skal være en grunnleggende forutsetning, det vil si at aktuelle sikringstiltak må ha en samfunnsøkonomisk nytte som samlet overstiger kostnadene.

Forhold utvalget særskilt skal vurdere:

Struktur, virkeområde og ansvarsforholdet for loven
Utvalget må vurdere hva som er den mest hensiktsmessige oppbyggingen av lovgivningen. Det må vurderes hvorvidt krav til militær og sivil sektor skal reguleres i samme lov eller om lovgrunnlaget skal deles. Utvalget skal videre foreta en vurdering av hvorvidt myndighetenes (herunder NSMs) oppgaver og ansvar skal reguleres i lovgrunnlaget/lovgrunnlagene, og på hvilken måte dette eventuelt skal gjøres. Utvalget kan vurdere å utarbeide en rammelov hvor nærmere krav angis i forskrift. Avhengig av lovens innhold og oppbygging må utvalget vurdere hvem som skal ha ansvar for den fremtidige forvaltning av loven(e) og dens forskrifter.

Kritisk infrastruktur og kritiske samfunnsfunksjoner
Det er et behov for å sikre kritisk infrastruktur og kritiske samfunnsfunksjoner. Utvalget bes om å vurdere hvorvidt en overordnet lovregulering på området kan bidra til bedre forebyggende sikkerhet. Utvalget skal foreta en gjennomgang av relevante sektorregelverk som regulerer beskyttelse av objekter og infrastruktur. Det skal vurderes hvorvidt sektorregelverket er tilstrekkelig for god sikring på det aktuelle området, eventuelt om enkelte forhold bør reguleres i lovgrunnlaget/lovgrunnlagene om forebyggende nasjonal sikkerhet. Utvalgte samfunns- og risikoområder, der tilsiktede uønskede hendelser vil ha store konsekvenser på tvers av fag- og ansvarsområder kan være helse, vann, mat, energi, finansielle tjenester og kommunikasjon.

Informasjonssikkerhet
Det er et økende trusselnivå mot norske IKT-baserte informasjonssystemer, og det avdekkes jevnlig flere sårbarheter. Systemene utsettes for stadig mer avanserte angripere som jobber målbevisst og langsiktig med det formål å få innpass i disse systemene. Dette stiller krav om tidsriktige og dynamiske verktøy for beskyttelse mot IKT-trusler. Sikkerhetsloven gir bestemmelser for håndtering av informasjon som er sikkerhetsgradert, og som skal beskyttes av hensyn til rikets sikkerhet og andre vitale nasjonale sikkerhetsinteresser. Imidlertid finnes det også i våre ugraderte systemer svært mye informasjon som kan være sensitiv og samfunnsviktig. I tillegg kan de ugraderte IKT-systemene i seg selv være viktige for samfunnets funksjonsdyktighet. Utvalget må ta stilling til i hvilken grad det er behov for å beskytte også denne type informasjon og IKT-systemer, herunder hva slags rettssubjekter som eventuelt bør underlegges krav. Utvalget må foreslå eventuell hensiktsmessig regulering.

Utvalget skal se hen til EU-kommisjonens forslag av 7. februar 2013 til direktiv om tiltak for å sikre et høyt felles nivå for nettverk- og informasjonssikkerhet i EU. Gjennom direktivet etableres sektorovergripende minimumsstandarder for nettverks- og informasjonssikkerhet. Direktivets anvendelsesområde omfatter offentlig forvaltning, tilbydere av informasjonssamfunnstjenester, samt eiere og driftere av samfunnskritisk IKT-infrastruktur. En eventuell implementering av direktivet i norsk rett vil forutsette at det etableres en lovhjemmel for de krav direktivet oppstiller.

I tillegg til sikkerhetsloven foreligger det i dag mange ulike lover og forskrifter som stiller krav til informasjonssikkerhet. Noen er sektorspesifikke mens andre er sektorovergripende. Utvalget skal identifisere eventuelle behov for en harmonisering av lovreguleringen på området.

Utvalget skal foreslå en modernisering av Instruks 17. mars 1972 for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter (beskyttelsesinstruksen). Det skal også vurdere om det er hensiktsmessig å implementere reglene i ny lovgivning.

Tilsyn
Utvalget skal vurdere hvordan det skal føres tilsyn med etterlevelsen av ny lovgivning. Utvalget skal også vurdere hvorvidt det er hensiktsmessig å skille mellom tilsynsoppgaver og rolle som forvaltningsorgan.

Kontroll med selskaper
Utvalget skal vurdere behov for regulering/kontroll overfor selskaper som håndterer informasjon, teknologi og/eller fysiske aktiva av betydning for samfunnets sikkerhet, herunder håndtering av endringer i statens eller andres eierskap i slike selskaper. Dette kan være selskaper innen forsvarssektoren eller sivil sektor.

Annet
Ut over de forhold som er nevnt ovenfor står utvalget fritt til også å vurdere andre områder

som bør reguleres i ny lovgivning for å sikre et helhetlig lovgrunnlag og for å ivareta de utviklingstrekk som er beskrevet innledningsvis.

Dersom utvalget ser behov for å gjøre endringer i mandatet skal dette tas opp med Forsvarsdepartementet og Justis- og beredskapsdepartementet.

3. Generelt
Utvalget skal basere seg på eksisterende kunnskapsgrunnlag og de sikkerhetsutfordringer som dagens moderne, teknologiske og globaliserte samfunn stiller oss overfor når det gjelder tilsiktede uønskede handlinger. Utvalget kan be om særskilte orienteringer og/eller utredninger fra eksperter/ekspertgrupper på enkeltområder. Som en del av vurderingen må utvalget se hen til rapporten fra det digitale sårbarhetsutvalget som leveres 1. september 2015.

Utvalget skal i sitt arbeid sikre at relevante innspill fra berørte aktører blir ivaretatt på en hensiktsmessig måte. Blant annet skal Nasjonal sikkerhetsmyndighets sikkerhetsfaglige råd tas med i vurderingen. Utvalget skal videre i sitt arbeid ta i betraktning relevant internasjonal lovgivning, herunder nordiske lands lovgivning, gjeldende EU-direktiver, NATOs standarder, samt Norges folkerettslige forpliktelser på handels- og investeringsområdet.

Utvalget skal i samsvar med utredningsinstruksen redegjøre for økonomiske, administrative og andre vesentlige konsekvenser av sine forslag. Minst ett av forslagene skal baseres på uendret ressursbruk.

Utvalget skal innen halvannet år etter oppnevningen legge fram en utredning i form av en NOU til Forsvarsdepartementet med forslag til nytt lovgrunnlag for forebyggende nasjonal sikkerhet. Utredningen skal utarbeides i en form som egner seg til å bli sendt på en offentlig høring. De delene av utvalgets arbeid som omfatter gradert informasjon, kan kun behandles av medlemmer som er sikkerhetsklarert for det aktuelle graderingsnivået. Materiale som er gradert utarbeides i separate vedlegg.

1.3 Utvalgets forståelse av mandatet

Utvalget forstår mandatet dit hen at det overordnede samfunnsmålet med et nytt lovgrunnlag for forebyggende nasjonal sikkerhet skal være å legge til rette for en tilfredsstillende sikkerhet rundt funksjonaliteten i kritiske samfunnsfunksjoner. I mandatet vises det til at «utvalgte samfunns- og risikoområder, der tilsiktede uønskede hendelser vil ha store konsekvenser på tvers av fag- og ansvarsområder kan være helse, vann, mat, energi, finansielle tjenester og kommunikasjon». Utvalget forstår *kritiske samfunnsfunksjoner* som nødvendige funksjoner for å holde nevnte tjenester på et nivå som sikrer forsvarlig utøvelse av myndighet og grunnleggende trygghet for befolkningen.

En ny sikkerhetslov med forskrifter skal bidra til å sikre disse samfunnsfunksjonene. For å oppnå dette, er det særlig aktuelt å sikre utvalgte informasjonssystemer, infrastrukturer og pålitelig personell, men loven kan også rette seg mot andre forhold som er nødvendig for sikre forsvarlig utøvelse av myndighet og grunnleggende trygghet for befolkningen.

Dagens sikkerhetslov har som formål å legge forholdende til rette for effektivt å kunne motvirke trusler mot «rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser», jf. sikkerhetsloven § 1 første ledd bokstav a), og omhandler i hovedsak beskyttelse av skjermingsverdig informasjon og skjermingsverdige objekter. Mandatets ordlyd innebærer, slik utvalget forstår det, en bredere tilnærming til lovens virkeområde enn det gjeldende sikkerhetslov har.

Utvalget forstår mandatets angivelse av hva som skal beskyttes som styrende for det nye lovgrunnlagets virkeområde. Kritisk infrastruktur og sensitiv informasjon eies og/eller forvaltes i dag i stor utstrekning av selvstendige rettssubjekter. Det vil i denne sammenheng også være naturlig for utvalget å vurdere hvorvidt det er hensiktsmessig å videreføre virkeområdet for dagens sikkerhetslov. Utvalgets vurdering av hvorvidt eksisterende sektorregelverk gir en tilstrekkelig god sikring, både innad og på tvers av samfunnssektorene, vil også være styrende for virkeområdet for en ny sikkerhetslov.

Med mandatets presisering av *tilsiktede uønskede hendelser* har utvalget lagt til grunn at en ny lov skal rette seg mot tilsiktede uønskede hendelser, og at andre sikkerhetstrusler i utgangspunktet ikke skal omfattes (jf. *safety*-perspektivet). Dette er i samsvar med dagens lov, som er avgrenset til *sikkerhetstruende virksomhet* (spionasje, sabotasje eller terrorhandlinger, jf. lovens § 3 første ledd nr. 2). Slik utvalget ser det, innebærer ikke dette at sikkerhetsarbeidet for henholdsvis tilsiktede og utilsiktede hendelser bør forstås som adskilte størrelser ved operasjonalisering av regelverket. For den enkelte virksomhet vil det

både være nødvendig og hensiktsmessig å kunne se arbeidet med forebyggende sikkerhet under ett, uavhengig av hvilke typer trusler det tas sikte på å beskytte seg mot. I motsatt fall risikerer man å utvikle suboptimale og lite kostnadseffektive løsninger.

Utvalget anser seg ikke bundet av definisjonen av *sikkerhetstruende virksomhet* i dagens sikkerhetslov. Definisjonen angir imidlertid noen typer trusler som det med en ny lov vil være særlig viktig å beskytte seg mot.

Utvalget vil gjøre ytterligere presiseringer og avgrensinger når det gjelder den begrepsbruk som er lagt til grunn i mandatet, herunder begrepene kritisk infrastruktur, kritiske samfunnsfunksjoner og sensitiv og samfunnsviktig informasjon.

Det fremgår også av mandatet at utvalget i samsvar med utredningsinstruksen skal redegjøre for økonomiske, administrative og andre vesentlige konsekvenser av sine forslag. 1. mars 2016 trådte en ny utredningsinstruks i kraft. Utvalget vil legge den nye utredningsinstruksen til grunn for sitt arbeid. Den nye instruksens hovedformål er å legge et godt grunnlag for beslutninger om statlige tiltak gjennom å identifisere alternative tiltak og å utrede og vurdere virkningen av tiltak. Når en utredning vurderer tiltak som forventes å ha vesentlige nytte- eller kostnadsvirkninger, herunder vesentlige budsjettmessige virkninger for staten, skal det gjennomføres samfunnsøkonomiske analyser. Analysen skal legge grunnlaget for å identifisere og prioritere de beste tiltakene for å legge til rette for en tilfredsstillende sikkerhet for funksjonaliteten i kritiske samfunnsfunksjoner.

Utvalget har lagt til grunn at hensynene til personvern og den enkeltes rettssikkerhet gjennomgående vil være et sentralt vurderingstema. Denne forståelsen av mandatet er også bekreftet av oppdragsgiver. Den nye utredningsinstruksen stiller krav om at i den grad de tiltak som vurderes berører prinsipielle spørsmål, skal utredningen drøfte disse på en balansert, systematisk og helhetlig måte. Et prinsipielt spørsmål, som dette utvalget særlig vil drøfte, er hvordan en på en balansert måte kan ivareta både nasjonal sikkerhet, rettssikkerhet og personvern. Utvalget vil i denne sammenheng understreke at en ny sikkerhetslov ikke må få virkninger som setter i fare de verdier som loven skal beskytte.

Utvalget legger til grunn for sitt arbeid at grunnleggende rettigheter og Norges folkerettslige forpliktelser, jf. Grunnloven og menneskerettighetsloven, utgjør rammen for en ny lov og for praktiseringen av den.

I henhold til ny utredningsinstruks skal utvalget også vurdere forutsetningene for en vellykket gjennomføring. Staten har et bredt spekter av virkemidler som kan benyttes for å sikre at samfunnsutviklingen går i ønsket retning. Utvalgets mandat er i utgangspunktet avgrenset til å vurdere ett av disse virkemidlene – påvirkning gjennom bruk av juridiske virkemidler i form av en ny lov om forebyggende nasjonal sikkerhet. Utvalget ser seg imidlertid ikke bundet av kun å se på loven, men også peke på andre tiltak som staten har i sin virkemiddelportefølje i den utstrekning dette anses nødvendig for å sikre at loven vil virke etter intensjonen.

1.4 Prosesser med innvirkning på utvalgets arbeid

Parallelt med utvalgets arbeid har det også pågått en rekke andre utredningsarbeider og prosesser med direkte eller indirekte innvirkning på tema og problemstillinger av relevans for arbeidet. Under følger en kort oversikt av noen av de viktigste utredningsarbeidene. Listen er ikke uttømmende.

- Den 28. april 2015 overleverte en uavhengig ekspertgruppe sin rapport Ekspertgruppen for Forsvaret av Norge – Et felles løft, til forsvarsminister Ine Eriksen Søreide. Ekspertgruppen hadde som mandat å utarbeide en rapport om Forsvarets forutsetninger for å kunne løse sine mest krevende oppgaver.
- Den 10. september 2015 overleverte Nasjonal sikkerhetsmyndighet (NSM) sitt sikkerhetsfaglige råd til Forsvarsdepartementet og Justis- og beredskapsdepartementet. NSM ble gitt i oppdrag å komme med en vurdering av hvordan samfunnet bør innrette arbeidet med forebyggende sikkerhet i perioden frem mot 2020 og hvordan Norge bør møte de økte sikkerhetstruslene.
- Den 30. november 2015 overleverte det digitale sårbarhetsutvalget (Lysne-utvalget) sin utredning til justis- og beredskapsministeren. Lysne-utvalget har kartlagt samfunnets digitale sårbarhet, og foreslått tiltak for å styrke beredskapen og redusere den digitale sårbarheten i samfunnet.
- Den 15. april 2016 godkjente regjeringen Solberg Prop. 97 L (2015–2016) Endringer i sikkerhetsloven (reduksjon av antall klareringsmyndigheter mv.). I proposisjonen ble det foreslått endringer i gjeldende sikkerhetslov som

det var behov for å få på plass raskt. I forbindelse med behandlingen av Innst. 352 L (2015–2016) til Prop. 97 L (2015–2016) om endringer i sikkerhetsloven, vedtok Stortinget regjeringens forslag den 8. juni 2016.[1]

- Den 17. juni 2016 fremmet regjeringen Solberg Prop. 151 S (2015–2016) Kampkraft og bærekraft – Langtidsplan for forsvarssektoren. I proposisjonen la regjeringen frem en rekke anbefalinger for å øke forsvarsevnen og tilpasse Forsvaret til den sikkerhetspolitiske situasjonen. Langtidsplanen er blant annet basert på forsvarssjefens fagmilitære råd (FMR) Et forsvar i endring. FMR er et uavhengig fagmilitært råd, hvor forsvarssjefen er gitt i oppdrag å vurdere hvordan Forsvaret på en best mulig måte kan ivareta sine dimensjonerende oppgaver og ambisjon, samt sikre at Forsvaret forblir relevant og troverdig også i fremtiden.
- Den 26. august 2016 overleverte Lysne II-utvalget sin utredning Digitalt grenseforsvar (DGF) til Forsvarsdepartementet. Lysne II-utvalget ble nedsatt for å utrede problemstillinger knyttet til Etterretningstjenestens mulig tilgang til elektronisk informasjon som kommuniseres i fiberoptiske kabler inn og ut av Norge.

Alle de nevnte utredningsarbeidene og prosessene behandler ulike aspekter ved forebyggende sikkerhet. Utvalgets utredning er et selvstendig bidrag, men må sees mot dette bakteppe.

1.5 Utvalgets arbeid

Utvalget har hatt 15 møter, fordelt på 27 møtedager.

Utvalget har i tillegg gjennomført studiebesøk til Brussel, Stockholm, København og London. I Stockholm møtte utvalget representanter fra den norske, britiske og nederlandske EU-delegasjon, representanter fra noen av EUs generaldirektorater, samt private aktører. I tillegg møte utvalget en rekke representanter fra ulike deler av NATOs organisasjon. I Stockholm møtte utvalget representanter fra Justitiedepartementet, Myndigheten för samhällsskydd och beredskap og Säkerhetspolisen. I Danmark ble det gjennomført møter med representanter fra Forsvarsministeriet, Justisministeriets, Forsvarets Efterretningstjeneste, Beredskapbsstyrelsen, Politiets Efterretningstjeneste, samt Danish Institute for International Studies. I London møtte utvalget representanter fra Cabinet Office, Royal United Services Institute, Home Affairs Select Committee, Home Office, MI5's Centre for the Protection of National Infrastructure, samt private aktører.

Utvalgets arbeid er basert på ulike metoder og faktiske grunnlag:

- Eksisterende utredninger og analyser.
- Skriftlige innspill og møter med en rekke sentrale aktører innen forebyggende sikkerhet, både offentlige og private virksomheter.
- Utredninger som er gjennomført av offentlige og private virksomheter på oppdrag fra utvalget.

Utvalget, og dets sekretariat, har i tillegg hatt en løpende dialog med en rekke virksomheter i utvalgsperioden, dels for å få utdypet og konkretisert ulike tema og problemstillinger og dels for å kvalitetssikre informasjon utvalget har innhentet og bearbeidet.

Utvalget har også gjennomført en halvdagskonferanse for å få belyst problemstillinger knyttet til sikkerhet og personvern i en digital tidsalder.

For en fullstendig oversikt over de aktørene utvalget har gjennomført møter med, og mottatt skriftlige innspill fra, vises det til vedlegg 2 og 3.

1.6 Struktur og innhold

Utredningen er delt inn i fire deler.

Del I gir en redegjørelse for utvalgets sammensetning og mandat, samt en beskrivelse av utvalgets mandatforståelse. I tillegg inneholder del I oppsummeringen av utvalgets konklusjoner og anbefalinger.

Del II redegjør for bakteppet som danner grunnlaget for utvalgets vurderinger og anbefalinger. Først gjennomgås sentrale begreper innen forebyggende sikkerhet og beredskap, samt relasjonen mellom de ulike begrepene. Deretter gis det en redegjørelse for hvordan det forebyggende sikkerhetsarbeidet i Norge er organisert, samt en overordnet beskrivelse av noen av de mest sentrale aktørene innen sikkerhetsarbeidet.

I tillegg gis det en gjennomgang av dagens sikkerhetsutfordringer. Først gis det en omtale av risikostyring i staten som grunnlag for å oppnå nasjonal sikkerhet og omtale av risikovurderingsmetodikk. Videre er beskrives hvilke verdier som må vernes, hvilke trusler som kan ramme verdiene og hvilke sårbarheter i samfunnet som trusselaktører kan utnytte. Avslutningsvis gjen-

[1] Lovvedtak 91, (2015–2016).

nomgås noen av de virkemidlene staten har til rådighet for å styre samfunnsutviklingen i en ønsket retning. Del II avsluttes med en beskrivelse av forholdet mellom forebyggende sikkerhet, rettssikkerhetsgarantier og personvern.

Del III er hoveddelen av utvalgets utredning. Her gis det en tematisk gjennomgang av utvalgets vurderinger og anbefalinger, samt de faktuelle beskrivelsene utvalget har lagt til grunn for vurderingene. Gjennomgangen er i stor grad basert på gjeldende sikkerhetslovs tematiske kapittelinndeling. Enkelte særlige temaer er også omtalt i egne kapitler.

Del IV består av utvalgets lovforslag og særlige merknader til de enkelte bestemmelsene.

Kapittel 2
Oppsummering

Norge er et grunnleggende trygt samfunn. Utredninger som avdekker sårbarheter og foreslår forbedringer i den forebyggende sikkerheten rokker ikke ved det. Samtidig er verden rundt oss, trusselbildet, og samfunnet som skal beskyttes, mer komplekst enn før. Staten må ha tilstrekkelige virkemidler i møte med disse utfordringene på borgernes vegne.

Statens aller viktigste oppgave er nettopp å beskytte landets borgere og samfunnet de er en del av. En stat som ikke evner å sikre sin egen og borgernes overlevelse misligholder samfunnskontrakten mellom stat og borger. For å ivareta denne oppgaven og overholde samfunnskontrakten er det helt avgjørende at staten makter å opprettholde samfunnets grunnleggende funksjoner uavhengig av hvilken ekstern påvirkning de utsettes for.

Sikkerhetsutvalget ble oppnevnt blant annet fordi anvendelsen av gjeldende sikkerhetslov avdekket grunnleggende uenigheter knyttet til lovens nedslagsfelt. Sammen med en negativ endring i risiko- og sårbarhetsbildet medførte dette et behov for en helhetlig gjennomgang og nytenkning av forebyggende nasjonal sikkerhet.

Utvalget har i sitt arbeid stått overfor en rekke grunnleggende avveininger, som har hatt direkte innvirkning på hvordan en ny lov kan og bør innrettes.

Et helt sentralt og gjennomgående tema har vært avveiningen mellom behovet for en helhetlig og sektorovergripende tilnærming til forebyggende sikkerhet på den ene siden, og ivaretakelsen av den enkeltes samfunnssektors særegenheter på den andre. Dette har betydning både for hvilket nedslagsfelt en ny lov bør ha, og for hvordan ansvars- og myndighetsfordelingen etter loven bør være. Denne avveiningen har også betydning for hvordan lovens krav bør innrettes.

Videre har en balansert avveining mellom forebyggende sikkerhet, rettssikkerhet og personvern, stått sentralt i utvalgets arbeid. En slik avveining er viktig for å hindre at sikkerhetstiltak som isolert sett er effektive, i et videre perspektiv undergraver de verdier som skal beskyttes. En nedtoning av rettssikkerheten vil derfor på sikt også svekke stats- og samfunnssikkerheten.

I tillegg har avveiningen mellom samfunnsøkonomisk og bedriftsøkonomisk lønnsomhet vært et viktig vurderingstema for utvalget. Sikkerhet har en kostnadsside som det ikke er mulig å komme utenom. I et samfunnsperspektiv vil de sikkerhetsmessige gevinstene samtidig kunne overstige de kostnadsmessige ulempene som enkeltvirksomheter påføres. Et grunnleggende premiss for utvalget er at kostnader som følger av loven, skal stå i et rimelig forhold til de nyttevirkningene som faktisk oppnås ved tiltaket.

Utvalget anbefaler i sitt lovforslag følgende:

- Lovens formål bør være å beskytte grunnleggende samfunnsfunksjoner. Det er disse funksjonene en trusselaktør vil forsøke å ta ut ved et anslag som rammer Norges mest grunnleggende interesser.
- Lovens virkeområde bør utvides og samtidig være mer målrettet. Virksomheter som er av kritisk betydning for at grunnleggende samfunnsfunksjoner skal kunne opprettholdes, bør underlegges loven uavhengig av eierskap eller organisasjonsform. En forutsetning for en slik utvidelse er at lovens krav har en funksjonell innretning som kan tilpasses den enkelte samfunnssektor.
- De generelle prinsippene for krisehåndtering og beredskap bør ligge fast, samtidig som behovet for en helhetlig og sektorovergripende tilnærming til forebyggende sikkerhet ivaretas. Dette bør gjenspeiles både i hvordan ansvar og myndighet fordeles, og i hvordan tilsyn med virksomheter som er underlagt loven skal innrettes.
- Loven bør pålegge norske myndigheter en rådgivningsplikt overfor virksomheter som omfattes av loven, og en plikt til å legge til rette for at sikkerhetsrelevant informasjon deles med berørte aktører.

- Alle informasjonssystemer som er av kritisk betydning for grunnleggende samfunnsfunksjoner, bør omfattes av loven. Dette gjelder informasjonssystemer som behandler sikkerhetsgradert informasjon, og andre systemer som er av kritisk betydning for opprettholdelse av samfunnsfunksjonene.
- Loven bør ha et systemfokus som også omfatter beskyttelse av infrastruktur som er av kritisk betydning for samfunnsfunksjonene.
- Loven må legge til rette for effektiv forebygging og avdekking av at utro tjenere får tilgang til informasjon eller områder hvor skadepotensialet er stort.
- Det bør etableres en mekanisme for å kontrollere og i ytterste konsekvens stanse utenlandske oppkjøp av selskaper som er av kritisk betydning for grunnleggende samfunnsfunksjoner.

Samfunnsutviklingen i stort har aktualisert og forsterket behovet for en mer helhetlig tilnærming til arbeidet med forebyggende nasjonal sikkerhet. En økende grad av digitalisering har resultert i økte gjensidige avhengigheter på tvers av tradisjonelle skillelinjer mellom samfunnssektorer, mellom privat og offentlig virksomhet, og mellom sivile samfunnssektorer og landets militære forsvar og forsvarssektoren for øvrig. Samtidig har fremveksten av et nettverksbasert samfunn ført til at de samme skillelinjene er blitt mindre markante. Denne utviklingen har vært positiv og gitt et avansert samfunn som kan håndtere store oppgaver, men har også skapt nye sårbarheter.

For å møte gamle og nye utfordringer mener utvalget at en ny lov på en balansert måte må ivareta både hensynet til den enkelte sektors særegenheter *og* behovet for sektorovergripende og helhetlig styring av den samlede nasjonale sikkerheten. På denne måten kan det bygges bro over de motsetningene som har gjort det vanskelig å anvende dagens sikkerhetslov. Dette fordrer en funksjonell innretning på loven, med sektortilpasninger som ansvarliggjør både den enkelte samfunnssektor og den enkelte virksomhet. Videre er det avgjørende at tiltak som skal redusere sårbarheter eller forebygge uønskede hendelser også er samfunnsøkonomisk lønnsomme. Kostnader som påløper i forbindelse med lovpålagte sikkerhetstiltak må stå i et rimelig forhold til den sikkerhetsmessige gevinsten som oppnås ved tiltaket. Det er her viktig å ha for øye at det kan være svært store kostnader ved å rammes av terrorisme, sabotasje og spionasje, både materielt og i form av tapte menneskeliv. Utvalget mener at de kostnadene som påføres virksomheter som følge av de krav som oppstilles i loven både er nødvendige og riktige sett i lys av dagens trusselbilde.

Forebyggende nasjonalt sikkerhetsarbeid er et felles anliggende. Fra virksomhets- til regjeringsnivå gjelder samme logikk: Nasjonen Norge er ikke sterkere enn det svakeste ledd, og reell samhandling for sikkerhet er den viktigste forutsetningen for å lykkes i å forbedre Norges sikkerhet – skritt for skritt.

2.1 Lovens virkeområde

Utvalget anbefaler at forebyggende nasjonal sikkerhet fortsatt reguleres i én lov som gjelder på tvers av sektorer og andre skillelinjer. Felles utfordringer krever felles løsninger, og én felles lov legger best til rette for tverrsektoriell samhandling og harmonisering av sikkerhetsnivået i samfunnet. Et felles rammeverk gir også de beste forutsetningene for god ledelse, styring, koordinering og ressursutnyttelse.

Utvalget mener at den nye sikkerhetsloven bør ha som formål å beskytte de *funksjonene* som er helt avgjørende for å ivareta de verdiene sikkerhetsloven skal hegne om. I ytterste konsekvens er det nettopp disse funksjonene en trusselaktør vil forsøke å ta ut ved et anslag mot Norge og dets mest grunnleggende interesser og verdier. En slik funksjonstilnærming vil også være i tråd med den øvrige metodikken i arbeidet med samfunnssikkerhet og beredskap. Utvalget har derfor valgt å benytte begrepet *grunnleggende nasjonale funksjoner* for å angi lovens virkeområde.

Selve grunnlaget for å beslutte hva som utgjør *grunnleggende nasjonale funksjoner*, er statens sikkerhetspolitiske ansvar for å ivareta Norges suverenitet, territorielle integritet og demokratiske styreform. En funksjon er å anse som grunnleggende for Norge dersom bortfall av denne får konsekvenser som truer disse overordnede interessene.

Utvalgets lovforslag innebærer en begrenset, men nødvendig utvidelse av virkeområdet sammenliknet med gjeldende sikkerhetslov. Loven vil ikke være en bred samfunnssikkerhetslov, men skal samtidig heller ikke være en ren statssikkerhetslov. Fra utvalgets side er utvidelsen av lovens virkeområde ment å reflektere den generelle samfunnsutviklingen som har funnet sted siden gjeldende sikkerhetslov trådte i kraft for 15 år siden.

Utvalget anbefaler at lovens virkeområde innrettes slik at enhver virksomhet, offentlig eller privat, *som har råderett over informasjon, informa-*

sjonssystemer, objekter eller infrastruktur, eller som driver aktivitet, som er av kritisk betydning for grunnleggende nasjonale funksjoner, omfattes av loven.

Den nærmere avgrensningen av hva som vil utgjøre grunnleggende nasjonale funksjoner i medhold av den nye sikkerhetsloven, vil slik utvalget ser det måtte avgjøres konkret basert på en helhetlig vurdering der både sektorovergripende og sektorspesifikke perspektiver ivaretas. For at loven skal få den ønskede effekt vil det være avgjørende å etablere et system for å identifisere grunnleggende nasjonale funksjoner og hvilke virksomheter som er av kritisk betydning for disse.

2.2 Ansvars- og myndighetsfordelingen

I dag utføres det mye godt og grundig sikkerhetsarbeid i de ulike sektorene og på tvers av dem. Praktiseringen av dagens sikkerhetslov har imidlertid vist seg utfordrende og tidvis trekker ulike gode krefter i forskjellige retninger. Dette fører ikke til god sikkerhet og er ikke god ressursutnyttelse.

En mer hensiktsmessig ansvars- og myndighetsfordeling innenfor forebyggende sikkerhet etter loven, har stått sentralt i utvalgets arbeid. Et utgangspunkt for utvalgets arbeid har vært at de generelle prinsippene for krisehåndtering og beredskap ligger fast, og at de også bør gjelde for innretningen på en ny sektorovergripende lov om forebyggende nasjonal sikkerhet.

Utvalgets målsetting med den foreslåtte fordelingen av ansvar og myndighet etter loven er å legge til rette for en god samhandling mellom de sentrale aktørene innenfor forebyggende sikkerhet, på tvers av samfunnssektorene. Slik utvalget ser det, er en slik samhandling helt avgjørende for at det forebyggende sikkerhetsarbeidet i Norge skal få full effekt. God samhandling oppnås først og fremst ved en balansert tilnærming til ansvarsprinsippet og samvirkeprinsippet.

I tråd med ansvarsprinsippet bør det primære ansvaret for forebyggende sikkerhet i de ulike samfunnssektorene ligge i det enkelte fagdepartement. Det er det enkelte departement som kjenner sin sektor best og har de beste forutsetningene for å kunne identifisere grunnleggende nasjonale funksjoner og virksomheter av kritisk betydning for disse, samt gjøre nødvendige samfunnsøkonomiske prioriteringer innad i sektoren. Utvalget anbefaler at det lovfestes en systematikk for hvordan de ulike departementene skal identifisere grunnleggende nasjonale funksjoner innenfor eget myndighetsområde, samt de virksomheter som har en kritisk rolle i understøttelsen av slike funksjoner. Som grunnlag for en slik identifisering, bør det utarbeides tverrsektorielle scenarier.

For å ivareta samvirkeprinsippet vil utvalget samtidig understreke at også det helhetlige og sektorovergripende perspektivet må ivaretas. Dette både for å kunne fange opp sektorovergripende avhengigheter som det enkelte fagdepartement ikke nødvendigvis har forutsetning for å identifisere, og for å bidra med faglig bistand og kvalitetssikring innenfor de ulike samfunnssektorene. Trusselbildet de enkelte virksomhetene står overfor, særlig innenfor cyber-domenet, er i mange tilfeller av sektorovergripende karakter.

Utvalget anbefaler at det sektorovergripende ansvaret fortsatt skal ivaretas av Nasjonal sikkerhetsmyndighet. Det bør imidlertid legges bedre til rette for at Nasjonal sikkerhetsmyndighet reelt sett skal kunne ivareta dette ansvaret. Utvalget mener at Nasjonal sikkerhetsmyndighet bør ha ansvaret for å utvikle og vedlikeholde en sektorovergripende nasjonal oversikt over departementenes identifisering av grunnleggende nasjonale funksjoner og hvilke virksomheter som omfattes av sikkerhetsloven ved enkeltvedtak. Nasjonal sikkerhetsmyndighet bør også ha ansvaret for å identifisere virksomheter som ikke naturlig faller inn under et departements myndighetsområde.

En slik ansvarsfordeling bør etableres også for tilsyn. Utvalget anbefaler en tilsynsmodell som ivaretar målsettingen om en helhetlig og tverrsektoriell tilnærming til forebyggende sikkerhet, samtidig som den ivaretar hensynet til den enkelte samfunnssektors særegenheter. I samfunnssektorer hvor det eksisterer sektormyndigheter med tilsynsansvar for forebyggende sikkerhetsarbeid, bør disse myndighetene også gjennomføre tilsyn med virksomheter som omfattes av den nye loven. Samtidig må Nasjonal sikkerhetsmyndighet ha en sentral rolle overfor de enkelte sektormyndigheter for å sikre en helhetlig tilnærming til det forebyggende sikkerhetsarbeidet.

Utvalget anbefaler at det opprettes et tvisteorgan for å avgjøre uenigheter mellom virksomheter som omfattes av loven og myndigheter, og myndigheter imellom. Et slikt tvisteorgan er viktig for å ivareta rettssikkerheten til virksomheter som gjennom enkeltvedtak blir underlagt loven, og for å sikre samfunnsøkonomisk lønnsomme prioriteringer. For virksomhetene vil tvisteorganet tjene som en rettssikkerhetsgaranti. Ved uenighet

mellom myndigheter skal tvisteorganet sørge for en rask og uavhengig avgjørelse.

Forvaltningsansvaret for sikkerhetsloven bør etter utvalgets syn fortsatt tilligge Forsvarsdepartementet. Imidlertid er det også ved utøvelsen av denne myndigheten helt avgjørende med god samhandling mellom de berørte aktørene. Ikke minst forutsettes det et godt samarbeid med Justis- og beredskapsdepartementet, som har det overordnede og koordinerende ansvaret for forebyggende sikkerhet i de sivile samfunnssektorene.

2.3 Rådgivning og informasjonsdeling

Innsikt i det aktuelle trusselbildet er en forutsetning for at den enkelte virksomhet skal være i stand til å kunne gjøre gode risikovurderinger og iverksette de riktige sikkerhetstiltakene. Flere aktører utvalget har vært i kontakt med har uttrykt et klart behov for mer og oppdatert informasjon om trusselbildet.

For å kunne motta tilstrekkelig informasjon om trusselbildet, må virksomheten omfattes av sikkerhetsloven slik at den er i stand til å motta og behandle sikkerhetsgradert informasjon. Et relevant og tilstrekkelig informasjonsgrunnlag om det aktuelle trusselbildet, må gjøres tilgjengelig i en form som er tilpasset og anvendbar for de virksomhetene som omfattes av loven.

Utvalget foreslår en tydeliggjøring og fremheving av sikkerhetsmyndighetens rådgivningsplikt overfor virksomheter som omfattes av loven. Nasjonal sikkerhetsmyndighet bør ha en fremoverlent og aktiv rolle overfor virksomhetene og være på tilbudssiden i sin rådgivningsvirksomhet. En slik rådgivning vil blant annet kunne bidra til økt forståelse hos virksomhetene om hvordan det forebyggende sikkerhetsarbeidet bør innrettes for å få størst mulig effekt.

Utvalget foreslår å lovfeste en plikt for Nasjonal sikkerhetsmyndighet til å legge til rette for og koordinere at nødvendig informasjon gjøres tilgjengelig for virksomheter og myndigheter som omfattes av loven. Andre myndighetsaktører som Etterretningstjenesten og Politiets sikkerhetstjeneste, har en sentral rolle i utarbeidelsen av trusselvurderinger. Sikkerhetsmyndighetens tilretteleggings- og koordineringsplikt fordrer således en tett og god samhandling med andre relevante myndighetsaktører.

For å kunne ha en god og oppdatert oversikt over sikkerhetstilstanden, er det nødvendig at Nasjonal sikkerhetsmyndighet mottar relevant informasjon om sikkerhetsrelaterte hendelser. Utvalget foreslår derfor en plikt til å rapportere slike hendelser for virksomheter som er underlagt loven. Dette vil også sette myndighetene bedre i stand til å forstå trusselbildet og iverksette nødvendige tiltak for å forebygge, samt bidra til å dele informasjon med andre utsatte samfunnssektorer og virksomheter.

I tillegg til generell informasjon om trusselbildet vil virksomheter underlagt loven kunne få konkret råd og veiledning fra sikkerhetsmyndighetene om hvordan det forebyggende sikkerhetsarbeidet bør innrettes for å få størst mulig effekt.

2.4 Beskyttelse av informasjonssystemer

Digitaliseringen av samfunnet har bidratt til økt IKT-avhengighet for virksomheter som understøtter grunnleggende nasjonale funksjoner. Digitale angrep utgjør en alvorlig og økende trussel mot norske verdier, og det oppdages stadig nye sårbarheter i IKT-systemene.

Utfordringene begrenser seg ikke til informasjonssystemer som behandler sikkerhetsgradert informasjon. Utvalget anbefaler derfor at alle informasjonssystemer som er av kritisk betydning for grunnleggende nasjonale funksjoner, omfattes av loven. Det vil omfatte alt fra tradisjonelle informasjons- og kommunikasjonssystemer til kontroll- og styringssystemer. Avgjørende for *om* informasjonssystemet skal beskyttes etter loven, er hvilken rolle systemet har i virksomhetens understøttelse av en grunnleggende nasjonal funksjon.

2.5 Beskyttelse av infrastruktur

Beskyttelse av objekter og infrastruktur av kritisk betydning for grunnleggende nasjonale funksjoner er ett av hovedelementene i forebyggende nasjonal sikkerhet. Det er særlig tre forhold som må være på plass for å oppnå et forsvarlig sikkerhetsnivå på dette området.

For det første må det gå klart frem av loven at det ikke er hensiktsmessig bare å vurdere beskyttelsesbehovet for hvert enkelt objekt isolert. Gjensidige avhengigheter i og mellom sektorer gjør det helt nødvendig å se på objektene i de systemene de er en del av. Utvalget mener det er viktig å ha et slikt systemfokus i forebyggende sikkerhet, og har derfor foreslått at dette gjenspei-

les i loven gjennom å lovregulere også *skjermingsverdig infrastruktur*.

Utvalget foreslår en videreføring av dagens systematikk, der ansvarlig departement for den enkelte samfunnssektor har det primære ansvaret for å utpeke, klassifisere og holde oversikt over skjermingsverdige objekter og infrastruktur.

Utvidelsen av lovens virkeområde gjør det også nødvendig med en mer funksjonell tilnærming til beskyttelse av slike objekter og infrastruktur. Det primære ansvaret for å sikre at objektene og infrastrukturen har et forsvarlig sikkerhetsnivå, tilligger den enkelte virksomhet. Også på dette området må det være en forutsetning at tiltakenes kostnader står i et rimelig forhold for til den sikkerhetsmessige effekten som oppnås. Ved vurderingen av hva som er forsvarlig, vil virksomhetene også måtte se hen til gjensidige avhengigheter og deres rolle i understøttelsen av en grunnleggende nasjonal funksjon.

2.6 Personellsikkerhet

Personellsikkerhet er et sentralt virkemiddel for å forebygge og avdekke at utro tjenere får tilgang til informasjon eller områder hvor skadepotensialet er stort. Dette er samtidig et område som må være strengt regulert, særlig av hensyn til de krav legalitetsprinsippet stiller til klare hjemmelsgrunnlag og kravene til tilfredsstillende rettssikkerhetsgarantier ved inngrep i personvernet.

Utvalget mener at dagens regelverk for personellsikkerhet i hovedsak har en hensiktsmessig tilnærming. Utvalget anbefaler imidlertid enkelte justeringer i loven, dels for å legge til rette for en mer effektiv behandling av klareringssaker og dels for å gjøre regelverket mer fleksibelt for individuelle tilpasninger.

Utvalget foreslår at det gis hjemmel for å foreta adgangsklarering for tilgang til skjermingsverdige objekter eller infrastruktur. En adgangsklarering vil innebære en mindre omfattende prosess enn en sikkerhetsklarering, samtidig vil den gi et bredere informasjonstilfang enn en ordinær vandelskontroll på grunnlag av en politiattest. Det overlates til det enkelte fagdepartement å treffe vedtak om krav til slike adgangsklareringer for konkrete objekter eller infrastruktur som utpekes i medhold av loven.

Utvalget mener det i større grad bør tas høyde for at forhold av betydning for en klarering kan endre seg innenfor en klarerings gyldighetstid. Utvalget foreslår derfor at klareringsmyndigheten skal få adgang til å anmode om fornyet personkontroll ved mistanke om nye forhold og som ledd i den sikkerhetsmessige oppfølgingen av vedkommende.

I tillegg foreslår utvalget en hjemmel for å kunne dele nærmere angitt informasjon med Politiets sikkerhetstjeneste der dette er nødvendig for at tjenesten skal kunne ivareta sitt samfunnsoppdrag, særlig knyttet til forebygging av overtredelser av straffelovens kapittel 17. Slik informasjonsdeling vil være avgrenset til opplysninger knyttet til aktuelle personers klareringsstatus, tjenestested og tilknytning til andre stater.

2.7 Eierskapskontroll

Utvalget har vurdert hvorvidt eksisterende regelverk gir tilstrekkelige virkemidler for å kunne ha kontroll med virksomheter som håndterer informasjon, teknologi og/eller fysiske aktiva av betydning for grunnleggende nasjonale funksjoner. Utvalget mener at det eksisterende regelverket alene ikke kan hindre at nasjonal sikkerhet blir skadelidende ved at strategisk viktige selskaper helt eller delvis blir kjøpt opp av utenlandske aktører. Særlig gjelder dette hensynet til forsyningssikkerhet og beredskap, samt behovet for å beholde nasjonal kontroll på nøkkelkompetanse. Utvalget anbefaler derfor en lovhjemmel som vil gjøre det mulig å kontrollere og i ytterste konsekvens stanse oppkjøp som vurderes å kunne ha skadevirkninger for nasjonal sikkerhet. Bestemmelsen er ment å skulle være en sikkerhetsventil for de tilfeller det vil være uforsvarlig ikke å gripe inn.

2.8 Avslutning

Med forslaget til ny lov om forebyggende nasjonal sikkerhet har utvalget lagt frem et helhetlig system for hvordan forebyggende sikkerhet knyttet til samfunnets mest grunnleggende funksjoner bør ivaretas. Forslaget er ambisiøst, men reflekterer med det også de betydelige utfordringene i sikkerhetsarbeidet som er avdekket i utvalgets arbeid.

Utvalget erkjenner samtidig at en ny sikkerhetslov ikke vil løse alle problemer Norge har i det forebyggende sikkerhetsarbeidet. Utvalget mener likevel at den nye loven vil være et bidrag til å kunne iverksette treffsikre og samfunnsøkonomisk lønnsomme sikkerhetstiltak.

Den foreslåtte nye loven er innrettet slik at den skal kunne stå seg over tid, tåle større sam-

funnsmessige endringer og teknologisk utvikling, samt dekke fred, krise og krig. Forebyggende sikkerhet må ses i et langsiktig strategisk perspektiv, hvor alle samfunnets tilgjengelige ressurser må trekke i samme retning for å løse de utfordringer nasjonen står overfor. Det vil derfor alltid være en utfordring – men samtidig påkrevet – å heve blikket og vurdere de langsiktige implikasjonene i det daglige forebyggende sikkerhetsarbeidet.

Utvalgets forslag til innretning på den nye loven legger et stort ansvar på de enkelte fagdepartementene, og forutsetter at de ulike samfunnssektorene ivaretar dette ansvaret. Nøkkelbegreper i denne sammenheng er tilstrekkelig kompetanse, samt evne og vilje til samhandling og samarbeid.

Samtidig påligger det regjeringen som kollektiv et særlig ansvar for å påse at forebyggende sikkerhetsarbeid følges opp på en helhetlig og forsvarlig måte.

God samhandling mellom sektormyndigheter og nasjonale myndigheter er essensielt for å oppnå et forsvarlig sikkerhetsnivå. Mange vil huske Gjørv-kommisjonens utsagn om at 22. juli-angrepene er historien om ressursene som ikke fant hverandre, da det gjaldt som mest. Utvalgets arbeid har avdekket at mangelfull samhandling har vært og er et problem også i forbindelse med anvendelsen av den nåværende sikkerhetsloven. Utvalgets viktigste tilbakemelding til samfunnet er derfor en sterk oppfordring til styrket *samhandling for sikkerhet*.

Del II
Bakteppe

Kapittel 3
Forebyggende sikkerhet

3.1 Innledning

For at den videre utredningen skal gi god mening er det viktig å redegjøre for utvalgets forståelse av en del grunnleggende begreper. Dette gjelder fremfor alt *forebyggende sikkerhet*, men også en del relaterte begreper som *beredskap* og *krisehåndtering*. Hva er forskjellen mellom forebyggende sikkerhet og beredskap? Og hva er sammenhengen mellom sikkerhetsarbeidet før, under og etter nasjonale kriser og hendelser? Selv om forebyggende sikkerhet per definisjon alltid foregår i tidsperioden forut for kriser og hendelser må man se helhetlig – også tidsmessig – på hvordan man best beskytter samfunnet mot tilsiktede uønskede hendelser.

Dette kapittelet fokuserer på faktabeskrivelser, men reiser også noen sentrale problemstillinger og utfordringer rundt forebyggende sikkerhet i Norge. Utvalget er i dette kapittelet mer opptatt av å reise problemstillinger enn å fremme forslag til løsninger og konkludere. Mange av problemstillingene utvalget har kommet over i sitt arbeid er det andre som må løse. Dette rokker ikke ved at utvalget kan bidra konstruktivt ved å rette oppmerksomhet mot konkrete forbedringspunkter.

Dette kapittelet vil kort skissere hvordan sentralforvaltningens sikkerhetsarbeid fungerer i dag, og hvordan Norges sikkerhetsapparat er bygget opp. Dette inkluderer en oversikt over hvem som har ansvar for sikkerhet på ulike nivåer i forvaltningen. En sentral problemstilling for sikkerhetsarbeidet ligger i spenningen mellom sektorprinsippet og samvirkeprinsippet. Førstnevnte foreskriver at hver statsråd styrer sin sektor og har konstitusjonelt ansvar og kompetanse innenfor sitt myndighetsområde. Samvirkeprinsippet setter derimot krav til nettopp samvirke på tvers av de tradisjonelle sektorlinjene. Disse to prinsipper er tidvis krevende å ivareta samtidig.

Norge opererer med et totalforsvarskonsept der sivil og militær sektor gjensidig skal kunne understøtte hverandre i fred, krise og krig. Samfunnssikkerheten har blitt viktigere for statens sikkerhetsarbeid. Det har også revitalisert interessen for totalforsvaret fra både den sittende og den forrige regjering. Dette er noe av bakgrunnen for at regjeringen i 2015 reviderte dokumentet Støtte og Samarbeid: en beskrivelse av totalforsvaret i dag.[1] Publikasjonen er et oppslagsverk som erstatter og bygger videre på et tilsvarende dokument utgitt i 2007.

Dette kapittelet avsluttes med en kort beskrivelse av Norges EOS-tjenester, samt EOS-utvalget og Direktoratet for samfunnssikkerhet og beredskap (DSB). Disse organisasjonene har nøkkelroller innen forebyggende sikkerhet, og i EOS-utvalgets tilfelle, demokratisk kontroll med de som ivaretar rikets sikkerhet.

3.2 Forholdet mellom forebyggende sikkerhet og beredskap

Sikkerhet er et bredt begrep som beskriver en tilstand, og som favner mange forskjellige prosesser. Store endringsprosesser i det internasjonale samfunn over de senere år, medfører at dagens sikkerhetsbegrep er bredere enn noen gang og omfatter blant annet territoriell, økonomisk, sosial og politisk sikkerhet. Nasjonal sikkerhet skal ivaretas gjennom hele krisespekteret – fra fred via sikkerhetspolitiske kriser til krig/væpnet konflikt. Begrepet *nasjonal sikkerhet* er nærmere omtalt under kapittel 3.3.

Forebyggende sikkerhet er i rapporten Terrorsikring – en veiledning i sikrings- og beredskapstiltak, utgitt av Politidirektoratet, Politiets sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet i 2015, definert som:

> Tiltak som skal hindre eller redusere effekten av den uønskede handlingen. Disse gjennomføres før en uønsket handling finner sted, ideelt

[1] Forsvarsdepartementet og Justis- og beredskapsdepartementet, *Støtte og Samarbeid: en beskrivelse av totalforsvaret i dag* (Oslo: Forsvarsdepartementet, 2015).

> for å unngå handlingen i utgangspunktet. Dette er både menneskelige, teknologiske og organisatoriske tiltak.[2]

I sikkerhetsloven § 3 nr. 1 er *forebyggende sikkerhetstjeneste* definert som:

> Planlegging, tilrettelegging, gjennomføring og kontroll av forebyggende sikkerhetstiltak som søker å fjerne eller redusere risiko som følge av sikkerhetstruende virksomhet (spionasje, sabotasje og terrorhandlinger).[3]

Forebyggende sikkerhet deles tradisjonelt inn i organisatorisk sikkerhet, informasjonssikkerhet, objektsikkerhet og personellsikkerhet. De tre sistnevnte formene for sikkerhet korresponderer henholdsvis med sikkerhetsgradering av informasjon, fysisk sikring av objekter og sikkerhetsklarering av personell. I tillegg brukes ofte organisatorisk sikkerhet om sikkerhetsstyringen og rutinene internt i en virksomhet. Sikkerhetsloven regulerer alle disse aspektene ved forebyggende sikkerhet.

Enkelte regelverk som regulerer forebyggende sikkerhet er av sektorovergripende karakter. Den viktigste av disse er sikkerhetsloven. Loven gjelder i utgangspunktet for alle forvaltningsorganer, uavhengig av hvilken samfunnssektor de tilhører. Krav til forebyggende sikkerhet er også regulert i særlovgivning. I kraftsektoren er energiloven og beredskapsforskriften eksempler på sektorspesifikke regelverk.

Forebyggende sikkerhet må ses i sammenheng med samfunnets og den enkelte virksomhets beredskap. *Beredskap* er i Terrorsikring – en veiledning i sikrings- og beredskapstiltak definert som:

> Forberedt evne til på kort varsel å kunne øke sikkerhetsnivå, håndtere en uønsket hendelse eller tilstand, eller evne til å gjenopprette tilfredsstillende tilstand etter en uønsket hendelse. Beredskap forebygger ikke at en uønsket hendelse finner sted, men er en forberedelse til krisehåndtering.[4]

Forebyggende sikkerhet omfatter altså både tiltak som reduserer sannsynligheten for at en uønsket hendelse inntreffer og tiltak som reduserer skadevirkningene ved en slik hendelse. Beredskap omhandler på sin side, både planleggingen i forkant av en hendelse og selve håndteringen når en hendelse inntreffer eller er nært forestående. Beredskap omfatter også håndteringen av det etterfølgende gjenopprettingsarbeidet.

Forebyggende sikkerhet må videre avgrenses mot politiets ansvar for å forebygge kriminalitet og andre krenkelser av den offentlige orden og sikkerhet, jf. politiloven[5] § 2 nr. 2 og politiinstruksen[6] § 2-2 nr. 1. Denne type hendelser kan være alvorlige, men vil som hovedregel ikke true den nasjonale sikkerheten. Utover de defensive tiltakene er det Politiets sikkerhetstjeneste (PST) som har ansvaret for offensiv forebygging på norsk territorium.

Med offensiv forebygging menes blant annet PSTs særskilte ansvar for å forebygge og etterforske overtredelser av straffeloven kap. 17 om Vern av Norges selvstendighet og andre grunnleggende nasjonale interesser, overtredelser av sikkerhetsloven og ulovlig etterretningsvirksomhet, jf. politiloven § 17 b første ledd nr. 1 og 2. I medhold av politiloven § 17 d kan PST få tillatelse til å benytte nærmere angitte tvangsmidler, eksempelvis hemmelig ransaking og overvåkning, som ledd i sin forebyggende virksomhet.

I en normalsituasjon, altså før en hendelse inntreffer, vil forebyggende sikkerhet og beredskap, i noen grad overlappe hverandre. Eksempelvis vil det å øke sikkerhetsnivået, avhengig av det konkrete trusselnivået, inneha elementer av både forebyggende sikkerhet og beredskap. Et godt beredskapssystem er et viktig forebyggende sikkerhetstiltak. Beslutningen om å etablere et slikt system, eksempelvis gjennom en beredskapsplan, vil falle inn under begrepet forebyggende sikkerhet, mens den konkrete innretningen på systemet vil være en del av beredskapsarbeidet.

Grunnsikringstiltak iverksettes i en normalsituasjon for å oppnå et tilfredsstillende sikkerhetsnivå. De omfatter blant annet en kombinasjon av tiltak for å unngå at uønskede hendelser inntreffer (sannsynlighetsreduserende tiltak) og tiltak for å begrense skadeomfanget dersom hendelsen likevel skulle inntreffe (skadereduserende tiltak). Dette vil typisk være tiltak som er av en slik art at myndighetene ikke kan vente med å iverksette dem til det foreligger mer konkrete opplysninger

---

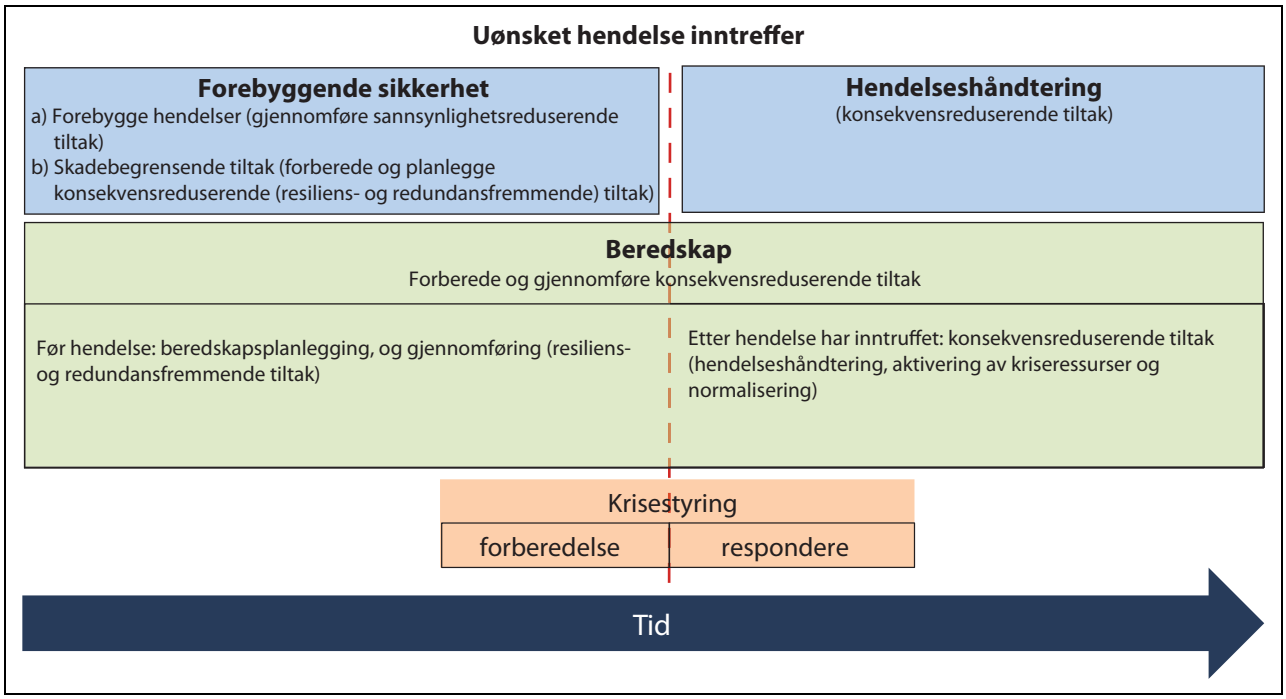
2 Nasjonal sikkerhetsmyndighet, Politidirektoratet og Politiets sikkerhetstjeneste, *Terrorsikring – En veiledning i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger* (2015), 9.

3 Lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven).

4 NSM, POD og PST, *Terrorsikring – En veiledning i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger* (2015), 9.

5 Lov 4. august 1995 nr. 53 om politiet (politiloven).

6 Instruks 22. juni 1990 nr. 3963 (politiinstruksen).



Figur 3.1 Samfunnssikkerhet og beredskap.

Sentrale begreper plassert i tid relativt i forhold til tidspunktet for en uønsket hendelse.

om at en trussel er overhengende. Andre tiltak kan følge på et senere tidspunkt. Dette kan karakteriseres som påbygningstiltak, som av forskjellige årsaker bør reserveres til taktisk tilpasning som ledd i et beredskapssystem.

Et eksempel på en slik taktisk tilpasning er regjeringens planverk og krisehåndteringsverktøy Nasjonalt beredskapssystem (NBS), som angir konkrete forhåndsplanlagte tiltak og handlemåter som kan iverksettes ved kongelig resolusjon, eller av den ansvarlige statsråd innen det aktuelle området. Formålet er å forebygge eller redusere skadeomfanget ved kriser. NBS ble innført i 2005 og er harmonisert med NATOs Crisis Response System (NCRS). NBS består av Sivilt beredskapssystem (SBS) og Beredskapssystemet for Forsvaret (BFF), som begge er hjemlet i beredskapsloven § 18, jf. § 3. (Se nærmere om beredskapsloven i kapittel 3.2.1). I tillegg kommer Politiets beredskapssystem (PBS), da politiet har en nøkkelrolle i sivil krisehåndtering.

At systemene er bygget opp over samme lest, og harmonisert med NATOs beredskapssystem, sikrer god kommunikasjon mellom sivil og militær side av Norges totalforsvar, og mellom Norge og NATO ved iverksetting av beredskapstiltak.

Noe av det viktigste forebyggende arbeidet staten gjør er å forhindre kriser fra å oppstå, eller begrense omfanget hvis krisen skulle inntreffe. Det forebyggende sikkerhets- og beredskapsarbeidet legger grunnlaget og føringer for Norges praktiske krisehåndtering. Det er helt avgjørende at det er god flyt mellom det som foregår før og etter en uønsket hendelse. Responsen må optimaliseres og læringspunktene fra evalueringen må inkorporeres i system og rutiner for å bedre beredskap og grunnsikring forut for neste hendelse. Figur 3.1 illustrerer noe av denne flyten, samt forholdet mellom forebyggende sikkerhet, krisehåndtering og beredskap.

Både forebyggende sikkerhet og beredskap, forutsetter kartlegging av verdier som skal beskyttes, aktuelle sårbarheter og hvilke trusler/uønskede hendelser som kan påvirke disse verdiene i negativ retning. Forut for en konkret hendelse vil det således være stor grad av overlapp mellom disse begrepene. Det må jobbes aktivt langs to spor der risikoen og sannsynligheten for at en uønsket hendelse inntreffer reduseres, samtidig som den beredskapen som søker å redusere konsekvensene i de tilfeller der uønskede hendelser inntreffer optimaliseres. Dette arbeidet styres både av beredskapslovgivning og sikkerhetslovgivning.

3.2.1 Beredskapslovgivningen

Beredskapslovgivning er vedtatt eller forberedt regelverk som grovt sagt trer i kraft dersom en sikkerhetspolitisk krise inntreffer, eller dersom Norge er i krig eller krig truer. Forebyggende sikkerhetstiltak, som beskrives i sikkerhetsloven med forskrifter og i annet relevant sektorovergripende eller sektorspesifikt regelverk, kan betegnes som defensive forebyggende tiltak eller sårbarhetsreduserende tiltak.

De ulike beredskapssystemene (SBS, BFF og PBS) er manualer som fordeler roller, ansvar og oppgaver. Disse systemene er ikke tilgjengelige for offentligheten i detalj, og deler av dem er sikkerhetsgradert. En nærmere omtale av dem her er følgelig verken mulig eller formålstjenlig. Beredskapslovutvalget definerte beredskapslovgivningen som:

> Vedtatt eller forberedt regelverk av lovgivningsmessig innhold, hvis iverksettelse er betinget av at riket er i krig, at krig truer riket, at rikets selvstendighet eller sikkerhet er i fare, eller at det foreligger en annen ekstraordinær krisesituasjon av militær art som truer vesentlige norske interesser.[7]

Definisjonen avgrenser både mot regelverk som gjelder beredskapsplanlegging i fredstid og mot regelverk som regulerer andre typer kriser enn sikkerhetspolitiske kriser. Ut fra ovennevnte definisjon identifiserte beredskapslovutvalget følgende beredskapslover:

- Drivstoffanleggloven[8]
- Beredskapsloven[9]
- Rekvisisjonsloven[10]
- Skipsrekvisisjonsloven[11]
- Forsyningsloven[12] (Opphevet)

I rapporten Støtte og samarbeid – en beskrivelse av totalforsvaret i dag[13] omtales, i tillegg til de lovene beredskapslovutvalget identifiserte, følgende lover som beredskapslover:

- Næringsberedskapsloven[14]
- Vernepliktsloven[15]
- Lov om beredskapslagring av petroleumsprodukt[16]
- Helseberedskapsloven[17]
- Sivilbeskyttelsesloven[18]

De sistnevnte lovene omhandler også beredskapsplanlegging i fredstid, og oppfyller således ikke beredskapslovsutvalget av 1995 sin definisjon av beredskapslover. Enkelte av lovene har fullmaktsbestemmelser, som først trer i kraft ved sikkerhetspolitisk krise eller krig. For denne utredningen er delene av lovene som omhandler normalsituasjonen forut for kriser mest relevant. Det er da forebyggende sikkerhetsarbeid nødvendigvis må finne sted.

3.3 Forebyggende nasjonal sikkerhet

Utvalgets mandat er å foreslå et nytt lovgrunnlag for «forebyggende nasjonal sikkerhet». Forebyggende nasjonal sikkerhet er ikke et legaldefinert begrep, og gjenfinnes heller ikke i gjeldende sikkerhetslov. Tradisjonelt har det vært et mer eller mindre skarpt skille mellom begrepene *statssikkerhet* og *samfunnssikkerhet.* Med statssikkerhet i snever forstand forstås gjerne ivaretakelse av statens eksistens, suverenitet og territorielle integritet:

> Statssikkerheten kan utfordres gjennom væpnet angrep, politisk og militært press mot politiske myndigheter og alvorlige anslag mot norske interesser fra statlige eller ikke-statlige aktører. Trusler mot statssikkerheten kan legitimere innsats av alle militære og andre ressurser.[19]

---

7 NOU 1995: 31, *Beredskapslovgivningen i lys av endrede forsvars- og sikkerhetspolitiske rammebetingelser*.

8 Lov 31. mars 1949 nr. 3 om bygging og sikring av drivstoffanlegg.

9 Lov 15. desember 1950 nr. 7 om særlige rådgjerder under krig, krigsfare og liknende forhold.

10 Lov 29. juni 1951 nr. 19 om militære rekvisisjoner.

11 Lov 19. desember 1952 nr. 2 om adgang til rekvisisjon av skip m.v. under krig eller kriseforhold.

12 Lov 14. desember 1956 nr. 7 om forsynings- og beredskapstiltak.

13 FD og JD *Støtte og samarbeid: en beskrivelse av totalforsvaret i dag*, (2015).

14 Lov 16. desember 2011 nr. 65 om næringsberedskap.

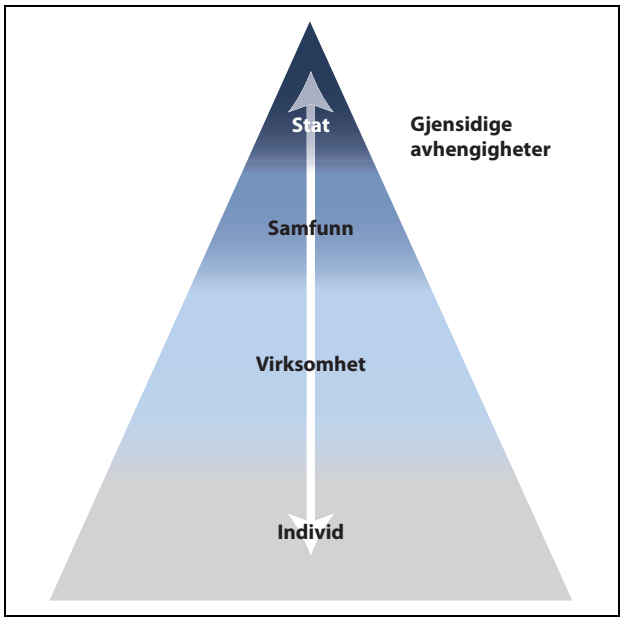
15 Lov 17. juli 1953 nr. 29 om verneplikt.

16 Lov 18. august 2006 nr. 61 om beredskapslagring av petroleumsprodukt.

17 Lov 23. juni 2000 nr. 56 om helsemessig og sosial beredskap.

18 Lov 25. juni 2010 nr. 45 om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret (sivilbeskyttelsesloven).

19 Ekspertgruppen for Forsvaret av Norge, *Et felles løft* (Oslo: Forsvarsdepartementet, 2015), 7.



Figur 3.2 Nivåer av sikkerhet.

Kilde: NSM, *Sikkerhetsfaglig råd*, 2015.

Begrepet samfunnssikkerhet er blant annet definert i Meld. St. 29 (2011–2012) Samfunnssikkerhet som:

> vern av samfunnet mot hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare. Slike hendelser kan være utløst av naturen, være et utslag av tekniske eller menneskelige feil eller av bevisste handlinger.[20]

I NSMs sikkerhetsfaglige råd beskrives samfunnssikkerhet som ivaretakelse av befolkningens liv, helse og trygghet, og sikring av sentrale samfunnsfunksjoner og viktig infrastruktur, og andre samfunnsmessige interesser mot skade.[21]

Figur 3.2 illustrerer at sikkerhet er viktig på fire ulike nivåer – stats-, samfunns-, virksomhets- og individsikkerhet, med gråsoner og overlappende områder mellom de enkelte kategoriene.

Utvalget anerkjenner og legger til grunn at begrepet forebyggende nasjonal sikkerhet, og de verdiene som skal beskyttes etter det nye lovgrunnlaget, innbefatter noe mer enn klassisk statssikkerhet. En endring av lovverket må reflektere at samfunnssikkerheten i økende grad er en viktig del av den forebyggende sikkerhet.

3.4 Ansvar, myndighet og krisehåndtering

Norges sikkerhetsorganisering er et resultat av politiske tradisjoner og en lang historisk utvikling. Den inkluderer noen av det norske samfunnets eldste institusjoner slik som fylkesmannsembetene og lensmannsetaten med røtter tilbake til 1100-tallet. Dette innebærer at organisasjonen og måten arbeidet er organisert på ikke alltid er et resultat av politiske valg som er tatt ut fra dagens kontekst. Strukturene og praksis oppstår også underveis, og ikke bare gjennom vedtatte reformer.

Sektorprinsippet er muligens det mest sentrale trekk ved den norske styringsmodellen, også innen sikkerhetsfeltet. Eivind Smith påpeker at sektorprinsippet med sitt ministerstyre ikke er en konstitusjonelt påkrevet styringsform, men snarere en sterk normativ føring for hvordan norske regjeringer velger å fordele kompetanse og arbeidsoppgaver.[22] Tydelige ansvarslinjer og tett kontakt til bakkenivået er andre sentrale trekk ved Norges sikkerhetsarkitektur. Dette kan sees som en form for villet desentralisering.

Sektorinndelingen forsterkes av den parlamentariske sedvane der statsråder svarer til Stortinget på vegne av sitt departement. Uttrykket «Stortinget kjenner bare statsråden» målbærer en markant sektorinndelt parlamentarisk praksis. Dette innebærer «at det er den enkelte statsråd alene, ikke regjeringskollegiet, som har ansvaret når noe går galt.»[23] Et annet viktig moment i den forbindelse er at Justis- og beredskapsdepartementet innehar en samordnende pådriverrolle for alt sikkerhetsarbeid som utøves i sivil sektor.

Blant fordelene med denne styringsformen er at den etablerer tydelige ansvarslinjer fordi det i de langt fleste saker vil fremkomme enighet om hvem som er den ansvarlige statsråd. Ulempen med systemet er at det hemmer overordnet tverrsektoriell tenkning og samordnende styring. Tidligere offentlige utredninger har ført til tiltak nettopp for å motvirke manglende samordning. I Meld. St. 29 (2011–2012) Samfunnssikkerhet ble *samvirke* lagt til som det fjerde prinsipp for krisehåndtering. De øvrige tre prinsippene for beredskap og krisehåndtering er som kjent *nærhet-, likhet- og ansvarsprinsippet* som beskrevet i boks 3.1.

[20] Meld. St. 29 (2011–2012), *Samfunnssikkerhet,* 9.

[21] Nasjonal sikkerhetsmyndighet, *Sikkerhetsfaglig råd*, 2015.

[22] Eivind Smith, «'Ministerstyre' - et hinder for samordning?», *Nytt Norsk Tidsskrift* 3 (2015).

[23] Ibid., 261.

Boks 3.1 Grunnleggende prinsipper for arbeidet med samfunnssikkerhet og beredskap

Beredskapsarbeidet bygger på fire grunnleggende prinsipper:

- *Ansvarsprinsippet* som innebærer at den organisasjon som har ansvar for et fagområde i en normalsituasjon, også har ansvaret for nødvendige beredskapsforberedelser og for å håndtere ekstraordinære hendelser på området.
- *Likhetsprinsippet* som betyr at den organisasjon man operer med under kriser i utgangspunktet skal være mest mulig lik den organisasjonen man har til daglig.
- *Nærhetsprinsippet* som betyr at kriser organisatorisk skal håndteres på lavest mulig nivå.
- *Samvirkeprinsippet* som betyr at myndigheter, virksomheter eller etater har et selvstendig ansvar for å sikre et best mulig samvirke med relevante aktører og virksomheter i arbeidet med forebygging, beredskap og krisehåndtering.

Prinsippene for beredskap og krisehåndtering legger føringer for hvordan sikkerhetsarbeidet utføres i Norge både i fred, krise og krig. Spesielt nærhetsprinsippet bidrar til en lav-nivå og desentralisert tilnærming innen norsk beredskap og krisehåndtering. Tankegangen i nærhetsprinsippet forsterkes også i det forebyggende sikkerhetsarbeidet gjennom ansvarsprinsippet og likhetsprinsippet. Det førstnevnte fastslår at den som har ansvaret for et felt i det daglige også har ansvaret når krisen inntreffer. Ansvarsprinsippet innebærer at alle grunnleggende samfunnsfunksjoner skal fortsette å operere som normalt og ha så lik drift og organisasjon som mulig i en krisesituasjon. Det vil imidlertid kunne være en rekke unntak fra disse prinsippene, for eksempel når et politidistrikt setter krisestab. Dette skal alltid være testet ut i øvelser før det settes ut i livet ved reelle hendelser.

Et annet viktig moment er at kriseressurser ikke må være bundet opp i daglig drift. Kriseressurser må nødvendigvis være tilgjengelige og gripbare i en krisesituasjon, uten at dette går på bekostning av andre kritiske samfunnsfunksjoner som er nødvendig for mest effektivt å løse krisen. Sykehusenes strømaggregater er et eksempel på en slik kriseressurs som ikke benyttes daglig, men kan være helt avgjørende for videre drift i en krisesituasjon med strømbrudd. Et illustrerende eksempel på feilbruk av kriseressurser ville være at brannbiler blir forringet som kriseressurs dersom de fjernes fra sentralt plasserte brannstasjoner og benyttes som lift-kapasitet andre steder.

Instruks for departementenes arbeid med samfunnssikkerhet og beredskap, Justis- og beredskapsdepartementets samordningsrolle, tilsynsfunksjon og sentral krisehåndtering (samordningsresolusjonen), gir nærmere regler for departementenes forebyggende sikkerhetsarbeid.[24]

Instruksen slår fast at det enkelte fagdepartement har ansvar for samfunnssikkerhet og beredskap innenfor egen sektor. Departementene har et ansvar for å samordne samfunnssikkerhets- og beredskapsarbeidet i egen sektor med det arbeidet som gjøres i andre departementer. Arbeidet med samfunnssikkerhet og beredskap skal være målrettet, systematisk og sporbart og være integrert i departementets planverk, styringssystemer og i styringsdialogen med underliggende virksomheter.

Hvert enkelt departement skal blant annet vurdere risiko, sårbarhet og robusthet i kritiske samfunnsfunksjoner i egen sektor som grunnlag for kontinuitets- og beredskapsplanlegging og hensiktsmessige øvelser. Det skal arbeides systematisk for å utvikle og vedlikeholde oversikten. Departementene skal videre vurdere og iverksette forebyggende og beredskapsmessige tiltak, og være forberedt på å håndtere alle typer kriser i egen sektor, samt yte bistand til andre departementer i kriser som involverer flere sektorer. Departementene skal også være forberedt på å kunne være lederdepartement.

For de sivile samfunnssektorene har Justis- og beredskapsdepartementet, i kraft av samordningsresolusjonen, en generell samordningsrolle for samfunnssikkerhet og beredskap. Departementet skal gjennom sin samordningsrolle sikre et koordinert og helhetlig arbeid med samfunnssikkerhet og beredskap på tvers av sektorgrenser.

Ordningen med lederdepartement ved kriser gjenspeiler og er forankret i sektor- og ansvarsprinsippet. Om ikke annet bestemmes er Justis- og beredskapsdepartementet ansvarlig for krisehåndteringen ved alle kriser innenlands i

[24] Instruks 16. juni 2012 nr. 535 om departementenes arbeid med samfunnssikkerhet og beredskap, Justis- og beredskapsdepartementets samordningsrolle, tilsynsfunksjon og sentral krisehåndtering.

fredstid. Dette er noe av bakgrunnen for at Krisestøtteenheten (KSE) formelt er lagt under Justis- og beredskapsdepartementet, selv om KSE også skal bistå andre departementer når Justis- og beredskapsdepartementet ikke er lederdepartement. Ved sikkerhetspolitiske kriser og væpnede konflikter har Forsvarsdepartementet ansvar for krisehåndteringen. Ved andre kriser enn de sikkerhetspolitiske og krig avgjøres hvem som er lederdepartement vanligvis i Regjeringens kriseråd, eventuelt av Regjeringens Sikkerhetsutvalg (RSU) og statsministeren selv i siste instans. Utenriksdepartementet har ansvar for å håndtere kriser som berører Norge utenlands og diplomatiske kriser mellom Norge og andre land. Den fatale terroraksjonen i In Amenas i 2013 er et eksempel på en krise der Utenriksdepartementet var lederdepartement.

I noen tilfeller vil sektorprinsippet og samvirkeprinsippet fremstå motstridende. Ett eksempel der sektorprinsipp og samvirke aktivt utfordres er ved såkalte hybridscenarier. Slike scenarier vil beskrives nærmere i kapittel 4.3.1 og er per definisjon designet for å vanskeliggjøre responsen, som delvis vil tilligge sivile sektorer og delvis militær sektor. Andre elementer av hybridkrig vil ikke nødvendigvis fordre noen respons, men være ren villeding og provokasjon. Ekspertgruppen for Forsvaret i 2015 konkluderte som følger:

> En ubestemmelig krise i gråsonen mellom krig og fred vil stille beslutningssystemet på alvorlige prøver. […] Ekspertgruppen vil fremheve behovet for å styrke samvirket med allierte i krise og krig og sette statsministeren og regjeringen bedre i stand til å lede krisearbeidet gjennom etableringen av en tilpasset enhet ved Statsministeren kontor.[25]

Statsministerens kontor (SMK) har hatt en tilbaketrukket rolle med tanke på krisehåndtering og sikkerhetsarbeidet sammenlignet med land det er naturlig å sammenligne Norge med, eksempelvis Det hvite hus i USA, det danske Statsministeriet og Storbritannias Cabinet Office. Embetsverket ved SMKs kanskje viktigste funksjon innen krisehåndtering er at regjeringsråden leder Regjeringens kriseråd. Videre huser SMK Regjeringens sikkerhetsutvalgs nyopprettede permanente sekretariat, som i noen grad kan betraktes som et konkret tiltak for å løse det beslutningsproblemet Ekspertgruppen for Forsvaret påpekte.

Uavhengig av hvilke tilpasninger som gjøres ved SMK, vil departementene med sine statsråder inneha et eksplisitt ansvar for det forebyggende sikkerhetsarbeidet innenfor sin sektor. Departementene og statsrådene med alle sine underliggende organer utgjør dermed bærebjelken i den norske sikkerhetsarkitekturen. Departementene har ansvar for å påse at det implementeres adekvate sikkerhetstiltak innenfor hele sin egen forvaltningssektor.

For å forstå det forebyggende sikkerhetsarbeidet i Norge må man derfor først ha innsikt i hvordan departementene styrer sine sektorer i tråd med sektorprinsippet. Skal man forstå samvirkeproblemene Norge opplever i sikkerhetsarbeidet er den sterke sektorstyringen en helt vesentlig faktor. Samtidig må man anerkjenne den tydelige vertikale styringslinjen sektorprinsippet etablerer. Figur 3.3 gir en generisk fremstilling av de vertikale styringslinjer fra storting til regjering og videre ned i det enkelte departement som igjen styrer underliggende direktorater og etater.

Stortinget er øverste lovgivende og bevilgende myndighet. De vedtar landets lover og statsbudsjettet. Den utøvende makt (regjeringen) og den dømmende makt (domstolene) må styre og dømme etter disse lovene.

Mye av arbeidet i Stortinget gjøres i komiteene. I komiteene kan partiene inngå forlik og tilkjennegi hvilke forslag og løsninger de ønsker å stemme for og imot. Dersom komitébehandlingen av en sak har vært god og konstruktiv vil ofte plenumsbehandlingen og utfallet av stemmegivningen nærmest være avklart på forhånd. Ett relevant og ferskt eksempel på dette er lovendringen av sikkerhetsloven i juni 2016. Etter forutgående behandling av i Utenriks- og forsvarskomiteen vedtok et enstemmig storting Innstilling 352 L (2015–2016).[26] Tilsvarende vil denne lovutredningen trolig etterfølges av et lovforslag som regjeringen ved Forsvarsdepartementet oversender Stortingets utenriks- og forsvarskomite.

Det går et markant skille mellom Stortinget og regjeringen. Regjeringen utgjør toppnivået i den utøvende sentralforvaltningen, og den styrer landet i det daglige. Ved maktskifter etter stortingsvalg ber Kongen statsministerkandidaten fra valgets vinnere om å danne en regjering. I statsråd vedtar regjeringen instrukser, kongelige resolusjoner og forskrifter. Disse er tilpasninger til lovverket vedtatt av Stortinget og styringsverktøy for

[25] Ekspertgruppen for Forsvaret av Norge, *Et felles løft,* 2015, 75.

[26] Innstilling 352 L (2015–2016), *Innstilling fra utenriks- og forsvarskomiteen om Endringer i sikkerhetsloven (reduksjon av antall klareringsmyndigheter mv.)*

Nivåer	Enheter og funksjoner	Møteform og arbeidsform
Parlamentsnivå	Stortinget	Plenumsdebatter, redegjørelser, vedtak spørretimer og votering
	Stortingskomite	Komitemøter, høringer, innstillinger og forarbeider
	Den utøvende sentralforvaltningen	
Regjeringsnivå	Regjeringen	Statsråd på slottet og Regjeringskonferanser
	Statsminister	Regjeringssjef. Utpeker ministre i statsråd
	Statsministerens kontor	Organiserer og gjennomfører statsråd og regjeringskonferanser
Departementsnivå Politisk	Statsråder (ministre)	Styrer departementene. Svarer i Stortinget på vegne av regjeringen og sitt departement.
	Politisk ledelse	Statsråden pluss statssekretærer og politiske rådgivere
Embetsnivå Administrativt	Departementsråd	Embetsverkets øverste leder i departementene
	Ekspedisjonssjefer	Leder avdelingene i departementene
Direktoratsnivå	Styres av direktører	Yter faglig støtte til departementene. Direktørene er også embetsmenn.

Figur 3.3 De vertikale styringslinjer fra storting til regjering, departement og direktorat.

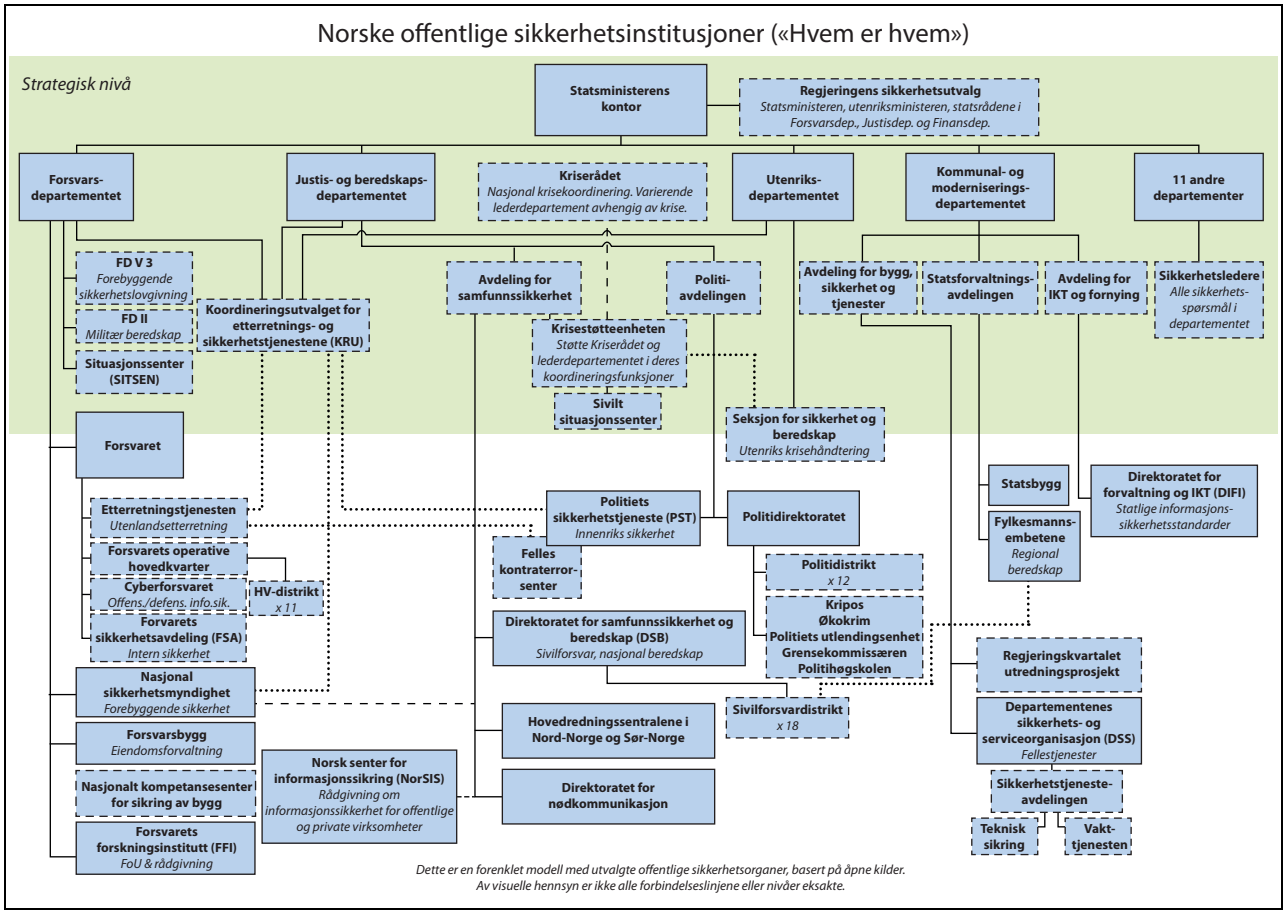
regjeringen. I tillegg utpekes departementenes politiske ledelse og embetsmenn i statsråd.

SMK er regjeringens sekretariat og organiserer statsråd. De tilrettelegger også for regjeringskonferanser, som er regjeringens øverste interne møter. Det er helt sentralt å få med seg at de konstitusjonelle styringslinjene ikke går via SMK. Det er den enkelte statsråd som har det konstitusjonelle ansvaret for sin sektor, og svarer for dette overfor regjeringskollegiet, statsministeren og ikke minst overfor Stortinget. Eivind Smith påpeker at dette er en valgt arbeidsform, og ikke et konstitusjonelt krav.[27]

Den enkelte statsråd styrer sitt departement ved hjelp av sin politiske ledelse og embetsverket. Den øverste leder for embetsverket er departementsråden som har det administrative ansvar internt i sitt departement. Under departementsråden finner man ekspedisjonssjefene som leder de ulike avdelingene i departementet med ulike faglige porteføljer. Ekspedisjonssjefene er i mange tilfeller etatsstyrere videre ut i forvaltningen mot underliggende direktorater. For eksempel går styringslinjen til Direktoratet for Samfunnssikkerhet og beredskap (DSB) gjennom samfunnssikkerhetsavdelingen i Justis- og beredskapsdepartementet, og styringen av politietaten går gjennom politiavdelingen. Det bør også nevnes at i vid forstand er hele departementet, fra topp til bunn, å regne som sekretariat for sin statsråd, og dermed en yttergrense for hva som kan benevnes som regjeringsapparatet.

Myndighet til å iverksette sikkerhetstiltak kan delegeres til underliggende etater, men ansvaret for å ivareta sikkerheten i egen sektor kan ikke et departement delegere seg bort ifra. Som eksempel har Justis- og beredskapsdepartementet delegert ansvar for implementering av forebyggende sikkerhet og samordning i sivil sektor til DSB i

[27] Eivind Smith, «'Ministerstyre' – et hinder for samordning?», 2015.



Figur 3.4 Norske offentlige sikkerhetsinstitusjoner.

Illustrasjon: Anders Grønli, spesialrådgiver Norges Bank, 2016.

Tønsberg. Delegeringen fra Justis- og beredskapsdepartementet til DSB innebærer ikke at departementet har mindre ansvar, kun at de bemyndiger DSB til å utføre et sett av departementets plikter i sitt sted, mens de opprettholder styringslinjen både administrativt og operativt gjennom samfunnssikkerhetsavdelingen i departementet. Et direktorat er normalt faglig rådgiver for sitt departement samtidig som det skal ivareta styringen av sitt fagområde på vegne av departementet.

Beveger vi oss fra den generelle styringen av sentralforvaltningen og til hvordan forebyggende sikkerhet faktisk utøves, blir bildet straks mer komplisert. En fullstendig skjematisk fremstilling av styrings- og ansvarslinjene, og de ulike etatene, på sikkerhetsfeltet i Norge er svært krevende å skissere. Figur 3.4 fanger opp mange sentrale aspekter ved styringen og sikkerhetsarbeidet i Norge på ulike nivåer.

Det er viktig å ikke glemme de vertikale styringslinjene gjennom departementene som er beskrevet i figur 3.3. Figur 3.4 er kompleks, men realiteten den beskriver og forenkler er som alltid enda mer kompleks. Det ligger blant annet store underliggende strukturer bak firkantene som symboliserer 11 HV-distrikter, 12 politidistrikter, 11 andre departementer og de 18 fylkesmannsembetene.

Figuren illustrerer hvor smalt toppnivået er og hvor bredt departementene favner. Den synliggjør også sektorprinsippet der styringslinjen ut til alle faglige og operative etater i figuren går gjennom departementene. Det er imidlertid ingen tvil om at det er på bakkenivå de fleste kriser håndteres og sikkerhetstiltak implementeres. Kommunene og fylkesmennene har sentrale roller i lokal krisehåndtering og grunnsikring av objekter. I tillegg finner man politidistriktene, sivilforsvarsdistriktene, helseregionene og hovedredningssentralene rundt dette nivået. Disse utgjør nøkkelkapasiteter i norsk beredskap. Det samme gjelder heimevernsdistriktene og Forsvarets operative avdelinger. Alle disse etatene hører hjemme i vertikale sektorer og styres av (minst) et departement.

Fylkesmannen står i den forbindelse i en særstilling, og utgjør et mellomnivå mellom kommune og stat. Embetet er et styringsmessig bindeledd mellom kommunene og sentrale statlige

myndigheter, med regionalt ansvar for at den nasjonale politikken gjennomføres. Fylkesmannen hører følgelig ikke hjemme i en enkelt sektor, men har et helhetlig ansvar på tvers av de ulike sektorer.

Fylkesmannsembetenes ansvarsområde på sikkerhets- og beredskapsfeltet, er forankret i Instruks for Fylkesmannens beredskapsarbeid.[28] Fylkesmannen skal samordne samfunnssikkerhets- og beredskapsarbeidet i fylket og ivareta en rolle som pådriver og veileder i arbeidet med samfunnssikkerhet og beredskap. I dette ansvaret ligger blant annet en plikt til å ha oversikt over risiko- og sårbarhet i fylket, holde sentrale myndigheter og regionale samarbeidende etater orientert om situasjonen i fylket, samt samordne den fylkesvise planleggingen og kontakten innenfor totalforsvaret. Totalforsvaret er nærmere beskrevet i kapittel 3.5. Videre har fylkesmannen også et samordnende ansvar for regional krisehåndtering. Ansvaret strekker seg helt ned på kommunenivå, ettersom Fylkesmannen skal føre tilsyn med kommunenes beredskapsarbeid, jf. forskrift om kommunal beredskapsplikt § 10.[29]

Forsvaret styres av forsvarssjefen som har delegert myndighet fra forsvarsministeren. Sivil kontroll med det militære er et nøkkelprinsipp for liberale demokratier, og er en forutsetning for NATO-medlemskap. Forsvarssjefen styrer Forsvaret via forsvarsstaben. Videre har forsvarssjefen en ledergruppe med lederne for 21 driftsenheter. Blant de viktigste og mest relevante for vårt formål, er grensjefene for Luftforsvaret, Sjøforsvaret og Hæren, samt sjefene for Heimevernet, E-tjenesten og Forsvarets spesialstyrker.

Alle militære operasjoner styres av Forsvarets operative hovedkvarter lokalisert på Reitan ved Bodø. I den grad Forsvarsdepartementet skal involveres i avgjørelser om pågående militære operasjoner fasiliteres dette gjennom Forsvarsdepartementets situasjonssenter (SITSEN). Ved situasjoner i hele krisespekteret til sjøs, vil Kystvakten involveres. Fremfor alt er deres rolle i søk og redning en kritisk kapasitet i Norges beredskap.

Der Forsvaret er strengt hierarkisk og sentralisert, er styringen av norsk politi mer desentralisert. Det er liten tvil om at Justis- og beredskapsdepartementet har sektoransvaret og kan instruere hele politi-Norge. Politiavdelingen er deres viktigste instrument for styring av politietaten. Imidlertid har politimestrene i Norge større grad av autonomi enn sjefene i Forsvaret. Der militærmakten alltid må være under streng politisk kontroll, både militært og politisk, står politidistriktene mer fritt til å løse de mange daglige oppdrag som tilkommer dem. Det finnes også en mulighet for at Politidirektoratet (POD) overtar en pågående politioperasjon fra et politidistrikt, men dette er foreløpig nærmest uprøvd terreng i praksis. Imidlertid er POD involvert når man flytter politioppdrag fra ett politidistrikt til et annet.

En utfordring siden opprettelsen i 2001 har vært PODs rolle opp mot Justis- og beredskapsdepartementets politiske departementsstyring og politimestrenes fullmakter til å gjennomføre den daglige tjeneste. POD representerer et samordnende ledd i sentralforvaltningen og dette har tidvis utfordret nærhetsprinsippet ned mot de lokale politidistriktene. POD har utvilsomt en viktig rolle innenfor akutt terrorbekjempelse på nasjonalt nivå, noe som ble tydelig illustrert under det som ofte kalles Operasjon sommer, da etterretningsrapporter i juli 2014 indikerte at ISIL-krigere var på vei til Norge for å gjennomføre et terrorangrep.

POD har også en sentral rolle i de tilfeller politiet fremmer bistandsanmodninger til Forsvaret. Det er etablert en omstendelig beslutningssløyfe der en anmodning til Forsvaret om bistand går fra politimesteren som ber om bistand via POD til Justis- og beredskapsdepartementet, før den går videre til Forsvarsdepartementet og Forsvarets ledelse. Selv om det ble innført nye hurtigprosedyrer med ny bistandsinstruks i 2012 (revidert i 2015), innebærer denne prosedyren fremdeles hele seks til åtte beslutningspunkter. I januar 2016 nedsatte regjeringen en egen arbeidsgruppe for å foreta en full gjennomgang av hele bistandsspørsmålet i lys av det nye lovgrunnlaget for militær bistand i fredstid som ble tatt inn i politiloven § 27 a i 2015. Denne gruppen anbefaler en kraftig forenkling og avbyråkratisering, blant annet gjennom å gi et langt større handlingsrom til de operative delene av politi og forsvar. Som en del av dette er prosedyren for anmodning om bistand anbefalt redusert til kun to beslutningspunkter: den anmodende politimesteren og Forsvarets operative hovedkvarter, men da innenfor rammen av § 27 a ved at politimesteren har en varslingsplikt til høyere myndigheter ved igangsetting av en bistandsoperasjon, slik at høyere myndigheter kan stanse operasjonen hvis de finner grunn til det.[30]

---

[28] Instruks 18. april 2008 nr. 388 for samfunnssikkerhets- og beredskapsarbeidet til Fylkesmannen og Sysselmannen på Svalbard.

[29] Forskrift 22. august 2011 nr. 894 om kommunal beredskapsplikt.

[30] Rapport fra arbeidsgruppen for utarbeiding av forslag til ny instruks for Forsvarets bistand til politiet, 2016, 51–53.

Figur 3.5 Sivilt-militært samarbeid og totalforsvaret.

Kilde: Sjef Forsvarsstaben, generalløytnant Erik Gustavson, presentasjon under Nødnettdagene i Trondheim, «Sivil-militært samarbeid», 19.04.2016, http://www.dinkom.no/PageFiles/14686/02_Erik_Gustavson.pdf

3.5 Totalforsvaret

Dagens totalforsvar omfatter samfunnets støtte til Forsvaret og Forsvarets støtte til det sivile samfunn. Totalforsvarstanken stammer fra den norske eksilregjeringen i London under andre verdenskrig, med invasjonstrusselen som bakteppe. Forsvarskommisjonen slo i 1949 fast at Forsvaret måtte styrkes ved å stille samfunnets ressurser i fredstid til disposisjon for Forsvarets håndtering av sikkerhetsutfordringer.[31] Tanken var at samfunnets samlede ressurser, inkludert private ressurser, skulle kunne settes inn for å støtte forsvaret av Norge.

Totalforsvarskonseptet har siden den tid blitt videreutviklet for å møte nye utfordringer og trusler. En naturlig konsekvens av det moderniserte totalforsvarskonseptet er økt fokus på Forsvarets rolle som bidragsyter til det sivile samfunn i håndtering av samfunnssikkerhetsutfordringer, i tillegg til det siviles forpliktelse til å støtte Forsvaret i krisesituasjoner.[32] Dette er avgjørende både for samfunns- og statssikkerheten.

I Langtidsplanen for forsvarsektoren beskrives det moderne totalforsvaret som et konsept med fleksibilitet og som optimaliserer sikkerhets- og beredskapseffekten av samfunnets samlede ressurser.

> Totalforsvarskonseptet gir vide rammer for det sivil-militære samarbeidet. Det gir nødvendig fleksibilitet ved at sivile og militære ressurser kan nyttes for å løse utfordringer både mot samfunns- og statssikkerhet.[33]

Dette skiller seg fra det tradisjonelle totalforsvarskonseptet som var ensidig innrettet mot å kraftsamle samfunnets ressurser for å stå imot en invasjonstrussel.

Figur 3.5 viser at det sivil-militære samarbeidet omfatter mer enn totalforsvarskonseptet. Den viser relasjonen mellom Forsvarets bistand til det sivile samfunn og det sivile samfunns støtte til Forsvaret gjennom hele spekteret, fra fred via sikkerhetspolitisk krise til væpnet konflikt.

Privatisering og samfunnets raske teknologiske utvikling har ført til at skillelinjene mellom Forsvaret og det sivile samfunn blir stadig mindre, og at den gjensidige avhengigheten øker. Komplekse systemer og eierskapsforhold fører med seg nye sårbarheter, og aktualiserer behovet for samarbeid i totalforsvaret i tiden fremover. Dagens forsvar er avhengig av sivil understøttelse i form av kompetanse, varer, logistikk, tjenester og infrastruktur for å opprettholde forsvarsevne og kunne ta imot alliert støtte. Strømforsyning, elektronisk kommunikasjon og satellittbaserte tjenester er innsatsfaktorer som kan være av kritisk betydning for Forsvarets operative evne.

[31] Forsvarskommisjonen av 1949, del 1, 64.
[32] FD/JD, *Støtte og samarbeid*, 2015, 12.
[33] Prop. 151 S (2015–2016), Kampkraft og bærekraft. Langtidsplan for forsvarssektoren, 45.

Et hovedmoment i det moderniserte totalforsvarskonseptet er å sikre best mulig utnyttelse av de begrensede ressurser samfunnet besitter. Den sivile støtte til Forsvaret er blant annet hjemlet i rekvisisjonsloven som slår fast de militære myndigheters mulighet til å «rekvirere alt som er nødvendig for krigsmakten og institusjoner som er knyttet til den», med unntak av eiendomsrett til fast eiendom.[34] Loven kan benyttes i krigstid, og i fredstid når krigsmakten bistår i beredskapssituasjoner og når det er nødvendig å iverksette beredskapstiltak (for eksempel under større øvelser).

Som et supplement til rekvisisjonsmuligheten har Forsvaret tegnet en rekke avtaler med direktorater, etater og kommersielle virksomheter. Det ble i 2015 utarbeidet retningslinjer for Forsvarets overtakelse av en rekke sivile tjenester i krise og krig, blant annet redningstjenesten, lostjenester og metrologiske tjenester. Av kommersielle avtaler er særlig avtalen mellom Wilhelmsen-gruppen og Forsvaret fra 2015 viktig. Avtalen forplikter rederiet til transport av materiell og personell i en potensiell krisesituasjon. Også Telenor har en samarbeidsavtale med Cyberforsvaret om utvikling av kompetanse, deling av informasjon om uønskede hendelser og felles trening.

Endringer i trussel- og risikobildet har også bidratt til å endre relasjonen mellom det sivile og det militæret. Terrorhandlingene 22. juli 2011 synliggjorde i all sin grusomhet behovet for å ha et forsvar som er klar til å yte bistand til det sivile på kort varsel. Blant de viktigste forebyggende sikkerhetskapasiteter Forsvaret kan tilby er utplassering av sikringsstyrker, blant annet fra Heimevernet og HMK Garden.[35]

Innsatsstyrke Derby fra HV-02 besørget vakthold rundt nøkkelobjekter som Stortinget i timene og dagene etter 22. juli. HMK Garden kalte også inn alt av tilgjengelige mannskaper og var blant de tidligst gripbare sikringsstyrkene etter 22. juli-angrepene, samt bidro med forsterket vakthold 23. juli. Garden var i tillegg de første som formelt varslet internt i Forsvaret om at en eksplosjon hadde funnet sted.[36]

Denne typen militær bistand rokker ikke ved arbeidsdelingen der Forsvarets primæroppgave er å hevde Norges suverenitet, mens de sivile myndigheter ivaretar samfunnssikkerheten. Forsvarets bistand til det sivile samfunn skal være et supplement til den sivile krisehåndteringen, i de situasjoner der det sivile samfunn mangler ressurser som Forsvaret besitter, og i den grad støtte er forenlig med Forsvarets primæroppgaver.[37] Forsvarets spesialstyrker bestående av Forsvarets spesialkommando (FSK) på Østlandet og Marinejegerkommandoen (MJK) i Nord-Norge og Bergen er spesielt relevante for bistand i tilfelle terroranslag.

Forsvarets helikoptre på Rygge og Bardufoss er også i konstant beredskap for å kunne bistå politiet. FSK, MJK og Forsvarets helikopter har alle dedikerte beredskapsoppgaver som gjør at organiseringen av disse ressursene delvis er tilpasset politiets behov for bistand.[38] Forsvaret kan også bistå politiet i objektsikring. Forsvarets bistand til politiet er hjemlet i Instruks om Forsvarets bistand til politiet (bistandsinstruksen).[39] I kjølvannet av 22. juli utga regjeringen en ny bistandsinstruks med raskere prosedyrer, se for øvrig kapittel 3.4.

Bistandsinstruksen fastslår i hvilke situasjoner politiet kan anmode Forsvaret om bistand, og gir retningslinjer for utøvelsen av bistanden. I en situasjon der Forsvaret skal yte bistand til politiet er det politimesteren i det aktuelle politidistriktet som er ansvarlig for ledelsen av operasjonen, og politiets og Forsvarets enheter blandes ikke under operasjonen. Forsvaret kan naturligvis også bistå ved rent sivile nasjonale kriser og katastrofer i fredstid, slik som under storflommen på Østlandet i 1995.

Det finnes to ulike typer bistand; håndhevelsesbistand og alminnelig bistand. Håndhevelsesbistand gjelder bistand knyttet til ettersøking og pågripelse av farlige personer, hvor liv og helse står på spill og i tilfeller der det er fare for omfattende anslag mot sentrale samfunnsinteresser, samt forebyggelse og bekjempelse av slike. Anmodning om håndhevelsesbistand krever politisk klarering. Den aktuelle politimesteren må rette anmodningen om behov for bistand fra Forsvaret via Politidirektoratet til Justis og beredskapsdepartementet, som eventuelt sender anmodning til Forsvarsdepartementet for avklaring.

Alminnelig bistand gjelder bistand i forbindelse med ulykker, naturkatastrofer eller lignende situasjoner. Også bruk av tilgjengelige ressurser

---

34 Lov 29. juni 1951 nr. 19 om militære rekvisisjoner.

35 FD/JD, *Støtte og samarbeid*, 2015, 51.

36 André Berg Thomstad, *Arbeidet mellom Forsvaret og politiet lokalt i Oslo er blitt bedre etter terrorangrepet på Oslo 22. juli*. Oslo Files on Defence and Security, nr. 1 (Oslo: Institutt for forsvarsstudier, 2016), 19–27.

37 FD/JD, *Støtte og samarbeid* 2015, 15.

38 Ibid., 6, 51.

39 Instruks 22. juni 2012 om Forsvarets bistand til politiet (bistandsinstruksen).

som materiell, transport, innkvartering i Forsvarets militærleirer og personell, som ikke direkte involveres i den operative politiaksjonen, regnes som alminnelig bistand. I slike situasjoner henvender vedkommende politimester seg direkte til Forsvarets operative hovedkvarter. I tilfeller der alminnelig bistand er svært omfattende, setter sikkerheten til Forsvarets ansatte i fare, eller fører med seg politiske eller prinsipielle problemstillinger trengs politisk klarering. I disse tilfeller benyttes prosedyren for håndhevelsesbistand. Både sivil og militær side er forpliktet til å opprette kontakt så fort som mulig i situasjoner der det kan bli behov for bistand for å sikre at responstiden blir så kort som mulig.

3.6 EOS-tjenestene, EOS-utvalget og DSB

Etterretnings-, overvåkings- og sikkerhetstjenestene (EOS-tjenestene) består av Etterretningstjenesten (E-tjenesten), Politiets sikkerhetstjeneste (PST), Nasjonal sikkerhetsmyndighet (NSM) og Forsvarets sikkerhetsavdeling (FSA). EOS-tjenestene skal ivareta nasjonale sikkerhetsinteresser, og er underlagt tilsyn av EOS-utvalget som skal påse at borgernes rettigheter ivaretas i disse tjenestenes svært viktige sikkerhetsarbeid. E-tjenesten, PST og NSM omtales som de «hemmelige tjenester» grunnet deres eksklusive myndighet og oppgaver. FSA regnes ikke blant de «hemmelige tjenestene» men benevnes som en EOS-tjeneste underlagt tilsyn fra EOS-utvalget, på lik linje med E-tjenesten, PST og NSM. Direktoratet for samfunnssikkerhet og beredskap (DSB) beskrives også i dette underkapittelet. DSB har en nøkkelrolle innenfor samfunnssikkerhet, spesielt hva angår uønskede hendelser som ikke er intendert, og fremfor alt storulykker.

Mange av de forutgående strukturene for EOS-tjenestene vokste fram etter andre verdenskrig, og rundt opprettelsen av NATO. Norge hadde et økende behov for hemmelighold og utveksling av gradert informasjon internt og med NATO-land i denne perioden. Med utgangspunkt i militær sektor ble systemer for grunnleggende forebyggende sikkerhet, og organisering av arbeidet, utviklet i denne perioden.

> Det stigende behovet for hemmelighold og egensikring økte altså i takt med utvidelsene av forsvarssektoren, noe som måtte få organisatoriske følger. Ved alle militære enheter skulle ledelsen i fred som i krig støtte seg på egne sikkerhetsoffiserer for å samordne tiltakene mot spionasje, sabotasje og illojale menige eller befal.[40]

Blant strukturene som begynte å ta form og finne sin funksjon etter krigen var Politiets overvåkningstjeneste (forløper til PST) og sikkerhetsavdelingen ved Forsvarets Overkommando. Sistnevnte var en forløper til Sikkerhetsstaben (FO/S), som senere ble etterfulgt av FSA og NSM. E-tjenestens forløpere befant seg i FO II, Etterretningskontoret.[41]

E-tjenesten er i dag Norges militære og sivile utenlands-etterretningstjeneste. E-tjenesten er en del av Forsvaret, underlagt forsvarsjefen, men løser oppgaver for hele myndighetsapparatet. Oppdrag utenfor forsvarssektoren formidles via Forsvarsdepartementet. E-tjenestens arbeidsoppgaver er hjemlet i etterretningstjenesteloven og inkluderer å innhente, bearbeide og analysere informasjon som angår norske interesser, sett i forhold til fremmede stater, organisasjoner eller individer.[42] Russland og nordområdene står sentralt i tjenestens arbeid, i tillegg til utviklingen i det internasjonale trusselbildet. Disse temaene vies stor oppmerksomhet også i E-tjenestens årlige åpne trusselvurderinger.

Gjennom innhenting av informasjon og produksjon av trusselanalyser legger E-tjenesten til rette for at myndighetene skal ha et best mulig beslutningsgrunnlag vedrørende utenriks-, sikkerhets- og forsvarspolitiske forhold. E-tjenesten skal også bistå Forsvaret i operasjoner internasjonalt og nasjonalt, og har et koordinerende og rådgivende ansvar for etterretningsvirksomhet i Forsvaret. I tillegg står støtte til bekjempelse av terrorisme og arbeid mot spredning av masseødeleggelsesvåpen sentralt.

E-tjenesten innhenter informasjon fra kilder både ved hjelp av tekniske og menneskebaserte metoder. Tjenesten skal varsle om forhold som kan true Norge og norske interesser. Denne oppgaven blir stadig mer krevende i en tid der et økende antall utfordringer er grenseoverskridende, for eksempel trusler i det i digitale rom og internasjonal terrorisme. Interessebegrepet som legges til grunn er ikke statisk, og Evalueringsutvalget for EOS-utvalget henviser til E-instruksens § 7 og slår fast at «hva som anses som "viktige

---

[40] Synstnes, Hans Morten, *Den innerste sirkel: Den militære sikkerhetstjenesten 1945–2002* (Oslo: Universitetet i Oslo, 2015) 69–70.

[41] Ibid.

[42] Lov 20. mars 1998 om Etterretningstjenesten.

nasjonale interesser" avhenger av hvilke sikkerhetsutfordringer Norge til enhver tid står overfor».[43]

PST er den nasjonale sikkerhetstjenesten, organisert som et særskilt organ direkte underlagt Justis- og beredskapsdepartementet. PSTs oppgaver er hjemlet i politiloven.[44] Der gis PST et spesifikt ansvar for å beskytte mot de tre overordnede aktivitetene sikkerhetsloven skal motvirke: ulovlig etterretning, sabotasje og politisk motivert vold, slik som terrorisme. PST er organisert med Den sentrale enhet (DSE) lokalisert i Nydalen i Oslo. I tillegg er det mindre desentraliserte enheter ute i politidistriktene, med unntak av Oslo som ivaretas av DSE.[45]

Kjerneoppgaven til PST er å forebygge og etterforske lovbrudd av relevans for nasjonens sikkerhet og selvstendighet. Herunder ligger ansvar for å innhente informasjon om, forebygge og etterforske terrorhandlinger og annen ekstremisme, ulovlig etterretningsvirksomhet mot Norge og norske interesser, ulovlig teknologioverføring, spredning av masseødeleggelsesvåpen, sabotasje og politisk motivert vold. PST har også ansvar for å forebygge og etterforske trusler mot statsledelsen og andre myndighetspersoner, samt utføre livvakttjeneste. Innsamling av informasjon, om personer og grupper som kan utgjøre en trussel, står sentralt i PSTs arbeid.

PST skal utarbeide periodiske trusselvurderinger, og vil også kunne gi oppdaterte trusselvurderinger rundt skjellsettende enkelthendelser, for eksempel ved raske endringer i trusselbildet. PST har også i spesielle tilfeller anledning til å benytte skjulte tvangsmidler til informasjonsinnhenting. Dette innebærer blant annet ransakinger, avlytting og skjult fjernsynsovervåking.[46]

Skillet mellom PSTs ansvar for rikets sikkerhet innenfor landets grenser, og Etterretningstjenesten tilsvarende ansvar utenfor Norges grenser er mindre klart i dag hvor trusselbildet i økende grad er grenseoverskridende. En ny samarbeidsinstruks for E-tjenesten og PST ble vedtatt i 2006 med det formål å fremme samarbeidet mellom tjenestene på områder av felles interesse.[47]

Terrorisme, spredning av masseødeleggelsesvåpen og fremmed etterretningsvirksomhet er områder der det er særlig viktig å samarbeide gjennom informasjonsutveksling og samhandling. Samarbeidet mellom PST og E-tjenesten følger fastlagte rutiner, og er underlagt tilsyn. Blant de viktigste institusjonene og tiltakene for å ivareta et godt mellomtjenstlig samarbeid er Felles kontraterrorsenter (FKTS) lokalisert ved DSE i Nydalen med ansatte fra begge tjenester. Senteret er en videreutvikling av Felles analyseenhet som ble opprettet i 2007, og var et konkret tiltak for å bedre kontraterror og beredskapen etter 22. juli.[48]

I Kronprinsregent resolusjon av 4. juli 2003 står det at Nasjonal sikkerhetsmyndighet (NSM) skal på Justisministerens og Forsvarsministerens vegne ivareta de utøvende funksjoner for den forebyggende sikkerhetstjeneste.[49] Videre er NSM Norges ekspertorgan for informasjons- og objektsikkerhet og fagmiljø for IKT-sikkerhet. NSM er et direktorat med tverrsektorielt mandat, administrativt underlagt Forsvarsdepartementet. Justis- og beredskapsdepartementet har instruksjonsmyndighet overfor NSM i saker innenfor departementets ansvarsområde. NSMs oppgaver og ansvar er også regulert i en egen instruks av 2. desember 2014 fra Forsvarsdepartementet til direktør NSM.[50]

Rådgiving står sentralt i NSMs rolle som ekspertorgan og koordineringsinstans for sikkerhetstiltak. Samtidig har NSM en tilsynsrolle med ansvar for å kontrollere sikkerhetstilstanden i de virksomheter som omfattes av sikkerhetsloven. NSM har fag- og kontrollansvar for personellsikkerhetstjenesten etter sikkerhetsloven. De skal også kontrollere og veilede kryptosikkerhetstjenesten. Dette innebærer ansvar for forvaltning av både nasjonalt og NATO kryptomateriell. Korrumpering av kryptomateriell kan ha enorme skadevirkninger.

En vesentlig del av NSMs arbeid omhandler sikkerhet i graderte informasjonssystemer. Direktoratet har ansvar for å varsle om og legge til rette for håndtering av alvorlige dataangrep mot Norge. Dette ivaretas hovedsakelig av NorCERT som er en del av NSM og fungerer som nasjonal varslings- og koordineringsinstans for alvorlige dataangrep og andre IKT-sikkerhetshendelser. NorCERT drifter også VDI (varslingssystem for digital infrastruktur). Deltakelse i VDI er en tjeneste

43 Dokument 16, (2015–2016), 67.

44 Lov 4. august 2005 om politiet (politiloven), § 17 b.

45 Dokument 16, (2015–2016), 63.

46 Ibid.

47 Kgl. res 13. oktober 2006 om samarbeidet mellom Etterretningstjenesten og Politiets sikkerhetstjeneste.

48 Dokument 16, (2015–2016), 76.

49 Kronprinsreg.res. 4. juli 2003, Fordeling av ansvar for forebyggende sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet.

50 Dokument 16, (2015–2016), 72.

utvalgte og utsatte private virksomheter kan få tilbud om å kjøpe, noe de gjør i betydelig grad.

Som et relativt nyopprettet tverrsektorielt direktorat utfordres NSMs rolle og status tidvis av andre aktører på sikkerhetsfeltet. Utpeking av skjermingsverdige objekter har vist seg å bli en krevende prosess for NSM, og tjenesten fremstår ikke tilfreds med resultatene av utpekingen. Slik utpeking styres i dag av det enkelte departement i tråd med sektorprinsippet, selv om NSM er gitt ansvar for å ivareta helheten og holde oversikt over kritiske nøkkelpunkter. Stortinget anerkjenner utfordringene i utpekingsarbeidet og konkluderer at «[i]nnenfor objektsikkerhetsområdet er det også avdekket uenighet mellom ulike sektorer om hva reglene skal ta sikte på å beskytte mot, og på hvilken måte».[51] Problemene rundt utpeking av objekter står i kontrast til den suksess NSM har hatt med å utvikle NorCERT og VDI. For en nærmere omtale av NSMs oppgaver vises det til kapittel 7.

Forsvaret har også en dedikert egen enhet som skal ivareta forebyggende sikkerhetstjeneste i Forsvaret. FSA er en del av forsvarsstrukturen og er administrativt direkte underlagt Forsvarsstaben. Avdelingen skal være en sentral stabsfunksjon for forebyggende sikkerhetstjeneste i Forsvaret. I tillegg sikkerhetsklarerer FSA tusenvis i Forsvaret årlig, og er med dette Norges største klareringsorgan i omfang. FSA skal «motvirke sikkerhetstruende virksomhet mot Forsvaret, for eksempel ulovlig etterretning, sabotasje og terrorhandlinger».[52]

FSA skal kun operere innenfor Forsvaret, men har ansvar for militær kontraetterretning ved og på militært område. I de tilfeller FSA avdekker mistanke om ulovlig etterretningsvirksomhet, sabotasje eller lignende, plikter FSA å informere PST.

FSA representerer forsvarssjefen internasjonalt overfor NATO og samarbeidende sikkerhetstjenester, samt nasjonalt overfor PST og NSM. FSA skal også holde seg orientert om «det sikkerhetsmessige risikobilde som omgir Forsvaret og norsk militær aktivitet både hjemme og ute».[53] Blant FSAs viktigste styringsdokumenter er Instruks om sikkerhetstjeneste i Forsvaret av 29. april 2010. Det understrekes i instruksens § 1 at «[i]nstruksen medfører ingen endringer i forholdet mellom NSM og Forsvarets virksomhet innen forebyggende sikkerhetstjeneste.»[54]

EOS-utvalget er et permanent kontrollutvalg underlagt Stortinget med ansvar for å kontrollere etterretnings-, overvåkings- og sikkerhetstjeneste som har til formål å ivareta nasjonale sikkerhetsinteresser. Tjenestenes andre formål slik som politiets alminnelige kriminalitetsetterretning omfattes ikke av kontrollmandatet. EOS-tjenestene som EOS-utvalget per i dag fører jevnlig kontroll med inkluderer E-tjenesten, PST, NSM og FSA.

EOS-tjenestene skal beskytte borgere og samfunnet fra trusler mot rikets sikkerhet, samtidig som de skal sikre at borgernes personlige rettigheter ivaretas i prosessen. EOS-utvalget er ansvarlig for å kartlegge om og forebygge at det øves urett, at tjenestene ikke benytter mer inngripende midler enn det som er nødvendig etter forholdene, samt å påse at tjenestene respekterer menneskerettighetene.[55] EOS-utvalgets mandat omfatter ikke personer som ikke er bosatt i Norge eller organisasjoner som ikke har tilhold i landet. Unntak gjøres også for utenlandske borgere som har opphold knyttet til tjeneste for fremmede stater, slik som diplomatisk personell.

EOS-utvalget består av syv medlemmer med en bredt sammensatt bakgrunn og blir valgt av Stortinget i plenum etter innstilling fra Stortingets presidentskap. Stortingsrepresentanter kan ikke sitte i utvalget samtidig som de sitter på Stortinget. EOS-utvalget har ingen instruksjonsmyndighet ovenfor tjenestene, men rapporterer og gir råd til Stortinget gjennom årsmeldinger. EOS-utvalgets parlamentariske forankring anses som en styrke, og har fått annerkjennelse internasjonalt.

Et evalueringsutvalg ble oppnevnt i mars 2015 for å vurdere hvordan EOS-utvalget har ivaretatt sine oppgaver, og hvordan dette bør gjøres videre. Evalueringsutvalget avla sin rapport 29. februar 2016. Utredningsutvalget har påpekt at EOS-utvalget har gjort en god jobb og har oppfylt intensjonen som lå bak etableringen i 1996.[56] Evalueringsutvalget fant også at EOS-utvalget har opparbeidet seg både allmenn respekt og respekt og tillit hos tjenestene. Blant de viktigste forslagene relatert til sikkerhetsloven er at sikkerhetsklareringssaker foreslås tatt ut av EOS-utvalgets kontrollområde, og at Hærens Etterretningsbataljon og Forsvarets spesialstyrker underlegges regelmessig og obligatorisk kontroll av EOS-utvalget.[57]

---

51 Innstilling 352 L (2015–2016).

52 Dokument 16, (2015–2016), 74.

53 Ibid.

54 Instruks 29. april 2010 om sikkerhetstjeneste i Forsvaret.

55 Lov 3. februar 1995 om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-kontrolloven), § 2.

56 Dokument 16 (2015–2016).

57 Ibid., 132–146.

Direktoratet for samfunnssikkerhet og beredskap (DSB) understøtter Justis- og beredskapsdepartementets koordinerings- og samordningsrolle innenfor samfunnssikkerhet og beredskap. DSBs koordinerende roller er fastsatt i en egen instruks.[58] I henhold til denne instruksen skal DSB blant annet:

- Ha oversikt over sårbarhets- og beredskapsutviklingen i samfunnet og ta initiativ for å forebygge hendelser med sikte på å hindre tap av liv, helse, miljø, viktige samfunnsfunksjoner og store materielle verdier.
- Ha et sektorovergripende perspektiv med vekt på store ulykker og ekstraordinære situasjoner.
- Bistå Justis- og beredskapsdepartementet i dets systemrettede tilsyn med det sivile beredskapsarbeidet i departementene.

DSB driver som navnet tilsier ikke primært med statssikkerhet. DSB har imidlertid en helt sentral plass i den sivile beredskap og anvender i stor grad andre lovhjemler enn sikkerhetsloven, og er den viktigste aktør på *safety*-feltet som i hovedsak omhandler ikke-intenderte ulykker. Samtidig er DSB opptatt av en helhetlig forebyggende sikkerhetstenkning på tvers av trussel- og risikospekteret. Dette fremheves særlig tydelig gjennom konseptet *all hazards*-tilnærming, som søker å kombinere *safety*- og *security*-aspektene. DSB skal ha et sektorovergripende perspektiv med vekt på store ulykker og ekstraordinære situasjoner, og de opptrer som etatstyrer overfor sivilforsvaret, med sine 18 sivilforsvarsdistrikt. DSB har i tillegg embetsstyringsansvaret for fylkesmannsembetene på samfunnssikkerhet og beredskapsfeltet.[59]

[58] Kgl.res. 24. juni 2005 nr. 688, Instruks for Direktoratet for samfunnssikkerhet og beredskaps koordinerende roller.

[59] FD/JD, *Støtte og Samarbeid,* 2015, 22.

Kapittel 4
Dagens sikkerhetsutfordringer

Forebyggende sikkerhet er en viktig del av arbeidet med nasjonal sikkerhet. Å oppnå sikkerhet har opptatt stater og nasjoner til alle tider, og definisjonene av sikkerhet er mange og ulike. På et grunnleggende plan kan sikkerhet defineres som «evnen til å unngå skader og tap som følge av uønskede hendelser enten disse er bevisste eller tilfeldige handlinger».[1] Risikobegrepet er derfor sentralt i diskusjonene om forebyggende nasjonal sikkerhet. Risiko kan fremstilles som et produkt av sannsynligheten for at en hendelse inntreffer og konsekvensen dersom den inntreffer. Det vil være knyttet usikkerhet til både sannsynligheten og vurderingen av mulig konsekvens.[2]

I den videre gjennomgangen av dagens sikkerhetsutfordringer er det innledningsvis en omtale av risikostyring i staten som grunnlag for å oppnå nasjonal sikkerhet og en omtale av risikovurderingsmetodikk. Videre beskrives hvilke verdier som må vernes, hvilke trusler som kan ramme verdiene og hvilke sårbarheter i samfunnet som trusselaktører kan utnytte. Dette er forhold som påvirker samfunnets risiko – og altså sikkerhet. Avslutningsvis gjennomgås noen av de virkemidlene staten har til rådighet for å styre samfunnsutviklingen i en ønsket retning, med sikte på å redusere risiko.

4.1 Risikohåndtering og forebyggende nasjonal sikkerhet

4.1.1 Risikostyring

Risikostyring er grunnlaget for systematisk sikkerhetsarbeid. Det innbefatter alle tiltak og aktiviteter som gjøres for å styre risiko.[3] Nasjonal sikkerhet påvirkes negativt av ulike typer risiko, og positivt av risikoreduserende tiltak. Den negative påvirkningen på nasjonal sikkerhet knyttes til risiko for et bredt spekter av uønskede hendelser. Uønskede hendelser kan deles inn i tre kategorier a) tilsiktede uønskede hendelser, som spionasje, sabotasje og terrorisme, samt annen kriminalitet, og utilsiktede uønskede hendelser forbundet med b) store menneskeskapte ulykker og c) naturhendelser. Staten, virksomheter og enkeltpersoner foretar valg om hvordan de vil forholde seg til ulike former for risiko. Valgene kan være foretatt bevisst eller ubevisst. Dersom man er kjent med at det knytter seg risiko til et bestemt forhold, kan man velge å forholde seg til høy grad av usikkerhet om hvor høy risikoen er. Dette innebærer at risikonivået er ukjent. Ved å identifisere og vurdere risiko vil man kunne fastsette risikonivået. Dersom risikonivået er kjent vil en kunne velge å foreta risikoreduserende tiltak, eller akseptere risikoen (risikoaksept). Risikoaksept vil være aktuelt dersom risikonivået er tilstrekkelig lavt eller at det fører med seg uforholdsmessig store ulemper (for eksempel kostnader) å gjennomføre risikoreduserende tiltak. Risiko vil også kunne omfatte forhold som ikke er identifisert og som man ikke har kjennskap til at eksisterer.[4] I forbindelse med vurdering av risiko vil informasjonstilgang og kunnskapsnivå ha stor innvirkning på usikkerhet i resultatet. Dette og andre forhold som medfører sårbarheter ved risikostyring er nærmere omtalt i kapittel 4.4.4. Risikoaksept og risikoreduksjon på samfunnsnivå er nærmere omtalt i kapittel 4.5.

Risikoreduserende tiltak som rettes inn mot uønskede hendelser vil i mange sammenhenger være effektive uavhengig av om det er risiko for tilsiktede eller utilsiktede hendelser man utsettes for eller ønsker å verne seg mot. I andre sammenhenger er tiltakene rettet mot risiko for en spesifikk hendelse og har ingen generell risikoreduserende effekt. Reduksjon av risiko i samfunnet skjer enten ved å minske sannsynligheten for at hendelser inntreffer eller gjennom å forberede

[1] Terje Aven, *Pålitelighets- og risikoanalyse* (Oslo: Universitetsforlaget, 1998), 11.

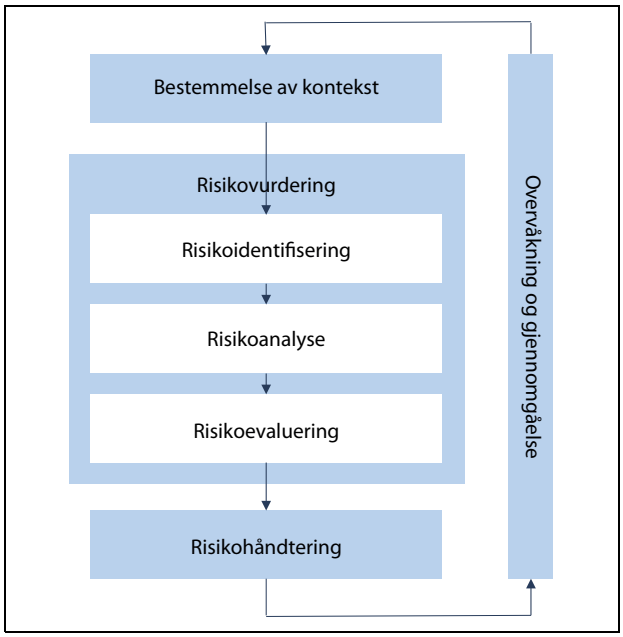
[2] Terje Aven, Willy Røed og Herman S. Wiencke, *Risikoanalyse* (Oslo: Universitetsforlaget, 2008), 27-32

[3] Terje Aven, «Risiko», Store norske leksikon, https://snl.no/risiko

[4] Terje Aven et. al, *Risikoanalyse* 2008.

samfunnet på å håndtere de hendelser som inntreffer, eller på annen måte sikre at konsekvensene av hendelser blir så små som mulig.

Risikostyring og risikoreduksjon vil være av egeninteresse for de fleste virksomheter, og det vil derfor være vanlig å ha en eller annen form for systematikk rundt dette. Graden av systematikk og hvilken metodisk tilnærming som benyttes vil imidlertid variere. Hvilken type risiko som er i fokus vil også variere. Staten stiller krav til offentlig virksomhet om at virksomheten skal styres etter visse prinsipper. Dette gjelder også hvordan virksomheter skal forholde seg til risiko. Et sentralt eksempel på dette området er Statens økonomireglement (blant annet § 4 Grunnleggende styringsprinsipper). I noen sammenhenger er det spesifikke krav til metodisk tilnærming til risiko. I e-forvaltningsforskriften § 15 stilles det krav til at alle offentlige virksomheter skal ha internkontroll på informasjonssikkerhetsområdet basert på anerkjente standarder. Et eksempel kan være ISO/IEC 27001 for sikkerhetsstyring. Slike formelle krav til risikostyring kan også finnes i sektorregelverk, og således gjelde selvstendige rettssubjekter, eventuelt i virksomhetenes egne retningslinjer. NS-ISO 31000 er en generell standard for risikostyring, og et eksempel på standard som mange virksomheter benytter.



Figur 4.1 Risikostyring.

Prinsippet for risikostyring bygger på at det foretas en risikovurdering for en bestemt problemstilling. Med bakgrunn i risikovurderingen vil risikoreduserende tiltak gjennomføres der risikoen oppfattes som uakseptabel.

Kilde: NS-ISO 31000:2009, *Risikostyring, prinsipper og retningslinjer*, utdrag fra figur 1.[1]

[1] Forholdet mellom prinsippene, rammeverket og prosessen for risikostyring fra NS-ISO 31000:2009 er gjengitt av Forsvarsdepartementet med tillatelse fra Standard Online AS 09/2016. Standard Online er ikke ansvarlig for eventuelle feil i gjengitt materiale. Se www.standard.no.

4.1.2 Tilsiktede hendelser versus utilsiktede hendelser – konsekvenser for sikkerhetsarbeidet

Forebygging av uønskede hendelser har en rekke likheter uavhengig av om det er snakk om tilsiktede eller utilsiktede hendelser. Tilsiktede uønskede hendelser har imidlertid særegenheter som gjør forebygging prinsipielt forskjellig fra forebygging av utilsiktede hendelser. *Tilsiktede uønskede hendelser* betyr at noen har en intensjon om å påføre en eller annen form for skade. I forbindelse med nasjonal sikkerhet og samfunnssikkerhet innebærer dette at noen har til hensikt å påføre samfunnet betydelig skade. I praksis betyr dette at den eller de som utfører eller planlegger å utføre handlingen vil kunne tilpasse handlingen til de sikkerhets- og beredskapstiltak som de har kjennskap til, eller som de forventer skal finnes. Dette fører til et behov for å ha et bevisst forhold til hvordan informasjon om risikoreduserende tiltak skal distribueres. Behovet for skjerming av slik informasjon er åpenbar. Samtidig er dette et forhold som det spilles aktivt på i sikkerhetssammenheng. Effektiv avskrekking oppnås gjennom den informasjon, forestilling og kunnskap en trusselaktør har om sikringstiltakene, og ikke nødvendigvis av det reelle sikringsnivået. Det er derfor en god strategi å synliggjøre at sikkerheten er god, samtidig som man skjermer informasjon på en måte som gjør det vanskelig å fullt ut forstå og ramme sikkerhets- og beredskapssystemene.

Videre er det en annen form for dynamikk forbundet med tilsiktede hendelser sammenlignet med utilsiktede. Ved tilsiktede hendelser er det en aktør som foretar valg om strategi og taktikk, samt utvelgelse av mål for handlingen(e). Som regel vil trusselaktører ønske å påføre samfunnet en bestemt type skade eller mest mulig skade med så lav operasjonell risiko som mulig. Operasjonell risiko ved væpnede aksjoner/operasjoner inkluderer alle forhold som reduserer sannsynligheten for at operasjonen lykkes. Dette vil ofte inkludere den personlige risikoen for de som deltar. Hensynet til operasjonell risiko kan lede til en form for opportunisme som fører til at dersom det gjennomføres betydelige risikoreduserende tiltak på enkelte områder vil risikoen øke på områder der det ikke er gjennomført risikoreduserende tiltak. Dette kalles ofte «innbruddsalarm-problema-

tikken». Har alle dine naboer installert innbruddsalarm, men ikke du, er ditt hus mer utsatt. Det er derfor av stor betydning med koordinert og samordnet risikohåndtering på tvers av virksomheter og sektorer.

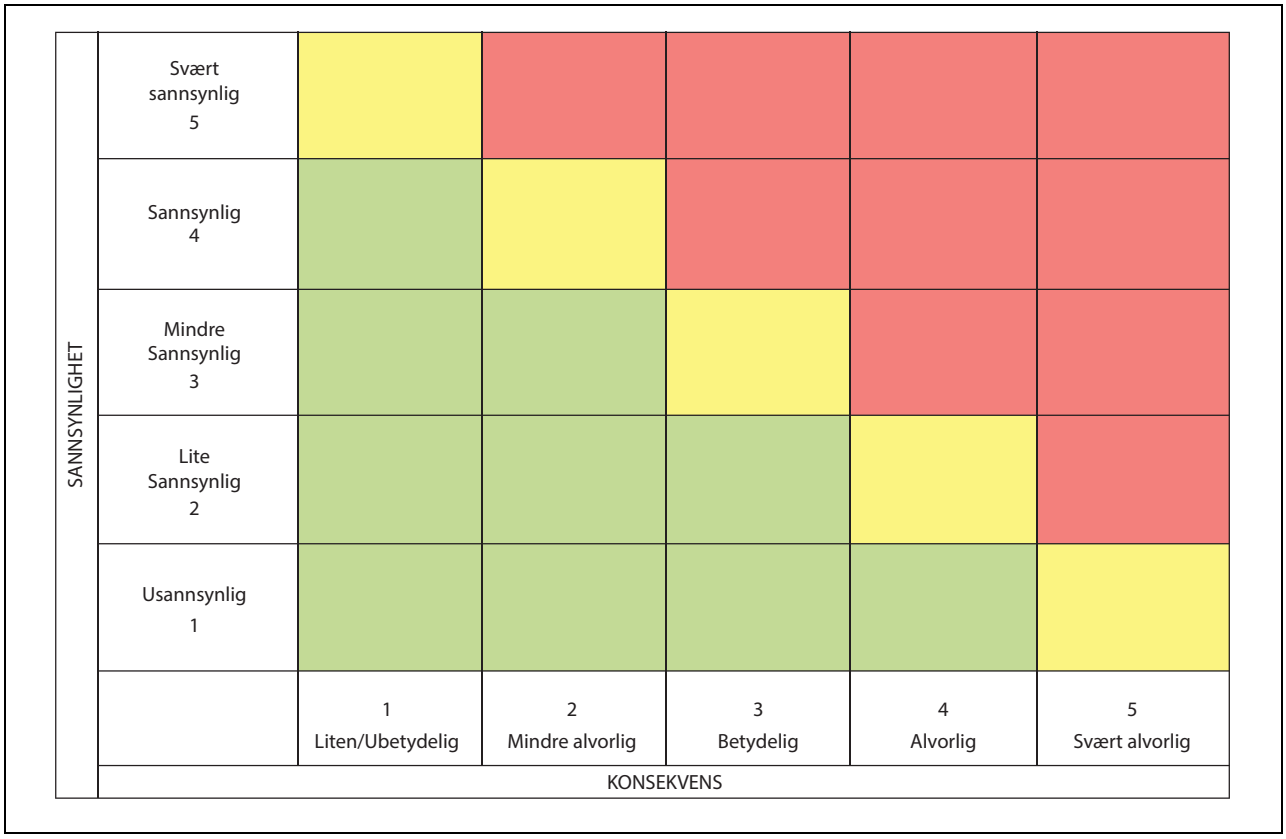
4.1.3 Tilnærminger til risikovurdering

Risikovurderinger er grunnlaget for prioritering av risikoreduserende tiltak i de fleste virksomheter. Det finnes ulike tilnærminger til risikovurderinger. Tradisjonelt har risiko blitt definert som en funksjon av sannsynlighet for og konsekvens av en hendelse, eller et sett med hendelser (figur 4.2). Det er denne tilnærmingen som beskrives i Norsk standard 5814:2008, Krav til risikovurderinger, som er en standard for risikovurderinger for både tilsiktede og utilsiktede uønskede hendelser. Det er flere måter å foreta vurdering av sannsynlighet og konsekvens på. Sannsynlighet kan vurderes ved hjelp av statistiske metoder om relevant statistikk er tilgjengelig, eller som en ikke-statistisk kunnskapsbasert vurdering dersom det ikke finnes egnet statistisk grunnlag. Kombinasjon av statistisk og ikke-statistisk tilnærming kan også benyttes.

I sikkerhetsmiljøene som arbeider med risikohåndtering av tilsiktede uønskede hendelser, er det vanlig å foreta vurderinger av risiko ut i fra det som omtales som tre-faktormodellen (figur 4.3), og som er innarbeidet i Norsk Standard 5832:2014, Samfunnssikkerhet, Beskyttelse mot tilsiktede uønskede handlinger, Krav til sikringsrisikoanalyse. I denne modellen foretas det en kartlegging av hvilke verdier som skal sikres, hvilke trusler som potensielt kan ramme verdiene, samt hvilke sårbarheter som bidrar til at verdiene kan rammes av de aktuelle truslene.

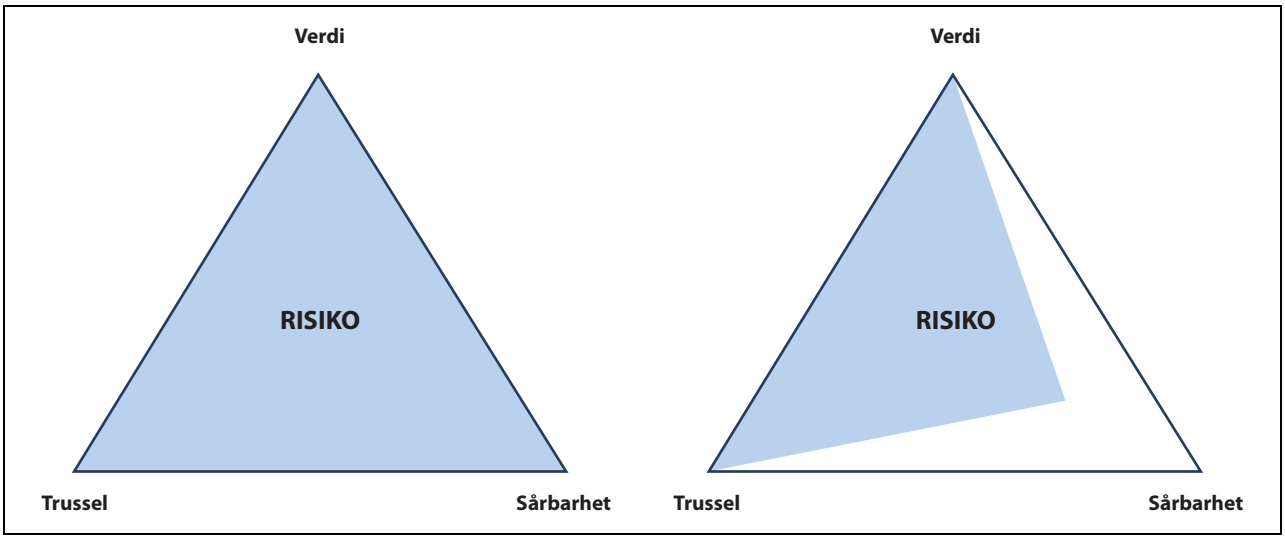
Forsvarets forskningsinstitutt (FFI) har utgitt en rapport der de to standardene for risikovurdering sammenlignes.[5] FFI konkluderer i sin rapport med at tilnærmingene har mange likhetstrekk, og at forskjellen hovedsakelig ligger i hvorvidt sannsynlighetsvurderingen er eksplisitt eller implisitt. I rapporten skriver de at begge modellene har svakheter knyttet til hvordan de kommuniserer usikkerheten knyttet til risikoen, og at det verken nasjonalt eller internasjonalt eksisterer en

[5] Odd Busmundrud, Maren Maal, Jo H. Kiran og Monica Endregard, «Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger», *FFI-rapport* 00923 (Kjeller: FFI, 2015).



Figur 4.2 Risikomatrise.

Den vanligste måten å vurdere risiko på er som en funksjon av sannsynlighet og konsekvens for at ulike hendelser inntreffer.



Figur 4.3 Risiko – trefaktormodellen.

Risiko kan betraktes som forholdet mellom verdier (som vi ønsker å verne), trusler som kan ramme disse verdiene og sårbarheten verdiene har i forhold til de aktuelle truslene. Risiko kan redusere gjennom å redusere trusler eller sårbarhet (gitt at verdiene skal vernes).

Kilde: NSM, *Sikkerhetsfaglig råd*, 2015.

beste fremgangsmåte for å vurdere tilsiktede uønskede hendelser.

4.2 Verdier av betydning for nasjonal sikkerhet

Formålet med forebyggende sikkerhet er å verne verdier. Verdi kan betraktes som kvaliteten ved noe, eller det som er godt ved noe. Verdi sies gjerne å bestemme en tings viktighet med hensyn til hvordan vi bør gjøre våre vurderinger og beslutninger.[6] Verdi kan i utgangspunktet tillegges alle ting (personer, objekter, handlinger, tilstander), og en ting blir gjerne sagt å ha en større eller mindre grad av verdi.

Det kan gjøres et skille mellom ulike typer verdi og ulike måter ting kan være verdifulle på. Særlig viktig er skillet mellom egenverdi og instrumentell verdi. Skillet går i korte trekk ut på at det som har egenverdi er verdifullt i kraft av å være det det er, mens det som har instrumentell verdi er verdifullt bare i kraft av å være et middel eller årsak til å realisere noe med egenverdi.

En verdi kan defineres som en «ressurs som hvis den blir utsatt for en uønsket påvirkning vil medføre en negativ konsekvens for den som eier, forvalter eller drar fordel av ressursen».[7] Det kan være verdier av materiell og ikke materiell art.

Som utgangspunkt for en gjennomgang av verdier som er av betydning for nasjonal sikkerhet er det sett hen til grunnlovens bestemmelser omkring grunnleggende verdier i vårt demokratiske samfunn; begrepet kritiske samfunnsfunksjoner som danner utgangspunktet for samfunnssikkerhetsarbeidet i staten; begrepene rikets sikkerhet og vitale nasjonale sikkerhetsinteresser slik disse benyttes i dagens sikkerhetslov, samt grunnleggende nasjonale interesser som reguleres i straffeloven og utlendingsloven.

I kapittel 6 fremkommer utvalgets vurderinger av hva som skal reguleres i et nytt lovgrunnlag for forebyggende nasjonal sikkerhet, sett i lys av verdiene og begrepene omtalt i dette kapittelet.

4.2.1 Grunnleggende verdier i vårt demokratiske samfunn

Det følger av utvalgets mandat at det «skal vurdere hva som bør reguleres i lov for å sikre nasjonal sikkerhet. Formålet med nytt lovgrunnlag skal være å beskytte kritisk infrastruktur, kritiske samfunnsfunksjoner og sensitiv informasjon mot tilsiktede, uønskede hendelser».

Det som i henhold til mandatet skal beskyttes er altså nasjonal sikkerhet – som oppnås gjennom å blant annet sikre kritisk infrastruktur, kritiske samfunnsfunksjoner og sensitiv informasjon.

Det er naturlig å se hen til Grunnloven som utgangspunkt for hvilke underliggende verdier som må sikres for å ivareta nasjonal sikkerhet.

6 «Verdi», Store norske leksikon, https://snl.no/verdi.

7 Norsk Standard 5830:2012, *Samfunnssikkerhet: Beskyttelse mot tilsiktede uønskede handlinger, Terminologi.*

Grunntanken fra naturretten om at menneskene er født frie og like og med det samme menneskeverd, ligger til grunn for både Norges grunnlov og Verdenserklæringen om menneskerettigheter fra 1948. Grunnloven danner et felles rettslig og politisk fundament, i tillegg til at den er et samlende symbol for nasjonen.

Det følger av Grunnloven § 1 at «Kongeriket Norge er et fritt, selvstendig, udelelig og uavhendelig rike. Dets regjeringsform er innskrenket og arvelig monarkisk.» Da bestemmelsen ble gitt i 1814, ble den ansett som Norges selvstendighets- og uavhengighetserklæring.[8] At Norge er og skal være en suveren stat er dermed en grunnleggende verdi. Et sentralt element i suverenitetsbegrepet er statens selvbestemmelsesrett innenfor et nærmere angitt territorium.

Det følger videre av Grunnloven § 2 at «Verdigrunnlaget forblir vår kristne og humanistiske arv. Denne Grunnlov skal sikre demokratiet, rettsstaten og menneskerettighetene.» Paragrafen uttrykker «sentrale og grunnleggende verdier i samfunnet og for staten, som konstitusjonen bygger på og bidrar til å bevare og fremme.»[9] Departementet uttrykte også at «[d]e grunnleggende prinsippene og verdiene vil bli operasjonalisert gjennom andre bestemmelser i Grunnloven som i større utstrekning direkte gir rettigheter og plikter», at bestemmelsen måtte utformes innen rammene av internasjonale forpliktelser, og at utformingen måtte balansere en rekke ulike hensyn, inkludert religionsfrihet.

Om bestemmelsens første punktum uttalte Gjønnes-utvalget[10] blant annet at «[g]runnloven er det dokumentet som konstituerer statsdannelsen Norge som et politisk og rettslig fellesskap, men dette bygger igjen på et grunnleggende nasjonalt fellesskap. Dersom man ønsker å fremheve dette nasjonale fellesskapet (etos) er det mest nærliggende med en verdiparagraf som viser til felles historie, kulturtradisjoner og samfunnsverdier.»

De tre grunnverdiene henviser til henholdsvis folkestyret, en uavhengig og upartisk domstol og til menneskerettighetene, jf. Grunnloven § 92. Det følger av sistnevnte en forpliktelse ikke bare overfor befolkningen, men også folkerettslig ved at «Statens myndigheter skal respektere og sikre menneskerettighetene slik de er nedfelt i denne grunnlov og i for Norge bindende traktater om menneskerettigheter».

At menneskerettighetene skal respekteres, innebærer at alle statsmakter må ta dem i betraktning, og følge dem. Avhengig av rettighetenes nærmere innhold og formål, danner de i utgangspunktet konstitusjonelle grenser for det ordinære flertalls politikk, og de skal være en normdannende rettesnor for alle statens myndigheter i deres maktutøvelse.

Det nærmere innholdet i begrepene «respektere» og «sikre» kan beskrives slik:

> At menneskerettighetene skal respekteres, innebærer at alle statsmakter må ta dem i betraktning, og følge dem. Avhengig av rettighetenes nærmere innhold og formål, danner de i utgangspunktet konstitusjonelle grenser for de ordinære flertalls politikk, og de skal være en normdannende rettesnor for alle statens myndigheter i deres maktutøvelse.
>
> At rettighetene skal sikres pålegger statsmaktene en aktivitetsplikt for ivaretagelse av rettighetene. For regjeringen og Stortinget ligger det i dette en aktivitetsplikt – de kan ikke unnlate å sikre menneskerettigheter de er klar over blir utfordret under gjeldende reguleringer. For domstolene innebærer sikringsplikten at de må håndheve ikke bare de menneskerettighetene som er nedfelt i Grunnloven, men også de for Norge bindende menneskerettighetsforpliktelser, og sørge for at eventuelle menneskerettighetsbrudd foretatt av andre myndigheter blir reparert, jf. Rt. 2014 s. 1105, Rt. 2014 s. 1292 og Rt. 2015 s. 93. [11]

Samlet utrykker Grunnloven §§ 1 og 2 nasjonens viktigste og mest beskyttelsesverdige verdier, statens suverenitet, demokratiet, rettsstaten og menneskerettighetene. Disse verdiene danner etter utvalgets syn et godt utgangspunkt for den videre utarbeidelsen av et nytt lovgrunnlag for nasjonal sikkerhet.

Her oppstår imidlertid et grunnleggende dilemma. Statens selvstendighet, suverenitet og handlefrihet er avgjørende for opprettholdelse av de mest grunnleggende verdiene i rettsstaten og i et demokratisk samfunn. Samtidig kan de sikkerhetstiltak som iverksettes for å forebygge trusler mot nasjonal sikkerhet, sette de grunnleggende samfunnsverdiene under press. Skal staten gjøre inngrep i grunnleggende rettigheter, for eksem-

---

8 Arne Fliflet, Rettsdata.no, Grunnloven § 1, note (2), sist hovedrevidert 27.04.2014.

9 St.meld. nr. 17 (2007–2008) *Staten og Den norske kirke*, 71.

10 Ibid.

11 Anine Kierulf, Rettsdata.no, Grunnloven § 92, note (197A3), sist hovedrevidert 17.06.2015

pel personvern og rettssikkerhet, må det begrunnes som legitimt og forholdsmessig for å beskytte andre grunnleggende rettigheter og hensyn. Slike formål kan være andre menneskerettigheter, men også hensynet til nasjonal sikkerhet, jf. Den europeiske menneskerettighetskonvensjonen art. 8(2). Vernet av den enkeltes personlige integritet og autonomi er i Norge en grunnlovsfestet rettighet, jf. Grunnloven § 102. En balansert avveining mellom nasjonal sikkerhet, menneskerettighetene og andre grunnleggende interesser, står sentralt i utvalgets arbeid.

En målsetting for utvalget vil være å fremme et lovforslag som ikke vesentlig endrer forholdet mellom de overordnede samfunnsmessige verdiene. Forholdet mellom forebyggende sikkerhet og rettssikkerhetsgarantiene utdypes nærmere i kapittel 5.

4.2.2 Samfunnets grunnleggende behov og kritiske samfunnsfunksjoner

En av de viktigste oppgavene for staten er å ivareta nasjonal sikkerhet. Dette omfatter ivaretagelse av nasjonens ytre sikkerhet og samfunnssikkerhet. Verdiene i samfunnet er knyttet til hvilke behov befolkningen har og i hvilken grad manglende oppfyllelse av behov har negative konsekvenser for individet.

Et spørsmål i denne sammenheng er hva som utgjør *samfunnets grunnleggende behov*. Dette kan også formuleres som et verdispørsmål: Hvilke verdier er det i et samfunnsmessig perspektiv helt grunnleggende å beskytte?

Infrastrukturutvalget la i sin utredning til grunn at en mulig måte å identifisere samfunnets grunnleggende behov på, var å ta utgangspunkt i Maslows behovspyramide. De grunnleggende behovene definisjonen peker på, kan knyttes til de to nederste trinnene i behovspyramiden – fysiologiske behov og trygghetsbehov (som også omfatter orden og stabilitet). Maslows teori var i utgangspunktet knyttet til menneskets psykologiske behov i en selvrealiseringsprosess. Teorien er imidlertid også blitt brukt i organisasjonsteori og samfunnsfag.[12]

Etter å ha identifisert de grunnleggende behovene/grunnleggende verdiene som må beskyttes, vil det neste steg være å identifisere hvilke samfunnsfunksjoner som er kritiske for å dekke disse behovene. Disse funksjonene vil da utgjøre det som omtales som kritiske samfunnsfunksjoner. Ulike kriterier kan legges til grunn for identifisering av kritiske samfunnsfunksjoner. DSB har i sin rapport Samfunnets kritiske funksjoner (KIKS) avgrenset identifiseringen til de mest tidskritiske funksjonene. Det vil si de som får umiddelbare negative konsekvenser for befolkningen selv ved kortvarig svikt. DSB har lagt til grunn følgende forutsetninger for operasjonaliseringen av begrepet:[13]

- Avgrensning i tid: Begrepet kritisk samfunnsfunksjon skal forbeholdes funksjoner som samfunnet ikke kan klare seg uten i syv døgn uten at dette truer grunnleggende behov.
- Kontekstuelle forutsetninger: Vurderingen av en funksjons kritikalitet baseres på konsekvenser om bortfall skjer på ugunstige tidspunkt, og at det kan være et ugunstig sammenfall av hendelser. Det forutsettes med andre ord at uønskede hendelser inntreffer.

DSB har, basert på disse kriteriene, sortert funksjonene i fire behovskategorier:

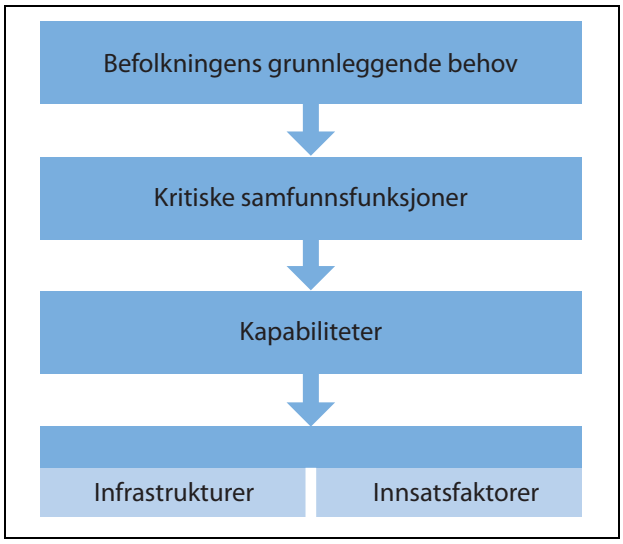
- Nasjonal styringsevne og suverenitet
  - (1) nasjonal styring, (2) forsvar
- Befolkningens sikkerhet
  - (3) lov og orden, (4) helse og omsorg, (5) redningstjenester, (6) sikkerhet mot eksponering av farlige stoffer, (7) informasjonssikkerhet, (8) overvåkning av naturfarer
- Befolkningens velferd
  - (9) matforsyning, (10) vann og avløp, (11) sosiale ytelser og tjenester, (12) finansielle tjenester, (13) energiforsyning, (14) elektronisk kommunikasjon, (15) transport, (16) satellittbaserte tjenester
- Kultur og natur
  - (17) vern av kulturelle verdier, (18) vern mot forurensning

Hvilke samfunnsfunksjoner som vil anses for kritiske, avhenger både av hvilke verdier/behov som legges til grunn for vurderingen og hvilke kriterier som legges til grunn for vurdering av kritikalitet.

I KIKS-rammeverket er den funksjonsevnen de ulike samfunnsfunksjonene må opprettholde beskrevet som *kapabiliteter*. Kapabilitetene gir uttrykk for hva ansvarlige virksomheter skal være i stand til for at samfunnsfunksjonen skal være iva-

[12] Abraham Maslow, «A Theory of Human Motivation», *Psychological review 50:4* (1943), 370.

[13] Direktoratet for samfunnssikkerhet og beredskap, *Samfunnets kritiske funksjoner: Hvilken funksjonsevne må samfunnet opprettholde til enhver tid?*, Høringsutgave september 2015, 20.



Figur 4.4 Kritiske samfunnsfunksjoner.

Befolkningens grunnleggende behov er utgangspunktet for å definere kritiske samfunnsfunksjoner, som kan operasjonaliseres i kapabiliteter. Disse er avhengige av infrastrukturer og innsatsfaktorer for å fungere.

Kilde: DSB, *Samfunnets kritiske funksjoner – Hvilken funksjonsevne må samfunnet opprettholde til enhver tid?* Høringsutgave september 2015.

retatt. DSB skiller mellom tre ulike kapabiliteter:[14]

- *Kontinuitetskapabiliteter*: Evne til å opprettholde leveranser fra virksomheter med samfunnskritisk betydning uansett hva som måtte inntreffe
- *Sikkerhetskapabiliteter*: Evne til å opprettholde akseptabelt sikkerhetsnivå i virksomheter som potensielt kan anrette skade på liv og helse, miljø eller tap av andre samfunnsmessige verdier
- *Beredskapskapabiliteter*: Evne til å iverksette forhåndsplanlagte aktiviteter når det oppstår en ekstraordinær situasjon

Befolkningens grunnleggende behov danner utgangspunktet for å definere kritiske samfunnsfunksjoner. Disse funksjonene kan igjen operasjonaliseres i ulike kapabiliteter, henholdsvis kontinuitets-, sikkerhets- eller beredskapskapabiliteter.

En ytterligere operasjonalisering vil i henhold til DSBs rapport være å beskrive nødvendige leveranser eller innsatsfaktorer for at kapabilitetene skal ivaretas. En slik kartlegging av verdikjeden bak hver kapabilitet med vurdering av sårbarhet og avhengigheter, er nødvendig for å ha tilstrekkelig oversikt og kontroll over samfunnsfunksjonene. Infrastruktur kan for eksempel være produksjonsanlegg, transformatorer, kraftnett og lignende som trengs for å understøtte energiforsyning og kjernenett, transportnett og svitsjer for understøttelse av elektronisk kommunikasjon. Innsatsfaktorer kan være personell (arbeidskraft, kompetanse, etc), kapital, naturressurser o.l.

De innsatsfaktorer som en virksomhet med kritisk samfunnsfunksjon er avhengig av for å kunne dekke samfunnets grunnleggende behov, betegnes som kritiske innsatsfaktorer.

På samme måte vil infrastruktur som er nødvendig for understøttelse av kritiske samfunnsfunksjoner betegnes som *kritisk infrastruktur*. Infrastrukturutvalget definerer kritisk infrastruktur på følgende måte:

> Kritisk infrastruktur er de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner som igjen dekker samfunnet grunnleggende behov og befolkningens trygghetsfølelse.[15]

Systematikk for kartlegging og identifisering av kritisk infrastruktur vil bli redegjort nærmere for i kapittel 7 og 9.

For å sikre ivaretakelse av samfunnets grunnleggende behov og opprettholdelse av kritiske samfunnsfunksjoner, er det nødvendig å iverksette visse sikkerhetstiltak. Dels er det nødvendig å sørge for en tilfredsstillende sikring av den infrastrukturen som er avgjørende for opprettholdelse av funksjonalitet. Dels må informasjon av avgjørende betydning for de samme funksjonene sikres også av hensyn til konfidensialitet, integritet og tilgjengelighet.

4.2.3 Rikets sikkerhet og vitale nasjonale sikkerhetsinteresser

I dagens sikkerhetslov er verdibegrepet først og fremst knyttet til i hvilken grad truslene kan skade rikets sikkerhet. Fokuset i dagens lov er med andre ord hvilke skadefølger kompromittering av skjermingsverdig informasjon vil få for Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser, jf. sikkerhetsloven § 11.

Det samme gjelder for skjermingsverdige objekter, hvor verdien indirekte er beskrevet gjennom de skadefølger redusert funksjonalitet, ska-

[14] Ibid., 21.

[15] NOU 2006: 6, *Når sikkerheten er viktigst: Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner.*

deverk, ødeleggelse eller rettsstridig overtakelse, vil kunne få for rikets selvstendighet og sikkerhet og for andre vitale nasjonale sikkerhetsinteresser, jf. sikkerhetsloven § 17a.

Dagens sikkerhetslov benytter i formålsbestemmelsen begrepsapparatet «rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser», jf. sikkerhetsloven § 1 første ledd bokstav a. Begrepene er ikke nærmere definert i loven. Hva gjelder begrepet «rikets sikkerhet» følger det av lovens forarbeider at:

> Med «rikets... sikkerhet» siktes både til rikets indre og ytre sikkerhet. Begrepet er for øvrig en utpreget rettslig standard som kan forandre seg med samfunnsutviklingen. Departementet ser ikke i lovforslaget her grunn til å søke å presisere begrepet utover det som allerede er antatt på bakgrunn av andre rettskilder (juridisk teori, domstolspraksis, forarbeider til andre lover, forvaltningspraksis, mv).[16]

Forarbeidene beskriver «vitale nasjonale sikkerhetsinteresser» som et samlebegrep som dekker samtlige felter innenfor rikets totale sikkerhetsbehov. Begrepet skal til enhver tid vurderes og defineres av overordnede politiske myndigheter. Terskelen for å anse noe for å true slike interesser i medhold av sikkerhetsloven vil være høy, og det understrekes at begrepet kan endres i pakt med samfunnsutviklingen og de sikkerhetsmessige utfordringer som Norge til enhver tid står overfor.

Infrastrukturutvalget la i sin utredning følgende forståelse av begrepene til grunn:

> Det følger av ovennevnte at begrepene «rikets sikkerhet» og «vitale nasjonale interesser» til sammen skal dekke samfunnets totale sikkerhetsinteresser, slik de defineres på bakgrunn av de sikkerhetsutfordringene Norge til enhver tid står overfor. Samtidig er det viktig at terskelen for å anse noe for å true «rikets sikkerhet» og «vitale nasjonale interesser» skal være høy.
>
> […] I denne utredningen favner begrepene «rikets sikkerhet» og «vitale nasjonale interesser» sikringen av landets kritiske infrastruktur og kritiske samfunnsfunksjoner.[17]

Til tross for at forarbeidene til sikkerhetsloven klart forutsetter at begrepene *rikets sikkerhet* og *vitale nasjonale sikkerhetsinteresser* er rettslige standarder, som vil kunne endres i takt med samfunnsutviklingen, og at senere utredninger har lagt til grunn at begrepene omfatter noe mer enn statssikkerhet i snever forstand, er det i dag forskjellige oppfatninger av det nærmere innholdet i disse begrepene.

4.2.4 Grunnleggende nasjonale interesser

Straffelovens kapittel 17 omhandler vern av Norges selvstendighet og andre grunnleggende nasjonale interesser. I Straffelovkommisjonens delutredning VIII[18] foreslo kommisjonen å samle i et nytt kapittel 17 alle straffebestemmelsene om rikets sikkerhet og grunnleggende nasjonale interesser, som tidligere fantes i 8de Kapitel, Forbrydelser mod Statens Selvstændighed og Sikkerhed og 9de Kapitel, Forbrydelser mod Norges Statsforfatning og Statsoverhoved. Det nye kapittel 17 ble foreslått å omfatte ni typer krenkelser:

1. Krenkelse av Norges selvstendighet og fred
2. Krenkelse av Norges statsforfatning
3. Angrep på de høyeste statsorganers virksomhet
4. Inngrep overfor andre samfunnsinstitusjoner
5. Landssvik
6. Ulovlig etterretningsvirksomhet
7. Avsløring av statshemmelighet
8. Avtale om krenkelse av Norges selvstendighet og forfatning, freden og andre grunnleggende nasjonale interesser
9. Privat militær virksomhet

Kommisjonen viste i sin utredning til at straffebudene i 8de og 9de Kapitel relaterte seg til Grunnlovens bestemmelser om statsforfatningen og rikets selvstendighet og udelelighet. Fanebestemmelsene var § 83 som vernet Norges statsrettslige stilling og statsområde, og §§ 98 og 99 som vernet statsforfatningen og de øverste statsmaktene. De øvrige straffebudene i kapitlene kunne i stor utstrekning ses i forlengelsen av disse bestemmelsene, ved at de vernet freden eller mot særlige trusler i krig eller når krig truer, eller mot farer som ellers kunne true rikets indre eller ytre sikkerhet.[19]

Under drøftelsen av hvilke interesser som burde vernes etter straffebestemmelsene i det nye kapittelet, konkluderte kommisjonen med at det bare er de grunnleggende nasjonale interes-

[16] Ot.prp. nr. 49 (1996–97) Om lov om forebyggende sikkerhetstjeneste (sikkerhetsloven).

[17] NOU 2006: 6.

[18] NOU 2003: 18, *Rikets sikkerhet*, 71.

[19] Ibid., 72–73.

Boks 4.1 Grunnleggende nasjonale interesser

Grunnleggende nasjonale interesser er omtalt i ny straffelov kapittel 17. I lovens § 121 om etterretningsvirksomhet mot statshemmeligheter, er grunnleggende nasjonale interesser nærmere beskrevet i bokstav a-f:

a. forsvars-, sikkerhets- og beredskapsmessige forhold,
b. de øverste statsorganenes virksomhet, sikkerhet eller handlefrihet,
c. forholdet til andre stater,
d. sikkerhetsopplegg for fremmede staters representasjon og ved større nasjonale og internasjonale arrangementer,
e. samfunnets infrastruktur, så som mat-, vann- og energiforsyning, samferdsel og telekommunikasjon, helseberedskap eller bank- og pengevesen, eller
f. norske naturressurser.

ser som burde omfattes av straffelovens bestemmelser til vern om rikets sikkerhet i vid forstand:

> Under enhver omstendighet finner utvalget at vernet mot innhenting og avsløring av hemmelige opplysninger, ikke bør begrenses til interesser som gjelder rikets sikkerhet i tradisjonell forstand, men at også grunnleggende nasjonale interesser ellers bør omfattes. Ved siden av forholdet til andre stater, herunder forhandlingsposisjoner, er det nærliggende å fremheve de interesser som er knyttet til infrastrukturen, energi-, mat- og vannforsyning, samferdsel og telekommunikasjon, helseberedskap, bank- og pengevesen og andre samfunnsøkonomiske forhold, […][20]

I Justis- og beredskapsdepartementets forarbeider til ny straffelov sa departementet seg enig med kommisjonen i at vernet mot ulovlig etterretningsvirksomhet burde utvides fra å gjelde *rikets sikkerhet* til *grunnleggende nasjonale interesser*.[21]

Begrepet *grunnleggende nasjonale interesser* har også erstattet *rikets sikkerhet* i utlendingsloven.[22] I forarbeidene til utlendingsloven har departementet gitt følgende begrunnelse for endringsforslaget:

> Begrepet «grunnleggende nasjonale interesser» er et mer dekkende begrep som klarere reflekterer hvilke interesser man ønsker å beskytte. Begrepet «rikets sikkerhet», i alle fall tolket i snever eller tradisjonell forstand, er noe utdatert ut fra den senere tids utvikling, særlig i forhold til terrorvirksomhet, der hensikten ikke alltid er å ramme rikets sikkerhet som sådan, men like mye å skape frykt i sivilbefolkningen, eller å inspirere eller motivere til ekstremistiske handlinger, uten at konkrete handlinger er begått. Begrepet «grunnleggende nasjonale interesser» må tolkes i lys av den generelle samfunnsutviklingen og endringer i det internasjonale trusselbildet, og har en dynamisk karakter.[23]

Evalueringsutvalget for Stortingets kontrollutvalg for etterretnings-, overvåknings- og sikkerhetstjeneste, som overleverte sin rapport til Stortinget 29. februar 2016, uttalte følgende om begrepet *nasjonal sikkerhet*:

> Rikets eller nasjonens sikkerhet omfatter flere felt. For det første nasjonal suverenitet og herredømme over landets territorium til lands, til sjøs og i luften. Et annet viktig felt er vern av det politiske styresettet, altså Norges demokratiske system og institusjoner. I tillegg kommer beskyttelse av andre viktige fysiske og digitale samfunnsstrukturer. Disse beskyttelsesverdige interessene er blant annet vernet gjennom straffelovens bestemmelser om vern av Norges selvstendighet og andre grunnleggende nasjonale interesser, samt bestemmelsene om straff for terrorhandlinger og terrorrelaterte handlinger. [24]

4.3 Trusler mot nasjonal sikkerhet

Nasjonal sikkerhet handler om å verne nasjonens verdier mot trusler. En trussel er en mulig uønsket handling som kan gi en negativ konsekvens for en virksomhets sikkerhet.[25] En trussel mot

[20] Ibid.

[21] Ot.prp. nr. 8 (2007–2008), om lov om endringer i straffeloven 20. mai 2005 nr. 28 mv. (skjerpende og formildende omstendigheter, folkemord, rikets selvstendighet, terrorhandlinger, ro, orden og sikkerhet, og offentlig myndighet).

[22] Lov 15. mai 2008 nr. 35 om utlendingers adgang til riket og deres opphold her (utlendingsloven).

[23] Ot.prp. nr. 75 (2006–2007) om lov om utlendingers adgang til riket og deres opphold her (utlendingsloven).

[24] Dok. 16 (2015–2016), 33.

nasjonal sikkerhet vil kunne ha negativ konsekvens for de grunnleggende nasjonale interesser.

Vern mot trusler oppnås gjennom enten direkte eller indirekte påvirkning. Direkte påvirkning av trusselen oppnås ved å håndtere, fjerne eller nøytralisere den. Dette kan gjøres ved bruk av maktmidler, eller ved å påvirke holdninger og strategi gjennom økonomisk påvirkning, kommunikasjon og diplomati, eller en kombinasjon av slike faktorer. Indirekte påvirkning av trusselen kan gjøres ved å endre kost/nytte-vurderingen hos en potensiell trusselaktør. Dette kan innbefatte alle virkemidler som kan bidra til å sannsynliggjøre overfor potensielle trusselaktører at sikringsnivået er høyt nok til å forhindre at uønskede handlinger kan utøves uten uforholdsmessig høy innsats og risiko for å mislykkes.

I en trusselvurdering foretas en vurdering av trusselaktørenes intensjoner og kapasiteter. Det er Etterretningstjenesten og Politiets sikkerhetstjeneste (PST) som har ansvar for å foreta trusselvurderinger for Norge og norske interesser i utlandet. Etterretningstjenesten har ansvar for utenlandsetterretning, mens PST har ansvar for innlandsetterretning. Nasjonal sikkerhetsmyndighet utgir også årlige vurderinger av sikkerhetstilstanden, inkludert rapporter med spesielt fokus på trusler i det digitale domenet. Disse dokumentene utgjør grunnlaget for statens sikkerhetsarbeid, og gjennom de åpne trusselvurderingene vil hele samfunnet kunne nyttiggjøre seg vesentlige deler av denne informasjonen.

En trussel mot nasjonal sikkerhet kan komme i form av for eksempel ulovlig etterretningsvirksomhet, sabotasje, svindel, vold, økonomisk press, politisk press, annet press, menneskehandel, annen kriminalitet, cyberangrep og militære angrep i en eller annen form. Vi lever i et informasjonssamfunn som er i rask utvikling. Det er derfor knyttet spesiell spenning til hvordan trusler i cyberdomenet vil arte seg og utvikles.

I tillegg til trusseltypene som er nevnt ovenfor, kan handlinger som skjer uten intensjon om å forårsake negative konsekvenser for en annen part forårsake betydelig skade i samfunnet og også falle inn under definisjonen av en trussel. Denne typen trusler faller imidlertid utenfor utvalgets mandat som er avgrenset til tilsiktede uønskede handlinger. Denne typen trusler kan imidlertid utnyttes av trusselaktører og blir således en sårbarhet for samfunnet. Dette er omtalt under kapittel 4.4.4.2.

[25] NS 5830:2012, *Samfunnssikkerhet: Beskyttelse mot tilsiktene unøskede hendelser, Terminologi.*

4.3.1 Aktuelle trusler

4.3.1.1 Etterretningsvirksomhet og spionasje

Etterretning er en viktig kapabilitet for militære og politiske formål. På strategisk nivå handler etterretning om å danne beslutningsgrunnlag for landets øverste ledelse. Etterretning omfatter innsamling, sammenstilling, analyse og tolkning av informasjon. Etterretning for militære og sikkerhetspolitiske formål gjennomføres blant annet for å skaffe til veie informasjon om en motstanders strategier og planer, militære kapasiteter, og for å kartlegge sårbarheter som kan utnyttes til egen fordel i en eventuell konflikt. Sårbarhetene kan være av organisatorisk, teknisk eller menneskelig karakter. Dette kan være informasjon om politiske forhold, teknologi og vitenskap, økonomi, industri, kommunikasjon, kraftforsyning, sosiale forhold, enkeltpersoner og annet. Slik kunnskap er avgjørende for hvordan forløpet, og dermed også utfallet, av en konflikt blir. Etterretning fra fremmede stater er i så måte en indirekte trussel mot et lands interesser, ved at innsamlingen danner grunnlaget for en eventuell vellykket gjennomføring av direkte trusler (slik som sabotasje) i en potensiell konfliktsituasjon. I mange sammenhenger kan innsamling av slik informasjon være avgjørende for å unngå at konflikter eskalerer.

Etterretning benyttes også for å få kunnskap og teknologi som kan benyttes for å videreutvikle egne kapabiliteter, enten i form av doktrine eller materiell. Etterretning har både sikkerhetspolitiske og militære anvendelse, men benyttes også for rent sivile formål som kan bidra til økt økonomisk vekst, økt konkuranseevne på internasjonale markeder, eller på andre måter gi velstandsutvikling. Mye etterretning innhentes gjennom åpne kilder eller andre lovlige midler. Informasjon som en part vurderer å være skjermingsverdig vil som regel være underlagt en eller annen form for beskyttelse/skjerming. For å få tak i slik informasjon vil etterretning baseres på fordekte og som regel ulovlige metoder. De fleste land innhenter etterretning utenlands, men bruken av kontroversielle eller ulovlige virkemidler vil variere fra stat til stat. Edvard Snowden vakte stor oppmerksomhet med sine lekkasjer til The Guardian og The Washington Post i juni 2013 om amerikanske NSAs (National Security Agency) innsamling av store mengder data om egne borgere og en rekke andre lands borgere og ledere, herunder allierte.

Avhengig av graden av beskyttelse vil en etterretningsaktør benytte ulike virkemidler for å få tak i informasjonen. Gjennom riktig verdivurdering av informasjon og dertil egnede sikkerhetstil-

tak, vil det kunne etableres en sammenheng mellom verdien av informasjon og ressursinnsatsen som en etterretningsaktør må benytte for å få tak i informasjonen og risikoen forbundet med innhentingsmetoden. Dette vil påvirke kost-/nyttevurderingen til en etterretningsaktør for å klarlegge om det vil være hensiktsmessig å gjøre forsøk på innhenting eller ikke. Samtidig vil det ved manglende verdivurdering oppstå risiko for at informasjon som er avgjørende for en trusselaktør lett blir tilgjengelig. For at en verdivurdering skal bli riktig, er det nødvendig med forståelse for hvilken verdi ulik informasjon har for ulike trusselaktører.

I Norge, som i alle andre land, er det ulovlig å bedrive etterretning mot statshemmeligheter og mot hemmeligheter som har betydning for våre alliertes sikkerhet. Det er også ulovlig å drive etterretning mot sensitive personopplysninger i henhold til straffeloven.

I dagens sikkerhetslov[26] § 3 nr. 3 er ulovlig etterretning omtalt som spionasje, og definert som «innsamling av informasjon ved hjelp av fordekte midler i etterretningsmessig hensikt».

Spionasje faller inn under fellesbetegnelsen «sikkerhetstruende virksomhet» som i dagens sikkerhetslov § 3 nr. 2 er definert som «forberedelse til, forsøk på og gjennomføring av spionasje, sabotasje eller terrorhandlinger, samt medvirkning til slik virksomhet».

Det er også ulovlig å avsløre uautoriserte innsamlede opplysninger (straffeloven[27]), og det stilles krav til hvordan informasjon skal sikres og forvaltes for å unngå at slik informasjon kommer på avveie (sikkerhetsloven).

Ulovlig etterretningsvirksomhet kan være sikkerhetspolitisk eller økonomisk motivert, og være utført av stater, private aktører eller en kombinasjon av disse. Teknologisk utvikling og økt digitalisering av samfunnet gjør at digital industrispionasje er en økende utfordring. Internasjonal cyberspionasje truer verdiskapingspotensialet og utgjør store økonomiske kostnader årlig. I 2013 ble Telenor utsatt for omfattende og målrettet industrispionasje. Datamaskiner ble tømt for alle data, inkludert e-post, passord og andre typer personlige data. Nettangrepet tok også delvis styring over maskinene via fjernkontroll. Det er usikkert hvem som sto bak, men den avanserte programvaren som ble benyttet tyder på høy kompetanse hos trusselaktøren.[28]

PSTs vurderinger peker i retning av at utenlandske etterretningstjenester vil fortsette sitt omfattende arbeid i og mot Norge også i tiden fremover. Deres mål er å få tilgang til sensitiv og skjermingsverdig informasjon, påvirke politiske, økonomiske og forvaltningsmessige beslutninger og undersøke muligheter for å kunne sabotere kritisk infrastruktur ved en eventuell fremtidig konfliktsituasjon. PST mener flere staters etterretningstjenester vil fortsette å fokusere på norsk petroleumsvirksomhet, både private virksomheter og offentlige beslutningsinstitusjoner. Etterretningstrusselen mot Norge er særlig høy fra Russland, Kina og Iran som er mer utfyllende beskrevet i kapittel 4.3.3.

Enkelte etterretningstjenester utfører informasjons-, påvirknings-, og propagandaoperasjoner i andre land for å svekke tilliten til myndighetene eller skape motsetninger, særlig i perioder med politiske spenninger. PST påpeker at dette er noe Norge også må være forberedt på.

4.3.1.2 Sabotasje

Sabotasje er et begrep som oppsto i forbindelse med de historiske arbeidskonfliktene i Frankrike. Det brukes om maktmiddel som er ment å sette produksjonsapparat ut av spill eller på annen måte sette ned produksjonstempoet. I militær sammenheng benyttes begrepet om lignende handlinger som motstandsgrupper utfører for å skade en okkupasjonsmakt eller kolonimakt, eller som medløpere og spesielt utsendte sabotører foretar i forbindelse med et angrep mot et land.[29]

I dagens sikkerhetslov § 3 nr. 4 defineres sabotasje som:

> tilsiktet ødeleggelse, lammelse eller driftsstopp av utstyr, materiell, anlegg, eller aktivitet, eller tilsiktet uskadeliggjøring av personer, utført av eller for en fremmed stat, organisasjon eller gruppering

Forståelsen av sabotasje som legges til grunn i denne utredningen skiller seg noe fra definisjonen ovenfor ved å ekskludere uskadeliggjøring av personer i form av drap og henrettelser. Uskadeliggjøring av personell kan være ett virkemiddel for å oppnå ødeleggelse, lammelse eller driftsstopp av utstyr, materiell, anlegg eller aktivitet, men å

---

[26] Lov 20. mars 1998 om forebyggende sikkerhetstjeneste (sikkerhetsloven)

[27] Lov 20. mai 2005 nr. 28 om straff (straffeloven)

[28] Per Anders Johansen, «Spionerte på Telenor-sjefer, tømte all e-post og datafiler», NRK, 17.03.2016.

[29] «Sabotasje», Det store norske leksikon, https://snl.no/sabotasje

ramme mennesker er ikke primærhensikten med sabotasje. Her skiller sabotasje seg fra terrorisme og attentater. Utvalget legger derfor til grunn følgende definisjon av sabotasje:

> Sabotasje er tilsiktet ødeleggelse, lammelse eller driftsstopp av utstyr, materiell, anlegg, eller funksjon, utført av eller for en fremmed stat, organisasjon, gruppering eller enkeltperson

Lovlig og ulovlig etterretning vil ofte være avgjørende for en vellykket sabotasjeaksjon. Med god etterretning vil det være mulig å planlegge målrettede aksjoner som vil påvirke motstanderen på ønsket måte, uten andre utilsiktede konsekvenser. Muligheten for å gjennomføre en sabotasjeaksjon vil være avhengig av tilgangen til objektet eller relevant infrastruktur. Dette kan være fysisk tilgang eller fjernaksess.

Et nylig eksempel på en sabotasjeaksjon mot kritisk infrastruktur er eksplosjonene mot strømforsyningslinjene til Krimhalvøya. I november 2015 ble strømforsyningene til Krimhalvøya, som i 2014 ble annektert av Russland, brutt som følge av at strømforsyningslinjene fra Ukraina til Krim ble ødelagt av eksplosjoner. Russiske medier hevder at ukrainske patrioter sto bak sabotasjeaksjonen som førte til unntakstilstand og at nærmere to millioner mennesker var uten strøm.[30]

Sabotasjeaksjoner mot infrastruktur og objekter kan også gjennomføres ved hjelp av digitale virkemidler. Allerede så tidlig som i 1982 ble en russisk gassledning i Sibir sprengt gjennom en digital sabotasjeaksjon. CIA hadde plantet datakoder i teknologiske komponenter i systemet som gjorde det mulig å overbelaste gassledningen til den eksploderte. Sprengningen var en del av en større aksjon gjennomført av CIA og FBI på 1980-tallet hvor formålet var å sabotere software som skulle til Sovjetunionen for å hindre overføringen av teknologi.[31] To dager før krigen mellom Russland og Georgia startet i 2008 ble rørledninger som frakter olje fra Det kaspiske hav, gjennom Aserbajdsjan og Georgia til den tyrkiske middelhavskyst, rammet av en eksplosjon. Eksplosjonen fant sted ved Refahiye i det østlige Tyrkia. Den tyrkiske regjering hevdet først at eksplosjonen skyldtes teknisk feil. Kurdistans arbeiderparti – Partîya Karkeren Kurdîstan (PKK) tok også på seg skylden for å stå bak eksplosjonen. Senere etterforskning peker derimot på at eksplosjonen ble utløst av et cyberangrep mot ledningenes kontroll- og sikkerhetssystem. Før eksplosjonen hadde hackere slått av alarmer og kuttet kommunikasjonen. Dette gjorde at ingen detektorer fanget opp at trykket i røret økte kraftig frem til rørledningen eksploderte. 60 timer med overvåkningsvideoer ble også slettet av hackere. Etterforskningen viste at det var overvåkningskameraene selv som var inngangen til systemet som hackerne hadde benyttet. Statoil var med på å bygge rørledningen og har eierandeler i ledningen.[32]

Den kanskje mest avanserte og ødeleggende cybersabotasjeaksjonen kjent så langt er Stuxnet-viruset som rammet Irans atomprogram i 2010. Viruset angrep det digitale styringssystemet og gjorde at sentrifugene for anrikning av uran spant ut av kontroll og ble ødelagt. Angrepet antas å ha satt Irans atomprogram to år tilbake i tid.[33]

4.3.1.3 Terrorhandlinger

Begrepet terror er videre og omfatter mer enn terrorisme. Terrorbegrepet har en glidende overgang mot sabotasje som i sin reneste form handler om å angripe installasjoner og objekter, snarere enn å drepe mennesker. Terrorhandlinger defineres i dagens sikkerhetslov som «ulovlig bruk av, eller trussel om bruk av, makt eller vold mot personer og eiendom, i et forsøk på å legge press på landets myndigheter eller befolkning eller samfunnet for øvrig for å oppnå politiske, religiøse eller ideologiske mål.» Denne formuleringen inkluderer både sabotasje brukt i terrorøyemed og terrorisme.

Terrorhandlinger har en politisk dimensjon fordi de er innrettet mot å påvirke styresmaktene og befolkningen gjennom å skape frykt. Ikke-statlige aktører, som terrorgrupper, forholder seg ikke til konvensjoner på samme måte som stater, og deres maktbruk er preget av en høy grad av

---

30 Morten Jentoft, «Sprengte strømmaster – to millioner på Krim uten strøm», Urix, 22.11.2015.

31 Aksjonen ble iverksatt etter at CIA fikk informasjon av en KGB-avhopper om at Sovjetrusserne over tid hadde stjålet vestlig teknologi. Avhopperen ga fra seg en liste over teknologi som var på Sovjets ønskeliste. Teknologi ble solgt til Sovjet med endrede komponenter Aksjonen ble først kjent i 1996 etter deklassifiseringen av de såkalte «Farewell Dossier» dokumentene, som var overlevert av en KGB-avhopper. Kim Zetter, *Countdown to zero Day. Stuxnet and the launch of the first digital weapon*. (New York: Crown Publishers, 2014).

32 Jordan Robertson og Michael Riley, Bloomberg Technology, «Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar», http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar (oppsøkt 03.04.2016).

33 Kim Zetter 2014.

asymmetri. Dette gjør at terrorhandlinger ofte rettes mot myke mål med lav beskyttelsesgrad, slik som sivilbefolkningen. Potensielle mål kan være kollektivtransport, kultur og idrettsarrangementer og andre store folkeansamlinger, representanter for staten, politi og beredskapspersonell eller infrastruktur med høy symbolverdi. Majoriteten av terrorangrep i 2013–2014 var rettet mot sivile og denne trenden ser ut til å øke. Etter sivile og deres eiendom var de fleste angrep rettet mot militæret, politiet, næringsliv, styresmakter og religiøse mål.[34]

De terrorhandlinger man har sett i Europa i nyere tid skiller seg fra tidligere bølger av terrorangrep fra grupperinger som IRA, ETA og RAF, som hadde som mål å fremme politiske krav, men samtidig begrense skadeomfanget for å beholde en viss folkelig støtte. Tidligere var normen at terrorgrupper hadde en nasjonal eller regional agenda. Nå er terrorisme oftere internasjonal eller global i sitt utsyn, selv om regional terrorisme vedvarer. Videre var den tradisjonelle terrorismen sjeldnere opptatt av å gjennomføre massedrap på flest mulige sivile. Noe av endringen skyldes den allmenne tilgangen på informasjon om fremstilling av eksplosiver og bomber, kombinert med den økte muligheten internett og sosiale medier gir til kontrollert formidling av bilder, film og annen informasjon fra terrorhandlinger. Dagens terrorister søker oftere større tap av liv, og simultane operasjoner for å gi inntrykk av stor slagkraft.

Samtidig har man de senere år sett flere eksempler på mindre aksjoner eksempelvis angrepene mot synagogen og Krudttønden i København (2015), det jødiske museet i Brussel og i Woolwich i London. I tillegg var 22. juli-angrepene i Norge tidenes mest brutale soloterroraksjon da det skjedde. Sett under ett ble disse gjennomført av små grupper eller enkeltpersoner som er inspirert av ulike ideologiske retninger som høyreekstremisme eller voldelig jihad. Aksjonene ble gjennomført i en tid da flere større terroraksjoner var blitt avverget av sikkerhetsmyndighetene. Det har vært en økt innsats i etterretning og mottiltak mot slike angrep, noe som også sannsynligvis har hatt en viss avskrekkende effekt. Samtidig har det i terrornettverk blitt oppfordret til soloterrorisme for å unngå å bli avslørt av etterretningsmiljøer. Effekten av terrorhandlinger går langt utover tapene av menneskeliv og materielle skader ved at handlingene skaper allmenn frykt i befolkningen og kan gjøre at styresmakter handler annerledes enn de ellers ville ha gjort.

4.3.1.4 Trusler i det digitale rom

Samfunnets økte avhengighet av IKT-baserte informasjonssystemer fører med seg alvorlige sårbarheter mot trusler i det digitale rom. Den økte avhengigheten av internett gjør at nettverksbaserte angrep kan ha omfattende skadevirkninger og har potensiale til å nå hele spekteret av norske interesser. Trusselaktører i det digitale rom inkluderer fremmede stater og ikke-statlige aktører som utfører nettverksbaserte etterretningsoperasjoner, organiserte kriminelle, hacktivister og terrorister. Metodene som benyttes blir stadig mer avanserte og målrettede.[35] I NATO benyttes Computer Network Operations (CNO) som en samlebetegnelse for Computer Network Attack (CNA), Computer Network Exploitation (CNE) og Computer Network Defence (CND). I Norge oversettes CNO med datanettverksoperasjoner, eller operasjoner i det digitale rom. Regjeringen avgjør om et cyberangrep mot Norge eller norske interesser skal anses som et væpnet angrep. Slike hendelser skal ifølge Forsvarsdepartementets cyber-retningslinjer håndteres av departementet. Forsvaret kan for øvrig gi bistand til sivile myndigheter etter anmodning i henhold til Instruks for Forsvarets bistand til politiet.

Truslene i det digitale rom handler i stor grad om informasjon: stjele informasjon, endre informasjon eller plante informasjon, eller forhindre overføring av informasjon/kommunikasjon. Truslene kan blant annet ramme store informasjonssystemer som inneholder sensitive opplysninger, kommando og kontrollsystemer for krisehåndtering og beredskap, styrings- kontrollsystemer for samfunnsviktige funksjoner og finansielle systemer. Trusselen er generell og alle digitale systemer er utsatt, men trusselen kan også rettes mot enkeltindivider eller spesifikke funksjoner/objekter.

Nettverksbaserte etterretningsoperasjoner fra fremmede stater mot offentlige myndigheter og virksomheter skjer løpende og representerer en alvorlig trussel mot viktige nasjonale sikkerhetsinteresser. Slike nettbaserte etterretningsoperasjoner kan være et kostnadseffektivt alternativ til tradisjonell spionasje. Særlig Russland og Kina er

[34] Institute for Economics & Peace, *Global terrorism index 2015: Measuring and understanding the impact of terrorism*, IEP report 36 (New York: Institute for Economics & Peace, 2015), 35.

[35] Nasjonal sikkerhetsmyndighet, *Helhetlig IKT-risikobilde 2015,* 28–30.

stater med stor offensiv kapasitet i det digitale domenet. Flere forsøk på nettverksbaserte etterretningsoperasjoner mot Norge og norske interesser har de siste årene blitt avdekket. Sommeren 2014 ble norsk olje- og energisektor utsatt for omfattende spionasjeangrep. Det er også grunn til å tro at angrep foregår uten å bli oppdaget.

Datanettverksoperasjoner er en forholdvis ny kapabilitet som kan anvendes stadig mer målbevisst og effektivt i konflikter, og flere stater har startet programmer for å utvikle slike kapasiteter. Estland opplevde i 2007 det som ofte omtales som den første cyber-krigen. Et massivt cyberangrep mot offisielle nettsider, medier og viktige nettbaserte tjenester som banker pågikk i tre uker. Cyberangrepet og demonstrasjoner i gatene var en protest mot en planlagt flytting av et sovjetisk krigsminnemonument. Virkningen av angrepet var at landets største bank måtte stenge alle nettbanktjenester og at all internasjonal nett-trafikk ble stoppet. Dette førte med seg stor økonomisk skade. Også under krigen i Georgia i 2008 ble offensive cyberkapasiteter brukt, og det har vært en markant økning i cyberangrep i forbindelse med Ukraina-konflikten. I januar 2016 ble datasystemene på Kievs hovedflyplass angrepet og det spekuleres om det var den såkalte *BlackEnergy*-skadevaren som rammet flere kraftleverandører i Ukraina i desember 2015. Dataangrepet gjorde at 80 000 personer var uten strøm i seks timer, og var i så måte banebrytende. Metoder som benyttes i cyber-angrep er ressurskrevende å utvikle og det er så langt ikke avdekket alvorlige tilfeller av at terrorgrupper bruker slike metoder. Likevel kan man ikke utelukke at cyberterrorisme kan bli en økende trussel i fremtiden, tatt i betraktning terrorgrupperingers økte bruk av internett til for eksempel planlegging av terroraksjoner og propagandaformål.[36]

4.3.1.5 Hybrid krigføring og taktikker

Kombinasjonen av fordekte forsøk på destabilisering ved bruk av indirekte og ikke-militære verktøy sammen med konvensjonell krigføring, omtales ofte som hybrid krigføring. Slik krigføring vanskeliggjør varsling og forberedelser. Hybrid krigføring kjennetegnes av nøye planlagt og koordinert bruk av et bredt spekter av konvensjonelle og ukonvensjonelle virkemidler. Dette kan inkludere bruk av umerkede regulære styrker, informasjonsoperasjoner, spesialstyrker, cyberangrep, økonomiske virkemidler og agitasjon til masseopptøyer.

Begrepet hybrid krigføring har fått fornyet oppmerksomhet etter Ukraina-krisen. Russland brukte i Ukraina et vidt spekter av metoder til å supplere konvensjonelle militære virkemidler, herunder destabilisering gjennom agenter og propaganda, informasjonskrig, cyberangrep og dramatisk øking av gassprisen. Hybridkriger inneholder en rekke ikke-kinetiske virkemidler, men uten kinetiske komponenter i bunnen vil slike taktikker i streng forstand snarere klassifiseres som destabilisering enn krigføring. Her er det imidlertid viktig å tydeliggjøre at bruk av tradisjonelle militære virkemidler kan være elementer som overhode ikke blir benyttet i de tidlige fasene av en konflikt, og avhengig av hvordan konflikten arter seg, ikke nødvendigvis vil komme til bruk. Figur 4.5 viser et eksempel på hvordan ulike virkemidler kan bli benyttet i ulike faser i opptrappingen av en operasjon for å sikre effektiv måloppnåelse.

Hybride taktikker kjennetegnes ved at det er svært vanskelig å spore og dokumentere hvem som står bak et angrep, for eksempel kan det benyttes proxy-aktører (stedfortredere). I krigshandlinger har proxy-aktører blitt benyttet gjennom å støtte opprørsgrupper, kriminelle eller andre grupper med våpen og ressurser.

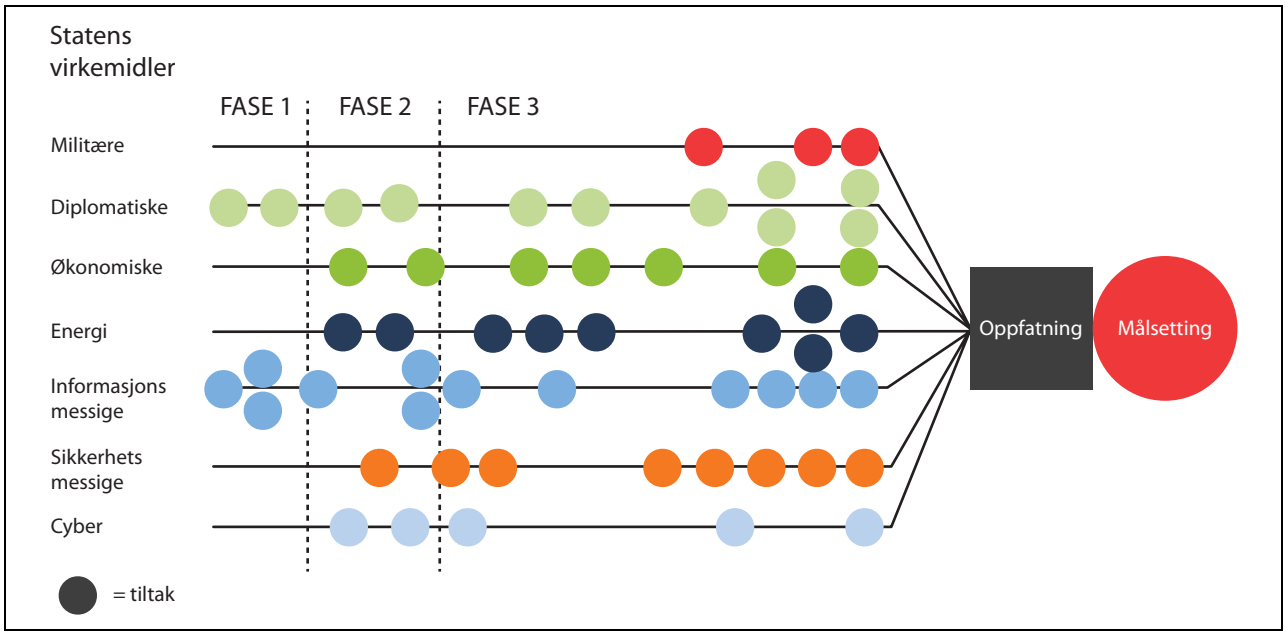
Kriminalitet og terrorisme kan inngå i irregulær krigføring for å oppnå strategiske mål. Smuglernettverk brukes også av statlige aktører for å bidra med våpen eller andre ressurser inn i konflikter. Karteller og kriminelle gjenger kan ha en voldskultur og kamperfaring som gjør dem til relevante aktører i hybrid krigføring. Bruk av ukonvensjonelle strategier, metoder, taktikker eller handlemåter gjør det vanskelig å identifisere hvilken stat som står bak.[37]

Hybride krigføringstaktikker vil kunne inneholde ulike former for fordekte operasjoner, enten hvor operasjonen selv er fordekt, eller operasjoner hvor identiteten til sponsoren bak er fordekt, for eksempel ved bruk av ikke-militært personell.

I tilfelle cyberangrep benyttes ofte front-selskaper for å gjøre det vanskelig å finne den reelle aktøren som står bak. Tyskland ble i 2015 rammet av en rekke dataangrep, blant annet mot parlamentet og telekommunikasjon- og energiselskaper. Hackerangrepene ble regnet som spionasje

[36] Nasjonal sikkerhetsmyndighet, Helhetlig IKT-risikobilde 2015, 30.

[37] Meld. St. 37 (2014–2015), *Globale sikkerhetsutfordringer i utenrikspolitikken: Terrorisme, organisert kriminalitet, piratvirksomhet og sikkerhetsutfordringer i det digitale rom*, 26.



Figur 4.5 Hybridkrig – eksempel på virkemiddelbruk.

Ved hybrid krigføring benyttes et bredt spekter av virkemidler for å oppnå en målsetting. Konflikten vil gjennomgå ulike faser der tradisjonelle militære virkemidler typisk kun vil bli benyttet dersom konflikten eskalerer.

siden formålet var å skaffe seg informasjon. Det er svært vanskelig å spore hvem som står bak slike angrep. I mai 2016 uttalte den tyske etterretningstjenesten BFV at de hadde bevis for at hackergruppene skal ha hatt tette bånd til den russiske staten. De samme gruppene skal angivelig også ha stått bak angrep mot polske statsansatte i 2014 og den franske TV-kanalen TV5. [38]

I de senere år har det særlig vært fokus på aktiv fordekt bruk av mediene som en del av krigføringen eller det sikkerhetspolitiske spillet. Det har vært antydet av Russland benyttet et stort antall personer som en del av sitt strategiske kommunikasjonsapparat under Ukraina-krisen. Russland kombinerte bruk av TV, radio, aviser og sosiale medier. De kombinerte bruk av offisiell informasjon fra statsapparatet, koordinerte informasjonskampanjer fremstilt som journalistikk og aktører som fremsto som en del av opinionen. Det ble benyttet kommunikasjonskanaler internt i Russland, men også i en rekke andre land i Europa og Nord-Amerika.

Storbritannia har gått ut med offisiell informasjon om at de har opprettet en enhet med et betydelig antall personer som skal bedrive strategisk kommunikasjon i forbindelse med meningsdannelse av britisk og andre lands opinion.

Også ikke-statlige voldelige aktører har blitt mer sofistikerte i sin mediebruk. Terrororganisasjonen Al-Qaida har i lengre tid anbefalt sine tilhengere å velge mål og taktikk som gir oppmerksomhet i media. Media, særlig TV, har vært benyttet for å spre budskap som skal skape frykt og medføre politisk press i vestlige land. Terrororganisasjonen ISIL har ytterligere basert seg på strategisk kommunikasjon for å spre sitt budskap, skape frykt, politisk press og rekruttering. Ikke-statlige aktørers bruk av mediene har imidlertid skilt seg fundamentalt fra det man har sett fra Russland ved at det først og fremst har vært tydelig kommunisert hvem som formidler budskapet, mens Russland i betydelig grad har brukt aktører fordekt som for eksempel journalister eller samfunnsengasjerte privatpersoner.

4.3.2 Dagens trusselbilde – trender og utsikter fremover

Nasjonal sikkerhet og det norske trusselbildet må ses i en internasjonal kontekst. Klare globale tendenser og markante enkelthendelser (som 9/11, 22. juli og annekteringen av Krim) har skjerpet bevisstheten om at dagens trusselbilde er et annet enn det var da dagens sikkerhetslov trådte i kraft i 2001. Nasjonale særegenheter og globale trender setter rammene for Norges sikkerhetssituasjon.

[38] Camilla Wernersen, «Beskylder russere for dataangrep i Tyskland», Urix, 13.05.2016.

4.3.2.1 Globale utviklingstrekk og strategisk stabilitet

Økende internasjonalisering gjør at globale utviklingstrekk har stadig mer å si for det nasjonale trusselbildet. Den internasjonale sikkerhetspolitiske situasjonen har blitt vesentlig endret i løpet av en relativt kort tidsperiode. Etter den kalde krigens slutt sto USA alene igjen som hegemon i en unipolar verdensorden, der fredsprosessen i Midtøsten og konfliktene på Balkan preget internasjonal sikkerhetspolitikk.

USAs internasjonale dominans har siden 90-tallet blitt svekket, samtidig som Asia har fått økt betydning både økonomisk og militært. Det strategiske spenningsnivået er høyt og tiltagende i Asia. Imidlertid inntreffer de viktigste skarpe konfliktene, som rokker global strategisk stabilitet, i randsonen av det europeiske kontinent med krigene i Irak, Libya, Syria og Ukraina som de fremste eksemplene. De siste tiårene har også en rekke svært voldelige konflikter fått eskalere dramatisk på det afrikanske kontinent. I hovedsak har de mange konfliktene i Afrika vært av begrenset betydning for norsk sikkerhet, men den negative utviklingen etter krigen i Libya, samt angrepet i In Amenas, viste at norske interesser kan rammes også i denne delen av verden.

Globalisering og internasjonalisering øker kontakten, sårbarheten og avhengigheten på tvers av landegrenser. Ikke-statlige aktører, som organiserte kriminelle nettverk og terroristgrupper, har alltid hatt en sentral rolle i det internasjonale sikkerhetsbildet. Flere steder foregår det en økende omfordeling av makt til disse aktørene på bekostning av statlige aktører på måter som påvirker den sikkerhetspolitiske situasjonen i Vesten i negativ retning (se kapittel 4.3.4.2). Svake stater, manglende internasjonalt samarbeid for å bekjempe fremveksten av internasjonale trusselnettverk, godt hjulpet at den teknologiske utviklingen som bidrar til å forenkle samhandling over store avstander, er avgjørende faktorer for denne utviklingen. For eksempel i Somalia, Syria og Irak, har ikke-statlige aktører styrket sin maktposisjon slik at myndighetenes suverenitet mer eller mindre har brutt sammen. Denne omfordelingen av makt gjør at ikke-statlige aktører får større spillerom for å utøve ulike former for makt, og i større grad får mulighet til å påvirke den internasjonale dagsorden.

Den globale teknologiutviklingen er et gode som samtidig fører med seg noen alvorlige og grenseoverskridende utfordringer. Trusselaktører i det digitale rom inkluderer fremmede stater og ikke-statlige aktører. Metodene som benyttes blir stadig mer avanserte og målrettede. Den økte avhengigheten på tvers av land og sektorer gjør at nettverksbaserte angrep kan ha omfattende skadevirkninger. Disse utviklingstrekkene har ført til et mer sammensatt og mindre forutsigbart trusselbilde. Denne usikkerheten er trolig et vedvarende trekk.

4.3.2.2 Norges særegenheter

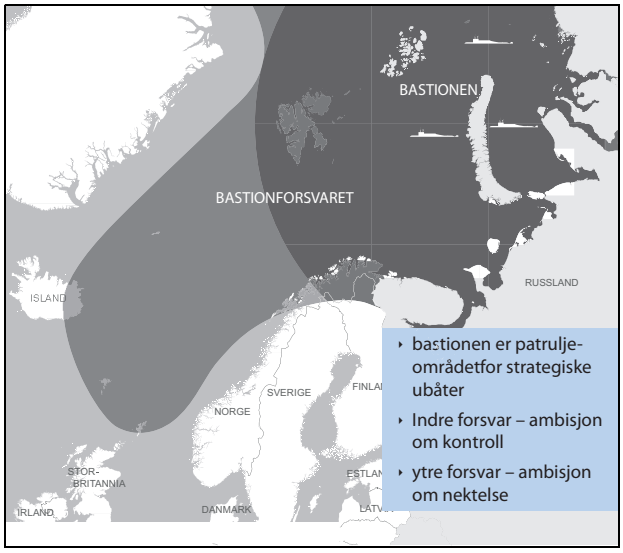
Som en småstat er Norge avhengig av avtaler og samarbeid med andre stater. NATO-medlemskapet spiller en nøkkelrolle i norsk sikkerhetspolitikk. Norge er avhengig av alliert støtte også i fremtiden, men denne støtten kan bli mer usikker ved at det amerikanske lederskapet er svakere enn før. Med manglende bidrag fra europeiske land har man en vedvarende ubalanse i byrdefordelingen internt i NATO. For å opprettholde alliert vilje til å bistå vil Norge også i fremtiden komme til å måtte vise innsatsvilje gjennom internasjonale bidrag.

Det er også en politisk målsetting for Norge å fremme fred og føre en engasjementspolitikk på felter som utvikling, bistand, miljø, multilateralisme og menneskerettigheter.

Norges rike tilgang på naturressurser er et annet kjennetegn som påvirker Norge som internasjonal aktør. Norge er den nest største eksportøren av gass til det europeiske markedet, etter Russland. Norsk eksport av gass dekker rundt 20 % av det europeiske forbruket. Norges rolle som strategisk energileverandør gir mer tyngde internasjonalt samtidig som det gjør landet mer sårbart og eksponert for konflikter i fjerne områder enn tidligere. Trusselen mot norsk energiproduksjon avhenger av den internasjonale situasjonen. Sikkerhetsutfordringene øker i perioder med konflikt i vårt område og i andre områder i verden hvor Norge, NATO eller mottakere av energi fra Norge er involvert. Hensikten bak potensielle angrep kan være å yte press mot Norge eller andre land som er avhengig av energi fra Norge. Å kontrollere tilgangen til energi er et maktpolitisk virkemiddel, slik Russland har illustrert ved flere ganger å skru av gasstilførselen for å øve politisk press. Angrep kan altså komme som et resultat av konflikter der Norge i utgangspunktet ikke er involvert,[39] slik vi så i In Amenas-angrepet i 2013 hvor fem Statoil-ansatte mistet livet.

---

[39] NOU 2000: 24 *Et sårbart samfunn – Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet*, 73.



Figur 4.6 Russlands bastionforsvar.

Kilde: Ekspertgruppen for forsvaret av Norge, *Et felles løft*, 2015.

Norge er en kyststat med havområder som er syv ganger større enn landområdet. Norge har en internasjonalt ledende maritim næring med skipsfart og eksport av fisk og petroleum blant våre viktigste inntektskilder. Dette bidrar til å gjøre nordområdene til Norges viktigste strategiske ansvarsområde. En hjørnestein i norsk nordområdepolitikk er å jobbe for at nordområdene forblir en region preget av stabilitet og lav spenning.

Svært viktig i Norges geopolitiske kontekst er nærheten til Russland. Naboskapet til Russland har alltid vært et asymmetrisk forhold. Konseptet bastionforsvaret står sentralt i russisk sikkerhetspolitikk i nordområdene. Dette innebærer at deler av norsk territorium er bak Russlands definerte forsvarslinje. I en periode hvor Russland forsøker å gjenreise seg som stormakt, og øker sitt fokus mot nordområdene, er dette foruroligende for Norge og våre allierte.

Våre omgivelser er stadig i endring og det er ikke nødvendigvis de hendelser som i dag preger nyhetsbildet og folks bevissthet som vil vise seg å ha størst konsekvenser på lang sikt. Det er derfor viktig å skille mellom dagsaktuelle hendelser og langsiktige trender. Med dette i bakhodet er det likevel viktig å se på generelle utviklingstrekk for å få indikasjoner på hvilke endringer som kan inntreffe, og med hvilken grad av sannsynlighet det vil kunne skje. Dette kan danne utgangspunkt for en vurdering av hvilke trusler fra statlige og ikkestatlige aktører som vil ha betydning for det nasjonale sikkerhetsbildet fremover. De neste kapitlene vil ta for seg hvilke trusler Norge står overfor i dag og i tiden fremover.

4.3.3 Trusler i form av statlige aktører

Etterretningstjenesten og PST er samstemt om at det i dag ikke er noen konkret overhengende trussel om væpnet angrep mot Norge fra statlige aktører. I henhold til Etterretningstjenesten er det stater som i dag har kapasitet til å ramme Norge militært, men det er ikke kjent at noen av de aktuelle statene har en intensjon om å angripe Norge. Globale utviklingstrekk og maktforhold er likevel førende for den nasjonale trusselsituasjonen, og følges derfor tett.

Etterretningsvirksomhet mot Norge og norske interesser skjer imidlertid i stor utstrekning. Dette er rettet mot norske myndigheter og mot private virksomheter. Etterretningsvirksomhet har blant annet til formål å kartlegge sårbarheter i det norske samfunnet, kartlegge militære kapasiteter og andre beredskapsressurser. Kjennskap til statlige militære kapasiteter kan fungere som strategiske virkemidler for å legge press på et annet land, gjennom å lamme viktige funksjoner. Det foregår også utstrakt aktivitet for å tilegne seg kunnskap og teknologi som staten og private aktører besitter. Slik aktivitet kan ha som formål å skaffe informasjon om hvordan viktige funksjoner kan rammes i en potensiell konfliktsituasjon, samt å styrke eget lands næringsutvikling og konkuranseevne. Slik etterretning kan ramme verdiskapingspotensialet.

Av de statlige aktørene som aktivt utfører spionasje mot Norge fremhever E-tjenesten og PST Russland, Kina og Iran i sine åpne trusselvurderinger. Disse landene vil bli diskutert under – både i lys av landenes generelle samfunnsutvikling og i lys av landenes etterretningsvirksomhet.

4.3.3.1 Russland

Daværende sjef for etterretningstjenesten Kjell Grandhagen oppsummerte nylig utviklingen i Russland som følger:

> Vi har sett et Russland gjennom det siste året som er villig til å bruke militær makt når de vurderer at vitale interesser står på spill. Vi ser et Russland som utvikler seg mer og mer i en autoritær retning, og tar et sterkere grep om mediene, et sterke grep mot en mulig liberal opposisjon. Vi ser en beslutningskrets rundt presidenten som blir smalere og smalere, og mer og mer preget av mennesker med hans

> samme bakgrunn. Det er et Russland i økonomisk krise og med langsiktig dårlig økonomiske utsikter. Og samtidig et Russland som til tross for dette velger å bruke mye mer av de ressursene de har på en militær opprustning. I sum er dette et bilde som leder mot større usikkerhet og større uforutsigbarhet i forhold til hva slags Russland Norge må forholde seg til i de kommende tiårene.[40]

Etter Sovjetunionens fall gikk Russland inn i en reorienterende fase. Det nye Russland måtte finne ut hvordan det skulle forholde seg til omverden. Etter en periode preget av oppmykning overfor Vesten, gikk russisk utenrikspolitikk etter hvert over i en mer konfronterende linje. En stadig mer sammensatt og offensiv russisk utenrikspolitikk under Putin har endret den sikkerhetspolitiske situasjonen i Europa og økt konfliktpotensialet. Særlig tilbakekomsten av mellomstatlig væpnet konflikt i Europa ved Russlands folkerettsstridige annektering av Krim var en oppvekker. Gjennom annekteringen av Krim og støtte til separatister i Øst-Ukraina har Russland demonstrert både evne og vilje til å bruke militær makt for å oppnå sine politiske mål. Russlands utenrikspolitiske linje har både elementer av kontinuitet og endring. Ønsket om innflytelse over tidligere Sovjet-republikker er ikke noe nytt, noe vi så under krigene i Georgia og Tsjetsjenia.

Etter Putins tilbakekomst som president i 2012 har det vært en dreining mot økt patriotisme og konservatisme i russisk politikk.[41] Ønsket om å gjenreise Russland som stormakt står sentralt i Putins prosjekt. Den stadig mer autoritære dreiningen har særlig rammet pressen og intern opposisjon hardt. Russland opplever en kraftig økonomisk nedgang. Blant årsakene er strukturelle faktorer som høy korrupsjon, dårlig investeringsklima og høy avhengighet av olje kombinert med vedvarende fall i oljeprisen.

Også de økonomiske sanksjonene i kjølvannet av Ukraina-konflikten har ytterligere forverret den økonomiske situasjonen i Russland. Den nedadgående økonomiske utviklingen nasjonalt sammenfaller med en mer opportunistisk utenrikspolitikk både i nærområdene rundt Kaukasus og i Syria-konflikten. Med opportunistisk menes her at man agerer hurtig, griper de sjanser som byr seg, og er tilpasningsdyktig til hendelsenes forløp og motpartens handlinger. Putins begrensede evne til å bedre den økonomiske nedgangen i Russland gjør at vi kan frykte en fortsatt autoritær tilstramning og en fortsatt opportunistisk utenrikspolitikk fremover. Putins uforutsigbare manøvre er ytterligere urovekkende dersom landet skulle gå inn i en enda dypere økonomisk krise. Den fremtidige økonomiske utviklingen i Russland kan ha stor betydning for den norske og europeiske sikkerhetspolitiske situasjonen.

Russisk militær tilstedeværelse i Midtøsten spiller en viktig rolle i å fremme Russlands stormaktsposisjon internasjonalt og motvirke vestlig innflytelse i internasjonal poltikk. Både annekteringen av Krim og Putins militære støtte til Assadregimet i kampen mot ISIL har stor støtte i befolkningen og har økt Putins popularitet. Den stadig mer offensive utenrikspolitikken Russland fører blir legitimert på hjemmebane gjennom offisiell russisk retorikk basert på fiendebilder om Vesten som formidler oppfatningen om Russlands offerrolle i møte med ytre fiender. Særlig NATO fremstilles svært negativt i russisk retorikk. Mistillitsforhold mellom Russland og Vesten kan potensielt vare lenge.

Etter krigen i Georgia begynte Russland en omfattende forsvarsreform som inkluderte en markant militær opprustning. Den militære opprustningen har resultert i en mer mobil militær organisasjon med utvidet rekkevidde og en atskillig raskere reaksjonsevne. Det har skjedd en modernisering av viktige våpenplattformer, kommando og kontrollsystemer, effektivisering av logistikksystemene og en styrkeproduksjon som gir Russland en kampkraft på et helt nytt nivå. Gjennom krigshandlinger i Ukraina og militær tilstedeværelse i Syria har Russland demonstrert hvordan deres moderniserte militærmakt er anvendbar til å støtte opp under utenrikspolitiske målsettinger. Særlig under Ukraina-konflikten benyttet Russland et bredt spekter av statlige virkemidler i et omfang og med en koordinering som fremstår som det beste eksempel på hybrid krigføring verden har sett. Dette øker viktigheten av et solid og gjennomtenkt forebyggende sikkerhetsarbeid.

Det russiske militæret øver hyppigere enn tidligere, blant annet i Norden og Østersjøområdet. Flere tilfeller av grensekrenkelse i luftrommet over Sverige, Finland og Baltikum har funnet sted samt utstrakt flyvning over Norskehavet og Nordsjøen nært norsk luftrom. Til tross for en mer offensiv russisk utenrikspolitikk har norske styresmakter gjentatte ganger understreket at de

---

[40] Sitat fra Etterretningstjenestens sjef Generalløytnant Kjell Grandhagens under hans tale «Trusler og risiki for Norge i et endret sikkerhetsbilde», NSMs sikkerhetskonferanse 2015, Oslo Kongressenter, 16.03.2015.

[41] Etterretningstjenesten, *Fokus 2015: Etterretningstjenestens vurdering*, 11.

ikke ser på Russland som en direkte militær trussel mot Norge. Uannonsert aktivitet i eller nært andre staters sjø- eller luftrom er likevel foruroligende og øker faren for misforståelser og ulykker.

Nordområdene er en viktig arena for Russland av både økonomiske og strategiske årsaker. I Russlands Arktis-strategi fra 2009 er Arktis definert som landets viktigste fremtidige ressursbase.[42] Smeltingen av polisen i Arktis gjør at større områder er tilgjengelig sommerstid for skipsfart, fiske og turisme langs Nordøstpassasjen. Russland har gjennom ulike tiltak markert sin interesse i Arktis, blant annet gjennom etableringen av den arktiske militære kommandoen 1. desember 2014. Russland har også gjenåpnet tidligere baser, samt opprettet nye baser i Arktis.[43] Å opprettholde sitt nærvær på Svalbard anses som viktig for Russland, særlig av militærstrategiske årsaker. Det kan ikke utelukkes at Russland i en gitt situasjon vil treffe militære eller andre tiltak for å ivareta russiske interesser på eller rundt Svalbard. Selv om samarbeidet med vår nabo i øst fremdeles anses som godt, har tilliten til Russland blitt påvirket i negativ retning etter blant annet Ukraina-krisen. Norges deltakelse i de internasjonale sanksjonene mot Russland, og Russlands motsvar på sanksjonene bidrar også til et mer sårbart og utfordrende samarbeidsklima.

Den spente relasjonen mellom NATO og Russland for tiden må ses i sammenheng med den stadig økende etterretningstrusselen. Ved siden av tradisjonelt menneskebasert innhenting pågår og en økt bruk av digitale hjelpemidler for å drive innhenting mot sensitive kommunikasjonsplattformer. Digital spionasje gir høyt etterretningsutbytte og utføres i stort omfang mot Norge og norske interesser.

I sin vurdering av etterretningstrusselen mot norske interesser mener PST at Russlands intensjon og kapasitet har størst skadepotensial. Det er flere forhold som gjør Norge til et interessant etterretningsmål. Norge besitter store naturressurser og har en strategisk viktig plassering. Norge representerer NATOs nordlige grense mot Russland og russisk etterretning søker derfor kunnskap om NATOs militære kapasiteter og aktiviteter blant annet fra norske kilder. Beslutninger i Norge og NATO fattet på bakgrunn av Ukrainakonflikten vil fremover være av særlig interesse for Russisk etterretningstjeneste. Slik informasjon kan styrke Russland militært og kan svekke norske og alliertes sikkerhetspolitiske interesser.

PST mener Russlands kontinuerlige kartlegging av norske forsvars-, sikkerhets- og beredskapskapasiteter har som formål å legge til rette for russiske militære disposisjoner i en eventuell endret sikkerhetspolitisk situasjon i fremtiden. Slik virksomhet kan i verste fall kunne true Norges territorielle kontroll og andre nasjonale interesser.

Mange borgere med tilknytning til Russland jobber i dag i sektorer med tilgang til sensitiv og skjermingsverdig informasjon. Disse er særlig utsatt for rekrutteringspress fra hjemlandets etterretningstjenester. Der dette lykkes, har det et stort skadepotensiale.

4.3.3.2 Kina

De siste årene har det vært en dreining i maktbalansen mot Asia. Verdensøkonomiens tyngdepunkt har beveget seg fra Vesten mot Asia. Kina har i dag verdens nest største økonomi, mens Japan er på tredjeplass. Den økonomiske veksten i Asia er som all økonomisk vekst reversibel. Samtidig er det et faktum at veksten har ført til økte forsvarsbudsjetter. I 2013 gikk de samlede forsvarsutgiftene i Asia og Stillehavsområdet forbi Europas.[44] Den militære maktbalansen preges og av at seks av verdens ni atomvåpenstater ligger i Asia.

Kinas president Xi Jinpings visjon for Kina er å gjenreise Kina som en mektig nasjon tuftet på sterk økonomi og en sterk militærmakt. Likesom i Russland ser man sterke nasjonalistiske strømminger i Kina og en mer selvhevdende utenrikspolitikk. Xi Jinpings ledelse går i en autoritær retning som slår hardt ned på opposisjon og har ført til innskrenkninger i ytringsfriheten, for eksempel ved økt internettsensur.

Kina og Russland har inngått et strategisk partnerskap i motvekt til Vesten, som blant annet inkluderer tidvis samarbeid i FNs sikkerhetsråd og økt handel. Kina og Russland har også felles militære øvelser som har blitt stadig større. Det er allikevel klare begrensninger for samarbeidet skyldt langvarig historisk mistro.

Kinas forsvarsbudsjett var på 790 milliarder norske kroner i 2014. Med dette har Kina det nest største forsvarsbudsjettet i verden etter USA. Kina investerer stort i digital krigføring.[45] Det er særlig i det digitale rom at Kina er av betydning for norsk

[42] Ibid. 23.
[43] Ibid., 2.
[44] Ibid., 50.
[45] Ibid., 58.

sikkerhet. Sammen med Russland er Kina en av de statene som er mest aktive bak nettverksbaserte etterretningsoperasjoner rettet mot Norge.[46] Kina har god evne og høy vilje til å gjennomføre cyber-operasjoner, og står bak digital spionasje i stort omfang. Landet retter særlig sin virksomhet mot høyteknologiske mål, herunder energi, maritim sektor og rombasert virksomhet. Mer tradisjonell etterretningsvirksomhet mot utenriks- og forsvarsektoren er også utbredt.[47]

Nettverksbaserte etterretningsoperasjoner er, sammen med terror, den mest alvorlige, akutte trussel mot norske interesser ifølge daværende sjef for Etterretningstjenesten, Kjell Grandhagen. Norske myndigheter og samfunnskritiske virksomheter blir fortløpende utsatt for fremmed etterretning fra Kina og andre.

4.3.3.3 Iran

Frykten knyttet til ambisjonene bak Irans atomprogram har tatt stor plass på den internasjonale dagsorden siden 2003. Flere runder med forhandlinger har funnet sted og resulterte i en atomavtale mellom Iran og P5+1 sommeren 2015. Avtalen går ut på at Iran skal begrense sin bruk av høysensitiv teknologi, ruste ned sin kapasitet til å anrike uran, redusere sitt lager med anriket uran, samt å gi Det internasjonale atomenergibyrået (IAEA) større innsyn i atomprogrammet. I bytte mot dette vil gradvis økonomiske sanksjoner mot Iran oppheves. Avtalen eliminerer ikke trusselen fra Iran, men vil redusere Irans mulighet til å utvikle kjernefysiske våpen og forlenge tiden det eventuelt ville ta.

Atomavtalen har ikke ført til færre skjulte anskaffelsesforsøk mot norske virksomheter.[48] Iran er en av hovedaktørene bak ulovlige og fordekte forsøk på anskaffelse av teknologi og kunnskap som kan benyttes til sitt atomprogram fra Norge. Slike ulovlige anskaffelser er en trussel både mot norske og alliertes interesser. Etterspørselen øker særlig etter flerbruksteknologi som ikke er underlagt eksportkontroll, men som i modifisert tilstand kan benyttes til å utvikle masseødeleggelsesvåpen. Dette øker risikoen for at enkeltbedrifter kan bli fristet til å utnytte situasjonen og selge slik teknologi for profitt, eller at bedrifter uten intensjon bidrar til at teknologien havner i feil hender fordi de ikke har et bevisst forhold til flerbrukspotensialet i teknologien de besitter. Anskaffelser knyttet til masseødeleggelsesvåpen går ofte gjennom mange land, slik at det er vanskelig å spore hvor teknologien ender opp, for eksempel gjennom bruk av stråmenn og selskaper som proxy-aktører. Særlig utsatt for anskaffelsesforsøk er forsvarsindustri, bedrifter som selger nisjeteknologi, og høyteknologiske bedrifter i olje- og gassektoren.

Også norske utdanningsinstitusjoner opplever stor pågang fra iranske studenter på utdanningsretninger som kan gi kunnskap som gagner det iranske atomprogrammet. Ved et strengere eksportregime blir det viktigere for Iran å selv produsere egen teknologi, norske utdanningsinstitusjoner kan derfor fremover forvente tiltagende påtrykk.[49]

4.3.4 Trusler fra ikke-statlige aktører

4.3.4.1 Terrorisme

Forskningen på terrorisme er delt i hvem som kan regnes som de første terrorister. Mange mener Feynianske voldelige dissidenter på 1800-tallet eller Russlands Navrodniker som drepte Tsaren er de tidligste terrorister i tråd med en moderne forståelse av begrepet. Anarkister og IRA tidlig på 1900-tallet trekkes også ofte fram. De lærde strides altså om terrorismens opprinnelse. Det er derimot bred enighet om at terrorisme som fenomen har endret seg fra 70-tallet og fram til i dag. 70-tallet regnes som tiåret da terrorismen for alvor ble internasjonalisert, med angrepet mot israelske utøvere i OL i München i 1972 som et av de tydeligste eksemplene. Tyskland slet også med hjemlige terrorister i Baader-Meinhof gruppen. Resultatet ble at Tysklands moderne anti-terror styrker ble toneangivende gjennom opprettelsen av Grenzschutzgruppe 9 (GSG9).

Utover på 80- og 90-tallet ble terrorismen stadig mer dødelig og operasjonene økte i kompleksitet. Hizbollahs bilbombing av forlegningene til franske fallskjermjegere og US Marines i Beirut i 1983, samt bombingen av Pan Am flight 103 over Lockerbie i 1986, er eksempler på dette med henholdsvis rundt 270 og 305 drepte. Al-Qaidas største terroranslag forut for 9/11-angrepene var mot amerikanske ambassader i Nairobi og Dar-es-Salam med rundt 224 drepte. Disse bombene sammen med angrepet mot USS Cole, i Adens havn i år 2000, utgjør opptakten til 9/11. De ovenfor nevnte angrepene er eksempler på spesielt dødelige angrep i terrorismens historie frem til 9/

[46] Politiets sikkerhetstjeneste, *Trusselvurdering 2015*.
[47] Ibid., 84.
[48] PST, *Trusselvurdering 2015*.
[49] Ibid.

11-angrepene. Disse drepte opp mot 3000 mennesker og sprengte skalaen fullstendig.

Det samme gjelder den statlige responsen på angrepet som ble voldsom ettersom krigen mot terror inkluderte storstilte bakkekriger både i Afghanistan og Irak. I tiåret etter 9/11-angrepene var USAs krig mot terror det rådende paradigme som la føringer på mye av samhandlingen på den globale storpolitiske arena. Utover i Obamas presidentperiode avtok fokuset på terrorisme noe. Med terrorangrepene i Paris og Brussel i 2015 og 2016, samt ISILs eksport av terrorisme til Europa, synes det avtagende fokus på terrorisme mot Vesten å opphøre.

Å definere terrorisme er krevende fordi begrepet er sterkt politisert samtidig som det er svært negativt ladet. Terrorisme er en praktisk retorisk etikett å feste på sine fiender. En akademisk definisjon av terrorisme må beskrive hvem som utøver terrorisme, hvem som rammes, og hvilken målsetting og effekt terroristene ønsker å oppnå. Legaldefinisjoner oppfyller en annen funksjon da de også må fungere godt som redskaper i rettsforfølgelse etter straffeloven. Fire ord oppsummerer essensen i fenomenet terrorisme: vold, politikk, frykt og strategi. Terrorisme er en fryktspredende, voldelig politisk strategi. Går man mer i dybden kan terrorisme forstås som «en ikke-statlig aktørs strategiske bruk av vold – eller trusler om vold – mot sivile eller ikke-stridende med den hensikt å spre frykt, skaffe oppmerksomhet om en politisk sak og å påvirke også andre enn de direkte ofrene for anslaget.»[50]

I dette ligger det at stater som angriper sivile ikke defineres som terrorister, men snarere begår krigsforbrytelser, forbrytelser mot menneskeheten, fordekt krigføring eller en form for statsterror. Videre er motivene til terrorister klarlagt som politiske, i tillegg til det å spre frykt og å påvirke både befolkninger og styresmakter.

Terrorisme representerer i de fleste tilfeller en krigserklæring mot samfunnet. Både Osama bin Laden og Anders Behring Breivik har utstedt krigserklæringer mot USA og Norge. Terrorisme forekommer i ulike sjatteringer fra det alvorligste av kriminalitet til lavintensitets asymmetrisk krigføring. Terroristangrep er innrettet mot midlertidig å omdanne det sivile samfunn til en krigssone, og utgjør dermed en av de mest alvorlige trusler mot samfunnssikkerheten.

Terrorismens logikk kombinerer fortid og fremtid for å spre frykt i nuet. Den er forankret i demonstrert evne til å gjennomføre dødelige angrep, kombinert med uttalt vilje til nye anslag i fremtiden. Slik sprer terrorister frykt i samfunnet. Terrorkampanjer må forstås som langt mer enn kalde fakta rundt antallet døde og skadede. Det er verdt å merke at terroristers sjokkerende voldsbruk har stått i mindre kontrast til staters voldsomme maktbruk i tidligere tider. Så sent som i andre verdenskrig var bombing av sivilbefolkning, for å knekke krigsmoralen og kampviljen, i tråd med militær doktrine både på alliert og aksemaktenes side. Etterkrigstiden brakte med seg en reaksjon mot dette gjennom Geneve-konvensjonene og annen internasjonal lovgivning om krigens folkerett.

Ettersom terrorisme inntreffer i grenselandet mellom krig og kriminalitet utgjør fenomenet en alvorlig trussel mot fred og sikkerhet. Antallet drepte i terrorangrep har blitt mer enn femdoblet siden 2000. Terrorangrepet 22. juli viser at Norge ikke er skånet mot terrorisme. Terrortrusselen fra ekstrem islamisme mot Norge og norske interesser anses som skjerpet og økende gjennom 2015. I tillegg kan økt fokus på militant islamisme, kombinert med konflikten og flyktningestrømmen fra Syria potensielt trigge fremmedfiendtlig hatkriminalitet helt opp til skarpe terrorhandlinger. Etterretningstjenesten peker og på militant islamisme som den mest alvorlige terrortrussel mot Norge og norske interesser.[51] Denne trusselen er særlig knyttet til hjemvendte fremmedkrigere som har fått kamperfaring fra Syria og Irak.[52]

I de senere år har det vært eksempler på at grupperinger som oppfattes å være terrororganisasjoner har tatt kontroll over større landområder. Fremveksten og ekspansjonen av Den islamske staten i Irak og Levanten (ISIL) er et særlig foruroligende eksempel. ISIL opererer per i dag som en selvfinansierende pseudo-stat drevet av en geriljagruppe. Gruppen skiller seg også fra andre terrorgrupperinger ved å ha en særlig bred global appell. Spesielt gjennom bruk av sosiale medier har ISIL lykkes i å redefinere internasjonal jihadisme til noe mer «trendy» som når ut til mange unge. Den selverklærte kalifen har også styrket statusen og hatt samlende effekt for sympatisører i ekstreme islamistiske miljøer verden rundt. Grupper fra Algerie, Libya, Egypt, Saudi-Arabia og Jemen har tilsluttet seg ISIL.

[50] Anders Romarheim, «Hva er terrorisme?», i Anders Ravik Jupskås (red.), Akademiske perspektiver på 22. juli (Oslo: Akademika, 2013), 36.

[51] Etterretningstjenesten, *Fokus 2015*, 73.

[52] PST, *Trusselvurdering 2015*.

Et stort antall fremmedkrigere fra rundt 90 land har dratt til Syria og Irak, inkludert fra Norge. Vi står i dag derfor overfor en trussel som kommer både utenfra, i form av fremmedkrigere som returnerer og innenfra i form av radikaliserte som kan la seg inspirere av ISILs oppfordring til voldelige handlinger. De store områdene styrt av ISIL benyttes til trening og planlegging av angrep mot mål i Europa. Paris-terroren november 2015 er et eksempel på et angrep med klare forgreininger til Syria. Treningen, kamperfaringen og indoktrineringen fremmedkrigere får mens de er i Syria og Nord-Irak utgjør en stor trussel når de vender hjem. Returnerte fremmekrigere vil trolig ha en lavere terskel for voldsbruk i Norge. Det er imidlertid viktig å påpeke at flertallet ikke vil utgjøre noen trussel ved hjemkomst.

Også andre grupperinger, ikke minst Al-Qaida-nettverket, forblir en betydelig terrortrussel mot vesten. Nettverket har intensjon og kapasitet til å gjennomføre terrorangrep i vestlige land.

Stor etterretningsinnsats mot terroraktører har likevel gitt betydelige resultater, og ført til at terrororganisasjoner må opptre med forsiktighet dersom de skal unngå å bli avslørt før de får utrettet sine aksjoner. Dette er en årsak til den endring i taktikk som har vært synlig i Europa i de senere år der soloterrorisme utført med relativt enkle midler har blitt hyppigere. Denne type terrorisme er vanskelig å avdekke og forebygge. Det har også vært en tendens til koordinerte angrep som rammer flere mål samtidig, eller suksessivt. Ekstreme islamister har i løpet av 2015–2016 utført en rekke voldelige angrep i Europa med angrep i Paris, Brussel og Nice som de mest alvorlige.

4.3.4.2 Svake stater som arnested for terrorisme

Svake og sårbare stater kjennetegnes ofte av nylig avsluttede eller pågående væpnede konflikter, et svakt statsapparat, manglende respekt for menneskerettigheter, høy korrupsjon og manglende rettshåndhevelse kombinert med fattigdom. Slike stater gir grobunn og stort spillerom for terrornettverk og annen organisert kriminalitet. Et særlig foruroligende eksempel er ISIL, som har lykkes i å skaffe seg kontroll over store landområder i Irak og Syria og opprettet en pseudo-stat. Sommeren 2016 mistet de dog betydelige landområder.

Et annet eksempel er den militante islamittiske gruppen Boko Haram som i august 2015 erklærte dannelsen av et kalifat i Nord-Nigeria. Terroristgruppen har i dag kontroll over et landområde på størrelse med Belgia. Gruppen er blant verdens mest dødelige og har erklært troskap til ISIL.[53] Boko Haram har som målsetting å fjerne den nigerianske regjering og innføre Sharia-lovgivning. Angrepene er hovedsakelig rettet mot offisielle institusjoner og personer, politiet og sikkerhetstyrkene.[54] Terrorgruppen finansierer i hovedsak sin virksomhet med penger fra bankran, kidnapping og innkreving av skatter i områdene de besitter. Mye tyder også på at penger fra piratangrepene langs Nigerias kyst ender opp hos Boko Haram. Nigeria er preget av et autoritært styre, høy korrupsjon, med høyt konflikt- og voldsnivå mellom etniske og religiøse grupper, og mellom sentralmyndighetene og de 36 delstatsguvernørene. Det svake statsapparatet og manglende rettshåndhevelse har gjort at Boko Haram har fått en sentral maktposisjon i landet.

Også i Afghanistan har ulike opprørsgrupperinger betydelig makt i store områder. Etter avviklingen av ISAF og uttrekningen av koalisjonsstyrkene har utviklingen vært negativ for landet. Taliban har erobret stadig større områder. Al-Qaida har re-etablert treningsleirer og ISIL har fått fotfeste og er i stadig fremgang i flere distrikter. Det er også et stort antall mindre mindre grupperinger som i ulik grad samarbeider. I dag foregår det en viss rivalisering mellom Taliban, ISIL og Al-Qaida i Afghanistan.

I Mali tok The Movement for Oneness and Jihad in West Africa (MOJWA) i 2013 kontroll over nordlige landområder i forsøk på å innføre et strengt islamittisk styre. De fikk raskt kontroll over større områder ved å inngå et samarbeid med den lokale Tuareg-befolkningen som var i opposisjon til myndighetene i Mali. Frankrike deltok militært i en motoffensiv som tok tilbake kontrollen over de fleste islamist-okkuperte områdene.[55]

Et siste eksempel der en svak stat har ført til store sikkerhetsutfordringer internasjonalt er Somalia. Landet har lenge vært regnet som kroneksempelet på en *failed state*. Al-shabaab og et stort antall voldelige kriminelle grupperinger med inntekter fra blant annet piratvirksomhet og menneskehandel har utnyttet dette maktvakuumet og spredd død og ustabilitet også utover landets grenser. Terrorangrepet mot Westgate-kjøpesen-

---

53 Institute for Economics & Peace, 2015, 5.

54 Emilie Oftedal, *Boko Haram- an overview*, FFI-rapport 01680 (Kjeller: Forsvarets Forskningsinstitutt, 2013).

55 Angrepet på Statoil-anlegget i In Amenas samme år anses blant annet som en hevnaksjon på den franske intervensjonen.

Boks 4.2 Radikalisering og deradikalisering

Terroristgrupper i Europa rekrutterer blant vanlige mennesker i det sivile samfunn. Når en person beveger seg fra å ha ekstreme meninger til å ville sette vold bak politiske krav og prosjekter, er vedkommende blitt radikalisert. Radikalisering kan defineres som «en prosess, der en person i økende grad aksepterer bruk av vold for å oppnå politiske, religiøse eller ideologiske mål.» (PST 2015). Prosessene som leder til radikalisering er mange og til dels ulike.

Samfunnets forebyggende arbeid mot terrorisme er helt avhengig av innsikt i radikalisering og deradikalisering. Forebyggende arbeid er både vanskelig og tidkrevende. I tillegg er resultatene tilnærmet umulig å anslå og dokumentere. Allikevel er dette noe av det viktigste arbeidet man kan gjøre for å bedre samfunnssikkerheten, og all sikkerhetslovgivning bør derfor ivareta det preventive aspekt. Det er dessverre slik at et konfronterende statsapparat, gjennom tiltak og lovgivning, kan støte ungdom som er i faresonen unna og bekrefte deres forestilling om eksklusjon fra det norske samfunnet.

Petter Nesser (2015) beskriver fire typiske roller som fylles i jihadistiske terrorgrupper i Europa. Disse er *entrepenøren*, *protegen*, *drifters* og *misfits*. De fleste terrorceller har en *leder/entreprenør* som knytter cellen opp mot internasjonale terroristnettverk. Under lederen står en *protege* som er nestkommanderende. Disse to funksjonene innehas oftest av personer med sterk ideologisk overbevisning og de har oftere høyere sosial kapital enn andre gruppemedlemmer, slik som utdanning. På bakkenivået finner vi søkende *drifters*, som gjerne eksperimenterer med ulike voldelige miljøer/gjenger før de lander mer permanent i en terrorgruppe. I tillegg har man de sosiale utskuddene *misfits* som tenderer til å ha en kriminell fortid. Disse kan søke til terrorgrupper av mer personlige grunner og har ofte en svakere ideologisk overbevisning. De kan være eventyrere på søken etter sosial tilhørighet. For denne typen terrorister vil voldsforherligelse være en viktigere motivasjonsfaktor enn ideologi, og tidligere erfaring med voldsbruk går igjen som et fellestrekk for mange av de som i dag trekkes inn i terroristgrupper (Crone 2015).

For samfunnssikkerheten er det sentralt å forhindre radikalisering på alle arenaer og fronter der dette er mulig. Noe av det viktigste forebyggende sikkerhetsarbeid som kan gjøres mot terrorisme er anti-radikalisering. Dette oppnås når man på et tidlig stadium klarer å avverge at en utsatt person i det hele tatt tar steget over til politisk vold og terrorisme. I de tilfeller der radikalisering allikevel inntreffer er deradikalisering resepten. Klarer man ikke forhindre at folk blir radikalisert, må man gjøre alt man kan for å få reversert radikaliseringsprosessen. I boken Leaving terrorism behind har Tore Bjørgo og John Horgan (2009) kartlagt under hvilke omstendigheter terrorister hopper av og forlater terroristgrupper. Mentorprogrammer i fengsler er blant metodene som har dokumentert deradikaliserende effekt. Fengsler er en velkjent radikaliseringsarena der hat mot samfunnet kan kanaliseres inn i ny forsterket vilje til voldelige angrep. Det er et fåtall av terrorismedømte som ønsker å delta i slike mentorprogrammer, men for de som deltar er resultatene oppløftende.

Kilde: PST, Trusselvurdering 2015. Petter Nesser, Islamist Terrorism in Europe: A history (London: Hurst, 2015.) Manni Crone, «Radicalization revisited: Violence, politics and the skills of the body», International Affairs, 92:3 2016, 587–604. Tore Bjørgo og John Horgan, Leaving Terrorism Behind: Individual and Collective Disengagement, (London: Routledge, 2009.)

teret i Nairobi i 2013 er et eksempel på dette. Shipping-næringen har også blitt rammet og i kortere perioder har enkelte rederier valgt å seile rundt hele det afrikanske kontinent, snarere enn å risikere å bli kapret av somaliske pirater.

Vi ser at terrororganisasjoner som får vokse seg store ikke bare er en trussel mot statsstrukturen i landene gruppene springer ut fra, men truer både regional og internasjonal stabilitet. Svikt i nasjonalt styresett regnes blant de faktorer som gir høyest risiko for internasjonal ustabilitet.[56] Andre vesentlige faktorer er historikk for mellomstatlig konflikt og tilgang på ressurser. Økt internasjonal ustabilitet påvirker også Norges trusselsituasjon. De siste årenes terrorangrep i Europa vitner om hvordan terrorgruppering med opphav i svake stater kan ha en internasjonal agenda, med ISILs eksport av terrorisme til Europa som det fremste eksempel.

[56] World Economic Forum, *Global risk report*, 2015.

4.3.4.3 Sikkerhetstruende kriminalitet

Internasjonal organisert kriminalitet er ikke en direkte trussel mot norsk sikkerhet. Fenomenet påvirker likevel norsk sikkerhet på en rekke felter. Den negative påvirkningen fra alvorlig internasjonal kriminell virksomhets på internasjonal handel rammer også Norge. Deler av norsk næringsliv blir også berørt direkte, for eksempel rederier som seiler i farvann utsatt for piratvirksomhet. I en tid preget av økte kontaktflater og økt avhengighet på tvers av landegrenser, forplikter Norge å bidra i internasjonalt samarbeid på felter som antikorrupsjonsarbeid og bekjempelse av organisert kriminalitet, som for eksempel militærbidraget til antipiratvirksomhet i Adenbukta. Også migrasjonsstrømmer som resultat av organisert kriminalitet og sammenhengen mellom hvordan organisert kriminalitet gir grobunn for terrorisme er av betydning for norsk sikkerhet.

Internasjonal organisert kriminalitet er en alvorlig global trussel og dreper titusener av mennesker årlig, flere enn det som dør i krig. De største sektorene i internasjonal organisert kriminalitet er våpensalg, narkotikahandel, menneskehandel og IKT-kriminalitet. I følge FNs kontor for narkotika og kriminalitet (UNODC) er kostanden av organisert kriminalitet estimert til mellom 120–300 billioner amerikanske dollar, omkring 10 % av global BNP. Korrupsjon og annen kriminalitet er i fattige land ikke kun en økonomisk utfordring. Korrupsjon og annen alvorlig kriminalitet undergraver også allerede svake statsfunksjoner som igjen truer fred og stabilitet. Korrupsjon øker risikoen for konflikt samtidig som konflikt øker risikoen for korrupsjon. Dette symbiotiske forholdet truer fred og stabilitet i svake stater og gir grobunn for ustabilitet, kriminalitet og terrorisme.[57]

Alvorlig internasjonal kriminalitet kan forskyve styrkeforholdet mellom styresmakter og kriminelle. I for eksempel Mexico har narkotikakartellene stor makt både i lokalsamfunnet og nasjonalt. Som en respons på myndighetens kamp mot narkotikatrafikken har gruppene begynt å infiltrere politiet, grensevakter og politiske miljøer. Dette har forskjøvet styrkeforholdet mellom myndighetene og kriminelle og gjør at de kriminelle grupper fungerer som en stat i staten.[58] Siden daværende president Felipe Calderón bestemte seg for å bekjempe narkokartellene med makt har narkokrigen krevd 164 000 liv mellom 2007 og 2014, ifølge mexicanske styresmakter.[59]

Globalisering og teknologisk utvikling bidrar til at internasjonal organisert kriminalitet øker i omfang. Utfordringene er vevet sammen og er grenseoverskridende. Cybertrusler, piratvirksomhet, terrorisme og annen organisert kriminalitet er koblet tett sammen.[60] Skillelinjene mellom disse gruppene er i økende grad utvisket ved at de deler teknikker, personell, ferdigheter og pengeinntjeningsaktiviteter. For eksempel ISIL finansierer terror gjennom ulovlig salg av olje og kulturskatter, trafficking, kidnapping og cybercrime.[61]

Sikkerhetstruende organisert kriminalitet er grenseoverskridende. Nasjonalstatens tradisjonelle kontroll på informasjon, militær og økonomi blir i økende grad utfordret av ikke-statlige aktører. Fordelene som globaliseringen fører med seg gjør det også lettere for sikkerhetstruende aktører å rekruttere, trene, finansiere og styre ulovlig aktivitet på tvers av landegrenser og i cyberspace. Særlig internett og sosiale media benyttes hyppig til å nå ut til mange for å rekruttere, dele teknisk kunnskap og å planlegge aksjoner.

Organisert kriminalitet som inntektskilde til terrorisme

For å finansiere sin virksomhet benytter mange terrorgrupperinger illegale strategier, og deler både teknikker og personell med organiserte kriminelle. Terrororganisasjoner har en rekke kostnader knyttet til propaganda og rekruttering av nye medlemmer og tilhengere. Grupperinger som besitter territorielle områder bruker også store ressurser på å sikre egen sikkerhet og territoriell kontroll. Anskaffelser av våpen og andre ressurser brukt til å planlegge og gjennomføre terrorhandlinger kan også være kostbart. Taliban får en tredjedel av sine inntekter fra beskatning av opiumhandelen. Også Boko Haram og al-Shabaab får store inntekter fra beskatning av trekullsmugling. Dette utgjør hovedinntekten til al-Shabaab (ca. 36–56 million USD i året). Nettverk i Libya får store deler av sine inntekter fra menneskesmugling.[62] Også ISIL benytter ulike former for kriminalitet til å finansiere sin terrorvirksomhet, her-

---

57 Transparency International Deutschland, *Corruption as a threat to stability and peace*, Policy Paper 2014. https://www.transparency.de/fileadmin/pdfs/Wissen/Publikationen/Study_Corruption_as_a_Threat_to_Stability_and_-Peace.pdf

58 Meld. St. 37 (2014–2015), 21.

59 Vanda Felbab-Brown, «The Rise of Militias in Mexico. Citizen's Security or Further Conflict Escalation», Brokings 2015, https://www.brookings.edu/wp-content/uploads/2016/07/Rise-of-Militias-Mexico.pdf

60 Meld. St. 37 (2014–2015).

61 Institute for Economics & Peace, 2015.

62 Meld. St. 37 (2014–2015), 20–21.

under ulovlig salg av olje og kulturskatter, trafficking, kidnapping og cyberkriminalitet.[63]

Analyser av terroristers finansieringsstrategier i Europa viser at terrorceller i dag mottar mindre ekstern finansiell støtte, og i økende grad er selvfinansierende gjennom lovlige midler som et resultat av innstramming av finansielle reguleringer i kjølvannet av 9/11. Finansiering gjennom illegal virksomhet er den nest vanligste metoden for å finansiere terrorhandlinger og ble benyttet av 38 % av vest-europeiske jihadister i perioden 1994 til 2014. Organiserte kriminelle som finansierer terror kan overføre sin profitt via svartebørsmarkeder. Ofte blir og verdifulle gjenstander, narkotika og våpen blir brukt i stedet for kontanter til å oppbevare og overføre ressurser. Gjenstandene kan selges for å generere penger eller bli byttet mot varer terroristene trenger. Et eksempel på terrorhandling finansiert gjennom kriminalitet er de koordinerte bombeeksplosjonene mot pendlertog i Madrid 2004 som tok livet av 191 personer. Angrepet var hovedsakelig finansiert gjennom ulovlig narkotikahandel. Narkotika ble også brukt som betalingsmiddel for anskaffelsen av ulovlige eksplosiver som var stjålet fra en gruve i Spania av en kriminell bande.[64]

Piratvirksomhet

De vanligste formene for piratvirksomhet inkluderer bording av skip for å stjele kontanter og verdisaker, kapring for å stjele lasten, og bortføring av besetning med påfølgende krav om løsepenger.[65] Piratvirksomhet har lange tradisjoner, og har fått fornyet oppmerksomhet de siste tiårene, særlig utenfor Øst-Afrika, Vest-Afrika og i Sørøst-Asia. Piratvirksomheten i Adenbukta og Det indiske hav nådde en topp i 2007. Mellom 2005 og 2010 fant 198 kapringer sted og 4000 sjøfolk ble holdt som gisler. Internasjonal innsats for å bekjempe piratvirksomhet, hvor også Norge har deltatt, har gitt gode resultater i området. Det er likevel kostbart å opprettholde det sjømilitære nærværet i Adenbukta, særlig når sikkerhetsutfordringene øker i Europa. Selv om det somaliske problemet er under kontroll ser piratvirksomheten ut til å øke i Guineabukten og i Sørøst-Asia. Hele 100 angrep fant sted i Guineabukta i 2013. Oljelaster kapres hyppig og varene selges i Nigeria, som er hovedbasen for denne organiserte kriminelle virksomheten. 1000 norskkontrollerte skip seiler i Guineabukta årlig, i tillegg til norske fartøyer i offshorevirksomheten som er viktige leverandører til Ghanas petroleumsindustri.

Piratvirksomhet er et globalt problem og truer både personer og økonomiske verdier. 80 % av verdens handel skjer sjøveien. I følge verdensbanken har somalisk piratvirksomhet kostet USD 18 milliarder årlig i form av tapt internasjonal handel.[66] Som verdens sjette største handelsflåte påvirkers Norges økonomi og næringsliv direkte av maritime sikkerhetsutfordringer.[67] Aktiviteten går ned som følge av utrygge farvann, rederinæringen må betale høyere forsikring og kostanden knyttet til å seile lange omveier eller iverksette sikkerhetstiltak om bord er høye.

Svake staters manglende rettshåndhevelse og liten kapasitet til å bidra til internasjonalt politisamarbeid gjør dem til egnet tilholdssted for planlegging av piratvirksomhet. I enkelte land har også gruppene bånd til statsmakten. Somalia har nærmest kontinuerlig vært i borgerkrig siden diktatoren Siad Barre ble styrtet i et militærkupp i 1991. Stadig rivalisering mellom ulike klaner er hovedårsaken til de langvarige konfliktene. Somalia har manglet både en fungerende regjering, politistyrke og nasjonalt rettsvesen, noe som har gjort det mulig for både piratvirksomhet og terroristgrupper som Al-Shabaab å operere nærmest uforstyrret. Det er grunn til å frykte at piratvirksomhet kan inngå i samarbeid med terrororganisasjoner. For eksempel ved at de tar seg av terroristene finansielle transaksjoner og terroristene gir våpen. Mye tyder på at penger fra piratvirksomhet i Guineabukta går til Boko Haram.

4.4 Nasjonale sårbarheter

4.4.1 Nye sårbarheter som følge av samfunnsutviklingen

Samfunnsutviklingen medfører betydelige endringer i hvordan samfunnsfunksjoner blir ivaretatt. Globaliseringsprosesser bidrar til å redusere betydningen av avstander og statsgrenser, og har i så måte brakt verden tettere sammen. På de fleste områder er denne generelle samfunnsutviklingen en ønsket utvikling, langt på vei drevet av befolkningen og samfunnets behov. Den teknologiske utviklingen og den strukturelle utviklingen av samfunnet fører til at befolkningen kan benytte

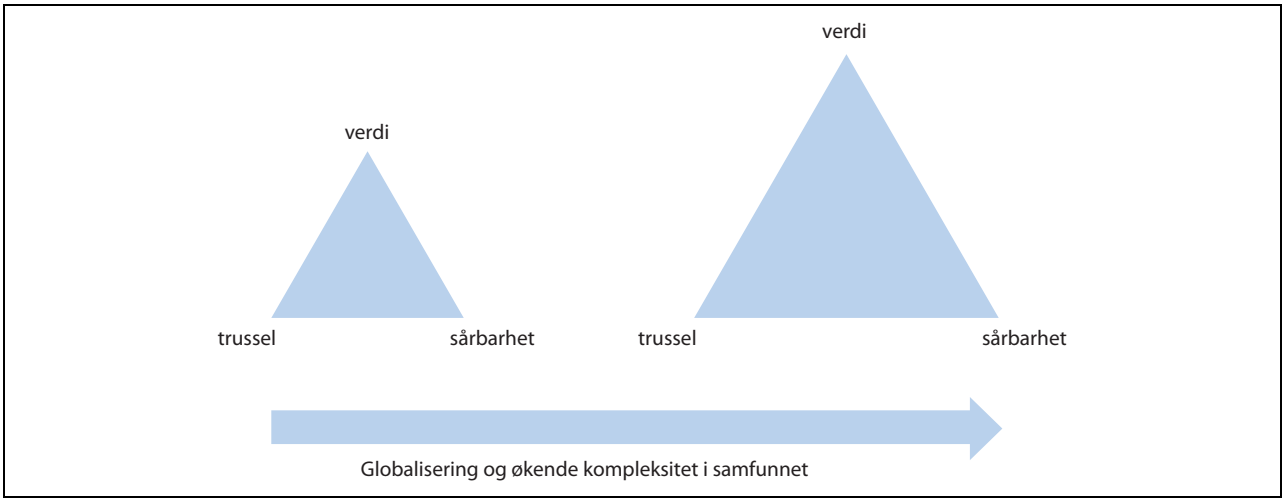
[63] Institute for Economics & Peace, 2015.

[64] Emilie Oftedal, *The financing of jihadi terrorist cells in Europe*, FFI-rapport 02234 (Kjeller: Forsvarets forskningsinstitutt 2014).

[65] Meld. St. 37 (2014–2015), 23.

[66] Ibid., 33.

[67] Ibid., 52.



Figur 4.7 Risiko og samfunnsutvikling.

Arealet i trekantene illustrerer omfanget av risiko. Globalisering og økende kompleksitet i samfunnet fører til at verdiene som vi må beskytte vokser. Vi må også forholde oss til et større spekter av trusler, og sårbarheten blir større. Dette fører til økt risiko, og økte forventinger og forpliktelser til risikohåndtering i samfunnet.

stadig flere tjenester. Individet kan i stadig større grad støtte seg på tjenester som forenkler eller beriker hverdagen og livet. Samfunnets strukturer vokser og øker i kompleksitet, og samfunnsfunksjonene vi er avhengige av (verdiene som må sikres) blir stadig flere (verdiene vokser).

Ved at individene i samfunnet gjør seg avhengig av flere tjenester, blir også sårbarheten overfor bortfall av tjenester større – både på grunn av den reelle avhengigheten til de ulike tjenestene/funksjonene og på grunn av at når antallet tjenester øker er det større sannsynlighet for at noen blir berørt i en hendelse.

Videre fører samfunnets økende kompleksitet til tilsvarende gjensidige avhengigheter mellom ulike samfunnsfunksjoner. Utviklingen i retning av økende avhengigheter er igjen drevet av effektivisering og gjensidig utnyttelse av strukturer, systemer og tjenester. Dette skaper et effektivt og hensiktsmessig samfunn under normale omstendigheter, og kan bidra til økt robusthet i mange samfunnsfunksjoner. Imidlertid kan effektiv og god ressursutnyttelse gi økt sårbarhet i systemer og funksjoner dersom disse blir utsatt for unormal påvirkning/påkjenning. Med økte avhengigheter vil sårbarheten forplante seg i verdikjedene. Sårbarheter kan være av menneskelig, organisatorisk eller teknisk art.[68]

Menneskelige sårbarheter kan være menneskers evne til å la seg lure, manglende motivasjon til å følge sikkerhetsbestemmelser som fører til merarbeid/ineffektivitet, eller manglende kunnskap. Menneskers evne til å la seg lure utnyttes aktivt gjennom sosial manipulasjon. Ansatte kan for eksempel lures til å gi fra seg passord, beskrive vedlikeholds- og sikkerhetsrutiner eller benytte minnepinner som er infisert.

Organisatoriske sårbarheter kan knyttes til manglende lederforankring og styring av arbeidet med sikkerhet. Videre kan mangel på hensiktsmessig ansvarsdeling og bevisstgjøring gi økt sårbarhet. Mangel på ressurser og kompetanse i sikkerhetsarbeidet kan være knyttet til manglende ledelsesforankring, og er ifølge NSM også en vesentlig svakhet i virksomheter de fører tilsyn med.[69] FFI har gjennomført en studie på oppdrag fra NSM der de har undersøkt årsaken til mangelfull sikkerhetstilstand ved virksomheter NSM fører tilsyn med. FFIs konklusjon er at organisatoriske forhold er den viktigste årsaken.[70]

På den tekniske siden finnes også en rekke sårbarheter. NSM trekker fram tekniske IKT-sårbarheter i SFR. Dette inkluderer ikke-oppdaterte dataprogrammer, bruk av ikke-sikre komponenter i IKT-systemer, samt implementasjons- og designfeil i IKT-produkter. Mulige sårbarheter kan finnes i maskinvare, operativsystemer og applikasjoner. Videre fremhever NSM at manglende logging av trafikk kan innebære en betydelig sårbarhet,

[68] NSM, *Sikkerhetsfaglig råd*, 2015.

[69] Ibid.

[70] Ingvill Moe Elgsaas og Hege Schultz Heireng, *Norges sikkerhetstilstand – en årsaksanalyse av mangelfull forebyggende sikkerhet,* FFI-rapport 00948 (Kjeller: Forsvarets Forskningsinstitutt, 2014).

samt mangel på tiltak for å oppdage irregulær bruk og aktivitet.

4.4.1.1 Befolkningsvekst, urbanisering og relaterte sårbarheter

Verdens befolkning nådde 7,3 milliarder i 2015 og er forventet å øke til 9,7 milliarder mennesker i 2050.[71] Kraftig befolkningsvekst og økt urbanisering er blant hovedtrekkene ved vår tids samfunnsutvikling. Mer enn halvparten av verdens befolkning bor i dag i byer, og ytterligere 3 milliarder mennesker er forventet å flytte til urbane strøk innen 2030. Antallet såkalte mega-byer, byer med mer enn 10 millioner innbygger, øker også kraftig. Den kraftige urbaniseringen kommer som et resultat av effektiviseringen av primærnæringene og sekundærnæringene som skjedde gjennom den industrielle og den grønne revolusjon. Et relativt lite antall mennesker i disse næringene kan betjene stor vekst i tertiærnæringene. At flere og flere bor i byer skaper innovasjon, økt produktivitet og økonomisk utvikling. Samtidig kan det enorme demografiske presset som følger de betydelige folkeforflytningene også være en kilde til forurensing, fattigdom, kriminalitet og økte helse- og ordensproblemer, spesielt når urbanisering skjer raskt og uten god styring. Den dramatiske økningen av mennesker bosatt i byer påvirker alle aspekter av samfunnet og gir sårbarheter knyttet til ressurstilgang og opprettholdelsen av kritiske samfunnsfunksjoner som følge av høy utnyttelsesgrad av naturresurser og systemer. Det oppstår videre nye utfordringer også i konfliktsituasjoner.

Den kraftige befolkningsveksten gir flere munner å mette, samtidig som andelen dyrket mark blir mindre. Økt urbanisering og nedbygging av jordbruksareal kombinert med klimaendringer gir større ustabilitet i matforsyningene. Også norsk kornproduksjon er i dag betydelig redusert, og stadig mer korn importeres utenfra. På 1980-tallet lå verdens kornlagre på om lag 130 dager. I de siste årene har de i snitt vært på 74 dager. Den økte norske avhengigheten av import og nedgangen i både kornlagre og matjord internasjonalt gir lav matsikkerhet og høy sårbarhet i krisesituasjoner. Norge har ikke lengre beredskapslagre med korn.

Tett befolkede urbane områder er mer krevende å administrere for å sikre befolkingens tilgang til grunnleggende behov som vann, mat og sikkerhet. Det er også krevende å sikre tilgang til velferdsgoder som utdanning, arbeid og helsetjenester i tett befolkede urbane områder, men opprettholdelse av disse er samtidig en forutsetning for å unngå sosial misnøye og uro. Opprettholdelsen av kritiske samfunnsfunksjoner som elektronisk kommunikasjon, kraft, vann og avløp er sårbare, spesielt når krisesituasjoner rammer. Orkanen Sandy som blant annet traff New York og New Jersey høsten 2012 førte til oversvømmelse av T-banesystemet og en rekke sentrale veituneller, oversvømmelse av Wall Street, brannutbrudd i Queens og at store deler av New York og omegn mistet strømmen i flere dager. 53 mennesker i New York mistet livet som følge av stormen.[72] Dette er et av mange eksempler på at storbyer kan ha høy sårbarhet og lav resiliens ved ulykkesscenarier.

Humanitære katastrofer og konfliktsituasjoner byr altså på andre utfordringer i urbane strøk enn i rurale områder. Hjelpeorganisasjoner og militæret har mer erfaring med humanitære kriser i rurale strøk. NGO-er har derfor måttet tilpasse seg nye utfordringer når et stort antall flyktninger fra Syria-krigen slo seg ned i urbane og tett befolkede områder i Jordan og Libanon. Faren for opprør, for eksempel rettet mot håpløse sosiale forhold, øker etter hvert som storbyer vokser frem på en ukontrollert måte. Det er svært krevende å løse voldelige konflikter i store byer. Det krever store styrker og medfører høy operasjonell risiko i alle deler av en operasjon. Den kraftige urbaniseringen tilsier at vestlige styrker i fremtiden i økende grad vil bli involvert urbane operasjoner som et ledd i å stabilisere konfliktsituasjoner som er kommet ut av kontroll.

4.4.2 Sårbarheter for samfunnsfunksjoner og infrastruktur

4.4.2.1 Vurdering av sårbarheter og kartlegging av avhengigheter

DSB fikk i oppdrag fra Justis- og beredskapsdepartementet å utvikle en modell som skal være et virkemiddel for myndigheter på sentral, regionalt og lokalt nivå i arbeidet med å identifisere hva som er kritisk infrastruktur og kritiske samfunnsfunksjoner.[73] DSBs rapport Samfunnets kritiske funksjoner, har som formål å identifisere kritiske

[71] United Nations, *World Population Prospects*, 2015 revision (New York: United Nations, 2015).

[72] Center for Disease Control and Prevention, «Deaths Associated with Hurricane Sandy – October–November 2012», http://www.cdc.gov/mmwr/preview/mmwrhtml/mm6220a1.htm

[73] Som en oppfølging av St. meld 22 (2007–2008), *Samfunnssikkerhet – Samvirke og samordning.*

samfunnsfunksjoner og definere hvilken funksjonsevne det er viktig å opprettholde til enhver tid i et samfunnssikkerhetsperspektiv.[74] Som omtalt i kapittel 4.2.2 er systematikken i rapporten bygget på Infrastrukturutvalgets utredning og baserer seg på å ivareta kritiske samfunnsfunksjoner gjennom å sikre innsatsfaktorer og infrastruktur.[75]

Gjennom å kartlegge sårbarhetene til kritisk infrastruktur og innsatsfaktorer kan en altså identifisere sårbarheten til de kritiske samfunnsfunksjonene som disse understøtter. Dette dreier seg om både infrastruktur og innsatsfaktorer som direkte understøtter en samfunnsfunksjon og indirekte ved de avhengigheter som er til andre samfunnsfunksjoner, innsatsfaktorer og infrastruktur lenger ut i verdikjedene.

Kartlegging av avhengigheter mellom samfunnsfunksjoner og hvilke sårbarheter som forplanter seg kan være komplisert. Ofte er det lange komplekse verdikjeder med sterke avhengigheter mellom funksjonene, og det kan være krevende å skaffe seg kunnskap om sårbarheter utover egen virksomhet.

Konsekvensene av helt eller delvis bortfall av en samfunnsfunksjon er avhengig av graden av kritikalitet eller nødvendighet for samfunnet eller befolkningen, graden av resiliens og redundans i systemene som understøtter den aktuelle funksjonen, samt annen beredskap for gjenopprettelse eller skadebegrensning. Her vil også avhengigheter mellom den aktuelle samfunnsfunksjonen og andre samfunnsfunksjoner være avgjørende for hvor omfattende konsekvensene av bortfall vil være. Konsekvensene vil også kunne variere avhengig av klima og andre naturfenomener, samt samfunnsmessige forhold.

De fleste funksjoner i samfunnet er sterkt avhengig av energiforsyning. På grunn av høy leveringsevne, fleksibel avlevert effekt og lav kostnad er elektrisitet distribuert gjennom elektrisitetsnettet den mest utbredte energiforsyningen i Norge (som i de fleste andre land). Forsyningen av elektrisk kraft har vært meget stabil og er tilrettelagt for å være robust mot ulike hendelser, særlig naturhendelser. Bortfall av forsyningen skjer imidlertid jevnlig over kortere perioder i begrensende områder. Det er særlig naturhendelser som sterk vind, skred og flom som er hyppige årsaker til bortfall. Følgelig er samfunnet rimelig robust overfor slike bortfall.

Robustheten er blant annet ivaretatt gjennom at mange virksomheter som er avhengig av kontinuerlig forsyning av elektrisk kraft har etablert generatorer og magasinert elektrisk kraft i batterier som sikrer nødvendig forsyning i en kortere periode med bortfall. Kraftreserver kan da både betraktes som en kritisk innsatsfaktor i seg selv, og som en sårbarhetsreduserende faktor for de funksjoner kraftreservene understøtter.

Videre vil sårbarhet i kraftreserver blant annet være knyttet til levetiden for kraftreserven. Levetiden til kraftreserven vil være basert på forventet behov, som igjen er definert ut fra en forventning til et maksimalt omfang av en hendelse, gjerne bestemt ut fra en risikovurdering. Dersom risikovurderinger er gjennomført vil sårbarheten således være avhengig av hvilke risikoreduserende tiltak som er iverksatt ut fra en vurdering av sannsynlighet og konsekvens for ulike typer hendelser, sett opp mot kostnaden ved å gjennomføre tiltak. Eksempel på risikomatrise der ulike hendelser er presentert sammen er vist i figur 4.8.

4.4.2.2 Trusselaktørers utnyttelse av sårbarheter

Historisk har sabotasje eller angrep mot kritiske samfunnsfunksjoner vært benyttet som virkemiddel i krise og krig. Bortfall av slike funksjoner rammer store deler av befolkingen og setter beslutningstagere under press. Angrep og sabotasje kan gjøres åpenlyst eller som fordekte operasjoner avhengig av hva som er målet for en trusselaktør. Naturhendelser og andre hendelser kan utnyttes for å øke effekten av tiltakene som blir gjennomført.

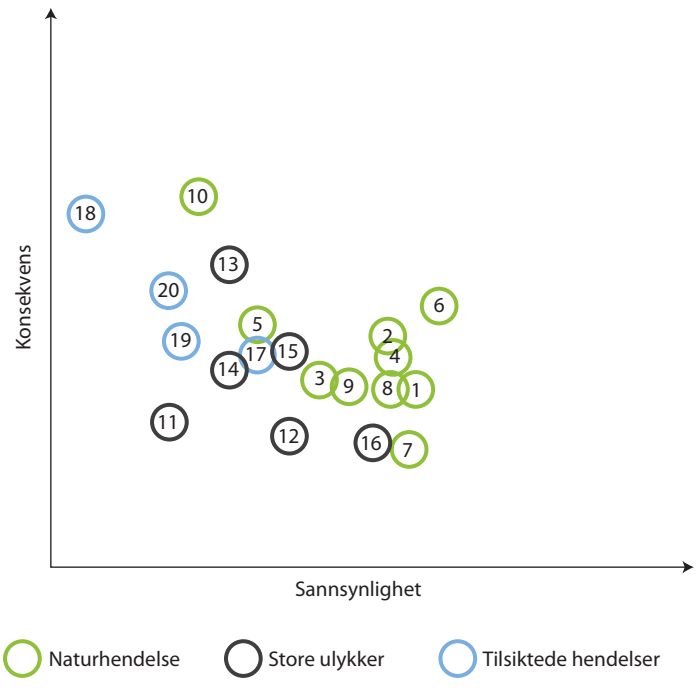
Som beskrevet i kapittel 4.4.1 vil en trusselaktør kunne utnytte menneskelige, teknologiske og organisatoriske sårbarheter. En trusselaktør med god innsikt i et lands samfunnsfunksjoner, infrastruktur og innsatsfaktorer vil kunne gjennomføre operasjoner med god kontroll over hvilken effekt operasjonen vil gi. Flere av trusselaktørene som er nevnt under kapittel 4.3 har kunnskap og kapasitet til å ramme kritiske samfunnsfunksjoner på måter som vil få alvorlige konsekvenser for Norge. PST, NSM og E-tjenesten er samstemt i at fremmede stater bedriver innhenting av informasjon om virksomheter og infrastruktur i Norge som øker vår sårbarhet.

Det skjer også innhenting om slike forhold fra ikke-statlige trusselaktører. Disse vil også kunne benytte noen av de samme metodene som statlige aktører for innhenting og for utnyttelse av slik kunnskap for målrettede angrep. Som regel vil imidlertid ikke-statlige aktører ha et kortere tids-

---

74 DSB, Samfunnets kritiske funksjoner – Hvilken funksjonsevne må samfunnet opprettholde til enhver tid, 2015.

75 NOU 2006: 6.



Scenarioene plassert i risikomatrise	
1	Storm i indre Oslofjord
2	Langvarig strømrasjonering
3	Flom på Østlandet
4	Varslet fjellskred i Åkneset
5	Kvikkleireskred i by
6	Pandemi i Norge
7	Tre samtidige skogbranner
8	100-års solstorm
9	Langvarig vulkanutbrudd på Island
10	Jordskjelv i by
11	Gassutslipp på industrianlegg
12	Brann på tanklager i by
13	Atomulykke på gjennvinningsanlegg
14	Olje- og gassutblåsning på borerigg
15	Skipskollisjon på Vestlandskysten
16	Brann i tunnel
17	Terrorangrep i by
18	Strategisk overfall
19	Cyberangrep mot finansielle strukturer
20	Cyberangrep mot ekom-infrastruktur

Figur 4.8 Nasjonalt Risikobilde 2014.

I Nasjonalt Risikobilde presenterer DSB ulike scenarier for uønskede hendelser. Konkrete scenarier blir risikovurdert og sammenstilt i en risikomatrise, som denne fra 2014. Når scenariene er konkrete, og ikke generiske, må ikke figuren forstås slik at for eksempel alle jordskjelv i byer (scenario 10) på generell basis vil ha verre konsekvenser enn et hvert terrorangrep i by (scenario 17).

Kilde: DSB, *Nasjonalt risikobilde*, 2014.

perspektiv på innhenting og gjennomføring av et angrep. De vil også ha mindre ressurser og som regel være teknologisk underlegne statlige etterretningsorganisasjoner.

I PSTs Trusselvurdering 2016 fremkommer det at utenlandsk etterretning benytter et bredt spekter av metoder for å innhente kunnskap om norsk infrastruktur, forsvars-, sikkerhets- og beredskapsforhold og andre grunnleggende nasjonale interesser. Russland trekkes frem som en hovedaktør. PST mener virksomheten har som formål å legge til rette for russiske militære disposisjoner i en eventuell endring i den sikkerhetspolitiske situasjonen.

Metodene som benyttes av fremmede staters etterretning spenner i følge PST bredt. Noen av metodene er etablering av personlige og fortrolige kontakter som har tilgang til og formidler fortrolig informasjon, tekniske metoder for å avlytte/avlese sensitiv informasjon i IKT-systemer, utpressing og trusler mot personer av utenlandsk opprinnelse som arbeider i sektorer med tilgang til sensitiv og skjermingsverdig informasjon.

Innsidere vil i tillegg til å lekke sensitiv informasjon også kunne ha en sentral rolle i en eventuell sabotasjehandling, enten den er i form av fysiske tiltak eller digitale angrep.

Digitale nettverksoperasjoner blir også fremhevet som et område der både etterretningsaktivitet, sabotasje og annen sikkerhetstruende virksomhet er gjeldende.

PST understreker at sårbarheten for de ulike metodene er avhengig av i hvilken grad relevante virksomheter har kjennskap til trusselen og skadepotensialet, samt i hvilken grad de tar sikkerheten på alvor. Mangel på kunnskap og god sikkerhetskultur gjør at sårbarheten vedvarer.

PSTs vurdering er at den endrede sikkerhetspolitiske situasjonene i Europa og økt bevissthet hos personer som tradisjonelt har vært etterretningsmål, har ført til redusert mulighet for bruk av tradisjonell menneskelig innhenting av informasjon i forhold til tidligere.

4.4.2.3 *Teknologisk utvikling som øker sårbarhetene i samfunnet*

Det digitale sårbarhetsutvalget har i sin rapport gjennomgått digitale sårbarheter i samfunnet.[76] I deres rapport er det en gjennomgang av kritiske samfunnsfunksjoners digitale sårbarheter. Rapporten fokuserer på samfunnets økte avhengighet av digital teknologi og er et godt grunnlag for videre arbeid med å redusere risikoen som er resultatet av disse avhengighetene.

Den teknologiske utviklingen åpner også nye muligheter for trusselaktører, fordi dette endrer sårbarheten i kritiske samfunnsfunksjoner. Det viktigste eksempelet er økt satsning på digitale nettverksoperasjoner. Dette er grundigere diskutert i kapittel 4.4.3.

Andre eksempler er miniatyriseringen av utstyr for avlytting av tale og akustiske og digitale signaler, samt foto og video og annet utstyr for fordekt innhenting av sensitiv informasjon. Miniatyriseringen bidrar til at utstyret kan skjules på nye steder med lav sannsynlighet for å bli kompromittert. I tillegg har utstyret lengre levetid som følge av bedre batterikapasitet. Kvaliteten på lyd og bilde er også vesentlig bedre enn tidligere.

Utviklingen av drone-teknologi og andre automatiserte og/eller eleverte plattformer for informasjonsinnhenting går fort. Dette gjør det mulig å bedrive innhenting av informasjon langt mer kostnadseffektivt enn tidligere, og med lavere risiko for å bli kompromittert.

Den økte bruken av sosiale medier gjør det lettere å kartlegge vennekretsen og interessene til potensielle etterretningsmål. Utstrakt bruk av mobiltelefoner med kamera gjør at bilder fra ulike lokasjoner er tilgjengelig i et stort omfang, ofte med nøyaktig posisjonering av hvor bildet er tatt og hvilke personer som er tilstede. Ukritisk publisering av bilder og video på sosiale medier kan gi trusselaktører informasjon som de ellers ville måtte benytte store ressurser for å innhente, potensielt med høy risiko.

4.4.3 Digitale sårbarheter

4.4.3.1 *Samfunnets avhengighet av digitale systemer og tjenester*

Dagens informasjonssamfunn er i sterk vekst og er drevet frem av økt globalisering og rask teknologisk utvikling. Informasjonsteknologiske gjennombrudd har ført til gjennomgripende samfunnsendringer som gir store gevinster i form av innovasjon og produktivitet. Digitaliseringen gjør det billigere å lagre og bearbeide informasjon i et mye større omfang enn tidligere. Dette fører imidlertid også med seg nye sårbarheter. Digitale tjenester og funksjoner kjennetegnes av lange, sammensatte og uoversiktlige verdikjeder. Det er altså komplekse avhengigheter mellom ulike funksjoner. Videre kjennetegnes slike tjenester og funksjoner av at informasjon kan overføres meget raskt mellom de ulike delene av en verdikjede. En feil som oppstår et sted, kan dermed forplante seg gjennom hele verdikjeden i løpet av svært kort tid – i enkelte sammenhenger i løpet av millisekunder. Bildet kompliseres ytterligere av at digital tjenesteutvikling og digitale tjenestetilbud er bransjer preget av høy grad av internasjonalisering. Det medfører at verdikjedene som en funksjon er avhengig av ofte inkluderer tjenester i andre land. For en virksomhet som er avhengig av digitale tjenester er det derfor svært vanskelig å ha tilstrekkelig innsikt i og kontroll over egne sårbarheter – ikke minst fordi en arver sårbarhetene til øvrige ledd i de digitale verdikjedene.

Norge er blant de mest digitaliserte land i verden.[77] Dette i kombinasjon med den raske utviklingen på feltet gjør at Norge ikke utelukkende kan basere seg på at andre større og mer ressurssterke nasjoner skal finne løsninger på alle de vesentlige utfordringer og problemer som følger av denne utviklingen. Det digitale sårbarhetsutvalget påpeker i sin rapport at det må forventes at noen problemer vil oppstå i Norge først, og at vi må ta hensyn til dette gjennom ulike risikoreduserende tiltak.[78]

Elektronisk kommunikasjon (ekom) er en innsatsfaktor i all vare og tjenesteproduksjon og økonomisk virksomhet. Helsevesen, betalingstjenester, stat, kommune og ordensmakt er avhengig av at ekom fungerer. I Norge har telenettet en sentral rolle som bærer av slike tjenester. I det digitale sårbarhetsutvalgets rapport fremheves Telenors kjerneinfrastruktur som spesielt viktig. I rapporten konkluderes det med at dette nettet er utbygd med tanker på robusthet og er operert profesjonelt. Likevel er risikoen forbundet med å ha kun et slikt kjernenett uakseptabelt høy, med tanke på de store verdiene dette nettet er bærer av. [79]

En av de gjennomgripende endringene digitalisering har ført med seg er hvordan vi styrer pro-

[76] NOU 2015: 13.

[77] NSM, *Helhetlig IKT-risikobilde 2015*.

[78] NOU 2015: 13.

[79] Ibid.

sesser. Digitale styringssystemer, eksempelvis SCADA-systemer (supervisory control and data acquisition), benyttes til å fjernstyre industriprosesser. Slike systemer har ført til betydelig effektivisering av en rekke prosesser. De første SCADA-systemene som ble etablert var ofte fysisk adskilt fra andre digitale nettverk og systemer. Imidlertid har det vært en utvikling i retning av at det i stadig større grad skjer en integrasjon mellom SCADA-systemer og andre styringssystemer, samt tettere kobling mot internett. Dette gir ytterligere effektiviseringspotensial, men fører også til økt sårbarhet for digital inntrenging i systemene og for at feil forplanter seg mellom systemer. Det er flere eksempler på hvordan SCADA-systemer har blitt utnyttet for å utføre sabotasje.

Ett eksempel på en cybersabotasjeaksjon mot SCADA-system er Stuxnet-viruset, som trolig ble iverksatt av USA og Israel for å ødelegge sentrifuger for anrikning av uran i Irans atomprogram. Angrepet gjorde at sentrifugene for anrikning av uran spant ut av kontroll, noe som antas å ha satt Irans atomprogram to år tilbake i tid. Et annet digitalt angrep som har fått konsekvenser for viktig infrastruktur er cyberangrepet mot kraftsektoren i Ukraina i desember 2015 hvor 80.000 mennesker mistet strømmen. Dette viser hvordan sårbarheten i digitale systemer kan utnyttes for å ramme viktige prosesser. Angrep på styringssystemer kan ha stort skadepotensiale og i mange sammenhenger er konsekvensene vanskelige å forutsi.

Inntrenging og forsøk på inntrenging i IKT-systemer skjer hyppig, med varierende alvorlighetsgrad. Angrep utføres for å kompromittere, stjele, endre eller ødelegge informasjon. Nettverksbaserte etterretningsoperasjoner fra fremmede stater mot offentlige myndigheter og virksomheter skjer løpende og representerer en alvorlig trussel mot viktige nasjonale sikkerhetsinteresser. Slike nettbaserte etterretningsoperasjoner sees som et kostnadseffektivt alternativ til tradisjonell spionasje. Særlig Russland og Kina er stater med stor offensiv kapasitet i det digitale domenet. Også aktivister, terrorister og profittmotiverte kriminelle utgjør en trussel mot norske mål.[80]

Informasjonssikkerheten i offentlige virksomheter og virksomheter som ivaretar kritiske samfunnsfunksjoner er avhengig av sikkerheten i IKT-systemene. Saksbehandling foregår etter hvert nesten utelukkende på PC eller andre digitale plattformer. Bruk av skytjenester øker i både offentlig og privat sektor så vel som hos privatpersoner. Ca. 30 % av norske næringslivaktører benytter seg av skytjenester.[81] At denne informasjonen lagres utenfor virksomhetens lokaler fører til sikkerhetsutfordringer. Også mobilitet og trådløshet øker i omfang, og sikkerheten til nettverkene varierer i høy grad og kan lett avlyttes ved manglende bruk av kryptering.[82]

Flere forsøk på nettverksbaserte etterretningsoperasjoner og andre digitale angrep mot offentlige og private virksomheter har de siste årene blitt avdekket. Sommeren 2014 ble 50 ulike selskap i norsk olje- og energisektor utsatt for omfattende spionasjeangrep. Dette er det største hackerangrepet mot norske interesser så langt. Forskeren Ruth Skotnes hevder at til tross for flere tilfeller av forsøk på inntrengning i egne driftskontrollsystemer, opplever norske nettselskaper trusselen mot egne systemer som relativt lav. Skotnes påpeker at dette er alvorlig tatt i betraktning at trusselbildet mot norske kraftdistributører er reelt. Sårbarhetene i sektoren øker ved bruk av IKT i distribusjon. Anleggene fjernstyres i dag fra et fåtall av driftssentraler i motsetning til tidligere hvor det var ansatte som overvåket og betjente hvert enkelt kraftforsyningsanlegg. Styringssystemene er i dag koblet til kontorstøtteverktøy og internett, som gjør dem sårbare mot angrep og teknisk svikt. Skotnes mener vi må forvente flere angrep mot driftskontrollsystemer som styrer industrielle prosesser og kritisk infrastruktur i tiden fremover.[83]

DNB opplevde sommeren 2014 et tjenestenektangrep (Distributed Denial-of-Service (DDoS) attack) som gjorde at det ikke var mulig å logge seg inn i nettbanken. I følge DNB dreide det seg ikke om hacking, men et overlagt sabotasjeangrep i form av at veldig mange påloggingsforsøk på en gang sprengte kapasiteten. Indikasjoner tyder på at angrepet kom fra utlandet. En rekke andre sentrale aktører ble også rammet, herunder Telenor, Norges Bank og Nordea.[84] Nedetid i finansielle tjenester som resultat av cyberangrep kan føre til stor økonomisk skade. Ved langvarige bortfall kan konsekvensene av mangel på finansielle tjenester få store ringvirkninger i samfunnet. Det vil kunne

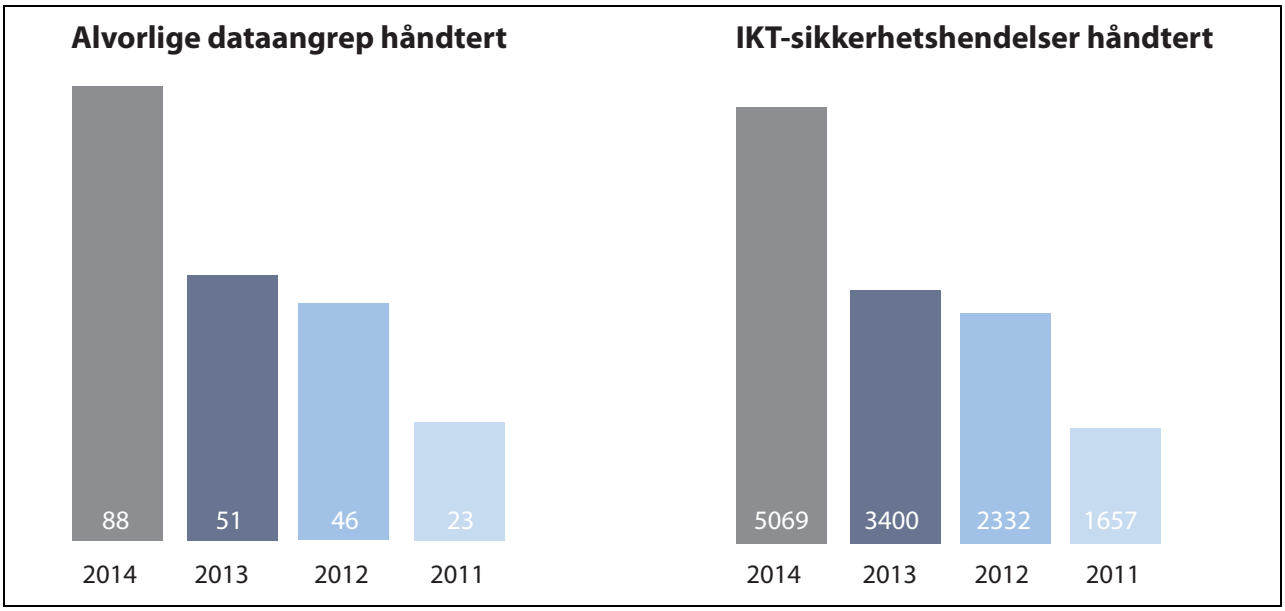
[80] Etterretningstjenesten, *Fokus 2015*.

[81] NSM, *Helhetlig IKT-risikobilde 2015*, 18.

[82] NSM, *Sikkerhetsfaglig råd 2015*.

[83] Ruth Ø. Skotnes, «Challenges for safety and security management of network companies due to increased use of ICT in the electric power supply sector», (Doktoravhandling, Universitetet i Stavanger 2015), 5.

[84] Teknisk ukeblad, «DNBs nettsider utsatt for nettangrep igjen», http://www.tu.no/artikler/dnbs-nettsider-utsatt-for-nettangrep-igjen/231295 (oppsøkt 21.04.2016).



Figur 4.9 Dataangrep og IKT-sikkerhetshendelser.

Antallet IKT-sikkerhetshendelser og alvorlige dataangrep som NSM håndterer har vært økende i flere år. De fire siste årene har det vært en markant økning. De fleste angrepene har som formål å stjele informasjon fra datasystemene til store eller viktige bedrifter.

Kilde: Nasjonal sikkerhetsmyndighet, *Risiko 2015*.

redusere norske myndigheters funksjons- og styringsevne, og kunne skape sosial uro i befolkningen.[85] Motivet for slike angrep kan være av politisk, personlig eller økonomisk art. Sabotasje og hærverk kan også utføres av aktører uten en klar agenda. Det er vanskelig å fastslå hva som er motivet uten god kunnskap om hvem som står bak. NSM mener det også foregår jevnlige og omfattende angrep mot norske virksomheter som ikke blir oppdaget.

Norges forsvar og våre allierte vil måtte forberede seg på å møte irregulær krigføring som hybridkrig og angrep i det digitale rom i tiden fremover. Man må være forberedt på operasjoner som har som mål å påvirke politiske beslutningstakere eller styre det videre konfliktforløpet. I det digitale rom vil slike operasjoner kunne omfatte blant annet sabotasjeaksjoner og nettverksbaserte etterretningsoperasjoner for å skaffe kunnskap om kritisk infrastruktur for å kunne gjennomføre fysiske sabotasjeaksjoner. Kraftforsyning, telekommunikasjon, betalingstjenester, samt politisk og militær ledelse kan alle være sårbare for slike angrep.[86] Det digitale rom blir trolig en viktig arena for kriser og konflikter i årene som kommer.

Moderne IKT og nettverksteknologi gir også andre muligheter og utfordringer i militær sammenheng. Teknologiutviklingen gjør at geografisk avstand har mindre betydning – noe som påvirker utviklingen av en rekke virkemidler for bruk i militær sammenheng. Eksempler på teknologi som påvirkes sterkt av IKT-utviklingen er: kommando, kontroll og kommunikasjonssystemer, datasyn (*computer vision*), ballistiske missiler og kryssermissiler, langtrekkende droner og satellitter.

Bruk av stordata gjør det mulig å analysere store informasjonsmengder som kan bidra til et bredt spekter av prediktive analyser. Slike analyser benyttes til alt fra å predikere folks handlemønster til å forutse store naturhendelser. Stordata kan også brukes til å kartlegge personer, grupper eller hele befolkninger. Når store mengder data analyseres kan enkeltopplysninger som i seg selv ikke er sensitive, sammenstilles til sensitiv informasjon. Ved bruk av enkle verktøy kan store mengder informasjon om vennekrets og interesseområder samles. Stordata setter dermed personvernet under press og gir sårbarheter mot kriminalitet, menneskelig etterretning og spionasjevirksomhet. Denne sårbarheten økes av individets økte bruk av internett til sosiale medier, kommunikasjon, lagring i skyen etc., og det såkalte *tingenes internett,* som vil si at flere og flere gjenstander kobles til internett, fra kjøleskap til smart-

[85] DSB, *Nasjonalt risikobilde 2014.*
[86] Etterretningstjenesten, *Fokus 2015.*

klokker. Dette er brukervennlige og praktiske tilskudd til hverdagen, men den teknologiske utviklingen går raskt og fører ofte til at etablerte strukturer og regelverk ikke klarer å henge med.[87]

4.4.3.2 Sårbarheter i IKT-systemer

Koblingen mellom informasjonssikkerhet og sikkerhet i IKT-systemer er blitt meget tett. IKT-systemer er i dag bærere av de fleste funksjoner i samfunnet, og således er de fleste samfunnsfunksjoner avhengig av sikkerheten i IKT-systemene. Dette betyr at sårbarhetene i IKT-systemene arves av samfunnsfunksjonene som disse understøtter. I likhet med andre områder er sårbarhetene i IKT-systemer av menneskelig, organisatorisk og teknisk art. IKT-systemer er sårbare for både digitale og fysiske angrep. God sikkerhet i IKT-systemer fordrer gode tekniske løsninger, så vel som god fysisk sikkerhet rundt infrastruktur og personellsikkerhet.

Sikkerhet i et IKT-system innebærer at en kan sikre konfidensialitet, integritet og tilgjengelighet av informasjonen som systemet behandler eller lagrer.

For skjermingsverdig og sikkerhetsgradert informasjon benytter Forsvaret og enkelte andre deler av statsforvaltningen sikkerhetsgodkjente IKT-systemer. Godkjente systemer har et tydelig regelverk som skal gi nødvendig sikkerhet. Det er ulike krav avhengig av hvilke graderingsnivåer systemene er sikkerhetsgodkjent for. Det er NSM som godkjenner systemer for sikkerhetsgradert informasjon og fører tilsyn med sikkerheten omkring slike systemer. Sikkerhetsgodkjente IKT-systemer er imidlertid ikke veldig utbredt i andre sektorer enn Forsvaret, noe som gjør sikkerhetsgradert kommunikasjon utfordrende både mellom og innad i sektorer. NSM påpeker i SFR behovet for økt mulighet for høygradert kommunikasjon i staten, og anbefaler at forsvarssektoren skal få tildelt ansvar for å utvikle felles løsninger for all statlig virksomhet.

Både statlig og privat virksomhet håndterer betydelige mengder informasjon som er sensitiv, men ikke sikkerhetsgradert. Hovedmengden av slik informasjon blir håndtert på systemer som ikke er godkjent for sikkerhetsgradert informasjon. Sikkerheten i IKT-systemene som behandler og lagrer sensitiv informasjon er variabel, og ofte dårlig. Mange systemer har betydelige sikkerhetsmessige mangler. EU har utarbeidet Network and Information Security (NIS)-direktivet som skal bidra til bedre cybersikkerhet i offentlig og privat virksomhet. Utgangspunktet for utarbeidelsen av NIS-direktivet er erkjennelsen av at cybersikkerhet er nødvendig for at personer og virksomheter skal kunne ha tillit til IKT-systemene og at dette er avgjørende for verdiskapingen i samfunnet. NIS-direktivet er grundigere omtalt i kapittel 8. Det digitale sårbarhetsutvalget anbefaler at Justis- og beredskapsdepartementet vurderer konsekvensene for Norge og understreker at det må ses i sammenheng med et eventuelt behov for å etablere en nasjonal minstestandard for sikkerhet i kritisk infrastruktur.

Både NSMs SFR og det digitale sårbarhetsutvalget påpeker viktigheten av gode krypteringsløsninger for å forhindre avlytting/avlesing av digital informasjon og kommunikasjon. Dette vil bli et viktig tiltak for å sikre sensitiv informasjon. I flere land diskuteres regulering av kryptering. Enkelte land og myndigheter argumenterer for at bruk av kryptering bør reguleres for å sikre myndighetenes mulighet til å avdekke sikkerhetstruende virksomhet og annen alvorlig kriminalitet. Andre mener at kryptering ikke bør reguleres. I Storbritannia arbeides det med lovforslaget «Investigatory Powers Bill». Her forslås det at leverandører av systemer som baserer seg på kryptert kommunikasjon skal lage løsninger for å kunne avlese informasjonen – å etablere såkalte bakdører. Tilsvarende forordninger blir også foreslått i en rekke andre land. Det vil kun være myndighetene som skal ha mulighet til å benytte seg av slike bakdører. Digitalt sårbarhetsutvalg anbefaler at bruk av kryptering ikke bør reguleres og tar til orde for at Norge aktivt skal arbeide mot slik regulering internasjonalt.

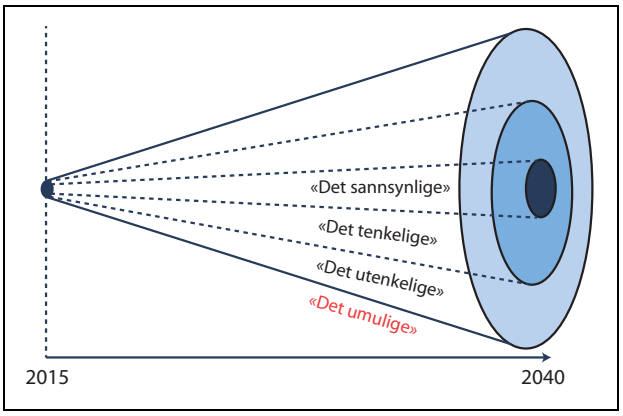
For de fleste IKT-systemer vil det være ønskelig med integrasjon mot flere andre systemer. Dette øker effektiviteten i informasjonsflyten mellom systemene. Dette fører til stadig større grad av koblinger mellom systemer, noe som fører til at sårbarheten for uautorisert tilgang til systemene øker.

4.4.4 Sårbarhet i risikostyring og sikkerhetskultur

4.4.4.1 Virksomheters risikostyring i et samfunnsperspektiv

Vi baserer samfunnets robusthet på forståelsen av hvilke risikofaktorer som kan påvirke oss, og iverksetter deretter relevante risikoreduserende tiltak. Vi foretar valg om hvordan vi vil forholde oss til ulike former for risiko. Dette kan bety at

[87] NSM, *Helhetlig IKT-risikobilde 2015*.



Figur 4.10 Utviklingsløp.

Illustrerer ulike utviklingsløp for samfunnet til bruk i strategisk planlegging. Denne metodiske tilnærmingen er også anvendelig for utvelgelse av scenarier eller hendelser som skal inngå i risikovurderinger.

Kilde: Alexander W. Beadle og Sverre Diesen, *Globale trender mot 2040 – implikasjoner for Forsvarets rolle og relevans* (Kjeller: Forsvarets forskningsinstitutt, 2015).

samfunnet a) velger å forholde seg til høy grad at usikkerhet (ukjent risikonivå), b) aksepterer en kjent risiko (risikoaksept), eller c) foretar risikoreduserende tiltak. Risikostyring er nærmere behandlet i kapittel 4.1 og 4.5.2.

Risiko for en gitt hendelse i en konkret virksomhet vil kunne vurderes som lav på grunn av at sannsynligheten for at nettopp denne virksomheten skal bli rammet er lav. Dette til tross for at konsekvensen av en eventuell hendelse vil være alvorlig. I et samfunnsperspektiv må en imidlertid vurdere den akkumulerte sannsynligheten for at en hendelse kan ramme alle tilsvarende virksomheter.

Videre vil en virksomhets egeninteresse først og fremst omfatte vurderinger av konsekvenser av ulike hendelser for egen virksomhet, og ikke nødvendigvis også omfatte konsekvenser for andre virksomheter lenger ut i verdikjeden.

Kvaliteten på risikovurderingene i de enkelte virksomheter er sårbar overfor kompetanse og ressurser for gjennomføring. Ikke minst er det utfordrende å foreta et riktig utvalg av relevante scenarier og hendelser som skal inngå i vurderingene. Det kan være spesielt krevende å fremskaffe tilstrekkelige kvalifiserte vurderinger, samt inneha nødvendig innsikt i trusler, verdier og sårbarheter, samt sannsynlighet og konsekvens forbundet med ulike uønskede hendelser. Det vil også være utfordrende å foreta vurderinger av mulige utviklingsløp for en trusselsituasjon. Det er derfor viktig å kjenne til hvilke usikkerhetsmomenter som inngår i risikovurderingene, og hvordan denne usikkerheten påvirker resultatet.

Figur 4.10 illustrerer ulike utviklingsløp for en situasjon der det skilles mellom det sannsynlige, det tenkelige, det utenkelige (men fortsatt mulige) og det umulige. Dette er en metodikk som lar seg anvende i utvalget av scenarier eller hendelser som skal inngå i en risikovurdering.

4.4.4.2 Manglende sikkerhetskultur og hendelige uhell

Truslene diskutert i kapittel 4.3 omhandler sabotasje, terrorhandlinger, hybrid krigføring og andre sikkerhetstruende hendelser. Det er likevel viktig å ikke glemme utilsiktede trusler knyttet til iboende svakheter i sikkerhetsstrukturene. Mangelfull sikkerhetskultur kan føre til hendelige uhell, det vil si at en handling får negative konsekvenser selv om personen som utførte handlingen verken hadde intensjon om å gjøre skade, eller handlet spesielt uforsiktig eller klanderverdig.

Mange virksomheter har et for lavt kunnskapsnivå, manglende opplæring av ansatte og en generelt svak sikkerhetskultur. Ifølge NSMs tilsynsrapporter er de fleste avvik i virksomheter av organisatorisk art, det vil si at avvikene kunne vært avverget dersom de organisatoriske rammene var bedre. Få teknologiske avvik skyldes teknologien alene, men at teknologiske tiltak er avhengig av menneskelige og organisatoriske tiltak. Det gir for eksempel dårlige resultater om man kjøper inn programvareoppdateringer dersom disse ikke blir installert på grunn av organisatorisk svikt.

Dårlig sikkerhetskultur i virksomheter gir utslag på ulike nivåer. Det er virksomhetens leder som er ansvarlig for virksomhetens forebyggende sikkerhet. Manglende sikkerhetskultur på dette nivået inkluderer at lederen ikke avser nok ressurser til sikkerhetsarbeidet og at sikkerhetsorganisasjonen er underdimensjonert i forhold til det reelle sikkerhetsbehovet. Også manglende evaluering av sikkerhetstilstanden og mangelfull gjennomføring av sikkerhetsmessige tiltak truer sikkerhetstilstanden.

Utilfredsstillende sikkerhetsfaglig opplæring av ansatte gjør også virksomheten utsatt for hendelige uhell. Dårlig opplæring kan skyldes at virksomheten selv har lav sikkerhetsfaglig kompetanse og derfor gir utilstrekkelig veiledning av personell som er ansvarlig for autorisasjon. Også dårlige rutiner for å sikre at den sikkerhetsfaglige kompetansen utvikles og vedlikeholdes bidrar til en mangelfull sikkerhetskultur.

En svak sikkerhetskultur kan komme fra manglende dokumentasjon av forebyggende sikkerhetsarbeid, manglende innrapportering av hendelser, mangelfulle øvelser av beredskapsplaner, mangelfull etterlevelse av lover og forskrifter og manglende veiledning og tilsyn.[88]

4.4.5 Sårbarhet i beredskap og krisehåndtering

I forbindelse med beredskap og krisehåndtering er ledelsessystemene samt kommando og kontroll-systemene avgjørende. Myndighetene er avhengige av effektiv utveksling av informasjon for å sikre et oppdatert situasjonsbilde, og for å kunne utøve effektiv ledelse. Det er derfor viktig at systemfunksjonalitet opprettholdes og at brukerne kan ha tillit til at systemene til enhver tid innehar autentisitet og integritet. Graderte kommunikasjonsplattformer kan lette kriseledelsens arbeid. Samtidig vil mangelfulle kommunikasjonsmuligheter utgjøre en sårbarhet.

Samfunnet er avhengig av IKT i ordinær drift. Behovet for IT-støtteverktøy vil øke i krisesituasjoner når mange geografisk spredte brukere skal samhandle for å håndtere de utfordringene krisene bringer med seg. I slike situasjoner kan imidlertid ikke alle brukere forvente å ha tilgang til elektroniske støttesystemer og kommunikasjonsmidler av kapasitetsgrunner. I tillegg vil kriser kunne medføre at kommunikasjonsnett blir degradert, korrumpert eller svikter helt.[89] I en krisesituasjon er det viktig å sikre effektiv krisehåndtering og raskest mulig gjenoppretting av kritiske systemer. Hensynet til liv og helse vil veie tungt.

Sårbarhetene i kommando- og kontrollinformasjonssystemer (KKIS) er direkte knyttet til sårbarhetene i IKT-systemene. Videre vil visse KKIS være avhengige av alminnelige ekomsystemer, og således arve sårbarheter fra disse systemene, som kabelbrudd, strømbrudd eller lignende. Forsvarets KKIS er bygget for å være robuste overfor en teknologisk avansert motstander. Systemene er godt beskyttet mot relevante trusler i militære operasjoner der Forsvaret i stor grad opererer uavhengig av sivile kapasiteter.

Sivile KKIS er imidlertid etablert for å dekke et større spekter av mindre hendelser, og er dimensjonert for å fungere i sitasjoner som er forbundet med naturhendelser, ulykker, eller tilsiktede uønskede hendelser. Sivile beredskapsressurser blir til stadighet anvendt i faktiske hendelser der mange ulike aktører må involveres fortløpende. Under storbrannen i Lærdal januar 2014 ble Telenors lokale infrastruktur totalt utradert. Dette kompliserte kommunikasjonen og krisehåndteringen.

Mobiletelefon har vist seg å være et av de viktigste kommunikasjonsmidlene i krisehåndtering. Også 22. juli 2011 måtte politiet ved flere anledninger lene seg på mobiltelefoni. Dette medfører alvorlige sårbarheter i tilfelle mobilnettet slutter å virke. Særlig Telenors kjerneinfrastruktur inngår som en komponent i svært mange digitale verdikjeder. Feil i Telenors mobilnett vil derfor kunne medføre alvorlige følger i en krisesituasjon. Ferdigstillingen av et nasjonalt Nødnett kan gi betydelig økt robusthet og flere ben å stå på.

Ekspertgruppen for Forsvaret har påpekt at krisehåndteringsstrukturene ikke er tilfredsstillende på øverste strategisk nivå. Dette utgjør en sårbarhet som en motstander som benytter hybride taktikker kan tenkes å utnytte. Beredskapssystemets organisering er beskrevet i kapittel 3. Ordningen med lederdepartement, og en sterk sektortenkning, kan føre til at man taper uvurderlig viktig tid i en nasjonal krise. I tillegg kan regjeringen ved å forhaste seg risikere at feil departement ender opp med eierskap til krisen.

Et eksempel på en situasjon der det måtte handles raskt er statsministerens beslutning 22. juli om at det ikke var en sikkerhetspolitisk krise som ville bety at Forsvarsdepartementet skulle ledet krisehåndteringen istedenfor Justis- og beredskapsdepartementet.[90] Dette fremstår som en enormt krevende beslutning å ta når Statsministerens kontor og Justis- og beredskapsdepartementet var utbombet og ingen kunne vite hvem som sto bak. Ekspertgruppen for forsvaret av Norge har påpekt at en mulig måte å redusere denne sårbarheten er ved å etablere et system der et forsterket SMK kan støtte statsministeren og regjeringen i arbeidet med beredskapsplanlegging og krisehåndtering, uten å rokke ved de konstitusjonelle ansvarsforholdene.[91]

---

[88] Elgsaas og Schultz Heireng, *Norges sikkerhetstilstand – en årsaksanalyse av mangelfull forebyggende sikkerhet*, 2014, 42–43.

[89] Håvard Fridheim og Janne Hagen, *Beskyttelse av samfunnet 5: Sårbarhet i kritiske IKT-systemer – sluttrapport*, FFI-rapport 01204 (Kjeller: Forsvarets Forskningsinstitutt, 2007).

[90] Bjerga, Kjell Inge og Håkenstad, Magnus, «Hvem eier krisen? Politi, Forsvar og 22. juli» i Tormod Heier og Anders Kjølberg (red.), *Mellom Fred og Krig: Norsk militær krisehåndtering* (Oslo: Universitetsforlaget, 2013).

[91] Ekspertgruppen for forsvaret av Norge, Et felles løft, 2015.

4.4.6 Militære sårbarheter

Militære sårbarheter skiller seg fra sivile sårbarheter på noen vesentlige punkter, men det grunnleggende utgangspunktet er likt. Også for Forsvaret er det sikkerhetstiltak som reduserer sårbarheten og risikoen for uønskede hendelser i møte med trusler. Sårbarhetene er særdeles store i militær sektor, men det er også sikringstiltakene. Følgelig er ikke risikoen Forsvaret lever med for uønskede hendelser særlig større enn for samfunnet utenfor. Det er i sårbarhet og iverksatte sikringstiltak at militær sektor skiller seg fra andre samfunnssektorer. Konsekvensene av et anslag mot landets forsvarsevne er dramatiske og potensielt eksistensielle for Norges overlevelse som stat.

Forsvaret er et ettertraktet mål for sabotasje og spionasje fra fremmede makter. Trusselen fra ulovlig utenlandsk etterretning på norsk jord er tiltagende i henhold til PST. Russland og Kina representerer den største etterretningstrussel mot Norge og norske interesser.[92] Overfor utvalget har PST også redegjort for konkrete sabotasjeaksjoner både mot sivile og militære mål som med stor sannsynlighet kan kobles til fremmede lands etterretningsoperasjoner på norsk jord.

Det er på denne bakgrunn at Forsvaret opererer med en annen grunnsikring og egne beredskaps- og sikringssystemer. Forsvaret setter sine egne beredskapsnivåer og har vært på et lavt, men likevel lett forsterket beredskapsnivå «Alfa» siden februar 2013. Tre og et halvt år med Alfaberedskap utgjør en ny normalsituasjon for Forsvaret. Utviklingen i trusselbildet er at Forsvaret fremstår mer utsatt i fredstid enn det har vært siden den kalde krigens slutt. Nedbygging av kapasiteter og bevilgninger til Forsvaret vil over tid også kunne gjøre Forsvaret mer sårbart og mindre motstandsdyktig mot alle trusler og utfordringer. En trussel mot Forsvaret er også en trussel mot samfunnet som helhet. Med totalforsvaret og sivil understøttelse av militære kapasiteter, er skillet mellom sivile og militære sårbarheter blitt mindre tydelig.

Totalforsvaret, som beskrevet i kapittel 3.5, innebærer sivil støtte til militær sektor og militær støtte til sivil sektor. Dette er nødvendig av hensyn til effektiv utnyttelse av ressurser, men fører med seg sårbarheter for militær sektor ettersom de sivile virksomhetene ofte ikke er innrettet for å motstå alvorlige trusler. Sårbarheten inkluderer Forsvarets avhengighet til kritiske innsatsfaktorer og kritisk infrastruktur i sivil sektor.

Forsvar handler om å kunne stanse ytre trusler med militærmakt i en potensiell konfliktsituasjon. Forsvaret er avhengig av tilstrekkelig operativ evne for å være troverdig og å ha en avskrekkende effekt. Forsvarets operative evne er et produkt av reaksjonsevne, kampkraft og utholdenhet. Dagens militære utfordringer knytter seg blant annet til at det forventes kortere reaksjonstider, samt en rask teknologisk utvikling som fører til mer avanserte våpen med høy effekt, og som det er vanskelig å beskytte seg mot. Eksempler på dette er utviklingen i cyberområdet og langtrekkende presisjonsvåpen. Forsvaret må kontinuerlig moderniseres for å opprettholde forsvarsevnen. Levetiden på mye av Forsvarets materiell må også forventes å være kortere enn tidligere på grunn av den teknologiske utviklingen.

Moderne forsvar er avhengig av avanserte og kostbare våpensystemer. Økt kostnadsnivå og høy effektivitet fører til at antallet enheter som regel er relativt lavt i forhold til tidligere tiders våpensystemer. Få, men avanserte våpenplattformer er effektivt så lenge de kan beskyttes mot en fiende. Dersom beskyttelsen ikke er effektiv vil våpenplattformene raskt bli ødelagt av motstanderen. Informasjon om militære våpensystemer har alltid vært svært følsomt, ettersom det er nøkkelinformasjon som kan avgjøre utfallet av en konflikt dersom den blir kjent for motstanderen.

Samfunnsutviklingen med økt privatisering og internasjonalt samarbeid i forsvarsindustrien fører imidlertid til nye utfordringer. At slik teknologi er tilgjengelig for en rekke andre aktører og stater fører til at det er vanskelig å sikre seg mot at viktig informasjon kommer på avveie. Dette forsterkes ytterligere ved at det sivile samfunn i stadig større omfang bidrar til både nyvinning og produksjon av teknologi som Forsvaret er avhengig av i sitt materiell.

Moderne forsvars avhengighet til avanserte og kostbare våpensystemer har ført til økt internasjonalt samarbeid ved utvikling og innkjøp av militært utstyr. Et eksempel på dette er NATOs *Smart Defence*, hvor allierte går sammen om å utvikle viktige kapasiteter. I tillegg til NATOs ulike samarbeidsprosjekter finnes det en rekke bilaterale direkte samarbeidsavtaler vedrørende anskaffelser og utvikling av militært utstyr. NATO trenger moderne militære kapasiteter for å sikre sin relevans og troverdighet. Imidlertid har over halvparten av NATOs medlemsland kuttet mer enn 10 % i forsvarsutgiftene etter finanskrisen i 2008. USA dekker om lag 70 % av NATOs utgifter, og har over lang tid utrykt at denne skjeve byrdefordelin-

[92] PST, *Trusselvurdering 2015.*

gen ikke kan fortsette, særlig i lys av at de fleste store truslene er på europeisk side.[93]

NATO-medlemskapet spiller en nøkkelrolle i norsk sikkerhetspolitikk. Ubalansen i NATOs interne byrdefordeling og potensielt svakere amerikansk lederskap representerer derfor en alvorlig sårbarhet. Dette er eksistensielle temaer for NATO som kan rokke ved hele stabiliteten i Europa og gjøre alle stater mer usikre og sårbare. I sikkerhetspolitikken kan usikkerhet om intensjoner og forpliktelser være like farlig som høyt spenningsnivå i en oversiktlig situasjon.

Forsvaret står overfor trusler fra alle tre hovedformer for uønskede tilsiktede hendelser: terrorisme, sabotasje og etterretning. Det er tale om konkrete trusler som kan ramme Forsvarets kjerneoppgaver og Forsvarets nøkkelpunkter. Selv om utviklingen knyttet til militære sårbarheter må sies å være klart negativ, som en konsekvens av trender i internasjonal terrorisme og forringelse av Vestens forhold til Russland og Kina, så er Forsvaret en aktør som er konstruert nettopp for å møte sikkerhetsutfordringer.

4.4.7 Sårbarheter for demokratiske samfunn

Samfunnets sårbarheter handler om mer enn kritisk infrastruktur og statssikkerhet i militær forstand. Siden 90-tallet har sikkerhetsbegrepet blitt utvidet og har i større grad omfattet det sivile samfunn og det enkelte individs sikkerhet. Borgernes forventninger til i hvilken grad staten skal beskytte dem mot ulike farer er høye og ikke alltid realistiske. Dette tydeliggjøres under kriser, også i utlandet. Tsunami-katastrofen og kritikken av Utenriksdepartementets håndtering av flodbølgekatastrofen er et eksempel.

Blant de mest toneangivende innspill om samfunn og individenes håndtering av risiko er den tyske sosiologens Ulrich Becks akademiske produksjon om risikosamfunnet. En oppdatert gjennomgang av feltet på norsk finnes i boken Perspektiver på samfunnssikkerhet. Beck beskriver «hvordan den samfunnsmessige utviklingen bidrar til å skape nye trusler som krever helt nye måter å tenke på hvis vi skal kunne beskytte oss».[94]

Beck mener videre at risikoaversjon preger vårt moderne samfunn, med forventninger om at samfunnet i utstrakt grad skal sikre individene mot det brede spekter av trusler. Denne typen tenkning er en vesentlig premissleverandør for begrepet samfunnssikkerhet. Det holder ikke i dag at staten sikrer landets yttergrenser, og at innbyggerne deretter ivaretar sin egen sikkerhet innenfor den etablerte rettsorden. Befolkningen forventer mer.

Vi garderer oss kontinuerlig mot ulike typer risiko i dagliglivet. Sikkerhetstiltakene innbyggerne gjør seg i det daglige liv er i noen grad en refleksjon av samfunnets forebyggende sikkerhetstiltak. Når innbyggerne utviser lite risikoaksept privat vil resultatet kunne bli et samfunn som viker unna risiko. Her finnes en fallgruve der et bevisst og nøkternt forhold til risiko og sikkerhet kan gli over i overdreven frykt for moderate – og i verste fall fiktive eller ufarlige – trusler.

Dette reiser demokratiske problemer. Et av dem handler om risikoaksept og restrisiko rundt terrorangrep. Forestillingen om at myndighetene kan avverge ethvert terrorangrep vil kunne lede til inngripende kontraterror-tiltak som undergraver demokratiske rettigheter til privatliv og ytringsfrihet. I USAs krig mot terror har *The Patriot Act* og *National Security Agencys* utstrakte registrering av kommunikasjon utfordret grensene for hva en demokratisk stat kan foreta seg i den hensikt å beskytte landet mot terrorhandlinger.

Mediene i pluralistiske samfunn vil alltid måtte vurdere om noe(n) har feilet i sikkerhetssektoren de gangene terrorister lykkes med et angrep. Etterspillet etter et terrorangrep kan forlede både mediene selv og befolkningen til å overse restrisikoen som utgjør et ikke-fjernbart handlingsrom for terrorister. Det er lett å si seg enig i at total og fullkommen beskyttelse mot terrorisme hverken er oppnåelig eller ønskelig. Noe helt annet er det å innrømme etter at liv har gått tapt at det dessverre var lite samfunnet kunne gjort annerledes.

Terroristen som gjennomførte 22. juli-angrepene opererte på en måte som gjorde det svært vanskelig å oppdage og avverge angrepet. Hans planlegging av terrorvirksomheten kan illustrere handlingsrommet som finnes i den restrisiko som gjenstår etter myndighetenes implementerte sikkerhetstiltak. Gjørv-kommisjonen konkluderte med at angrepet ikke var umulig å stoppe, men at det heller ikke var grunnlag for å klandre PST for at så ikke skjedde. Kommisjonen var hardere i sin dom rundt svikten i det forebyggende objektsikringsarbeid rundt regjeringskvartalet. Disse punktene sto helt sentralt i Gjørv-kommisjonens konklusjon og utgjorde to av kommisjonens seks hovedkonklusjoner som gjengitt under:

---

93 Prop. 151 S (2015–2016), 31.

94 Ole Andreas H. Engen et al, *Perspektiver på samfunnssikkerhet* (Oslo: Cappelen Damm, 2016), 37.

> Angrepet på regjeringskvartalet 22/7 kunne ha vært forhindret gjennom effektiv iverksettelse av allerede vedtatte sikringstiltak. […] Med en bedre arbeidsmetodikk og et bredere fokus kunne PST ha kommet på sporet av gjerningsmannen før 22/7. Kommisjonen har likevel ikke grunnlag for å si at PST dermed kunne og burde ha avverget angrepene.[95]

Misoppfatninger om hva sikkerhetsmyndigheter faktisk kan forventes å avverge, gitt skrankene og føringene for deres arbeid, er en skummel fallgruve. Samfunnet kan ende opp med å stille urimelige krav til beskyttelse overfor aktører som PST og E-tjenesten. Tilliten mellom sikkerhetstjenestene, regjeringen og befolkningen kan undergraves dersom forståelsen av trusselbildet og muligheten til å avverge terror spriker for mye aktørene imellom. En slik tillitssvikt utgjør et demokratisk problem da behovet for beskyttelse mot ytre trusler og vold utgjør en del av samfunnskontrakten i liberale samfunn.

4.4.7.1 Sårbarheter overfor strategisk kommunikasjon og informasjonsoperasjoner

Den frie presses viktige samfunnsoppdrag som nyhetsformidler og kilde til objektiv informasjon har blitt utfordret av økt kommersialisering og fremveksten av sosiale medier. Utviklingen har på mange måter demokratisert mediene ved at mangfoldet av informasjonskanaler har økt og det aldri tidligere har vært lettere å nå ut til omverden med sine synspunkter. Spredningen av informasjon skjer også hurtigere enn før. Flere konflikter i Midtøsten, inkludert Den arabiske våren, har vist hvilken kraft sosiale medier kan ha på politikken i konfliktsituasjoner.

PST fremhever i sin trusselvurdering for 2016 hvordan enkelte etterretningstjenesters bruk av informasjons-, påvirknings- og propagandaoperasjoner i andre land har som målsetting å svekke tilliten til myndighetene eller skape motsetninger. At slike strategier tas i bruk i perioder med høy spenning er noe også Norge må være forberedt på.[96] Under en tilspisset sikkerhetspolitisk krise vil en motstander kunne så tvil om blant annet myndighetenes intensjoner om og evne til å beskytte befolkningen mot voldelige anslag fra terrorister eller andre kriminelle.

Det digitale rom og internett spiller en viktig rolle som kamparena i moderne konflikter og kriger.[97] Strategisk kommunikasjon, eller stratkom, er en sentral faktor for å vinne i konflikter. Kommunikasjonen av strategiske narrativer kan være avgjørende for utfallet av en konflikt og fører derfor til en kamp mellom stater, organisasjoner, og i økende grad også enkeltindivider, om å definere eller etablere «sannheter» om konflikten. Strategiske narrativer kan spres gjennom sosiale medier, som for eksempel Facebook, Twitter, Instagram, blogger og YouTube. Under krigføringen i Gaza og i Syria ble særlig Facebook og Twitter brukt aktivt av mange parter. Lokalbefolkning og andre vitner bidrar kontinuerlig til rapportering fra slagmarken. På den digitale slagmarken har også andre grupper engasjert seg, eksempelvis nettaktivister og hackergrupper. Anonymous tok for eksempel palestinernes side i den siste Gaza-konflikten, og utførte millioner av angrep mot israelske nettsider.[98]

Informasjons- og kommunikasjonsinfrastruktur er ofte klare militære mål under væpnet konflikt, med Balkan, Irak, Georgia, Nord-Afrika og Midtøsten som eksempler. På Balkan og i Irak angrep koalisjonsstyrkene både elektrisitetsforsyning og kringkastingsinfrastruktur. De siste årene har vist at internettet i seg selv er blitt et mål – myndighetene i Syria tok ned internettforbindelsen for å hindre at opprørere organiserte seg. Dette understreker behovet for evne til å håndtere bortfall av informasjons- og kommunikasjonsinfrastruktur.[99] Angrep på informasjons- og kommunikasjonsinfrastruktur kan gjennomføres i en så tidlig fase av en konflikt at det ennå ikke er definert som en sikkerhetspolitisk krise, og det vil kunne utføres med fordekte midler som også vil gjøre det vanskelig å knytte hendelser til en av partene i konflikten.

Både angrep på informasjons- og kommunikasjonsinfrastruktur og psykologiske operasjoner benyttes som del av hybride krigsstrategier. Målsettingen trenger ikke å være full kontroll på informasjonsflyten, men kan være å sette ut så mange ulike historier at befolkningen forvirres. Vi vurderer den informasjonen vi får basert på hvilken annen informasjon som er tilgjengelig. Når majoriteten av informasjon tilgjengelig er manipulert blir man fanget i et system av falske oppfatninger.

---

95 NOU 2012: 14, *Rapport fra 22. juli-kommisjonen, 449.*

96 Politiets sikkerhetstjeneste, *Trusselvurdering 2016*, 8.

97 Henning André Søgaard og Janne Merete Hagen, *Kampen om Sannheten,* FFI-Fokus 02 (Kjeller: Forsvarets forskningsinstitutt, 2014), 2.

98 Janne Merete Hagen og Henning André Søgaard, *Strategisk kommunikasjon som redskap i Krisehåndtering*, FFI-rapport 03101 (Kjeller: Forsvarets Forskningsinstitutt, 2013), 18.

99 Ibid.

Økt bruk av internett og fremveksten av sosiale medier har økt antallet kanaler slik desinformasjon kan spres gjennom. Å villede gjennom desinformasjon, undergraving av sannheten og manipulering av nyheter, kan støtte opp under militære virkemidler. Dette gjøres på nye og mer omfattende måter i dag. Skjønt, allerede for 2500 år siden slo Sun Tzu fast at «all warfare is based on deception».[100]

Under andre verdenskrig benyttet begge sider strategisk kommunikasjon, herunder propaganda og psykologisk påvirkning i stort monn. Under den kalde krigen var frontene mellom øst og vest stabile og det utspant seg en statisk kamp mellom klassisk sovjet-propaganda og Vestens frihets- og demokratiidealer. Bildet ble langt mer flytende og dynamisk etter murens fall. Under Balkan-krigene på 90-tallet ble manipulering av mediene og villeding av befolkningen brukt aktivt som en del av krigsstrategien. I 1992 trodde 20,5 % av Beograds befolkning at det var serberne som bombarderte Sarajevo, mens 38,4 % trodde det var muslimsk-kroatiske styrker.[101]

Den første Gulfkrigen er også en stilstudie i manipulasjon av befolkningers persepsjoner om krig. Presisjonsbombing, 100 timers-krigen, samt Iraks informasjonsminister «Komiske Ali» er blant levningene etter denne første krigen som ble mediedekket i sann tid. Nærmere vår tid er krigen mot terrorisme et eksempel på en krig der forestillinger og narrativene om krigen har vært helt avgjørende for krigens utfall. Obama valgte å ikke videreføre konseptet *krig mot terror*, ikke minst fordi negativt ladede tortur-narrativer var blitt knyttet tett opp mot krigen. Guantanamo, Waterboarding og kidnappinger utgjorde etter hvert uslettelige moralske pletter på krigen mot terrors omdømme, som var lite forenlige med grunnleggende demokratiske verdier. Dette ledet til økt sårbarhet fordi det undergravde legitimiteten til hele krigen mot terror og det utstrakte forebyggende sikkerhetsapparatet krigen brakte med seg.

Under Ukraina-krisen var informasjons- og kommunikasjonsinfrastrukturen både utsatt for angrep som førte til bortfall og psykologiske operasjoner for å påvirke meningsdannelsen. Ukrainske kommunikasjonskanaler ble utsatt for cyberangrep som resulterte i at Krimhalvøya ble avskåret fra omverden. Samtidig foregikk en informasjonskampanje der hovedbudskapet var beskyttelse av russiske minoriteter.[102] Undersøkelser viser at antallet som støttet løsrivelse og ønsket å bli en del av Russland økte kraftig som et resultat av ensidige tv-sendinger som fokuserte på hvordan etniske russere på Krim ville bli annenrangs borgere i Ukraina.[103] Russlands bruk av propagandaverktøy og psykologiske operasjoner som del av sin informasjonsstrategi støttet den militære anneksjonen av Krim.

Ulike aktørers satsning på strategisk kommunikasjon skaper utfordringer for pluralistiske samfunn der mediene spiller en sentral samfunnsrolle. I tillitbaserte samfunn stilles det store krav til mediene om at de skal informere befolkningen om viktige spørsmål og utviklingen lokalt, regionalt og globalt. 22. juli var en påminner om hvor vanskelig det kan være å verifisere informasjon når krisen treffer. Etablerte systemer og rutiner klarte ikke å håndtere trykket, og det oppsto et vakuum der en flom at vitner og egenobservasjoner fikk spillerom uten den nødvendige kontakten med politiet for å bekrefte eller avkrefte ryktene.[104] Mange medier og kommentatorer gikk langt i å feilaktig antyde at islamistiske grupperinger eller Al-Qaida sto bak angrepet.[105]

Når man ser hvor misvisende deler av mediedekningen rundt 22. juli ble, helt uten noen kapabel villedende motstander, forstår man at rommet for en høykompetent hybrid-motstander til å manipulere norske medier og offentlighet utgjør en betydelig sårbarhet. I en situasjon der ressurssterke aktører utnytter alle informasjonskanaler for å bedrive propaganda og fordekt strategisk kommunikasjon, må mediene være spesielt ryddige med å oppgi kilden til informasjonen de kommuniserer. Dette må gjøres gjennom hele informasjonskjeden, slik at det fremkommer hvem som angivelig er primærkilde.

Hybride strategier er designet nettopp for å være uhåndgripelige og uhåndterlige og sette motparten ut av balanse. Det er vanskelig å iverksette egnede mottiltak mot hybride trusler siden de vanskelig lar seg identifisere, og preges av *high deniability*. Som et tillitsbasert samfunn, og som en av de mest digitaliserte landene i verden, kan Norge vært utsatt for aktører som ønsker å misbruke strategisk kommunikasjon for å påvirke

---

[100] Sun Tzu, *The Art of War* (Oxford: Oxford University Press, 1963), Chapter 1.

[101] Jonathan Glover, *Humanity: A Moral History of the Twentieth Century* (London: Pimlico, 2001).

[102] Hagen og Søgaard, 2013.

[103] Kofman, Michael og Matthew Rojansky, «A Closer look at Russia's 'Hybrid War'», Kennan Cable 07 (Wilson Center / Kennan Institute, 2015).

[104] Hagen og Søgaard, 2013, 14.

[105] Morgenbladet, «Analyse i kaos», 05. 08. 2011.

meningsdannelsen i opinionen, mobilisere en befolkning eller skape motsetninger.[106]

Det er manglende langsiktig strategisk tenkning på politisk nivå om hvilke effekter informasjons-, påvirknings- og propagandaoperasjoner kan ha, og hvordan den økte bruken av sosiale medier kan misbrukes til å villede og påvirke befolkningen. Verken Forsvaret eller befolkningen forøvrig er særlig godt forberedt til å møte slike trusler. For å redusere sårbarheten er det behov for mottiltak mot slike strategier, og økt bevissthet rundt truslene. For en liten stat vil maktmidlene i en krise oftere være internasjonal rett, diplomati, diskreditering av propaganda snarere enn militærmakt. Strategisk kommunikasjon er derfor en (krise)ressurs for Forsvaret. NATO satser også på strategisk kommunikasjon i sin strategi og alliansens retningslinjer vil også gjelde for Norge. Norge bør være i stand til å bruke slike digitale plattformer på en mer strategisk målrettet måte i framtiden.[107]

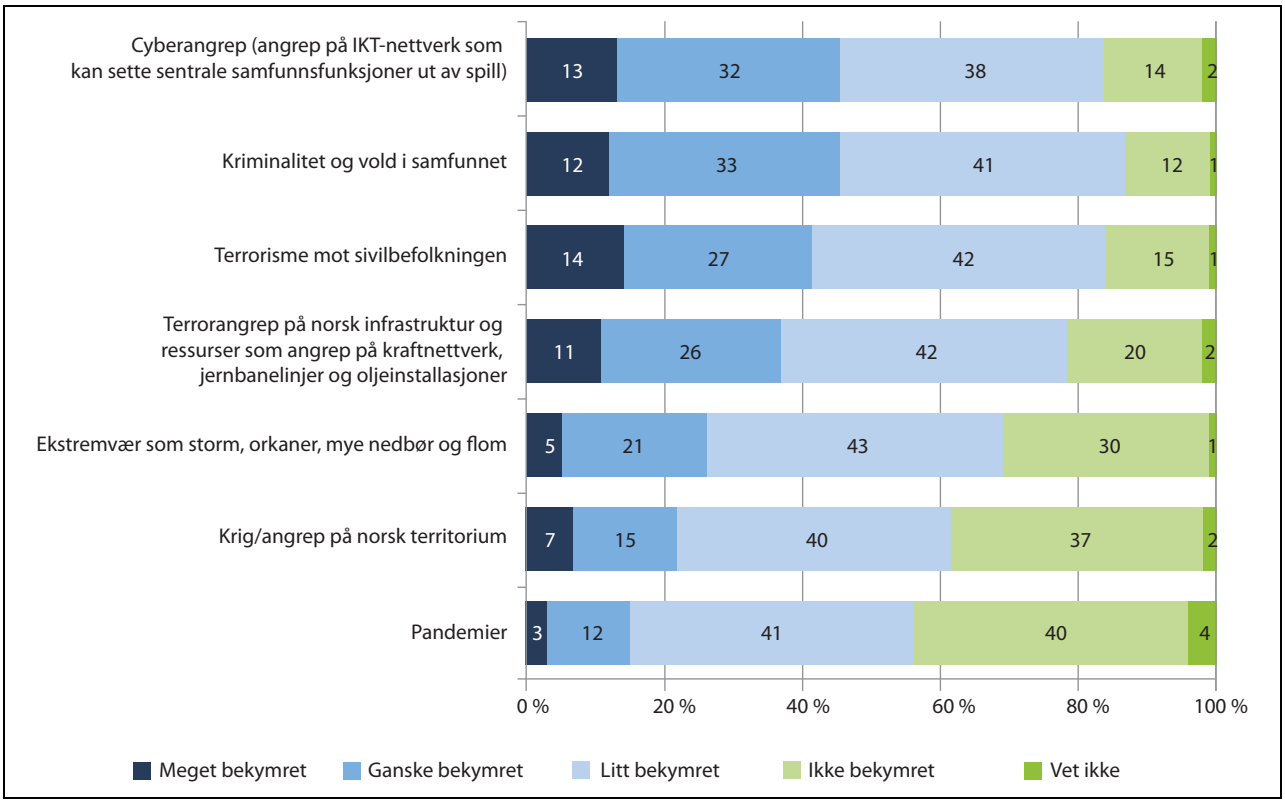
[106] Hagen og Søgaard, 2013, 19.
[107] Ibid.

4.4.7.2 Politiske prioriteringer

Liberale demokratiers styrke ligger i at det er befolkningen som gjennom sine valgte representanter bestemmer hvordan ressurser benyttes og skal fordeles. Det er dermed viktig at befolkningen er godt opplyst om hvilke utfordringer som må løses og har god forståelse for det faktiske ressursbehovet. Med stadig internasjonalisering og økende kompleksitet i samfunnet øker befolkningens behov for informasjon. Den teknologiske utviklingen har ført til en enorm effektivisering av informasjonsspredning, og informasjon er tilgjengelig for befolkningen i langt større grad enn tidligere. Dette skaper imidlertid utfordringer for den enkelte i å velge ut relevant informasjon.

Befolkingens kunnskapsnivå og tilgang til informasjon er styrende for hvilke trusler som anses som viktigst å sikre seg mot. Forsvaret gjennomfører innbyggerundersøkelser for å kartlegge hvilke trusler mot nasjonal sikkerhet norske innbyggere er mest bekymret for. Funnene av innbyggerundersøkelsen fra 2015 vises under.

Forebyggende sikkerhetsarbeid er kostbart, og ofte brukes penger på tiltak man håper man aldri får bruk for. Det er derfor viktig at informasjon er tilgjengelig for å gi befolkning og politikere et godt grunnlag for å forstå situasjonen og



Figur 4.11 Graden av bekymring i befolkningen knyttet til ulike typer trusler.

Kilde: Forsvarets innbyggerundersøkelse 2015.

diskutere alternative løsninger og tiltak. Økt åpenhet fra etterretnings- og sikkerhetsmiljøene omkring trussel og sikkerhetssituasjonen har vært en trend i de fleste vestlige demokratier de siste tiårene. E-tjenestens og PSTs åpne trusselvurderinger, samt NSMs årlige vurdering av sikkerhetssituasjonen og DSBs Nasjonalt risikobilde, er alle gode eksempler på dette.

Større endringer i politiske prioriteringer, nasjonalt og internasjonalt, kan medføre endringer i trusselsituasjonen. Dette kan videre bidra til endringer som påvirker hvilket nivå det må være på sikkerheten. Eksempelvis kan informasjon som oppfattes som ikke-skjermingsverdig på et tidspunkt, og som blir skjermingsverdig ved endringer i trusselbildet eller sikkerhetssituasjonen, skape utfordringer. På samme måte kan det føre til at visse typer virksomhet får et større beskyttelsesbehov enn tidligere, noe som krever ressurser for å få iverksatt nødvendige tiltak raskt.

4.5 Virkemidler for å oppnå nasjonal sikkerhet

Kapittel 4.2, 4.3 og 4.4 omtaler henholdsvis verdier, trusler og sårbarheter som sammenstilt gir et bilde av risiko for at tilsiktede uønskede hendelser skal ramme verdiene vi ønsker å beskytte. Regulering av forebyggende sikkerhet har som formål å redusere risiko (eller øke sikkerheten) i samfunnet. Forebyggende sikkerhetstiltak vil hovedsakelig rette seg mot å redusere sårbarhetene i samfunnet. Det er imidlertid en viktig og sterk sammenheng mellom sårbarhetene i samfunnet og hvordan samfunnsutviklingen endrer hvilke verdier som må beskyttes, samt hvordan truslene utvikler seg. Som omtalt i innledningen til kapittel 4.3 om trusler, vil blant annet et høyt sikkerhetsnivå endre kost-/nyttevurderingene hos en potensiell trusselaktør slik at intensjonen om å utføre handlinger som forårsaker skade bortfaller.

Bruk av virkemidler må ses i sammenheng for å sikre god effekt. Effekten av virkemidlene må betraktes ut i fra et samfunnsøkonomisk perspektiv. Dette blir omtalt i første del av kapittelet. Videre i dette kapittelet gjennomgås bruk av ulike virkemidler og hvordan disse kan benyttes ut ifra generelle betraktninger. Utvalgets vurderinger av hvordan den lovmessige reguleringen av forebyggende sikkerhet bør innrettes på ulike tematiske områder fremkommer i del III. Der blir det også redegjort for tilfeller der utvalget mener lovregulering bør suppleres med andre virkemidler.

4.5.1 Samfunnsøkonomisk lønnsomme tiltak

Samfunnets ressurser er knappe og mange formål i samfunnet konkurrerer om de samme ressursene, både i offentlig og privat virksomhet. Samfunnsøkonomiske analyser er et verktøy som brukes i offentlig forvaltning til å identifisere og belyse konsekvensene av tiltak. Før en beslutning skal tas bør vi ha et tydelig bilde av hvilket samfunnsproblem som bør løses og hvilke måter det kan løses på. Ulike tiltak vil ha ulike positive og negative konsekvenser for ulike aktører i det offentlige, i det private næringsliv, for privatpersoner og andre grupperinger.

Det er aktørenes samlede konsekvenser som utgjør den samfunnsøkonomiske lønnsomheten, og som påvirker samfunnets velferd. Aktørene kan være alt fra samfunnet som helhet til ulike grupper i samfunnet i privat eller offentlig sektor. Samfunnsøkonomisk lønnsomhet viser altså hva som er best for Norge som helhet – vurdert ut fra konsekvenser for enkeltgrupper. Gjennom mandatet er utvalget bedt om å ta slike hensyn. I mandatet står det følgende:

> Forslaget skal sikre en kostnadseffektiv regulering, som sikrer balanse mellom akseptabel restrisiko, og kostnaden for sikkerhetsnivået. Samfunnsøkonomisk lønnsomhet skal være en grunnleggende forutsetning, dvs. at aktuelle sikringstiltak må ha en samfunnsøkonomisk nytte som samlet overstiger kostnadene.

Der hvor utvalget lander på en løsning hvor sikkerhetstiltakene skal spesifiseres i lov, må det altså gjøres slike vurderinger. Alternativet til å spesifisere krav til sikkerhetstiltak i loven er å spesifisere hvem som har myndighet til å beslutte hvilke tiltak som skal gjennomføres og å stille krav til hvordan prosessen som leder frem til beslutning skal være. I slike tilfeller vil det være nødvendig å fastsette at slike vurderinger skal være en del av beslutningsgrunnlaget.

Det er viktig for utvalget å understreke at det er foretatt vurderinger av konsekvensene av de løsninger som er foreslått. Det er vurdert konsekvenser i vid forstand, der hovedeffektene av de foreslåtte tiltak vil ha sikkerhetsmessige konsekvenser, personvernkonsekvenser og økonomiske konsekvenser. Nytte- og kostnadsvurderinger vil altså innbefatte alle slike typer virkninger.

I utvalgets kontekst skal det vurderes ulike typer sikkerhetstiltak som kan iverksettes. Utvalget vurderer alt fra et utvidet virkeområde for

loven, til mer organisatoriske tiltak. Nytten av utvalgets anbefalte tiltak vil tilfalle mange samfunnsaktører. Felles for de fleste gjelder det at de tilfaller samfunnet som helhet – vi får det tryggere. I tillegg vil mange sikkerhetstiltak spesielt tilfalle noen sektorer eller grupper i en sektor. Det enkelte tiltak som iverksettes på virksomhetsnivå vil også ha nytte for enkeltvirksomheter i form av for eksempel sikrere IKT-systemer og bedre sikkerhet mot alvorlig kriminalitet eller robusthet mot uhell eller naturhendelser. Tiltakene gjør både virksomhetens aktivitet og deres brukere og kunder tryggere.

Iverksetting av tiltak vil i de fleste tilfeller også føre med seg ulemper av enten kostnadsmessig art eller andre typer ulemper, som for eksempel inngrep i personvernet. Kostnader ved tiltak vil gjerne i første rekke dukke opp på virksomhetsnivå. Kostnader kan være alt fra direkte investerings- eller driftskostnader, eller andre typer ulempekostnader som blant annet kan følge av forsinkelse av prosesser som følge av omfattende og tidkrevende prosedyrer. Enkeltvirksomheter vil sannsynligvis være opptatt av hva utvalgets forslag vil bety for dem – gjerne i form av kostnader med direkte utslag på bunnlinjen, eller i form av mulige konkurransefordeler eller -ulemper. Slike konsekvenser er inkludert i utvalgets vurderinger av den samfunnsøkonomiske lønnsomheten av tiltakene.

Så langt utvalget er i stand til, gis det en beskrivelse av positive og negative konsekvenser av forslagene. Dette inkluderer å synliggjøre hvilke aktører i samfunnet som drar nytte av tiltakene, og hvem som bærer kostnadene. For noen enkelttiltak som utvalget foreslår, vil det være mulig å gi et mer konkret bilde av hva nytten av tiltaket består i, og hvem som forventes å måtte bære kostnaden, samt hva den består av. Utvalget er imidlertid ikke i stand til å beregne hva nytten og kostnaden samlet sett vil bli for summen av de enkeltaktører som blir påvirket, som utgjør samfunnet i vår vurdering.

En viktig årsak til at de fleste konsekvensvurderingene er begrenset til en overordnet beskrivelse, er at utvalget kun skal utrede lovgrunnlaget, som på mange områder vil være innrettet med overordnede formuleringer. Den detaljerte utformingen og operasjonaliseringen av lovgrunnlaget vil måtte utformes i forskrifter. Dette innebærer at konsekvensene først kan beregnes i den etterfølgende fasen av lovarbeidet. Selv i den etterfølgende fasen vil det sannsynligvis være vanskelig å beregne den samfunnsøkonomiske nettonytten ut fra kjente verdsettingsutfordringer, spesielt på nyttesiden. Et eksempel vil være problemene som oppstår hvis en prøver å gi gode, kvantifiserte anslag på nytten av økt sikkerhet i Norge.

Et annet ytterligere kompliserende poeng i konsekvensvurderingen er at utvalgets forslag utgjør en helhet, og tiltakene og virkningene vil påvirke hverandre. Det er den samlede porteføljen av tiltak utvalget foreslår som vil ha den ønskede effekten på samfunnets sikkerhet.

4.5.2 Risikoreduserende tiltak, restrisiko og risikoaksept

Staten har et bredt spekter av virkemidler som kan benyttes for å sikre at samfunnsutviklingen går i ønsket retning. Myndighetene kan benytte ulike styringsverktøy for å påvirke menneskers og virksomheters handlemåte. Tiltak kan benyttes som en fellesbetegnelse for de handlinger myndighetene ønsker å utløse med sin virkemiddelbruk. Tiltak omfatter både fysiske tiltak (for eksempel installering av rotasjonsporter eller kameraovervåkning) og atferdsendringer (for eksempel større forsiktighet med bruk av skytjenester). Virkemidlene innrettes på ulike måter. Eksempelvis kan de innrettes for å sikre at spesifikke sikkerhetstiltak blir gjennomført, alternativt kan de kan bidra til å styre prosessene og vurderingene som leder frem til valget av hvilke tiltak som blir gjennomført. De viktigste virkemidlene staten benytter er oppsummert i figur 4.12. Utvalgets mandat er å utrede lovregulering av forebyggende nasjonal sikkerhet. Samtidig skal samfunnsøkonomisk lønnsomhet være en forutsetning, slik det er beskrevet ovenfor.

Utvalget legger vekt på at utgangspunktet for oppnevnelsen av utvalget er behov for en lovregulering som tar inn over seg utviklingen i samfunnet. Utvalget har derfor vært opptatt av at utredningen må gjenspeile at lovregulering er ett av virkemidlene som kan benyttes, og at lovregulering må ses i sammenheng med en mer helhetlig strategi for bruk av virkemidler.

Valg av virkemidler for å oppnå god nasjonal sikkerhet kan settes inn i en helhetlig risikostyringskontekst, som omtalt i kapittel 4.1, der man sammenholder ulike typer risiko og risikoreduserende tiltak. Beslutninger om hvilket sikkerhetsnivå man ønsker og dermed hvilke tiltak som kan gjennomføres for å oppnå dette nivået, sett opp mot ulempene tiltakene fører med seg, vil være viktig. Her vil virkemiddelbruk ha stor betydning for både sikkerhetsnivået og ulempene det medfører.

Fastsettelse av sikkerhetsnivå og valg av sikkerhetstiltak er komplisert. Samfunnsøkonomiske analyser kan benyttes som et verktøy for å velge hvilke tiltak som skal gjennomføres. Slike analyser gjøres ved å sammenlikne ulike alternative løsninger og vurdere fordeler og ulemper i de ulike alternativene. Grunntanken bak den samfunnsøkonomiske analysen vil således kunne benyttes for både fastsettelse av hvilket sikkerhetsnivå som er ønskelig, hvilke tiltak som bør iverksettes for å nå sikkerhetsnivået, samt hvilke virkemidler som skal benyttes for å styre iverksettelsen av ulike typer tiltak. Forebyggende nasjonal sikkerhet er som beskrevet i de foregående kapitler avhengig av mange forhold og krever et bredt spekter av tiltak. Det ligger derfor i sakens natur at det vil være behov for en sammensatt virkemiddelpakke. Det ligger også i sakens natur at det å vurdere risiko og iverksette risikoreduserende tiltak vil være en kontinuerlig prosess. Som en del av dette bildet vil det selvfølgelig også være en vurdering av hvilke risikofaktorer det vil være samfunnsøkonomisk lønnsomt å gjøre noe med. I tillegg kommer tilfellene der det ikke finnes tilstrekkelige relevante tiltak og det derfor vil være nødvendig å leve med risikoen. Det kan også være komplisert å forutsi effekten av sikkerhetstiltak. Dette skyldes at det i mange sammenhenger vil være mange prosesser og faktorer som virker inn på hverandre. Dette vil være spesielt relevant i forbindelse med det å forhindre tilsiktede uønskede hendelser fordi tiltakene som iverksettes her vil påvirke trusselaktørenes strategi og taktikk. Et eksempel på dette er hvordan norsk deltagelse i internasjonale operasjoner er innrettet for å redusere fremveksten av internasjonal terrorisme påvirker sikkerhetssituasjonen i Norge. Internasjonal terrorisme oppfattes å utgjøre en av de mest alvorlige truslene mot samfunnet. Bidrag i slike operasjoner er viktig for norsk sikkerhet både på grunn av viktigheten av å vise handlingsvilje overfor allierte, og på grunn av behovet for å stabilisere områder som er i negativ utvikling. Slik deltakelse kan imidlertid føre til at Norge blir et mål for de aktuelle terrorgrupperingene. Videre vil det å iverksette en militær operasjon i et område kunne føre til at flere mobiliseres for deltagelse i kamphandlingene, og dermed kan føre til en eskalering av konfliktnivået.

Et av grunnelementene med samfunnsøkonomiske analyser er å være tydelig på hvilke mål vi ønsker å oppnå med tiltak. Tydelige mål vil være med på å sikre at virkemidler som blir innført for å løse et problem ikke fører til at andre grunnleggende verdier rammes. Et eksempel på slike motstående målsettinger kan være knyttet til det å opprettholde høy sikkerhet og samtidig legge til rette for rask utvikling i cyber-området. Streng regulering og streng kontroll vil legge begrensninger på hvordan tjenester og produkter utvikler seg, men vil gjøre det lettere å sikre viktige systemer og funksjoner mot cyber-angrep.

4.5.3 Statens styring og bruk av virkemidler

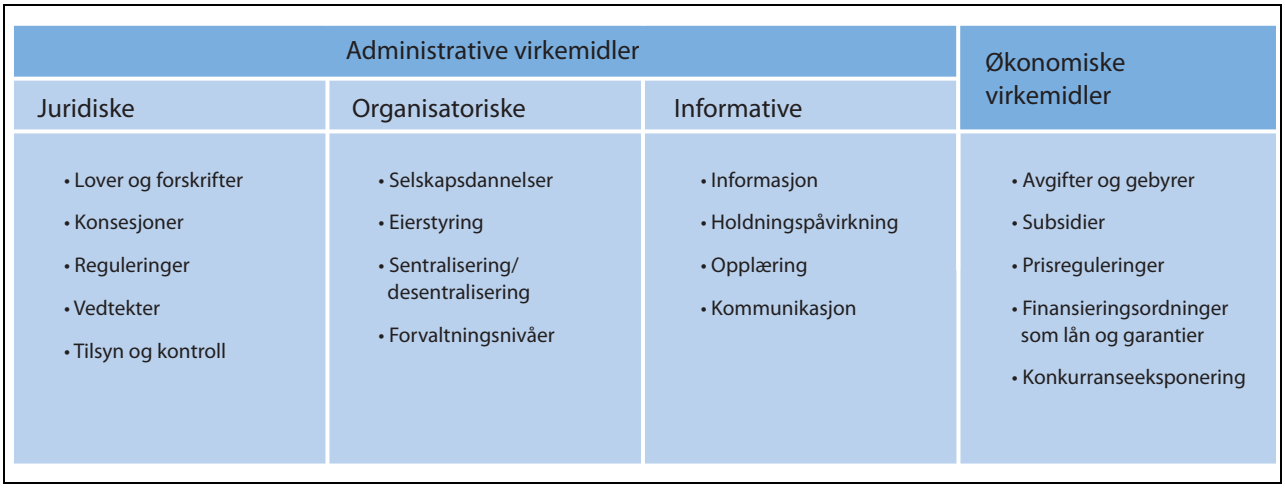
Som det fremkommer av figur 4.12 er det to hovedtyper av virkemidler: administrative og økonomiske. Administrative virkemidler er en fellesbetegnelse for andre virkemidler enn de økonomiske. Blant de administrative virkemidlene er det juridiske virkemidler som har størst praktisk betydning. Juridiske virkemidler består som regel av forbud eller påbud i ulike kombinasjoner. En vanlig brukt betegnelse på offentlige forbud og påbud er direkte regulering. Også erstatningsreglene og avtaleinngåelser kan regnes som juridiske virkemidler. Andre kategorier av administrative virkemidler er informasjon og fysiske virkemidler (tilrettelegging av sikkerhetsgodkjente IKT-systemer, fysiske barrierer etc.). Mens direkte reguleringer virker ved å forplikte aktørene til å handle på bestemte måter, virker økonomiske virkemidler gjennom å påvirke aktørenes vurdering av hva det er økonomisk fordelaktig å foreta seg. Økonomiske virkemidler omfatter særlig hovedgruppene avgifter, omsettelige kvoter, pantesystemer og ulike former for tilskudd og subsidier.[108]

Grensen mellom ulike virkemiddelkategorier er ikke skarp. Blant annet vil juridiske virkemidler ofte utgjøre et nødvendig grunnlag for annen virkemiddelbruk. Økonomiske virkemidler må ha et juridisk fundament, for eksempel i form av påbud om å fremskaffe dokumentasjon i tilknytning til avgiftsberegningen, og påbud om å innbetale avgiften. Omvendt vil juridiske virkemidler kunne ha en bestanddel av økonomisk karakter, som bot, inndragning, forurensningsgebyr eller erstatning.[109]

Organisatoriske virkemidler er viktige i staten. Regjeringen og departementene har en generell myndighet til å instruere alle virksomheter som er organisert innenfor staten (statlige forvaltningsorganer). Dette betegnes som etatsstyring.

Når en virksomhet er organisert som selvstendig rettssubjekt, kan ikke departementene benytte instruksjonsmyndighet, men må i stedet

[108] NOU 1995: 4.
[109] Ibid.



Figur 4.12 Eksempler på ulike virkemidler og styringstiltak som staten kan benytte for å styre samfunnsutviklingen.

Kilde: Direktoratet for økonomistyring, *veileder i samfunnsøkonomiske analyser,* 2014.

styre gjennom andre virkemidler. Juridiske virkemidler er de viktigste. Men også eierstyring kan være et aktuelt virkemiddel for heleide statlige foretak, med de begrensninger i mulighetene for styring som følger av denne organisasjonsformen.

Informative virkemidler omfatter alt som har å gjøre med informasjon og formidling av kunnskap. Det kan være målrettede informasjonskampanjer, bruk av konferanser og folkemøter, eller det kan være mer løpende informasjonsarbeid. Slike virkemidler har en sentral rolle i sikkerhetsarbeid. Utfordringene ligger både i å innhente ny kunnskap om sikring, sårbarheter og trusler, men også å sikre at den kunnskap som finnes, faktisk blir benyttet. NSM og FFI peker på at manglende sikkerhetskultur er den viktigste årsaken til at sikkerhetsnivået i mange situasjoner er for lavt.

Innretningen av virkemidler må styres av i hvilken grad det er behov for å nå et absoluttnivå for sikkerhet eller om det er behov for å fleksibelt kunne styre adferd i en bestemt retning. Det vil også ha betydning i hvilken grad det er usikkerhet i risikovurderingene (se kapittel 4.4.4) og i forståelsen av sammenhengen mellom virkemidler og påvirkning av adferd.

Videre må det legges vekt på om det er hensiktsmessig å ha betydelig grad av fleksibilitet i virkemidlene for å oppnå et dynamisk sikkerhetsnivå som kan justeres i forhold til endringer i trusselbildet og den generelle samfunnsutviklingen, eller om det er viktig at sikkerhetsnivået ligger fast over tid.

Kapittel 5
Forebyggende sikkerhet og rettssikkerhetsgarantier

5.1 Innledning

Vernet av demokratiet, rettsstaten og menneskerettighetene står sentralt i samfunnskontrakten mellom staten og borgerne. Dette vernet følger direkte av Grunnloven § 2 og er videre konkretisert i kapittel E Menneskerettigheter (§§ 92-113). Herunder skal statens myndigheter respektere og sikre menneskerettighetene slik de kommer til uttrykk i bindende traktater om menneskerettigheter, jf. § 92 og menneskerettsloven § 2, som blant annet viser til Den europeiske menneskerettighetskonvensjonen (EMK) og FNs konvensjon om sivile og politiske rettigheter (SP).

Arbeidet med forebyggende sikkerhet er nettopp motivert ut i fra ønsket om å beskytte et styresett og et samfunn som virkeliggjør bestemmelsene i Grunnloven, ikke minst de som gjelder menneskerettigheter. Menneskerettighetene er imidlertid ikke absolutte størrelser, og hver rettighet kan ikke alltid realiseres i sin ideelle form. For eksempel ville et fullstendig vern av ytringsfriheten gått på bekostning av personvernet, fordi man også måtte tillatt hatefulle og diskriminerende ytringer.

Skal staten gjøre inngrep i grunnleggende rettigheter, som for eksempel personvern og rettssikkerhet, må det begrunnes som legitimt og forholdsmessig for å beskytte andre grunnleggende rettigheter og hensyn. Slike formål kan være andre menneskerettigheter, men også hensynet til nasjonal sikkerhet, jf. EMK art. 8(2). I spenningsfeltet mellom ivaretakelse av nasjonal sikkerhet og personvernet, befinner det seg til dels motstridende interesser og verdier som må veies opp mot hverandre.

Inngripende tiltak overfor borgerne, i form av overvåkning eller andre former for kontroll, kan medføre nedkjølingseffekt i samfunnet. I henhold til stortingsmelding nr. 23 (2013–2014) Datatilsynets og Personvernnemndas årsmeldinger for 2013, oppstår nedkjølingseffekten i situasjoner hvor utøvelse av legitime handlinger innskrenkes eller motvirkes gjennom trusselen om mulige sanksjoner.

En balansert avveining mellom nasjonal sikkerhet, menneskerettighetene og andre grunnleggende interesser har stått sentralt for utvalgets arbeid. Utvalget har hatt som utgangspunkt at en i den grad det er mulig, bør velge tiltak som ikke, eller i minst mulig grad, kommer i konflikt med individuelle rettigheter og friheter. For inngrep som likevel må anses påkrevd av hensynet til nasjonal sikkerhet, har utvalget lagt vekt på at tiltakene skal kunne skaleres slik at disse ikke medfører inngrep i større grad, eller for lengre tid, enn hva som anses nødvendig i det konkrete tilfellet. I tillegg skal det i slike tilfeller etableres tilfredsstillende rettssikkerhets- og personverngarantier for den som blir eksponert for tiltak etter loven. En privat virksomhet, eller andre selvstendige rettssubjekter, som blir pålagt inngripende og kostbare tiltak for å sikre samfunnskritiske funksjoner, skal således ha tilgang til rettssikkerhetsgarantier for å sikre legalitet, kontradiksjon, likebehandling med videre. Tilsvarende bør for eksempel personer som gjennomgår personkontrollundersøkelser i forbindelse med en søknad om sikkerhetsklarering i rimelig grad sikres innsyn i prosessen og selvbestemmelse.

I arbeidet med å balansere hensynet til forebyggende sikkerhet og andre grunnleggende hensyn og rettigheter er *rettssikkerhet* og *personvern* sentrale begreper.

I den videre fremstillingen vil det innledningsvis gis en redegjørelse for utvalgets forståelse av begrepene rettssikkerhet og personvern, og forholdet mellom disse. Deretter vil det nærmere innholdet i de to begrepene bli behandlet, før utvalget avslutningsvis trekker opp noen generelle retningslinjer for hvordan avveiningen mellom de ulike hensynene vil bli foretatt i utvalgets videre arbeid.

5.2 Begrepsavklaring

Rettssikkerhet er et flertydig begrep, det brukes på ulike måter og med noe forskjellig vektlegging avhengig av om det for eksempel er strafferett eller forvaltningsrett som er rammen for begrepsforklaringen. Kjernen i rettssikkerhet er kravet om at enkeltindividet skal være beskyttet mot vilkårlige og uforholdsmessige inngrep fra myndighetenes side. Den enkelte skal dessuten ha mulighet til å forutberegne sin rettsstilling og forsvare sine interesser. I tillegg kan hensynet til likhet og rettferdighet inngå i begrepet.[1] Rettssikkerhet er grunnleggende knyttet til begrepet *rettsstat*, og forutsetter at inngripende avgjørelser skal bygge på lovgivning som er kjent, og som blir anvendt på forutberegnelige og rettsriktige måter, det vil si i samsvar med gjeldende rettsregler. Rettssikkerhet forutsetter blant annet uavhengige domstoler, som gjennom sin virksomhet bekrefter og etablerer gjeldende rettsregler, og kontrollerer at inngrep overfor den enkelte skjer i samsvar med loven.

Virkemidlene for å oppnå rettssikkerhetskravene omtales gjerne som rettssikkerhetsgarantier. Rettssikkerhetsgarantiene er enkeltelementer som hver for seg – og samlet – bidrar til å ivareta rettssikkerhetskravene.

Personvern i tradisjonell forstand ble definert av Personvernkommisjonen på følgende måte:

> Personvern dreier seg om ivaretakelse av personlig integritet; ivaretakelse av enkeltindividers mulighet for privatliv, selvbestemmelse (autonomi) og selvutfoldelse.[2]

Alle mennesker har behov for en privat sfære, hvor man kan være i fred fra innblanding fra andre. Personvernet innebærer imidlertid ikke bare en rett til å ha en slik privat sfære, men også retten til å ha kontroll over opplysninger om seg selv. Beskyttelsen av personopplysninger betegnes ofte *personopplysningsvern*.

Personvernkommisjonen har i sin utredning lagt følgende definisjon av *personopplysningsvern* til grunn:

> 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.[3]

Retten til en personlig sfære, uten innblanding eller overvåkning fra myndighetenes side, kan sies å være en av bærebjelkene i et reelt demokrati. Metodekontrollutvalget understreket at «[u]ten et privat rom der individet fritt kan drøfte, utdype og teste sine tanker og oppfatninger, vil det ikke ha grunnlag for å utøve sin rolle som deltaker i de demokratiske prosessene».[4]

Personvernkommisjonen omtalte personvernets betydning for demokratiet, som beskyttelsen av «rettigheter og friheter som igjen beskytter grunnleggende offentlige friheter, som friheten til å delta i demokratiske prosesser».[5] Når det gjelder utøvelse av offentlig myndighet, kan begrepene rettssikkerhet og personvern langt på vei sies å smelte sammen. I Personvernkommisjonens utredning er begrepene omtalt på følgende måte:

> Det tradisjonelle personvernet, forstått som respekt for og beskyttelse av integritet og individets ukrenkelighet, vil ofte gå hånd i hånd med kravet til rettssikkerhet. Det motsatte vil imidlertid ofte være tilfellet med personopplysningsvernet. Grunnleggende rettssikkerhetsgarantier som innsynsrett i forvaltningssaker og fri bevisbedømmelse vil ofte innebære behandling og spredning av personlig informasjon som den registrerte ikke kan ha kontroll over. For å sikre borgernes rettssikkerhet vil det derfor ofte være nødvendig å sette personopplysningsvernet helt eller delvis til side.[6]

Ved offentlig myndighetsutøvelse som innebærer inngrep overfor den enkelte, vil man ut fra rettssikkerhetsbetraktninger blant annet stille krav om at inngrepet er hjemlet i lov, forutsigbart, forholdsmessig og formålsbestemt. Videre stilles det krav til saksbehandlingen, herunder at den enkelte får anledning til kontradiksjon, at de berørte parter har rett til innsyn i saksdokumen-

---

1 Torstein Eckhoff og Eivind Smith, *Forvaltningsrett*, 10. utgave (Oslo: Universitetsforlaget, 2014), 56–57.

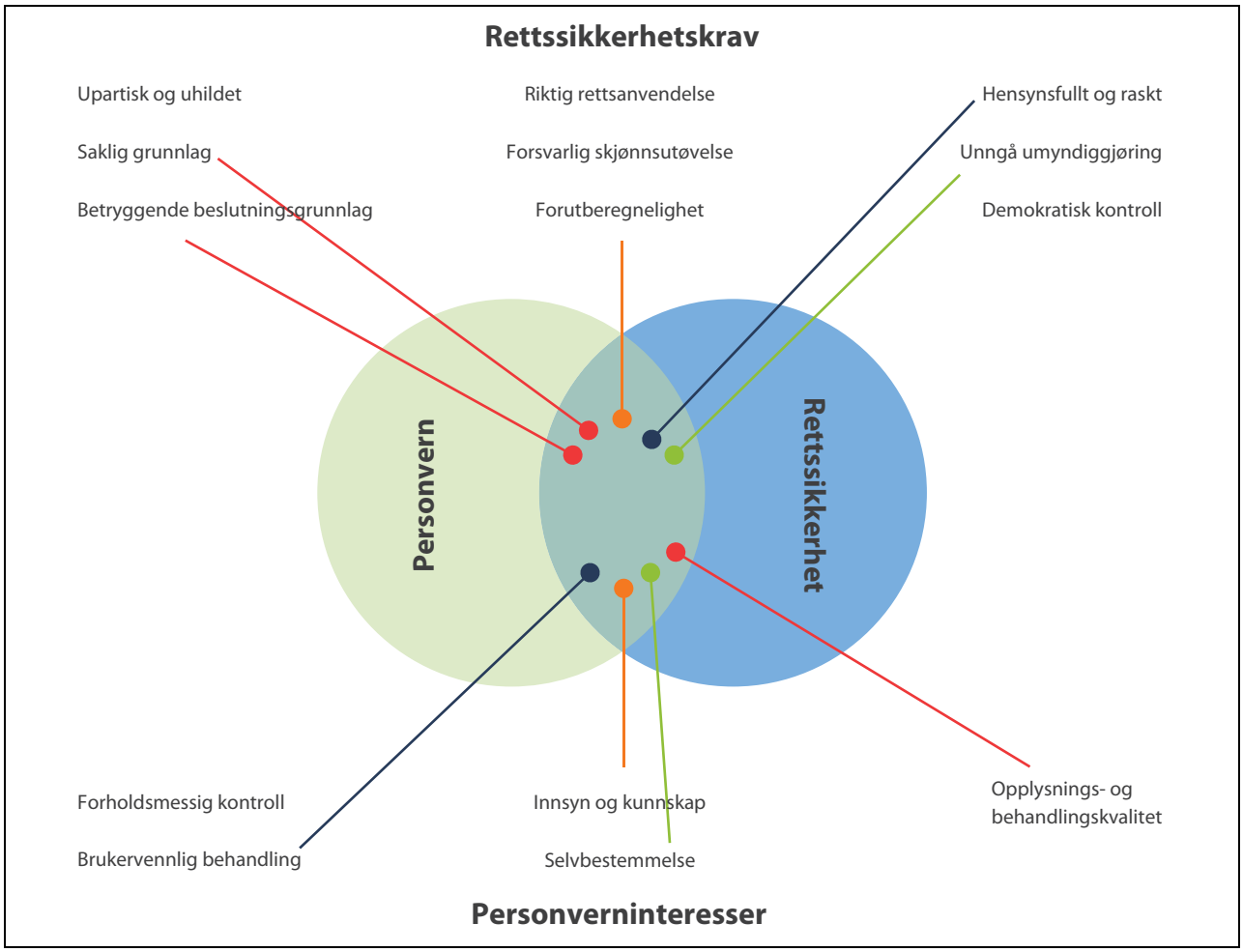
2 NOU 2009: 1, *Individ og integritet – Personvern i det digitale samfunnet*, 32.

3 Ibid.

4 NOU 2009: 15, *Skjult informasjon – åpen kontroll — Metodekontrollutvalgets evaluering av lovgivningen om politiets bruk av skjulte tvangsmidler og behandling av informasjon i straffesaker*, 50

5 NOU 2009: 1, 39.

6 NOU 2009: 1, 33.



Figur 5.1 Forholdet mellom rettssikkerhet og personvern.

Illustrasjon: Dag W. Schartum, professor, Universitet i Oslo, det juridisk fakultet.

tene, at de blir underrettet om utfallet av avgjørelsen, og at det gis anledning til å påklage vedtaket.

Ut fra en personvernbetraktning vil en typisk sørge for at det ikke blir behandlet flere opplysninger enn nødvendig ut i fra formålet, at opplysningene som brukes er korrekte og oppdaterte, at de aktuelle personene har kunnskap om behandlingen, innsyn i egne opplysninger med videre.

De enkelte komponentene i henholdsvis rettssikkerhets- og personvernidealene kan beskrives i form av *krav* og *interesser*. En sammenstilling av slike beskrivelser anskueliggjør slektskapet mellom de to tilnærmingene, se figur 5.1.

Figuren illustrerer at de to idealene grunnleggende sett bør ses som separate, men med overlappende tilnærminger. Samtidig gjelder de likeartede spørsmål. Lik farge på strekene, markerer likeartet innhold. Mens rettssikkerhet primært gjelder myndighetsutøvelse generelt, gjelder personopplysningsvern uavhengig av om det utøves myndighet eller ikke. Det betyr blant annet at personopplysningsvern alltid er relevant når det samles inn opplysninger om enkeltindivider, mens rettssikkerhet primært er relevant når disse opplysningene brukes til å utøve offentlig myndighet.

Både personvern og rettsikkerhet kan ivaretas på systemnivå og på individuelt nivå. For ivaretakelse av personvern er det i lovgivningen særlig lagt vekt på å stille krav til informasjonssystemer som behandler personopplysningene. Således skal den generelle behandlingen av personopplysninger i systemene ha rettslig grunnlag (for eksempel lovhjemmel); skje i henhold til på forhånd fastlagte formål; ikke behandle flere opplysninger enn nødvendig for formålet; og sikre tilstrekkelig opplysningskvalitet og informasjonssikkerhet med videre. På systemnivå ivaretas rettssikkerhet særlig gjennom prosesslovgivning som fastsetter hvordan saker ved domstolene og forvaltningsmyndigheter skal behandles. På individuelt nivå begrunner både rettssikkerhet og personvern individuelle rettigheter, for eksempel ret-

ten til innsyn, kontradiksjon, begrunnelse, klage med videre.

5.3 Internasjonale forpliktelser og grunnlovsvern

5.3.1 Personvern og rettssikkerhet

Norge har gjennom flere internasjonale konvensjoner forpliktet seg til å verne om både personvern og rettssikkerhet.

EMK art. 5 om vern mot vilkårlig frihetsberøvelse, art. 6 om retten til rettferdig rettergang og art. 7 om legalitetsprinsippet og forbudet mot tilbakevirkning i strafferetten er grunnleggende bestemmelser i en rettssikkerhetssammenheng. EMK art. 5 og art. 7 har imidlertid primært betydning i en strafferettslig kontekst. I uttrykket rettferdig rettergang, jf. EMK art. 6, ligger flere viktige rettssikkerhetsprinsipper, herunder tilgang til en uavhengig og upartisk domstol, kontradiksjon, likestilling mellom partene, tilstedeværelse og begrunnelse, samt et forbud mot selvinkriminering.

EMK art. 8 og SP art. 17 omhandler statens forpliktelser til å verne den enkeltes krav på respekt for sitt privatliv, familieliv, sitt hjem og sin korrespondanse. Begge bestemmelsene inneholder både rettssikkerhets- og personvernelementer.

EMK art. 8 lyder:

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

SP. art. 17 lyder:

1. Ingen må utsettes for vilkårlige eller ulovlige inngrep i privat- eller familieliv, hjem eller korrespondanse, eller ulovlige inngrep på ære eller omdømme.
2. Enhver har rett til lovens beskyttelse mot slike inngrep eller angrep.

Selv om ordlyden i de to bestemmelsene er ulike, viser praksis fra den Europeiske menneskerettighetsdomstolen (EMD) og FNs menneskerettighetskomite at de nærmere vurderingstemaene etter bestemmelsene er sammenfallende.

Disse bestemmelsene er sentrale for Norges folkerettslige forpliktelser til å ivareta den enkeltes rettssikkerhet og personvern.

Retten til vern om privatliv og korrespondanse etter art. 8 og 17 er ikke absolutt. Inngrep i de beskyttede interessene kan imidlertid kun skje dersom tre kumulative vilkår er oppfylt:

- Inngrepet må være foreskrevet ved lov (lovskravet)
- Inngrepet må ivareta beskyttelsesverdige formål
- Inngrepet må være nødvendig i et demokratisk samfunn (nødvendighetskravet)

Lovskravet innebærer at et inngrep i de beskyttede interessene må ha hjemmel i nasjonal lovgivning. Av rettspraksis fra EMD fremgår det at denne hjemmelen må oppfylle visse kvalitative krav. Loven må være tilgjengelig for de berørte, sikre forutberegnelighet med hensyn til konsekvensene av lovgivningen, samt være i overensstemmelse med rettsstatsprinsippene.[7]

De *beskyttelsesverdige formål* som kan begrunne inngrep i den enkeltes privatliv eller korrespondanse, reiser sjelden tvil i EMD-praksis. Dette skyldes i hovedsak at de oppregnede formålene er så bredt formulert at de dekker de fleste tilfeller hvor statene har behov for å foreta inngrep i beskyttede rettigheter.[8] Imidlertid er relativt presise formålsangivelser en forutsetning for et reelt vern.

I et nytt lovgrunnlag for forebyggende nasjonal sikkerhet, vil hensynet til den nasjonale sikkerhet være en gjennomgående begrunnelse for de tiltak som foreslås implementert. Dette formålet favner imidlertid så vidt at det, slik utvalget ser det, i flere sammenhenger er nødvendig med nærmere konkretiseringer.

Nødvendighetskravet innebærer både at inngrepet må være *forholdsmessig*, og at det må være *formålsmessig*. Med formålsmessig menes i denne sammenheng at de tiltak som tillates, må være egnet til å oppnå det aktuelle formålet.

For at inngrepet skal anses nødvendig i et demokratisk samfunn må det videre være forholdsmessig i forhold til de legitime formål som

[7] Weber and Saravia vs. Germany (54934/00), avsnitt 84.
[8] NOU 2009: 15, 63.

forfølges. Forholdsmessighetsvurderingen er en konkret skjønnsmessig vurdering hvor en rekke faktorer tas i betraktning. EMD har lagt til grunn at statene har en relativt vid skjønnsmargin i interesseavveiningen mellom retten til vern av privatliv og hensynet til nasjonal sikkerhet.[9]

Retten har samtidig understreket den iboende risikoen for at inngripende tiltak av hensyn til nasjonal sikkerhet kan undergrave, eller i verste fall ødelegge demokratiet, under et dekke av å skulle beskytte nettopp dette. Det må derfor være etablert adekvate og effektive mekanismer som forhindrer misbruk av slike tiltak. Hvorvidt tiltakene vil være forholdsmessige avhenger av en konkret vurdering av omstendighetene i saken.

Vernet av den enkeltes personlige integritet og autonomi er i Norge en grunnlovsfestet rettighet. Det følger av Grunnloven § 102, som ble endret i 2014, at:

> 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.

I motsetning til EMK art. 8 og SP art. 17 åpner ikke ordlyden i Grunnloven § 102 for å gjøre unntak fra dette vernet. Det fremgår imidlertid av forarbeidene at bestemmelsen er en grunnlovfesting av det vern som følger av tidligere Grunnloven § 102, ulovfestet rett, menneskerettsloven og annen ordinær lovgivning.[10] Det er også slått fast i rettspraksis at det kan gjøres inngrep i de rettsgoder som bestemmelsen verner:

> Til forskjell fra SP artikkel 17 og EMK artikkel 8, inneholder Grunnloven § 102 ingen anvisning på om det overhodet kan gjøres lovlige begrensninger i privat- og familielivet. Men grunnlovsvernet kan ikke være – og er heller ikke – absolutt. I tråd med de folkerettslige bestemmelsene som var mønster for denne delen av § 102, vil det være tillatt å gripe inn i rettighetene etter første ledd første punktum dersom tiltaket har tilstrekkelig hjemmel, forfølger et legitimt formål og er forholdsmessig, jf. Rt-2014-1105 avsnitt 28. Forholdsmessighetsvurderingen må ha for øye balansen mellom de beskyttede individuelle interessene på den ene siden og de legitime samfunnsbehovene som begrunner tiltaket på den andre.[11]

5.3.2 Personopplysningsvernet

SP art. 17 og EMK art. 8 er som nevnt sentrale bestemmelser for beskyttelsen av rettssikkerhet og personvern. De samme bestemmelsene danner også fundamentet for personopplysningsvernet. FNs menneskerettighetskomité uttalte i 1988 at for å ivareta de forpliktelser SP art. 17 oppstiller må statene blant annet utarbeide regelverk som verner personopplysninger.

Det kommer ikke direkte til uttrykk at personopplysninger er vernet gjennom bestemmelsen i Grunnloven § 102. Ser vi imidlertid på uttalelser fra Stortingets kontroll- og konstitusjonskomité, Høyesterett og EMD er det klart at bestemmelsen også verner personopplysninger ved at systematisk innhenting, oppbevaring, lagring eller bruk av opplysninger om andres personlige forhold bare kan finne sted i henhold til lov, benyttes i henhold til lov eller informert samtykke, at loven må være forholdsmessig og ivareta et legitimt formål og at opplysningene må slettes når formålet ikke lenger er til stede.

Under henvisning til blant annet EMK art. 8 vedtok Europaparlamentet og Rådet 24. oktober 1995 Direktiv om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (Personverndirektivet), som ble førende også for utforming av norsk regelverk. Ved innlemmelsen av Personverndirektivet av 25. juni 1999 i EØS-avtalen, ble reglene også folkerettslig bindende for Norge. Direktivet pålegger medlemsstater innen EU/EØS å vedta lovgivning i samsvar med direktivets regler. Den norske personopplysningsloven søker nettopp å oppfylle dette kravet, se kapittel 5.5.

EU vedtok 27. april 2016 en personvernreform bestående av en forordning om beskyttelse av personopplysninger generelt og et direktiv for myndighetenes behandling av personopplysninger i politi- og straffesektoren. Begge regelverkene skal implementeres i norsk rett. Ikrafttredelse er satt til mai 2018 for EU. Dette vil gjelde også for Norge med mindre noe annet bestemmes ved innlemmelse av forordningen i EØS-avtalen.

I grove trekk videreføres gjeldende rett i personverndirektivet og personopplysningsloven. Vedtakelse av et nytt generelt regelverk i form av en EU-forordning skal føre til en større grad av

---

9 Blant annet i Weber and Saravia vs. Germany, avsnitt 105.

10 Dok. Nr. 16 (2011–2012), *Rapport fra Menneskerettighetsutvalget om menneskerettighetene i Grunnloven*, 178.

11 RT-2015-93, avsnitt 60.

harmonisering av personvernreglene i EØS-området. Et utvidet samarbeid mellom nasjonale tilsynsmyndigheter skal ytterligere bidra til en lik rettsutvikling.

Blant endringene kan nevnes for det første virkeområdet for regelverket. Fra å gjelde virksomheter som er etablert innenfor EØS-området, skal reglene nå også gjelde alle som behandler EØS-borgeres personopplysninger når behandlingen består i å tilby varer eller tjenester til disse borgerne eller å overvåke deres atferd innenfor EØS-området.

Innen strafferettspleien tar de nye reglene sikte på å bedre beskyttelsen av personopplysningene til både siktede, fornærmede og vitner. Informasjonsutveksling mellom nasjonale myndigheter skal også utvides.

Videre erstattes den nåværende meldeplikten for behandling av personopplysninger med en del andre plikter for den behandlingsansvarlige og databehandlere. Dette gjelder blant annet plikt til å føre dokumentasjon, til å varsle tilsynsmyndigheten og/eller den registrerte ved eventuelle databrudd. Gjennom en risikobasert tilnærming til behandlingen av personopplysninger skal hensiktsmessige tekniske og organisatoriske sikkerhetstiltak iverksettes.

Den registrertes rettigheter til blant annet innsyn, informasjon, sletting og medbestemmelse utvides. Videre innføres regler om dataportabilitet og personprofiler, og en sertifiseringsordning som skal synliggjøre hvilke virksomheter som tar personvern på alvor. Av spesiell interesse er også art. 25 som blant annet stiller krav til *innebygget personvern*, det vil si til å nedfelle hensynet til personvern i de informasjonssystemer som behandler personopplysninger.

Forordningen viderefører i grove trekk det virkeområdet som gjaldt for direktivet av 1995. Det fremgår av forordningen art. 2 at den ikke får anvendelse på behandling av personopplysninger som utføres i anledning forhold som faller utenfor EU-regelverkets virkeområde, for eksempel nasjonal sikkerhet og forsvar.

For de virksomheter forordningen gjelder for, åpner art. 23 – i likhet med direktivet art. 13 – for unntak fra reglene om den registrertes rettigheter blant annet av hensyn til nasjonal sikkerhet, forsvar og samfunnssikkerhet (*public security*), dersom unntaket gjøres i lovs form og det er nødvendig og proporsjonalt i et demokratisk samfunn.

Da direktivet gjennom personopplysningsloven ble innlemmet i norsk rett ble det besluttet å gi den norske personopplysningsloven et bredere virkeområde enn det Norge var forpliktet til. Til forskjell fra EU-retten gjelder dermed personopplysningsloven som utgangspunkt også for eksempelvis virksomhet innen nasjonal sikkerhet og forsvar. Så lenge personopplysningsloven gjelder, må eventuelle unntak gjøres ved lov. Det gjenstår å se om denne løsningen blir videreført når den nye forordningen skal innlemmes i norsk rett. Utvalget er imidlertid ikke kjent med at det er planlagt endringer her.

5.4 Rettssikkerhet

I det norske lovverket finnes det en rekke lover og enkeltbestemmelser som har som hovedformål å ivareta rettssikkerheten. Prosesslovgivningen, herunder straffeprosessloven og forvaltningsloven, er sentrale eksempler. Dagens sikkerhetslov, har ivaretakelse av den enkeltes rettssikkerhet som et uttalt formål, se § 1 bokstav b. Av loven § 6 annet ledd fremgår det således at det ved utøvelse av forebyggende sikkerhetstjeneste, skal tas særlig hensyn til den enkeltes rettssikkerhet. Forvaltningsloven[12] har en rekke bestemmelser som skal bidra til at forvaltningsorganer behandler saker på en rettssikker måte. For myndighetsutøvelse som berører enkeltpersoner eller selvstendige rettssubjekter, vil forvaltningsloven danne utgangspunkt for myndighetenes saksbehandling med mindre det gjøres eksplisitt unntak fra reglene i loven.

Tradisjonelt deles rettssikkerhetskravene inn i to grupper; materiell rettssikkerhet om overordnede krav til avgjørelsens innhold (kapittel 5.4.1), og prosessuell rettssikkerhet om fremgangsmåten for hvordan slike avgjørelser skal treffes (kapittel 5.4.2).[13]

5.4.1 Materielle rettssikkerhetsgarantier

Legalitetsprinsippet er et sentralt element i det materielle rettssikkerhetsbegrepet, og gjenspeiler også lovskravet som følger av Norges folkerettslige forpliktelser etter EMK og SP.

Det strafferettslige legalitetskravet følger av Grunnloven § 96. På strafferettens og straffeprosessens område gjelder det et strengt krav til lovhjemlenes klarhet og presisjon. Utenfor strafferettens område var legalitetsprinsippet lenge ansett for å være konstitusjonell sedvanerett, basert på den ulovfestede læren om at inngrep i borgernes

[12] Lov 10. februar 1967 om behandlingsmåten i forvaltningssaker (forvaltningsloven).

[13] NOU 2009: 15, 60.

rettssfære trenger hjemmel i lov. Ved Grunnlovsendringen i 2014 ble dette prinsippet, utenfor strafferettens område, lovfestet i Grunnloven § 113. Bestemmelsen lyder:

> Myndighetenes inngrep overfor den enkelte må ha grunnlag i lov.

Legalitetsprinsippet har en sentral plass i forståelsen av den norske rettsstaten. Myndighetenes inngrep overfor den enkelte skal være basert på en demokratisk prosess og være forankret i folkeflertallets vilje. På mange måter utgjør lovfestingen av det generelle legalitetsprinsippet en garanti for ivaretakelsen av de verdier Grunnloven skal verne om – rettstaten, demokratiet og menneskerettighetene, jf. Grunnloven § 2.

Et sentralt element i legalitetsprinsippet er hensynet til *forutberegnelighet*. At inngrep i borgernes private rettssfære følger direkte av lovgivningen, gjør at den enkelte settes i stand til å forutberegne sin rettsstilling. En viktig forutsetning for å kunne forutberegne sin rettsstilling er at inngrepshjemlene er tilgjengelige for allmennheten, slik at borgerne har mulighet til å sette seg inn i det aktuelle regelverket. En forutsetning for forutberegnelighet er at inngrepshjemlene er tilstrekkelig presise og at reglene ikke i for stor grad er av skjønnsmessig karakter. I dette ligger en spesifisering av hvilke vilkår som må være oppfylt for at et vedtak skal kunne treffes, og hvilket innhold vedtaket kan eller skal ha. En slik forutberegnelighet vil også skape gode muligheter for overprøving og kontroll av forvaltningen av regelverket.

En annen grunnleggende rettssikkerhetsgaranti er *forholdsmessighetsprinsippet*. I dette ligger både at det må gjøres en konkret vurdering av hvorvidt det aktuelle tiltaket vil utgjøre et uforholdsmessig inngrep i den enkeltes rettssfære sett opp mot de sikkerhetsmessige gevinstene et slikt tiltak vil antas å få, og en vurdering av hvilken effekt det aktuelle tiltaket antas å få sett opp mot den aktuelle risiko det søker å beskytte mot.

Innen forebyggende sikkerhetstjeneste kommer forholdsmessighetsprinsippet til uttrykk i sikkerhetsloven § 6, hvor det fremgår at det ikke skal nyttes mer inngripende midler og metoder enn det som fremstår som nødvendig i forhold til den aktuelle sikkerhetsrisiko og omstendighetene for øvrig. Dette kan også ses på som et subsidiaritetsprinspipp. Dersom samme effekt kan oppnås ved bruk av at mindre inngripende virkemiddel, skal det minst inngripende virkemidlet benyttes. I forarbeidene til dagens sikkerhetslov fremgår det imidlertid at valg av virkemiddel avhenger av en helhetsvurdering, der også andre forhold enn forholdsmessighetsprinsippet vil spille inn:

> Utgangspunktet i den enkelte situasjon vil være valg av det minst inngripende middel, men det vil likevel kunne være behov for å anvende midler som går utover den umiddelbare måloppnåelse dersom sikkerhetsrisikoen er meget alvorlig. Forståelsen av bestemmelsen må derfor bygge på en helhetsvurdering, hvor en også tar hensyn til troverdigheten av norske myndigheters hevdelse av suverenitet og suverene rettigheter og ivaretakelse av rikets sikkerhet eller andre vitale nasjonale sikkerhetsinteresser.[14]

5.4.2 Prosessuelle rettssikkerhetsgarantier

Med prosessuelle rettsikkerhetsgarantier menes de saksbehandlingsreglene som må følges ved en avgjørelse som medfører inngrep overfor den enkelte. De generelle reglene for forvaltningens saksbehandling følger av forvaltningslovens bestemmelser, jf. kapittel II og III. For vedtak som gjelder rettigheter eller plikter til en eller flere bestemte personer, såkalte enkeltvedtak, er det særlige regler for forvaltningens saksbehandling i forvaltningsloven kapittel IV-VI.

En sentral rettssikkerhetsgaranti er retten til *kontradiksjon*. Som nevnt over kan retten til kontradiksjon også utledes av EMK art. 6. Gjennom kontradiksjon vil den enkelte, enten det er enkeltpersoner eller private virksomheter, gis muligheten til å forsvare sine interesser ved kunne å fremlegge sitt syn på saken, og ved å kunne korrigere og supplere faktiske forhold som kan være av betydning for den avgjørelse som skal treffes. Kontradiksjon er i mange tilfeller avgjørende for å sikre at myndighetene fatter en materielt sett riktig avgjørelse. Også i forhold til borgernes tillit til myndighetene vil det være av stor betydning at den avgjørelsen retter seg mot opplever å få en rettferdig behandling. Det motsatte vil lett kunne bli tilfelle, dersom man ikke får anledning til å imøtegå det faktiske og rettslige grunnlaget som legges til grunn for avgjørelsen.[15]

Retten til kontradiksjon ved klareringssaker er i dagens sikkerhetslov søkt ivaretatt ved at sikkerhetssamtale skal gjennomføres der dette ikke anses som åpenbart unødvendig, jf. sikkerhetslo-

---

14 Ot.prp. nr. 49 (1996–97), kapittel 11.

15 Magnus Matningsdal, «Kontradiksjon i sivile saker og straffesaker», *Jussens Venner* (2013), 1-115.

ven § 21 tredje ledd. I tillegg vil den enkelte gjennom utfylling av en personopplysningsblankett ha mulighet til å gi all informasjon som den enkelte mener er relevant for saken.

For at den enkelte skal kunne gjøre bruk av sin rett til kontradiksjon, er det imidlertid en forutsetning at vedkommende har kjennskap til at myndighetene har til hensikt å fatte en avgjørelse som vil kunne utgjøre et inngrep overfor vedkommende. Dette stiller krav til *åpenhet* fra myndighetenes side. I forvaltningsloven ivaretas dette etter bestemmelsene om forhåndsvarsel etter forvaltningsloven § 16 og partsoffentlighet etter § 17 annet og tredje ledd og § 18 flg. Etter dagens sikkerhetslov er det innen personellsikkerhet gjort enkelte unntak fra forvaltningsloven kapittel IV om saksforberedelse ved enkeltvedtak og kapittel V om vedtaket. For å ivareta den enkeltes rettssikkerhet er det i stedet fastsatt egne bestemmelser om blant annet begrunnelse og underretning (§ 25) og innsyn i saksdokumentene (§ 25a).

En annen sentral rettssikkerhetsgaranti etter norsk rett er at forvaltningen som utgangspunkt plikter å gi en *samtidig begrunnelse* for det vedtak som fattes, se forvaltningsloven § 24 følgende. Plikten til å gi samtidig begrunnelse har nær sammenheng med retten til å *klage* på myndighetens avgjørelse, jf. forvaltningsloven kapittel VI. Retten til samtidig begrunnelse i sikkerhetsklareringssaker følger av sikkerhetsloven § 25 tredje ledd. Som utgangspunkt skal det også her gis en samtidig begrunnelse. Det er imidlertid gjort unntak fra denne retten i tilfeller der begrunnelse ikke kan gis uten å røpe nærmere angitte opplysninger, herunder opplysninger av betydning for rikets sikkerhet. Forvaltningslovens bestemmelser om klage, gjelder som utgangspunkt også i sikkerhetsklareringssaker, jf. sikkerhetsloven § 25c. Innen objektsikkerhet har selvstendige rettssubjekter klagerett på de vedtak som treffes etter objektsikkerhetsforskriften, jf. § 4-4.

5.5 Personvern

Personvern er et vidt begrep hvis innhold kan beskrives på forskjellige måter avhengig av ståsted og tilnærming. Interesseteorien, personvernprinsippene, integritetsperspektivet, maktperspektivet og beslutningsperspektivet gir med sine ulike tilnærminger på ulikt vis innhold til personvernet. Som det vil fremgå har beskyttelsen av personopplysninger en sentral rolle i personvernet.

Personvernprinsippene springer ut fra et ideal om at alle skal ha bestemmelsesrett over personopplysninger om dem selv. Forebyggende sikkerhetstiltak vil i varierende grad kunne innebære behandling av personopplysninger, for både offentlige og private virksomheter som er underlagt loven. For utvalgets arbeid vil personvernprinsippene derfor stå sentralt.

Personvernprinsippene har sitt utgangspunkt i en europarådskonvensjon, retningslinjer fra OECD og EU sitt personverndirektiv. Disse er allment benyttet og henvist til i norsk personvernlitteratur. Sammen danner prinsippene et fundament for ivaretakelsen av personvernet både i lovgivning og ved utformingen av tiltak som har betydning for personvernet. Det følgende utvalget av prinsipper tar utgangspunkt i EUs Personvernforordning[16] art. 5.

Behandlingen av personopplysninger må være *rettmessig, rettferdig og åpen*. Det må for det første foreligge et behandlingsgrunnlag, enten samtykke, lovhjemmel eller behandlingen må være nødvendig for å ivareta ett av de i loven fastsatte formål. Videre må selve behandlingen være rettferdig og åpen slik at den registrerte får informasjon om formålet med lagringen, prosessen og sine rettigheter. Prinsippet kommer til uttrykk i forordningen art. 5(a) og personopplysningsloven[17] § 8. I sikkerhetsklareringssaker vil eksempelvis ikke personkontroll bli igangsatt før vedkommende som er gjenstand for kontrollen har samtykket i dette gjennom å fylle ut, og underskrive en personopplysningsblankett. Det fremgår uttrykkelig av sikkerhetsloven § 20 at personkontroll ikke skal finne sted uten at den som sikkerhetsklareres er gjort oppmerksom på, og har samtykket i at slik kontroll vil bli foretatt.

Prinsippet om *formålsbestemthet* går ut på at personopplysninger kun skal samles inn for bestemte, legitime formål. Personopplysninger skal kun behandles i samsvar med det formålet de i utgangspunktet ble samlet inn for[18]. Prinsippet om formålsbestemthet er også sentralt innen sikkerhetsklarering av personell. Det følger av sikkerhetsloven § 20 sjette ledd at opplysninger som er gitt klareringsmyndigheten i forbindelse med personkontroll, ikke skal benyttes til andre formål enn vurdering av sikkerhetsklarering.

---

[16] Europaparlamentets- og rådsforordning (EU) 2016/679 av 27. april 2016 (EUs personvernforordning).

[17] Lov 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven).

[18] Se Personvernforordningen art. 5(b) og personopplysningsloven § 11.

Relevans- og minimumsprinsippet handler om at personopplysninger bare skal innhentes, lagres og behandles i den grad det er nødvendig for å oppnå et angitt formål. Det skal ikke registreres flere opplysninger enn strengt nødvendig, slik at overskuddsinformasjon unngås. Innsamlede data som ikke lenger er nødvendige for det angitte formålet må slettes eller anonymiseres. Prinsippet kommer til uttrykk i forordningen art. 5(c) og personopplysningsloven § 28. I personopplysningsforskriften kommer disse prinsippene til uttrykk i kapittel 6, som gir nærmere bestemmelser om blant annet bevaring og kassasjon/sletting av personopplysning som ikke lenger er nødvendig å lagre.

Bruk av personopplysninger til historiske, statistiske eller vitenskapelige formål settes i en særstilling, ved at det gjøres unntak fra minimumsprinsippet og til dels prinsippet om formålsbestemthet. Behovet for utvidet lagring skal imidlertid kontrolleres jevnlig.[19]

Gjennom *fullstendighets- og kvalitetsprinsippet* sikres at beslutninger ikke tas på ufullstendig eller feilaktig grunnlag. Personopplysningene må være relevante, oppdaterte, korrekte og fullstendige sett opp mot hva de skal brukes til.[20] Klareringsmyndigheten plikter å påse at saken er så godt opplyst som mulig før avgjørelse treffes, jf. sikkerhetsloven § 20 tredje ledd. Dersom det ikke er åpenbart unødvendig, plikter klareringsmyndigheten også å gjennomføre en sikkerhetssamtale med vedkommende som skal klareres. Gjennom en sikkerhetssamtale gis den som skal sikkerhetsklareres mulighet til å korrigere og supplere opplysninger om seg selv, slik at klareringsmyndighetens avgjørelsesgrunnlag er korrekt og fullstendig.

Ansvarlighetsprinsippet retter seg mot den behandlingsansvarlige, som har ansvar for at all behandling av personopplysninger skjer i samsvar med de krav som fremgår av gjeldende rettsregler.[21]

Beslutningsperspektivet[22] er ett av flere perspektiver som beskriver personvernet med en litt annen vinkling en de nevnte prinsippene. Beslutningsperspektivet tar utgangspunkt i at personopplysninger danner grunnlag for myndighetenes beslutning som har betydning for personen. Jo viktigere beslutning det er tale om for den enkelte, jo viktigere er det at beslutningsprosessen er forsvarlig. Det vil følgelig være mange likhetstrekk mellom beslutningsperspektivet og rettssikkerhet. Eksempelvis kan en beslutning om sikkerhetsklarering ha avgjørende betydning for en persons arbeidssituasjon. Følgelig bør det stilles strenge krav til klareringsprosessen. Beslutningsperspektivet bidrar til en passende dimensjonering av beskyttelsen.

5.6 Tilsyns- og kontrollordninger

En sentral mekanisme for ivaretakelse av rettssikkerhet og personvern er å ha *effektive kontrollsystemer*. Den etterfølgende kontrollen skal fungere skjerpende for de behandlingsansvarlige, tillitvekkende for samfunnet for øvrig, og i mange tilfeller som substitutt for de tiltak som i varierende grad griper inn i rettssikkerheten og personvernet.

I flere saker vedrørende inngrep av hensyn til nasjonal sikkerhet har den europeiske menneskerettighetsdomstolen (EMD) fokusert på at inngrepet skal ha en klar hjemmel i nasjonal lovgivning og hvorvidt det er etablert tilstrekkelige garantier mot misbruk. Etter en gjennomgang av flere saker om overvåkning oppsummerer Møse:

> Et helhetsinntrykk er at Domstolen ikke foretar noen streng materiell prøvning av hensynet til rikets sikkerhet, men stiller betydelige krav til den nasjonale hjemmelen og garantier mot misbruk.[23]

Som en del av nødvendighetsvurderingen, pekte EMD i saken *Klass mfl. V. Tyskland* (A 28 1978), på noen hovedmomenter om kontrollordningen. Møse skriver:

> Relevante momenter er arten, omfanget og varigheten av kontrolltiltakene, grunnlaget for dem, hvilke myndigheter som har kompetanse til å gi tillatelse, utføre og kontrollere slike inngrep, samt hvilke nasjonale prøvningsinstanser som finnes.[24]

---

[19] Se Personvernforordningen art. 5(e) og personopplysningsloven § 9(h).

[20] Se Personvernforordningen art. 5(d) og personopplysningsloven § 11.

[21] Se Personvernforordningen art. 5(f) og personopplysningsloven § 11.

[22] Dag Wiese Schartum og Lee Bygrave, *Personvern i informasjonssamfunnet, 2. utgave* (Oslo: Fagbokforlaget, 2011), 32.

[23] Erik Møse, *Menneskerettigheter, 1. utgave* (Oslo: Cappelen Akademisk forlag, 2002), 408.

[24] Ibid.

I den konkrete saken uttalte også EMD at judisiell prøvning var å foretrekke, men at også administrativ kontroll kan være tilstrekkelig.

For Norges del har både domstolene, Datatilsynet, Sivilombudsmannen og Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget) viktige roller for å ivareta den enkeltes rettssikkerhet og personvern. Domstolene fører for eksempel kontroll med politiets mest inngripende etterforskningsmetoder, jf. straffeprosessloven § 216 a om kommunikasjonsavlytting. Datatilsynet skal blant annet, i medhold av personopplysningsloven § 42 andre ledd nr. 3, kontrollere at lover og forskrifter som gjelder for behandling av personopplysninger blir fulgt, og at feil eller mangler blir rettet.

Behandling av personopplysninger som er nødvendig av hensyn til rikets sikkerhet, er i personopplysningsforskriften § 1-2 unntatt fra lovens bestemmelser om tilsynsmyndighetenes tilgang til opplysninger. Dette innebærer i praksis at Datatilsynet ikke har tilsynsmyndighet etter sikkerhetslovens bestemmelser om forebyggende sikkerhetstjeneste generelt, og sikkerhetsklarering av personell spesielt. Av samme grunn er det også gjort unntak fra reglene om melde- og konsesjonsplikt. EUs nye personvernforordning åpner også for å gjøre unntak av slike hensyn, se Personvernforordningen art. 23. I så fall må et kontrollorgan og dets myndighet spesifiseres.

Det fremgår av sikkerhetsloven § 30 at «[f]orebyggende sikkerhetstjeneste i medhold av loven her er underlagt kontroll og tilsyn av Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste», i samsvar med EOS-loven. I praksis innebærer dette at alle forvaltningsorganer, og selvstendige rettssubjekter underlagt loven, i prinsippet er gjenstand for kontroll og tilsyn av EOS-utvalget.

Hovedformålet med EOS-utvalgets kontroll er å ivareta den enkeltes rettssikkerhet[25]. Mer konkret fremgår det av EOS-loven § 2-1 at formålet er «å klarlegge om og forebygge at det øves urett mot noen, herunder påse at det ikke nyttes mer inngripende midler enn det som er nødvendig etter forholdene, og at tjenestene respekterer menneskerettighetene», jf. EOS-loven § 2 nr. 1).

EOS-utvalget skal føre regelmessig tilsyn med tjenestene, undersøke klager fra enkeltpersoner og organisasjoner og av eget tiltak ta opp forhold som utvalget finner formålstjenlig å undersøke. EOS-utvalget har, i motsetning til personvernmyndighetene, krav på innsyn i alt materiale som har betydning for kontrollene.

I Dok.16 (2015–2016), har Evalueringsutvalget blant annet foreslått at den stortingsoppnevnte kontrollen med EOS-tjenestene bør styrkes.[26]

EOS-utvalgets forankring i Stortinget er, etter Evalueringsutvalgets oppfatning, en styrke ved dagens kontrollmodell og bør således videreføres.[27] Forankringen i Stortinget gir EOS-utvalget den nødvendige uavhengigheten gjennom organisatorisk avstand til den uøvende makt, og bidrar også til at Stortinget gjøres oppmerksom på viktige problemstillinger og saker knyttet til EOS-tjenestenes virksomhet.

Evalueringsutvalget har også foreslått at EOS-utvalget ikke lenger bør føre kontroll med avgjørelser om sikkerhetsklarering.[28] EOS-utvalget står overfor store kapasitetsmessige utfordringer, og etter Evalueringsutvalgets syn, bør EOS-utvalget gis anledning til å konsentrere seg om de delene av EOS-tjenestenes virksomhet der kontrollbehovet er størst. Avgjørelser om sikkerhetsklarering skiller seg fra annen virksomhet EOS-tjenestene bedriver, ved at den avgjørelsen om klarering gjelder er kjent med og har godtatt, både at avgjørelse fattes og at personopplysninger innhentes i den forbindelse. I tillegg er det etablerte rettssikkerhetsgarantier for den enkelte, i form av rett til underretning og begrunnelse, samt klagerett på de avgjørelser som fattes. Evalueringsutvalget foreslår derfor at kontrollfunksjonen ivaretas av andre enn EOS-utvalget, for eksempel av Sivilombudsmannen. For en nærmere omtale av EOS-utvalget, vises det til kapittel 3.6.

5.7 Avveiningen mellom nasjonal sikkerhet og rettssikkerhet og personvern

Et komplekst og sammensatt risiko- og trusselbilde, kombinert med en rask teknologisk utvikling, skaper nye sårbarheter og utfordringer for samfunnet som helhet. Hensynet til å ivareta nasjonal sikkerhet nødvendiggjør en robust grunnsikring for våre mest sentrale samfunnsfunksjoner. Den teknologiske utviklingen representerer samtidig nye muligheter for å styrke den forebyggende sikkerheten.

[25] Ot.prp. nr. 83 (1993–94) Om lov om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste, 4.

[26] Dok. 16 (2015–2016).

[27] Ibid., 126.

[28] Ibid., 132 flg.

Personvern, rettssikkerhet og nasjonal sikkerhet er grunnleggende verdier i et demokratisk samfunn, hvor ingen av natur er mer tungtveiende enn andre. Ivaretakelse av alle disse verdiene er essensielt for å opprettholde demokratiet og rettsstatsprinsippene.

I tråd med statens forpliktelser etter Grunnloven og EMK må inngripende tiltak ha hjemmel i formell lov. Særlig inngripende tiltak tilsier at en legger et strengt legalitetsprinsipp til grunn, med en så klar og uttømmende regulering som mulig. Slik sikres forutberegnelighet og det skapes grunnlag for effektiv legalitetskontroll og domstolsprøving. Også hensynet til en åpen demokratisk diskurs om de motstående hensynene, tilsier at lovgiver går konkret inn på de mange dilemmaer en her står overfor.

Som et generelt utgangspunkt vil utvalget legge følgende prinsipper og retningslinjer til grunn ved vurderingen av sikkerhetsmessige tiltak som kan få en negativ innvirkning på den enkeltes rettssikkerhet og personvern:

- Presisjon i formulering av hjemmel for sikkerhetstiltaket (lovskravet)
- Vurdere hvilken effekt man får ved sikkerhetstiltaket, sett opp mot allerede eksisterende tiltak (formålsmessighet)
- Vurdere forholdsmessigheten mellom den sikkerhetsmessige effekten og hvor inngripende tiltakene er i forhold til personvern og rettssikkerhet (forholdsmessighet)
- Vurdere alternative, og mindre inngripende, tilnærminger til å oppnå samme effekt (subsidiaritetsprinsippet)
- Etablere tilstrekkelige personvern- eller rettssikkerhetsgarantier der det gjøres inngrep i den enkeltes rettssfære (prosessuelle mekanismer)

Denne fremgangsmåten vil slik utvalget ser det også ivareta de krav som stilles for unntak i Personvernforordningen art. 23, se kapittel 5.3.2.

Slik utvalget ser det vil personvernmessige konsekvenser i første rekke gjøre seg gjeldende innenfor regelverket for personellsikkerhet. Innen personellsikkerhet skjer det en utstrakt behandling av personopplysninger, med det siktemål å kontrollere den enkeltes sikkerhetsmessige skikkethet. I tillegg er det enkelte andre områder innen forebyggende sikkerhet, hvor sikkerhetsmessige hensyn gjør det nødvendig å behandle personopplysninger i en viss utstrekning, særlig sikkerhetstiltak innenfor informasjonssystemsikkerhet.

Når det gjelder inngrep overfor selvstendige rettssubjekter, som staten ikke har alminnelig instruksjons- og kontrollmyndighet over, vil det være sentralt at det etableres tilstrekkelige og tilfredsstillende rettssikkerhetsgarantier der det gjøres inngrep overfor slike rettssubjekter.

I den utstrekning utvalget foreslår inngrep i den enkeltes rettssikkerhet, eller foreslår tiltak som har betydning for selvstendige rettssubjekters rettssikkerhet, vil utvalget så godt det lar seg gjøre forsøke å begrunne det sikkerhetsmessige behovet for at slike inngrep gjøres, herunder om alternative og mindre inngripende tilnærminger kan gi tilstrekkelig sikkerhetsmessig effekt. Utvalgets vil videre forsøke å påse at hensynet til formålsmessighet og forholdsmessighet ivaretas ved utforming av regelverket, og at det etableres nødvendige garantier for å sikre at personvern og rettssikkerhet ivaretas på en tilfredsstillende måte.

Del III
Tematisk gjennomgang og utvalgets vurderinger

Kapittel 6
Lovens formål og virkeområde

6.1 Innledning

Hva angår lovens formål og virkeområde er utvalget gitt følgende mandat:

> Utvalget skal vurdere hva som bør reguleres i lov for å sikre nasjonal sikkerhet. Formålet med nytt lovgrunnlag skal være å beskytte kritisk infrastruktur, kritiske samfunnsfunksjoner og sensitiv informasjon mot tilsiktede, uønskede hendelser.

Det er en utfordring med dagens sikkerhetslov at den ikke har gjennomgått den dynamiske utviklingen lovgiver forutsatte da loven ble vedtatt. Forarbeidenes henvisning til begrepet *rikets sikkerhet* som en rettslig standard, hvis meningsinnhold var ment å forandre seg i takt med samfunnsutviklingen, har slik utvalget ser det ikke blir fulgt opp i praksis. Det er også store ulikheter i hvordan de enkelte samfunnssektorene forstår og praktiserer lovens virkeområde. Enkelte samfunnssektorer oppfatter sikkerhetsloven som en ren statssikkerhetslov, mens andre legger til grunn at loven må forstås i lys av den generelle samfunnsutviklingen som har funnet sted de senere årene – og derfor at loven også i dag har et bredere nedslagsfelt enn ren statssikkerhet.

Siden lovens ikrafttredelse har det skjedd store endringer i hvordan staten organiserer sin virksomhet. Stadig større deler av det som tidligere ble regnet som statlig virksomhet blir i dag konkurranseutsatt. Disse endringene er problematiske sett hen til hvordan det saklige virkeområde til gjeldende sikkerhetslov er innrettet.

I tillegg til omorganiseringen av statlig virksomhet, medfører den teknologiske utviklingen at den gjensidige avhengigheten mellom virksomheter – og mellom samfunnssektorer – er økende. Skillelinjene mellom de ulike samfunnssektorene, og mellom offentlig og privat virksomhet, har i økende grad blitt visket ut ved etableringen av et nettverksbasert samfunn. Dette skaper nye sårbarheter, som igjen kan føre til at redusert funksjonalitet hos en virksomhet kan få store konsekvenser for andre virksomheter.

Et annet forhold som har betydning for forebyggende nasjonal sikkerhet er globaliseringen av samfunnet. For å tilpasse seg konkurranse i et internasjonalt marked vil tilførsel av kapital kunne være av stor betydning for en rekke virksomheter. Dette påvirker igjen de etablerte eierstrukturene, hvor utenlandske aktører i økende grad får eierinteresser i norske virksomheter. I tillegg er norske virksomheter avhengig av å kunne anskaffe varer og tjenester i et globalt marked. Sett i lys av et endret og mer komplekst trusselbilde, vil en slik globalisering kunne medføre økt sårbarhet.

Utvalgets målsetting med et nytt lovgrunnlag for forebyggende nasjonal sikkerhet er å legge til rette for et harmonisert sikkerhetsnivå for de mest kritiske samfunnsfunksjonene, på tvers av samfunnssektorene, som er mer utfyllende diskutert i kapittel 6.7.3. En tenkende trusselaktør vil søke etter det svakeste leddet og utnytte eksisterende sårbarheter. Økt sikkerhetsnivå i enkelte samfunnssektorer, vil således samtidig kunne skape en økt risiko for de samfunnssektorer som ikke har tilsvarende høyt sikkerhetsnivå. En forutsetning for et slikt harmonisert sikkerhetsnivå er at loven favner over alle samfunnssektorene.

En ytterligere målsetting for utvalget er at et nytt lovgrunnlag reflekterer en grundig og betryggende avveining mellom nasjonale sikkerhetsbehov på den ene siden og rettssikkerhets- og personvernhensyn på den andre. Lovforslaget må innrettes på en slik måte at sikkerhetsmessige tiltak etter loven, ikke samtidig undergraver individuelle rettigheter og andre grunnleggende verdier i et demokratisk samfunn.

Det har også vært en målsetting for utvalget at etablering av sikkerhetstiltak etter loven skal stå i et rimelig forhold til det som oppnås ved tiltaket. Regelverket må ikke medføre uforholdsmessig høye kostnader for den enkelte virksomhet, sett opp mot den sikkerhetsmessige gevinsten som oppnås i et samfunnsperspektiv.

En grunnleggende problemstilling utvalget må ta stilling til er hvor bredt nedslagsfelt et nytt lovgrunnlag bør ha, herunder i hvor stor grad loven bør få anvendelse for virksomheter som ikke er forvaltningsorganer.

En annen grunnleggende problemstilling er hvor stor grad av sentral styring en bør ha sett opp mot den enkelte samfunnssektors autonomi.

I den videre omtalen av regulering av forebyggende sikkerhet er det i stor grad benyttet samme begrepsapparat som i DSBs KIKS-rammeverk (se kapittel 4.2.2). Dette innebærer at det legges vekt på opprettholdelse av samfunnsfunksjoner, som har direkte betydning for befolkningen/landets interesser og behov. Opprettholdelse av samfunnsfunksjonene sikres gjennom ivaretakelse av nødvendig infrastruktur og nødvendige innsatsfaktorer. Eksempler på innsatsfaktorer som er relevante i forebyggende sikkerhetssammenheng er: personell, teknisk materiell, informasjon og informasjonssystemer og kapital.

6.2 Gjeldende sikkerhetslovs regulering

Sikkerhetslovens[1] formål, virkeområde og legaldefinisjoner finnes i lovens kapittel 1 – Alminnelige bestemmelser. I det følgende vil det først redegjøres for lovens tredelte formål. Deretter vil det gis en nærmere redegjørelse for lovens virkeområde. For å få en fullstendig forståelse av lovens virkeområde, er det også nødvendig å se dette i lys av lovens formålsbestemmelse. Avslutningsvis vil lovens bestemmelse om legaldefinisjoner omtales.

6.2.1 Lovens formål

6.2.1.1 Rikets sikkerhet og andre vitale nasjonale sikkerhetsinteresser

Sikkerhetslovens formål følger av loven § 1. For det første skal loven legge forholdene til rette for effektivt å kunne motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser. Begrepet *rikets sikkerhet* er en rettslig standard, som ifølge forarbeidene kan forandre seg med samfunnsutviklingen.

Forarbeidene beskriver videre begrepet *vitale nasjonale sikkerhetsinteresser* som et samlebegrep som dekker samtlige felt innenfor rikets totale sikkerhetsbehov. Begrepet skal til enhver tid vurderes og defineres av overordnede politiske myndigheter. Terskelen for å si at noe truer slike interesser i medhold av sikkerhetsloven vil være høy, og det understrekes at begrepet kan endres i takt med samfunnsutviklingen og de sikkerhetsmessige utfordringer som Norge til enhver tid står overfor.

Utvalget har inntrykk av at en utfordring med dagens regelverk er hvordan begrepsapparatet *rikets sikkerhet* og *andre vitale nasjonale sikkerhetsinteresser* har blitt forstått og praktisert. Forarbeidenes henvisning til at overordnede politiske myndigheter til enhver tid skal vurdere og definere innholdet i begrepene, har i liten grad blitt fulgt opp i praksis. Det er i dag motstridende synspunkter på det nærmere meningsinnholdet i begrepene. Enkelte hevder at lovens formål og virkeområde er avgrenset til beskyttelse av statssikkerheten i snever forstand, herunder ivaretakelse av statens eksistens, suverenitet, suverene rettigheter og integritet. Andre hevder at begrepene må forstås i lys av den generelle samfunnsutviklingen de senere år, som i stor grad har medført at det tradisjonelle skillet mellom statssikkerhet, samfunnssikkerhet og individuell sikkerhet og trygghet har blitt visket noe ut.

6.2.1.2 Skjermingsverdig informasjon og objekter

Loven skal beskytte skjermingsverdig informasjon mot kompromittering[2] og skjermingsverdige objekter mot redusert funksjonalitet, ødeleggelse eller rettsstridig overtakelse av uvedkommende.[3]

Med *skjermingsverdig informasjon* menes informasjon hvor kompromittering kan få skadefølger for Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser, jf. loven § 11, jf. § 3 nr. 8 og 9. Informasjonen skal klassifiseres på bakgrunn av en verdivurdering, hvor graden av skadefølger er avgjørende for hvilken klassifisering som skal legges til grunn.

I skadevurderingen som ligger til grunn for klassifisering av skjermingsverdig informasjon, jf. loven § 11, er begrepene rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser, supplert av to andre begreper; *alliertes sikkerhet* og *forholdet til fremmede makter*. For å forstå hele lovens formål, er det følgelig nødvendig å inkludere § 11.

Med *skjermingsverdige objekter* menes områder, bygninger, anlegg, transportmidler eller annet materiell, hvor redusert funksjonalitet, ska-

[1] Lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven).

[2] Sikkerhetsloven kapittel 4.

[3] Sikkerhetsloven kapittel 5.

deverk eller rettsstridig overtakelse kan få skadefølger for rikets selvstendighet og sikkerhet og andre nasjonale vitale sikkerhetsinteresser, jf. loven § 17a, jf. § 3 nr. 12 og 13. Også skjermingsverdige objekter skal klassifiseres på bakgrunn av en verdivurdering, hvor graden av skadefølger er avgjørende for klassifiseringen.

For det andre skal loven bidra til å ivareta den enkeltes rettssikkerhet. I forarbeidene er det vist til at det særlig er innenfor området personellsikkerhet og sikkerhetsklareringer at den enkeltes interesser «berøres av legitime sikkerhetsinteresser».[4] De rettssikkerhetsgarantier som er etablert i den forbindelse, vil bli grundigere behandlet i kapittel 10. Som et generelt prinsipp, følger det av loven § 6 første og annet ledd at det ved utøvelse av sikkerhetstjeneste etter loven ikke skal nyttes mer inngripende midler og metoder enn det som fremstår som nødvendig, og at det skal tas særlig hensyn til den enkeltes rettssikkerhet.

For det tredje skal loven trygge tilliten til, og forenkle grunnlaget for, kontroll med forebyggende sikkerhetstjeneste etter loven. I loven kapittel 8 er det fastsatt at forebyggende sikkerhetstjeneste er underlagt kontroll og tilsyn av EOS-utvalget, jf. § 30 første ledd. Etter annet ledd kan Kongen etablere særskilte ordninger for å kontrollere Nasjonal sikkerhetsmyndighet og andre virksomheters forebyggende sikkerhetstjeneste.

For forsvarssektorens vedkommende har Forsvarsdepartementet fastsatt en egen instruks om sikkerhetstjeneste i Forsvaret. For å styrke departementets tilsyn med Forsvarets sikkerhetsavdeling (FSA) er det i instruksen § 7 etablert et eget tilsynsutvalg for FSA.[5] Dette tilsynet kommer i tillegg til EOS-utvalgets ansvar for å kontrollere EOS-tjeneste.

6.2.1.3 Begrepet rikets sikkerhet i annet regelverk

Som redegjort for i kapittel 4.2.4. har begrepet *rikets sikkerhet* blitt erstattet med *grunnleggende nasjonale interesser* i ny straffelov av 2005 og i utlendingsloven.

Straffelovkommisjonen konkluderte i sin utredning med at vernet mot innhenting og avsløring av hemmelige opplysninger, ikke burde begrenses til interesser som gjaldt *rikets sikkerhet* i tradisjonell forstand, men at også *grunnleggende nasjonale interesser* burde omfattes. Kommisjonen fremhevet i den forbindelse de interesser som er knyttet til infrastruktur, energi-, mat- og vannforsyning, samferdsel og telekommunikasjon, helseberedskap, bank- og pengevesen og andre samfunnsøkonomiske forhold.[6]

I utlendingsloven som trådte i kraft 1. januar 2010, ble begrepet *rikets sikkerhet* i den tidligere lov av 24. juni 1988 nr. 64, erstattet med *grunnleggende nasjonale interesser*. I forarbeidene til utlendingsloven påpekte departementet at begrepet grunnleggende nasjonale interesser var et mer dekkende begrep, som klarere reflekterer hvilke interesser man ønsker å beskytte. Det ble vist til at begrepet *rikets sikkerhet* er noe utdatert i lys av den senere tids utvikling. Begrepet *grunnleggende nasjonale interesser* må ifølge forarbeidene tolkes i lys av den generelle samfunnsutviklingen og endringer i det internasjonale trusselbildet, og at begrepet har en dynamisk karakter.[7]

6.2.1.4 Sikkerhetstruende virksomhet

Sikkerhetsloven skal legge til rette for effektivt å motvirke *trusler* mot rikets sikkerhet m.m., jf. loven § 1 første ledd. Hvilke *trusler* det er tale om følger implisitt av definisjonen av forebyggende sikkerhetstjeneste i loven § 3 nr. 1. Med forebyggende sikkerhetstjeneste menes i lovens forstand: planlegging, tilrettelegging, gjennomføring og kontroll av forebyggende sikkerhetstiltak som søker å fjerne eller redusere risiko som følge av *sikkerhetstruende virksomhet*.

Med *sikkerhetstruende virksomhet* menes «forberedelse til, forsøk på og gjennomføring av spionasje, sabotasje eller terrorhandlinger, samt medvirkning til slik virksomhet», jf. loven § 3 nr. 2. Begrepene *spionasje*, *sabotasje* og *terrorhandlinger* er videre definert i loven § 3 nr. 3-5.

Lovens formål er således avgrenset til å legge til rette for effektivt å motvirke nærmere bestemte typer *tilsiktede uønskede hendelser*, samt forberedelse til, forsøk på og medvirkning til slik virksomhet.

Arbeidsgruppen som evaluerte sikkerhetsloven påpekte at lovens avgrensing til beskyttelse mot *sikkerhetstruende virksomhet*, kan være noe snever sett hen til hvilke faktorer som kan utgjøre en trussel mot de verdier loven tar sikte på å beskytte. Andre forhold, som forsettlige lekkasjer av sikkerhetsgradert informasjon, utro tjenere og

---

4 Ot.prp. nr. 49 (1996–97), pkt. 5.6.8

5 Forskrift 29. april 2010 nr. 695, *Instruks om sikkerhetstjeneste i Forsvaret*, fastsatt av Forsvarsdepartementet 29. april 2010 med hjemmel i instruksjonsmyndighet.

6 NOU 2003: 18, 72 flg.

7 Ot.prp. nr. 75 (2006–2007), 385.

organisert kriminalitet, kan utgjøre en like stor trussel for samfunnet.[8]

6.2.2 Lovens virkeområde

6.2.2.1 Saklig virkeområde

Sikkerhetsloven har i utgangspunktet et organisatorisk avgrenset virkeområde. Det følger av loven § 2 første ledd at loven gjelder for *forvaltningsorganer*. Som forvaltningsorgan regnes i denne sammenheng ethvert organ for stat eller kommune. I forarbeidene til loven uttrykkes det at begrepet *forvaltningsorgan* skal forstås på samme måte som i forvaltningsloven og offentlighetsloven.[9]

6.2.2.2 Forvaltningsorganer

Hvorvidt en virksomhet er å anse som et forvaltningsorgan etter forvaltningsloven må avgjøres etter en konkret vurdering. I vurderingen legges det blant annet vekt på virksomhetens formål, dens arbeidsoppgaver og finansiering, samt graden av organisatorisk tilknytning til det offentlige og graden av politisk styring.[10]

Når det gjelder statsforetak følger det av statsforetaksloven § 4 at forvaltningsloven ikke gjelder for statsforetak. Arbeidsgruppen som evaluerte sikkerhetsloven uttalte i sin rapport at dette reiser spørsmålet om hvorvidt et statsforetak vil kunne være omfattet av sikkerhetsloven. Den anbefalte at ved en eventuell revisjon av loven, burde det bli sett nærmere på hvilken stilling statsforetak har, eller bør ha under sikkerhetsloven.[11]

Forsvarsdepartementet har i sin praktisering av sikkerhetsloven lagt til grunn at statsforetak ikke er å anse som forvaltningsorganer i lovens forstand. Statsforetak må derfor etter gjeldende praksis, på lik linje med andre selvstendige rettssubjekter, gjennom enkeltvedtak underlegges loven i medhold av gjeldende § 2 tredje ledd. Tidligere Luftforsvarets Hovedverksted Kjeller (LHK), nå AIM Norway SF, ble således underlagt sikkerhetsloven gjennom vedtak fra Forsvarsdepartementet[12].

I brev av 19. desember 2014 har Helse- og omsorgsdepartementet gjort en vurdering og kommet til at de regionale helseforetakene, helseforetakene, samt Norsk Helsenett SF, er å anse som forvaltningsorganer, og således omfattes av loven etter hovedregelen.

Avinor AS er omfattet av sikkerhetsloven, men ikke etter enkeltvedtak. Etter en lengre prosess ble det vurdert at selskapet var å anse som et forvaltningsorgan, og således underlagt etter hovedregelen i § 2, første ledd.

Endringene i hvordan staten organiserer sin virksomhet på, nærmere omtalt i kapittel 6.5, utfordrer innretningen av gjeldende lovs virkeområde. Stadig større deler av det som tradisjonelt har vært å anse som statlig virksomhet, blir omdannet til andre virksomhetsformer, herunder statsforetak, statlige aksjeselskaper og hel- eller delprivatiserte selskaper.

6.2.2.3 Leverandører i sikkerhetsgraderte anskaffelser

Selvstendige rettssubjekter er kun direkte omfattet av sikkerhetsloven for det tilfellet at de er leverandører av varer i forbindelse med en sikkerhetsgradert anskaffelse, jf. §2 annet ledd.

En sikkerhetsgradert anskaffelse innebærer at leverandøren vil få tilgang til skjermingsverdig informasjon eller et skjermingsverdig objekt, eller at anskaffelsen må sikkerhetsgraderes av andre årsaker, jf. loven § 3 nr. 17. Anskaffelsen må da gjennomføres etter reglene i lovens kapittel 7, samt forskrift om sikkerhetsgraderte anskaffelser. Dette regelverket vil bli nærmere omtalt i kapittel 11.

6.2.2.4 Kongens vedtaksmyndighet

Sikkerhetsloven § 2 tredje ledd gir Kongen fullmakt til å bestemme at loven helt eller delvis også kan gjøres gjeldende for ethvert annet rettssubjekt, herunder enkeltpersoner, foreninger, stiftelser, selskaper og privat og offentlig næringsvirksomhet, dersom ett av følgende vilkår er oppfylt:

- rettssubjektet eier eller på annen måte har kontroll over eller fører tilsyn med skjermingsverdig objekt, eller
- et forvaltningsorgan gir rettssubjektet tilgang til sikkerhetsgradert informasjon.

---

8 Forsvarsdepartementet, *Evaluering av sikkerhetsloven – Rapport fra arbeidsgruppe under ledelse av Forsvarsdepartementet* (Oslo: Forsvarsdepartementet, 2012, 17–18.

9 Ot.prp. nr. 49 (1996–97), pkt. 11.

10 Se for eksempel Justis- og beredskapsdepartementet v/ Lovavdelingens tolkningsuttalelse av 17. desember 2003.

11 Arbeidsgrupperapport, *Evaluering av sikkerhetsloven – Rapport fra arbeidsgruppe under ledelse av Forsvarsdepartementet*, 2012, 13.

12 AIM Norway SF ble omdannet til aksjeselskap med virkning fra 1. august 2016, jf. lov 17. juni 2016 nr. 44

Boks 6.1 Selvstendige rettssubjekter underlagt loven:

- Senter for informasjonssikring (NorSIS)
- Telenor ASA
- NSB AS
- Posten AS
- Avinor AS (vurdert som forvaltningsorgan)
- CargoNet AS
- Flytoget AS
- Det Kongelige Hoff
- Næringslivets sikkerhetsråd (NSR)
- Broadnet AS
- ROM Eiendom AS
- Aerospace Industrial Maintenance Norway (AIM Norway SF)
- Space Norway AS

Kilde: Nasjonal sikkerhetsmyndighet, https://www.nsm.stat.no/publikasjoner/regelverk/lover/

Kongens myndighet etter denne bestemmelsen er delegert til Forsvarsdepartementet.[13] I praksis vil Forsvarsdepartementet treffe slike vedtak etter en begrunnet anmodning fra ansvarlig fagdepartement. For rettssubjekter som eier eller råder over skjermingsverdige objekter, er det fastsatt egne regler for hvordan identifisering og utpeking skal skje i loven kapittel 5 om objektsikkerhet med underliggende forskrift.

En gjennomgående utfordring med vedtaksmyndigheten etter loven § 2 tredje ledd, er at den ikke angir noen form for systematikk for hvordan selvstendige rettssubjekter, som oppfyller vilkårene for å bli underlagt loven, skal identifiseres. Loven pålegger verken Forsvarsdepartementet eller de enkelte fagdepartementene noen konkret plikt til å kartlegge eller på annen måte identifisere hvilke virksomheter som bør underlegges sikkerhetsloven. Det har heller ikke gjennom praksis blitt etablert noen form for mekanisme som kan fange opp når et eventuelt behov for å vurdere og treffe vedtak, melder seg.

6.2.2.5 Særregler for domstolene

Det følger av § 2 fjerde ledd at loven også gjelder for domstolene, men med de særregler som følger av bestemmelsene om sikkerhetsklarering og autorisasjon i medhold av domstolloven og straffeprosessloven.

Med hjemmel i domstolloven §§ 12, 21 og 91 er det fastsatt særbestemmelser for domstolene i personellsikkerhetsforskriften kapittel 7. Bestemmelsene i forskriften kapittel 7 gjelder i saker ved domstolene hvor det blir lagt frem dokumenter, gitt opplysninger fra dokumenter eller avgitt forklaringer som inneholder sikkerhetsgradert informasjon. Bestemmelsene gjelder for fagdommere, lagrettsmedlemmer, meddommere, prosessfullmektiger, forsvarere, sakkyndige og andre som kan få tilgang til sikkerhetsgradert informasjon.[14]

At det ikke stilles krav om sikkerhetsklarering og autorisasjon for dommere i Høyesterett følger implisitt av domstolloven § 5 – som i motsetning til de tilsvarende bestemmelsene for lagmannsrettene og tingrettene i domstolloven §§ 12 og 21 – ikke inneholder noen bestemmelse om sikkerhetsklarering og autorisasjon. Dette er også berørt i forarbeidene til loven hvor det uttales at «[d]et foretas i dag ikke sikkerhetsklarering av Høyesteretts dommere. Lovforslaget tar ikke sikte på å endre på dette».[15]

Regjeringen fremmet i Prop. 97 L (2015–2016) om endringer i sikkerhetsloven, forslag om en uttrykkelig lovfesting av unntaket for dommere i Høyesterett. Stortinget har, i forbindelse med behandlingen av Innst. 352 L (2015–2016) til Prop. 97 L (2015–2016) om endringer i sikkerhetsloven, vedtatt regjeringens forslag til lovfesting av unntaket.

6.2.2.6 Unntak for Stortinget og dets organer

Det fremgår av § 2 femte ledd at loven ikke gjelder for Stortinget, Riksrevisjonen, Stortingets ombudsmann for forvaltningen og andre organer for Stortinget.

I forarbeidene er unntaket omtalt på følgende måte:

> At loven formelt ikke gjøres gjeldende for Stortingets organer, er i samsvar med gjeldende praksis og følger også av konstitusjonelle hensyn. Som i dag, er dette naturligvis ikke til hinder for at disse organer etter egen beslutning finner det hensiktsmessig å anvende reglene så langt de passer.[16]

---

[13] Kgl.res. 27. juni 2003 nr. 802, Delegering av myndighet til Forsvarsdepartementet etter sikkerhetsloven § 2 tredje ledd.

[14] Forskrift 29. juni 2001 nr. 722 om personellsikkerhet (personellsikkerhetsforskriften), § 7-1 første og annet ledd.

[15] Ot.prp. nr. 49 (1996–97), 30.

[16] Ibid., pkt. 11.

Verken ordlyden i bestemmelsen, eller forarbeidene til loven, gir nærmere veiledning om hva som ligger i «andre organer for Stortinget». De organer som er eksplisitt nevnt i bestemmelsen er Stortingets eksterne kontrollorganer. En naturlig forståelse av ordlyden vil da være at også andre kontrollorganer for Stortinget vil være omfattet av unntaket.

Tilsvarende unntak fra loven finnes også i forvaltningsloven § 4 fjerde ledd og offentleglova § 2 tredje ledd. Forarbeidene til forvaltningsloven eller offentleglova gir heller ikke noen nærmere begrunnelse for unntaket. Utredningen som lå til grunn for offentleglova viste til at deres mandat ikke la opp til at utvalget skal vurdere disse bestemmelsene generelt, og at utvalget uansett ikke foreslo endringer i disse reglene.[17]

I forarbeidene til den nå opphevede offentlighetsloven av 1970 fremgår følgende om unntaket for Stortinget og dets organer:

> Selv om man ved anvendelsen av loven tar utgangspunkt i hvorvidt den virksomhet det gjelder etter sin art er forvaltningsvirksomhet, må ikke dette synspunkt føres til sin ytterste konsekvens. Det følger således av seg selv at Stortinget og de organer som er underlagt dette – Riksrevisjonen og Stortingets ombudsmann for forvaltningen – ikke faller inn under loven selv om f.eks. Stortinget i en viss utstrekning utøver forvaltningsmyndighet.[18]

Forvaltningsloven og sikkerhetsloven har som felles utgangpunkt at de gjelder for *forvaltningsorganer*. Unntaket for Stortinget og dets organer synes her like mye å følge som en konsekvens av at Stortinget ikke anses som et forvaltningsorgan, som av rent konstitusjonelle hensyn. De konstitusjonelle hensyn, som gjør seg gjeldende etter dagens sikkerhetslov synes i all hovedsak å rette seg mot de deler av loven hvor myndighetsorganer er tillagt oppgaver som, anvendt overfor Stortinget, vil kunne bryte med maktfordelingsprinsippet, herunder bestemmelsene knyttet til autorisasjon og sikkerhetsklarering, samt NSMs tilsynsmyndighet og adgangsrett.

Stortinget, Riksrevisjonen og Sivilombudsmannen har i tråd med uttalelsene i forarbeidene, etter egen beslutning valgt å regulere forholdet til sikkerhetsloven i eget regelverk.

I Stortingets forretningsorden er forholdet til sikkerhetsloven berørt i § 75 annet ledd bokstav a), hvor det fremgår at stortingsrepresentantene har taushetsplikt om det som de under utøvelsen av stortingsvervet får kjennskap til om informasjon som er gradert i henhold til sikkerhetsloven eller beskyttelsesinstruksen.[19]

I riksrevisjonsloven[20] § 16 fremgår det at bestemmelsene i sikkerhetsloven gjelder så langt de passer for Riksrevisjonens behandling av sikkerhetsgradert informasjon. Etter bestemmelsens annet ledd kan Stortinget gi utfyllende bestemmelser om forholdet til sikkerhetsloven. Utfyllende bestemmelser er gitt i Instruks om Riksrevisjonens virksomhet[21] § 14, hvor det fremgår at sikkerhetsloven § 9 første ledd bokstav c (om NSMs tilsynsmyndighet) og § 10 (om NSMs adgangsrett) ikke gjelder for Riksrevisjonen. Av bestemmelsens annet ledd fremgår det at Riksrevisjonen er klareringsmyndighet for eget og tilknyttet personell.

I sivilombudsmannsloven[22] § 9 annet ledd fremgår det at ombudsmannen har taushetsplikt om informasjon som er gradert i henhold til sikkerhetsloven eller beskyttelsesinstruksen. Taushetsplikten varer ved også etter ombudsmannens fratreden. Den samme taushetsplikt påhviler hans personale og andre som bistår ved utførelsen av ombudsmannens arbeidsoppgaver.

6.2.2.7 Unntak for regjeringens medlemmer

Regjeringen fremmet i Prop. 97 L (2015–2016) om endringer i sikkerhetsloven, det forslag å lovfeste praksisen om at regjeringsmedlemmer er unntatt plikt til autorisering og sikkerhetsklarering. Etter fast og langvarig praksis fulgt av ulike regjeringer, foretas det ingen autorisasjon og sikkerhetsklarering av regjeringsmedlemmer.

Stortinget har, i forbindelse med behandlingen av Innst. 352 L (2015–2016) til Prop. 97 L (2015–2016) om endringer i sikkerhetsloven, vedtatt regjeringens forslag til lovfesting av praksisen om at regjeringens medlemmer er unntatt plikt til autorisering og sikkerhetsklarering.

6.2.2.8 Lovens anvendelse i krise og krig

Sikkerhetsloven er i utgangspunktet en fredstidslov, men det følger av forarbeidene at loven var

---

17 NOU 2003: 30, *Ny offentlighetslov*, 66.

18 Ot.prp. nr. 70 (1968–69) om lov om offentlighet i forvaltningen, 30.

19 Forskrift 7. juni 2012 nr. 618, om Stortingets forretningsorden, § 75.

20 Lov 7. mai 2004 nr. 21, om riksrevisjonen (riksrevisjonsloven).

21 Forskrift 11. mars 2004 nr. 700, Instruks om Riksrevisjonens virksomhet.

22 Lov 22. juni 1962 nr. 8 om Stortingets ombudsmann for forvaltningen (sivilombudsmannsloven),

Boks 6.2 Skjerpet taushetsplikt

For medlemmer av regjeringen, Stortinget og Høyesterett, samt medlemmer av landets øverste sivile og militære ledelse, er det skjerpede straffebestemmelser for avsløring av statshemmeligheter, jf. straffeloven § 124.

ment å gjelde fullt ut også i krise- og krigssituasjoner:

> Lovforslagets bestemmelser er primært utformet med henblikk på anvendelse under normale fredsforhold. Dersom krig truer eller rikets selvstendighet eller sikkerhet er i fare, kan eventuelle tilpasninger om nødvendig fremmes for Stortinget eller skje med hjemmel i beredskapslovgivningens fullmakter. Departementet anser det ikke nødvendig eller hensiktsmessig å regulere sikkerhetstjenestens oppgaver eller beføyelser i krise og krig i det foreliggende lovforslag.[23]

6.2.2.9 Lovens stedlige virkeområde

Det følger av § 2 sjette ledd at loven gjelder for Svalbard og Jan Mayen i den utstrekning Kongen bestemmer. Loven er gjort gjeldende for Svalbard og Jan Mayen i forskrift av 31. mai 2013 nr. 558. Begrunnelsen for utvidelsen var dels at norske forvaltningsorganer på Svalbard og Jan Mayen har behov for å kunne behandle sikkerhetsgradert informasjon, og dels at det er etablert bakkestasjoner for det europeiske satelittnavigeringsprogrammet Galileo her. Bakkestasjonene må kunne håndtere sikkerhetsgradert informasjon, og EU anser disse stasjonene som kritisk infrastruktur.

Det beror på vedkommende lov, lest i lys av folkeretten, hvilket geografisk virkeområde den har. Norsk lov er ikke nødvendigvis begrenset til å gjelde på norsk territorium (territorial–jurisdiksjon). Eksempelvis kan Norge gi lover anvendelse for norske borgere i utlandet (personaljurisdiksjon). Normalt reguleres virksomheten til norske foretak i utlandet av reglene i den staten der virksomheten drives. Norsk selskapslovgivning og regnskapsplikt gjelder imidlertid for norske selskaper selv om de driver virksomhet i utlandet.

Lovens anvendelse i utlandet er ikke regulert i loven, men det står følgende i forarbeidene:

> I den utstrekning loven får anvendelse for norske forvaltningsorganer, vil den selvfølgelig også gjelde for slike i utlandet, f.eks for militære enheter som deltar i internasjonale fredsoperasjoner, norske utenriksstasjoner i andre land, osv, med mindre noe annet skulle følge av folkerettslige regler.[24]

Forarbeidene omtaler ikke lovens anvendelse for selvstendige rettssubjekter, som ved enkeltvedtak er underlagt loven, i utlandet. Hvorvidt loven vil gjelde for disse rettssubjektene i utlandet vil bero på det enkelte vedtak, samt eventuelle folkerettslige jurisdiksjonsregler.

6.2.3 Legaldefinisjoner

Dagens sikkerhetslov opererer med en rekke legaldefinisjoner i loven § 3 første ledd nr. 1–20. Begrepene som defineres, benyttes i varierende grad i de etterfølgende bestemmelsene.

Enkelte begreper, som for eksempel *sikkerhetstruende virksomhet*, jf. § 3 nr. 2, benyttes ikke i loven. Begrepet har imidlertid en sentral betydning i forståelsen av hva loven skal legge til rette for beskyttelse mot.

Andre begreper som er legaldefinert, inngår kun som et element i andre legaldefinisjoner. Sikkerhetstruende virksomhet består som nevnt av tre nye begreper – *spionasje*, *sabotasje* og *terrorhandlinger* – som utover å være elementer i beskrivelsen av sikkerhetstruende virksomhet, kun benyttes i en enkelt bestemmelse i loven.[25]

Enkelte andre begreper benyttes kun i svært begrenset utstrekning, enten i en enkelt lovbestemmelse eller i bestemmelser som står i nær sammenheng med hverandre.

6.3 Fremmed rett

6.3.1 Sverige

Formål og virkeområde for den svenske säkerhetsskyddslagen (1996) fremgår av loven 1 § om lovens virkeområde, 6 § om hva som menes med säkerhetsskydd og 7 § om hvilke typer sikkerhetstiltak som skal iverksettes.

Av lovens 1 § fremgår det at loven gjelder for stat, kommuner og landsting. Loven gjelder også for aksjeselskap, handelsbolag, foreninger og stiftelser, hvor myndighetene utøver en rettslig

[23] Ot.prp. nr. 49 (1996–97), 30.

[24] Ot.prp. nr. 49 (1996–97), 65.

[25] Sikkerhetsloven § 21 Vurderingsgrunnlaget for sikkerhetsklarering.

bestemmende innflytelse. Vurderingen av rettslig bestemmende innflytelse for de ulike selskapsformene, baseres blant annet på myndighetenes aksje- eller stemmeandel i aksjeselskaper og selskapet, jf. 4 §. Loven gjelder også for rettssubjekter som driver virksomhet av betydning for rikets sikkerhet eller som særskilt behøver beskyttelse mot terrorhandlinger. Loven gjelder i begrenset utstrekning for Riksdagen og dens underlagte organer, jf. 2 §.

Loven skal i henhold til 6 § legge til rette for beskyttelse mot spionasje, sabotasje og andre straffbare handlinger som kan true rikets sikkerhet. Loven skal også gi beskyttelse i andre tilfeller av opplysninger som omfattes av hemmelighold etter *offentlighets- og sekretesslagen* (2009:400), og som har betydning for rikets sikkerhet. I tillegg skal loven tilrettelegge for beskyttelse mot terrorhandlinger etter *lag om straff för terroristbrott* (2003:148), selv om handlingen ikke truer rikets sikkerhet.

Hvilke sikkerhetstiltak som kan iverksettes etter loven følger av 7 §, hvor det fremgår at beskyttelsen skal omfatte informasjonssikkerhet, adgangsbegrensninger og sikkerhetsklarering av personell.

Säkerhetsskyddslagen (1996) er for tiden under revisjon, og i mars 2015 ble en ekspertutredning overlevert til den svenske regjeringen.[26]

I rapporten foreslås blant annet en endring av lovens formålsbestemmelse. Begrepet *rikets säkerhet* foreslås erstattet med *Sveriges säkerhet*. Det presiseres imidlertid at dette bare er en språklig endring, som ikke vil innebære en utvidelse av lovens formål. Ved vurderingen av lovens formål så ekspertgruppen også hen til den nylig reviderte *Brottsbalken kapittel 19 Om brott mot Sveriges säkerhet*.

Lovens formålsbestemmelse foreslås i SOUen utvidet til også å omfatte virksomhet som ivaretar Sveriges internasjonale forpliktelser på sikkerhetsområdet.

Også lovens virkeområde foreslås endret. I utredningen foreslås et funksjonsbasert virkeområde:

– Virksomhet som innebærer håndtering av sikkerhetsgradert informasjon. Dette omfatter informasjon som enten er av betydning for Sveriges sikkerhet, eller som må beskyttes av hensyn til internasjonale forpliktelser.
– Virksomhet som av andre årsaker har et sikkerhetsmessig beskyttelsesbehov (i övrigt säkerhetskänslig verksamhet).

Om innholdet i begrepet *säkerhetskänslig verksamhet*, sies det i utredningen at:

> Det motsvarar delvis vad som i dag skyddas inom ramen för skydd mot terrorism, dvs. i huvudsak verksamhet vid skyddsobjekt, flygplatser och vissa verksamheter som ska skyddas enligt folkrättsliga åtaganden om luftfartsskydd, hamnskydd och sjöfartsskydd. Det skyddsvärda området bör dock inte avgränsas genom regleringen om skyddsobjekt utan ska även kunna innefatta annat slag av säkerhetskänslig verksamhet, t.ex. verksamheter som innefattar hantering av itsystem eller av sammanställningar av uppgifter som är av central betydelse för ett fungerande samhälle eller verksamhet som behöver skyddas på den grunden att den kan utnyttjas för att skada nationen, t.ex. vissa verksamheter inom det kärntekniska området.[27]

6.3.2 Danmark

Danmark har ikke noen generell sektorovergripende lov om forebyggende sikkerhet.

Sikkerhetsgraderte informasjon og sikkerhetsklarering av personell er nærmere regulert i *Sikkerhedscirkulæret* av 19. desember 2014.[28]

Danmark har ikke et sektorovergripende lovverk om beskyttelse av kritisk infrastruktur. Beredskapsstyrelsen har en generell plikt til å veilede myndighetene om beredskapsplanleggingen, men har ikke et tverrsektorielt ansvar for myndighetenes virkemidler overfor eiere og operatører av kritisk infrastruktur. Beredskapsstyrelsen har en *all hazards approach* til beskyttelse av kritisk infrastruktur.

Den 7. oktober 2015 fremmet den danske regjering forslag til Folketinget om en ny lov om nett- og informasjonssikkerhet for tilbydere av elektronisk kommunikasjon.[29] Formålet med den nye loven er å «fremme net- og informationssikkerheden i samfundet», jf. lovforslaget § 1. Forslagets virkeområde er avgrenset til å gjelde for tilby-

[26] SOU 2015:25, *Betänkande av Utredningen om säkerhetsskyddslagen.*

[27] SOU 2015:25, 290.

[28] *Cirkulære om sikkerhedsbeskyttelse af informationer af fælles interesse for landende i NATO eller EU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt.*

[29] L 10 Forslag til lov om net- og informationsikkerhed, fremsatt 07-10-2015.

dere av elektroniske kommunikasjonstjenester, som tilbyr offentlig tilgjengelige nett og tjenester. Lovforslaget vil bli nærmere omtalt under kapittel 8.

6.3.3 Storbritannia

Security Service Act (1989) danner det lovmessige grunnlaget for sikkerhetstjenestens virksomhet (*Security Service*). Funksjonen *Security Service* beskrives i artikkel 1 (2) på følgende måte;

> The function of the Service shall be the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means.

I tillegg skal sikkerhetstjenesten omfatte beskyttelse av Storbritannias økonomiske velferd (art. 1 (3)), samt understøttelse av politi og kriminalitetsbekjempelse (art. 1 (4)).

Loven fastslår sikkerhetstjenestens funksjon og virkeområde, men fastsetter for øvrig ingen nærmere regler om hvilke krav som settes til offentlige og sivile virksomheters arbeid med forebyggende sikkerhet.

Arbeidet med beskyttelse av kritisk infrastruktur er etter det utvalget har fått opplyst lovmessig forankret i Security Service Act (1989), og ivaretas av MI5s *Centre for the Protection of National Infrastructure* (CPNI). CPNI har en utstrakt rådgivningsvirksomhet overfor private aktører som eier eller forvalter kritisk infrastruktur, men har ikke myndighet til å gi pålegg eller sette krav til sikringen av slik infrastruktur. Informasjonssikkerhet for sikkerhetsgradert informasjon er nærmere regulert i policy for *Goverment Security Classifications,* utgitt av Cabinet Office i april 2014. Retningslinjene har ikke lovmessig status, men er etablert innenfor rammene av nasjonal britisk lovgivning og inkluderer de krav som følger av *Official Secrets Acts* (1911 og 1989), *Freedom of Information Act* (2000) og *Data Protection Act* (1998).

6.4 Tidligere vurderinger av lovens virkeområde

Det har i tidligere utredninger og revisjonsprosesser vært vurdert hvorvidt sikkerhetslovens virkeområde burde utvides til også automatisk å gjelde selvstendige rettssubjekter.

Forsvarsdepartementet opprettet sommeren 2000 en interdepartemental arbeidsgruppe med mandat til å fremme forslag til forskrift om objektsikkerhet med hjemmel i sikkerhetsloven kapittel 5[30]. I rapporten foreslo arbeidsgruppen blant annet at lovens virkeområde skulle utvides slik at også selvstendige rettssubjekter som eier eller råder over et skjermingsverdig objekt, eller er leverandører til slike, omfattes. Arbeidsgruppen anbefalte at det burde vurderes om sikkerhetsloven også burde komme til anvendelse overfor enhver som kan få rettmessig tilgang til skjermingsverdig informasjon.

Infrastrukturutvalget uttrykte i sin utredning at det ikke ville være hensiktsmessig å gjøre loven gjeldende for alle rettssubjekter:

> Utvalget mener at lovens innretting og virkemidler er av en slik karakter at det ikke vil være hensiktsmessig å gjøre loven generelt gjeldende for alle rettssubjekter. Å lage bestemte kriterier i loven for å angi hvilke virksomheter loven skal omfatte vil etter utvalgets mening være for upresist, og vil kunne medføre behov for lovendringer dersom justeringer ble påkrevd.[31]

Arbeidsgrupperapporten fra 2002 dannet grunnlaget for Forsvarsdepartementets forslag til revisjon av sikkerhetsloven. Når det gjaldt arbeidsgruppens forslag om å utvide sikkerhetslovens virkeområde, viste departementet til gjeldende vedtaksregime, og uttalte at:

> Etter departementets oppfatning gir dette et tilstrekkelig grunnlag i dag for å gi sikkerhetsloven anvendelse på de enkelte private rettssubjekter som har eierskap til skjermingsverdige objekter. Ved at det ved enkeltvedtak skal tas stilling til om et privat rettssubjekt skal omfattes av sikkerhetsloven, vil det for hvert enkelt tilfelle kunne foretas en interesseavveining, herunder hvilke økonomiske, administrative og sosiale konsekvenser som en anvendelse av sikkerhetsloven på rettssubjektet vil få. Departementet fremmer derfor ikke et lovforslag om endringer av sikkerhetslovens virkeområde.[32]

---

[30] Arbeidsgrupperapport, *Forebyggende sikring av objekter mot terror- og sabotasjehandlinger*, avgitt til Forsvarsdepartementet 24. mai 2002.

[31] NOU 2006: 6, 82.

Arbeidsgruppen som evaluerte sikkerhetsloven var delt i synet på om selvstendige rettssubjekter som eier eller forvalter et skjermingsverdig objekt, automatisk burde underlegges loven. Det ble fremhevet i arbeidsgruppen at det ikke ble ansett som hensiktsmessig å kartlegge samtlige virksomheter innenfor samfunn og næringsliv med sikte på å underlegge selvstendige rettssubjekter loven:

> Det er tvilsomt både om dette er mulig og om det er ønskelig. Det måtte i så fall kreve en grundig prosess og en konsekvensanalyse, herunder en analyse av økonomiske konsekvenser ved å legges inn under loven. Arbeidsgruppen vil ikke anbefale en nærmere vurdering av en så vidtgående endring av loven ved en revisjon nå.[33]

6.5 Organisering av offentlig virksomhet

Et spørsmål utvalget må ta stilling til er om dagens virkeområde er hensiktsmessig og bør videreføres. Organiseringen av offentlig virksomhet er et sentralt moment i denne vurderingen. Offentlig virksomhet omfatter både staten og kommunesektoren.

Tradisjonelt har staten organisert sin aktivitet i statlige virksomheter, det vil si innenfor staten som rettssubjekt og med direkte instruksjonsmyndighet. Utviklingen de siste tiår har imidlertid gått i retning av at det som tradisjonelt sett har blitt betraktet som statlig aktivitet, både i større grad utføres av selvstendige rettssubjekter og konkurranseutsettes til private aktører.

I NOU 2003: 34 Mellom stat og marked oppsummeres den forvaltningspolitiske utviklingen på følgende måte:

> Et hovedtrekk ved de statlige omstillingene siden slutten av 1980-tallet er at det er gitt større frihetsgrader innenfor staten og at virksomhetene er skilt ut i selvstendige rettssubjekter. Et annet viktig trekk er utvikling av supplerende virkemidler for regulering. Resultatet er videre økonomiske og administrative fullmakter for en rekke forvaltningsorganer, opprettelse av nye, mer fristilte organer, delegering av myndighet til ytre-/lavere organer i forvaltningshierarkiet og utskilling av virksomheter i rettslig selvstendige enheter. Arbeidsdelingen mellom offentlig sektor og privat sektor er i endring.[34]

Tradisjonelt grupperes de statlige tilknytningsformene i to hovedgrupper: statlige forvaltningsorganer som er en og samme juridiske person som staten, eller som statlige selskap som juridisk sett er utenfor staten. Disse kan igjen deles inn i undergrupper:[35]

Statlige forvaltningsorganer:

- Ordinære forvaltningsorganer, som for eksempel departementene, direktorater og tilsyn
- Forvaltningsorganer med særskilte budsjettfullmakter
- Forvaltningsbedrifter

Statlige selskaper:

- Statsaksjeselskap, det vil si statlige helheide aksjeselskaper organisert etter aksjeloven med de særbestemmelser som loven setter for slike selskaper
- Statsforetak, organisert etter statsforetaksloven
- Særlovselskap, som benyttes som betegnelse på selskaper som er regulert i egen lov, som også inneholder særskilte organisatoriske regler
- Stiftelser

En rekke større statlige forvaltningsbedrifter har de senere år blitt omdannet til statsforetak, særlovselskaper eller statsaksjeselskaper. Hovedregelen for disse er at de enten organiseres som statsaksjeselskap eller statsforetak.[36]

I henhold til Finansdepartementets liste over selskaper, er det i dag 70 selskaper hvor staten har et direkte eierskap. En rekke av disse selskapene ivaretar viktige samfunnsfunksjoner innen blant annet energi, ekom, helse, samferdsel.[37]

I tillegg til den statlige aktiviteten i offentlig sektor, blir også mye tjenesteproduksjon utført i

---

32 Ot.prp. nr. 21 (2007–2008) Om lov om endringer i lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven),19.

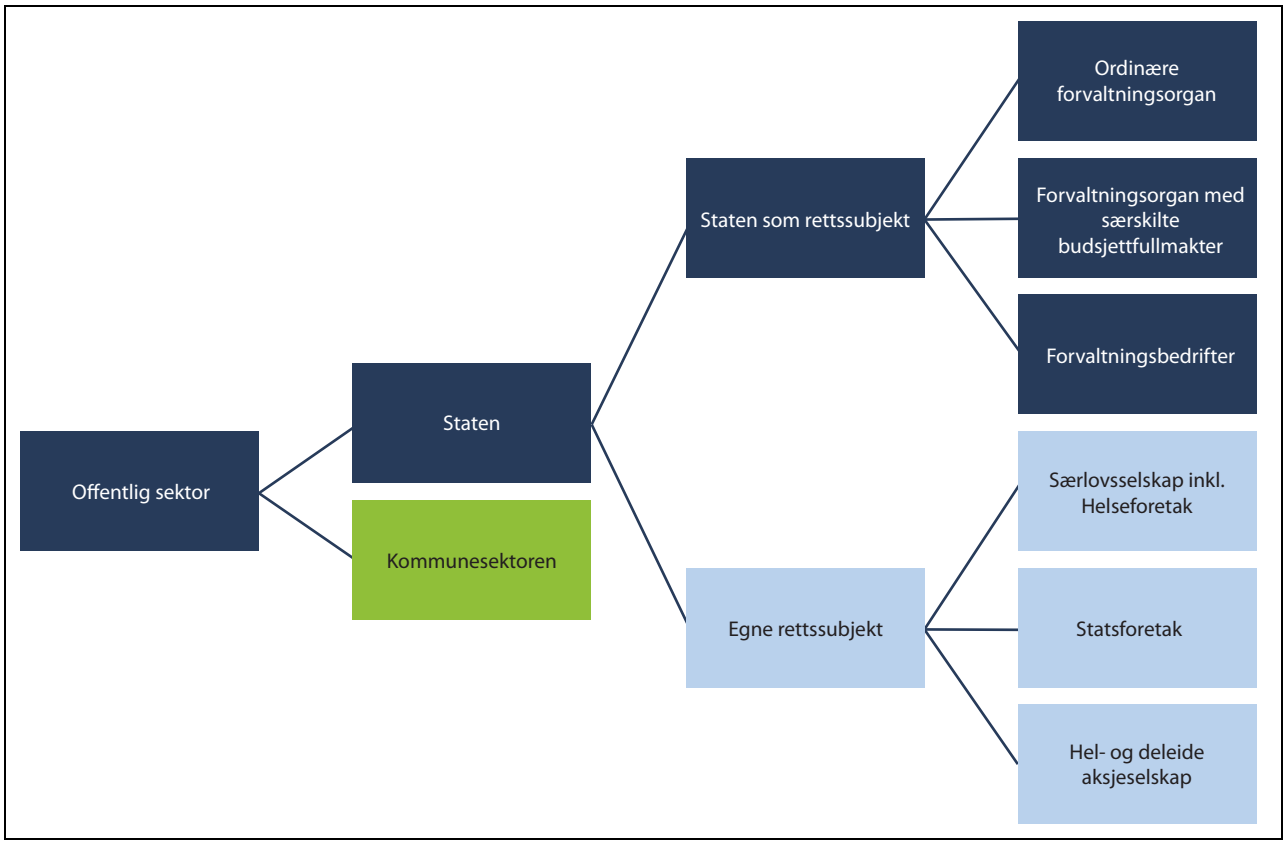
33 Arbeidsgrupperapport, *Evaluering av sikkerhetsloven – Rapport fra arbeidsgruppe under ledelse av Forsvarsdepartementet*, 2012, 14.

34 NOU 2003: 34, *Mellom stat og marked*, 12.

35 Ibid., 36 flg.

36 Difi 2014:1, *Fra stat til marked. Veileder om utskilling av virksomhet fra staten*, 8.

37 https://www.regjeringen.no/contentassets/63686604f2af43a8947448f242463208/oversikt_12_jan_2016.pdf.



Figur 6.1 Organisering av statlig virksomhet

Kilde: NOU 2015: 14, Bedre beslutningsgrunnlag, bedre styring – Budsjett og regnskap i staten, figur 3.5.

kommunal sektor, finansiert via tilskudd over statsbudsjettet. Kommunesektoren spiller en sentral rolle som tjenesteleverandør i norsk offentlig forvaltning. Kommunene har ansvar for grunnleggende tjenester til innbyggerne som for eksempel grunnskoleopplæring, primærhelsetjeneste og vann, avløp og renovasjon, mens fylkeskommunene har ansvar for regionalt kollektivtilbud.

Som redegjort for i kapittel 3.5, er det også en økende grad av gjensidig avhengighet mellom den militære og sivile sektoren. I en totalforsvarssammenheng er Forsvaret på flere områder helt avhengig av kompetanse, varer og tjenester fra private aktører. Disse private aktørene vil utgjøre en sentral innsatsfaktor for at Forsvaret skal kunne opprettholde kampkraft i en potensiell konfliktsituasjon. I regjeringens langtidsplan for forsvarssektoren beskrives Forsvarets avhengighet av det sivile samfunn på følgende måte:

> Sivil støtte til Forsvaret har hatt liten oppmerksomhet de siste årene. Samtidig har Forsvarets avhengighet av sivile leveranser økt. Det må derfor legges fornyet vekt på sivil støtte til Forsvaret. Dette aktualiseres ytterligere av at den sikkerhetspolitiske utviklingen øker behovet for at Forsvaret styrker sin beredskap.[38]

Det er en uttalt målsetting å gjøre offentlig sektor mer fleksibel og effektivt. En rendyrking av organisasjonsformer, hvor forvaltningsmessige og kontrollerende funksjoner holdes i statsadministrasjonen, mens mer forretningsmessige sider av virksomheten privatiseres, er en ønsket utvikling, som gir en rekke fordeler. Samtidig innebærer privatiseringen av offentlig virksomhet en økt sårbarhet ved at kritiske samfunnsfunksjoner, eller den direkte understøttelsen av disse, settes ut til selvstendige rettssubjekter.

Infrastrukturutvalget beskrev i sin utredning omorganiseringen av offentlig virksomhet som en utfordring for sikkerhet og beredskap:

> Virksomheter med sikkerhets- og beredskapsoppgaver omorganiseres og omreguleres. Det gjelder også virksomheter som på grunn av deres kritiske funksjon kan sies å ha betydning for rikets sikkerhet og vitale nasjonale interes-

[38] Prop. 151 S (2015–2016), 46.

Boks 6.3 Infrastrukturutvalgets kontrollpunkter:

1. Hvordan ivaretas sikkerhet og beredskap i virksomheten?
2. Hvilke konsekvenser har endringen for ivaretakelse av sikkerhet og beredskap i virksomheten?
3. Påvirker endringen regulering av sikkerhet og beredskap i virksomheten?
4. Påvirker endringen ivaretakelse av hensynet til rikets sikkerhet og vitale nasjonale interesser?
5. Hva er ressursinnsatsen til sikkerhet og beredskap i virksomheten før og etter endringen?
6. Hvilke underleverandører er virksomheten kritisk avhengig av for å opprettholde driftskontinuitet?
7. Leverer virksomheten samfunnskritiske varer og tjenester?
8. Hvordan skal spørsmål knyttet til sikkerhet og beredskap håndteres av virksomhetens ledelse og styrende organer?

> ser. Det må sies å være en sikkerhetsutfordring at hensynet til forretningsmessig drift kan komme i konflikt med hensynet til sikkerhet og beredskap. Overfor disse virksomhetene er det behov for å sikre at sikkerhets- og beredskapsoppgavene ivaretas på en hensiktsmessig måte.[39]

Infrastrukturutvalget beskrev også utfordringene knyttet til bortsetting av eksempelvis drift av IKT-systemer. Bildet kompliseres ytterligere av at sentrale tjenester settes bort uavhengig av geografi, noe som kan medføre at det oppstår situasjoner hvor nasjonal kontroll med kritisk infrastruktur og kritiske samfunnsfunksjoner begrenses av andre lands prioriteringer.

Grunnet de sikkerhetsmessige utfordringene som kan oppstå ved en omorganisering av offentlig virksomhet, anbefalte Infrastrukturutvalget at en liste over kontrollpunkter, som sikrer at hensynet til sikkerhet og beredskap blir ivaretatt, ble benyttet i fremtidige omorganiseringsprosesser.[40]

I DIFI's beskrivelse av sentrale hensyn ved valg av tilknytningsform, er et av vurderingskriteriene om virksomheten skal ivareta særskilte samfunnsoppgaver. Hensynet til sikkerhet og beredskap er ikke eksplisitt berørt i veilederen[41].

6.6 Kritisk infrastruktur og kritiske samfunnsfunksjoner

I Infrastrukturutvalgets utredning defineres kritisk infrastruktur på følgende måte:

> Kritisk infrastruktur er de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner som igjen dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse.[42]

Denne definisjonen er i hovedtrekk også lagt til grunn i senere rapporter og utredninger.

I sivilbeskyttelsesloven § 3 bokstav d) har man lagt til grunn samme definisjon av kritisk infrastruktur som i Rådsdirektiv 2008/114/EF av 8. desember 2008 om identifisering og utpeking av europeisk kritisk infrastruktur og vurdering av behovet for å beskytte den bedre, artikkel 2 bokstav a):

> anlegg, systemer eller deler av disse som er nødvendige for å opprettholde sentrale samfunnsfunksjoner, menneskers helse, sikkerhet, trygghet og økonomiske eller sosiale velferd og hvor driftsforstyrrelse eller ødeleggelse av disse vil kunne få betydelige konsekvenser.

Selv om ordlyden i sivilbeskyttelsesloven avviker noe fra den definisjonen som er lagt til grunn blant annet av Infrastrukturutvalget, er det i liten grad noen meningsforskjell mellom de definisjonene.

Infrastrukturutvalgets definisjon av kritisk infrastruktur består av tre hovedelementer:

1. Kritisk infrastruktur – som er de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner.
2. Samfunnets kritiske funksjoner – som er de funksjonene som dekker samfunnets grunnleggende behov.
3. Samfunnets grunnleggende behov.

---

39 NOU 2006: 6, 44.

40 Ibid., 87.

41 Difi 2014:1, *Fra stat til marked. Veileder om utskilling av virksomhet fra staten*.

42 NOU 2006: 6, 32.

Boks 6.4 Kritiske infrastruktursystemer – overordnet oversikt

Matforsyning	Produksjonsanlegg, distribunaler, logistikksystemer, butikker
Vann og avløp	Vannverk, renseanlegg, pumper, høydebasseng
Sosiale ytelser og tjenester	NAVs it-systemer
Finansielle tjenester	Finansiell infrastruktur
Energiforsyning	Kraftverk, transformatorer, kraftnett osv. Fjernvarmeanlegg, pumpestasjoner, ledningsnett Raffinerier, havneanlegg, tankanlegg, bensinstasjoner
Elektronisk kommunikasjon	Kjernenett, transportnett, svitsjer
Transport	Veinett, jernbanelinjer, terminaler, trafikkstyringssystemer
Satellittbaserte tjenester	Satellitter, bakkestasjoner

Kilde: DSB, Samfunnets kritiske funksjoner, høringsutgave september 2015, 85–86.

Definisjonen av kritisk infrastruktur tar utgangspunkt i begrepet *samfunnets grunnleggende behov*. Ut fra dette begrepet, kan det nærmere innholdet i de to andre begrepene utledes. Det kan ut fra definisjonen oppstilles tre spørsmål som må besvares for å kunne identifisere kritisk infrastruktur:

1. Hva er samfunnets grunnleggende behov?
2. Hvilke samfunnsfunksjoner er kritiske for å dekke disse behovene?
3. Hva slags systemer og anlegg er helt nødvendige for å opprettholde disse funksjonene?

Ved å besvare disse tre spørsmålene vil man kunne identifisere de systemene og anleggene som i henhold til Infrastrukturutvalgets vurdering må anses som kritisk infrastruktur.

Det første spørsmålet som må besvares er hva som utgjør samfunnets grunnleggende behov. Dette kan også formuleres som et verdispørsmål – hvilke verdier er det i et samfunnsmessig perspektiv helt grunnleggende å beskytte?

Som nevnt i kapittel 4.2.2, har DSB ut fra samfunnets grunnleggende behov, utledet hva som utgjør samfunnets kritiske funksjoner. Utledningen er gjort ut fra en vurdering av de mest tidskritiske funksjonene, hvor selv en kortvarig svikt vil få umiddelbare negative konsekvenser for befolkningen. I DSBs rapport er det identifisert 18 kritiske samfunnsfunksjoner, fordelt på fire undergrupper:

- Nasjonal styringsevne og suverenitet
- Befolkningens sikkerhet
- Befolkningens velferd
- Kultur og natur

Hvilke samfunnsfunksjoner som anses for kritiske, vil avhenge både av hvilke verdier og behov som legges til grunn for vurderingen og hvilke kriterierier som legges til grunn for vurdering av kritikalitet.

I rapporten Samfunnets kritiske funksjoner har DSB utarbeidet en overordnet oversikt over infrastruktur, som ut fra gitte kriterier anses som kritiske i et samfunnsperspektiv[43] er rapporten fokusert på infrastruktursystemer, altså infrastrukturer som utgjør et nettverk som leverer varer eller tjenester til et stort antall mottakere, og der svikt kan få mer vidtrekkende konsekvenser – det vil si kritiske infrastruktursystemer på et nasjonalt nivå.

Kritikaliteten i infrastrukturene i tabellen over vil variere, blant annet som følge av grad av avhengighet og redundans.[44] Veitransportsystemet er for eksempel generelt redundant de fleste steder, hvor det som regel finnes alternative kjøreruter og/eller transportformer (for eksempel båt). Noen strekninger, som betjener store befolkningsmengder, har imidlertid lite redundans. Her vil et avbrudd kunne få langt større konsekvenser. Det samme gjelder innenfor andre samfunnsfunksjoner, eksempelvis energiforsyning og elektronisk kommunikasjon. Noen deler av systemet er mer kritiske enn andre, enten fordi graden av

[43] DSB, *Samfunnets kritiske funksjoner – Hvilken funksjonsevne må samfunnet opprettholde til enhver tid,* 2015.

[44] Ibid., 87.

avhengighet er høy eller fordi redundansen i det aktuelle området er svak.

DSB presiserer i rapporten at vurderingen av hva som utgjør kritisk infrastruktur bør foretas av de myndigheter og virksomheter som kjenner den aktuelle infrastrukturen best, og bør gjøres gjennom analyser av hvilke avhengigheter som knytter seg til de ulike samfunnsfunksjonene.

I DSBs rapport KIKS 1[45] fremkommer det at kritisk infrastruktur betraktes som en nødvendig, men ikke tilstrekkelig forutsetning for opprettholdelse av kritiske samfunnsfunksjoner. For at samfunnsfunksjonene skal opprettholdes er de også avhengig av en rekke andre innsatsfaktorer.

De innsatsfaktorer som en virksomhet med kritisk samfunnsfunksjon er avhengig av for å kunne dekke samfunnets grunnleggende behov, betegnes her som kritiske innsatsfaktorer. Innsatsfaktorer som leveres av andre virksomheter skaper avhengigheter mellom samfunnsfunksjoner, infrastrukturer og virksomheter.

6.7 Utvalgets vurderinger

De senere års endringer av hvordan staten organiserer sin virksomhet, hvor stadig flere tjenester konkurranseutsettes og offentlige virksomheter hel- eller delprivatiseres, har medført at en rekke kritiske innsatsfaktorer eies og forvaltes av selvstendige rettssubjekter. Utvalget mener at gjeldende lovs virkeområde, som i utgangspunktet kun gjelder for *forvaltningsorganer*, er i utakt med den samfunnsutviklingen som har skjedd siden lovens ikrafttredelse.

Som Lysne-utvalget har vist til i sin utredning, regnes Norge som et av de mest digitaliserte landene i verden.[46] Denne digitalisering har ført til gjennomgripende samfunnsmessige endringer, noe som har gitt oss store effektiviserings- og moderniseringsgevinster. Samtidig har dette også ført til at Norge er et av de landene der endringene i risiko- og sårbarhetsbildet har kommet lengst, med sammensatte og komplekse avhengigheter på tvers av virksomheter og samfunnssektorer. Omorganiseringen av statlig virksomhet medfører også at disse avhengighetene går på tvers av offentlig og privat virksomhet. Dette har betydning for hvordan en ny sikkerhetslov bør innrettes.

Loven må, slik utvalget ser det, i tillegg reflektere at Norge i dag står overfor et bredt og sammensatt trusselbilde, hvor både statlige og ikkestatlige aktører utgjør en potensiell risiko for Norges mest grunnleggende interesser.

Utvalget har vurdert ulike alternativer for å strukturere et nytt lovgrunnlag for forebyggende nasjonal sikkerhet. Ifølge mandatet skal det konkret vurderes hvorvidt krav til «militær og sivil sektor skal reguleres i samme lov eller om lovgrunnlaget skal deles». En fordel med en delt løsning er at en egen lov innen forsvarssektoren vil kunne bidra til å ivareta Forsvarets særegne behov når det gjelder forebyggende sikkerhet. På den andre siden er heller ikke de sivile samfunnssektorene en homogen gruppe. Alle samfunnssektorer har i større eller mindre utstrekning særegenheter og særlige behov, som må ivaretas i det forebyggende sikkerhetsarbeidet. Utvalget har heller ikke sett det som en aktuell løsning å foreslå sektorvise lover. Gjensidige avhengigheter går på tvers av samfunnssektorene, og det er derfor av avgjørende betydning å ha en helhetlig tilnærming til arbeidet med forebyggende sikkerhet. For å oppnå en slik tilnærming mener utvalget at det er nødvendig å ha et sektorovergripende lovverk, som legger til rette for samhandling og koordinering på tvers av samfunnssektorene. Hensynet til den enkelte sektors særegne behov bør i stedet adresseres i hvordan selve loven utformes. Dette gjelder både for hvordan krav etter loven skal utformes og hvilke mekanismer som er nødvendige for å ivareta sektorspesifikke hensyn. Som en konsekvens av dette har utvalget kommet til at den beste løsningen vil være en sektorovergripende rammelov.

6.7.1 Ulike alternativer for lovens formål og virkeområde

Utvalget har vurdert ulike alternativer for et nytt lovgrunnlags formål og saklige virkeområde.

Et alternativ har vært å beholde begrepsapparatet i dagens sikkerhetslov. En fordel med en slik tilnærming er at *rikets sikkerhet* og *andre vitale nasjonale sikkerhetsinteresser*, er et etablert begrep innenfor forebyggende sikkerhet mot *terrorhandlinger*, *spionasje* og *sabotasje*. Som fremhevet i både forarbeidende og Infrastrukturutvalgets utredning, er begrepsapparatet ment å være en rettslig standard som skulle forandre seg i takt med samfunnsutviklingen. I teorien burde således samfunnsutviklingen siden lovens ikrafttredelse

[45] Direktoratet for samfunnssikkerhet og beredskap, *Sikkerhet i kritisk infrastruktur og kritiske samfunnsfunksjoner – modell for overordnet risikostyring*. KIKS-prosjektet – 1. delrapport, 2012.

[46] NOU 2015: 13.

være gjenspeilet i måten loven blir praktisert på i dag. Erfaringen så langt med praktiseringen av loven, viser imidlertid at det knytter seg stor grad av usikkerhet til hvordan begrepsapparatet skal forstås og praktiseres. Enkelte hevder at begrepsapparatet må forstås videre enn en snever fortolkning av statssikkerheten, mens andre hevder det motsatte. Ved en videreføring av dagens begrepsapparat risikerer man å videreføre denne usikkerheten. Man risikerer også at virkeområdet for den nye loven vil bli for snevert, både sett hen til utvalgets mandat og med hensyn til de verdier det er avgjørende å beskytte. Et annet forhold er at en videreføring av gjeldende lovs begrepsapparat, også vil medføre at det nye lovgrunnlaget fortsatt vil være i utakt med den moderniseringen som har skjedd i beslektet lovverk for øvrig.

Utvalget har vurdert hvorvidt man bør benytte det samme begrepsapparatet som den nye straffeloven og utlendingsloven – *grunnleggende nasjonale interesser*. En fordel med en slik harmonisering med beslektede regelverk, ville vært at praksis etter ny straffelov og utlendingsloven kunne bringes inn som tolkningsfaktorer ved forståelsen av en ny sikkerhetslovs formål og virkeområde. Basert på erfaringene med dagens sikkerhetslov, antar utvalget at rettspraksis etter henholdsvis straffeloven kapittel 17 og utlendingslovens bestemmelser knyttet til grunnleggende nasjonale interesser, vil være betydelig mer omfattende enn rettspraksis etter den nye sikkerhetsloven.

Også den generelle samfunnsutviklingen tilsier en dreining av fokus fra et rent statssikkerhetsperspektiv (slik noen hevder dagens sikkerhetslov har), til også i noen grad å omfatte det som tradisjonelt har blitt ansett som en del av den generelle samfunnssikkerheten.

Når utvalget likevel har kommet til at det ikke anses hensiktsmessig å benytte straffelovens og utlendingslovens begrepsapparat, skyldes ikke dette at man er uenig i dreiningen av fokus i straffeloven kapittel 17 og utlendingsloven. Sett i lys av samfunnsutviklingen, mener utvalget tvert imot at en dreining av fokus i retning samfunnssikkerhetsperspektivet er helt riktig og nødvendig. Utvalget mener imidlertid at en ny lov om forebyggende nasjonal sikkerhet bør ha som formål å beskytte de *funksjonene* som er helt avgjørende for at staten skal kunne ivareta de verdiene sikkerhetsloven skal beskytte. Det er disse funksjonene en trusselaktør i ytterste konsekvens vil forsøke å ramme, ved et anslag mot Norge og dets mest grunnleggende interesser og verdier. En slik funksjonsbasert tilnærming vil også være i tråd med metodikken i arbeidet med samfunnssikkerhet og beredskap for øvrig. Utvalget har derfor valgt å benytte begrepet *grunnleggende nasjonale funksjoner* for å angi lovens virkeområde.

Utvalget mener at lovens virkeområde bør innrettes slik at enhver virksomhet, offentlig eller privat, *som har råderett over informasjon, informasjonssystemer, objekter eller infrastruktur, eller som driver aktivitet, som er av kritisk betydning for grunnleggende nasjonale funksjoner*, omfattes av loven.

Utvalgets forslag til innretning av lovens formål og virkeområde vil sannsynligvis medføre at flere virksomheter vil bli underlagt den nye loven. Det er vanskelig å vurdere konkret hvor mange virksomheter som vil bli underlagt loven. Som det blir nærmere redegjort for i kapittel 7.7.1, foreslår utvalget en systematikk for å identifisere virksomheter som bør omfattes av loven for å sikre grunnleggende nasjonale funksjoner.

For virksomheter som ikke tidligere har vært underlagt sikkerhetsloven, vil en slik underleggelse kunne få vesentlige konsekvenser. Utvalget erkjenner at økte krav til sikkerhet også vil innebære økte kostnader, som kan virke tyngende for den enkelte virksomhet sett ut fra et bedriftsøkonomisk perspektiv. Utvalget mener likevel at de sikkerhetsmessige gevinstene i et samfunnsperspektiv overstiger de ulempene en utvidelse av lovens virkeområde vil kunne få for enkelte virksomheter. De gjensidige avhengighetene på tvers av samfunnssektorer og på tvers av virksomheter, gjør at det ikke er mulig å sikre de grunnleggende nasjonale funksjonene, uten at det samtidig stilles sikkerhetsmessige krav til de virksomheter som har en kritisk betydning for disse funksjonene.

Hvilke konsekvenser dette vil ha for den enkelte virksomhet, vil imidlertid avhenge av en rekke faktorer. For det første vil virksomhetens allerede etablerte sikkerhetstiltak, blant annet i medhold av relevant sektorregelverk, ha betydning for om, og i så fall hvor omfattende, behovet for forsterkede sikkerhetstiltak vil være. For det andre vil den nærmere årsaken til at virksomheten underlegges loven, ha betydning for hvilke krav til sikkerhetstiltak som vil være relevante for virksomheten – dersom en virksomhet blir vurdert å være nødvendig for å sikre våre grunnleggende nasjonale funksjoner. Dersom en virksomhet ikke har råderett over objekter eller infrastruktur av kritisk betydning for grunnleggende nasjonale funksjoner, men utelukkende har behov for å behandle sikkerhetsgradert informasjon i et begrenset omfang, vil det kun være de deler av loven som gjelder håndtering av slik informasjon som vil være relevante. Det vil være informasjons-

sikkerhet, informasjonssystemsikkerhet og personellsikkerhet i tillegg til de generelle krav til forebyggende sikkerhet.

Utvalget mener imidlertid at det for den enkelte virksomhet også vil være en rekke fordeler forbundet med å bli omfattet av den nye loven. At en virksomhet underlegges loven, vil innebære at denne blir satt i stand til å håndtere sikkerhetsgradert informasjon, herunder detaljert trusselinformasjon fra myndighetene. Økt kunnskap om, og forståelse for det til enhver tid gjeldende trusselbildet, vil sette den enkelte virksomhet bedre i stand til å kunne gjøre gode vurderinger og iverksette de riktige sikkerhetstiltakene, både ut fra et bedriftsøkonomisk og samfunnsøkonomisk perspektiv. I tillegg til generell informasjon om trusselbildet, vil virksomheter underlagt loven kunne få konkrete råd og veiledning fra sikkerhetsmyndighetene om hvordan det forebyggende sikkerhetsarbeidet bør innrettes for å få størst mulig effekt.

For sikkerhetsmyndighetene vil konsekvensene ved at flere virksomheter underlegges loven, kunne medføre økt ressursbruk blant annet knyttet til rådgivning, oppfølging og kontroll med virksomhetene. På den andre siden vil informasjonstilfanget knyttet til uønskede hendelser kunne øke, noe som igjen vil sette sikkerhetsmyndighetene i bedre stand til å forstå trusselbildet og iverksette nødvendige tiltak for å forebygge at slike hendelser skjer. Gode mekanismer for informasjonsdeling, eksempelvis gjennom hendelsesrapportering, vil også gjøre at myndighetene får bedre oversikt over sikkerhetsrelevante hendelser slik at informasjon om dette kan deles med andre utsatte aktører.

For samfunnet vil konsekvensene være positive ut fra et sikkerhetsmessig perspektiv. Økt sikkerhetsnivå i virksomheter som har en sentral rolle i understøttelsen av grunnleggende nasjonale funksjoner, vil gjøre samfunnet som helhet mer robust mot tilsiktede uønskede hendelser. Spesielt i en potensiell nasjonal krise, vil et generelt høyere sikkerhetsnivå ha stor betydning for nasjonens evne til å håndtere krisen.

Samlet sett vurderer utvalget at de positive virkningene for samfunnet ved økt sikkerhet for nasjonen ved en utvidelse av virkeområdet, vil overstige summen av kostnadsvirkningene for samfunnet. Utvalgets foreslår derfor å utvide lovens virkeområde til beskyttelse av *grunnleggende nasjonale funksjoner*. Forslaget innebærer, slik utvalget ser det, en begrenset men nødvendig utvidelse av virkeområdet sett hen til gjeldende sikkerhetslov. Loven vil ikke være en bred samfunnssikkerhetslov, men skal samtidig heller ikke være en ren statssikkerhetslov. I likhet med ny straffelov kapittel 17 og endringene i utlendingsloven, er utvidelsen av lovens virkeområde ment å reflektere den generelle samfunnsutviklingen som har funnet sted siden ikrafttredelsen av gjeldende sikkerhetslov.

6.7.2 Grunnleggende nasjonale funksjoner

Utgangspunktet for å beslutte hva som utgjør *grunnleggende nasjonale funksjoner*, er statens ansvar for å ivareta Norges suverenitet, territorielle integritet og demokratiske styreform. Disse grunnleggende interessene er igjen avhengige av at visse funksjoner kan opprettholdes i hele krisespekteret. En funksjon er å anse som grunnleggende for Norge dersom bortfall av denne får konsekvenser som truer de overordnede interessene.

Utvalget har valgt å kategorisere de overordnede interessene som de *grunnleggende nasjonale funksjoner* skal ivareta i fem underkategorier. De tre første underkategoriene er identiske med oppregningen av de tre første grunnleggende nasjonale interesser i straffeloven § 121 (bokstav a-c). Praksis vedrørende forståelsen av de aktuelle interessene i straffeloven, vil således også ha betydning som tolkningsfaktor for de motsvarende interessene i den nye sikkerhetsloven.

De øverste statsorganers virksomhet, sikkerhet eller handlefrihet. Med øverste statsorganer menes i første rekke regjeringen, Stortinget og Høyesterett. Også de enkelte departementene, særlig i kraft av rollen som regjeringens sekretariater, vil inngå i de øverste statsorganenes virksomhet. At de øverste statsorganene kan opprettholde sin virksomhet er helt avgjørende for å kunne ivareta Norges interesser, både nasjonalt og i en sikkerhetspolitisk kontekst.

Forsvars-, sikkerhets- og beredskapsmessige forhold utgjør blant annet det som tradisjonelt er omtalt som beskyttelsen av rikets sikkerhet overfor en annen stat eller statssikkerhet i snever forstand. Forsvarets operative evne er i siste instans helt avgjørende for opprettholdelse av Norges eksistens, suverenitet og integritet.

Krisehåndtering og beredskap vil også naturlig falle inn under denne kategorien. I tråd med ansvars- og nærhetsprinsippene skal kriser organisatorisk håndteres av den organisasjon som har ansvar i en normalsituasjon og på lavest mulige nivå. Samtidig vil det for kriser av større omfang være behov for en sentralisert koordinering og styring av kriseressursene.

Under sikkerhetsmessige forhold inngår blant annet etterretnings- og sikkerhetstjenestenes virksomhet, det vil si virksomheten til blant annet PST, Etterretningstjenesten og NSM.

Med *forholdet til andre stater* menes for det første nasjonens evne til overholdelse av bi- og multilaterale forpliktelser overfor allierte eller andre samarbeidspartnere. Et innlysende eksempel i denne forbindelse er Norges forpliktelser i NATO. Også Norges evne til å overholde sin forpliktelse til å gi ambassader og residenser den beskyttelsen Wien-konvensjonen 18. april 1964 om diplomatisk samkvem krever, vil ha betydning for forholdet til andre stater.

Forholdet til andre stater kan også skades dersom innsatsfaktorer som er helt nødvendige for en annens stats opprettholdelse av sine grunnleggende funksjoner, rammes. Et eksempel på slike innsatsfaktorer kan være norske gassleveranser til Europa. Dersom disse leveransene kuttes eller sterkt reduseres, vil dette i en gitt situasjon og eventuelt sammenholdt med andre hendelser, kunne ha stor innvirkning på den aktuelle nasjonens opprettholdelse av sine grunnleggende funksjoner. En slik hendelse vil også kunne skade forholdet mellom Norge og den berørte nasjonen.

Landets økonomiske trygghet og velferd er slik utvalget ser det en grunnleggende forutsetning for Norges evne til å ivareta egen sikkerhet. Et anslag som rammer virksomheter som har en helt sentral rolle for ivaretakelsen av landets økonomiske trygghet og velferd, vil ikke bare ha stor symbolverdi. Det vil i ytterste konsekvens kunne ha en vesentlig negativ innvirkning på nasjonens evne til å opprettholde økonomisk trygghet og velferd.

Norsk petroleumsvirksomhet er av sentral betydning for landets økonomiske trygghet og velferd. Norges petroleumsforvaltning skal skape størst mulige verdier for samfunnet, og inntektene skal komme staten og dermed hele samfunnet til gode. I 2015 sto petroleumssektoren for 15 prosent av Norges bruttonasjonalprodukt og for omtrent 20 prosent av statens totale inntekter. I tillegg sto petroleumssektoren for 39 prosent av norsk eksport. Hvorvidt virksomheter i petroleumssektoren er av en slik betydning at de bør underlegges loven, vil måtte avgjøres konkret i tråd med den systematikken utvalget anbefaler i kapittel 7.7.1.

Et annet eksempel på funksjoner av sentral betydning for økonomisk trygghet og velferd kan være sentralbankvirksomheten. Norges Bank utfører viktige samfunnsoppgaver og forvalter store verdier på vegne av fellesskapet. Gjennom sentralbankvirksomheten skal Norges Bank fremme stabilitet i den norske økonomien. Norges Bank opplyser også selv om at deres oppgjørssystem (NBO) skal sikres i henhold til kravene for samfunnskritisk infrastruktur. Andre aktører som kan tenkes å ha en slik betydning, kan være en del av de større bankenes betalingssystemer for eksempel.

Et av siktemålene med kategorien *befolkningens grunnleggende sikkerhet og overlevelse,* er å fange opp beskyttelse mot terrorhandlinger av et visst omfang eller med en viss målrettethet, som vil innebære en trussel mot grunnleggende nasjonale funksjoner og således også nasjonens mest grunnleggende interesser, uavhengig av om terrorhandlingen er rettet mot et objekt eller en infrastruktur som er omfattet av loven eller ikke. Ethvert enkeltstående terrorangrep vil ikke nødvendigvis være å anse som et angrep av en slik karakter. Det vil være en glidende, og i mange sammenhenger uklar grense mellom terrorhandlinger og annen alvorlig kriminalitet.

Loven gjelder ikke dermed for enhver virksomhet som disponerer eiendom eller annet som kan bli gjenstand for terrorhandlinger. Det loven imidlertid vil bidra til er offentlige myndigheters virksomhet for å motvirke sannsynligheten for, og konsekvensene av, terrorhandlinger i samfunnet. Blant annet bør myndigheters arbeid mot terror i enkelte tilfeller omfattes av reglene om informasjonssikkerhet, selv om myndigheten ikke på annen måte forvalter virksomhet som er av kritisk betydning for grunnleggende nasjonale funksjoner. I utgangspunktet innebærer dette at loven vil gjelde for alle forvaltningsorganer som oppfyller vilkårene i § 1-2.

Av dette alternativet omfattes også virksomheter som forvalter objekter eller infrastruktur som må anses som særlig utsatte for terrorhandlinger. Et eksempel her kan være sentrale knutepunkter for lufttrafikken eller for styringen av denne.

For å sikre befolkningens grunnleggende behov for overlevelse vil de regionale helseforetakene, gjennom sitt ansvar for å sikre spesialisthelsetjenester til regionens befolkning, ha en helt avgjørende betydning i en krisesituasjon. Norsk Helsenett vil i denne forbindelse også være av stor betydning.

Enkelte sentrale vannverk vil etter omstendighetene kunne være av en slik betydning for befolkningens sikkerhet og overlevelse at de bør pålegges særlige krav til sikkerhetstiltak etter loven.

Loven skal være sektorovergripende og vil således gjelde for virksomheter i alle samfunns-

sektorer som oppfyller vilkårene i loven. Gjensidige avhengigheter på tvers av sektorer innebærer også at en virksomhet i en samfunnssektor kan bli ansett for å være av en slik betydning for en grunnleggende nasjonal funksjon i en annen samfunnssektor, at virksomheten må omfattes av loven.

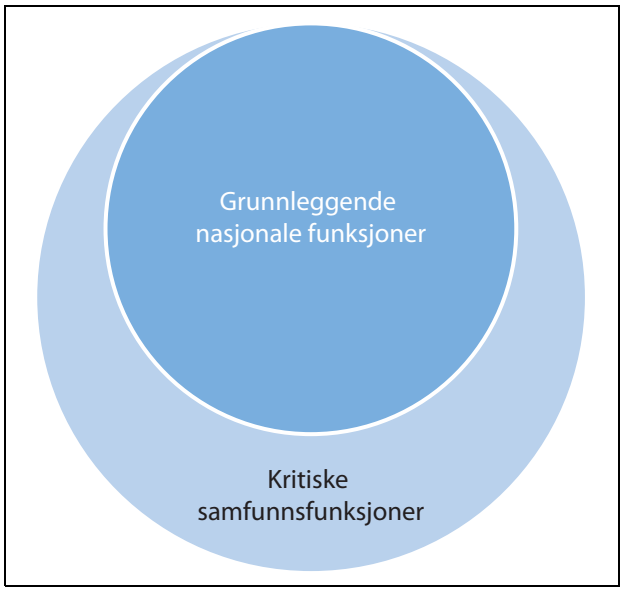
Hvilke samfunnsfunksjoner som vil være å anse som *grunnleggende nasjonale funksjoner,* vil slik utvalget ser det, kunne endres i takt med den generelle samfunnsutviklingen. Selv om ordlyden i det nye lovforslaget ikke er identisk med ny straffelov kapittel 17 og utlendingsloven, vil rettspraksis vedrørende forståelsen av begrepet *grunnleggende nasjonale interesser* også ha en viss betydning for hvordan *grunnleggende nasjonale funksjoner* skal forstås og praktiseres.

Den nærmere avgrensningen av hva som vil utgjøre *grunnleggende nasjonale funksjoner* i medhold av den nye sikkerhetsloven, vil slik utvalget ser det måtte avgjøres konkret basert på en helhetlig vurdering der både de sektorovergripende og sektorspesifikke perspektivene ivaretas. For at loven skal få den ønskede effekt vil det være avgjørende at det etableres et system for å kunne identifisere grunnleggende nasjonale funksjoner og hvilke virksomheter som er av kritisk betydning for disse. Etter utvalgets syn er det en svakhet ved dagens regelverk at det ikke gis nærmere føringer for en slik systematikk. Utvalgets forslag til systematikk er nærmere beskrevet i kapittel 7.7.1.

6.7.3 Relasjonen mellom grunnleggende nasjonale funksjoner og kritiske samfunnsfunksjoner

DSB har også en funksjonsbasert tilnærming til sitt arbeid med samfunnssikkerhet og beredskap, og benytter i denne sammenheng begrepsapparatet *kritiske samfunnsfunksjoner*. DSB har i medhold av KIKS-metodikken identifisert 18 kritiske samfunnsfunksjoner.[47] Denne metodikken bygger på en overordnet samfunnsmessig vurdering av hvordan bortfall av en samfunnsfunksjon vil påvirke befolkningens sikkerhet – uavhengig av hvordan dette bortfallet skjer (*all-hazards*). Metodikken tar også høyde for funksjoner med regional og lokal betydning.

I motsetning til KIKS-metodikken, fokuserer utvalgets forslag til ny lov utelukkende på de funksjoner og verdier som er av nasjonal betydning, og



Figur 6.2 Relasjonen mellom kritiske samfunnsfunksjoner og grunnleggende nasjonale funksjoner.

tar således ikke sikte på å beskytte funksjoner som kun har regional eller lokal betydning. Det vil imidlertid kunne tenkes hendelser av regional eller lokal karakter, som på grunn av sin alvorlighetsgrad eller konsekvenser for sentrale samfunnsinstitusjoner, vil måtte anses å være av nasjonal betydning. I tillegg er utvalgets lovforslag avgrenset til beskyttelse av funksjonene mot tilsiktede uønskede hendelser.

En rekke av de samfunnsfunksjonene som identifiseres som kritiske i henhold til KIKS-metodikken, vil imidlertid også være å anse som *grunnleggende nasjonale funksjoner* i en ny sikkerhetslov. Samtidig vil det også være funksjoner som er identifisert som kritiske i henhold til DSBs terminologi, som ikke vil anses som grunnleggende nasjonale funksjoner etter den nye loven.

Grunnleggende nasjonale funksjoner kan således ses på som en delmengde av kritiske samfunnsfunksjoner i henhold til KIKS-metodikken:

Hvilke konkrete funksjoner som vil være å anse som grunnleggende nasjonale funksjoner, vil som nevnt tidligere måtte vurderes konkret avhengig av både hvilke verdier som legges til grunn for vurderingen og hvilke kriterier som legges til grunn for kritikalitet.

Eksempelvis vil samfunnsfunksjonen *Overvåkning av naturfarer* være en funksjon som faller utenfor sikkerhetsloven, fordi den utelukkende er innrettet mot uønskede utilsiktede hendelser. Et annet eksempel kan være samfunnsfunksjonen *Vern av kulturelle verdier,* som er definert som kri-

[47] DSB, *Samfunnets kritiske funksjoner. Hvilken funksjonsevne må samfunnet opprettholde til enhver tid?,* 2015.

tisk av DSB. Dette vil ikke være å anse som en grunnleggende nasjonal funksjon etter den nye sikkerhetsloven.

6.7.4 Tilsiktede uønskede hendelser og utilsiktede uønskede hendelser

Utvalget har vurdert hvorvidt den nye loven bør ha som siktemål å beskytte mot alle typer trusler, både tilsiktede og utilsiktede (en såkalt *all hazards*-tilnærming), eller om den burde avgrenses til de tilsiktede uønskede hendelsene. En rekke aktører utvalget har hørt gjennom sitt arbeid, har tatt til orde for en *all hazards*-tilnærming. En fordel med en slik tilnærming er at det vil kunne gi en mer helhetlig tilnærming til forebyggende sikkerhet, uavhengig av om risikoen knytter seg til en tilsiktet eller utilsiktet hendelse. En slik tilnærming vil også kunne redusere risikoen for målkonflikt, hvor krav til sikkerhetstiltak for å forebygge tilsiktede hendelser potensielt vil være i konflikt med krav til sikkerhetstiltak for utilsiktede hendelser.

Når utvalget likevel har kommet til at lovens virkeområde bør avgrenses til beskyttelse mot *tilsiktede uønskede hendelser* skyldes dette flere forhold. For det første vil risikovurderinger og sikkerhetstiltak, slik utvalget ser det, kunne være annerledes for henholdsvis tilsiktede og utilsiktede hendelser. Eksempelvis vil en tenkende trusselaktør kunne tilpasse seg etablerte sikkerhetstiltak ved valg av metode for å forsøke og utnytte sårbarheter. Dette stiller andre krav til hvordan man innretter de aktuelle sikkerhetstiltakene. For det andre vil en *all hazards*-tilnærming for en ny lov innebære en dobbeltregulering av beskyttelse mot utilsiktede hendelser, som sannsynligvis vil kunne medføre behov for justeringer i annet regelverk. Et tredje forhold er at utvalgets mandat fra oppdragsgiver er klart avgrenset til å foreslå et nytt lovgrunnlag for å beskytte mot tilsiktede uønskede hendelser.

I tråd med arbeidsgruppen som evaluerte sikkerhetsloven, ser utvalget ingen grunn til å avgrense loven til utelukkende beskyttelse mot såkalt *sikkerhetstruende virksomhet* (terrorhandlinger, spionasje og sabotasje), slik som dagens sikkerhetslov gjør. Det tas sikte på beskyttelse mot de tilsiktede uønskede hendelsene som kan utgjøre en trussel mot grunnleggende nasjonale funksjoner. Denne avgrensningen vil i seg selv være styrende for hvilke typer tilsiktede hendelser som er aktuelle. Terrorhandlinger, ulovlig etterretningsvirksomhet og sabotasje, vil være de mest aktuelle formene for tilsiktede uønskede hendelser. Men det kan også tenkes andre former for tilsiktede uønskede hendelser, herunder enkelte typer organisert kriminalitet, som vil kunne være så alvorlige at de rammer *grunnleggende nasjonale funksjoner*.

Selv om utvalget ikke foreslår en *all hazards*-tilnærming i den nye loven, vil utvalget presisere viktigheten av at virksomhetene har en helhetlig tilnærming til hvordan risiko skal håndteres når det kommer til operasjonaliseringene av de krav som stilles til virksomhetene, både etter en ny sikkerhetslov og etter øvrig regelverk som er relevant for den enkelte virksomhet.

6.7.5 Hvilke virksomheter vil omfattes av den nye loven

Utvidelsen av lovens virkeområde, vil få betydning for hvilke virksomheter som omfattes av den nye loven. Utvalget legger til grunn at de virksomheter som allerede i dag er omfattet av sikkerhetsloven, enten i kraft av å være forvaltningsorgan eller ved enkeltvedtak i medhold av gjeldende lov, også vil være omfattet av den nye loven.

Som nevnt under kapittel 6.7.1 foreslår utvalget at lovens virkeområde innrettes slik at enhver virksomhet, offentlig eller privat, som har *råderett over informasjon, informasjonssystemer, objekter eller infrastruktur, eller som driver aktivitet, som er av kritisk betydning for grunnleggende nasjonale funksjoner*, omfattes av loven.

En kartlegging og identifisering av hvilke funksjoner som er grunnleggende i et nasjonalt perspektiv, er avgjørende for å kunne identifisere hvilke virksomheter som har en sentral rolle i understøttelsen av disse funksjonene. Slik understøttelse kan i praksis skje på flere måter.

Det kan for det første knytte seg til informasjon og informasjonssystemer, hvor det kan ha alvorlige skadefølger for de grunnleggende funksjonene dersom informasjonen blir kjent for uvedkommende. Videre kan understøttelsen knytte seg til objekter eller infrastruktur, hvor opprettholdelse av funksjonalitet vil være av kritisk betydning for grunnleggende nasjonale funksjoner. Det kan også være annen aktivitet, som verken knytter seg til konkret informasjon eller konkrete objekter eller infrastruktur.

Virksomheter som tilvirker, eller har behov for tilgang til, gradert informasjon, må etter utvalgets oppfatning omfattes av den nye loven. Utvalget har gjennom sitt arbeid fått inntrykk av at samhandlingen mellom myndigheter som PST, NSM og Etterretningstjenesten og det private næringsliv, er utfordrende med dagens regelverk. Etter-

spørselen etter graderte og detaljerte trusselvurderinger er stor blant private aktører som forvalter infrastruktur og objekter, eller på annen måte driver aktivitet av kritisk betydning for grunnleggende nasjonale funksjoner. All den tid disse virksomhetene ikke er underlagt krav til hvordan slik informasjon skal håndteres, vil imidlertid ikke myndighetene kunne dele slik informasjon uten å samtidig bryte dagens sikkerhetslov. Det stilles eksempelvis store forventninger til at PST skal dele informasjon i forbindelse med sitt forebyggende sikkerhetsarbeid. PST har overfor utvalget fremholdt at det kan være nødvendig å dele gradert informasjon for å sikre at disse selskapene iverksetter nødvendige forebyggende tiltak eller får forståelse for den risikoen de er utsatt for.

Utvalget mener videre at virksomheter som eier eller forvalter infrastruktur eller objekter av kritisk betydning for de grunnleggende nasjonale funksjonene, må omfattes av en ny sikkerhetslov. Hvilke objekter eller infrastruktur som har en slik betydning vil måtte avgjøres konkret. Utvalgets forslag til systematikk for identifisering og utvelgelse av objekter og infrastruktur av kritisk betydning er nærmere omtalt i kapittel 9.

Utvalget mener videre at virksomheter som har en rolle i Nasjonal beredskapssystem (NBS), enten i Sivilt beredskapssystem (SBS) eller Beredskapssystemet for Forsvaret (BFF), bør vurderes underlagt en ny sikkerhetslov. NBS er i seg selv sikkerhetsgradert, og det er en svakhet ved dagens system at ikke alle aktører som har en rolle i NBS, kan håndtere gradert informasjon. Det er heller ikke etablert kommunikasjonslinjer med alle relevante aktører i beredskapskjeden hvor gradert informasjon kan kommuniseres. Dette vanskeliggjør beredskapsarbeidet og medfører risiko for at sentrale aktører ikke sitter med et korrekt eller fullstendig situasjonsbilde i en krisesituasjon.

Forsvaret er avhengig av sivil understøttelse for å kunne utføre sine oppgaver. Den sivile støtten til Forsvaret er i dag i hovedsak basert på kommersielle ordninger og samarbeid med sivil sektor gjennom leveranse- og beredskapsavtaler. Ved omfattende eller langvarige sikkerhetspolitiske kriser vil det kunne være aktuelt å anvende beredskapslovgivningen for å sikre nødvendig støtte til Forsvaret. En effektiv understøttelse av Forsvaret forutsetter, slik utvalget ser det, at de aktører som har en sentral rolle i dette også har innsikt i Forsvarets behov i gitte scenarioer. Dette vil ofte være sikkerhetsgradert informasjon, hvor informasjonsdeling forutsetter at aktørene er satt i stand til å forvalte denne informasjonen på en forsvarlig måte, etter fastsatte krav. Utvalget mener, som et generelt utgangspunkt, at det bør vurderes om aktører med en sentral rolle i Totalforsvaret, gjennom sin understøttelse av Forsvarets virksomhet, skal underlegges den nye loven. Dette vil både lette samhandlingen mellom Forsvaret og sivile aktører, og gi myndighetene mulighet til å stille sikkerhetsmessige krav overfor disse virksomhetene ut over rent kontraktuelle forpliktelser.

Forsvaret skal i henhold til Instruks om sikring og beskyttelse av objekter, beslutte hvilke sivile og militære objekter som skal utpekes som nøkkelpunkter, og hvilke av disse det skal forberedes objektsikring av. I vurderingen av sivile objekter skal Forsvaret rådføre seg og på annen måte samarbeide med berørte sivile myndigheter, herunder politiet, fylkesmennene, NSM og DSB. Med «nøkkelpunkter» menes i denne sammenheng sivile og militære objekter (og personer) som er av avgjørende betydning for forsvarsevnen og det militære forsvar i krig, og som er å anse som lovlige militære mål i krig. Forsvarets ansvar for nøkkelpunkter bygger på et selvstendig hjemmelsgrunnlag, og er i utgangspunktet uavhengig av objektsikkerhetsregelverket i dagens sikkerhetslov. Utvalget mener imidlertid at virksomheter som har bestemmelsesrett over sivile objekter som er utpekt som nøkkelpunkter av Forsvaret, bør omfattes av den nye loven.

Den nærmere avgrensningen av hvilke virksomheter som vil omfattes av den nye loven, vil måtte avgjøres konkret. På samme måte som for identifisering av grunnleggende nasjonale funksjoner vil det være avgjørende at det etableres et system for å kunne identifisere slike virksomheter. Utvalgets forslag til systematikk er nærmere beskrevet i kapittel 7.7.1.

6.7.6 Kompensatoriske ordninger

I enkelte tilfeller vil det ut fra samfunnsøkonomiske betraktninger kunne være behov for å pålegge omfattende sikkerhetstiltak for en spesifikk virksomhet eller innenfor en hel samfunnssektor. Et eksempel kan være en konkret virksomhet som er av helt avgjørende betydning for en eller flere grunnleggende nasjonale funksjoner. Dersom slike pålegg medfører uforholdsmessig stor belastning for den aktuelle virksomhet eller sektor sett i forhold til den egenverdi tiltakene har for virksomheten/sektoren, kan det være behov for å vurdere kompensatoriske tiltak.

Som nevnt i kapittel 4.5, har staten et bredt spekter av virkemidler som kan benyttes for å

oppnå god nasjonal sikkerhet, hvor også økonomiske insentiver inngår. Utvalget ser det ikke som formålstjenlig å spesifisere eventuelle kompensatoriske tiltak i loven. Hvis slike pålegg skulle bli nødvendig, mener utvalget at dette så langt som mulig bør søkes løst gjennom tett dialog mellom sikkerhetsmyndighetene, aktuelle sektormyndigheter og berørte virksomheter. Bruk av økonomiske insentiver, eller andre kompensatoriske tiltak, kan da tenkes å være aktuelle virkemidler for å avbøte en uforholdsmessig stor økonomisk belastning for den enkelte virksomhet.

Kapittel 7
Ansvar for og utøvelse av forebyggende sikkerhet, samt tilsynsfunksjon

7.1 Innledning

Når det gjelder ansvar og myndighet etter loven er utvalget gitt følgende mandat:

> Utvalget skal videre foreta en vurdering av hvorvidt myndighetenes (herunder NSMs) oppgaver og ansvar skal reguleres i lovgrunnlaget/lovgrunnlagene, og på hvilken måte dette eventuelt skal gjøres.

En sentral utfordring med praktiseringen av dagens sikkerhetslov har vært operasjonaliseringen av forholdet mellom ansvars- og samordningsprinsippet, som er styrende prinsipper for arbeidet med forebyggende sikkerhet og beredskap.

En annen utfordring er knyttet til mangelfull formalisering og/eller praktisering av samhandlingen mellom tilsynsregimet etter sikkerhetsloven og de ulike tilsynsregimene etter annet relevant sektorregelverk.

Utvalgets målsetting med reguleringen av ansvars-, myndighets- og tilsynsansvar etter loven er å legge til rette for en god samhandling mellom de sentrale aktørene i forebyggende sikkerhet, på tvers av samfunnssektorene. En slik samhandling er helt avgjørende for at det forebyggende sikkerhetsarbeidet i Norge skal få full effekt, slik utvalget ser det.

En annen målsetting har vært å lage et helhetlig og robust regelverk for forebyggende sikkerhet, hvor hensynet til kostnadseffektive løsninger står sentralt. Fra myndighetenes side er det nødvendig å sikre at virksomheter av kritisk betydning for grunnleggende nasjonale funksjoner, har et forsvarlig sikkerhetsnivå. Hvordan et slikt sikkerhetsnivå oppnås, vil imidlertid kunne variere mellom de ulike virksomhetene og sektorene.

En av de mest sentrale problemstillinger som en regulering skal omfatte, er ansvarsfordelingen mellom ulike aktører. Mange av de sentrale aktørene i forebyggende nasjonal sikkerhet er omtalt i kapittel 3. Det er viktig å tydeliggjøre hvilke plikter og rettigheter som følger ulike myndigheter, ulike statlige virksomheter og private aktører. I forbindelse med regulering av forebyggende sikkerhet for grunnleggende nasjonale funksjoner, vil graden av sektorautonomi sett opp mot behovet for en helhetlig nasjonal sikkerhetsstyring stå sentralt.

En grunnleggende problemstilling i denne sammenheng er fordelingen av ansvar og myndighet for å identifisere grunnleggende nasjonale funksjoner, og for å utpeke virksomheter som er av kritisk betydning for slike funksjoner. Det er også et spørsmål om det bør etableres mekanismer for å kunne overprøve de vedtak som ulike myndigheter fatter.

En annen grunnleggende problemstilling er hvordan tilsynsfunksjonen etter loven bør innrettes for å både kunne ivareta den enkelte samfunnssektors særegne behov og samtidig ivareta behovet for en helhetlig og sektorovergripende tilnærming til forebyggende sikkerhet. I relasjon til denne problemstillinger er også spørsmål om hvilke myndighetsaktører som bør kunne stille krav til, og komme med pålegg overfor, virksomheter underlagt loven. Skal noen, og i så fall hvem, ha myndighet til å påpeke behov for endringer i sikkerhetsnivå, og hvordan skal tiltak på tvers av samfunnssektorer og virksomheter koordineres slik at tiltak blir iverksatt der det er mest samfunnsøkonomisk lønnsomt.

En forutsetning for en tilfredsstillende gjennomføring av forebyggende sikkerhet for å sikre grunnleggende nasjonale funksjoner, er at det etableres et system hvor roller, ansvar og plikter er avklart og tilstrekkelig definert.

7.2 Gjeldende sikkerhetslovs regulering

7.2.1 Overordnet ansvar for forebyggende sikkerhet

Ansvarsforholdene etter sikkerhetsloven er regulert i §§ 4 og 5.

Det følger av loven § 4 at *departementet* har det overordnede ansvaret for forebyggende sikkerhetstjeneste. I Kronprinsregentens resolusjon av 4. juli 2003 fordeles det overordnede ansvaret for forebyggende sikkerhetstjeneste mellom Justis- og beredskapsdepartementet og Forsvarsdepartementet. Justis- og beredskapsministeren har et overordet ansvar i sivil sektor, mens forsvarsministeren har det overordnede ansvaret i militær sektor. Nasjonal sikkerhetsmyndighet (NSM) skal i henhold til samme resolusjon ivareta de utøvende funksjonene på vegne av henholdsvis justis- og beredskapsministeren og forsvarsministeren.

7.2.2 Den enkelte virksomhets plikter

Det følger videre av loven § 5 at enhver virksomhet plikter å utøve forebyggende sikkerhetstjeneste i henhold til bestemmelsene gitt i, eller i medhold av loven. Med virksomhet menes i sikkerhetslovens forstand et forvaltningsorgan eller annet rettssubjekt som loven gjelder for, jf. sikkerhetsloven § 3 første ledd nr. 6.

Virksomheten plikter å utarbeide en intern instruks for å ivareta sikkerheten, sørge for at virksomhetens ansatte og engasjerte får tilstrekkelig opplæring i sikkerhetsspørsmål, samt regelmessig kontrollere sikkerhetstilstanden i virksomheten, jf. § 5 andre ledd bokstav a-c.

Ansvaret for utøvelse av forebyggende sikkerhetstjeneste i den enkelte virksomhet er et lederansvar, jf. § 5 tredje ledd. Virksomhetens leder kan etter samme bestemmelse delegere utøvende funksjoner internt i virksomheten. Dersom dette gjøres, skal det dokumenteres skriftlig.

Det følger videre av fjerde ledd at det påhviler en plikt for enhver ansatt eller engasjert personell til å ivareta sikkerhetsmessige hensyn, og til å bidra til forebyggende sikkerhetstjeneste gjennom sitt arbeid eller oppdrag for virksomheten.

Sikkerhetsadministrasjon er den administrative og organisatoriske styring som ligger til grunn for forebyggende sikkerhetstjeneste, og er regulert i gjeldende sikkerhetslov § 5 om den enkelte virksomhets plikter. I tillegg er det gitt utfyllende bestemmelser om sikkerhetsadministrasjon i sikkerhetsadministrasjonsforskriften.[1]

I forskriften § 1-2 nr. 1 er sikkerhetsadministrasjon definert som «internkontroll ved gjennomføring av systematiske tiltak for å sikre at virksomhetens aktiviteter planlegges, organiseres, utføres og revideres i samsvar med krav fastsatt i og i medhold av sikkerhetsloven». Forskriften gir nærmere bestemmelser om blant annet ansvar og organisering av forebyggende sikkerhetstjeneste, risikohåndtering og sikkerhetsrevisjon, samt reaksjon ved sikkerhetstruende hendelser.

7.2.3 Vedtaksmyndighet for Kongen i statsråd og varslingsplikt

Regjeringen har i Prop. 97 L (2015–2016) Endringer i sikkerhetsloven, foreslått en ny bestemmelse §5a, om varslingsplikt og vedtaksmyndighet for Kongen i statsråd. Bestemmelsen pålegger virksomheter underlagt sikkerhetsloven en varslingsplikt til departementet ved kunnskap om risiko for at sikkerhetstruende virksomhet blir etablert eller gjennomført. Bestemmelsen gir også Kongen i statsråd myndighet til å fatte vedtak for å hindre at slik virksomhet blir etablert eller gjennomført – uten hensyn til begrensningene i forvaltningsloven § 35 – og uavhengig av om aktiviteten er tillatt etter annen lov eller annet vedtak.

Formålet med bestemmelsen er ifølge forarbeidene, å etablere en hjemmel i loven for å kunne forebygge mer frittstående høyteknologisk virksomhet som kan innebære en fare for rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser, som ikke spesifikt er knyttet til sikkerhetsgradert informasjon eller skjermingsverdige objekter.

Bestemmelsen lyder:

> **§ 5 a Varslingsplikt og myndighet til å fatte vedtak ved risiko for sikkerhetstruende virksomhet**
>
> En virksomhet som får kunnskap om en planlagt eller pågående aktivitet som kan medføre en ikke ubetydelig risiko for at sikkerhetstruende virksomhet blir etablert eller gjennomført, skal varsle overordnet departement om dette. Dersom den varslingspliktige virksomheten ikke er underlagt noe departement, skal varselet gis til Forsvarsdepartementet. Varslingsplikten gjelder uten hinder av lovbestemt taushetsplikt. Ved behandling av varsel etter første og andre punktum bør det innhentes råd-

[1] Forskrift 29. juni 2001 nr. 723 om sikkerhetsadministrasjon (sikkerhetsadministrasjonsforskriften).

givende uttalelser fra relevante organer med kompetanse innenfor det aktuelle fagområdet.

Kongen i statsråd kan fatte nødvendige vedtak for å hindre en planlagt eller pågående aktivitet som nevnt i første ledd første punktum. Et slikt vedtak kan fattes uten hensyn til begrensningene i forvaltningsloven § 35, og uavhengig av om aktiviteten er tillatt etter annen lov eller annet vedtak. Vedtak etter første punktum er særlig tvangsgrunnlag etter tvangsfullbyrdelsesloven kapittel 13.

Kongen i statsråd kan gi forskrift om varslingsplikten i første ledd og om hvilke vedtak som kan fattes etter andre ledd.

I de særlige merknadene til vedtaksmyndigheten i bestemmelsens annet ledd skriver departementet:

> Andre ledd første punktum gir en hjemmel for Kongen i statsråd til å fatte nødvendige vedtak for å hindre en planlagt eller pågående aktivitet som nevnt i første ledd første punktum. At vedtaket skal være «nødvendig» innebærer at Kongen i statsråd ikke skal fatte mer byrdefulle vedtak enn det som er påkrevd, og som vurderes som rimelig i den konkrete saken. Bestemmelsen vil være en sikkerhetsventil, og den forutsettes benyttet kun i helt spesielle tilfeller. Kompetansen til å fatte vedtak er lagt til Kongen i statsråd, og den kan ikke delegeres. Departementet legger til grunn at det vil være tale om et lite antall saker, og at disse sakene etter sin art vil være alvorlige og spesielle, jf. også formålet med sikkerhetsloven. At kompetansen legges til Kongen i statsråd sikrer at eventuelle tiltak som iverksettes, er resultat av en vurdering på høyt nivå, og at de står i et rimelig forhold til den foreliggende risikoen.
>
> I henhold til andre ledd andre punktum kan vedtak etter første punktum for det første fattes uten hensyn til begrensningene i forvaltningsloven § 35. Bestemmelsen tar høyde for tilfeller der forvaltningen allerede har fattet et vedtak, og det av hensyn til risiko for sikkerhetstruende virksomhet anses nødvendig å omgjøre vedtaket. Videre slås det i bestemmelsen fast at vedtak etter første punktum også kan fattes uten hensyn til om aktiviteten er tillatt etter annen lov eller annet vedtak. Et vedtak av Kongen i statsråd kan derfor i praksis sette til side en rekke ulike former for vedtak og aktiviteter som i utgangspunktet er tillatt, f.eks. nekte gjennomføring eller stille ytterligere vilkår for en byggetillatelse, frekvenstillatelse, ferdselsrett, jaktrett, en våpentillatelse eller et privat oppkjøp av en virksomhet.
>
> I andre ledd tredje punktum er det fastsatt at vedtak etter første punktum er tvangsgrunnlag etter tvangsfullbyrdelsesloven kapittel 13. Dette innebærer at vedtak som fattes av Kongen i statsråd, kan tvangsfullbyrdes av namsmyndighetene, uten at man først må få dom for dette. Slik tvangsfullbyrdelse kan f.eks. gå ut på fravikelse av fast eiendom, ved at personer eller løsøre fjernes fra eiendommen, etter tvangsfullbyrdelsesloven § 13-11, rett for staten til å gjennomføre riving eller fjerning av installasjoner etter tvangsfullbyrdelsesloven § 13-14 første ledd eller pålegg om å stille sikkerhet etter tvangsfullbyrdelsesloven § 13-16 første ledd.[2]

I forarbeidene til lovforslaget har departementet også vurdert hvordan slike vedtak stiller seg med hensyn til Grunnloven §§ 97 og 10, samt den europeiske menneskerettighetskonvensjonens (EMK) tilleggsprotokoll 1 art. 1:

> Departementet har vurdert hvordan forslaget om at Kongen i statsråd skal kunne treffe slike vedtak stiller seg med hensyn til Grunnloven §§ 97 og 105 og EMKs tilleggsprotokoll 1 art. 1. Vurderingen er at forslaget er i overensstemmelse med de krav legalitetsprinsippet og EMKs prinsipp om «rule of law» stiller, og at det heller ikke foreligger noe brudd på forbudet mot tilbakevirkende lover. Selv om selve lovforslaget vurderes å være i overensstemmelse med Grunnloven, menneskerettighetsloven og Norges internasjonale forpliktelser, vil dette måtte vurderes konkret også på det tidspunktet et eventuelt vedtak fattes med hjemmel i bestemmelsen.[3]

Stortinget har, i forbindelse med behandlingen av Innst. 352 L (2015–2016) til Prop. 97 L (2015–2016) om endringer i sikkerhetsloven, vedtatt regjeringens forslag om varslingsplikt og myndighet til å fatte vedtak for Kongen i statsråd.

7.2.4 Utøvelse av forebyggende sikkerhetstjeneste og samarbeid

Et generelt prinsipp for utøvelse av forebyggende sikkerhetstjeneste følger av loven § 6. Ved utøvelse av forebyggende sikkerhetstjeneste skal det

[2] Prop. 97 L (2015–2016), pkt. 13.

[3] Ibid., pkt. 4.4.

ikke nyttes mer inngripende midler og metoder enn det som framstår som nødvendig i forhold til den aktuelle sikkerhetsrisiko og omstendighetene for øvrig. Det skal videre tas særlig hensyn til den enkeltes rettssikkerhet ved utøvelse av forebyggende sikkerhetstjeneste, jf. bestemmelsen andre ledd.

Loven § 7 gir Kongen fullmakt til å fastsette nærmere bestemmelser om nasjonalt, regionalt og lokalt samarbeid om forebyggende sikkerhetstjeneste. I sikkerhetsadministrasjonsforskriften er samordningsplikten regulert nærmere i § 2-6, som blant annet regulerer ansvarsforholdene ved større prosjekter eller anskaffelser som involverer sikkerhetsgradert informasjon, samt ansvarsforholdene der to eller flere virksomheter er tilkoblet et felles informasjonssystem.

7.3 Nasjonal sikkerhetsmyndighet

7.3.1 Historisk tilbakeblikk

Funksjonen Nasjonal sikkerhetsmyndighet[4] tillå forsvarssjefen frem til 1. januar 2003.

I Ot.prp. nr. (1996–97) tok ikke departementet stilling til hvordan forsvarsministerens utøvende sikkerhetsfunksjoner skulle organiseres i fremtiden. Departementet foreslo imidlertid at det fortsatt burde være ett sentralt organ med ansvar for koordinering av de forebyggende sikkerhetstiltakene, herunder forestå veiledning, opplæring og kontroll. Dette organet ble foreslått benevnt Nasjonal sikkerhetsmyndighet. Organisasjonsmodellen den gang innebar at forsvarssjefen var tildelt funksjonen som nasjonal sikkerhetsmyndighet. Fremtidige endringer i organiseringen av denne myndigheten ble forespeilet forelagt for Stortinget på vanlig måte.

I St.meld. nr. 17 (2001–2002) Samfunnssikkerhet – Veien til et mindre sårbart samfunn, uttalte regjeringen at:

> Nasjonal sikkerhetsmyndighet skal ha ansvar for forebyggende sikkerhetstjeneste etter sikkerhetsloven i sivil og militær sektor. Det vil sikre en helhetlig tilnærming til sikkerhetsarbeidet på tvers av militær og sivil sektor, og sikre en effektiv utnyttelse av ressursene innenfor forebyggende sikkerhet. Etter regjeringens oppfatning tilsier imidlertid Nasjonal sikkerhetsmyndighets ansvarsområde, særlig innenfor sivil sektor, at Nasjonal sikkerhetsmyndighet organiseres utenfor Forsvarets militære organisasjon. Det anses i den sammenheng som naturlig og hensiktsmessig at Nasjonal sikkerhetsmyndighet etableres som et direktorat rett under et fagdepartement. Regjeringen går inn for at Nasjonal sikkerhetsmyndighet skal opprettes som et eget direktorat administrativt underlagt Forsvarsdepartementet. Videre legges det opp til at Nasjonal sikkerhetsmyndighet skal rapportere (med faglig ansvarslinje) i militær sektor til Forsvarsdepartementet, og til Justisdepartementet i sivil sektor.[5]

Ved Justis- og forsvarskomiteens behandling av stortingsmeldingen i Innst. S nr. 9 (2002–2003) merket komiteens flertall seg at Forsvarets overkommando/sikkerhetsstaben ble foreslått oppgradert til et eget direktorat. Flertallet påpekte i denne sammenhengen viktigheten av klare kommandolinjer og ansvarsforhold. Komiteens mindretall støttet også opprettelsen av direktoratet, men mente at dette administrativt burde underlegges daværende Justisdepartementet (nå Justis- og beredskapsdepartementet).

I St.prp. nr. 1 (2002–2003) viste regjeringen til forslaget i St.meld. nr. 17 (2001–2002) om at Nasjonal sikkerhetsmyndighet skulle opprettes som eget direktoratet administrativt underlagt Forsvarsdepartementet. Regjeringen foreslo videre at Nasjonal sikkerhetsmyndighet (NSM) skulle opprettes fra 1. januar 2003:

> Stortingsmeldingen ble ikke behandlet i vårsesjonen 2002, men det foreslås likevel at NSM opprettes som et eget direktorat fra 1. januar 2003.
>
> Organiseringen av NSM innebærer at FO/S nedlegges, og at hoveddelen av de ressurser som ligger i FO/S i dag overføres til det nye direktoratet. Forsvarets militære organisasjon må imidlertid beholde en egen sikkerhetskompetanse og kapasitet på sentralt nivå, som skal ivareta sikkerhetstjenesten i Forsvaret. Det opprettes derfor en forsvarssjefens sikkerhetsavdeling (FSA). FSA skal være operativ samtidig med opprettelsen av det nye direktoratet.[6]

Under komiteens behandling av St.prp. nr. 1 hadde komiteen ingen merknader til dette forslaget.[7]

---

[4] For en nærmere begrepsavklaring, se kapittel 7.7.3, tekstboks 7.3.

[5] St.meld. nr. 17 (2001–2002), Samfunnssikkerhet, 103.

[6] St.prp. nr. 1 (2002–2003), Forsvarsdepartementet, pkt. 3.12.

Fordelingen av ansvaret for Nasjonal sikkerhetsmyndighet ble fulgt opp av regjeringen i Kronprinsregentens resolusjon av 4. juli 2003[8], hvor NSM ble tillagt ansvaret for å ivareta de utøvende funksjoner for den forebyggende sikkerhetstjenesten på vegne av justisministeren og forsvarsministeren.

7.3.2 Direktoratet Nasjonal sikkerhetsmyndighets ansvar og myndighet

Direktoratet NSM har en relativt bred oppgaveportefølje, og sjef NSM rapporterer til både Forsvarsdepartementet og Justis- og beredskapsdepartementet. Direktoratets kjerneoppgaver er som beskrevet ovenfor å ivareta funksjonen Nasjonal sikkerhetsmyndighet slik det fremkommer av sikkerhetsloven kapittel 3. Disse og NSMs øvrige oppgaver er nedfelt i Forsvarsdepartementets Instruks for sjef nasjonal sikkerhetsmyndighet. Den løpende etatsstyringen av NSM skjer gjennom de årlige iverksettingsbrevene (IVB) fra Forsvarsdepartementet til NSM og etatsstyringsmøter mellom NSM, Forsvarsdepartementet og Justis- og beredskapsdepartementet, og oppdatering av instruksen.

NSMs generelle oppgaver er beskrevet i sikkerhetsloven § 8. NSM skal i henhold til bestemmelsen koordinere de forebyggende sikkerhetstiltak etter loven, og kontrollere sikkerhetstilstanden hos virksomheter underlagt loven. I tillegg er NSM i den samme bestemmelsen utpekt som utøvende organ i forholdet til andre land og internasjonale organisasjoner.

Oppgavene er nærmere detaljert i loven § 9. NSM skal for det første innhente og vurdere informasjon av betydning for gjennomføringen av forebyggende sikkerhetstjeneste. På bakgrunn av dette oppdraget utarbeider NSM hvert år en rapport om sikkerhetstilstanden. Vurderingene i rapporten bygger på funn fra virksomheter underlagt sikkerhetsloven og andre utvalgte kilder. Risikobildet som beskrives i rapporten er ment å være relevant for både offentlige og private virksomheter.

NSM skal videre søke internasjonalt samarbeid med tilsvarende tjenester i andre land og i relevante internasjonale organisasjoner når dette tjener norske interesser. I kraft av dette oppdraget er NSM nasjonalt kontaktpunkt opp mot NATO og mot nasjoner Norge har sikkerhetsmessig samarbeid med.

NSM har videre ansvaret for å føre tilsyn med sikkerhetstilstanden i virksomheter underlagt loven. Hovedformålet med NSMs tilsyn er ifølge direktoratet selv å avdekke behov for forbedring av virksomhetenes forebyggende sikkerhetstjeneste og å vurdere den enkelte virksomhets sikkerhetstilstand. NSMs tilsyn gjennomføres som styringssystemrevisjon, med utgangspunkt i standarden NS-EN ISO 19011, understøttet av fagrevisjoner.

NSM skal også bidra til at sikkerhetstiltak utvikles, herunder iverksette forskning og utvikling på områder av betydning for forebyggende sikkerhet. Som en del av dette arbeidet bidrar NSM blant annet inn i et forsknings- og utdanningssenter for informasjonssikkerhet – Center for Cyber and Information Security. Dette er et samarbeid som inkluderer fire høgskoler, NSM, Politiets sikkerhetstjeneste (PST), Politidirektoratet (POD), Oslo politidistrikt, samt en rekke andre offentlige og private aktører. Målet for samarbeidet er å etablere en av Europas største akademiske faggrupper innen informasjonssikkerhet.

NSM har også i sin oppgaveportefølje å gi informasjon, råd og veiledning til virksomheter underlagt sikkerhetsloven, og har i kraft av dette ansvaret utarbeidet en rekke veiledninger, blant annet innenfor objektsikkerhet, informasjonssikkerhet og systemteknisk sikkerhet. I tillegg til utarbeidelse av skriftlige veiledninger, skal NSM også gi konkrete råd og veiledning til virksomheter underlagt loven på de fagområdene loven dekker. Aktører utvalget har vært i kontakt med gjennom sitt arbeid, etterlyser imidlertid et NSM som er enda mer på tilbudssiden når det gjelder sin rådgivningsvirksomhet. Det kan synes som om NSM er tilbakeholdne med å gi konkrete råd og veiledninger overfor virksomheter som også er tilsynsobjekter.

I tillegg til de ovenfor beskrevne oppgaver, er NSM tillagt en rekke oppgaver på de enkelte fagområdene som er regulert i loven, herunder informasjonssikkerhet, personellsikkerhet, objektsikkerhet og sikkerhetsgraderte anskaffelser. I den videre fremstillingen blir disse oppgavene omtalt nærmere der de tematisk sett hører hjemme.

NSM skal understøtte Justis- og beredskapsdepartementet og Forsvarsdepartementet på IKT-sikkerhetsområdet i form av råd og veiledning, og gjennom å identifisere og foreslå nasjonale tiltak og krav innenfor IKT-sikkerhet. Denne oppgaven strekker seg ut over IKT-sikkerhet knyttet til behandling av sikkerhetsgradert informasjon.

---

7 Budsjett-Innst. S. nr. 7 (2002–2003), Innstilling fra forsvarskomiteen om bevilgninger på statsbudsjettet for 2003 vedkommende Forsvarsdepartementet mv.

8 Kronprinsreg.res. 4. juli 2003 nr. 900.

I Nasjonalt beredskapssystem er sjef NSM gitt fullmakt til å pålegge andre aktører å iverksette visse sikkerhetstiltak.

7.3.3 NorCERT/VDI

NSM driver i dag en nasjonal responsfunksjon for alvorlige dataangrep mot kritisk infrastruktur (NorCERT). NorCERT (Norwegian Computer Emergency Response Team) ble etablert som en integrert del av NSM fra 1. januar 2006, og var en oppfølging av St.meld. nr. 39 (2003–2004) Samfunnssikkerhet og sivil-militært samarbeid. Formålet med NorCERT er å legge til rette for effektiv håndtering av alvorlige IKT-sikkerhetsangrep mot viktig infrastruktur og informasjon i Norge. Et sentralt element i NorCERTs oppgaver er innhenting, verifisering, analyse og videreformidling av informasjon om sårbarheter, potensiell risiko, angrepsmetoder og ondsinnet kode. Dette skjer dels gjennom Nasjonalt varslingssystem for digital infrastruktur (VDI), men også gjennom mottak av informasjon fra nasjonale og internasjonale samarbeidspartnere. Den totale mengde data danner grunnlag for analyse i forbindelse med håndtering av alvorlige hendelser, og er avgjørende for koordinering med, og bistand til, nasjonale og internasjonale samarbeidspartnere.

VDI består av et nettverk av sensorer som utplasseres hos utvalgte offentlige og private virksomheter som innehar kritisk infrastruktur i tilknytning til deltakernes datanettverk. Sensorene samler inn data som skal gjøre det mulig for NSM å tidlig detektere, verifisere og varsle om koordinerte og alvorlige dataangrep.

VDI startet som et forsøksprosjekt i 1999, etablert mellom Etterretningstjenesten, PST og NSM. Fra 2003 ble driften av VDI lagt under NSM og er i dag en integrert del av NSMs organisasjon.

Ved håndtering av allerede inntrufne alvorlige angrep, bistår NorCERT også med analyse av infisert maskinvare.

Den nasjonale evnen til å håndtere alvorlige dataangrep mot kritisk infrastruktur og informasjon er avhengig av et nært samspill mellom EOS-tjenestene. Til sammen har disse tjenestene i oppdrag å oppdage, varsle, motvirke og etterforske alvorlige IKT-hendelser. Samarbeidet mellom tjenestene er formalisert og regulert i egne retningslinjer av 15. mai 2013, fastsatt av sjefene for de tre tjenestene.

NSM samarbeider også med en rekke andre offentlige og private samarbeidsparter, herunder ulike sektorvise responsmiljøer (sektor-CERT) og relevante sektormyndigheter.

Tilknytning til VDI er basert på frivillighet og tilbys etter en nærmere vurdering av virksomhetenes betydning for kritisk infrastruktur. NSM inngår en avtale med den enkelte deltaker, hvor partenes rettigheter og plikter i samarbeidet er nærmere regulert. Private virksomheter som deltar i VDI-samarbeidet, forplikter seg gjennom avtalen med NSM til å bidra til finansieringen av VDI og NorCERT gjennom et årlig vederlag.

Tilknytning til VDI er ikke ment å erstatte virksomhetenes egne sikkerhetstiltak, men skal komplementere virksomhetens egne tiltak. Virksomhetenes rett og plikt til å ivareta sikkerheten i egne systemer, er således uavhengig av VDI-samarbeidet.

Regjeringen fremmet i Prop. 97 L (2015–2016) om endringer i sikkerhetsloven, forslag om å lovfeste virksomheten som utøves av NSM gjennom NorCERT og VDI i sikkerhetsloven § 9 som en del av NSMs oppgaver. Regjeringen vurderte også i denne sammenheng om det burde etableres en hjemmel for å pålegge enkelte virksomheter med kritisk infrastruktur å tilknytte seg VDI. På bakgrunn av høringsinstansenes tilbakemelding kom imidlertid departementet til at en slik påleggsmyndighet må utredes nærmere, og bør dessuten ses i sammenheng med en vurdering av den fremtidige finansieringsmodellen for NorCERT/VDI.

Stortinget har, i forbindelse med behandlingen av Innst. 352 L (2015–2016) til Prop. 97 L (2015–2016) om endringer i sikkerhetsloven, vedtatt regjeringens forslag til lovfesting av NorCERT og varslingssystemet for digital infrastruktur.

7.4 Ansvar og myndighet etter relevant sektorregelverk

7.4.1 Kraftsektoren

Olje- og energidepartementet (OED) har det overordnet ansvaret for energiforsyningen. Energiforsyningen er en fellesbetegnelse for forsyning av elektrisitet (strøm) og fjernvarme. Elektrisitet og varme er basiskapabiliteter i et moderne samfunn ut fra et samfunnssikkerhets- og samfunnstryggheтsperspektiv.

Forsyningssikkerhet i energiforsyningen kan defineres som energisystemets evne til å kontinuerlig levere strøm av en gitt kvalitet til sluttbruker. For å sikre dette kreves et samspill mellom en rekke virkemidler, blant annet konsesjonsbehandling av nett- og produksjonsanlegg, krav til leveringskvalitet, økonomisk regulering av nettselskapene og beredskapskrav. Beredskapskravene går dels på forebyggende tiltak for å skape barrierer

og hindre avbrudd og dels på evne til rask gjenoppretting av energiforsyningen ved avbrudd.

Det sentrale sektorregelverket for beredskap i energiforsyningen er energiloven[9] kapittel 9 om beredskap og beredskapsforskriften.[10] Beredskapsforskriften omfatter selskap som eier store produksjonsanlegg (vannkraft, vindkraft og fjernvarme) eller energianlegg (ledninger, kabler, transformatorstasjoner, varmesentraler osv). Dammer (uansett formål) reguleres av damsikkerhetsforskriften.[11] Damsikkerhetsforskriften har egne krav om beredskapsmessig sikring for dammene i høyeste konsekvensklasse (klasse 3 og 4). Både beredskapsforskriften og damsikkerhetsforskriften er basert på et klassifiseringssystem, der anlegg med de største konsekvensene for samfunnet blir identifisert og underlagt de strengeste kravene til sikkerhets- og beredskapstiltak.

Norges vassdrags- og energidirektorat (NVE) er sektormyndighet for energiforsyningen, og er utpekt som beredskapsmyndighet etter energiloven. Som sektormyndighet for energisektoren benytter NVE en rekke virkemidler. Regelverkskrav framgår av energiloven og en rekke underliggende forskrifter, blant annet beredskapsforskriften med en utfyllende veileder. Beredskapsforskriften har krav om risiko- og sårbarhets (ROS)-analyser, krav til beredskapsplanverk, krav til fysiske sikringstiltak avhengig av klasse, informasjonssikkerhet, beskyttelse av driftskontrollsystem osv. NVE driver også en betydelig tilsynsaktivitet der både stedlige revisjoner, skriftlig tilsyn og inspeksjoner etter hendelser benyttes.

NVE er i beredskapsforskriften delegert myndighet til å benytte en rekke virkemidler for å påse at bestemmelsene i forskriften etterleves. NVE kan gi de pålegg som er nødvendige for gjennomføring av bestemmelsene i forskriften (§8-2), og kan ilegge tvangsmulkt (§8-4) og overtredelsesgebyr (§8-5) ved overtredelse av bestemmelsene.

NVE har omfattende dialog direkte med virksomhetene i egen sektor gjennom seminarer, innlegg i ulike fora, informasjonsskriv og stedlige besøk. NVE samarbeider med bransjeorganisasjoner om sentrale tema, for eksempel IKT-sikkerhet og sjøkabelberedskap, og har initiert opprettelsen av KraftCERT fra 2015. NVE deltar også i samarbeidsforum og har utstrakt informasjonsutveksling med andre myndigheter, blant annet Direktoratet for Samfunnssikkerhet og beredskap, Nasjonal kommunikasjonsmyndighet og NSM.

Både produksjons- og nettselskapene er selvstendige rettssubjekter. Ingen av selskapene i kraftsektoren er per dags dato underlagt sikkerhetsloven.

I medhold av energiloven § 9-1 er Kraftforsyningens beredskapsorganisasjon (KBO) etablert. KBO består grovt sagt av alle selskaper som eier eller driver anlegg for produksjon eller distribusjon av elektrisitet eller fjernvarme over en viss størrelse. KBO-enhetene kan pålegges oppgaver under beredskap og i krig. KBO-enhetene er inndelt i 14 distrikter, som stort sett følger fylkesgrensene. I hvert distrikt er det utpekt en distriktssjef (KDS) fra ett av de største nettselskapene, og denne er NVEs forlengede arm ved kriser og andre hendelser. KDS deltar i fylkesberedskapsrådet.

I helt ekstraordinære situasjoner kan hele energiforsyningen underlegges Kraftforsyningens sentrale ledelse, som vil bestå av OED/NVE og Statnett. Dette har ikke skjedd i fredstid.

7.4.2 Petroleumssektoren

Arbeids- og sosialdepartementet har det overordnede ansvaret for sikkerhet og beredskap for petroleumsvirksomhet på norsk sokkel.

Siden myndighetenes gjennomgang etter Kielland-ulykken og petroleumslovsreformen i 1985, har regulering av petroleumsvirksomheten blitt ivaretatt gjennom en sektortilnærming med en *all hazards*-tilnærming til regulering og tilsyn. Det sentrale sektorregelverket for petroleumssektoren er petroleumsloven[12] med underliggende forskrifter. Regelverket stiller krav til forebyggende, risikoreduserende tiltak, og konsekvensreduserende tiltak dersom en hendelse inntreffer.

Ansvaret for oppfølging av petroleumslovens § 9-3 om beredskap mot bevisste anslag ble i 2013 delegert fra Arbeids- og sosialdepartementet til Petroleumstilsynet (Ptil). Ptil er sektormyndighet med ansvar for tilsyn med og regulering av sikkerhet og arbeidsmiljø i petroleumsvirksomhet til havs og på enkelte landanlegg.

I medhold av petroleumsloven § 9-3 tredje ledd, kan Ptil gi pålegg om gjennomføring av sikringstiltak for å hindre tilsiktede uønskede hendelser.

---

9 Lov 29. juni 1990 nr. 50 om produksjon, omforming, overføring, omsetning og fordeling av energi m.m. (energiloven).

10 Forskrift 7. desember 2012 nr. 1157 om forebyggende sikkerhet og beredskap i energiforsyningen (beredskapsforskriften).

11 Forskrift 18. desember 2009 nr. 1600 om sikkerhet ved vassdragsanlegg (damsikkerhetsforskriften).

12 Lov 29. november 1996 nr. 65 om petroleumsvirksomhet (petroleumsloven).

Ptil har gjennom mange år gitt politiet faglig bistand under politiets etterforskning av alvorlige hendelser i petroleumsvirksomheten. Dialogen og den koordinerte samhandlingen mellom Ptil og politiet i forbindelse med etterforsking og granskinger fungerer ifølge Ptil svært godt. Ptil og politiet samarbeider også om kompetansebygging innen etterforskning, gransking og regelverksforståelse. Ved de årlige Gemini-øvelsene samarbeider Ptil både med politiet og Forsvaret. Øvelse Gemini har til hensikt å øve kontra-terrorsamvirke mellom Forsvar og politi ved bevisste anslag mot innretninger og/eller anlegg i petroleumsvirksomheten.

De senere år har Ptil hatt tett dialog med NSM/ NorCERT på de områder som angår blant annet fysisk sikring av objekter, sikkerhetstilstanden i næringen, nytt metodeverktøy for sikringsrisikovurderinger, og Cyber/IKT-sikkerhet (varsel og håndtering av alvorlige IKT-hendelser). Ptil har også etablert dialog med PST om blant annet endringer av trusselbildet og terrorsikring.

Norsk olje og gass (NOROG) er en interesse- og arbeidsgiverorganisasjon under Næringslivets hovedorganisasjon for oljeselskaper og leverandørbedrifter knyttet til utforsking og produksjon av olje og gass på norsk kontinentalsokkel. Organisasjonen representerer 53 oljeselskaper og 54 leverandørbedrifter. [13] NOROG har etablert et varslingssystem for sikringshendelser – Petroleum Industry Security Alert System (PISAS). PISAS eies og administreres av NOROG.

Gassco AS er et statlig selskap som siden 2002 har hatt operatøransvaret for transport av gass fra den norske kontinentalsokkelen. Transportsystemet er omfattende og består av flere plattformer og tusenvis av kilometer med rørledninger. Gassco er operatør for Gassled, som er et interessentskap og den formelle eieren av infrastrukturen forbundet med gasstransporten fra norsk sokkel.[14]

Ingen av de selvstendige rettssubjektene i petroleumssektoren er per dags dato underlagt sikkerhetsloven.

Drivstoffanleggloven[15] gir i § 1 Kongen fullmakt til å gi pålegg til eier eller bruker av drivstoffanlegg av vesentlig betydning for landets beholdning av drivstoffer, om sikringstiltak mot skade som følge av krigshandlinger og sabotasje. I tillegg kan Kongen gi pålegg til eier eller bruker om å foreta slike utvidelser eller nybygg som anses nødvendige av forsvarsmessige hensyn. Kongens myndighet ble i Kgl.res. av 9. mars 1979 delegert til Olje- og energidepartementet.

Etter loven § 3 kan departementet gi nærmere bestemmelser om tiltak for sikring av landets anlegg for flytende drivstoffer. Departementet kan pålegge eier eller bruker av anlegg av vesentlig betydning for landets forsyning av drivstoff å sette i verk eller å finne seg i rådgjerder til sikring av forsyningene under krig.

7.4.3 Elektronisk kommunikasjon

Samferdselsdepartementet har det overordnede ansvaret for elektronisk kommunikasjon (ekom) – ekomsektoren.

Det sentrale sektorregelverket for ekomsektoren er ekomloven[16] og ekomforskriften.[17]

Nasjonal kommunikasjonsmyndighet (Nkom) har ansvaret for å forvalte ekomloven og føre tilsyn med ekomtilbydere. Nkom arbeider for bærekraftig konkurranse i ekomsektoren, slik at brukere i hele landet kan tilbys gode tjenester til konkurransedyktige priser. Samtidig arbeider Nkom også sammen med ekomtilbyderne for å forebygge uønskede hendelser, og begrense konsekvensene av hendelser som inntreffer.

Formålet med Nkoms arbeid er å sikre brukere i hele landet gode og robuste ekomtjenester. Dette skjer blant annet gjennom normgivning, veiledning og ved å påse at ekomtilbyderne følger de pliktene de er pålagt. Nkom har en rekke virkemidler å spille på i sin oppfølging overfor aktørene, herunder veiledning, pålegg, tvangsmulkt, overtredelsesgebyr og tilbakekall av tillatelser. I henhold til Nkoms reaksjonsstrategi skal de ilegge reaksjoner som er nødvendige, hensiktsmessige og forholdsmessige.

Sentrale selvstendige rettssubjekter i ekomsektoren er underlagt sikkerhetsloven, herunder Telenor ASA, Broadnet AS og Posten AS.

En annen sentral aktør innenfor elektronisk kommunikasjon er Direktoratet for nødkommunikasjon (DNK). Justis- og beredskapsdepartementet har det overordnede ansvaret for styring og kontroll med DNK. DNK har ansvaret for forvaltning og videreutvikling av digitalt nødnett i Norge. Nødnett er et nytt digitalt samband for

---

[13] NOU 2015: 13, 147.

[14] Ibid., 147.

[15] Lov 31. mars 1949 nr. 3 om bygging og sikring av drivstoffanlegg (drivstoffanleggloven).

[16] Lov 4. juli 2003 om elektronisk kommunikasjon (ekomloven).

[17] Forskrift 16. februar 2004 nr. 401 om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften).

politi, brannvesen, helsetjenesten og andre aktører med et nød- og beredskapsansvar. Nødnett er et avlyttingssikret sambandssystem som skal gi bedre funksjonalitet, talekvalitet, dekning og kapasitet enn dagens samband. Nødnett er likevel ikke godkjent for å kommunisere sikkerhetsgradert informasjon.

7.4.4 Luftfartssektoren

Samferdselsdepartementet har det overordnede ansvaret for samfunnssikkerheten og beredskapen i luftfartssektoren. Departementet har utarbeidet Strategi for samfunnssikkerhet i samferdselssektoren. I følge denne skal virksomhetene i samferdselssektoren, herunder luftfartssektoren, forebygge og være i stand til å håndtere store uønskede hendelser, utilsiktede i form av naturødeleggelser og teknisk- og menneskelig svikt, samt tilsiktede i form av kriminalitet, terror, sabotasje og spionasje. Departementet forutsetter at virksomhetene i samferdselssektoren oppfyller krav i relevante regelverk med betydning for samfunnssikkerheten, herunder sikkerhetsloven med forskrifter.

Sivil luftfart reguleres i utstrakt grad av EU-rettsakter som er integrert i lover og forskrifter. Det sentrale sektorregelverket for luftfartssektoren er luftfartsloven[18] med underliggende forskrifter.

Forskrift om forebyggelse av anslag mot sikkerheten i luftfarten mv.[19] regulerer sikkerhetsgodkjenning og sikkerhetstiltak, sikkerhetskontroll og adgang til sikkerhetsbegrenset område. Flysikringstjenesten reguleres av forskrift om felles krav for yting av flysikringstjenester.[20]

Luftfartstilsynet er sektormyndighet i luftfartssektoren. Luftfartstilsynets hovedoppgave er å bidra til økt sikkerhet i all norsk sivil luftfart gjennom å integrere nasjonalt og internasjonalt regelverk, utarbeide forskrifter for norsk luftfart, samt føre tilsyn med at aktørene følger gjeldende lover, regler og forskrifter.

Luftfartstilsynet kan i medhold av luftfartsloven gi pålegg om retting og endring (§13 a-3), ilegge tvangsmulkt ved overtredelse av krav etter lov og forskrift (§ 13 a-4) og gi pålegg om overtredelsesgebyr for overtredelse eller unnlatelse av å etterkomme nærmere angitte bestemmelser i loven (§13 a-5).

Sikkerhetsrådet for luftfarten (SFL) er et rådgivende organ for berørte myndigheter som skal forebygge anslag rettet mot den sivile luftfart. Luftfartstilsynet leder sikkerhetsrådet, som for øvrig består av representanter fra Samferdselsdepartementet, Forsvarsdepartementet, Justis- og beredskapsdepartementet, Utenriksdepartementet, POD, PST og NSM.

Avinor AS er et statlig eid aksjeselskap der eierskapet forvaltes av Samferdselsdepartementet. Selskapet har ansvaret for å eie, drive og utvikle et landsomfattende nett av lufthavner for den sivile luftfarten og en samlet flysikringstjeneste for den sivile og militære luftfarten. I relasjon til sikkerhetsloven er Avinor ansett for å være et forvaltningsorgan, og er således omfattet av loven.

7.4.5 Vannforsyning

Helse- og omsorgsdepartementet (HOD) er overordnet ansvarlig og samordnende departement for sikkerhet og beredskap når det gjelder vannforsyning, og skal sørge for samordning og nødvendige avklaringer mellom involverte aktører på fagområdet.

Mattilsynet har ansvar for godkjenning, tilsyn og beredskap. Folkehelseinstituttet utfører forvaltningsstøtte, som bistand ved utbrudd av vannrelatert sykdom, analyser og helsefaglig rådgivning.

Drikkevannsforskriften[21] er hjemlet i matloven[22], helseberedskapsloven[23] og folkehelseloven[24]. Forskriften ivaretar kravene i EUs drikkevannsdirektiv og deler av EUs rammedirektiv for vann. Det er vannverkseiers ansvar at vannet oppfyller drikkevannsforskriftens krav. Forskriften har bestemmelser om krav til leveringssikkerhet og beredskap for normale forhold, kriser og katastrofer i fredstid og ved krig. Forskriften har unntaksbestemmelser for vannforsyning under ekstraordinære forhold. Noen vannforsyningsanlegg eller deler av disse omfattes av sikkerhetsloven.

---

18 Lov 11. juni 1993 nr. 101 om luftfart (luftfartsloven).

19 Forskrift 1. mars 2011 nr. 214 om forebyggelse av anslag mot sikkerheten i luftfarten mv.

20 Forskrift 22. desember 2014 nr. 1902 om felles krav for yting av flysikringstjenester.

21 Forskrift 4. desember 2001 nr. 1372 om vannforsyning og drikkevann (drikkevannsforskriften).

22 Lov 19. desember 2003 nr. 124 om matproduksjon og mattrygghet mv. (matloven).

23 Lov 23. juni 2000 nr. 56 om helsemessig og sosial beredskap (helseberedskapsloven).

24 Lov 24. juni 2011 nr. 29 om folkehelsearbeid (folkehelseloven).

Det pågår for tiden et arbeid med å revidere drikkevannsforskriften. På bakgrunn av en endret sikkerhetssituasjon og økt sårbarhet foreslår HOD blant annet en egen bestemmelse om forebyggende sikring. Det foreslås også krav om opplæring av ansatte med sikte på å etablere en sikkerhetskultur for å redusere sårbarhet.

7.4.6 Finansielle tjenester

Finansdepartementet er overordnet ansvarlig for forebyggende sikkerhet og beredskap i finanssektoren. Finansnæringen er en næring som i stor grad leverer sine tjenester på digitale plattformer, noe som medfører både høy grad av kompleksitet og en rekke gjensidige avhengigheter til andre innsatsfaktorer.

Det sentrale sektorregelverket for finanssektoren er blant annet finansforetaksloven[25], verdipapirhandelloven[26] og betalingssystemloven[27]. I tillegg er IKT-forskriften[28] sentral for IKT-sikkerhetsarbeidet i finanssektoren.

Finanstilsynet er i medhold av finansstilsynsloven[29] det sentrale offentlige organet som kontrollerer og vurderer om finansinstitusjoner følger de lover og regler som er vedtatt for finansmarkedet, og driver virksomheten på hensiktsmessig og betryggende måte. Denne kontrollen inkluderer banker, finansieringsforetak, e-pengeforetak, betalingsforetak, forsikringsselskap, pensjonskasser, verdipapirforetak, forvaltningsselskap for verdipapirfond, regulerte markeder (inkl. børser), oppgjørssentraler og verdipapirregister, eiendomsmeglingsforetak, inkassoforetak, regnskapsførere og revisorer mv.[30]

Finanstilsynet har i medhold av finanstilsynsloven hjemmel til å gi pålegg om å innrette virksomhetens internkontroll etter de bestemmelser tilsynet fastsetter, jf § 4 nr. 2. IKT-forskriften er gitt med hjemmel i blant annet denne bestemmelsen.

Hvis et pålegg gitt av Finanstilsynet ikke etterkommes, kan Finansdepartementet ilegge de ansvarlige dagmulkt til forholdet er rettet, jf. finanstilsynsloven § 10 annet ledd.

Beredskapsutvalget for finansiell infrastruktur (BFI)[31] har blant annet ansvaret for å komme frem til og koordinere tiltak for å forebygge og å løse krisesituasjoner og andre situasjoner som kan resultere i store forstyrrelser i den finansielle infrastruktur. BFI skal forestå nødvendig koordinering av beredskapssaker innenfor finansiell sektor. Utvalget skal herunder, på grunnlag av Sivilt beredskapssystem (SBS), samordne utarbeidelse og iverksettelse av varslingsplaner og beredskapstiltak ved sikkerhetspolitiske kriser og krig. Finanstilsynet er ansvarlig leder og sekretariat for BFI.

7.4.7 Helse og omsorg

HOD er overordnet ansvarlig innenfor helse- og omsorgssektoren.

Helseberedskapsloven[32] har som formål å verne befolkningens liv og helse. Loven skal også bidra til at nødvendig helsehjelp, helse- og omsorgstjenester og sosiale tjenester kan tilbys under krig og ved kriser og katastrofer i fredstid, jf. loven § 1. Virksomhetene som omfattes av loven skal i slike tilfeller kunne fortsette, og om nødvendig legge om og også utvide driften, på basis av den daglige tjeneste, oppdaterte planverk og gjennomføre regelmessige øvelser.

Loven inneholder også fullmaktsbestemmelser (§§ 3-1, 4-1, 5-1 og 5-2, jf. § 1-5) som gir Helse- og omsorgsdepartementet særskilte fullmakter i krig og når krig truer. Fullmaktene gjelder også ved kriser og katastrofer i fredstid etter beslutning av Kongen. Etter § 3-1 gis nærmere bestemmelser om rekvisisjon av fast eiendom, rettigheter og løsøre som trengs til bruk for blant annet helse- og omsorgstjenester. I medhold av § 4-1 kan nærmere angitt personell pålegges å forbli i tjeneste ut over ordinær arbeidstid, samt pålegges oppmøte- og arbeidsplikt. Etter §§ 5-1 og 5-2 har departementet hjemmel til å pålegge virksomheter som omfattes av loven ulike plikter av hensyn til ansvars-, oppgave- og ressursfordeling, samt pålegg om omlegging av virksomheten og restriksjoner på omsetning av varer.

---

25 Lov 10. april 2015 nr. 17 om finansforetak og finanskonsern (finansforetaksloven).

26 Lov 29. juni 2007 nr. 75 om verdipapirhandel (verdipapirhandelloven).

27 Lov 17. desember 1999 nr. 95 om betalingssystemer m.v. (betalingssystemloven).

28 Forskrift 21. mai 2003 nr. 630 om IKT systemer i banker mv. (IKT-forskriften).

29 Lov 7. desember 1956 nr. 1 om tilsynet med finansforetak mv. (finanstilsynsloven).

30 Finanstilsynet.no, http://www.finanstilsynet.no/no/Venstremeny/Om-Finanstilsynet/

31 Finanstilsynet.no, http://www.finanstilsynet.no/no/Tverrgaende-temasider/Beredskapsutvalget-for-finansiell-infrastruktur-BFI/

32 Lov 23. juni 2000 nr. 56 om helsemessig og sosial beredskap (helseberedskapsloven).

Tabell 7.1 Et utvalg relevante lover og tilhørende ansvarsmyndighet

Lov/Traktat	Angår	Ansvarlig dept./etat
Sikkerhetsloven med forskrifter	Forebyggende sikkerhet	JD/FD (NSM)
Ekonomloven med forskrifter	Utstedelse av frekvenstillatelser samt innmelding av satelittnettverk til ITU. Tekniske målinger av radiospekteret	SD (Nkom)
Svalbardtraktaten	Bruk av Svalbard til ikke-militære formål	UD/JD
Romloven	Lov om oppskyting av gjenstander fra norsk territorium	NFD
International Convention on Maritime Search and Rescue	Internasjonal koordinering av SAR	JD
Metarea 19	Værvarsling	KD (met.no, Kystverket)
Galileo/Copernicus-forordningene	Beskyttelse av infrastruktur og tjenester	NFD (NRS)
Romregistreringskonvensjonen	Forvaltning og romregister for norske satelitter	UD (NRS)
ITU-konvensjonen	Frekvensfordeling	SD (Nkom)
Svalbardloven med forskrifter	Etablering, drift og bruk av bakkestasjoner med mer	SD
Havressursloven med forskrifter	Krav til satelittsporingsutstyr om bord på fiskebåter med mer	NFD, Fiskeridirektoratet
Lov om petroleumsvirksomhet med forskrifter	Satelittsporing av seismikkskip	OED
Skipssikkerhetsloven med forskrifter	Krav til kommunikasjonsutstyr med mer	NFD

Kilde: NOU 2015: 13, *Digital sårbarhet – sikkert samfunn – Beskytte enkeltmennesker og samfunn i en digitalisert verden*, 122.

7.4.8 Satellittbaserte tjenester

Med satellittbaserte tjenester menes tjenester for posisjonsbestemmelse, navigasjon og presis tidsangivelse (PNT), kommunikasjonstjenester og jordobservasjonstjenester.

I følge Lysne-utvalgets utredning er leveranse av satellittbaserte tjenester i hovedsak et internasjonalt anliggende. Det er imidlertid flere norske virksomheter som er premissleverandører og har en myndighetsrolle på området. Det er ingen utpekt aktør som har det overordnede ansvaret for satellittbaserte tjenester i Norge, men det finnes en rekke myndighetsaktører som har en sentral rolle innen romvirksomheten.[33]

Regulering av romvirksomheten er hjemlet i en rekke ulike lover og forskrifter, og ansvaret for oppfølging tilhører ulike departementer og etater. I tabell 7.1 er det gitt en ikke uttømmende oversikt over relevante lover og tilhørende ansvarlige myndigheter.

Space Norway AS er underlagt sikkerhetsloven ved enkeltvedtak.

7.5 Tilsynsmyndigheters organisering og oppgaver i Norge

Tilsyn kan forstås som tilsynsmyndighetenes undersøkelse av status i henhold til de krav som er gitt i medhold av lov eller forskrift. I den videre fremstillingen gis det en nærmere redegjørelse for organisering av tilsyn på generell basis, herunder Tilsynsmeldingens[34] anbefalinger og eksisterende mekanismer for samordning og koordinering av tilsyn.

Det eksisterer i dag over 30 statlige forvaltningsorganer i Norge som innehar en eller annen

[33] NOU 2015: 13, 121–122.

[34] St.meld. nr. 17 (2002–2003), Om statlige tilsyn (tilsynsmeldingen).

Boks 7.1 Beredskapsutvalget for finansiell infrastruktur

Følgende institusjoner er representert i BFI som faste medlemmer og varamedlemmer:

- Finanstilsynet
- Norges Bank
- Finans Norge (FNO)
- Bits AS (bank- og finansnæringens infrastrukturselskap)
- Nets Norge
- Evry ASA
- Verdipapirsentralen ASA (VPS)
- DNB Bank ASA
- Nordea Bank Norge ASA
- Sparebank 1 Gruppen
- Eika Gruppen (representerer andre banker)

Som observatører:

- Finansdepartementet
- FinansCERT
- Verdipapirforetakenes forbund
- Verdipapirfondenes forening
- Nasjonal Sikkerhetsmyndighet (NSM) v/NorCERT
- Nasjonal Kommunikasjonsmyndighet (Nkom)
- Telenor Norge
- Norges Vassdrag- og energidirektorat (NVE)
- Posten Norge

form for tilsynsfunksjon. I tillegg til dette kommer fylkesmennenes tilsyn med kommunesektoren, de enkelte kommuners direkte tillagte tilsynsoppgaver, samt offentlige tilsynsoppgaver som ivaretas av selvstendige rettssubjekter.[35]

Tilsynsorganer kan grovt sett kategoriseres etter tre typer kriterier: Hva slags *oppgaver* (funksjoner/roller) de har, hvilke *formål* de forvalter og hvilke *målgrupper* tilsynsfunksjonen retter seg mot.[36]

Det er stor variasjon i hvilke *oppgaver* som tilligger forvaltningsorganene som innehar tilsynsfunksjoner i de ulike sektorer. Enkelte tilsynsmyndigheter har en tilnærmet rendyrket rolle som tilsynsorgan. Et eksempel er Helsedirektoratet som ivaretar direktoratsfunksjonen, mens Helsetilsynet har tilsynsfunksjonen. Andre sektorer har en mer integrert tilnærming, hvor fagmyndigheten i tillegg til tilsynsoppgaver har et bredt spekter av oppgaver som tilligger direktoratsnivået i myndighetsstrukturen. Nasjonal kommunikasjonsmyndighet synes å ha en integrert tilnærming, hvor både fagmyndighets- og tilsynsfunksjonen ivaretas av samme etat. Fylkesmennsembetene har sannsynligvis den mest integrerte tilnærmingen, hvor fylkesmannsrollen kombinerer et svært bredt spekter av oppgaver med tilhørende funksjoner. Fylkesmennene innehar hovedtyngden av tilsynsoppgavene overfor kommunene og deres ansvar og plikter spenner over de fleste sektorer og tjenesteområder i kommunene.[37]

Forvaltningsorganer tillagt tilsynsfunksjoner har gjennomgående en nokså sammensatt oppgaveportefølje, og er i hovedsak organer utenfor departementsstrukturen. Det avgjørende for hvilke roller de enkelte tilsynsmyndigheter er tillagt, er de lovgrunnlag og styrende dokumenter som legger grunnlaget for deres virksomhet. Til tross for anbefalingene i Tilsynsmeldingen[38], synes det overveiende flertall av forvaltningsorganer med tilsynsfunksjoner å ivareta flere roller parallelt.

De eksisterende tilsynsregimene dekker de fleste samfunnsområder og representerer et bredt spekter av ulike *formål*. Statskonsult gjennomførte i 2002 en gjennomgang av statlige tilsynsordninger.[39] I rapporten kategoriserte Statskonsult de norske tilsynsregimene etter fire hovedformål:

- Sikkerhet for liv, helse, miljø og materielle verdier/ressurser
- Fungerende samferdsel, kommunikasjon og energiforsyning (infrastruktur)
- Fungerende markeder
- Integritetsvern og ideelle verdier[40]

I hvor stor utstrekning tilsynsorganene er spesialisert innenfor de ulike formålene, varierer i stor grad. Enkelte tilsyn ivaretar relativt snevre og spesifikke formål, eksempelvis har Datatilsynet som eneste formål å påse at den enkeltes personvern ikke blir krenket gjennom behandling av person-

35 Preben Hempel Linde, et.al., *Risiko og tilsyn, 2. utgave* (Oslo: 2015), 86–87.

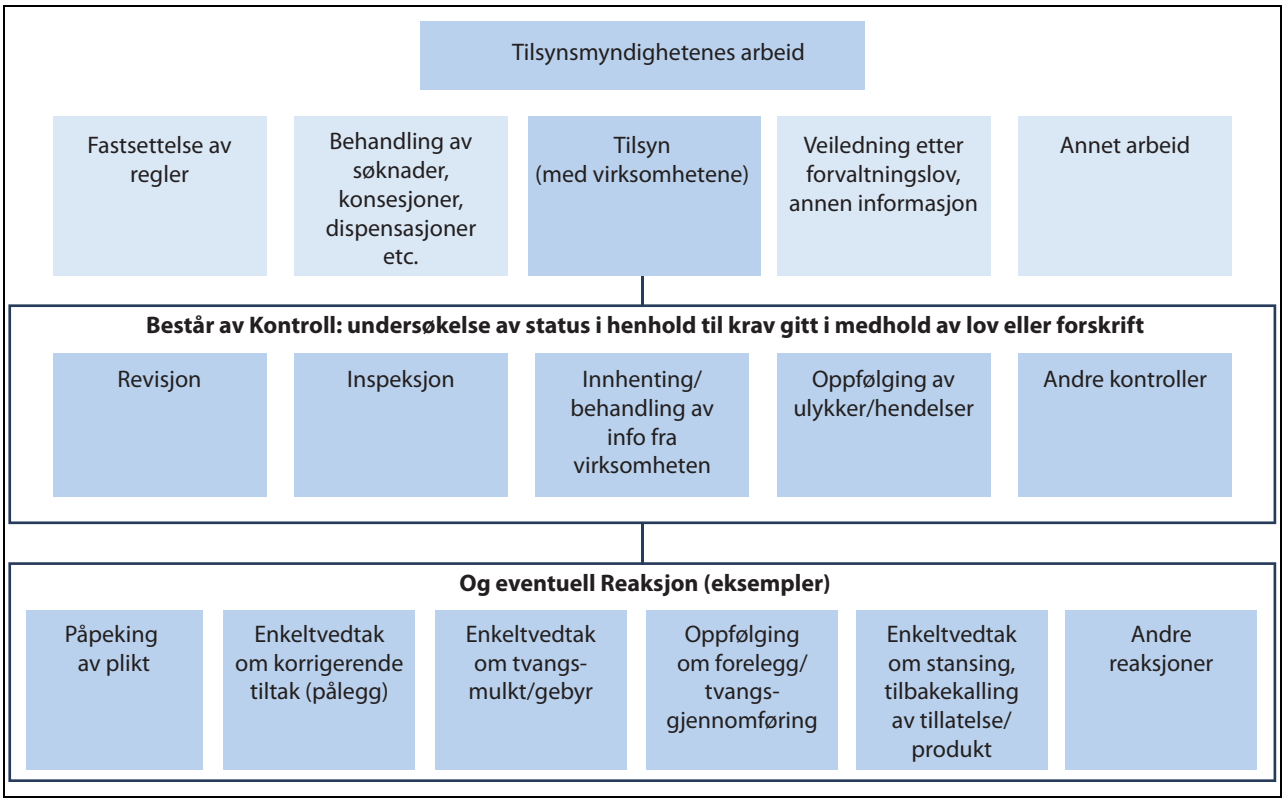
36 Ibid.

37 Ibid., 89–90.

38 St.meld. nr. 17 (2002–2003), tilsynsmeldingen

39 Rapport 2002:12, *(Be)grep om tilsyn – Gjennomgang av statlige tilsynsordninger*, https://www.difi.no/sites/difino/files/2002-12.pdf

40 Ibid., 53–54.



Figur 7.1 Grafisk fremstilling av tilsynsmyndighetens arbeid og begrepsapparat.

Kilde: Preben Hempel Lindøe, Geir Sverre Braut og Jacob Kringen, *Risiko og tilsyn, 2. utgave,* (Oslo: Universitetsforlaget, 2015.)

opplysninger. Andre tilsyn ivaretar et bredt spekter av formålsområder.

Også når det gjelder *målgrupper* er det variasjon. I grove trekk finnes det to modeller for inndeling av tilsyn etter målgrupper. Enkelte tilsyn er såkalte sektortilsyn, hvor målgruppen er definert ut fra den aktuelle sektorens inndeling. Nasjonal kommunikasjonsmyndighet, Petroleumstilsynet og Finanstilsynet er eksempler på rene sektortilsyn, som ivaretar tilsynsfunksjonen i sine respektive sektorer. Andre tilsyn har en mer sektorovergripende tilsynsfunksjon, hvor formålet med tilsynsfunksjonen strekker seg over en rekke forskjellige bransjer og sektorer. Eksempler på sektorovergripende tilsyn er Arbeidstilsynet, Konkurransetilsynet og det tilsyn med størst relevans for sikkerhetsloven: Nasjonal sikkerhetsmyndighet.

Den tradisjonelle integrerte modellen hvor flere roller må ivaretas innenfor en og samme organisasjon, har gjerne vært begrunnet i verdiene demokrati og effektivitet. Ved en slik organisering kan myndighetene fremstå på en enhetlig måte utad, og vil samtidig kunne sørge for helhetlig og samordnet styring og effektiv utnyttelse av kompetanse og ressurser. Samorganisering av flere oppgaver kan også bidra til å gi en bedre samordning mellom politikkutforming og de ulike iverksettingsoppgavene i en sektor eller på tvers av sektorer, noe som igjen kan bidra til en bedre politisk styring og måloppnåelse. En deling av arbeidsoppgavene mellom flere forskjellige aktører, eksempelvis i et rent tilsynsorgan, et ordinært direktorat og et eget tjenesteproduserende organ, kunne medføre at fagmiljøene blir små og sårbare. Formål og funksjoner ivaretas mest rasjonelt og effektivt dersom forvaltningen utnytter den samlede kunnskapen om fag og disipliner, sektorer og næringer, klienter og målgrupper. Hensynet til brukerne og målgruppene kan også være et argument for ikke å gjøre et slikt skille.[41]

Som figur 7.1 viser kan tilsynsmyndighetenes oppgaveportefølje i en tradisjonell integrert modell, grovt sett kategoriseres i fire hovedoppgaver: fastsettelse av regler, behandling av søknader og konsesjoner, tilsyn og veiledning. I tillegg har en del tilsyn enkelte andre oppgaver utover disse fire vanligste gjøremålene.

[41] Linde et.al, Risiko og tilsyn, 2015, 108.

7.5.1 Tilsynsmeldingens idealer for organisering og utføring av tilsynsfunksjonen

Det er få rettslige føringer for hvordan rollekonflikter skal identifiseres og håndteres på institusjonelt nivå i forvaltningen. Likevel er det i flere sektorer (som tele og kraft) EØS-reguleringer som stiller krav om at den nasjonale håndhevingsmyndigheten skal organiseres adskilt fra tjenesteproduksjon. Forvaltningslovens regulering av habilitet knytter seg til personnivå og mulige sammenblandinger av private og offentlige interesser. Samtidig gir forvaltningslovens habilitetsbestemmelse uttrykk for generelle prinsipper, som kan tenkes å ha anvendelse for tilsvarende problemer på institusjonelt nivå.

I Tilsynsmeldingen[42] fremmet regjeringen (Bondevik II) en rekke idealer for organisering og utføring av tilsynsfunksjonen. Formålet med å fremme idealene var å legge grunnlaget for en kvalitetsreform for statlige tilsyn, for å sette dem i bedre stand til å møte kravene om en mer funksjonsdyktig offentlig sektor.

I meldingen ble organisering av tilsyn knyttet til to hoveddimensjoner: den horisontale organisering og den vertikale organisering. Med horisontal organisering menes hvordan oppgaver og myndighet er fordelt mellom ulike myndigheter på samme hierarkiske nivå i forvaltningen. Den vertikale organiseringen omhandler relasjonen mellom underordnet og overordnet myndighet, herunder graden av delegert myndighet fra, og graden av faglig uavhengighet fra, overordnet departement.

I meldingen presiseres det at idealene for organisering og utføring av tilsynsvirksomhet er ment å angi en generell ønsket retning. Hvorvidt idealene bør gjennomføres innenfor den enkelte sektor, må bero på en konkret vurdering, hvor blant annet sektorspesifikke hensyn kan tilsi avvik fra en ideell organisering.

7.5.1.1 En klar og tydelig rolle for tilsynene

For å styrke tilsynsfunksjonen og sikre allmennhetens og tilsynsobjektenes tillit til myndighetene, bør det tilstrebes visse organisatoriske skiller mellom tilsynsrollen og andre roller. Avveiningen av hvilke rollekonflikter som er problematiske må foretas konkret overfor det enkelte tilsyn. I tilsynsmeldingen vises det blant annet til den åpenbare rollekonflikten som oppstår når tilsynsorganet, i tillegg til å kontrollere, også står for kommersiell tjenesteproduksjon overfor tilsynsobjektet.

Som en konsekvens av ønsket om mer ryddighet i offentlige roller, ble blant annet Petroleumstilsynet skilt ut fra Oljedirektoratet med virkning fra 1. januar 2004. Dette ble begrunnet i potensialet for rollekonflikt som lå i organiseringen av Oljedirektoratet, som både hadde rådgivende oppgaver overfor departementene og delegert regelverkskompetanse og tilsyn med sikkerhet og arbeidsmiljø i petroleumsvirksomheten. I meldingen ble det riktignok presisert at dette ikke hadde vært et problem i enkeltsaker Oljedirektoratet hadde behandlet.[43]

7.5.1.2 Klare og tydelige formål for tilsynene

Det er en målsetting å unngå motstridende formål i samme tilsyn. Endringer i tilsynsorganiseringen må ifølge tilsynsmeldingen ta sikte på at samme tilsyn normalt ikke skal ivareta formål som kan stå i konflikt med hverandre.

Det er også en målsetting å unngå at samme formål ivaretas av forskjellige tilsyn. En bedre koordinering av tilsyn med samme forhold vil ifølge meldingen bidra til enkelhet og klarhet ovenfor tilsynsobjektene og allmennheten. Det vil også kunne bidra til å redusere belastningen for de ulike tilsynsobjektene.

7.5.1.3 Økt faglig uavhengighet fra departementene

Idealet i tilsynsmeldingen er at det fremstår som klart om en beslutning er fattet på faglig eller politisk grunnlag, ved at grensesnittet mellom politikk (departement/regjering) og fag (direktorat/tilsyn) er så klart og entydig som mulig. I realiteten vil imidlertid vedtak og retningslinjer være en blanding av politikk og faglige vurderinger.

Økt faglig uavhengighet vil innebære at muligheten for politisk overprøving av tilsynene i enkeltsaker vil reduseres. Dette må imidlertid balanseres mot behovet for å sikre en politisk og demokratisk styring med de samfunnsmessige prioriteringene.

7.5.1.4 Styrket fagkompetanse i tilsynene

Høy faglig kompetanse er en viktig forutsetning for at tilsynene kan gis en mer uavhengig rolle og få nødvendig tillit og legitimitet. Ulike tilsyn har i

[42] St.meld. nr. 17 (2002–2003), tilsynsmeldingen.

[43] Ibid., 41.

dag forskjellig tilsynsfilosofi og tilsynsmetodikk. Enkelte tilsyn er tilbakeholdne med å gi råd og veiledning til tilsynsobjektene i konkrete saker, blant annet fordi de ikke ønsker å skape et inntrykk av at tilsynet gjennom dette har garantert for at løsningene er i overensstemmelse med regelverket. Andre tilsyn driver derimot en nokså utstrakt faglig veiledning av sine tilsynsobjekter.

I meldingen påpeker regjeringen at hvis tilsynsfunksjonen også skal legge grunnlaget for et dynamisk næringsliv, bør tilsynene også kunne gi faglig veiledning til tilsynsobjektene. Tilsynene bør i denne sammenheng ikke nøye seg med en påpekning av at et gitt forhold ikke er i overensstemmelse med regelverket, men bør i sin tilnærming til sakene tilstrebe å være løsningsorienterte ved å komme med forslag til hvordan en virksomhet kan finne en løsning som er i overensstemmelse med regelverkets krav. Dette stiller høye krav til tilsynenes kompetanse.

7.5.2 Samordning og koordinering av tilsyn

I Tilsynsmeldingen[44] er det en uttalt målsetting å legge til rette for at styrking av tilsyn skal gå hånd i hånd med en dynamisk næringsutvikling. Mange av tilsynsobjektene – ikke minst i næringslivet – opplever ofte tilsynsmyndighetene og andre regulerende myndigheter som en begrensning for egen utvikling. Detaljregulering, lang saksbehandlingstid og uklare myndighetsforhold medfører også en uforutsigbarhet for virksomhetene.

På enkelte områder i samfunnet er det flere tilsyn som ivaretar dels sammenfallende formål og/eller har klare grenseflater mot andre tilsyn. Et ideal for statlig tilsynsvirksomhet er ifølge meldingen å unngå at samme formål ivaretas av forskjellige tilsyn.

På HMS-området er det en rekke forskjellige tilsynsmyndigheter, som har ansvar for å føre tilsyn med at virksomhetene følger opp de kravene som er stilt til den enkelte virksomhet gjennom regelverk eller vedtak. En fellesnevner for tilsynsvirksomheten på dette området er at den retter seg mot forholdene i arbeidslivet, hvor tilsynsobjektene i stor grad er private næringsvirksomheter.

I Tilsynsmeldingen ble det anbefalt at tilsynsfunksjonene i større grad rendyrkes for å unngå at de ulike rollene kan komme i konflikt med hverandre og bidra til at det stilles spørsmål ved tilsynets legitimitet. Det påpekes i denne sammenheng at ikke alle rollekombinasjoner er like problematiske, men at man i det minste burde unngå at et offentlig tilsyn også opptrer som tjenesteleverandør for sine egne tilsynsobjekter.

7.5.2.1 Koordinerende tilsynsetater for HMS

For å redusere problemet med at virksomheter utsettes for tilsyn fra flere forskjellige tilsynsmyndigheter, med til dels sammenfallende formål, utpekte regjeringen i meldingen tre koordinerende etater for HMS-tilsyn: Arbeidstilsynet, Petroleumstilsynet og Direktoratet for samfunnssikkerhet og beredskap. Dette ble igjen fulgt opp av tre kongelige resolusjoner – en for hver koordinerende etat – som angir hva etatene skal koordinere.

Arbeidstilsynet ble i kgl.res. av 17. september 2004 utpekt som koordinerende instans for HMS-tilsyn med virksomheter på land, med unntak av landanleggene innenfor petroleumsvirksomheten hvor koordineringsrollen ivaretas av Petroleumstilsynet. Arbeidstilsynets koordineringsansvar omfatter de etater som fører tilsyn etter internkontrollforskriften.[45]

Utgangspunktet for koordinering av tilsynet sentralt og lokalt kan være forhold som er tilnærmet like for flere etater, det vil si innsatsområder der resultatene blir bedre dersom to eller flere etater samarbeider.

Ptil ble utpekt som koordinerende myndighet for HMS-myndighetene for petroleumsvirksomheten på norsk kontinentalsokkel, samt den samlede virksomheten ved landanleggene for petroleumsvirksomhet ved kronprinsregentens resolusjon 19. desember 2003. I Instruks om Petroleumstilsynet[46] fremgår det at koordineringsansvaret omfatter saksområder som krever samhandling på myndighetssiden.

I tillegg til den instruksfestede koordineringsrollen er det etablert en rekke avtaler om bistand, som gir Ptil anledning til å trekke på sakkyndig bistand fra en rekke HMS-etater.[47]

DSB har hovedansvaret som koordinerende organ for myndighetenes oppfølging av sikkerhetsrapporter og tilsyn med virksomheter som

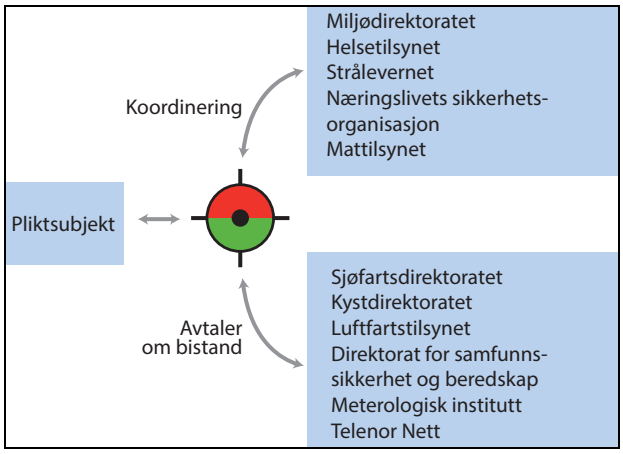
---

[44] Ibid.

[45] Forskrift 6. desember 1996 nr. 1127 om systematisk helse-, miljø- og sikkerhetsarbeid i virksomheter (internkontrollforskriften).

[46] Forskrift 19. desember 2003 nr. 1594 Instruks om koordinering av tilsynet med HMS i petroleumsvirksomheten på norsk kontinentalsokkel, og på enkelte anlegg på land (instruks om Petroleumstilsynet).

[47] Rapport 27. august 2013, *Tilsynsstrategi og HMS-regelverk i norsk petroleumsvirksomhet*, https://www.regjeringen.no/globalassets/upload/AD/publikasjoner/rapporter/2013/Utvalgsrapport_HMS_regelverk.pdf, 52.



Figur 7.2 Grafisk fremstilling av Petroleumstilsynets tilsynsansvar.

Kilde: *Tilsynsstrategi og HMS-regelverk i norsk petroleumsvirksomhet*, rapport avgitt av ekspertgruppe 27.08.2013.

omfattes av storulykkeforskriften.[48] Formålet med koordineringen er at landbaserte virksomheter som omfattes av forskriften skal behandles på en helhetlig måte, og at de opplever et koordinert og mest mulig samordnet tilsyn fra myndighetenes side. Det er etablert en egen koordineringsgruppe, ledet av DSB, for oppfølgning av storulykkeforskriften, bestående av DSB, Arbeidstilsynet, Statens forurensningstilsyn, Næringslivets sikkerhetsorganisasjon og Ptil.

7.5.2.2 Nasjonal sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighet er som omtalt i kapittel 7.3 tillagt tilsynsfunksjon etter sikkerhetsloven, og har i den forbindelse et koordinerende ansvar innen objektsikkerhet. Det følger av loven § 9 første ledd bokstav c) at NSM skal føre tilsyn med sikkerhetstilstanden i virksomheter, herunder kontrollere at den enkeltes plikter i eller i medhold av loven overholdes. NSM gis i samme bestemmelse myndighet til å gi pålegg om forbedringer der sikkerhetstilstanden ikke er tilfredsstillende.

I utgangspunktet innehar NSM tilsynsfunksjonen innen alle fagområder knyttet til forebyggende sikkerhetstjeneste etter loven. For objektsikkerhet er det imidlertid tilsynsansvaret fordelt mellom NSM og aktuelle sektortilsyn.

NSM skal føre tilsyn med at utvelgelse og klassifisering av skjermingsverdige objekter skjer i henhold til lov og forskrift, jf. objektsikkerhetsforskriften § 4-3 første ledd.

Når det gjelder den konkrete oppfølgingen av objekteiere, følger det av forskriften § 4-3 annet ledd at tilsynsorganer med ansvar for forebyggende sikkerhet i en sektor skal ivareta tilsynsfunksjonen overfor objekteiere innen den aktuelle sektoren. For de sektorer der det ikke finnes slike sektortilsyn, vil NSM ivareta tilsynsfunksjonen overfor objekteierne. NSM skal i tillegg føre et overordnet tilsyn, som «sikrer implementering av sektorovergripende harmoniserte sikkerhetstiltak» i henhold til forskriften.

7.6 Tverrsektorielle scenarier

Forsvarets forskningsinstitutt (FFI) har på oppdrag fra utvalget foretatt en sikkerhetsfaglig vurdering av hvorvidt sektorregelverket er tilstrekkelig for god sikring av kritisk infrastruktur og kritiske samfunnsfunksjoner.[49] FFI ble også anmodet om å vurdere hvorvidt en overordnet lovregulering kan bidra til bedre forebyggende sikkerhet for ivaretakelse av kritiske samfunnsfunksjoner og hvilke forhold som eventuelt bør reguleres i et slik overordnet regelverk.

FFI har i sin utredning til utvalget kommet med flere anbefalinger som kan bidra til å sikre grunnleggende nasjonale funksjoner. En av FFIs konkrete anbefalinger er å etablere tverrsektorielle scenarier, blant annet som grunnlag for å kunne gjøre tilfredsstillende verdivurderinger:

> Det bør etableres nasjonale tverrsektorielle scenarioer som dekker hele krisespekteret. Disse bør etableres ved et samarbeid mellom Justis- og beredskapsdepartementet og Forsvarsdepartementet i nær kontakt med øvrige departementer, vedtas i regjeringen og gjøres gjeldende for alle sektorer. De nasjonale scenarioene bør organiseres i overordnede scenarioklasser og legges til grunn for etablering av verdivurdering, ROS-analyser, forebyggende tiltak, samt beredskapsøvelser.

DSB utarbeider i dag Nasjonalt risikobilde NRB, som også i en viss utstrekning inkluderer tilsiktede hendelser som terrorisme og strategisk overfall. Forsvarets planprosesser er også basert på en

[48] Kgl.res. 24. juni 2005, jf. St.meld. nr. 17 (2001–2002) og St.meld. nr. 17 (2002–2003).

[49] Forsvarets forskningsinstitutt, *Vurdering av forebyggende sikkerhet innen kraft, petroleum og luftfart*, FFI-rapport 00702 (Kjeller: Forsvarets forskningsinstitutt 2016), digitalt vedlegg nr. 3.

Boks 7.2 Nasjonal sikkerhetsmyndighets erfaring med tilsyn etter objektsikkerhetsregelverket

Gjeldende objektsikkerhetsregelverk trådte i kraft 1. januar 2011. I forskriftens § 5-2 ble det fastsatt en overgangsbestemmelse hvor gjennomføring av sikkerhetstiltak skulle skje innen tre år fra ikrafttredelse. Bestemmelsen åpnet også for utsettelse med gjennomføring av tiltak ytterligere ett år, etter godkjennelse fra NSM. Mange objekteiere søkte og fikk innvilget slik utsettelse. Regimet med kontroll av iverksatte sikkerhetstiltak hos objekteiere har derfor i realiteten virket i relativt kort tid. NSM har opplyst utvalget om at det, grunnet de nevnte implementeringsfristene, kun er en forholdsvis liten andel av det totale antallet objekteiere som er kontrollert per tid. NSM besitter derfor noe begrenset erfaring på området.

Der det i sektoren foreligger relevant og dekkende regelverk skal sektortilsyn, etter objektsikkerhetsforskriften, føre kontroll med at iverksatte sikkerhetstiltak hos objekteierne tilfredsstiller de funksjonelle kravene i objektsikkerhetsregelverket. For noen sektorer fremstår det mer tydelig enn for andre, at det foreligger et regelverk som både er relevant og dekkende for objektsikkerhet.

For enkelte sektorer oppfatter NSM at det er avklart at sektortilsynene har en rolle med å føre tilsyn med sikringstiltakene for skjermingsverdige objekter. Når det gjelder andre sektorer har de aktuelle sektormyndighetene vurdert det slik at de ikke omfattes av objektsikkerhetsregelverket. En tredje gruppe er sektorer hvor det er uklart hvorvidt det foreligger et relevant og dekkende regelverk, eller om aktuelle sektortilsyn er bevisst rollen de har med å kontrollere iverksatte sikringstiltak for skjermingsverdige objekter.

Eksempler på sektorer og regelverk hvor dette er avklart er innen ekom-lovgivningen og luftfartslovgivningen, hvor henholdsvis Nasjonal kommunikasjonsmyndighet Nkom og Luftfartstilsynet er sektortilsyn. Når det gjelder Mattilsynets rolle som aktuelt sektortilsyn, opplyser NSM at det tidligere vært noe uklarhet knyttet til dette. I forslag til ny drikkevannsforskrift er det imidlertid foreslått bestemmelser som NSM oppfatter blant annet er ment å hjemle de funksjonelle kravene i objektsikkerhetsregelverket. Finanstilsynet har ifølge NSM, vurdert det slik at det ikke har hjemmel til å føre tilsyn med objekteiere som kunne vært aktuelle i denne sektoren. Petroleumssektoren og energisektoren har ikke utpekt skjermingsverdige objekter.

NSMs tilsynsprogram for 2015 og 2016 har omfattet en rekke aktuelle sektortilsyn. Hensikten med dette har blant annet vært å avdekke hvorvidt sektortilsyn oppfatter at de har en rolle i å føre tilsyn med skjermingsverdige objekter, samt hvorvidt slike tilsyn faktisk er gjennomført.

NSM kartlegger relevante sektortilsyn. NSM har opplyst utvalget om at de på bakgrunn av denne oversikten, vil gå i dialog med sektortilsynene for å få bekreftet en omforent oppfatning om ansvar og myndighet. Dette innebærer også en mer systematisk gjennomgang av de ulike sektorregelverk for mer konkret å kunne avgjøre hvilke objekter/objekteiere som er underlagt andre sektorer enn de ovenfor nevnte.

Innen ekomsektoren har det vært gjennomført felles tilsyn mellom Nkom og NSM. NSM har opplyst utvalget om at de også kjent med at Nkom har gjennomført ytterligere tilsyn hvor objektsikkerhet har vært tema for tilsynet.

Det foreligger per i dag ingen rutine for at NSM mottar informasjon om gjennomførte tilsyn med skjermingsverdige objekter fra sektortilsynene. Etter NSMs oppfatning burde det imidlertid vært en fast prosedyre at de ulike sektormyndigheter, for eksempel på årlig basis, rapporterer til NSM om hvilke skjermingsverdige objekter/objekteiere som har vært gjenstand for tilsyn. Dette for at NSM skal kunne oppfylle sine oppgaver etter sikkerhetsloven.

Kilde: NSM.

scenariobasert tilnærming, både når det gjelder langtidsplanlegging og utviklingen av doktriner, anskaffelser, utdanning og trening av personell etc. Etter dagens sikkerhetslov er det imidlertid ikke på samme måte utarbeidet scenarioer som grunnlag for identifisering av virksomheter som bør være underlagt loven eller for identifisering og utpeking av skjermingsverdige objekter. FFI mener dette er en svakhet ved dagens regelverk.

7.7 Utvalgets vurderinger

Ansvars- og myndighetsfordelingen innenfor forebyggende sikkerhet etter loven har stått sentralt i utvalgets arbeid. Et utgangspunkt for utvalgets arbeid har vært at de generelle prinsippene for krisehåndtering og beredskap ligger fast, og også bør gjelde for innretningen på en ny sektorovergripende lov om forebyggende nasjonal sikkerhet.

I tråd med ansvarsprinsippet bør det primære ansvaret for forebyggende sikkerhet i de ulike samfunnssektorene tilligge det enkelte fagdepartement. Det er det enkelte fagdepartement som kjenner sin sektor best, og har de beste forutsetningene for å kunne identifisere grunnleggende nasjonale funksjoner og virksomheter av kritisk betydning for disse, samt gjøre nødvendige samfunnsøkonomiske prioriteringer innad i sektoren.

Regjeringens anledning til å fordele myndighetene til det departement den måtte ønske, jf. Grunnloven § 12 annet ledd, vil ikke utfordres av utvalgets forslag. Ansvaret for forebyggende sikkerhet i en samfunnssektor vil følge den til enhver tid gjeldende myndighetsfordelingen mellom de ansvarlige statsrådene.

Samtidig mener utvalget at det er helt avgjørende for å kunne ha en helhetlig tilnærming til forebyggende sikkerhet på tvers av samfunnssektorene, at det sektorovergripende perspektivet ivaretas i tråd med samordningsprinsippet. Som utvalget kommer inn på nedenfor, anbefales det at ansvaret for å ivareta det sektorovergripende perspektivet tillegges funksjonen Nasjonal sikkerhetsmyndighet. Utvalgets forslag er ikke ment å rokke ved Justis- og beredskapsdepartementets overordnede ansvar for forebyggende sikkerhet i de sivile samfunnssektorene og Forsvarsdepartementets ansvar for forsvarssektoren, slik dette er fordelt i Kronprinsregentens resolusjon av 4. juli 2003 og i samfunnssikkerhetsarbeidet for øvrig. Ansvaret for utøvelsen av funksjonen Nasjonal sikkerhetsmyndighet, vil således være utledet av det overordnede ansvaret til henholdsvis Justis- og beredskapsdepartementet og Forsvarsdepartementet.

7.7.1 Systematikk for identifisering og utvelgelse

For at en ny lov om forebyggende nasjonal sikkerhet skal få nødvendig effekt, er det nødvendig å etablere et system for å kunne identifisere grunnleggende nasjonale funksjoner og hvilke virksomheter som er av kritisk betydning for disse.

Utvalget har vurdert om det i første instans bør være opp til den enkelte virksomhet selv å vurdere hvorvidt virksomheten faller inn under loven eller ikke. Den enkelte virksomhet vil imidlertid ha begrensede forutsetninger for å kunne gjøre en fullstendig og forsvarlig vurdering av egen virksomhets betydning for grunnleggende nasjonale funksjoner. Dette gjelder særlig de selvstendige rettssubjektene som kan tenkes å falle inn under loven. En slik mekanisme vil være avhengig av at den enkelt virksomhet både har nødvendig informasjonsgrunnlag og tilstrekkelig kompetanse til å gjøre de riktige vurderingene, samt være sitt samfunnsansvar bevisst. Utvalget tror ikke en slik tilnærming vil fungere i praksis og vil derfor ikke anbefale den.

Det er i dag allerede etablert et system hvor det enkelte fagdepartement har ansvaret for identifisering av kritiske samfunnsfunksjoner gjennom Instruks for departementenes arbeid med samfunnssikkerhet og beredskap (samordningsresolusjonen).[50] I samordningsresolusjonen stilles det krav om at departementene skal ha oversikt over kritiske samfunnsfunksjoner og kritisk infrastruktur i egen sektor. På bakgrunn disse oversiktene skal departementene blant annet vurdere risiko, sårbarhet og robusthet for de aktuelle kritiske samfunnsfunksjonene. Utvalget mener det vil være hensiktsmessig å bygge på disse etablerte strukturene, også for identifisering av grunnleggende nasjonale funksjoner og virksomheter som vil falle inn under den nye lovens virkeområde. Som nevnt innledningsvis, mener utvalget at de enkelte departementene – i tråd med ansvarsprinsippet – bør ha det primære ansvaret for forebyggende sikkerhet innenfor sitt myndighetsområde. Sektorspesifikk kunnskap og kompetanse er av sentral betydning for å kunne identifisere de funksjoner og virksomheter som er av grunnleggende nasjonal betydning i den enkelte samfunnssektor. En avgjørende forutsetning for at en slik systematikk skal fungere i praksis, er at de enkelte fagdepartementene er sitt ansvar bevisst og følger opp det ansvaret de tillegges gjennom loven. For enkelte departementer innebærer dette behov for kompetanseheving på forebyggende sikkerhet.

Fordi det finnes en etablert systematikk og strukturer for departementenes arbeid med samfunnssikkerhet og beredskap å bygge på, vil systematikken for identifisering og utvelgelse av virk-

[50] Forskrift 15. juni 2012 nr. 535, Instruks for departementenes arbeid med samfunnssikkerhet og beredskap. Justis- og beredskapsdepartementets samordningsrolle, tilsynsfunksjon og sentral krisehåndtering.

somheter som omfattes av loven sannsynligvis ikke innebære noen vesentlig større ressursbruk hos de enkelte departementene.

Gjensidige avhengigheter mellom virksomheter, og mellom samfunnssektorer, medfører samtidig et behov for at noen ivaretar et helhetlig og sektorovergripende perspektiv. Dette både for å kunne fange opp sektorovergripende avhengigheter som det enkelte fagdepartement ikke nødvendigvis har forutsetninger for å kunne identifisere, og for å kunne bidra med faglig bistand og kvalitetssikring av det enkelte departements identifisering innen egen sektor.

Også trusselbildet de enkelte virksomhetene står overfor, særlig innenfor cyber-domenet, er i mange tilfeller av sektorovergripende karakter. Både behovet for informasjonsdeling om slike trusler på tvers av samfunnssektorene, og etablering av sikkerhetstiltak for å forebygge disse truslene, underbygger behovet for å ivareta et helhetlig og sektorovergripende ansvar. I tillegg vil det kunne være selvstendige rettssubjekter som ikke naturlig faller inn under et fagdepartements myndighetsområde. For disse virksomhetene vil det være nødvendig å etablere en mekanisme for identifisering og utvelgelse på lik linje med det enkelte fagdepartements myndighet i egen sektor. Dette er et tiltak som sannsynligvis vil kreve ressursbruk hos den aktøren som skal ivareta et slikt ansvar. Utvalget foreslår at et slik sektorovergripende ansvar tillegges funksjonen Nasjonal sikkerhetsmyndighet.

Funksjonen Nasjonal sikkerhetsmyndighet vil ha en bedre oversikt over sektorovergripende avhengigheter enn de enkelte fagdepartement. Utvalget mener derfor det vil være nødvendig at Nasjonal sikkerhetsmyndighet fremmer begrunnede forslag om virksomheter som bør underlegges sikkerhetsloven til fagdepartementene.

I tillegg mener utvalget at funksjonen Nasjonal sikkerhetsmyndighet burde ha anledning til å påklage tilfeller der den mener at departementenes identifisering og utvelgelse av virksomheter omfattet av loven, er uforsvarlig.

Departementenes og funksjonen Nasjonal sikkerhetsmyndighete vedtak om at selvstendige rettssubjekter omfattes av loven, vil være inngripende overfor den enkelte virksomhet. Utvalget mener derfor det bør etableres tilfredsstillende rettssikkerhetsgarantier for slike vedtak, både i form av at den enkelte virksomhet har rett til å bli hørt før vedtak fattes og at de har anledning til å påklage en slik avgjørelse til et uavhengig tvisteorgan.

Utvalget foreslår at det etableres et eget tvisteorgan, som både kan behandle klager fra selvstendige rettssubjekter som det blir fattet vedtak overfor, og klager fra funksjonen Nasjonal sikkerhetsmyndighet der et departements identifisering og utvelgelse av virksomheter vurderes som uforsvarlig. De nærmere vurderingene rundt hvordan et slikt tvisteorgan bør innrettes er omtalt i kapittel 7.7.7.

7.7.2 Tverrsektorielle scenarier

Som nevnt i kapittel 7.6, har Forsvarets forskningsinstitutt (FFI) i sin utredning til utvalget anbefalt at det bør etableres nasjonale tverrsektorielle scenarier som dekker hele krisespekteret, som grunnlag for blant annet utpeking av skjermingsverdige objekter. FFI mener at slike nasjonale scenarier bør organiseres i overordnede scenarioklasser og legges til grunn for etablering av verdivurdering, ROS-analyser, forebyggende sikkerhetstiltak, samt beredskapsøvelser.

Utvalget er enig med FFI i at det bør etableres tverrsektorielle scenarier som er relevante for sikkerhetslovens virkeområde. En verdivurdering basert på de overordnede kriteriene som fremgår av loven, vil i begrenset grad kunne gi veiledning for utøvelsen av de enkelte fagdepartementenes ansvar etter loven. Utvalget tror en scenariobasert tilnærming, på linje med det DSB gjør i Nasjonalt risikobilde og Forsvaret gjør for sine interne planprosesser, vil kunne bidra til at en ny sikkerhetslov får et presist nedslagsfelt. Slike scenarier bør derfor legges til grunn både for identifisering av grunnleggende nasjonale funksjoner og for identifisering og utvelgelse av virksomheter som er av kritisk betydning for understøttelsen av disse funksjonene. Utvalget finner det ikke naturlig å foreslå en lovfesting av plikten til å utvikle slike scenarier, men anbefaler en tilnærming for den videre implementeringen av loven.

I tråd med FFIs anbefalinger, mener utvalget at slike scenarier bør utvikles gjennom et samarbeid mellom Justis- og beredskapsdepartementet og Forsvarsdepartementet, i nær kontakt med øvrige berørte departementer. I tillegg mener utvalget at de aktuelle fagmyndighetene bør ha en sentral rolle som premissgivere for slike scenarier.

7.7.3 Funksjonen Nasjonal sikkerhetsmyndighet

Utvalget har lagt til grunn for sitt arbeid at funksjonen Nasjonal sikkerhetsmyndighet skal videre-

Boks 7.3 Sikkerhetsmyndighet versus Nasjonal sikkerhetsmyndighet

Utvalget legger følgende begrepsbruk til grunn for den videre fremstillingen:

- Sikkerhetsmyndigheten er den funksjon som omtales i utvalgets lovforslag.
- Nasjonal sikkerhetsmyndighet er den funksjonen som omtales i gjeldende sikkerhetslov.
- Direktoratet Nasjonal sikkerhetsmyndighet omtales i den videre utredningen som NSM.

føres. Etableringen av funksjonen Nasjonal sikkerhetsmyndighet var i sin tid et utslag av blant annet NATOs krav overfor medlemsnasjonene til å ha en såkalt National Security Authority (NSA), med det overordnede ansvaret for å ivareta sikkerheten for NATO-gradert informasjon.[51] Norge er således forpliktet til å ha en slik funksjon, og utvalget mener uansett at en sentral fagmyndighet for forebyggende sikkerhet er viktig for å kunne ha en helhetlig tilnærming til sikkerhetsarbeidet på tvers av samfunnssektorene. Dette vil også kunne bidra til å sikre en effektiv utnyttelse av ressursene innenfor forebyggende sikkerhet. For å unngå uklarheter mellom funksjonen Nasjonal sikkerhetsmyndighet, og direktoratet med samme navn, foreslår utvalget at selve funksjonen i loven benevnes *Sikkerhetsmyndigheten*.

Utvalgets anbefaling om distinksjonen mellom funksjonen Sikkerhetsmyndigheten og direktoratet Nasjonal sikkerhetsmyndighet, er utelukkende av pedagogisk karakter. Utvalget mener det fortsatt vil være naturlig at direktoratet Nasjonal sikkerhetsmyndighet, ivaretar de oppgavene som tillegges Sikkerhetsmyndigheten i loven.

Utvalget har vurdert ulike alternativer til hvordan denne funksjonen bør innrettes, hvilke oppgaver den bør tillegges og hvordan samhandlingen med relevante sektormyndigheter bør være.

Utvalget foreslår at funksjonen Sikkerhetsmyndigheten på samme måte som i dag blir organisert etter en tradisjonell integrert modell, hvor flere roller ivaretas innenfor samme organisasjon. Utvalget har vurdert hvorvidt det burde skilles mellom rollen som fagmyndighet og rollen som tilsynsmyndighet. En av fordelene med et slikt klart organisatorisk skille vil være at det kan bidra til å sikre tilliten til tilsynsmyndighetens uavhengighet. Når utvalget likevel har kommet til at en tradisjonell integrert modell vil være den beste løsningen, skyldes dette i hovedsak at forebyggende sikkerhet mot tilsiktede uønskede hendelser er et relativt snevert fagfelt, hvor tilgangen til kvalifisert kompetanse er begrenset. En organisatorisk oppsplitting av rollene som fagmyndighet og tilsynsmyndighet kan, slik utvalget ser det, medføre at det skapes små og sårbare kompetansemiljøer. Alternativet vil være at det vil måtte bygges opp dupliserende kompetansemiljøer i henholdsvis fagmyndigheten og tilsynsmyndigheten, noe som også vil være en mer kostbar løsning. En integrert modell kan bidra til kompetanseoverføring og kompetanseheving mellom de ulike kompetansemiljøene innad i samme organisasjon, noe som igjen kan bidra til en samordnet og effektiv utnyttelse av kompetanse og ressurser. Utvalget forutsetter at Sikkerhetsmyndigheten, på samme måte som direktoratet NSM i dag, har nødvendige skiller mellom tilsynsrollen og andre roller innad i egen organisasjon.

Utvalget mener at Sikkerhetsmyndigheten bør tillegges ansvaret for å holde en tverrsektoriell oversikt over departementenes identifisering og utvelgelse av grunnleggende nasjonale funksjoner og virksomheter omfattet av loven, og i tillegg ha ansvaret for å identifisere virksomheter som ikke naturlig faller inn under et departementets myndighetsområde. Ansvaret for å ha en slik tverrsektoriell oversikt, vil være nødvendig for å kunne ivareta en helhetlig tilnærming til forebyggende sikkerhet.

En av hovedoppgavene for Sikkerhetsmyndigheten, i henhold til utvalgets forslag, er å gi informasjon, råd og veiledning til virksomheter underlagt loven. Konkret rådgivning overfor de enkelte virksomhetene bør være en helt sentral oppgave for Sikkerhetsmyndigheten innenfor alle de fagområder loven spenner over. Storbritannias *Centre for the Protection of National Infrastructure* (CPNI) sin rolle i det britiske systemet for beskyttelse av kritisk infrastruktur, kan tjene som eksempel på hvordan rådgivningsvirksomheten bør innrettes. CPNI driver utstrakt utadrettet og aktiv rådgivningsvirksomhet mot både offentlige myndigheter og andre virksomheter som råder over kritisk infrastruktur, og har gjennom sin organisatoriske tilknytning og sin fagkompetanse en betydelig tillit og innflytelse overfor de berørte aktørene. En slik løsning vil forutsette at Sikkerhetsmyndighetens kapasitet til å gi råd til virksomheter, dimensjoneres slik at virksomheter kan få rettidige og gode råd i sitt arbeid med forebyggende

[51] NATO Security Policy C-M, (2002), 49.

sikkerhet etter loven. Det bør i denne sammenheng også ses hen til andre nasjonale kompetansemiljøer, herunder Nasjonalt kompetansesenter for sikring av bygg (NKSB), som i dag er organisert som en enhet i Forsvarsbygg og Forsvarets kompetansesenter for objektsikring. Utvalget mener også det bør vurderes hvorvidt det er hensiktsmessig med flere slike kompetansemiljøer på samme fagområde i den grad de er dublerende, eller om denne kompetansen bør samordnes.

I tillegg til konkret rådgivning og veiledning overfor enkeltvirksomheter, bør Sikkerhetsmyndigheten – som i dag – ha ansvaret for å utarbeide og tilgjengeliggjøre generell informasjon om loven og hvordan denne skal praktiseres i form av rundskriv, veiledere etc. For å øke allmennhetens innsikt i, og tillit til, det forebyggende sikkerhetsarbeidet etter loven, mener utvalget slik generell informasjon i så stor utstrekning som mulig bør være offentlig tilgjengelig. Offentlig tilgjengelig informasjon vil også kunne komme virksomheter som ikke er underlagt sikkerhetsloven til nytte i virksomhetenes generelle sikkerhetsarbeid.

7.7.4 Tilsynsfunksjon og samhandling med relevante sektormyndigheter

Utvalget har i mandatet blitt bedt om å vurdere hvordan det skal føres tilsyn med etterlevelsen av ny lovgivning, herunder om det vil være hensiktsmessig å skille mellom tilsynsoppgaver og rollen som forvaltningsorgan. Som nevnt i kapittel 7.7.3 anbefaler utvalget at funksjonen Sikkerhetsmyndigheten organiseres etter en tradisjonell integrert modell, hvor flere roller ivaretas innenfor samme organisasjon. Utvalget har vurdert ulike alternativer for hvordan tilsynsfunksjonen etter den nye loven bør innrettes.

Et alternativ er å ha en sentral tilsynsmyndighet, med tilsynsansvar for alle virksomheter som omfattes av loven. En slik tilnærming vil i stor grad kunne legge til rette for en helhetlig tilnærming til forebyggende sikkerhet, og sikre et harmonisert sikkerhetsnivå, på tvers av ulike virksomheter og ulike samfunnssektorer.

På den andre siden vil en sentral tilsynsmyndighet i liten grad ha den bransjespesifikke kunnskapen som er nødvendig for å forstå de ulike samfunnssektorenes særegenheter og behov. En annen ulempe vil være at virksomhetene i de ulike samfunnssektorene vil bli utsatt for dupliserende tilsyn fra tilsynsmyndigheter med like, eller lignende, målgrupper og formål.

Et annet alternativ utvalget har vurdert, er hvorvidt tilsynsfunksjonen etter loven bør legges direkte til de enkelte sektortilsynene, og at Sikkerhetsmyndigheten gis en rent koordinerende funksjon opp mot de ulike sektortilsynene. En fordel med et slikt delegert tilsyn, er at dette vil være i tråd med nærhetsprinsippet og ansvarsprinsippet. Som nevnt tidligere utgjør disse prinsippene tunge føringer for hele samfunnets sikkerhets- og beredskapsarbeid. Et delegert tilsyn vil også kunne bidra til å legge til rette for at tilsynsobjektene ikke utsettes for dupliserende tilsyn.

Delegert tilsynsmyndighet – i tråd med ansvarsprinsippet – innebærer også at man vil kunne få et helhetlig eierskap til hele sektorens sikkerhetsarbeid, samlet i et tilsyn. Andre sikkerhetsfaglige organer vil med en slik løsning i liten grad kunne komme inn fra sidelinjen og diktere sektorenes sikkerhetsarbeid med tilsyn og pålegg. Videre vil delegert tilsynsmyndighet være i tråd med nærhetsprinsippet. De som tar avgjørelsene har dermed trolig bedre kjennskap til virksomhetene enn en sentral sikkerhetsmyndighet.

Ulempen med et slikt rendyrket delegert tilsyn, er at det vil kunne bli en rekke ulike tilnærminger og standarder for tilsyn av sikkerhetsarbeidet rettet mot tilsiktede hendelser i de ulike samfunnssektorene. Det vil også kunne vanskeliggjøre den helhetlige tilnærmingen til forebyggende sikkerhet etter loven på tvers av samfunnssektorene, som loven for øvrig legger opp til.

Utvalget har kommet til at det beste vil være å etablere en tilsynsmodell som både ivaretar målet om en helhetlig og tverrsektoriell tilnærming til forebyggende sikkerhet, samtidig som samfunnssektorenes særegenheter og behov ivaretas i tilstrekkelig grad.

I samfunnssektorer der det finnes sektormyndigheter med tilsynsfunksjoner som omfatter beskyttelse av informasjon, objekter eller infrastruktur, bør disse føre tilsyn med virksomheter som omfattes av loven i den aktuelle sektor. Hvorvidt det finnes relevante og tilstrekkelig kompetente sektormyndigheter i den aktuelle sektor, bør etter utvalgets oppfatning avgjøres av det enkelte fagdepartement – i tett samarbeid med Sikkerhetsmyndigheten.

I samfunnssektorer der det ikke finnes slike sektormyndigheter, eller de aktuelle sektormyndighetene ikke innehar den kompetansen som er nødvendig for å ivareta tilsynsfunksjonen etter loven, bør tilsynsansvaret legges til Sikkerhetsmyndigheten.

For å sikre en helhetlig, samordnet og tverrsektoriell tilnærming til forebyggende sikkerhet foreslår utvalget at Sikkerhetsmyndigheten gis

myndighet til å føre tilsyn med sektormyndigheter tillagt tilsynsansvar etter loven.

For departementsfelleskapet bør Sikkerhetsmyndigheten som i dag ha ansvaret for å føre tilsyn med departementenes etterlevelse av loven.

En slik tilnærming forutsetter et tett og nært samarbeid mellom Sikkerhetsmyndigheten og de aktuelle sektormyndighetene. Utvalget foreslår også å lovfeste en samhandlingsplikt mellom Sikkerhetsmyndigheten og aktuelle sektormyndigheter. Denne samhandlingen foreslås formalisert gjennom en samarbeidsavtale som nærmere fastlegger samhandlingen. Det kan her tenkes løsninger der forholdet mellom Sikkerhetsmyndigheten og sektormyndigheten kan variere på ulike fagområder. En slik avtale kan også regulere sektormyndighetenes bruk av kompetanse fra Sikkerhetsmyndigheten på enkelte områder, eksempelvis informasjonssikkerhet.

For å ivareta sitt ansvar som sektorovergripende myndighet, bør Sikkerhetsmyndigheten gis myndighet til å utarbeide grunnleggende kriterier for hvordan tilsyn etter loven skal innrettes og gjennomføres. Med et delegert tilsynsansvar i enkelte samfunnssektorer vil det være nødvendig med slike grunnleggende kriterier for å sikre en mest mulig enhetlig tilnærming i de ulike sektorene. Sikkerhetsmyndigheten bør også ha en sentral rolle i opplæringen av tilsynspersonell hos de relevante sektortilsynene, slik at personellet har den nødvendige sikkerhetsfaglige kompetanse for gjennomføring av tilsyn etter loven.

Sikkerhetsmyndighetens ansvar for å ha et sektorovergripende perspektiv forutsetter tilgang til informasjon om sikkerhetstilstanden i de ulike samfunnssektorene hvor de selv ikke har et direkte tilsynsansvar. Utvalget foreslår derfor en plikt for sektormyndigheter med tilsynsansvar etter loven til å orientere Sikkerhetsmyndigheten om hovedfunn fra gjennomførte tilsyn. En slik rapporteringsplikt fra sektormyndighetene til Sikkerhetsmyndigheten, vil kunne innebære noe økt ressursbruk. Der det gjøres funn av betydning av sektormyndigheten, vil dette sannsynligvis uansett måtte dokumenteres, og det antas derfor at den økte ressursbruken vil være beskjeden.

Dersom virksomhetene ikke oppfyller sine plikter etter loven, har tilsynsmyndighetene myndighet til å gi pålegg om gjennomføring av tiltak. For samfunnssektorer hvor det finnes relevante sektormyndigheter med tilsynsansvar, vil påleggsmyndigheten tilligge den aktuelle sektormyndigheten. Utvalget forslår også at Sikkerhetsmyndigheten gis påleggsmyndighet overfor de sektormyndighetene som har tilsynsansvar etter loven. Formålet med en slik påleggsmyndighet er å kunne gripe inn overfor en sektormyndighet dersom det skulle vise seg at sikkerhetsnivået i den aktuelle samfunnssektoren utvikler seg på en utilfredsstillende måte.

Slik utvalget ser det er tilsynsmyndighetens virkemiddelportefølje etter dagens sikkerhetslov ikke tilfredsstillende overfor virksomheter som ikke følger opp kravene etter lov og forskrift. Tilsynsmyndigheten har i medhold av dagens lov § 9 første ledd bokstav c), myndighet til å gi pålegg om forbedringer dersom avvik avdekkes. Dersom slike pålegg ikke følges opp av den enkelte virksomhet, er anmeldelse det eneste virkemidlet tilsynsmyndigheten har tilgjengelig. Terskelen for å gå til anmeldelse av en virksomhet, vil i de fleste tilfeller være høy. Utvalget mener derfor at tilsynsmyndighetens virkemiddelportefølje bør utvides ved at det gis myndighet til å ilegge tvangsmulkt dersom det avdekkes brudd på regelverket, eller der pålegg ikke følges opp innen en gitt tidsfrist. I nærmere angitte tilfeller, bør tilsynsmyndigheten også kunne ilegge overtredelsesgebyr ved brudd på regelverket. På samme måte som for påleggsmyndigheten, foreslår utvalget at myndigheten til å ilegge tvangsmulkt og overtredelsesgebyr bør legges til den myndigheten som er tildelt tilsynsansvaret.

7.7.5 Informasjonsdeling

En grunnleggende forutsetning for at virksomheter skal kunne gjøre en tilfredsstillende risiko- og sårbarhetsanalyse, og iverksette riktige og forsvarlige sikkerhetstiltak, er at de har tilgang til tidsriktig og relevant informasjon om hvilke trusler de er utsatt for. Utvalget har gjennom sitt arbeid fått et klart inntrykk av at etterspørselen av slik trusselinformasjon er stor, også fra virksomheter som i dag forvalter infrastruktur av kritisk betydning for grunnleggende nasjonale funksjoner. Det er utvalgets inntrykk at denne utfordringen også erkjennes fra myndighetens side.

For digital hendelseshåndtering har Lysne-utvalget påpekt viktigheten av å maksimere mulighetene innenfor det handlingsrommet som finnes for deling av informasjon, og har stilt spørsmål ved at det ikke har blitt etablert tilstrekkelig samarbeid og mekanismer for informasjonsdeling på dette området.[52] Utvalget er enig i vurderingen fra Lysne-utvalget, og mener at etablering av samarbeid og mekanismer for informasjonsdeling er viktig på alle fagområdene loven gjelder for.

[52] NOU 2015: 13, 272.

En forutsetning for å kunne dele gradert trusselinformasjon med virksomheter, er at disse er satt i stand til å kunne håndtere slik informasjon. Virksomhetene må da være omfattet av loven, og vil måtte ha personell som er sikkerhetsklarert og autorisert for tilgang til slik informasjon. I den utstrekning virksomhetene har behov for å behandle sikkerhetsgradert informasjon, vil de også måtte ha informasjonssystemer som er godkjent for dette.

Utvalget foreslår i lovforslaget at Sikkerhetsmyndigheten pålegges å legge til rette for at sektormyndigheter og virksomheter som er omfattet av loven får informasjon om trusselvurderinger og annen sikkerhetsinformasjon som er av betydning for deres etterlevelse av loven. Ettersom relevante trusselvurderinger ofte vil utarbeides av andre myndighetsaktører, herunder Politiets sikkerhetstjeneste og Etterretningstjenesten, vil Sikkerhetsmyndigheten i de fleste tilfeller ikke være eier av den informasjonen som skal deles. Sikkerhetsmyndigheten, bør imidlertid i kraft av sin funksjon ha en generell plikt til å koordinere tilgjengeliggjøring av slik informasjon og påse at det etableres nødvendige arenaer for dette. Slik arenaer bør etableres i tett samarbeid med aktuelle sektormyndigheter i de enkelte samfunnssektorene.

Utvalget mener løsningen vil bidra til å maksimere mulighetene for å kunne dele sikkerhetsrelevant informasjon med virksomheter som har behov for denne. Den vil således være et viktig bidrag til at både private og offentlige virksomheter blir satt i bedre stand til å kunne gjøre gode vurderinger og iverksette forsvarlige tiltak i sitt forebyggende sikkerhetsarbeid.

7.7.6 NorCERT og varslingssystemet for digital infrastruktur

Utvalget har vurdert hvorvidt det burde være en plikt for virksomheter underlagt loven å være tilknyttet varslingssystemet for digital infrastruktur. I likhet med de vurderingene som ble gjort i Prop. 97 L (2015–2016), mener imidlertid utvalget at dagens finansieringsmodell for VDI-samarbeidet gjør det utfordrende å lovfeste en slik plikt. Utvalget støtter derfor regjeringens tilnærming om at en eventuell lovfesting av en slikt plikt, bør ses i sammenheng med den fremtidige finansieringsmodellen for VDI. Utvalget vil i den forbindelse også fremheve viktigheten av at et slikt arbeid igangsettes raskt.

Videreføringen av NorCERT-funksjonen foreslås regulert som en egen bestemmelse. Dette skyldes utelukkende at den nasjonale responsfunksjonen er en operativ funksjon, som ikke naturlig faller inn under de øvrige fagmyndighetsoppgavene som er foreslått tillagt Sikkerhetsmyndigheten. Utvalget har ikke vurdert om responsfunksjonen organisatorisk skal plasseres andre steder enn i dag.

Utvalget mener det er viktig at virksomheter som råder over digital infrastruktur av kritisk betydning for grunnleggende nasjonale funksjoner får tilbud om, og anbefales å tilknytte seg dagens VDI-samarbeid. Dette forutsetter at NorCERT/VDI kapasitetsmessig innrettes slik at alle relevante aktører gis anledning til slik tilknytning.

7.7.7 Tvisteorgan

Som nevnt over mener utvalget det er behov for å etablere et tvisteorgan som kan ta stilling til klager fra virksomheter som blir underlagt loven ved enkeltvedtak, og til klager fra Sikkerhetsmyndigheten på departementenes etterlevelse av loven. Formålet med tvisteorganets virksomhet er å komme frem til de samfunnsmessig beste løsningene i et helhetsperspektiv.

En grunnleggende utfordring med dagens system for forebyggende sikkerhet etter gjeldende sikkerhetslov er, slik utvalget ser det, at det ikke finnes noen form for mekanisme for å avklare uenigheter mellom sikkerhetsmyndighetene og relevante sektormyndigheter. Justis- og beredskapsdepartementet har det sektorovergripende ansvaret for forebyggende sikkerhet og beredskap for de sivile samfunnssektorene, men er i liten grad gitt myndighet til å kunne instruere de ulike fagdepartementene i deres arbeid.

Etter dagens sikkerhetslov har Nasjonal sikkerhetsmyndighet det utøvende ansvaret på vegne av Forsvarsdepartementet og Justis- og beredskapsdepartementet. Men heller ikke Nasjonal sikkerhetsmyndighet, eller de to departementene NSM har fått delegert sin myndighet fra, har noen instruksjonsmyndighet overfor det øvrige departementsfellesskapet.

Sett hen til dagens organisering av statsforvaltningen, og den strenge praktiseringen av sektorprinsippet, mener utvalget det vil være vanskelig å tillegge et enkelt departement en myndighet til å treffe vedtak overfor det øvrige departementsfellesskapet. Utvalget anbefaler derfor at det etableres et eget kollegialt tvisteorgan som gis myndighet til å treffe vedtak i klagesaker etter loven.

Konkret forslår utvalget at Kongen gis myndighet til å peke ut et kollegialt organ med fem medlemmer. Ved oppnevningen av medlemmer

foreslår utvalget at det i tillegg til sikkerhetsfaglig kompetanse, skal legges vekt på kompetanse innen personvern og selvstendige rettssubjekters rettssikkerhet, jf. den foreslåtte formålsbestemmelsen i § 1-1.

Det vil være både effektivt og ha kompetansemessige fordeler om organet knyttes til eksisterende strukturer i sentralforvaltningen. Et naturlig valg i denne sammenheng vil være å etablere tvisteorganet under Regjeringens sikkerhetsutvalg (RSU) eller Kriserådet. Tvisteorganet bør derfor sannsynligvis ledes av en representant på høyt embetsnivå fra SMK.

En slik konstruksjon vil også fordre en sekretariatsfunksjon med ansvar for saksforberedelse av klagesakene for organet. Utvalget mener en slik sekretariatsfunksjon burde kunne tillegges det nyoppnevnte permanente sekretariatet for RSU. Dette vil imidlertid fordre en styrking av dette sekretariatet.

Tvisteorganet bør ha myndighet til å kunne treffe midlertidige vedtak i saker som må avgjøres raskt. Utvalget foreslår derfor at leder, eller nestleder, sammen med minst to medlemmer av organet, gis myndighet til å treffe slike vedtak i hastesaker. Et slikt midlertidig vedtak må da følges opp av en etterfølgende saksbehandling, hvor det opprinnelige vedtaket underlegges en tilfredsstillende utredning og saksbehandling. Av hensyn til allmennhetens tillit til myndighetene, bør tvisteorganet i lov pålegges å utarbeide en årlig rapport om sin virksomhet. Den årlige rapporten bør innrettes på en slik måte at den kan gjøres offentlig tilgjengelig.

7.7.8 Vedtaksmyndighet for Kongen i statsråd

Utvalget er enig i at det er behov for en hjemmel for å kunne stanse virksomhet som kan ha kritiske skadevirkninger for grunnleggende nasjonale funksjoner, se kapittel 7.2.3, og foreslår derfor å videreføre den vedtatte § 5a i en form som er tilpasset utvalgets lovforslag.

Slik bestemmelsen er utformet i regjeringens forslag, og omtalt i forarbeidene, vil myndighetene ha et bredt spillerom i forhold til hvilke typer vedtak som kan fattes med hjemmel i den aktuelle bestemmelsen. Formålet med bestemmelsen er å etablere en hjemmel i loven for å kunne stanse, eller nærmere regulere enkelte typer virksomhet som kan innebære en fare for grunnleggende nasjonale funksjoner. Vedtakene må nødvendigvis også være av en slik art og karakter at de forbygger slik aktivitet, noe som vil kunne variere ut fra hvilken type aktivitet det er tale om.

Samtidig mener utvalget at bestemmelsens inngripende karakter gjør det nødvendig å etablerer ytterligere rettssikkerhetsgarantier enn det som følger av regjeringens forslag.

For det første mener utvalget at myndigheten til Kongen i statsråd bør avgrenses til å gjelde enkeltvedtak, det vil si vedtak som retter seg mot bestemte personer eller virksomheter eller nærmere avgrensede grupper av slike.

For det andre bør det kunne påvises med stor grad av sannsynlighet at den aktuelle aktiviteten vil kunne få slike skadevirkninger at det er tvingende nødvendig å gripe inn. Bevisbyrden for at aktiviteten er av en slik alvorlighetsgrad, vil påligge myndighetene.

For det tredje mener utvalget at det ved avgjørelsen av hvilke vedtak som skal treffes, må påligge myndighetene et uttrykkelig forholdsmessighetskrav. I dette ligger en plikt til å vurdere vedtakets varighet, og forholdsmessigheten mellom vedtaket og den risiko aktiviteten utgjør.

Før vedtak fattes må saken utredes så godt som tiden tillater det. I denne utredningsplikten ligger en plikt til å innhente rådgivende uttalelser fra relevante organer, herunder PST, Etterretningstjenesten og NSM. I den utstrekning det er mulig bør også berørte parter få anledning til å uttale seg. Dersom tidskritiske forhold medfører at ordinære krav til utredning ikke kan følges, bør det gjennomføres en etterfølgende utredning for å sikre at vedtaket er fattet på et korrekt grunnlag.

Utvalget foreslår at det i forskriftsarbeidet også vurderes hvorvidt det vil være enkelte typer vedtak som vil kunne utløse rett til kompensasjon til personer og virksomheter som får sin rettslige posisjon svekket som følge av vedtak fattet i medhold av bestemmelsen. Med kompensasjon menes i denne sammenheng ikke nødvendigvis kompensasjon i form av erstatning. Også andre virkemidler vil kunne være aktuelle som avbøtende tiltak.

Etter utvalgets oppfatning fremstår det som relativt klart at vedtak som innebærer en tvangsavståelse av eiendom, der eiendomsretten overføres til andre, vil kunne utløse erstatningsplikt for myndighetene etter Grunnloven § 105.

Når det gjelder vedtak som innebærer en rådighetsinnskrenkning, vil det måtte gjøres en konkret helhetsvurdering av om inngrepet fremstår som sterkt urimelig, jf. blant annet Rt. 2005 s. 469. På generelt grunnlag mener imidlertid utvalget at denne type vedtak, ut fra at hensynet til nasjonal sikkerhet som hovedregel ikke vil frem-

stå som sterkt urimelig verken overfor allmennheten eller for den vedtaket retter seg mot. Formålet med et slikt vedtak vil være å hindre planlagte eller pågående tilsiktede uønskede hendelser, som kan ramme grunnleggende nasjonale funksjoner. Utvalget vil også presisere at bestemmelsen må ses på som en beredskapshjemmel for ekstraordinære tilfeller. Forholdet til Grunnloven, den europeiske menneskerettighetskonvensjonen (EMK) med videre, bør vurderes konkret i det enkelte tilfelle der det blir aktuelt å bruke bestemmelsen.

Vedtak fattet av Kongen i statsråd etter denne bestemmelsen, kan ikke påklages til tvisteorganet. Utvalget mener det vil by på konstitusjonelle utfordringer dersom et vedtak fra Kongen i statsråd skal kunne påklages til et organ som er utpekt av Kongen. Personer eller andre rettssubjekter som blir berørt av et slikt vedtak, vil således være henvist til å ta rettslige skritt for eventuelt å få overprøvd vedtaket.

7.7.9 Generelle krav til forebyggende sikkerhet

Utvalgets forslag til ny lov er gjennomgående basert på at det stilles funksjonelle krav til virksomhetene som omfattes av loven. Den enkelte virksomhet skal, basert på en risiko- og sårbarhetsanalyse, iverksette de nødvendige sikkerhetstiltakene. Så lenge tiltakene tilfredsstiller grunnleggende krav til sikkerhetsnivå, kan virksomheten selv velge hvilke sikkerhetstiltak som er nødvendige.

Et sentralt forhold i utvalgets arbeid har vært hvilken detaljeringsgrad som er nødvendig for de kravene som oppstilles i loven. På den ene siden tilsier hensynet til den enkelte samfunnssektors særegenheter at kravene bør gjøres relativt overordnede. Et for detaljert sektorovergripende regelverk, vil kunne innebære risiko for at regelverket kommer i konflikt med relevant sektorregelverk på området. Enkelte utvalgsmedlemmer har også uttrykt bekymring for at en for detaljert lov kan skape problemer i form av dobbeltregulering. Utvalget har hatt en grundig diskusjon av disse problemstillingene.

Avgjørende for utvalgets vurdering og anbefaling har vært hensynet til virksomhetene, og spesielt selvstendige rettssubjekters behov for forutsigbarhet. En for vag og skjønnsmessig angivelse av hvilke krav som oppstilles etter loven, vil svekke virksomhetens mulighet til å forutberegne sin rettsstilling og til å kunne forstå konsekvensene av de krav som følger av loven. For å ivareta en slik forutberegnelighet er det nødvendig at loven trekker opp de ytre rammene, både for myndighetenes og virksomhetenes skjønnsutøvelse. Utvalget har derfor anbefalt som et generelt og gjennomgående krav at virksomhetene skal iverksette de sikkerhetstiltak som er nødvendige for å oppnå et forsvarlig sikkerhetsnivå. Forholdet til sektorregelverk er nærmere behandlet i kapittel 7.7.12.

At sikkerhetsnivået skal være *forsvarlig* er en rettslig standard som trekker opp de ytre rammene for hvilket handlingsrom virksomhetene har for etablering av sikkerhetstiltak. Hva som vil utgjøre et forsvarlig sikkerhetsnivå for den enkelte virksomhet, og på de enkelte fagfeltene loven dekker, vil måtte vurderes opp mot hva som anses som god faglig praksis på de enkelte fagområdene, herunder informasjons- og informasjonssystemsikkerhet, objekt- og infrastruktursikkerhet og personellsikkerhet. Den nærmere grensedragningen bør, slik utvalget ser det utvikles i samarbeid mellom Sikkerhetsmyndigheten og de aktuelle sektormyndighetene. Dette vil også gi mulighet til å kunne gjøre sektorspesifikke tilpasninger der det er behov.

I tillegg vil det være en avgjørende forutsetning for at den enkelte virksomhet skal kunne gjøre en forsvarlig risiko- og sårbarhetsanalyse, at det gis tilstrekkelig informasjon til at de forstår trusselbildet. Utvalgets forslag til mekanismer for å kunne tilgjengeliggjøre og dele relevant informasjon om trusselbildet, er et viktig virkemiddel for å sette den enkelte virksomhet i stand til å gjøre forsvarlige vurderinger.

I tillegg vil Sikkerhetsmyndighetens rådgivning være et sentralt bidrag til den enkelte virksomhets vurdering av hva som utgjør et forsvarlig sikkerhetsnivå, sett hen til den trusselen de står ovenfor.

Et annet element som er fremhevet i utvalgets forslag, er at kostnadene ved sikkerhetstiltak etter loven skal stå i et rimelig forhold til det som oppnås ved tiltaket. Rett og plikt til å gjøre vurderinger av samfunnets samlede nytte ved tiltaket, sett opp mot de kostnader sikkerhetstiltaket fører med seg er, slik utvalget ser det, en nødvendig konsekvens av forslaget om å justere lovens virkeområde. Som utvalget har vært inne på i kapittel 6 vil justeringen av lovens virkeområde sannsynligvis medføre at flere selvstendige rettssubjekter blir omfattet av loven. Økt sikkerhet vil føre til mange konsekvenser for ulike aktører, inkludert økonomiske. Det er en fare for at dersom virksomheten ikke gis anledning til å gjøre kost-/nyttevurderinger i forhold til hvilke sikkerhetstiltak

som bør og skal iverksettes, kan dette medføre at kostnadene ved å etablere sikkerhetstiltak blir uforholdsmessig høye. Spesielt for selvstendige rettssubjekter som blir omfattet av loven, vil det i ytterste konsekvens kunne virke konkurransevridende dersom disse blir pålagt å iverksette uforholdsmessig kostbare sikkerhetstiltak.

Hvorvidt virksomhetene etablerer tilfredsstillende og forsvarlige sikkerhetstiltak, vil også være gjenstand for tilsynsmyndighetenes kontroll etter loven. Sikkerhetsmyndigheten, og de aktuelle sektormyndighetene, har i loven en rekke virkemidler for å kunne påvirke sikkerhetsnivået hos den enkelte virksomhet. Utvalget vil presisere viktigheten av at «myke» virkemidler i form av informasjon om trusler, råd og veiledning som hovedregel bør forsøkes først, før det tilsynsmyndigheten eventuelt gir konkrete pålegg om iverksettelse av tiltak for å etterleve lovens krav. Også tilsynsmyndighetens pålegg overfor virksomhetene som er omfattet av loven skal være basert på en vurdering av samfunnsøkonomisk lønnsomhet – at tiltakenes samlede nytte for samfunnet overstiger kostnadene de fører med seg.

Ved utarbeidelse og gjennomføring av sikkerhetstiltak er det viktig at det tas hensyn til personvernet. Som redegjort for i kapittel 5 gjelder personopplysningsloven som utgangspunkt for alle typer virksomheter, herunder virksomheter som omfattes av sikkerhetsloven. Den nye personvernforordningens virkeområde favner imidlertid ikke så bredt. Utvalget har ikke fått signaler om at en revidert personopplysningslov vil få et virkeområde tilsvarende forordningen, og på den måten snevre inn virkeområdet i forhold til dagens lovgivning. Likevel, for å understreke viktigheten av og sikre at virksomheter underlagt sikkerhetsloven også for fremtiden tar hensyn til grunnleggende personvernprinsipper, mener utvalget at det i den nye loven bør henvises til prinsippene for behandling av personopplysninger, slik de fremgår av personvernforordningen artikkel 5. Det skal imidlertid ikke utelukkende tas personvernhensyn ved utarbeidelse og gjennomføring av sikkerhetstiltak. Loven viser derfor også til unntaksbestemmelsen i artikkel 23.

Utvikling av forsvarlighetsstandarden, kombinert med virksomhetenes og tilsynsmyndighetenes plikt til å gjøre vurderinger av samfunnets nytte sett i forhold til kostnadene, vil også være styrende for graden av risikoaksept etter den nye loven. Etter utvalgets vurdering er det ikke mulig, ønskelig eller hensiktsmessig å gjennomføre sikkerhetstiltak som vil eliminere risikoen for at tilsiktede uønskede hendelser inntreffer. Ved å etablere forsvarlige og kostnadseffektive sikkerhetstiltak, vil man imidlertid kunne redusere sannsynligheten for, og konsekvensene av, slike hendelser. I siste omgang vil det være opp til regjering og Stortinget å definere hvilken risiko som er akseptabel for våre grunnleggende nasjonale funksjoner. Utvalget mener at forslaget om å etablere tverrsektorielle scenarioer, som grunnlag for virksomhetenes risiko og sårbarhetsanalyser, og for hvilke sikkerhetstiltak som skal iverksettes, vil være et nyttig bidrag for å avgjøre hva som er akseptabel risiko.

For at myndighetene skal kunne danne seg et helhetlig bilde av sikkerhetsnivået og trusselbildet for de ulike virksomhetene og samfunnssektorene, mener utvalget det er nødvendig å pålegge virksomheter underlagt loven en plikt til å rapportere hendelser. Rapporteringslinjene bør i utgangspunktet følge fordelingen av tilsynsansvaret, slik at den enkelte virksomhet plikter å rapportere til den aktør som er tillagt tilsynsansvar etter loven. For å ivareta det sektorovergripende perspektivet, er det imidlertid også nødvendig at Sikkerhetsmyndigheten får tilgang til hendelsesrapportering fra alle samfunnssektorer. Utvalget har vurdert hvorvidt det vil være tilstrekkelig at den enkelte sektormyndighet pålegges å videreformidle slike varsler til Sikkerhetsmyndigheten, der dette vurderes som relevant. Dette vil imidlertid kunne medføre at de aktuelle sektormyndighetene blir et forsinkende ledd i rapporteringslinjen. I tillegg kan hendelser som blir vurdert som mindre relevante i en samfunnssektor, kunne være viktig informasjon for å forstå det helhetlige trusselbildet – noe sektormyndighetene ikke nødvendigvis har forutsetninger for vurdere. Utvalget anbefaler derfor at Sikkerhetsmyndigheten varsles parallelt i de tilfeller en sektormyndighet er tillagt tilsynsansvar etter loven. En slik dobbeltrapportering vil medføre noe økt ressursbruk hos Sikkerhetsmyndigheten, ved at kapasiteten for å motta og behandle slike varsler må være tilstrekkelig dimensjonert. Utvalget mener imidlertid at den sikkerhetsmessige gevinsten ved at Sikkerhetsmyndigheten har et mer fullstendig bilde over hendelser av sikkerhetsmessig betydning, overstiger de kostnadsmessige ulempene.

7.7.10 Forskriftsregulering

En rekke av bestemmelsene i utvalgets lovforslag legger opp til at det skal utarbeides et underliggende forskriftsverk innenfor de ulike fagområdene loven omhandler. Dette er en naturlig konsekvens av utvalgets forslag til innretning på loven,

som et overordnet rammeverk for forebyggende nasjonal sikkerhet. Forskriftsmyndigheten er i hovedsak foreslått lagt til Kongen. På særlige viktige spørsmål, har utvalget foreslått at forskriftsmyndigheten legges til Kongen i statsråd, det vil si at myndigheten ikke kan delegeres til det departement som innehar forvaltningsansvaret for loven.

Som nevnt tidligere er utvalgets forslag til ny lov gjennomgående basert på at det stilles funksjonelle krav til virksomhetene som omfattes av loven. Sett hen til utvalgets mandat om å foreslå et dynamisk og helhetlig lovgrunnlag som er relevant og robust med hensyn til dagens og fremtidens trusselbilde, mener utvalget det er helt nødvendig at loven har en funksjonell innretning. Funksjonelle krav, hvor det i stor grad overlates til den enkelte virksomhet å iverksette de tiltak som er nødvendige for å oppnå et forsvarlig sikkerhetsnivå, vil også bidra til en kostnadseffektiv regulering og implementering av forebyggende sikkerhet.

Utvalget vil presisere viktigheten av at det i det videre forskriftsarbeidet i så stor utstrekning som mulig benyttes funksjonelle krav. Dersom et funksjonelt innrettet lovverk følges opp av et detaljert og kravsbasert forskriftsverk, frykter utvalget at loven ikke vil virke etter sin hensikt.

I lovforslaget legges det som nevnt opp til at det i utgangspunktet er opp til den enkelte virksomhet å innrette sikkerhetstiltakene slik at et forsvarlig sikkerhetsnivå oppnås, hvor kostnaden ved tiltakene skal stå i et rimelig forhold til det som oppnås. I dette ligger det også et klart element av risikoaksept, hvor den enkelte virksomhet på bakgrunn av en risiko- og sårbarhetsanalyse må ta stilling til hvor mye risiko de er villige til å akseptere. Den rettslige standarden *forsvarlig sikkerhetsnivå* vil her uansett fungere som en skranke for virksomhetens risikoaksept, som også gir tilsynsmyndighetene anledning til å korrigere virksomheten der sikkerhetsnivået vurderes som uforsvarlig. I tillegg vil en slik funksjonell innretning kunne legge til rette for sektorspesifikke tilpasninger.

Dersom det i det underliggende forskriftsverket fastsettes detaljerte krav til hvordan et *forsvarlig sikkerhetsnivå* skal oppnås, vil mulighetene både for å kunne gjøre konkrete samfunnsøkonomiske lønnsomhetsvurderinger, og for å gjøre sektorspesifikke tilpasninger der det er behov for dette, bli sterkt redusert.

Forskriftsarbeidet bør også gjøres i tett samarbeid mellom ansvarlig departement, Sikkerhetsmyndigheten og berørte sektordepartementer og -myndigheter. Utvalget vil i denne sammenheng vise til utredningsinstruksens krav[53] om at berørte departementer, og andre berørte aktører, involveres så tidlig som mulig i utredningsarbeidet. Lovforslagets sektorovergripende karakter tilsier at de aller fleste sektordepartementene, i større eller mindre grad, vil bli berørt av loven og dens underliggende forskrifter. Tidlig involvering av berørte aktører vil kunne bidra til at både sektorovergripende og sektorspesifikke hensyn ivaretas i det videre arbeidet med å utarbeide forskrifter etter loven.

7.7.11 Forvaltningsansvaret for loven

Utvalget skal i henhold til mandatet, og avhengig av lovens innhold og oppbygging, vurdere hvem som skal ha ansvar for den fremtidige forvaltning av loven og dens forskrifter. Ved vurderingen av hvilket departement som bør ha forvaltningsansvaret er det noen sentrale forhold som bør tas med i betraktningen.

Forvaltningsansvaret for loven innebærer for det første det overordnede ansvaret for å påse at loven etterleves. Forvaltningsansvaret innebærer også ansvar for å holde regelverket oppdatert, og eventuelt fremme forslag til endringer av loven. Det innebærer også myndighet til å kunne gi autoritative uttalelser om hvordan loven skal forstås. Normalt sett delegeres også Kongens myndighet etter loven til det departement som innehar forvaltningsansvaret for loven. Slik utvalget vurderer det, er det med dagens departementsinndeling bare to departementer som vil kunne ivareta et slikt forvaltningsansvar.

Forsvarsdepartementet innehar forvaltningsansvaret for dagens sikkerhetslov med underliggende forskrifter. Slik dagens lov har vært innrettet, med et sterkt fokus på statssikkerheten og beskyttelse av rikets selvstendighet og sikkerhet, og dermed et primært nedslagsfelt i militær sektor, har dette vært en naturlig og riktig løsning. Sikkerhetsloven har også sitt opphav i tidligere instrukser som i utgangspunktet gjaldt for Forsvarets virksomhet, basert på krav fastsatt av NATO, blant annet for håndtering av NATO-gradert informasjon. Selv om lovens formål og virkeområde utvides noe for bedre å reflektere den generelle samfunnsutviklingen, vil det vesentlige av lovens nedslagsfelt fortsatt ligge innenfor statssikkerhetsdomenet. Forsvarsdepartementets ansvar for, og kompetanse innenfor, det forsvars- og sikker-

[53] Instruks 19. februar 2016 nr. 184, Instruks om utredning av statlige tiltak (utredningsinstruksen).

hetspolitiske området taler for at forvaltningsansvaret for loven fortsatt bør tilligge Forsvarsdepartementet. Utvalgets lovforslag legger også opp til at loven fortsatt skal være harmonisert med de forpliktelser Norge har overfor NATO når det gjelder håndtering av sikkerhetsgradert informasjon.

På tross av utvidelsen av lovens virkeområde, vil fortsatt Forsvaret være største bruker av loven, både når det gjelder behandling av sikkerhetsgradert informasjon, klarering av personell og bruk av regelverket for sikkerhetsgraderte anskaffelser. Også dette taler for at forvaltningsansvaret bør beholdes av Forsvarsdepartementet.

En mulig betenkelighet utvalget ser ved at Forsvarsdepartementet fortsatt gis forvaltningsansvaret for loven, er at departementet i mindre utstrekning innehar den kompetansen som er nødvendig for å forstå de sivile samfunnssektorenes særegenheter og særegne behov.

På den andre siden vil lovforslagets innretning medføre at loven får et større nedslagsfelt i de sivile samfunnssektorene. Utvalget legger til grunn at de aller fleste nye virksomheter som vil bli omfattet av loven, vil være fra disse sivile sektorene. Justis- og beredskapsdepartementet har allerede i dag det samordnende ansvaret for samfunnssikkerheten og beredskapen på sivil side. En overføring av forvaltningsansvaret til Justis- og beredskapsdepartementet vil kunne bidra til å understøtte Justis- og beredskapsdepartementets ansvar på dette området, og vil kunne styrke departementets mulighet til å sette krav til de øvrige departementenes arbeid med forebyggende sikkerhet innen eget myndighetsområde.

En mulig betenkelighet utvalget ser ved en overføring av forvaltningsansvaret til Justis- og beredskapsdepartementet, er at statssikkerhetsperspektivet, altså ivaretakelse og beskyttelse av statens suverenitet og territorielle integritet, kan bli utvannet dersom dette utelukkende ses i sammenheng med det generelle arbeidet med samfunnssikkerhet og beredskap.

Samlet sett mener utvalget at de beste grunner taler for at Forsvarsdepartementet fortsatt bør ha forvaltningsansvaret for sikkerhetsloven. Avgjørende for utvalget syn på dette spørsmålet har vært at en effektiv forvaltning og oppfølging av sikkerhetsloven vil kreve god sikkerhetsfaglig kompetanse – spesielt innenfor det statssikkerhetsmessige domenet. Denne kompetansen ligger i dag i Forsvarsdepartementet. Forvaltningsansvaret må imidlertid, slik utvalget ser det, utøves i tett samarbeid med Justis- og beredskapsdepartementet, og dets samordnende ansvar for de sivile samfunnssektorene og særlige ansvar for beskyttelse av kritisk infrastruktur og kritiske samfunnsfunksjoner på sivil side. En slik samhandling vil også være i tråd med den ansvarsfordelingen som er fastsatt i Kronprinsregentens resolusjon av 4. juli 2003 etter dagens sikkerhetslov.

7.7.12 Forholdet til sektorlovgivning

Utvalget har vurdert hvorvidt forslaget til ny lov vil kunne komme i konflikt med ulike sektorregelverks regulering av forebyggende sikkerhet og beredskap. Utvalgets vurdering er at lovforslagets overordnede og funksjonelle innretning, sammenholdt med de foreslåtte mekanismene for ansvarsfordeling og samhandling mellom departementene, Sikkerhetsmyndigheten og relevante sektormyndigheter, gjør at lovforslaget vanskelig vil kunne komme i direkte konflikt med relevant sektorregelverk. At tilsynsansvaret legges til relevante sektormyndigheter, der slike finnes, gjør også at eventuelle uklarheter som måtte oppstå i relasjonen mellom sektorovergripende- og sektorspesifikt regelverk, vil kunne oppklares og løses på en tilfredsstillende måte.

At virksomheter i en samfunnssektor må forholde seg til flere ulike regelverk, er ikke unikt for forebyggende sikkerhet. I den videre operasjonaliseringen av kravene som stilles, vil virksomhetene måtte ta hensyn til regelverk som stiller krav til sikkerhet både når det gjelder tilsiktede og utilsiktede hendelser.

Kapittel 8
Informasjonssikkerhet

8.1 Innledning

Den teknologiske utviklingen og digitaliseringen siden dagens sikkerhetslov ble vedtatt har hatt store konsekvenser både for samfunnet som helhet og for virksomheter av betydning for nasjonal sikkerhet. Blant annet har digitaliseringen av samfunnet bidratt til større grad av tverrsektorielle avhengigheter, mer elektronisk behandling av sikkerhetsgradert materiale og økt IKT-avhengighet for virksomheter med ansvar for grunnleggende nasjonale funksjoner.

Det er slått fast i mandatet, ble gjentatt og ytterligere belyst av Lysne-utvalget, og er også blitt bekreftet gjennom utvalgets arbeid, at digitale angrep utgjør en alvorlig og økende trussel mot norske verdier, og at det stadig oppdages nye sårbarheter i våre IKT-systemer. Dagens regelverk om informasjonssikkerhet er ikke godt nok tilpasset det digitaliserte samfunnet og den raske utviklingen.

Samfunnsendringene gjør det nødvendig å videreutvikle regelverket om informasjonssikkerhet for virksomheter som er underlagt sikkerhetsloven. En ny sikkerhetslov må ta høyde for fortsatt rask utvikling i samfunnet generelt og IKT spesielt. Den nye loven må videre anerkjenne at grunnleggende nasjonale funksjoner i stor utstrekning er avhengig av velfungerende IKT-systemer og -infrastruktur. Dette gjelder:

- informasjonssystemer som behandler sikkerhetsgradert informasjon, som uttrykkelig skal beskyttes etter dagens lov
- andre IKT-systemer som er av kritisk betydning for grunnleggende nasjonale funksjoner. Det kan være informasjons- og kommunikasjonssystemer i en virksomhet som er så viktig at dersom de ikke virker, evner ikke virksomheten å opprettholde sin kritiske rolle i understøttelsen av en grunnleggende nasjonal funksjon
- kontroll- og styringssystemer som har en avgjørende rolle for styring av viktige prosesser og tjenesteleveranser i ulike sektorer som følge av økt digitalisering, eksempelvis i infrastruktur for telekom og strømproduksjon.

De to sistnevnte IKT-systemene er av kritisk betydning for grunnleggende nasjonale funksjoner, men beskyttes ikke direkte i dagens lov – med mindre de er utpekte som skjermingsverdige objekter etter objektsikkerhetsregelverket.

Utvalgets mål med nye regler for informasjonssikkerhet er at reglene skal være tilpasset digitaliseringen av samfunnet. Reglene må legge til rette for et forsvarlig og tilpasset sikkerhetsnivå for den enkelte virksomhet, både sett opp imot dagens trussel- og sårbarhetsbilde og fremtidige utfordringer.

Dagens sikkerhetslov beskytter informasjon særlig mot faren for at den blir kjent for uvedkommende. Utvalget har vurdert om ivaretakelse av informasjonens integritet og tilgjengelighet er tilstrekkelig ivaretatt i dagens sikkerhetslovgivning.

Utvalget har også sett nærmere på om dagens bestemmelser om informasjonssystemsikkerhet gir god nok beskyttelse. Utvalget har herunder drøftet hvor i loven de nye bestemmelsene om beskyttelse av informasjonssystemer bør plasseres. IKT-systemer som behandler sikkerhetsgradert informasjon har nær sammenheng med informasjonssikkerhet, mens kontroll- og styringssystemer hører mer naturlig sammen med infrastruktursikkerhet. Imidlertid er det også en del fellesnevnere, hvilket taler for en felles behandling av alle typer IKT-systemer.

En neste utfordring har vært detaljeringsnivået på bestemmelsene. Det er svært ulike IKT-systemer som skal beskyttes og reglene skal fungere over tid – to momenter som taler for et lavt detaljeringsnivå. Samtidig er det viktig at regler som har personvernkonsekvenser er så detaljerte at det er mulig å forstå hva de faktisk innebærer – et moment som tilsier et høyere detaljeringsnivå.

Mandatet nevner særskilt at utvalget må vurdere behovet for å beskytte informasjon som er sensitiv, men ugradert. Utvalget mener dette først

og fremst må ses i tilknytning til lovens virkeområde og tydeligere regler om beskyttelse av IKT-systemer.

Ifølge mandatet skal utvalget «se hen til EU-kommisjonens forslag av 7. februar 2013 til direktiv om tiltak for å sikre et høyt felles nivå for nettverk- og informasjonssikkerhet i EU». Utvalget er også bedt om å identifisere eventuelle behov for en harmonisering av den fragmenterte lovreguleringen av informasjonssikkerhet, samt å foreslå en modernisering av beskyttelsesinstruksen.

Når informasjon sikkerhetsgraderes, gjøres den samtidig utilgjengelig for allmennheten. Offentlighetsprinsippet er viktig og må ivaretas. Utvalget vurderer derfor det nye lovforslaget opp mot offentlighetsloven.

Det finnes en rekke lover og forskrifter som regulerer informasjonssikkerhet i Norge. Noen regler er sektorovergripende og andre er sektorspesifikke. Sikkerhetsloven og forskrift om informasjonssikkerhet står helt sentralt for beskyttelse av informasjon som har betydning for nasjonal sikkerhet, og blir gjennomgått først. Videre vil utvalget behandle sektorovergripende- og sektorspesifikt regelverk.

8.2 Gjeldende sikkerhetslovs regulering

Informasjons- og informasjonssystemsikkerhet er regulert i sikkerhetsloven kapittel 4. Kapittelet inneholder helt grunnleggende bestemmelser om informasjonssikkerhet, som sikkerhetsgradering av informasjon, og enkelte bestemmelser om informasjonssystemsikkerhet, kryptosikkerhet og tekniske sikkerhetsundersøkelser.

Lovbestemmelsene er relativt generelle og samtlige inneholder forskriftshjemmel. I § 13 om sikkerhetsmessig godkjenning og § 14 om kryptosikkerhet er forskriftsmyndigheten gitt til Nasjonal sikkerhetsmyndighet. For øvrige bestemmelser er forskriftsmyndigheten gitt til Kongen.

Mange av forskriftsbestemmelsene innenfor informasjons- og informasjonssystemsikkerhet er samlet i informasjonssikkerhetsforskriften.[1] Forskriften gir gjennom 12 kapitler detaljerte bestemmelser om sikkerhetsgradering, tilgang til sikkerhetsgradert informasjon, dokumentsikkerhet, informasjonssystemsikkerhet, fysisk sikring mot ulovlig inntrenging, administrativ kryptosikkerhet, kurerposttjeneste, sikring av blant annet konferanserom mot uønsket avlytting og innsyn, tekniske sikkerhetsundersøkelser, samt monitoring av og inntrengning i informasjonssystemer.

8.2.1 Informasjonssikkerhet

De grunnleggende prinsippene for hvordan sikkerhetsgradert informasjon skal håndteres er nedfelt i lovgivningen. Hovedelementene i reguleringen består av en verdivurdering for å bestemme hvilken informasjon som skal beskyttes, samt sikkerhetsgradering av skjermingsverdig informasjon og gjennomføring av passende sikkerhetstiltak.

I sikkerhetsloven § 12 pålegges den som får tilgang til sikkerhetsgradert informasjon taushetsplikt. Det fremgår av sikkerhetsloven § 11 at for å bestemme hvilken informasjon som skal beskyttes i henhold til loven, skal det foretas en verdivurdering og en sikkerhetsgradering ut fra informasjonens skadepotensiale dersom den blir kjent for uvedkommende:

a) STRENGT HEMMELIG nyttes dersom det kan få helt avgjørende skadefølger for Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.
b) HEMMELIG nyttes dersom det alvorlig kan skade Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.
c) KONFIDENSIELT nyttes dersom det kan skade Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.
d) BEGRENSET nyttes dersom det i noen grad kan medføre skadefølger for Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.

Systemet bygger på en forutsetning om en betydelig større grad av risikoaksept på det lavgraderte nivået sammenlignet med det høygraderte. Det nærmere innholdet i begrepet «Norges eller dets alliertes sikkerhet...» ble drøftet under kapittel 6.2.

Det er den som utsteder eller på annen måte tilvirker skjermingsverdig informasjon som plik-

[1] Forskrift 1. juli 2001 nr. 744 om informasjonssikkerhet.

ter å sørge for at informasjonen merkes med aktuell sikkerhetsgrad, jf. sikkerhetsloven § 11 andre ledd. Det ligger i dette for det første en plikt til å foreta en verdivurdering av informasjonen og for det andre en plikt til å merke informasjonen. Det skal ikke brukes høyere sikkerhetsgradering enn nødvendig. I bestemmelsens tredje og fjerde ledd er det gitt nærmere regler om graderingstid og inngåelse av sikkerhetsavtaler med andre nasjoner eller internasjonale organisasjoner.

Det andre sentrale vurderingstema i hva som utgjør den nedre grense for hvilken informasjon som skal beskyttes (BEGRENSET), er hva som ligger i uttrykket «i noen grad kan medføre skadefølger». Forarbeidene[2] gir noe veiledning:

> Forskjellen mellom KONFIDENSIELT («kan skade») og BEGRENSET («i noen grad kan medføre skadefølger») ligger etter dette først og fremst i at skaderisikoen kan være mindre sannsynlig og omfattende, og mer indirekte, når det gjelder informasjon som skal sikkerhetsgraderes BEGRENSET, enn for informasjon som skal sikkerhetsgraderes KONFIDENSIELT.

Forarbeidene trekker frem noen eksempler:

> Opplysninger som må skjermes for å forebygge alvorlige terrorhandlinger, selv om terrorhandlingene ikke utføres av eller for en fremmed makt e l og således ikke nødvendigvis vil direkte berøre rikets territorielle sikkerhet. En annen grunn til å medta begrepet er hensynet til situasjoner hvor norske vitale sikkerhetsinteresser gjør seg gjeldende i utlandet, eksempelvis hensynet til å forebygge alvorlige trusler mot sikkerheten til norske styrker som deltar i internasjonale fredsoperasjoner, hvis beskyttelse neppe kan sies å berøre rikets sikkerhet.

Den nedre grensen for informasjon som skal sikres må være av en slik art at den har et visst skadepotensiale. Ikke nødvendigvis for rikets territorielle sikkerhet, men helt essensielle og samfunnsviktige funksjoner må være utsatt.

Da verdivurderingen av informasjon viser at informasjonen, om den blir kjent for uvedkommende, har et visst skadepotensiale for nasjonal sikkerhet, gjelder sikkerhetsloven og dens forskrifter. Informasjonen skal merkes med sikkerhetsgraderingen BEGRENSET og behandles deretter. Høyere graderinger krever strengere sikkerhetstiltak, men også behandling av informasjon på det laveste nivået krever en rekke tiltak.

Personer som skal ha tilgang til informasjonen må autoriseres, og taushetsplikt inntrer. Informasjonssystemene og kryptosystemene som brukes til gradert informasjon må godkjennes. Nasjonal sikkerhetsmyndighet kan foreta tekniske sikkerhetsundersøkelser av virksomheten. Ved sikkerhetsgraderte anskaffelser må det inngås sikkerhetsavtale. Avtaler med utenlandske leverandører må godkjennes av Nasjonal sikkerhetsmyndighet. Plikter som følger av forskrift om sikkerhetsadministrasjon må følges. Informasjonssikkerhetsforskriften har regler om merking, journalføring, forsendelse, utlån, tilintetgjøring med mer av dokumenter. Forskriften stiller også systemtekniske og administrative krav til graderte informasjonssystemer, krav om fysisk sikring mot ulovlig inntrengning, samt krav til kryptosystemer som skal benyttes.

8.2.1.1 Informasjonssystemsikkerhet

Ut over plikten til at informasjonssystemer skal godkjennes før de kan behandle sikkerhetsgradert informasjon, jf. kapittel 8.2.1.2, følger de grunnleggende bestemmelsene om beskyttelse av informasjonssystemer av informasjonssikkerhetsforskriften kapittel 5. Det heter i forskriften § 5-1 at sikkerhet i informasjonssystemer skal vurderes opp mot de grunnleggende egenskapene autensitet, konfidensialitet, integritet og tilgjengelighet til systemets data og tjenester. Videre fremheves brukernes ansvarlighet for egne handlinger og tilliten til at sikkerhetstiltak er korrekt implementerte og ivaretar sikkerheten på en effektiv og hensiktsmessig måte. § 5-2 setter som hovedmål for sikkerheten en sikker plattform, sikker drift, vedlikehold og sikker hendelseshåndtering og gjenoppretting.

I forskiften §§ 5-3 og 5-4 gis det bestemmelser om hva som skal oppnås gjennom sikkerhetstiltak. For eksempel skal tilgjengelighet sikres ved at data beskyttes mot uønsket sletting og tjenester beskyttes mot uønsket reduksjon/stans. Tiltakene skal videre forebygge, detektere, reagere på, kontrollere sikkerhetsbrudd, samt gjenopprette informasjonssystemets sikre tilstand.

Sikkerhetsprinsipper som skal legges til grunn ved utarbeidelse av tiltak, følger av forskriften § 5-5, se tekstboks 8.1. Videre gis det i forskriften kapittel 5 regler om systemtekniske og administrative sikkerhetskrav, sikkerhetsgodkjenning

[2] Ot.prp. nr. 49 (1996–97) punkt 7.2.2

Boks 8.1 Informasjonssystem-sikkerhet – sikkerhetsprinsipper:

a) Minimalisme. Sikkerhetsrelevante funksjoner skal ikke ha mer funksjonalitet eller kompleksitet enn strengt nødvendig for å utføre sin tilsiktede oppgave.
b) Minste privilegium. Brukere og funksjoner skal bare tildeles rettigheter som er strengt nødvendige.
c) Redundans. Funksjoner skal ha ekstra kapasitet for å tåle overbelastning og utstyrssvikt.
d) Forsvar i dybden. Flere funksjoner skal ivareta samme sikkerhetsbehov.
e) Selvbeskyttelse. Funksjoner skal ikke ha unødige sikkerhetsmessige avhengigheter til andre sikkerhetsdomener. Dette gjelder både internt i systemet, for eksempel mellom avdelinger, og eksternt mot andre informasjonssystemer.
f) Kontrollert dataflyt. Informasjonsutveksling skal følge veldefinerte mønstre som er underlagt sentral kontroll.
g) Balansert styrke. Sikkerhetsnivået til funksjoner som ivaretar samme sikkerhetsbehov skal være tilnærmet likt på tvers av systemet.

av informasjonssystemer og sikkerhetsdokumentasjon.

8.2.1.2 Sikkerhetsmessig godkjenning av informasjonssystemer

Det er i forarbeidene lagt til grunn at sikkerhetsmessig kontroll av informasjonssystemer først og fremst skal skje i form av forutgående godkjenning. Det fremgår av sikkerhetsloven § 13 at Nasjonal sikkerhetsmyndighet, eller den de bemyndiger, må forhåndsgodkjenne informasjonssystemer som skal behandle sikkerhetsgradert informasjon. Informasjonssystemer som ikke behandler sikkerhetsgradert informasjon er ikke regulert i loven.

Det følger av informasjonssikkerhetsforskriften § 5-28 *Godkjenningsansvarlig* at det i utgangspunktet er virksomhetens leder som er godkjenningsansvarlig. Det fordrer imidlertid at systemet er lokalisert i Norge og at det ikke har forbindelse til andre systemer utenfor egen virksomhet, utenfor kontrollert område eller til utlandet. Avhengig av systemets operasjonsmåte, kan virksomhetslederen godkjenne systemer som skal behandle opp til og med HEMMELIG informasjon. Systemer som skal behandle STRENGT HEMMELIG informasjon godkjennes alltid av Nasjonal sikkerhetsmyndighet.

8.2.1.3 Monitoring

Etter at systemene er tatt i bruk kan de kontrolleres ved inspeksjon, monitoring og inntrengningstesting for å avdekke uregelmessigheter i behandlingen av gradert informasjon og undersøke systemenes motstandsdyktighet og sikkerhetstilstand.

Monitoring av informasjonssystemer som sikkerhetstiltak reguleres i sikkerhetsloven § 15 og informasjonssikkerhetsforskriften kapittel 11. Kort fortalt gis virksomheten anledning til å benytte seg av Nasjonal sikkerhetsmyndighets kompetanse for gjennomføring av dette spesifikke tiltaket.

Begrepet monitoring i sikkerhetslovens forstand innebærer ifølge forarbeidene kontroll av «tjenestlig kommunikasjon i og mellom informasjonssystemer, gjennom avlytting av tale eller avlesing av elektroniske signaler». Hensikten med monitoring er «å avdekke om det lagres, behandles eller kommuniseres informasjon med høyere sikkerhetsgrad eller skjermingsverdi enn det systemet er godkjent for», jf. informasjonssikkerhetsforskriften § 11-1.

Monitoring er et inngripende tiltak og i forarbeidene diskuteres behovet for monitoring opp mot personvern- og rettssikkerhetskonsekvensene. Om behovet for videreføring av tiltaket og om hensynet til personvernet uttales det at:

> Det er departementets syn at monitoring er et viktig tiltak for å oppnå god forebyggende informasjonssikkerhet, og at monitoringtjenesten således bør opprettholdes. Sikkerhetsbrudd forekommer fremdeles. Rapporter fra Nasjonal sikkerhetsmyndighet om sikkerhetsbrudd blir tatt alvorlig av avdelinger i Forsvaret, og ordningen må antas å ha en positiv effekt ved å bidra til å hindre at et større antall kompromitteringer forekommer. Ordningen er et supplement, ikke et alternativ, til andre virkemidler for å oppnå respekt for skjermingsverdig informasjon. For øvrig bør nevnes at dagens monitoringstjeneste uansett må opprettholdes som følge av forpliktelser etter NATOs regelverk. […]

> De gjeldende restriktive begrensninger mht gjennomføringen av kontrollen, vil naturligvis bli opprettholdt. Den Norske Advokatforening uttaler om dettte i sin høringsuttalelse at en «... har merket seg at det foreslås lovfestet at monitoring ikke i noe tilfelle skal omfatte privat kommunikasjon som blir formidlet til eller fra andre enn virksomheter og at informasjon som fremkommer ved kontroll skal makuleres når den ikke lenger har betydning for kontrollen. Av personvernhensyn er det viktig at det i forskriftene etableres betryggende kontrollrutiner for å sikre at disse regler blir fulgt.» Departementet slutter seg til uttalelsen, og vil sørge for at betryggende kontrolltiltak iverksettes.[3]

Om konklusjonen uttaler departementet:

> Dagens monitoringsvirksomhet har etter departementets oppfatning et aktverdig formål, representerer ikke et uforholdsmessig inngrep og kan ikke ses å ha vesentlige rettssikkerhetsmessige implikasjoner, bl.a tatt i betraktning de begrensninger og retningslinjer for gjennomføring av monitoring som er nedfelt i gjeldende direktiver gitt av Forsvarssjefen. Selv om hjemmelsgrunnlaget anses tilfredsstillende i dag, basert på eierrådighetsbetraktninger og avtale-/samtykkesynspunkter, vil det være naturlig å lovfeste hovedreglene om monitoring i en samlet lov om forebyggende sikkerhetstjeneste.

Av rettssikkerhets- og personvernhensyn stiller loven flere absolutte krav som må være oppfylt før monitoring kan iverksettes. Den virksomhet som skal kontrolleres må enten selv anmode om eller, dersom NSM har tatt initiativet, samtykke til gjennomføring av kontrollen. Samtykket eller anmodningen skal skje skriftlig, jf. informasjonssikkerhetsforskriften § 11-4 fjerde ledd. Monitoring kan dessuten kun iverksettes i virksomheter som er underlagt sikkerhetsloven og bare tjenestlig kommunikasjon kan kontrolleres. Dersom det i løpet av kontrollen viser seg at nevnte vilkår ikke er oppfylt, skal monitoringen avbrytes umiddelbart, jf. informasjonssikkerhetsforskriften § 11-7.

Det stilles også krav om at alle ansatte og andre direkte berørte må varsles i forkant om at det vil bli gjennomført kontroll, om hensikten med og varigheten av kontrollen, at NSM gjennomfører og på hvilken måte kontrollert informasjon blir behandlet. Det er kun NSM som kan gjennomføre monitoring i henhold til sikkerhetsloven. Etter endt monitoring skal NSM rapportere til virksomheten om resultatet av kontrollen.

8.2.1.4 Inntrengning i informasjonssystemer

Inntrengningstesting reguleres sammen med monitoring i sikkerhetsloven § 15 og informasjonssikkerhetsforskriften kapittel 11. De to sikkerhetstiltakene har en del til felles, men det er også noen forskjeller.

Hensikten med inntrengningstesting er å kontrollere om sikkerhetsgradert informasjon blir beskyttet i samsvar med fastsatte krav, gjennom prøving av motstandsdyktigheten i informasjonssystemer, jf. informasjonssikkerhetsforskriften § 11-2.

Som for monitoring kan kontrollen i utgangspunktet kun gjennomføres i virksomheter underlagt sikkerhetsloven, og det er NSM som står for gjennomføringen. Videre må det foreligge anmodning eller samtykke fra virksomheten før inntrengningstesting kan settes i gang. Det er også tilsvarende regler om varsling av ansatte og andre berørte. I tillegg skal det informeres om hvordan eventuelle oppdagede avvik vil bli fulgt opp. Det er ikke en tilsvarende regel om å avbryte kontrollen dersom kontrolløren kommer over privat informasjon, slik som det er for monitoring.

NSM skal rapportere til virksomheten etter at kontrollen er ferdig.

8.2.1.5 Sikkerhetsmessig overvåkning av informasjonssystemer

Regjeringen fremmet i Prop. 97 L (2015–2016) om endringer i sikkerhetsloven, forslag om en ny bestemmelse § 13a om sikkerhetsmessig overvåkning av informasjonssystemer.

Forslaget går ut på at virksomhetene selv skal sørge for overvåkning av sine informasjonssystemer, med mål om å avdekke ulovlig inntrengning. Begrunnelsen for lovfesting er dels at overvåkningen kan gripe inn i personvernet, dels at det er et økende behov for overvåkning og dels at det må klargjøres hva som inngår i sikkerhetsmessig overvåkning.

Overvåkningen skal bidra til å motvirke sikkerhetstruende virksomhet mot informasjonssystemet, særlig i form av ondsinnet programvare. Overvåkning av systemet innebærer både registrering og lagring av aktivitet i systemet (logging), automatiserte alarmer og manuell sammenstilling

[3] Ot.prp. nr. 49 (1996–97), 46–47.

og analyse av data relatert til sikkerhetstruende hendelser. Som det fremgår av forarbeidene:

> skal loggingen gjøre virksomheten i stand til å foreta en vurdering av omfanget og karakteren av skaden som har oppstått, gjenopprette sikker tilstand, samt sikre sporbarhet og ansvarlighet for utførte handlinger i samsvar med kravene i sikkerhetsloven for øvrig.[4]

For at overvåkningen skal være effektiv, vil det i mange tilfeller være behov for overvåkning også av innholdet i kommunikasjonen. I den grad det kommuniseres informasjon som er personsensitiv, kan overvåkning kun tillates etter å ha fulgt prosedyrene oppstilt i kapittel 5.7. Om ivaretakelse av personvernhensyn uttales det i forarbeidene s. 38):[5]

> Departementet vil innledningsvis presisere at forslaget er avgrenset til systemer som er godkjent for behandling av sikkerhetsgradert informasjon. Dette er systemer som er klare etterretningsmål, og som derfor må ha et høyt sikkerhetsnivå. Sikkerhetsmessig overvåking av disse systemene slik at angrep på et tidlig tidspunkt kan oppdages, og omfanget kartlegges, framstår derfor etter departementets vurdering som nødvendig. De systemer som vil være gjenstand for overvåking etter forslagets § 13 er i mindre grad egnet til, eller beregnet for, kommunikasjon av privat karakter, eller annen type privat bruk. Dette er lukkede systemer uten direkte tilknytning til internett. Omfanget av privat kommunikasjon og privat bruk av disse systemene vil derfor være begrenset. Det vil likevel være slik at kommunikasjon av privat karakter vil kunne forekomme, da primært som e-post eller nettprat med videre, mellom brukerne i det lukkede systemet. […]
>
> Omfanget av systemer som blir gjenstand for sikkerhetsmessig overvåking etter § 13 a er også av et begrenset omfang. Det er kun et fåtall systemer i offentlig forvaltning som er godkjent for å behandle sikkerhetsgradert informasjon, og som således vil være underlagt kravene til sikkerhetsmessig overvåking i § 13 a.

Det pekes også på mulige tiltak, blant annet særegen lagring av loggdata, tilgangsrestriksjoner, informasjon, opplæring av personell, som skal ivareta personvernhensyn. Departementet viser også til forholdsmessighetsprinsippet i gjeldende sikkerhetslov § 6 om at det ikke skal brukes mer inngripende midler og metoder enn det som framstår som nødvendig. Det bemerkes dessuten at omfanget av logging vil være større på høyt graderte systemer enn på de lavere graderte systemene.

Stortinget har, i forbindelse med behandlingen av Innstilling 352 L (2015–2016) til Prop. 97 L (2015–2016) om endringer i sikkerhetsloven, vedtatt regjeringens forslag til ny bestemmelse om sikkerhetsmessig overvåkning av informasjonssystemer. Ettersom den nye bestemmelsen ikke har trådt i kraft ennå, er informasjonssikkerhetsforskriften § 5-2 fortsatt den gjeldende reguleringen av sikkerhetsmessig overvåkning.

8.2.1.6 Tekniske sikkerhetsundersøkelser

Et siste tiltak som hjemles i sikkerhetsloven, er tekniske sikkerhetsundersøkelser som skal avdekke illegalt avlyttingsutstyr og eventuelle sårbarheter i blant annet den fysiske sikringen. Nasjonal sikkerhetsmyndighet kan i medhold av § 16 gjennomføre tekniske sikkerhetsundersøkelser (TSU) av steder der sikkerhetsgradert informasjon skal behandles, for å avverge uønsket avlytting og innsyn.

Det nærmere innholdet er regulert i informasjonssikkerhetsforskriften kapittel 10. Formålet, bakgrunnen og behovet for TSU er beskrevet slik i forarbeidene:

> Hovedformålet med TSU-tjenesten er å avsløre illegalt avlyttingsutstyr og eventuelt påvise de svakheter i bygningskonstruksjoner, installasjoner og fysisk sikring som er av en slik art at de øker faren for avlytting o l, slik at nødvendige forholdsregler kan iverksettes. TSU vil også ha som formål å virke avskrekkende bl.a overfor potensielle avlyttere. TSU-tjenesten må opprettholdes også av hensyn til våre NATO-forpliktelser.[6]

I tillegg fremgår det av informasjonssikkerhetsforskriften § 10-1 at noe av hensikten med TSU er å gi Nasjonal sikkerhetsmyndighet grunnlag for å gi råd eller pålegg om hvordan sårbarhetene som avdekkes kan reduseres eller fjernes.

Nasjonal sikkerhetsmyndighet kan delegere TSU-oppdrag til andre, jf. sikkerhetsloven § 16. Forskriften stiller krav om at de som eventuelt

[4] Prop. 97 L (2015–2016), 39.

[5] Prop. 97 L (2015–2016), Ibid., 38.

[6] Ot.prp. nr. 49 (1996–97), 42.

bemyndiges til å gjennomføre TSU må ha leverandørklarering for HEMMELIG eller høyere, at de må rapportere til virksomhetens leder i etterkant av gjennomført TSU, og at utstyr og teknikker som benyttes i en TSU minst skal graderes BEGRENSET.

Det forutsettes i forarbeidene at TSU som hovedregel vil være avtalt med den enkelte virksomhet:

> I motsetning til monitoring av og inntrengning i informasjonssystemer, bør det ikke kreves at virksomheten på forhånd skal være gjort kjent med og ha gitt samtykke til undersøkelsene. TSU blir kun utført der det (skal) behandles eller tales skjermingsverdig informasjon. Tjenesten må betraktes som en regulær godkjennings- og inspeksjonsvirksomhet for å forebygge og kontrollere at skjermingsverdig informasjon ikke kompromitteres, og kan sammenlignes med hva som gjelder ved inspeksjon av dokumentsikkerhet. Det ligger imidlertid i dagen at undersøkelsene normalt vil være forhåndsvarslet og avtalt på forhånd med den berørte virksomhet, da dette vil være mest hensiktsmessig for begge parter og gjøre prosedyren mer planmessig og effektiv.

At Nasjonal sikkerhetsmyndighet på eget initiativ kan gjennomføre TSU, er direkte hjemlet i informasjonssikkerhetsforskriften § 10-2 andre ledd.

8.2.1.7 Kryptosikkerhet

Det går frem av sikkerhetsloven § 14 at «[b]are kryptosystemer som er godkjent av Nasjonal sikkerhetsmyndighet, tillates brukt for beskyttelse av skjermingsverdig informasjon». Bestemmelsen fastsetter også at Nasjonal sikkerhetsmyndighet er nasjonal forvalter av kryptomateriell og leverandør av kryptosikkerhetstjenester. De gis også hjemmel til å fastsette nærmere bestemmelser om krypto i forskrift, hvilket er gjort i informasjonssikkerhetsforskriften kapittel 7.

8.3 Annet relevant regelverk

8.3.1 Sektorovergripende regelverk

Personopplysningsloven og personopplysningsforskriften har egne bestemmelser om informasjonssikkerhet. Reglene har et stort nedslagsfelt og for virksomheter som forvalter samfunnskritisk infrastruktur, men som ikke behandler informasjon som er gradert etter sikkerhetsloven, er det antakelig personopplysningsforskriftens bestemmelser som er det regelverket for informasjonssikkerhet de forholder seg til i praksis.[7]

Personopplysningsloven § 13 Informasjonssikkerhet pålegger den som er ansvarlig for behandlingen av personopplysninger å «gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger». Det følger av EUs personverndirektiv 95/46/EF artikkel 17 (som er implementert i personopplysningsloven), krav til forholdsmessige sikkerhetstiltak mot både tilfeldig og ulovlig ødeleggelse, og en dynamisk tilpasning til endringer i den teknologiske utviklingen. Nærmere krav til ivaretakelse av informasjonssikkerheten følger av personopplysningsforskriften kapittel 2. Innholdsmessig går kravene ut på å etablere og etterleve et internt styringssystem, beslektet med det som er foreskrevet i innarbeidede internasjonale *best practice*-standarder.[8] §§ 2-10 – 2-13 inneholder bestemmelser om henholdsvis, fysisk sikring og sikring av konfidensialitet, tilgjengelighet og integritet. Verdt å nevne er også § 2-15 som pålegger den behandlingsansvarlige å forsikre seg om at den man overfører personopplysninger til tilfredsstiller kravene i forskriften.

Etter personopplysningsforskriften § 2-1 gjelder det forholdsmessige krav om sikring av personopplysninger. Tiltakene som treffes i medhold av forskriften skal «stå i forhold til sannsynligheten for og konsekvens av sikkerhetsbrudd». Tiltakene retter seg ikke mot å identifisere eller sikre samfunnskritiske funksjoner eller infrastruktur. Oppfyllelse av kravene bidrar antakelig til et høyere sikkerhetsnivå i den enkelte virksomhet, og har på den måten positiv effekt utover bare å beskytte personopplysninger.

For de aller fleste forvaltningsorganer oppfylles kravene til informasjonssikkerhet i eForvaltningsforskriften 25. juni 2004 nr. 988, gitt i medhold av forvaltningsloven av 10. februar 1967 § 15a, gjennom det samme styringssystemet som de følger etter personopplysningsforskriften.[9] Forskriften gjelder for offentlig forvaltning som kommuniserer elektronisk med innbyggere, næringsliv eller andre forvaltningsorganer. Bestemmelsene om informasjonssikkerhet byg-

---

7 Herbjørn Andersen, *Kartlegging av sektorlovgivning som regulerer virksomheters tiltak mot tilsiktede hendelser*, Høgskolen i Oslo og Akershus, elektronisk vedlegg 1, 8.

8 Ibid., 8.

9 Ibid., 9.

ger i all hovedsak på samme *best practice*-grunnlag som personopplysningsforskriften.

8.3.2 Utvalgt sektorregelverk

I finanssektoren har Finanstilsynet gitt IKT-forskriften som blant annet oppstiller krav om planlegging, risikoanalyse, tilgangskontroll, systemvedlikehold og prosedyrer for avviks- og endringshåndtering.[10] Verdt å nevne er forskriften § 5, som retter seg direkte mot tilsiktede uønskede hendelser:

> Foretaket skal utarbeide prosedyrer som skal sikre beskyttelse av utstyr, systemer og informasjon av betydning for foretakets virksomhet, jf. § 1, mot skader, misbruk, uautorisert adgang og endring, samt hærverk.

Bestemmelsen henviser til personopplysninger og fastslår at oppfyllelse av personopplysningsforskriftens krav til informasjonssikkerhet, skal anses som oppfyllelse av kravene i § 5. Forskriften skal sikre at IKT-virksomheten leverer de tjenester som er avtalt, også der hele eller deler av IKT-virksomheten er utkontraktert til andre aktører.

Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen 7. desember 2012 nr. 1157, hjemlet i energiloven, har i kapittel 6 og 7 bestemmelser om henholdsvis informasjonssikkerhet og driftskontrollsystemsikkerhet. Kapittel 6 oppstiller kriterier for hva som regnes som kraftsensitiv informasjon, og krav til at virksomhetene skal identifisere den sensitive informasjonen, vite hvor den befinner seg, og vite hvem som har tilgang til den. Kapittel 7 fastsetter blant annet en generell plikt til å beskytte systemet og sørge for at det virker etter sin hensikt. Videre må den enkelte virksomhet blant annet fastsette sikkerhetskrav, ha oppdatert dokumentasjon om systemet, kontrollere brukertilgangen og sørge for effektiv håndtering av feil, sårbarhet og sikkerhetsbrudd, samt ha beredskap og forberedte tiltak for fortsatt drift av anlegg ved svikt i driftskontrollsystemet.

Petroleumsloven § 9-3 skal bidra til å hindre bevisste anslag mot innretninger i petroleumssektoren. Hvorvidt dette også omfatter krav til forsvarlig IKT-sikkerhet er ikke nærmere angitt i lov eller forskrift. Imidlertid har interesse- og arbeidsgiverorganisasjonen Norsk olje og gass (NOROG) utviklet retningslinjer for IKT-sikkerhet i sektoren. I retningslinje 104 Anbefalte retningslinjer krav til informasjonssikkerhetsnivå i IKT-baserte prosesskontroll-, sikkerhets- og støttesystemer, anbefales ganske ordinære tiltak for IKT-sikkerhet, blant annet krav om sikkerhetsstyring, risikovurdering, brukerkompetanse, beredskapsplaner og varslingsprosedyrer.

8.3.3 Beskyttelsesinstruksen

Beskyttelsesinstruksen[11] anvendes for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven. Instruksen forvaltes av Statsministerens kontor (SMK).

Instruksen er gitt med hjemmel i Kongens instruksjonsmyndighet. Dette innebærer at instruksen kun kan gjøres gjeldende overfor virksomheter som ligger innenfor regjeringens alminnelige instruksjons- og kontrollmyndighet – det vil si statsforvaltningen.

Som det fremgår av instruksens tittel er anvendelsesområdet et annet enn for sikkerhetsloven, men det er likevel enkelte likhetstrekk mellom regelverkene. Som etter sikkerhetsloven er det en skadevurdering som ligger til grunn for gradering av dokumenter. FORTROLIG og STRENGT FORTROLIG benyttes dersom det vil kunne forårsake henholdsvis skade eller betydelig skade for offentlige interesser, en bedrift, en institusjon eller en enkeltperson, at dokumentets innhold blir kjent for uvedkommende.

Elektronisk behandling av dokumenter som er gradert i medhold av beskyttelsesinstruksen, skal i henhold til instruksen § 12 skje i samsvar med nærmere angitte bestemmelser i informasjonssikkerhetsforskriften.

En viktig forskjell mellom de to regelverkene er det absolutte tilleggsvilkåret for gradering etter beskyttelsesinstruksen, om at dokumentet må kunne unntas fra offentlighet i medhold av offentleglova, jf. instruksen § 3. Dette henger sammen med at instruksen ikke har hjemmel i formell lov, og derfor ikke utgjør en selvstendig hjemmel for unntak fra innsyn etter offentleglova.

Instruksen er nevnt enkelte steder i forarbeidene til sikkerhetsloven:

> Deler av sikkerhetstjenestens oppdrag er dessuten nedfelt i direktiver som dekker elementer av tjenestens ansvarsområde. I første rekke av

[10] Forskrift 21. mai 2003 nr. 630 om IKT-systemer i banker mv.

[11] Instruks 17. mars 1972 nr. 3352 for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter (beskyttelsesinstruksen).

disse direktiver står Sikkerhetsinstruksen, gitt ved kgl res av 17 mars 1972. Instruksen regulerer ulike sikkerhetsmessige aspekter ved behandling av sikkerhetsgradert informasjon. Denne instruksen er for øvrig gitt samtidig med Beskyttelsesinstruksen, som regulerer tilsvarende aspekter ved behandling av informasjon som trenger beskyttelse av andre grunner enn de som ligger til grunn for Sikkerhetsinstruksens bestemmelser. Statsministerens kontor har ansvaret for Beskyttelsesinstruksen.

Lovforslaget vil ikke gjelde informasjon som trenger beskyttelse av andre grunner (for eksempel av personvernhensyn etter Beskyttelsesinstruksen). Dette er i samsvar med Forsvarsministerens oppdrag i kgl res 24 september 1965, som ansvarlig for rikets sikkerhet i hele statsforvaltningen.

I den grad innføringen av begrepet (vitale nasjonale sikkerhetsinteresser, red. anm.) i det hele tatt kan ses på som en utvidelse i forhold til gjeldende regler, vil det for praktiske formål få som konsekvens at enkelte opplysninger som tidligere ble gradert etter Beskyttelsesinstruksen, i stedet skal behandles som skjermingsverdig informasjon og sikkerhetsgraderes etter det fremlagte lovforslaget.[12]

Et eksempel på anvendelse av beskyttelsesinstruksen finner vi i forskrift 9. november 2007 nr. 1268 om folkeregistrering § 3-2 Registrering av andre faktiske og rettslige forhold som finner sted i Norge, nummer 10:

Adressesperring gjort med hjemmel i Beskyttelsesinstruksen registreres, med unntak for barnevernsaker, på grunnlag av melding fra Kripos.

Det fremgår videre av forskriften § 9-5:

Skattedirektoratet beslutter i barnevernsaker om og hvor lenge en adresseopplysning skal graderes etter Beskyttelsesinstruksen. Beslutningen treffes etter anmodning fra barneverntjenesten.

Søknad om utlevering av adresseopplysning som er gradert etter Beskyttelsesinstruksen avgjøres i barnevernsaker av barneverntjenesten. I andre saker avgjøres søknaden av politiet.

Adressesperring med gradering Fortrolig kan skattekontoret utlevere til offentlig myndighet uten å innhente samtykke fra barneverntjenesten eller politiet.

I heftet Om r-konferanser, utgitt av SMK, gis det retningslinjer om forberedelse av saker til regjeringskonferanse. Det fremgår der at regjeringsnotater tidvis graderes i henhold til Beskyttelsesinstruksen.[13]

8.3.4 Offentleglova

Offentleglova[14] bygger på offentlighetsprinsippet. Som det fremgår av formålsbestemmelsen i § 1, skal loven:

[L]eggje til rette for at offentleg verksemd er open og gjennomsiktig, for slik å styrkje informasjons- og ytringsfridommen, den demokratiske deltakinga, rettstryggleiken for den enkelte, tilliten til det offentlege og kontrollen frå ålmenta.

Dette er viktige hensyn som loven skal ivareta. Det er samtidig klart at andre hensyn tidvis kan begrunne unntak fra hovedregelen. Eksempelvis må regjeringen kunne diskutere statsbudsjettet internt før forslaget legges frem for Stortinget.

Etter offentleglova § 13 er det forbudt å gi innsyn i opplysninger som i lov eller i medhold av lov er underlagt taushetsplikt. Som nevnt over er all sikkerhetsgradert informasjon belagt med taushetsplikt, jf. sikkerhetsloven § 12.

Offentleglova § 21 hjemler muligheten til å unnta opplysninger fra innsyn av hensyn til nasjonale forsvars- og sikkerhetsinteresser. Dette er ikke en forbudsbestemmelse. Om opplysningen skal unntas må vurderes konkret. Meroffentlighet, jf. offentleglova § 11 skal på vanlig måte vurderes.

Forarbeidene til dagens sikkerhetslov drøfter forholdet mellom sikkerhetsgradering av informasjon av hensyn til rikets sikkerhet, og offentlighetslovens bestemmelser om unntak fra innsyn. Problemstillingen var om den nye sikkerhetsloven ville få konsekvenser for praktiseringen av offentlighetsprinsippet. På den ene side ble vilkårene for sikkerhetsgradering av informasjon skjerpet i forhold til tidligere instruks. På den

[12] Ot.prp. nr. 49 (1996–97), 35.

[13] Retningslinjer, *Om r-konferanser*, Statsministerens kontor 2014, 19.

[14] Lov 19. mai 2006 nr. 16 om rett til innsyn i dokument i offentleg verksemd (offentleglova).

andre siden ble lovens virkeområde noe utvidet ved at den nye loven skulle få anvendelse for hele offentlig sektor. Departementets vurdering var at totalt sett ville den nye loven innebære en styrking av offentlighetsprinsippet.

Om forholdet mellom de to unntakshjemlene – taushetsplikt og hensynet til rikets sikkerhet – uttaler departementet i forarbeidene til sikkerhetsloven i kapittel 7.2.2:

> Det er vanskelig å forestille seg praktiske eksempler på sikkerhetsgradert informasjon som skal unntas etter § 5a [om taushetsplikt], men som ikke omfattes av unntaksbestemmelsen i § 6 første ledd nr 1 [hensynet til rikets sikkerhet]. Omvendt må det imidlertid understrekes at det kan tenkes dokumenter som kan unntas fra offentlighet etter offentlighetsloven § 6 nr 1, men som ikke kan sikkerhetsgraderes.

Vurderingen ble gjort opp mot den da gjeldende lov 19. juni 1970 nr. 69 om offentlighet i forvaltningen – offentlighetsloven. I 2009 trådte den nye lov om rett til innsyn i dokument i offentleg verksemd i kraft, som erstatning for loven av 1970. Den mest betydningsfulle endringen for forholdet til sikkerhetsgradert informasjon, var at det som utgangspunkt var opplysninger som kunne unntas, og ikke hele dokumenter. Muligheten til å kunne unnta opplysninger av hensyn til nasjonale forsvars- og sikkerhetsinteresser, ble ikke endret. Forbudet mot å gi innsyn i opplysninger som ved lov eller med hjemmel i lov er underlagt taushetsplikt, ble heller ikke endret.

8.4 Fremmed rett

8.4.1 NATO

8.4.1.1 Generelt

Bestemmelser om beskyttelse av NATO sikkerhetsgradert informasjon er i dag gitt i *NATO Security Policy C-M(2002)49*, som sammen med flere understøttende direktiver er bindende for alle medlemslandene, inkludert Norge.

Sikkerhetsavtalen danner det formelle grunnlag for et relativt omfattende, og til dels teknisk regelverk for beskyttelse av NATO sikkerhetsgradert informasjon.[15] De overordnede rammer og prinsipper for regelverket er vedtatt av NATOs råd, mens utfyllende bestemmelser er fastsatt av de fagansvarlige komiteer, henholdsvis *Security Committee* og *C3 Board*. NATOs sikkerhetsregelverk er dels bindende for nasjonene og dels veiledende.

Norge er bundet av NATO-regelverket kun i den utstrekning det er tale om NATO-relatert informasjon og NATO-relaterte objekter. Norge står dermed fritt til å regulere sikkerheten for egen informasjon og egne objekter. Imidlertid er det per i dag samsvar mellom de to regelsettene slik at for eksempel informasjonssystemer som er godkjent for BEGRENSET i Norge også er godkjent for å behandle NATO RESTRICTED. Der man har behov for å behandle både nasjonale- og NATO-dokumenter, for eksempel i forsvarssektoren, ville man uten slikt samsvar måttet operere med to informasjonssystemer.

Det fremgår av forarbeidene til sikkerhetsloven at:

> I 1955 forelå NATOs sikkerhetsdirektiv C-M(5515)(Final). Direktivet ble gjort gjeldende for samtlige NATO-land, også Norge, og fastsatte krav til beskyttelsestiltak for NATO-eiet og NATO-gradert informasjon. Det ble dessuten gitt bestemmelser om krav til sikkerhetsvurdering og klarering for alt personell som skulle gis adgang til slike dokumenter. Nasjonalt var det hensiktsmessig ikke å ha to regelsett å forholde seg til. NATOs direktiv ble derfor styrende for utforming av nasjonale regler, og fungerte i all hovedsak som en minstestandard.[16]

NATO-regelverket danner altså grunnlaget for dagens bestemmelser om forebyggende sikkerhet. Det må imidlertid understrekes, som det fremgår av det siterte, at regelverket i all hovedsak fungerer som en minstestandard for våre nasjonale regler.

NATOs tilnærming og krav til sikring av informasjonssystemer som skal håndtere sikkerhetsgradert informasjon, er i stor grad sammenfallende med hva som for nasjonale systemer i dag er nedfelt i informasjonssikkerhetsforskriften kapittel 5 om informasjonssystemsikkerhet, og i kapittel 7 om administrativ kryptosikkerhet.

8.4.1.2 Grunnprinsipper

NATOs bestemmelser om forebyggende sikkerhet regulerer informasjons-, informasjonssystem- og personellsikkerhet, fysisk sikring og sikker-

[15] C-M(2002)49 Enclosure «A», Security agreement.

[16] Ot.prp. nr. 49 (1996–97), 14.

hetsgraderte anskaffelser. Det fastslås flere steder i regelverket at det må inntas en helhetlig tilnærming til arbeid med forebyggende sikkerhet. Det innebærer at tilstrekkelig sikkerhet forutsetter at hele spekteret av sikkerhetstiltak ses i sammenheng.

I hovedavtalen om sikkerhet forplikter NATOs medlemsland seg til å beskytte gradert informasjon.[17] Beskyttelsen skal realiseres gjennom etablering og implementering av sikkerhetsstandarder som skal sørge for et felles nivå for beskyttelse av gradert informasjon for alle NATO-land.

Grunnprinsippene og standardene for sikkerhet i NATO:[18]

a) NATO medlemsland og NATO sivile og militære enheter (bodies) skal sørge for beskyttelse av gradert informasjon i tråd med de standarder som fastsettes i den foreliggende *Council Memorandum* (C-M).
b) Gradert informasjon skal deles kun etter *need-to-know*-prinsippet til personer som har blitt tilstrekkelig orientert om sikkerhetsprosedyrer. Sikkerhetsklarering er en forutsetning for tilgang til informasjon merket CONFIDENTIAL.
c) Sikkerhetsrisikostyring er obligatorisk i sivile og militære NATO-enheter, men frivillig for medlemslandene.
d) Sikkerhetstiltakene skal være balansert og bestå av både personell-, fysisk-, informasjons- og IKT-sikkerhet (INFOSEC).
e) Mistanke om sikkerhetsbrudd skal varsles til relevant sikkerhetsmyndighet, og følges opp av relevante myndigheter.
f) Den som utsteder gradert informasjon, gir dette til NATO under forståelse av at den blir behandlet og beskyttet i tråd med gjeldende NATO retningslinjer.
g) Gradert informasjon skal undergis utstederkontroll.
h) Utgivelse (*release*) av NATO-gradert informasjon til ikke-NATO-mottakere må kun skje i tråd med nærmere fastsatte regler.

Det er fastsatt to fundamentale tiltak for god nasjonal sikkerhet.[19] For det første skal det være en nasjonal sikkerhetsorganisasjon med ansvar for *behandling* av trusselinformasjon.[20] For det andre skal det være et jevnlig samarbeid mellom statlige myndigheter og direktorater om identifisering av gradert informasjon som trenger beskyttelse. Det skal også samarbeides for å etablere og implementere et felles beskyttelsesnivå i tråd med NATO-kravene.

Medlemslandene må peke ut en nasjonal sikkerhetsmyndighet som skal være ansvarlig for å implementere sikkerhetstiltakene og være kontaktpunkt mot NATO innen forebyggende sikkerhet. *NATO Office of Security* fører også tilsyn med sikkerhetstilstanden i medlemslandene, i samarbeid med de respektive nasjonale sikkerhetsmyndigheter. Den nasjonale sikkerhetsmyndigheten (i Norge NSM) har blant annet ansvar for:

a) å opprettholde sikring av gradert informasjon,
b) å føre periodisk og forholdsmessig tilsyn med sikkerhetstiltak i alle nasjonale organisasjoner på alle nivåer, både militære og sivile,
c) at alle som får tilgang til informasjon merket *CONFIDENTIAL* eller over sikkerhetsklareres i tråd med NATO-retningslinjene og
d) å utarbeide beredskapsplaner (emergency plans) for å unngå at gradert informasjon kommer uvedkommende i hende.

8.4.1.3 Informasjons- og informasjonssystemsikkerhet

Informasjonssikkerhetstiltakene skal motvirke, oppdage og gjenopprette etter tap eller kompromittering av informasjon. Et grunnleggende tiltak er at informasjon skal graderes ut fra den potensielle skade det kan medføre for NATO eller medlemslandene om den blir kjent for uvedkommende. NATO har følgende skadevurdering og sikkerhetsgradering:[21]

a) COSMIC TOP SECRET (CTS) – unauthorised disclosure would result in exceptionally grave damage to NATO,
b) NATO SECRET (NS) – unauthorised disclosure would result in grave damage to NATO,
c) NATO CONFIDENTIAL (NC) – unauthorised disclosure would be damaging to NATO, and
d) NATO RESTRICTED (NR) – unauthorised disclosure would be detrimental to the interests or effectiveness of NATO.

---

17 C-M(2002)49 Enclosure «A», Security agreement.

18 C-M(2002)49 Enclosure «B», Basic principles of security, punkt 5.1.

19 Ibid. punkt 5.2.

20 Med behandling menes blant annet innhenting, ivaretakelse, sentralisering og utlevering av trusselinformasjon.

21 C-M(2002)49 Enclosure «B», Basic principles of security, punkt 18.

Beskyttelsen skal gjennom hele informasjonens livssyklus være på et nivå tilpasset sikkerhetsgraderingen. En må påse at informasjon graderes og merkes, men ikke over lenger tid enn nødvendig. Informasjonssikkerhet er nærmere regulert i *Enclosure «E»*.

Det er utsteder av informasjonen som er ansvarlig for å fastsette korrekt graderingsnivå. Endring av sikkerhetsgradering kan skje, men kun etter samtykke fra utsteder. NATO-medlemsland og -enheter skal gjennom tiltak legge til rette for at informasjon som tilvirkes i NATO eller gis til NATO, blir korrekt gradert og beskyttet i henhold til det foreliggende regelverket.

NATO-medlemsland og -enheter må videre ha beredskapsplaner for beskyttelse eller ødeleggelse av informasjon i krisesituasjoner. Sikkerhetsbrudd må varsles straks til relevant sikkerhetsmyndighet, og evalueres av fagpersoner som ikke er berørt av hendelsen. Et grunnkrav for utlevering av NATO-gradert informasjon til ikke-NATO-land er samtykke fra utsteder, i tillegg til andre mer spesifikke krav.

Informasjonssystemsikkerhetstiltakene (*CIS security*) skal beskytte informasjon som behandles i kommunikasjons-, informasjons- og andre elektroniske systemer mot brudd på konfidensialitet, integritet og tilgjengelighet, både ved utilsiktede og tilsiktede hendelser. Tiltakene skal også beskytte mot brudd på integritet i og tilgjengelighet til selve systemet. Tiltakene skal gi et minimum av beskyttelse mot kjente trusler av både tilsiktet og utilsiktet art. Ytterligere sikkerhetstiltak skal iverksettes der en konkret risikovurdering tilsier det.

Alle IKT-systemer som behandler gradert informasjon må gjennomgå en sikkerhetsgodkjenningsprosess, som kan fastslå om et relevant sikkerhetsnivå er oppnådd og blir opprettholdt. Den nasjonale sikkerhetsmyndigheten kan delegere godkjenningsmyndigheten til andre.

Systemer som behandler gradert informasjon må sikres på bakgrunn av risikovurderinger og risikostyring i tråd med NATO-retningslinjer. IKT-sikkerheten er nærmere regulert i *Enclosure «F»*.

8.4.2 Sverige

I Sverige er informasjonssikkerheten i relasjon til *rikets säkerhet* regulert i *säkerhetsskyddslagen* (1996:627) og i *säkerhetsskyddsförordningen* (1996:633).

Det fremgår av *säkerhetsskyddslagen* 7 § 1 at sikkerhetstiltakene skal forebygge at opplysninger som er sensitive av hensyn til rikets sikkerhet ikke må avsløres, endres eller slettes uten autorisasjon. Hvilke beskyttelsesbehov som oppstår når informasjonen behandles automatisk, skal særlig vurderes ved utforming av regler om informasjonssikkerhet, jf. 9 §.

Säkerhetsskyddsförordningen 9–13 §§ inneholder mer konkrete regler om informasjonssikkerhet. Alle virksomheter som omfattes av loven må dessuten gjennomføre en *säkerhetsanalys* for å kartlegge hvilke opplysninger i deres virksomhet som må holdes hemmelig av hensyn til rikets sikkerhet, jf. förordningen 5 §. Videre er det regler om varsling av sikkerhetsbrudd, nedtegning av såkalte *hemliga handlinger* og forsendelse av dokumenter.

Den 1. april 2016 trådte 10 a § om informasjonssystemsikkerhet i kraft. IKT-hendelser (*IT-incident*) i en myndighets informasjonssystem skal straks varsles til en nærmere fastsatt sikkerhetsmyndighet, dersom hendelsen i alvorlig grad kan påvirke sikkerheten i et informasjonssystem som enten behandler hemmelige opplysninger av et visst omfang eller trenger særlig beskyttelse mot terrorisme, eller hendelsen ble oppdaget gjennom bistand fra Försvarets radioanstalt, jf. 4 § *Förordning* (2007:937) *med instruktion för Försvarets radioanstalt*. Der Försvarsmakten er mottaker av varsel, skal Säkerhetspolisen også varsles. Dersom hendelsen får betydning for myndighetens eventuelle tjenesteleveranser, skal også andre berørte informeres om hendelsen.

Elektroniske registre over opplysninger som kan skade totalforsvaret dersom de blir kjent for uvedkommende, må ikke opprettes før Försvarsmakten er konferert, jf. 12 §. Registrering av opplysninger som av andre grunner har betydning for rikets sikkerhet, skal konfereres med Säkerhetspolisen. Bestemmelsen sier videre at informasjonssystemer som brukes av flere personer og som behandler hemmelig informasjon, må ha funksjoner for adgangskontroll og registrering av sikkerhetshendelser. Slike systemer må dessuten sikkerhetsgodkjennes før de tas i drift.

Etter 13 § må statlige myndigheter forvisse seg om at det er god nok sikkerhet i det nettet de bruker til å sende hemmelig informasjon, når dette nettet er utenfor egen kontroll.

I *SOU 2015:25 En ny säkerhetsskyddslag*, foreslås flere endringer i dagens regler om informasjonssikkerhet. Det pekes på utviklingsbehov av hensyn til blant annet gjeldende retts sterke fokus på konfidensialitetsbeskyttelse og ivaretakelse av Sveriges internasjonale forpliktelser.

I forslaget til en ny *säkerhetsskyddslag* deles tiltakene for å beskytte informasjon i to kategorier.

For det første gjelder tiltakene beskyttelse av graderte opplysninger mot uautorisert endring, sletting og innsyn. For det andre gjelder tiltakene beskyttelse av informasjon som av andre grunner er av betydning for *säkerhetskänslig verksamhet* (Folkbokföringen trekkes frem som et eksempel). Sistnevnte kategori har ikke samme behov for konfidensialitetsbeskyttelse, og ivaretakelse av integritet og tilgjengelighet fremheves.

Sikkerhetsgradert informasjon foreslås delt inn i fire klasser basert på hvilket skadepotensiale informasjonen har om den blir kjent for uvedkommende. Sikkerhetsgraderingene som skal benyttes i ny lov er *kvalificerat hemlig*, *hemlig, konfidentiell* eller *begränsad*. Som begrunnelse vises det blant annet til at inndeling i fire klasser (slik som i for eksempel EU og NATO), legger bedre til rette for internasjonal samhandling og mer nyansert beskyttelse av nasjonale interesser.

Det foreslås også en ny *Säkerhetsskyddsförordning*, som blant annet inneholder bestemmelser for beskyttelse av IT-systemer. Det stilles krav til gjennomføring av ROS-analyse ved opprettelse eller vesentlig endring i IT-systemer som er av betydning for *säkerhetskänslig verksamhet*. Kravet gjelder for systemer som skal behandle informasjon som er gradert *konfidentiell* eller høyere, og for systemer «som är av motsvarande betydelse för Sveriges säkerhet, även om de inte behandlar säkerhetsskyddsklassificerade uppgifter», jf. forslag til ny forordning 2 §. Formålet er at beskyttelsesbehovet skal oppdages tidlig, hvilket skal redusere sikringskostnadene. Aggregering nevnes særskilt for å gjøre oppmerksom på at behandling eller lagring av større mengder informasjon på et visst nivå, kan skape faktisk behov for sikring på et høyere nivå.

Kravet om samråd med Försvarsmakten eller Säkerhetspolisen ved opprettelse av elektronisk register, jf. dagens lov 12 §, foreslås videreført. Samrådsplikten skal i ny lov også gjelde der man vesentlig endrer et IT-system, samt for IT-systemer som er av betydning for Sveriges sikkerhet selv om de ikke behandler gradert informasjon. Kravet gjelder ikke for systemer som skal behandle *begränsad* informasjon eller på annet tilsvarende vis er av betydning for Sveriges sikkerhet.

Det foreslås å styrke beskyttelsen av IT-systemer som skal benyttes av mer enn én person. Slike systemer må sikres gjennom blant annet tilgangskontroll, logging av hendelser i systemet som er av betydning for sikkerheten og beskyttelse mot uautorisert avlytting, inntrengning, skadelig kode og forstyrrende signaler. Det stilles ikke tilsvarende krav til systemer som ikke behandler gradert informasjon, fordi det antas at slike systemer er så forskjellige at det er vanskelig å utforme gode felles sikkerhetskrav.

Ordningen med forhåndsgodkjenning av IT-systemer som skal behandle gradert informasjon, foreslås videreført. Kravet om kommunikasjonsbeskyttelse, jf. dagens lov 13 §, foreslås også videreført. Det samme gjelder dagens regler om at krypto som skal brukes i graderte systemer, må godkjennes av Försvarsmakten.

8.4.3 Danmark

De sentrale dokumentene for ivaretakelse av informasjonssikkerhet i Danmark er Statsministeriets *Cirkulære om sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO eller EU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt* (Sikkerhedscirkulæret).[22] Cirkulæret gjelder i utgangspunktet kun for Statsministeriet, men forutsettes å gjelde for andre departementer og deres underlagte etater. Etter avtale kan cirkulæret også gjøres gjeldende for private.[23]

Sikkerhedscirkulæret har flere likhetstrekk med sikkerhetsregelverket i både Norge og NATO. Det regulerer informasjonssikkerhet i vid forstand, og inneholder bestemmelser om sikkerhetsmyndigheter, personellsikkerhet og fysisk sikkerhet, i tillegg til konkrete bestemmelser om informasjonssikkerhet. Sammenlignet med norske regler, ligger cirkulærets detaljeringsnivå et sted mellom sikkerhetsloven og de tilhørende forskriftene.

Som utgangspunkt for den konkrete beskyttelsen av informasjon, skal det foreligge en klassifisering av informasjon, i henhold til det skadepotensialet som uautorisert tilgang til informasjonen «ville kunde forvolde Danmark eller lande i NATO eller EU, overordentlig alvorlig skade», jf. cirkulæret § 1. De fire graderingene YDERST HEMLIGT, HEMMELIGT, FORTROLIGT og TIL TJENESTEBRUG skal tilsvare NATOs og EUs graderingssystem. Klassifiseringen TIL TJENESTEBRUG forutsetter for så vidt ikke uttrykkelig skadepotensiale for Danmark eller landene i NATO eller EU, men skal brukes om informasjon «der ikke må offentliggøres eller komme til uvedkommende kendskap.»

Sikkerhetstiltakene som skal iverksettes for å beskytte gradert informasjon er i grove trekk de

[22] CIS nr 10338 af 17. desember 2014.
[23] SOU 2015:25.

samme som i Norge. Cirkulæret inneholder bestemmelser om sikkerhetsklarering av personer som skal ha tilgang til gradert informasjon, behandling av dokumenter som inneholder gradert informasjon, sikkerhetsgodkjenning av elektroniske informasjonssystemer, forsendelse av informasjon, oppbevaring, fysisk sikkerhet, områdesikkerhetsgodkjenning, mobilt elektronisk informasjonsutstyr, virusbeskyttelse, sikkerhetsstyring og tilsyn, samt beskyttelse av «andre informationer af sikkerhetdsmæssig betydning.»

Sistnevnte gir hjemmel for enhver offentlig myndighet til å bestemme at sikkerhetscirkulærets regler skal gjelde for informasjon som av andre grunner enn i § 1 er av sikkerhetsmessig betydning. Det gis i slike tilfeller åpning for at IT-sikkerhetsmyndigheten kan tillate lemping av enkelte sikkerhetstiltak.

Ifølge § 27 må alle former for elektroniske informasjonssystemer som skal behandle HEMMELIGT eller FORTROLIGT informasjon, sikkerhetsgodkjennes av den nasjonale IT-sikkerhetsmyndigheten. Etter § 28 skal den nasjonale IT-myndigheten også godkjenne nye versjoner av *software* som benyttes i sikkerhetsgodkjente systemer. Systemer som skal behandle informasjon TIL TJENESTEBRUG trenger ikke sikkerhetsgodkjenning, men de må registerføres.

Det fremgår av § 56 at den nasjonale sikkerhetsmyndighet og den nasjonale IT-sikkerhetsmyndighet fører tilsyn med overholdelsen av Danmarks internasjonale forpliktelser om informasjonssikkerhet, og skal foreta periodiske inspeksjoner.

For å styrke Danmarks ekom-infrastruktur, ble *lov nr. 1567 om net- og informationssikkerhed* vedtatt 15. desember 2015. Loven regulerer i hovedsak informasjonssikkerheten i virksomheter som tilbyr offentlige nett- og kommunikasjonstjenester. Dette omfatter ikke bare infrastrukturaktører, men også aktører som har mobiltelefoni, fasttelefoni, bredbånd og lignende som hovedbeskjeftigelse – i loven kalt *erhvervsmæssige udbydere*.[24] Center for Cybersikkerhed gis relativt vidtgående myndighet for utforming av regelverk om og tilsyn med virksomhetenes informasjonssikkerhet.

I medhold av § 3 skal Center for Cybersikkerhed fastsette regler om minimumskrav til informasjonssikkerhet for tilbydere av offentlig tilgjengelige nett og tjenester. Reglene kan omfatte både tekniske, prosessuelle og organisatoriske tiltak. Ifølge forarbeidene forutsettes bemyndigelsen anvendt til administrativ fastsettelse av krav til risikostyringsprosessene, herunder krav om at sikkerhetsarbeidet skal ta utgangspunkt i relevante og anerkjente internasjonale standarder.[25] Videre kan det settes krav om at tilbydernes risikostyring skal ta høyde for sikkerhetsutfordringer ved leveranser av eksempelvis *hardware* og *software*, og utsetting av driftsoppgaver. Herunder kan det stilles krav til dokumenterte prosedyrer for verifisering av at konfigurasjonen i anskaffet *hardware*, *firmware* eller *software* ikke utgjør en trussel mot informasjonssikkerheten. Center for Cybersikkerhet kan videre pålegge at nærmere angitte forhold tas med i en virksomhets risikostyringsprosess.

Dersom det er av *væsentlig samfundsmæssig* betydning, kan virksomhetene pålegges å gjennomføre konkrete informasjonssikkerhetstiltak:

> Dette kan være funktioner, som er særligt vigtige for samfundets og demokratiets opretholdelse og sikkerhed samt borgernes tryghed, herunder funktioner inden for sundhed, energi, transport, forsyning, finans, forskning, medier og kommunikation samt funktioner, som har stor økonomisk betydning for samfundet.

Center for Cybersikkerhed fastsetter nærmere regler om hvilke konkrete tiltak som skal kunne iverksettes, eksempelvis sikkerhetsundersøkelse av *software* og *hardware* og sikkerhetsgodkjenning av personell som skal drifte kritiske deler av ekom-nettene. Som utgangspunkt må virksomheten selv bære kostnadene for gjennomføring av tiltakene. Det fremgår imidlertid av forarbeidene at slike pålegg kan innebære ekspropriative inngrep, hvilket på bakgrunn av en konkret vurdering kan gi grunnlag for erstatning.

Center for Cybersikkerhed kan ikke med hjemmel i disse reglene regulere eierforhold, fastsette forbud mot å inngå avtale med enkelte leverandører eller forbud mot eierskap av bestemte nettverk eller produkter.

Videre gir § 4 Center for Cybersikkerhed myndighet til å fastsette regler om opplysnings- og varslingsplikt. Formålet med bestemmelsen er å gi myndigheten bedre overblikk over den samlede ekom-infrastruktur. Det kan blant annet stilles krav om varsling av påtenkte avtaleinngåelser av visse leveranser til vesentlige deler av tilbydernes virksomhet.

[24] Forslag til Lov om elektroniske kommunikationsnet og -tjenester, 17. november 2010, Bemærkninger til lovforslaget.

[25] Ibid.

Erhvervsmæssige udbydere forpliktes videre til å informere om det endelige avtaleutkastet umiddelbart forut for avtaleinngåelsen. Det kan fastsettes regler om en kortere *standstill*-periode. Dette skal gi Center for Cybersikkerhed ytterligere en mulighet til å gå i dialog med tilbyderen om eventuelle informasjonssikkerhetsutfordringer. Det fremgår videre av forarbeidene at:

> [d]en foreslåede ordning giver udbyderne mulighed for at tage højde for eventuelle trusler mod informationssikkerheden i forbindelse med aftaleforhandlingerne. Dermed får udbyderne mulighed for at undgå, at de efterfølgende mødes af uforudsete krav til informationssikkerheden i deres net og tjenester.

Det kan også fastsettes regler for varsling av brudd på informasjonssikkerheten som har vesentlig betydning for leveransen av nett eller tjenester.

Loven har videre bestemmelser om beredskaps- og andre ekstraordinære situasjoner, om sikkerhetsklarering av personell og tilsyn. Som ledd i tilsynsvirksomheten kan Center for Cybersikkerhed i medhold av § 10 blant annet offentliggjøre en rekke av de vedtak som fattes i medhold av loven, resultater av tilsyn og resyméer av dommer der det er idømt bot i medhold av loven.

8.4.4 Storbritannia

I Storbritannia benyttes de tre sikkerhetsgraderingene OFFICIAL, SECRET eller TOP SECRET, for beskyttelse av informasjon.[26] Tidligere opererte man i Storbritannia med seks graderinger.

Det skal foretas en vurdering av all informasjon som myndighetene (*Government*) behandler. Denne skal baseres på en vurdering av skadepotensialet ved uautorisert tilgang til, tap eller misbruk av informasjonen. Alle som samarbeider med eller arbeider på oppdrag for myndighetene må også respektere retningslinjene.

Graderingen danner grunnlaget for hvilke tiltak for personell-, fysisk- og informasjonssikkerhet som må iverksettes.

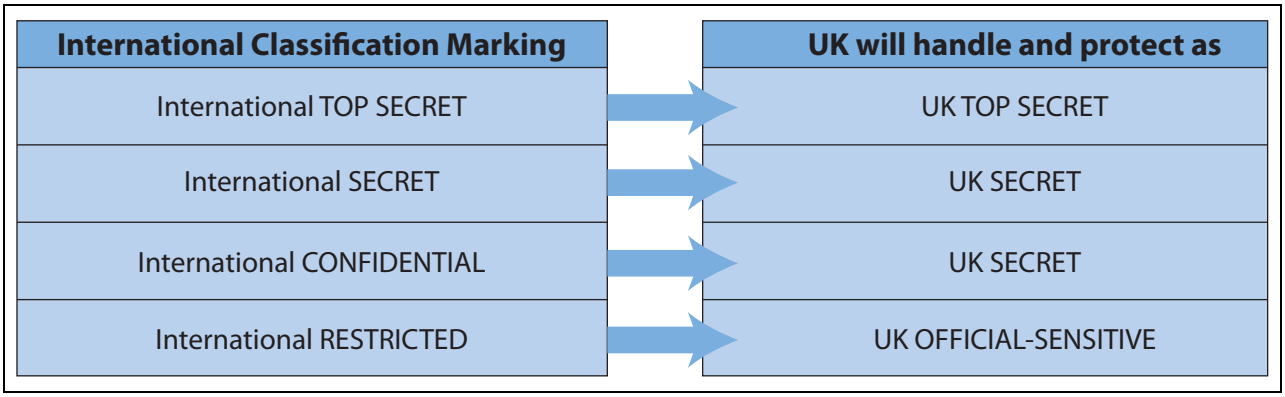
I kategorien OFFICIAL faller majoriteten av informasjonen som blir behandlet i offentlig sektor. Dette er informasjon hvis tap eller publisering kan ha skadelige konsekvenser, men som det ikke knytter seg særlige trusler til. Beskyttelsesbehovet sammenlignes her med større private virksomheter som leverer verdifulle tjenester og behandler verdifull informasjon. Særlig aktuelle trusselaktører som tiltakene skal beskytte mot er *hacktivister*, kompetente individuelle *hackere* og flertallet av kriminelle grupper og individer.

SECRET brukes om informasjon som er særlig sensitiv. Sikkerhetstiltakene skal beskytte informasjonen mot meget kompetente trusselaktører, som for eksempel særlig kapable kriminelle grupper og noen statlige aktører, og dermed unngå betydelig skadefølger for blant annet militære kapasiteter, internasjonale relasjoner og etterforskningen av alvorlig kriminalitet.

TOP SECRET gjelder for den mest sensitive informasjonen, som hvis den kommer på avveie, kan innebære betydelig tap av liv eller på annen måte true nasjonen eller alliertes sikkerhet eller økonomiske velferd (*economic wellbeing*). Informasjonen må beskyttes mot de mest sofistikerte angrepene fra særlig kapable statlige aktører, og svært liten risiko aksepteres.

I *International Classified Exchanges*, utgitt av *Cabinet Office*, gis det retningslinjer for behand-

[26] Cabinet Office, *Government Security Classifications*, 2014.



Figur 8.1 Forholdet mellom internasjonal og britisk sikkerhetsgradering.

Kilde: Cabinet Office, *International Classified Exchanges*, v. 1.2 – Jul 2015.

ling av internasjonal sikkerhetsgradert informasjon. Forholdet mellom de ulike graderingene fremgår av figur 8.1.

Det legges i veiledningen til grunn at det er nær forbindelse mellom nasjonale og internasjonale sikkerhetskrav for de korresponderende graderinger. Som det fremgår av figur 8.1, opereres det i praksis med to nivåer innen OFFICIAL – OFFICIAL-SENSITIVE og OFFICIAL.

Med utgangspunkt i figur 8.1, med sammenstilling av graderingsnivåer, kan også beskyttelsestiltakene for de ulike graderingene sammenlignes. For eksempel skal sikkerhetstiltakene for beskyttelse av UK OFFICIAL-SENSITIVE i hovedsak være de samme som for beskyttelse av BEGRENSET etter den norske sikkerhetsloven. For behandling av informasjon som er kategorisert internasjonalt RESTRICTED, har *Cabinet Office* utarbeidet en egen veileder,[27] som i grove trekk gir et sammendrag av Storbritannias internasjonale forpliktelser. Kravene er kjent fra norsk regulering, og det vises blant annet til *need-to-know*-prinsippet, varsling, merking, sikkerhetsstyring, fysisk håndtering, deling og at det ikke er krav om sikkerhetsklarering. Informasjonssystemer som skal behandle slik informasjon må være sikkerhetsgodkjent, og for øvrig oppfylle kravene som følger av den aktuelle internasjonale organisasjonens retningslinjer.

8.4.5 EU

8.4.5.1 Informasjonssikkerhet i EU

Det europeiske Rådet fattet 23. september 2013 beslutning om regler for beskyttelse av EUs sikkerhetsgraderte informasjon (2013/488/EU). Beslutningen fastsetter prinsipper og minimumsstandarder for beskyttelse av sikkerhetsgradert EU-informasjon (*EU classified information* – EUCI). Beslutningen gjelder for Rådet og dets sekretariat og skal overholdes av medlemslandene i henhold til nasjonalt regelverk, slik at enhver kan være trygg på at informasjonen beskyttes tilstrekkelig.

Informasjon skal sikkerhetsgraderes ut fra en vurdering av skadepotensialet uautorisert tilgang til informasjonen kan få for EU eller en eller flere av medlemsstatenes interesser, jf. beslutningen art. 2. EU TOP SECRET brukes dersom uautorisert tilgang kan få avgjørende skadefølger,[28] EU SECRET ved mulige betydelige skadefølger for vesentlige interesser, EU CONFIDENTIAL ved mulige skadefølger for EUs vesentlige interesser eller EU RESTRICTED ved mulige negative følger for EUs interesser.

Boks 8.2 EUs prinsipper for cybersikkerhet

- EUs kjerneverdier gjelder tilsvarende i den digitale som i den fysiske verden
- Beskyttelse av fundamentale rettigheter, ytringsfrihet, personvern og personopplysninger
- Tilgang for alle
- Demokratisk og effektiv multi-stakeholder styring
- Et felles ansvar for å ivareta sikkerheten

Videre er det bestemmelser om blant annet merking, risikostyring, personellsikkerhet, fysisk sikkerhet, forvaltning av gradert informasjon og industrisikkerhet.

Art. 10 regulerer beskyttelse av gradert informasjon som behandles i kommunikasjons- og informasjonssystemer, og det følger av art. 10(1):

> Ved informasjonssikring (IA) i forbindelse med kommunikasjons- og informasjonssystemer forstås tilliten til, at disse systemer beskytter den informasjon, de håndterer, og at de fungerer, som de skal, når de skal, under de legitime brukeres kontroll. Effektiv IA sikrer et passende nivå for fortrolighet, integritet, tilgjengelighet, uavviselighet og autensitet. IA baseres på en risikostyringsprosess.

Alle informasjonssystemer som skal behandle gradert informasjon må godkjennes, med det formål å sikre at alle nødvendige sikkerhetstiltak er gjennomført, og at det er oppnådd tilstrekkelig grad av beskyttelse. Kryptoutstyr må også godkjennes i henhold til art. 10(6).

Ifølge direktivet skal hver medlemsstat etablere en rekke myndighetsfunksjoner, som blant annet nasjonal sikkerhetsmyndighet, kompetent myndighet og sikkerhetsgodkjenningsmyndighet.

---

[27] Cabinet Office, *Guidance: Protecting international RESTRICTED classified information,* version 1.1, July 2014.

[28] Engelsk: exceptionally grave prejudice, Svensk: synnerligt men, Dansk: overordentlig alvorlig skade for EUs vesentlige interesser.

8.4.5.2 NIS-direktivet

Den 7. februar 2013 lanserte EU-kommisjonen EUs strategi for cybersikkerhet, *An Open, Safe and Secure Cyberspace*.[29] Strategien fastsetter EUs prinsipper for cybersikkerhet, se tekstboks 8.2. Som ett av flere tiltak for å nå målene i strategien lanserte Kommisjonen samtidig et forslag til direktiv om tiltak for et høyt felles sikkerhetsnivå i nettverks- og informasjonssystemer i EU (NIS-direktivet).[30]

Direktivet ble vedtatt i EU 6. juli 2016. Formålet med direktivet er å forbedre funksjonaliteten til det indre markedet, gjøre EU mer konkurransedyktig i en globalisert verden, skape tillit til digitale tjenester og bidra til økonomisk vekst i Europa.

Direktivet retter seg mot medlemslandene, som hver for seg pålegges å sørge for gjennomføring av direktivet. For noen deler legges det likevel opp til at det skal foregå et internasjonalt samarbeid om implementeringen. Ulike deler av direktivet skal oppfylles av medlemslandene til ulike tider. Blant annet skal medlemsstatene delta i samarbeidsgruppene innen 6 måneder, og identifisere hvilke virksomheter som anses omfattet av direktivet innen 27 måneder. Det er foreløpig ikke tatt endelig stilling til om direktivet kommer inn under EØS-avtalen og dermed skal implementeres i Norge.

Grovt sett kan direktivet deles i tre hoveddeler, som setter krav til henholdsvis etablering av nasjonale rammeverk for IKT-sikkerhet, etablering av internasjonale samarbeidsfora og IKT-sikkerhet for virksomheter.

Nasjonale rammeverk og internasjonalt samarbeid

Det går uttrykkelig frem av art. 1(6) at direktivet ikke skal innskrenke medlemslandenes frihet til å ivareta nasjonal sikkerhet eller opprettholde lov og orden.

Det følger av art. 1(7) at dersom eksisterende sektorregelverk stiller krav om IKT-sikkerhet eller hendelsesvarsling, og reglene har minst like god effekt som NIS-direktivet, skal sektorregelverket anvendes.

Medlemslandene plikter å utarbeide og implementere en nasjonal IKT-sikkerhetsstrategi, jf. art. 7. Bestemmelsen setter kvalitative krav til strategiens innhold. Medlemslandene må også peke ut – eventuelt først etablere – en eller flere CSIRTer (*Computer Security Incident Response Team*), jf. art. 9. Nærmere krav til CSIRTen fremgår av direktivet vedlegg I. Strategien og CSIRTen(e) må ha et virkeområde som minst dekker de virksomheter som omfattes av NIS-direktivet.

Etter art. 8 plikter medlemslandene å peke ut en eller flere nasjonale kompetente myndigheter for IKT-sikkerhet, som skal påse at direktivet implementeres nasjonalt. Et kontaktpunkt (*single point of contact*) må også utpekes, som skal ivareta samarbeid mellom medlemslandene, samarbeid med relevante nasjonale myndigheter i andre land, i samarbeidsgruppen og i CSIRT-gruppen. En eksisterende myndighet kan pekes ut til å være både kompetent myndighet og *single point of contact*. Dersom CSIRTen og kontaktpunktet er separate virksomheter, plikter disse å samarbeide, jf. art. 10.

Gjennom art. 11 etablerer direktivet en samarbeidsgruppe bestående av representanter fra medlemslandene, Kommisjonen og det europeiske byrået for nettverks- og informasjonssikkerhet (ENISA). Kommisjonen ivaretar sekretariatsfunksjonen. Samarbeidsgruppen skal blant annet utarbeide en handlingsplan for implementering av direktivet, strategiske råd til CSIRT-nettverket og utveksle *best-practice* om medlemslandenes identifisering av essensielle tjenester, kapasitetsbygging, og informasjonsdeling relatert til hendelseshåndtering.

For å bidra til trygghet og tillit mellom medlemslandene etablerer direktivet i art. 12 et nettverk bestående av de nasjonale CSIRTene og CERT-EU. EU-Kommisjonen skal ha observatørstatus, og ENISA skal holde sekretariatet. Nettverket skal blant annet dele informasjon om tjenester, operasjoner og samarbeidskapasiteter med hverandre, bidra til håndtering av grensekryssende hendelser, og i noen tilfeller diskutere samlet respons på hendelser.

IKT-sikkerhet for virksomheter

I art. 14 og 16 stilles det krav om at medlemslandene sørger for sikkerheten i nettverkene og informasjonssystemene tilhørende to kategorier av virksomheter: Operatører av essensielle tjenester og tilbydere av digitale tjenester. Det stilles forskjellige sikkerhetskrav til disse to kategoriene virksomheter. Felles for alle virksomhetene er imidlertid at de nettverk og informasjonssystemer virksomhetene benytter seg av skal beskyttes.

Virksomheter som oppfyller vilkårene i art. 4(4), anses som operatører av essensielle tjenes-

[29] JOIN(2013) 1 final.
[30] 2013/0027 (COD).

Boks 8.3 NIS-direktivet: Sektorer med operatører av essensielle tjenester

- Energi (*elektrisitet, olje og gass*)
- Transport (*luft, jernbane, sjø og vei*)
- Helse (*helsetjenester*)
- Bank
- Finansmarkeds-infrastruktur
- Drikkevannsforsyning og -distribusjon
- Digital infrastruktur

ter. For det første må virksomheten være nevnt i direktivets vedlegg II, som er en opplisting av relevante operatører i markedet. For det andre må virksomheten oppfylle vilkårene i art. 5(2). Virksomheten må tilby en tjeneste som er essensiell for opprettholdelse av kritiske samfunnsmessige og/eller økonomiske aktiviteter, tjenesteleveransen må være avhengig av nettverk og informasjonssystemer, og en hendelse i tjenestens nettverk og informasjonssystemer vil få en *vesentlig forstyrrende virkning* på leveransen. Ved vurderingen av hva som er *vesentlig forstyrrende virkning*, skal både tverrsektorielle og sektorspesifikke momenter tas i betraktning, jf. art. 6.

Innen 27 måneder etter direktivets ikrafttreden skal medlemslandene ha identifisert hvilke virksomheter som omfattes av direktivet. Deretter skal medlemsstatene sørge for at operatørene av essensielle tjenester iverksetter sikkerhetstiltak, jf. art. 14.

Sikkerhetstiltakene er ikke konkret angitt. En risikobasert tilnærming skal danne grunnlaget for iverksetting av sikkerhetstiltak som står i rimelig forhold til risikoen. Opprettholdelse av tjenesteleveransen er hovedmålet med tiltakene.

Operatører av essensielle tjenester må også varsle om alvorlige sikkerhetshendelser til en på forhånd bestemt kompetent myndighet eller CSIRT. Hvor mange mennesker som er rammet av hendelsen, geografisk omfang og hendelsens varighet, er bestemmende for om hendelsen skal anses som alvorlig, jf. art. 14(4). Det skal kun varsles om hendelser som faktisk innvirker negativt på tjenesteleveransen. Kompromittering av konfidensialitet, integritet eller tilgjengelighet er ikke varslingsgrunn når det ikke har betydning for tjenesteleveransen.

For den andre kategorien av virksomheter – tilbydere av digitale tjenester – er det ikke en tilsvarende utpekingsprosess. Art. 16 sier at medlemsstatene skal sørge for at tilbydere av tjenester som opplistet i vedlegg III til direktivet, sikrer sine nettverk og informasjonssystemer. Berørte virksomheter er tilbydere av nettbaserte markedsplasser, jf. art. 4(17), nettbaserte søkemotorer, jf. art. 4(18) og skytjenester, jf. art 4(19).

Også for denne kategorien skal en risikobasert tilnærming danne grunnlaget for iverksetting av tiltak som står i et rimelig forhold til den risiko virksomheten er utsatt for. Sikkerhetstiltakene skal blant annet adressere systemsikkerhet, hendelseshåndtering og kontinuitet i tjenesteleveransen.

Denne kategorien virksomheter skal varsle om alvorlige sikkerhetshendelser, og de samme momenter skal vurderes for å bestemme hendelsens alvorlighetsgrad. I tillegg skal omfanget av forstyrrelsen for tjenestens funksjon og virkningen for økonomiske og samfunnsmessige aktiviteter vurderes, jf. art. 16(4).

Fordi virksomheter i denne kategorien ofte leverer tjenester på tvers av landegrenser, står medlemslandene i mindre grad fritt til å fastsette andre sikkerhetskrav enn direktivet.

8.5 Utvalgte tema

8.5.1 Informasjon som må beskyttes

For å kunne iverksette hensiktsmessige sikkerhetstiltak for å beskytte informasjon, trengs det en nærmere analyse av informasjonen som behandles og hvilke sårbarheter og trusler det må tas høyde for.

For det første må informasjonens verdi angis. Verdivurderingen gir svaret på om informasjonen er beskyttelsesverdig. Informasjonens verdi deles ofte opp i ulike kategorier. De mest brukte er konfidensialitet, integritet og tilgjengelighet. Avhengig av situasjonen benyttes også eksempelvis sporbarhet, ikke-benektbarhet[31] og flere andre. I det videre er det tilstrekkelig å benytte de tre hovedkategoriene.

Med *konfidensialitet* menes at det har en verdi at informasjonen ikke blir kjent for uvedkommende. Et eksempel på informasjon som må beskyttes av konfidensialitetshensyn, er Norges Banks sikkerhetsrutiner.

Med *integritet* menes at det har en verdi at informasjonen er korrekt. Eksempelvis må programkode være korrekt for at dataprogrammet skal virke. Beskyttelse mot tap av integritet inne-

[31] Det å knytte en handling til avsender slik at avsender ikke senere kan benekte å stå bak handlingen.

bærer å sørge for at det ikke lar seg gjøre å endre programkoden. I motsetning til beskyttelse av konfidensialitet er det ikke viktig om andre kan lese programkoden.

Med *tilgjengelighet* menes at det har en verdi at informasjonen er tilgjengelig ved behov. Eksempelvis er det fordelaktig å ha bruksanvisningen til badevekten som er tilkoblet hjemmenettverket tilgjengelig den dagen det kommer opp en feilmelding i displayet. Beskyttelse eller ivaretakelse av tilgjengeligheten kan innebære å mangfoldiggjøre informasjonen og oppbevare den på et lett tilgjengelig sted.

Dersom verdivurderingen konkluderer med at informasjonen er beskyttelsesverdig, er neste steg å vurdere informasjonens beskyttelsesbehov. Det må foretas en vurdering av aktuelle sårbarheter og trusler.

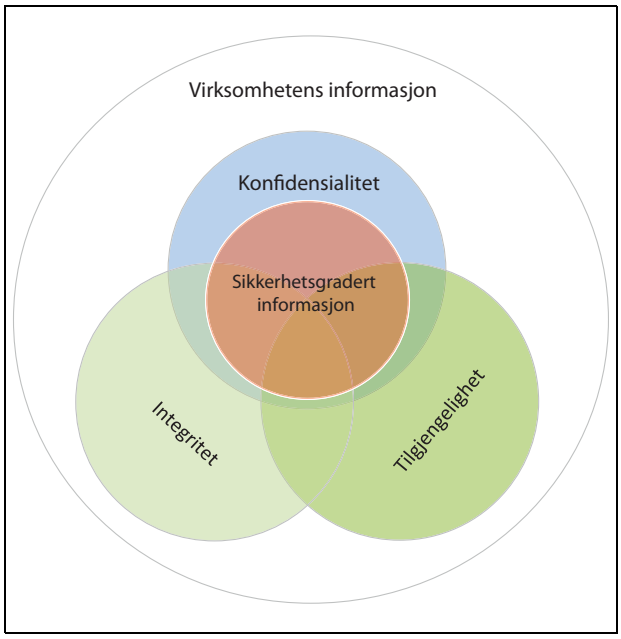
I mange tilfeller vil verdivurderingen vise at informasjonen er verdifull i flere henseender. Nasjonale beredskapsplaner kan tjene som eksempel. Om planene er kjent for trusselaktøren, kan de lett bli mindre effektive. Integriteten må ivaretas slik at man kan stole på at planen er korrekt. Tilgjengeligheten må også ivaretas slik at de som skal iverksette tiltak har planen for hånden når situasjonen tilsier det.

Eksempelet viser at sikkerhetstiltakene må tilpasses informasjonens konkrete beskyttelsesbehov. For å kunne iverksette hensiktsmessige sikkerhetstiltak, må verdi, sårbarheter og trusler ses i sammenheng.

Dagens sikkerhetslov følger delvis denne fremgangsmåten. Det skal først foretas en verdivurdering, som danner grunnlaget for om informasjonen skal anses beskyttelsesverdig og, som dermed skal sikkerhetsgraderes. Men etter sikkerhetsloven § 11 er det kun konfidensialitetshensynet som skal vurderes. I kapittel 8.2.1 er verdivurderingen behandlet nærmere. Dette innebærer at informasjon som ikke har konfidensialitetsbehov ikke beskyttes av sikkerhetsloven.

Sikkerhetsloven anerkjenner imidlertid at sikkerhetsgradert informasjon kan ha andre beskyttelsesbehov enn konfidensialitet, jf. sikkerhetsloven § 12 andre ledd andre punktum som gir Kongen myndighet til å «gi regler om plikt til å legge forholde til rette for at sikkerhetsgradert informasjon er korrekt, fullstendig og tilgjengelig.»

Informasjonssikkerhetsforskriften kapittel 5 Informasjonssystemsikkerhet Del E. Sikkerhetsdokumentasjon, § 5-40 fastsetter at «[bruker]instruksen skal være kjent og lett tilgjengelig for alle brukere. I forskriften kapittel 4 Dokumentsikkerhet, § 4-27 Utlånskontroll er hovedregelen at sikkerhetsgraderte dokument ikke skal beholdes av saksbehandler over lengre tid og returneres arkivet. Det gjøres av hensyn til tilgjengeligheten unntak for blant annet beredskapsplaner. For digital informasjon – i informasjonssikkerhetsforskriften kalt data – er det i informasjonssikkerhetsforskriften §§ 5-1, 5-3 og 5-7 gitt tydeligere og mer generelle krav om beskyttelse av tilgjengelighet og integritet.



Figur 8.2 Sikkerhetsgradert informasjon.

Fraværet av regler kan tyde på at lovgiver ikke i særlig grad har sett stort behov for beskyttelse av verken tilgjengelighet eller integritet. Det er likevel grunn til å tro at disse forholdene i praksis er en del av helhetsvurderingen når det skal avgjøres hvilke sikkerhetstiltak som skal iverksettes.

Forholdet mellom de ulike verdikategoriene er forsøkt illustrert i figur 8.2. Figuren tar utgangspunkt i en virksomhets totale informasjonsmengde. Merk at forholdene mellom størrelsen på sirklene og tangeringspunkter ikke er ment som angivelser av reelle størrelsesforhold mellom de ulike typer av informasjon.

Noe informasjon er ikke beskyttelsesverdig om man nøyer seg med å vurdere konfidensialitet, integritet og tilgjengelighet. Dette er farget hvitt. Noe informasjon hører hjemme i én kategori, noe i to og annen i tre kategorier. Den røde sirkelen angir sikkerhetsgradert informasjon. Blant denne informasjonen vil det også være informasjon med ulikt beskyttelsesbehov – noe har integritetsbe-

hov, noe har tilgjengelighetsbehov og noe faller innenfor alle kategoriene. Fellesnevneren for sikkerhetsgradert informasjon er imidlertid at det alltid vil være behov for beskyttelse mot brudd på konfidensialiteten.

8.5.2 Informasjonssystemer som må beskyttes

Det er to hovedkategorier av informasjonssystemer som må beskyttes av hensyn til nasjonal sikkerhet. Den første kategorien er systemer som behandler sikkerhetsgradert informasjon. Dette vil normalt være de tradisjonelle informasjonssystemer hvis hovedfunksjon er å tjene som saksbehandlingsstøtte. Informasjonssystemene i den andre kategorien har det til felles at systemets funksjonalitet er svært viktig for at virksomheten skal kunne levere sine kritiske tjenester. I denne kategorien finner vi både tradisjonelle kontorstøttesystemer og kontroll- og styringssystemer. Eksempler på slike systemer kan være et departements saksbehandlingssystem og et styringssystem som har en viktig rolle i strømproduksjonen.

Sistnevnte gruppe, kontroll- og styringssystemer, også kalt prosesskontrollsystemer, SCADA-systemer og industriprosesskontrollsystemer, skiller seg ofte fra de mer ordinære informasjonsbehandlingssystemene. Som følge av sin funksjon behandler de normalt verken sikkerhetsgradert informasjon eller personopplysninger.

Det kan antakelig tenkes systemer der konfidensialitetsbeskyttelse vil være uvesentlig. Dette anses imidlertid ikke som hovedregelen.[32] Konfidensialitet er normalt viktig også for kontroll- og styringssystemer, om enn ikke i samme omfang som for graderte systemer, der konfidensialiteten er svært viktig.

De grunnleggende beskyttelsesbehovene vil være de samme for de to kategoriene systemer. Sikkerhetstiltak som sikkerhetsmessig overvåkning og inntrengningstesting, vil måtte utføres ganske forskjellig avhengig av type informasjonssystem. Det kan likevel slås fast at som utgangspunkt anses tiltakene som hensiktsmessige for alle typer systemer.

Samlet innebærer dette at god informasjonssystemsikkerhet handler om grundig analyse av det enkelte system der ulike hensyn vurderes i sammenheng. Denne analysen vil danne utgangspunkt for iverksetting av tilpassede sikkerhetstiltak.

Utvalget har valgt å bruke begrepet *informasjonssystem* som en fellesbetegnelse for både informasjonsbehandlingssystemer og kontroll- og styringssystemer.

8.6 Utvalgets vurderinger og forslag

For å sikre et dynamisk og tidsriktig regelverk om informasjonssikkerhet i tråd med digitaliseringen og samfunnsutviklingen, mener utvalget det må gjøres endringer i dagens sikkerhetslov. Spesielt gjelder dette beskyttelse av informasjonssystemer, som har fått en langt tydeligere og større plass i forslaget til ny lov. Videre er det også gjort tilpasninger for bedre å ivareta personvernet. For øvrig er endringene av redaksjonell og språklig karakter.

8.6.1 Beskyttelse av sikkerhetsgradert informasjon og tilhørende informasjonssystemer

Dagens system for beskyttelse av sikkerhetsgradert informasjon, herunder gradering og beskyttelse av informasjonssystemer, fungerer godt per i dag og har fungert godt i lang tid. Systematikken bygger på, og er nært tilknyttet, NATO-regelverket. Dette innebærer at den også er vel etablert i en rekke land, også utenfor NATO. I *SOU 2015:25 En ny säkerhetsskyddslag*, tas det til orde for en innføring av denne systematikken i svensk rett. Med et slikt utgangspunkt må eventuelle forslag om endringer begrunnes godt.

Som nevnt i kapittel 8.5.1 fokuserer dagens regelverk på lovs nivå særlig på informasjonens konfidensialitet. Utvalget har vurdert om informasjonens integritet og tilgjengelighet bør likestilles med konfidensialiteten. Informasjon kan i mange tilfeller være svært viktig for nasjonens sikkerhet, herunder opprettholdelse av grunnleggende nasjonale funksjoner. Dersom en trusselaktør klarer å endre, slette eller gjøre informasjonen utilgjengelig for de som trenger den, vil dette kunne ha negativ innvirkning på sentrale myndigheters evne til å opprettholde viktige funksjoner. Det er fullt mulig både å endre, slette og gjøre informasjon utilgjengelig uten at en er kjent med informasjonen. Dette vil særlig gjelde for elektronisk lagret informasjon, men også dokumenter må beskyttes mot uønsket påvirkning.

[32] National Institute of Standards and Technology, *Guide to Industrial Control Systems (ICS) Security*, NIST Special Publication 800-82, revision 2, U.S. Department of Commerce.

Utvalget har ikke funnet grunn til å endre kriteriene for angivelse av hvilken informasjon som skal beskyttes etter sikkerhetsloven. Det bør fortsatt være behovet for å bevare informasjonens konfidensialitet, som er inngangskriteriet for om informasjonen skal sikkerhetsgraderes, og dermed beskyttes etter sikkerhetsloven. Etter utvalgets syn ville det unødig komplisere identifiseringen av informasjon som skal beskyttes, dersom integritet og tilgjengelighet skulle vært ytterligere inngangskriterier. Sett i sammenheng med digitaliseringen og at viktige ugraderte informasjonssystemer skal beskyttes, legger utvalget til grunn at mye viktig ugradert informasjon fanges opp og beskyttes gjennom bestemmelsene om informasjonssystemsikkerhet.

Informasjon som er blitt sikkerhetsgradert skal så beskyttes både av hensyn til konfidensialitet, integritet og tilgjengelighet. At de to sistnevnte hensynene ikke fremgår av dagens lov, betyr antakelig ikke at de anses irrelevante. Blant annet nevnes alle hensynene som relevante for informasjonssystemsikkerhet, jf. informasjonssikkerhetsforskriften kapittel 5. Utvalget mener i alle tilfelle at plikten til å ivareta alle tre hensynene bør komme tydelig frem i loven. I denne sammenheng må det understrekes at et forsvarlig sikkerhetsnivå forutsetter en god verdivurdering.

Gjeldende sikkerhetslov sondrer mellom begrepene *skjermingsverdig informasjon* og *sikkerhetsgradert informasjon*. Førstnevnte brukes om all informasjon i materiell eller immateriell form som må beskyttes av hensyn til rikets sikkerhet. Skjermingsverdig informasjon oppfyller kriteriene for sikkerhetsgradering. Hvorvidt informasjonen har blitt sikkerhetsgradert etter sikkerhetsloven § 11 har ikke betydning for om informasjonen skal anses som skjermingsverdig. Begrepet *sikkerhetsgradert informasjon* omfatter skjermingsverdig informasjon som er blitt påført sikkerhetsgradering i henhold til § 11.

Utvalget mener det ikke er behov for å videreføre en slik sondring. Begrepet *sikkerhetsgradert informasjon* foreslås benyttet for all informasjon som trenger beskyttelse av hensyn til grunnleggende nasjonale funksjoner. Begrepet *sikkerhetsgradert informasjon* i den nye loven vil dermed omfatte både *skjermingsverdig* og *sikkerhetsgradert* informasjon etter gjeldende sikkerhetslov, det vil si all informasjon som skal beskyttes etter den nye sikkerhetsloven.

Forslaget til ny sikkerhetslov vil føre til at flere virksomheter skal behandle sikkerhetsgradert informasjon. Dette gir grunnlag for å se nærmere på hvilke praktiske konsekvenser det vil kunne få for en virksomhet å bli underlagt sikkerhetsloven når det gjelder informasjonssikkerhet.

Å være omfattet av sikkerhetsloven vil arte seg ulikt for forskjellige virksomheter. Enkelte trenger ingen graderte systemer, mange vil klare seg med kun én datamaskin som er godkjent for behandling av informasjon gradert BEGRENSET, mens vi i den andre enden av skalaen finner Etterretningstjenesten som produserer, behandler og kommuniserer høygradert informasjon kontinuerlig. De største brukerne av gradert informasjon er allerede i dag omfattet av loven, og lovforslaget vil således ikke ha større konsekvenser for disse. Blant virksomhetene som per i dag er omfattet av loven, opererer mange i praksis med både graderte og ugraderte systemer. Det er kun ved beskyttelse av graderte informasjonssystemer at det tas hensyn til minimumsstandardene i NATO-regelverket.

Videre er det ikke slik at en virksomhet som går fra å være ikke omfattet til å være omfattet av sikkerhetsloven vil måtte bytte ut alle sine IKT-systemer. Det kommer an på hvilken sikkerhetsrisiko den enkelte virksomhet står overfor og hvilket behov den har for å behandle sikkerhetsgradert informasjon.

Utvalget legger til grunn at de aller fleste virksomheter ikke trenger å kommunisere informasjon som er høyere gradert enn BEGRENSET. Dette for å kunne ta imot trusselinformasjon og ta tilstrekkelig del i nødvendig informasjonsdeling. Beredskapsplanverket er gradert og trusselinformasjon er ofte gradert. At mange virksomheter gjøres i stand til å kommunisere BEGRENSET-informasjon, vil være et stort fremskritt for landets sikkerhet. Det kan være nyttig å kunne behandle også høyere gradert informasjon, men oppgraderingen fra ugradert til BEGRENSET er det aller viktigste steget slik situasjonen er per i dag.

Alternativet til dagens systematikk ville være å etablere et nasjonalt regime for behandling av nasjonal sensitiv informasjon i tillegg til NATO-regimet. Dette er blitt gjort blant annet i Storbritannia, som nevnt ovenfor. Etter utvalgets oppfatning vil det bli komplisert å forholde seg til en slik løsning i praksis. Dette er i tråd med synspunktene i forarbeidene til dagens lov og flere andre nasjoner, senest Sverige. Det vil kunne bli kostbart å etablere en helt ny informasjons- og kommunikasjonsinfrastruktur med høyt sikkerhetsnivå. Ikke minst gjelder det for aktører som jevnlig produserer og behandler mye høygradert informasjon.

NATO-regelverket og dets brede oppslutning har klare fordeler. Kontakten med våre allierte forenkles i stor grad nettopp fordi vi gjennom et felles og anerkjent regelverk har de samme forpliktelsene. Vi kan stole på at andre tar godt vare på nasjonal og felles sensitiv informasjon. Et felles minimumsnivå for håndtering av gradert informasjon muliggjør dessuten også digital kommunikasjon i større grad.

Utvalget har i sin kontakt med virksomheter underlagt sikkerhetsloven, ikke fått inntrykk av at det knytter seg slike utfordringer til behandlingen av gradert informasjon at reglene bør endres. Det er snarere utfordringer når det kommer til samhandling og praktisering av regelverket. Dette er forhold som ikke løses ved å etablere et nytt regime for beskyttelse av sikkerhetsgradert informasjon.

Utvalget har ikke sett det som formålstjenlig å gjennomføre en grundig analyse av NATO-regelverket. Det fremstår likevel som klart at det for den enkelte nasjon foreligger et betydelig handlingsrom ved vurderingen av hva som må til for å oppfylle minstekravene for håndtering av NATO-gradert informasjon. Dette handlingsrommet er godt utnyttet per i dag, men kan antakelig utnyttes i enda større grad ved behov.

Ut over fremhevingen av at informasjonens integritet og tilgjengelighet også skal ivaretas, foreslår utvalget derfor at dagens regler for behandling av sikkerhetsgradert informasjon i all hovedsak videreføres med de tilpasninger som er nødvendige av hensyn til den nye lovens innretning. Imidlertid bør det ved utarbeidelse av en ny informasjonssikkerhetsforskrift søkes å gjøre systemet så fleksibelt som mulig. Videre bør, i tråd med utvalgets forslag for øvrig, både sektorovergripende og sektorspesifikke hensyn ivaretas så godt det lar seg gjøre. Dette innebærer blant annet å la sektormyndigheter ta ansvar for sikkerheten i egen sektor der NATO-regelverket åpner for dette. Utarbeidelsen av regelverket bør skje som et samarbeid mellom relevante aktører.

8.6.2 Beskyttelse av ugradert informasjon og ugraderte informasjonssystemer

I mandatet er utvalget bedt om å vurdere behovet for å beskytte ugraderte IKT-systemer og informasjon som er sensitiv, men ikke sikkerhetsgradert. Utvalget legger til grunn en vid forståelse av begrepet *ugraderte informasjonssystemer*. Det omfatter alle informasjonssystemer som ikke behandler sikkerhetsgradert informasjon. Denne type informasjons- og kommunikasjonssystemer kan være av avgjørende betydning for om en virksomhet evner å opprettholde sin kritiske rolle og levere sine kritiske tjenester. Slike systemer er dermed av kritisk betydning for grunnleggende nasjonale funksjoner. Her stilles det ikke internasjonale krav til sikkerhet og sikkerhetsnivået og sikkerhetstiltakene kan tilpasses det enkelte systems skjermingsbehov.

I kategorien ugraderte IKT-systemer befinner det seg både tradisjonelle informasjons- og kommunikasjonssystemer, og såkalte kontroll- og styringssystemer.[33] Nærmere bestemt er dette datasystemer som styrer, og eller kontrollerer, industrielle prosesser og tjenesteleveranser, eksempelvis innenfor telekom og strømproduksjon. Utvalget mener at denne typen systemer, i den grad de er kritiske for grunnleggende nasjonale funksjoner, må beskyttes mot uønskede tilsiktede hendelser. Konfidensialiteten er ikke nødvendigvis like viktig for disse systemene, men den kan heller ikke avskrives. Her som ellers må det foretas en konkret vurdering av det enkelte systems skjermingsbehov. Først etter en slik vurdering blir det klart om informasjonens konfidensialitet må beskyttes.

De ugraderte IKT-systemer som skal beskyttes etter den nye loven, har det til felles at dersom systemet faller ut vil det svekke virksomhetens evne til å understøtte eller opprettholde den grunnleggende nasjonale funksjonen som gjør at de omfattes av sikkerhetsloven. Et grunnleggende spørsmål ved vurderingen er: hva må beskyttes for at den grunnleggende nasjonale funksjonen skal opprettholdes?

I mange tilfeller vil det være klart hvilken kategori det enkelte system faller inn under, i andre tilfeller kan systemene havne i begge kategorier. Utvalget har ikke funnet det hensiktsmessig å problematisere, definere og kategorisere aktuelle IKT-systemer nærmere. Utvalget mener at den beste måten å identifisere hvilke IKT-systemer som er skjermingsverdige på, er at det foretas en konkret vurdering i hver virksomhet. Virksomhetens ROS-analyse, jf. lovforslaget § 4-3, skal identifisere hvilke ressurser, inkludert IKT-systemer, som er nødvendig for opprettholdelse av funksjonalitet.

For det tilfelle at et IKT-system både behandler sikkerhetsgradert informasjon og utgjør en viktig brikke i en virksomhets funksjonalitet, må systemets samlede beskyttelsesbehov danne

[33] Generelt om kontroll- og styringssystemer, US National Institute of Standards and Technology, *Guide to Industrial Control Systems (ICS) Security*, 800-82r2.

utgangspunkt for hvilket sikkerhetsnivå som er riktig. Hvis for eksempel et BEGRENSET system er svært viktig for at en sentral myndighet skal være i stand til å ivareta sin funksjon i krise eller krig, kan det være grunn til å ha et høyere sikkerhetsnivå enn det som følger av NATO-kravene for informasjonssystemer som skal behandle BEGRENSET informasjon. En slik helhetlig tilnærming vil følge av lovforslaget § 6-2, jf. § 4-1.

8.6.3 Informasjonssystemer og infrastruktur

Utvalget har vurdert om IKT-sikkerhet hører hjemme under informasjonssikkerhet, infrastruktursikkerhet, eller om det er det noe eget. Informasjons- og kommunikasjonssystemer er hjelpemidler for å produsere, lagre, kryptere og formidle informasjon. Slik utvalget benytter seg av begrepet informasjonssystemer, omfattes også kontroll- og styringssystemer for ulik tjenesteproduksjon, industriprosesser og telekom infrastruktur. Informasjonssystemer kan også kalles informasjonsinfrastruktur, og slik utvalget oppfatter det hører informasjonssystemsikkerhet hjemme under både informasjonssikkerhet og infrastruktursikkerhet. I noen tilfeller er informasjonssystemets rolle som informasjonsbehandler fremtredende, mens det i andre tilfeller er systemets rolle i tjeneste- og industriproduksjon som er viktigst.

Til tross for det vide spekteret av bruksområder, har IKT-systemene flere felles egenskaper, som gjør det hensiktsmessig med en felles behandling. Både trusler og sårbarheter er relativt likeartede. Videre vil det være flere sikkerhetstiltak som er egnet for alle typer systemer, for eksempel logging og inntrengningstesting. IKT-systemer skiller seg dessuten fra annen infrastruktur ved at de fysiske egenskapene er annerledes. Ett IKT-system kan være lokalisert på forskjellige steder. Man kan få tilgang til systemet uten å være fysisk til stede. Ulike IKT-systemer står overfor det samme trussel- og sårbarhetsbildet. På denne måten skiller IKT-systemer seg fra annen type infrastruktur. Disse momentene har vært avgjørende for utvalgets forslag om å regulere beskyttelse av IKT-systemer i et eget kapittel i loven.

Utvalget vil imidlertid understreke betydningen av å se på de ulike aspektene av sikkerhet i sammenheng. Et skjermingsverdig IKT-system er ikke godt nok beskyttet bare gjennom reglene om informasjonssystemsikkerhet. Informasjons-, informasjonssystem-, personell- og infrastruktursikkerhet må ses i sammenheng for å oppnå tilstrekkelig beskyttelse. Er et systems funksjonalitet viktig, og det er enkelt å skaffe seg fysisk tilgang til systemet, er det naturlig nok ikke tilstrekkelig å iverksette logiske sikkerhetstiltak. Da er det også behov for fysisk beskyttelse, og personer som skal ha tilgang må være autorisert.

Som samlebetegnelse for alle IKT-systemer som skal beskyttes etter loven – både graderte og ugraderte – foreslår utvalget å benytte begrepet *skjermingsverdige informasjonssystemer*.

I den utstrekning skjermingsverdige informasjonssystemer også blir identifisert og utpekt som skjermingsverdig infrastruktur, jf. lovforslaget § 7-1, vil bestemmelsene om objekt- og infrastruktur også være aktuelle for sikring av slike informasjonssystemer.

8.6.4 Sikkerhetstiltak

Utvalget foreslår en videreføring av de fleste av dagens lovbestemmelser om sikkerhetstiltak. Sikkerhetsmessig godkjenning, monitoring, inntrengningstesting, sikkerhetsmessig overvåkning og tekniske sikkerhetsundersøkelser foreslås videreført. Kryptosikkerhet foreslås derimot ikke videreført i loven.

Utvalget mener at *sikkerhetsmessig godkjenning av informasjonssystemer* er et viktig sikkerhetstiltak som bør videreføres. Utvalget har vurdert om også ugraderte informasjonssystemer som omfattes av loven, bør underlegges et slikt godkjenningssystem. En godkjenningsplikt vil kunne bidra til at både anskaffelse og anvendelse av så vidt viktige informasjonssystemer holder et forsvarlig sikkerhetsnivå. Når det gjelder informasjonssystemer som skal behandle sikkerhetsgradert informasjon, anbefaler utvalget at dagens krav til forhåndsgodkjenning videreføres. Det kan imidlertid stille seg annerledes for ugraderte informasjonssystemer. Det kan også for slike systemer være riktig å kreve forhåndsgodkjenning. Utvalget mener likevel at det for disse systemene ikke skal være en lovbestemt plikt til forhåndsgodkjenning. Dette vil dessuten gjøre overgangen fra gjeldende til ny sikkerhetslov enklere. Utvalget anbefaler at det overlates til Kongen å utforme nærmere bestemmelser om godkjenningsprosessen. Dette inkluderer om det er behov for ulike løsninger i ulike sektorer eller for ulike typer informasjonssystemer, hvor omfattende prosessene skal være, og hvem som skal gis myndighet til å kunne godkjenne slike systemer.

Monitoring, jf. sikkerhetsloven § 15 gjelder kun for informasjonssystemer som er godkjent for behandling av sikkerhetsgradert informasjon og

systemer hvor sikkerhetsgradert informasjon kan tenkes behandlet eller kommunisert. Tiltaket innebærer å kontrollere om det i et informasjonssystem befinner seg eller kommuniseres informasjon som er høyere sikkerhetsgradert enn det systemet er godkjent for. Utvalget har ikke undersøkt i hvor stor utstrekning virksomheter i dag benytter seg av denne tjenesten fra Nasjonal sikkerhetsmyndighet. Utvalget har på den andre siden heller ikke mottatt signaler om at tiltaket er unødvendig. Utvalget viser for øvrig til omtalen av monitoring i kapittel 8.2.1.3, herunder de drøftelsene som ble gjort i forarbeidene om tiltaket. Utvalget slutter seg i hovedsak til de vurderingene som da ble gjort. Når utvalget foreslår en videreføring må det understrekes at det er en absolutt forutsetning om en videreføring også av forbudet mot kontroll av privat kommunikasjon og kommunikasjon med virksomheter som ikke er underlagt sikkerhetsloven.

Bestemmelsen om *inntrengningstesting* foreslås også videreført. Til forskjell fra monitoring vil dette sikkerhetstiltaket gjelde for alle ugraderte informasjonssystemer. Utvalget har vurdert å lovfeste en plikt for virksomheten til å få gjennomført denne typen tester, men har kommet til at det ikke er behov for det. Av hensyn til de forskjelligartede informasjonssystemer som omfattes av bestemmelsen, kunne beskrivelsen av plikten vanskelig blitt veldig konkret. Utvalget vil dessuten ikke utelukke at tiltaket i enkelte tilfeller er direkte uhensiktsmessig. Inntrengningstesting vil dessuten kunne innebære behandling av personopplysninger. Utvalget antar at det vil kunne virke mindre inngripende at den enkelte virksomhet må ta initiativ til gjennomføring av tiltaket, fremfor at det foreligger en rettslig plikt.

Slik dagens bestemmelse er utformet mener utvalget at personvernhensynet ikke kommer klart nok frem. Det bør gå tydelig frem av bestemmelsen at i de tilfeller tiltaket innebærer behandling av personopplysninger må det foretas en konkret vurdering der omfanget av og metoden for kontrollen veies opp mot personvernhensyn. Det er utvalgets klare oppfatning at det her er tale om et sikkerhetstiltak som er hensiktsmessig for svært mange informasjonssystemer.

Etter gjeldende sikkerhetslov § 13 a gjelder en plikt til *sikkerhetsmessig overvåkning* av informasjonssystemer som behandler sikkerhetsgradert informasjon. Utvalget foreslår å videreføre bestemmelsen, men har sett behov for justeringer, dels av personvernhensyn, dels av hensyn til at den nye loven vil gjelde for flere typer systemer. Sikkerhetsmessig overvåkning er et helt nødvendig tiltak for å beskytte skjermingsverdige informasjonssystemer i tilstrekkelig grad. Derfor må virksomhetene ha en plikt til å gjennomføre tiltaket for alle typer av informasjonssystemer som skal beskyttes etter den nye sikkerhetsloven.

I § 13 a andre ledd er plikten konkretisert ved at nærmere angitt utveksling av informasjon skal registreres og lagres. Enkelte høringsinstanser påpekte i høringen av Prop. 97 L (2015–2016), at slik lagring vil kunne bli svært byrdefullt. Denne bekymringen blir enda mer aktuell med den nye loven, som skal gjelde for flere typer informasjonssystemer. Etter utvalgets oppfatning bør derfor ikke plikten være absolutt. Det må først vurderes konkret i hvilket omfang det enkelte system bør overvåkes. Når dette er kartlagt inntrer plikten til å lagre og registrere.

Utvalget foreslår også en mer generell angivelse av hvilken informasjon som kan lagres og registreres. Det er flere grunner til dette. Den nye overvåkningsbestemmelsen gjelder for flere typer systemer og det er ikke klart for utvalget at angivelsen i § 13 a er treffende nok i alle tilfeller. En videre hjemmel er forsvarlig fordi lagrings- og registreringsplikten ikke er absolutt. Overvåkningen må begrunnes i sikkerhetshensyn og det skal etter forslagets tredje ledd tas personvernhensyn.

Det fremgår av Prop. 97 L (2015–2016) at informasjonen som lagres og registreres også skal analyseres. Slik utvalget har oppfattet det vil slik analyse i mange tilfeller være helt nødvendig for å oppnå formålet med overvåkningen. Det bør dermed fremgå klart av loven en hjemmel til å analysere informasjonen som innhentes gjennom overvåkningen.

Logging vil i mange tilfeller gripe inn i personvernet til personer som bruker det overvåkede systemet. Utvalget støtter de drøftelser som gjøres over temaet i Prop. 97 L (2015–2016), men mener samtidig at det bør tas inn en proporsjonalitetsregel i bestemmelsen. Det blir da tydeligere for virksomheten at det ved den konkrete vurderingen av behovet for logging også må tas hensyn til personvernkonsekvensene. At slike vurderinger er gjort bør også kunne kontrolleres i ettertid. I praksis skal dette litt enkelt sagt føre til at høygraderte systemer kan overvåkes i større utstrekning enn lavgraderte og ugraderte systemer. Videre foreslår utvalget mindre språklige justeringer for å gjøre ordlyden mer tilgjengelig og for å tydeliggjøre formålet med overvåkningen.

Tekniske sikkerhetsundersøkelser bør fortsatt kunne gjennomføres i samme utstrekning som tidligere. Utvalget har i sitt arbeid i liten grad mottatt innspill om dette sikkerhetstiltaket. Slik utval-

get oppfatter det er det fortsatt behov for hjemmel for å foreta denne typen undersøkelser. Tiltaket benyttes blant annet i forkant av møter og ved sikkerhetsgodkjenning av rom. Utvalget foreslår derfor bestemmelsen videreført.

Utvalget har ikke mottatt særlige synspunkter om *kryptosikkerhet*. Det fremstår likevel klart at det er behov for en videreføring av dagens ordning. Utvalget ser imidlertid ikke behov for å regulere kryptosikkerhet på lovs nivå. Det er her tale om spesifikke sikkerhetstiltak som ikke må reguleres i lov, og utvalget foreslår derfor at hele reguleringen flyttes til forskrift. For utvalgets del synes det mest naturlig at Nasjonal sikkerhetsmyndighet fortsetter å være forvalter av kryptosikkerhet.

8.6.5 Forholdet til NIS-direktivet

Hovedformålet med NIS-direktivet er å bidra til et velfungerende indre marked. Antakelig vil en rekke virksomheter, dersom direktivet implementeres i norsk rett, omfattes av både NIS-direktivet og av en ny sikkerhetslov. Det går ikke klart frem av direktivet hvilket sikkerhetsnivå som vil bli innført. Ut i fra direktivets tittel er ambisjonen et høyt felles nivå på sikkerheten. Det kan nok likevel ikke utelukkes – tatt EUs kompromissvillighet i betraktning – at det i realiteten blir tale om et felles minimumsnivå for sikkerheten i første omgang.

Etter utvalgets oppfatning synes NIS-direktivet å være et godt tiltak som vil løfte sikkerheten i mange virksomheter som leverer samfunnsviktige tjenester. Samtidig synes det klart at sikkerhetsloven ikke er den riktige plasseringen av en eventuell norsk implementering av direktivet. De to regelverkene har ulikt formål, ulikt nedslagsfelt og ulike ambisjoner for sikkerhetsnivået.

8.6.6 Harmonisering av sektorregelverk

Utvalget mottok 7. desember 2015 rapporten Kartlegging av sektorlovgivning som regulerer virksomheters tiltak mot tilsiktede hendelser.[34] Som det ligger i navnet handler rapporten om noe mer enn, men omfatter likevel, regler om informasjonssikkerhet.

I sitt arbeid med nytt lovgrunnlag for nasjonal sikkerhet har utvalget naturligvis sett hen til sektorregelverk innen alle relevante områder, herunder også informasjonssikkerhet. Ved utarbeidelsen av lovforslaget har utvalget forsøkt å kommer frem til en løsning der den sektorovergripende sikkerhetsloven er tilpasset det eksisterende regelverket. Gitt ny sikkerhetslovs overordnede nivå har det imidlertid vært begrenset behov for konkret tilpasning. Imidlertid er systematikken slik at man ved gjennomføring av den nye loven skal benytte seg av og i minst mulig grad gripe inn i eksisterende og velfungerende sikkerhetsregelverk.

Dette gjelder også for informasjonssikkerhet. Slik utvalget ser det foreslås det ikke bestemmelser som kommer i konflikt med eksisterende regelverk. Utvalget antar samtidig at man ved utarbeidelsen av en informasjonssikkerhetsforskrift i større grad må tilpasse denne til eksisterende regelverk eventuelt harmonisere nytt og gammelt regelverk. Dette understreker ytterligere behovet for at utarbeidelse av forskrifter til ny sikkerhetslov må foretas av flere aktører i samarbeid.

8.6.7 Beskyttelsesinstruksen

Beskyttelsesinstruksens anvendelsesområde er behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter. Instruksen plasserer seg dermed per definisjon utenfor sikkerhetslovens anvendelsesområde.

Som det fremgår av kapittel 6.7.1 foreslår utvalget en utvidelse av gjeldende sikkerhetslovs anvendelsesområde. Dersom beskyttelsesinstruksen skal implementeres i en ny sikkerhetslov må anvendelsesområdet utvides ytterligere, slik at også hensynet til andre offentlige interesser, bedrifter, institusjoner og enkeltpersoner ivaretas gjennom loven. Ved vurderingen av om informasjon skal sikkerhetsgraderes må man trekke inn andre momenter enn beskyttelse av grunnleggende nasjonale funksjoner. Etter utvalgets oppfatning vil det innebære en samling av vurderingstemaer som tematisk har lite med hverandre å gjøre.

Et første skritt på veien til en revisjon og modernisering av beskyttelsesinstruksen, ville være å identifisere hvilke aktører som bruker instruksen og samle deres erfaringer. Ettersom instruksens anvendelsesområde per definisjon er et annet enn for sikkerhetsloven, ville det i stor grad være tale om å ta kontakt med andre aktører enn de utvalget har vært i kontakt med for å vurdere sikkerhetsloven. Med dette som utgangspunkt har utvalget ikke funnet det hensiktsmessig

[34] Herbjørn Andersen, *Kartlegging av sektorlovgivning som regulerer virksomheters tiltak mot tilsiktede hendelser*, Høgskolen i Oslo og Akershus, elektronisk vedlegg 1.

å vurdere beskyttelsesinstruksen nærmere i sammenheng med det øvrige arbeidet med sikkerhetsloven.

8.6.8 Forholdet til offentlighetsloven

En utvidelse av lovens virkeområde vil antakelig innebære at mer informasjon blir sikkerhetsgradert. Det er flere grunner til at utvalget ikke ser dette som problematisk i en offentlighetssammenheng.

Dagens sikkerhetslov gjelder for hele den offentlige sektor og kun i noen grad for andre virksomheter. Et utvidet virkeområde vil først fremst innebære at flere virksomheter utenfor offentlig sektor vil bli omfattet av loven.

Den informasjonen som er aktuell for sikkerhetsgradering og dermed unntatt offentlighet, er i svært mange tilfelle unntatt offentlighet av ulike årsaker. Ett eksempel på slik informasjon – uten at utvalget dermed tar stilling til forholdet til en ny sikkerhetslov – er beredskapsforskriften, jf. kapittel 8.3.2. Det er videre grunn til å tro at informasjon som er aktuell for sikkerhetsgradering i mange tilfeller er underlagt taushetsplikt.

I alle tilfeller vil sikkerhetsgradert informasjon ha et særlig beskyttelsesbehov som i seg selv er grunn til å unnta opplysningene fra innsyn. Et viktig lovfestet prinsipp som utvalget foreslår videreført, er at sikkerhetsgradering ikke skal skje i større utstrekning eller for lengre tid enn det som er nødvendig av hensyn til nasjonal sikkerhet.

Kapittel 9
Objekt- og infrastruktursikkerhet

9.1 Innledning

Som det fremkommer av kapittel 6 *Lovens formål og virkeområde*, samt tidligere kapitler, er formålet med regulering av forebyggende nasjonal sikkerhet å forhindre at terror, sabotasje eller andre tilsiktede hendelser rammer *grunnleggende nasjonale funksjoner*. Videre skal forebyggende nasjonal sikkerhet bidra til at samfunnet blir robust, for å forhindre uforholdsmessig store konsekvenser dersom slike hendelser inntreffer. Forebygging av spionasje og annen etterretningsvirksomhet er et viktig tiltak for økt sikkerhet.

Dersom tilsiktede uønskede hendelser rammer viktige samfunnsfunksjoner, kan det medføre alvorlige konsekvenser. Konsekvensene av en tilsiktet hendelse vil kunne få betydelig større omfang enn det som var intensjonen fra den eller de som planla og utførte handlingen, på grunn av avhengigheter som fører til følgefeil. I andre sammenhenger vil konsekvensene bli langt mindre enn trusselaktøren har antatt på grunn av robusthet i systemer og i samfunnet.

Noe av bakgrunnen for nedsettelsen av utvalget er at dagens objektsikkerhetsregelverk praktiseres svært ulikt i ulike sektorer, og at det er uklarheter knyttet til hvilke objekter som er skjermingsverdige i sikkerhetslovens forstand. Hvilke kriterier som ligger til grunn for utvelgelse, klassifisering og sikringstiltak, varier mye fra sektor til sektor. Dette fører til store ulikheter i terskelen for utpeking av objekter som skjermingsverdige, samt hvilke type objekter som utpekes. Videre er det uklarheter og uenigheter knyttet til hvordan disse bør sikres mot uønskede hendelser på en kostnadsmessig balansert måte. En utfordring med dagens situasjon er dermed at sikkerhetsnivået i ulike sektorer er lite harmonisert. Dette kan være problematisk ved at sikkerhetsnivået i en sektor eller virksomhet ikke bare er avhengig av eget sikkerhetsarbeid, men også av at alle kritiske innsatsfaktorer holder tilsvarende sikkerhetsnivå.

I følge NSMs sikkerhetsfaglige råd har sikkerhetsarbeidet som utøves for å ivareta viktige samfunnsmessige interesser lang tradisjon for å være detaljregulert i lover, forskrifter og instrukser. Dette oppfattes som problematisk for flere av sektorene og aktørene som blir omfattet av regelverket. Dette anses å gi for detaljerte krav til for eksempel fysisk sikring, og det gir lite fleksibilitet med hensyn til hvilke andre tiltak som skal iverksettes for å oppnå et tilstrekkelig og helhetlig sikkerhetsnivå.

Dagens objektsikkerhetsregelverk fungerer godt med tanke på sikring av enkeltobjekter, men har svakheter når det gjelder ivaretakelse av kritisk infrastruktur. Direktoratet for samfunnssikkerhet og beredskap (DSB) og andre har påpekt at dagens regelverk gir få incentiver for å utvikle robuste systemer, kun robuste objekter. Dette er problematisk sett i lys av hvordan ulike objekters funksjonalitet er avhengig av en rekke innsatsfaktorer. Lange komplekse verdikjeder, blant annet som resultat av økt digitalisering, gir sterke avhengigheter som bidrar til å gjøre grunnleggende nasjonale funksjoner sårbare.

Utvalgets målsetting med regulering av forebyggende sikkerhet for objekter og infrastruktur er å beskytte kritisk infrastruktur og objekter som er nødvendig for å understøtte *grunnleggende nasjonale funksjoner* mot tilsiktede uønskede hendelser. Dette innebærer å forebygge at hendelser inntreffer, og å sikre at konsekvensene dersom hendelser inntreffer blir så små som mulig.

En viktig målsetting er å oppnå et harmonisert sikkerhetsnivå, samtidig som det legges til rette for fleksible sikkerhetstiltak tilpasset den enkelte virksomhet og sektor.

En ytterligere målsetting er å sikre en samfunnsøkonomisk lønnsom regulering. Dette innebærer at samfunnets kostnad ved å gjennomføre sikringstiltak står i rimelig forhold til den nytten samfunnet får ved risikoreduksjon. Samfunnsøkonomisk lønnsomhet er nærmere omtalt under kapittel 4.5.1. Sikringstiltak må ses i sammenheng og på tvers av ulike samfunnssektorer, slik at tiltak iverksettes der det gir størst effekt. Slike vur-

deringer bør gjøres på tvers av virksomheter og samfunnssektorer.

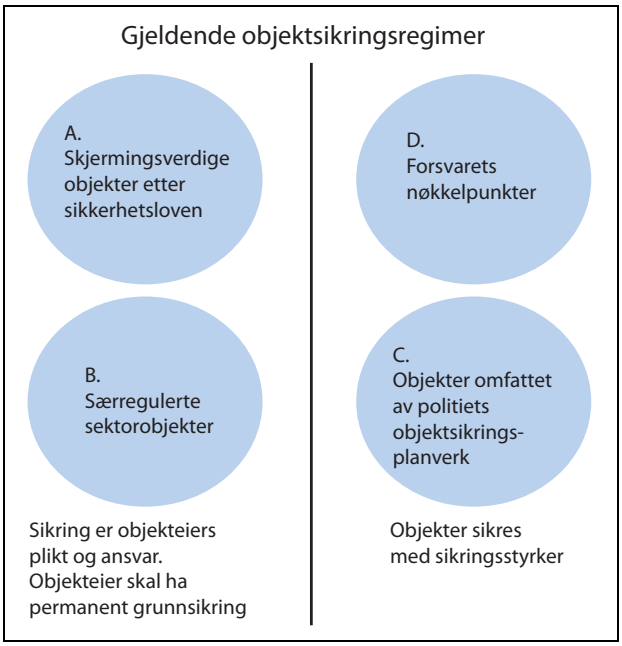
En grunnleggende problemstilling er hvordan regelverket kan innrettes og hvordan myndighetsansvaret bør fordeles for best å a) forebygge at tilsiktede uønskede hendelser rammer *grunnleggende nasjonale funksjoner*, og b) sikre at konsekvensene blir så små som mulig, dersom en hendelse likevel inntreffer.

En annen problemstilling er hvordan man skal redusere sårbarhetene i samfunnet som følger av økt avhengighet mellom ulike virksomheter og samfunnsfunksjoner, særlig i forbindelse med digitalisering. Utvalget må ta stilling til hvordan man oppnår tversektoriell koordinering og harmonisering som gir et tilstrekkelig nasjonalt sikkerhetsnivå. Samtidig er det ønskelig at sektorene beholder nødvendig autonomi og at det legges til rette for fleksible og effektive risikoreduserende tiltak.

Som beskrevet i kapittel 6.7.6 er en grunnleggende problemstilling knyttet til det asymmetriske avhengighetsforholdet mellom ulike virksomheter og *grunnleggende nasjonale funksjoner*. Enkelte sikkerhetstiltak vil kunne ha stor samfunnsøkonomisk nytte, men liten egenverdi og høy kostand for de virksomheter der tiltakene må iverksettes. Dette er problematisk for den berørte virksomhet, blant annet i et konkurranseperspektiv. Det er en utfordring å balansere tiltak slik at man hindrer unødig negative effekter for den enkelte virksomhet samtidig som man sikrer et helhetlig og tilstrekkelig nasjonalt sikkerhetsnivå.

9.2 Gjeldende sikkerhetslovs regulering

Forebyggende sikkerhet for kritisk infrastruktur og objekter av kritisk betydning for *grunnleggende nasjonale funksjoner*, er i dag regulert gjennom flere lover, forskrifter og andre bestemmelser. De viktigste reguleringsregimene er illustrert i figur 9.1. Reguleringen er delvis knyttet til sektorregelverk og delvis til sektorovergripende regelverk. For forebyggende nasjonal sikkerhet er sikkerhetsloven mest sentral. Denne er i sin helhet relevant, og både informasjonssikkerhet, personellsikkerhet, og kontroll av leverandører og med sikkerhetsgraderte anskaffelser, er forhold som er av stor betydning for sikkerheten ved infrastruktur og objekter. Disse temaene er imidlertid omtalt i egne kapitler. Den delen av sikkerhetslovgivningen som har størst direkte relevans her er objektsikkerhetsregelverket.[1]



Figur 9.1 Objektsikkerhet er i dag regulert i diverse regelverk.

Kilde: Nasjonal sikkerhetsmyndighet.

Dagens objektsikkerhetsregelverk regulerer identifisering og utpeking av objekter som omfattes av loven. Videre reguleres klassifisering basert på hvor viktige objektene er som grunnlag for fastsettelse av krav til sikkerhetsnivå og krav til beskyttelse/sikring av objekter. Det er naturlig å ta utgangspunkt i disse temaene i en gjennomgang av regelverket.

Hovedformålet med objektsikkerhetsregelverket er å gi en helhetlig og overordnet tilnærming på tvers av samfunnssektorene når det gjelder utvelgelse, beskyttelse og tilsyn med skjermingsverdige objekter. Disse er definert som «eiendom som må beskyttes mot sikkerhetstruende virksomhet av hensyn til rikets eller alliertes sikkerhet eller andre vitale nasjonale sikkerhetsinteresser».[2] Med eiendom forstås løsøre, bygninger, områder, naturmiljøet og andre stasjonære og mobile objekter.[3] Det fremkommer av forarbeidene at dagens definisjon av skjermingsverdig objekt også under visse omstendigheter dekker lokaliteter der aktiviteter finner sted og bestemte personer oppholder seg:

---

1 Sikkerhetsloven, kapittel 5 og Forskrift av 22. oktober 2010 om objektsikkerhet (objektsikkerhetsforskriften).

2 Sikkerhetsloven, § 3 første ledd nr. 12.

3 Ot.prp. nr. 49 (1996–97).

> Det forutsettes at aktiviteter i seg selv kan være skjermingsverdige, og vil indirekte kunne dekkes av definisjonene her, ved at stedet aktiviteten foregår pga aktiviteten vil være et skjermingsverdig objekt.
>
> Definisjonene vil også i gitte situasjoner dekke bygninger eller områder hvor personer befinner seg, utelukkende som følge av personenes tilstedeværelse, dersom personene for eksempel har en slik funksjon i den nasjonale beslutningsprosessen e.l. at det vil kunne skade rikets sikkerhet mv om deres tiltenkte funksjon elimineres eller på annen måte umuliggjøres eller hemmes som følge av sikkerhetstruende virksomhet.[4]

Objektsikkerhet er regulert i sikkerhetsloven kapittel 5 og i forskrift om objektsikkerhet. Dagens regler trådte i kraft 1. januar 2011.[5]

Historisk har forebyggende sikkerhetstjeneste vært rettet mot beskyttelse av informasjon, ikke objekter, noe også dagens sikkerhetslov bærer preg av. Objektsikkerhetsregelverket er relativt nytt og regelverket har ikke fungert etter hensikten. Hovedutfordringen med dagens regelverk er at det har vært uenigheter mellom departementene om hvordan utpeking av skjermingsverdige objekter skal praktiseres, og om hvordan disse bør sikres best mulig mot skade eller ødeleggelse på en kostnadsmessig og balansert måte. Dette omtales blant annet i DSBs brev til utvalget.[6]

I forbindelse med implementeringen av objektsikkerhetsregelverket ble det gitt en frist for utpeking og klassifisering av skjermingsverdige objekter, 31. desember 2012. Videre var det fastsatt en frist for implementering av sikringstiltak innen 31. desember 2013. Det har vist seg vanskelig å etablere en tilstrekkelig ensartet praksis mellom departementene omkring utpeking av skjermingsverdige objekter. Uenigheter mellom ulike departementer og andre myndigheter rundt dette, sammen med utviklingen i samfunnets sårbarhet og et endret trusselbilde, var noe av utgangspunktet for at regjeringen oppnevnte dette utvalget.

Utfordringene med dagens objektsikkerhetsregelverk gir seg også utslag i forbindelse med avhengigheter til andre objekter. I forskrift om objektsikkerhet fremkommer det at dersom et objekt er avhengig av et annet objekt for å opprettholde egen funksjon, skal denne avhengigheten meddeles den virksomheten som rår over det understøttende objektet.[7]

DSB har i sitt brev til utvalget[8] gitt uttrykk for at det er en svakhet med dagens regelverk at det «gir lite insitament til å utvikle robuste systemer». Dette understøttes også av utredningen som FFI har gjort på oppdrag fra utvalget.[9]

9.2.1 Utpeking av skjermingsverdige objekter etter sikkerhetsloven

Prinsippene for utvelgelse av skjermingsverdige objekter følger av sikkerhetsloven § 17. Det er hvert enkelt fagdepartement som er ansvarlig for å utpeke skjermingsverdige objekter innenfor sitt myndighetsområde. Det skal være en høy terskel for utpeking, og det må dreie seg om objekter som etter en skadevurdering anses å være av vesentlig samfunnsinteresse. Utpekingen skal skje på grunnlag av en skadevurdering. Innenfor lovens formål skal det særlig ses hen til objektets:

a) betydning for sikkerhetspolitisk krisehåndtering og forsvar av riket,
b) kritiske funksjoner for det sivile samfunn,
c) objektets symbolverdi, og
d) muligheten for å utgjøre en fare for miljøet eller befolkningens liv og helse.

Etter § 17 annet ledd skal det i skadevurderingen også tas hensyn til hva som vil være en akseptabel tidsperiode for funksjonssvikt, muligheten til å gjenopprette funksjonalitet, og hensynet til objektets betydning for andre objekter.

Det er den enkelte virksomhet som eier eller råder over et potensielt skjermingsverdig objekt som skal levere en dokumentert skadevurdering til vedkommende fagdepartement, jf. forskrift om objektsikkerhet § 2-1 annet ledd. Der det finnes tilsynsorgan for sektoren, kan tilsynsorganet foreslå objekter som skjermingsverdige uavhengig av objekteiers vurdering.

NSM kan også foreslå skjermingsverdige objekter overfor departementene, jf. forskriften § 2-1 tredje ledd. Utpeking skal ikke skje i større

---

4 Ot.prp. nr. 21 (2007–2008), 19.

5 Ibid., og Innst. O. nr. 33 (2007–2008), Innstilling fra forsvarskomiteen om lov om endringer i lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven).

6 Brev fra Direktoratet for samfunnssikkerhet og beredskap til sikkerhetsutvalget, «Innretning av ny sikkerhetslov - DSBs foreløpige vurderinger», 20.04.2016.

7 Objektsikkerhetsforskriften § 2-1 femte ledd.

8 Brev fra DSB til sikkerhetsutvalget, «Innretning av ny sikkerhetslov – DSBs foreløpige vurderinger».

9 Forsvarets forskningsinstitutt, *Vurdering av forebyggende sikkerhet innen kraft, petroleum og luftfart*, FFI-rapport 00702 (Kjeller: Forsvarets forskningsinstitutt 2016), elektronisk vedlegg nr. 3.

utstrekning enn nødvendig, jf. forskriften § 2-1 fjerde ledd.

I forskriften § 2-1 femte og sjette ledd er det regulert hvordan man skal forholde seg dersom et objekt er avhengig av andre objekter for å kunne fungere etter sin hensikt, og dersom et objekt som er vurdert som skjermingsverdig tilhører en virksomhet som ikke er underlagt sikkerhetsloven.

Myndigheten til å utpeke et objekt som skjermingsverdig er tillagt vedkommende fagdepartement og ikke den enkelte virksomhet. Et argument for dette er at departementet har en overordnet og mer helhetlig oversikt enn den enkelte virksomhet kan forutsettes å inneha.

Som nevnt i kapittel 9.1 og i innledningen til kapittel 9.2, har praksis ved innmelding av skjermingsverdige objekter til NSM vist at det er ulike oppfatninger om hvor terskelen for utpeking og klassifisering ligger. DSB understreker også at dette er en svakhet med dagens sikkerhetslov.[10]

9.2.2 Klassifisering av skjermingsverdige objekter etter sikkerhetsloven

Et skjermingsverdig objekt skal klassifiseres ut fra den skade som kan oppstå dersom objektet får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettstridig overtakelse som følge av *sikkerhetstruende virksomhet*. Dagens regelverk etablerer tre klasser:

a) MEGET KRITISK nyttes dersom det kan få helt avgjørende skadefølger for rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser om objektet får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse av uvedkommende.
b) KRITISK nyttes dersom det alvorlig kan skade rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser om objektet får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse av uvedkommende.
c) VIKTIG nyttes dersom det kan skade rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser om objektet får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse av uvedkommende.[11]

Fagdepartementet fastsetter klassifiseringsgraden basert på en skadevurdering som er utarbeidet av virksomheten som eier eller råder over skjermingsverdig objekt, jf. objektsikkerhetsforskriften § 2-2. Det skal ikke brukes høyere klassifiseringsgrad enn nødvendig. Videre er det bare de skjermingsverdige deler av objektet som skal omfattes av klassifiseringen, samtidig som objektet kan inndeles i forskjellige klassifiseringsgrader. Det skal tas hensyn til objektets betydning for andre objekter, jf. forskriften § 2-2 tredje ledd.

Det skal foretas en omklassifisering av objektet ved endring av forhold som er relevante for den foreliggende skadevurderingen, jf. forskriften § 2-3. Slik fastsettelse foretas av fagdepartementet. Det er en forutsetning at objekteier melder inn forhold som tilsier en ny slik skadevurdering.

Innmelding av skjermingsverdige objekter til NSM har vist at det kan være vanskelig å vurdere hva som er et korrekt klassifiseringsnivå. En grunn kan være at det er snakk om et relativt nytt regelverk.

NSM driver tilsyn og veiledning for å oppnå en sektorovergripende harmonisert tilnærming til bruk av de ulike klassifiseringsnivåene. Det store flertall av innmeldte objekter er vurdert til det laveste klassifiseringsnivået VIKTIG. Enkelte virksomheter savner en tydeligere beskrivelse av hva som er de dimensjonerende truslene for de tiltak som skal iverksettes i henhold til objektsikkerhetsbestemmelsene. Dette er ikke beskrevet i lov eller forskrift i dag. Det er heller ikke omtalt i forarbeidene utover en kort og generell henvisning til at det må tas utgangspunkt i at mulige trusselaktører er fremmede makter og internasjonale terrororganisasjoner.[12]

NSMs tilsyn viser at etterlevelsen av regelverket er mangelfull. Blant annet er det store mangler i gjennomføring av risikovurderingene som skal ligge til grunn for klassifiseringen, og det er mangel på kartlegging av avhengigheter.[13]

9.2.3 Plikt til å beskytte skjermingsverdige objekter etter sikkerhetsloven

Etter utpeking plikter objekteier å beskytte objektet med de nødvendige sikkerhetstiltak, jf. sikkerhetsloven § 17 b. Regelverket gir funksjonelle krav til sikringstiltak (grunnsikring), der tiltakene skal bestå av en kombinasjon av barrierer, deteksjon, verifikasjon og reaksjon. Objekt klassifisert

[10] Brev fra DSB til sikkerhetsutvalget, «Innretning av ny sikkerhetslov – DSBs foreløpige vurderinger».

[11] Sikkerhetsloven § 17 a.

[12] Ot.prp. nr. 21 (2007–2008), 13.

[13] Elgsaas og Schultz Heireng, *Norges sikkerhetstilstand – en årsaksanalyse av mangelfull forebyggende sikkerhet*, 2014.

som MEGET KRITISK skal beskyttes slik at tap av funksjon, ødeleggelse eller rettsstridig overtakelse avverges. Objekt klassifisert som KRITISK skal beskyttes slik at tap av funksjon eller ødeleggelse begrenses og rettsstridig overtakelse avverges. Objekt klassifisert som VIKTIG skal beskyttes slik at tap av vesentlig funksjon og ødeleggelse begrenses.

Sikkerhetstiltakene skal også ta sikte på å redusere muligheten for etterretningsaktivitet mot objektet, jf. § 17 b tredje ledd.

Kongen kan bestemme at det kreves sikkerhetsklarering for den som skal gis tilgang til objekt klassifisert MEGET KRITISK eller KRITISK, jf. § 17 b fjerde ledd. Det er med andre ord ikke noe krav om sikkerhetsklarering for personer som gis tilgang til objekt klassifisert som VIKTIG, jf. § 17 b fjerde ledd.

Kongen kan videre gi nærmere bestemmelser om planlegging og gjennomføring av sikkerhetstiltak, herunder bruk av sikringsstyrker, jf. § 17 b femte ledd. Etter objektsikkerhetsforskriften § 3-5 skal objekteier som er ansvarlig for et skjermingsverdig objekt, legge til rette for at sikringsstyrker kan forberede, øve og gjennomføre tiltak på og ved objektet for å beskytte dette.

Med unntak av at ansvarlig departement kan stille krav om sikkerhetsklarering for tilgang til skjermingsverdig objekt,[14] gir sikkerhetsloven i dag ikke noen uttrykkelig hjemmel for å implementere andre beskyttelsestiltak enn de tiltak som objekteier selv kan iverksette i kraft av sin egen eierrådighet over objektet.

Som tidligere omtalt har praksis omkring innmelding og klassifisering vist at det er ulike oppfatninger mellom departementene om det skal foretas slik innmelding og klassifisering av objekter etter sikkerhetsloven. Dette gjelder særlig i de tilfeller der man har eget sektorregelverk som anses å ivareta behov på tiltakssiden.

NSMs tilsyn har avdekket vesentlige mangler i oppfølgingen av objektsikkerhetsregelverket, både hva gjelder gjennomføring av sikkerhetstiltak etter objektsikkerhetsforskriften og oppfølging av pålegg gitt i forbindelse med tilsyn. Manglende oppfølging får sjelden konsekvenser utover pålegg.[15]

For å oppnå en nødvendig beskyttelse av skjermingsverdige objekter, kan det i særlige tilfeller være behov for å iverksette beskyttelsestiltak utover den egenbeskyttelse objekteier selv kan etablere. Dette kan eksempelvis være tiltak for å beskytte objektet mot uønsket kartlegging av dets funksjonalitet eller sårbarheter. Stortinget har i forbindelse med behandlingen av Innst. 352 L (2015–2016) til Prop. 97 L (2015–2016) om endringer i sikkerhetsloven, vedtatt regjeringens forslag til ny bestemmelse § 5 a om *varslingsplikt og myndighet til å fatte vedtak ved risiko for sikkerhetstruende virksomhet.*[16] Denne bestemmelsen gir virksomheter som får kunnskap om en planlagt eller pågående aktivitet som kan medføre en ikke ubetydelig risiko for at sikkerhetstruende virksomhet blir gjennomført, plikt til å varsle overordnet departement om dette. Kongen i statsråd er gitt myndighet til å fatte nødvendige vedtak for å hindre slik sikkerhetstruende virksomhet.[17]

9.3 Annet relevant regelverk

Ved siden av sikkerhetsloven er det flere lover, forskrifter og andre bestemmelser som regulerer forebyggende sikkerhet for infrastruktur og objekter. Særlig relevant er regulering av sikring mot tilsiktede uønskede hendelser mot samfunnsfunksjoner i sektorregelverk.

Som omtalt i kapittel 6.6 har DSB arbeidet med å definere hva som inngår i samfunnets kritiske funksjoner, og utviklet en tilnærming til hvordan disse skal sikres gjennom identifisering og sikring av infrastruktur og innsatsfaktorer som er nødvendig for understøttelse. DSBs arbeid med kritiske samfunnsfunksjoner har en *all hazards*-tilnærming. Dette innebærer at kritikaliteten til samfunnsfunksjoner, innsatsfaktorer og infrastruktur utelukkende baseres på konsekvenser ved bortfall, og ikke i hvilken grad de er sårbare for ulike typer uønskede hendelser. Systematikken og arbeidet må ses i sammenheng med reguleringen av forebyggende sikkerhet.

Sivilbeskyttelsesloven[18] gir bestemmelser om sivile beskyttelsestiltak og beskyttelse av kritisk infrastruktur. EUs EPCIP-direktiv er tatt inn i sivilbeskyttelsesloven og vil bli diskutert under.

Forebyggende sikkerhet omhandler både grunnsikring og forsterkningstiltak. Således er *Instruks om sikring og beskyttelse av objekter ved bruk av sikringsstyrker* også relevant.

---

14 Objektsikkerhetsforskriften § 3–6.

15 Elgsaas og Schultz Heireng, *Norges sikkerhetstilstand – en årsaksanalyse av mangelfull forebyggende sikkerhet*, 2014.

16 Prop. 97 L (2015–2016).

17 Ibid.

18 Lov 25. juni 2010 nr. 45 om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret (sivilbeskyttelsesloven).

9.3.1 Sektorregelverk

Sikkerhetsutvalget har gitt Høyskolen i Oslo og Akershus (HiOA) i oppdrag å kartlegge sektorregelverk som regulerer beskyttelse av objekter og infrastruktur. HiOA har utarbeidet en rapport.[19]

HiOA har delt funn av sektorregelverk inn i følgende områder (sektorer):

- CBRNE (chemical, biological, radiological, nuclear and explosive)
- Energi
- Samferdsel
- IKT-infrastruktur og informasjonssikkerhet
- Elektronisk kommunikasjon (ekom)
- Finans
- Helse
- Samordning

På alle områder, unntatt *helse* og til dels *IKT* er det i HiOAs arbeid gjort funn av sektorregelverk som regulerer sikring mot tilsiktede uønskede hendelser for samfunnsfunksjoner, infrastruktur eller objekter. Innretningen på regelverket varierer.

Bruk av klassifisering er benyttet i flere sammenhenger i sektorlovgivningen, der ulike kategorier anlegg/virksomhet er underlagt ulike krav til sikring. Klassifiseringen er som regel knyttet til kritikalitet for samfunnet ved bortfall av tjeneste og funksjon. For ekom er det lagt opp til at objekter som faller inn i øvre klasse vil bli definert som skjermingsverdig objekt og således falle inn under sikkerhetslovens objektsikkerhetsbestemmelser. Bestemmelsen er fastsatt i klassifiseringsforskrifta,[20] der anlegg klassifiseres i kategoriene A til D. I forskriften slås det fast at kategori A er omfattet av sikkerhetsloven.

For kraftforsyning er det også benyttet klassifisering av anlegg basert på kritikalitet ved bortfall, men her er det ikke bestemmelser som knytter objekter til sikkerhetsloven gjennom klassifisering. Damsikkerhetsforskriften[21] fastsetter kriterier for kategorisering av damanlegg. Tilsvarende benyttes klassifisering i forskrift om forebyggende sikkerhet og beredskap i energiforsyningen[22] og i forskrift om sikring av havner,[23] forskrift om sikring av havneanlegg,[24] og i sikkerhetsforskriften[25] til skipssikkerhetsloven.

Innenfor petroleumssektoren har det tradisjonelt vært fokus på HMS og *safety* med et velutviklet regelverk på dette området. Selv om lovfestede krav til sikkerhet innen petroleumsvirksomheten har vært HMS- og internkontrollbaserte, er det ikke slik at man har unnlatt sikring mot tilsiktede uønskede hendelser. Det har vært oppmerksomhet om terrorfaren tilbake til 1970 tallet. Dette har imidlertid vært håndtert i et annet spor, med innsats fra politiets beredskapstropp og Forsvarets spesialkommando (FSK).[26] FSK ble etablert i 1982 for å håndtere terrortrusselen mot oljeplattformene på sokkelen.[27]

Det er verdt å merke seg at det eksisterende sektorregelverket eksisterer sammen med gjeldende sikkerhetslov, og at i den grad objekter er utpekt som skjermingsverdig objekt omfattes de av dette regelverket.

Forsvarets forskningsinstitutt (FFI) har på oppdrag fra Sikkerhetsutvalget foretatt en sikkerhetsfaglig vurdering av regelverket i tre ulike sektorer.

Når det gjelder forebyggende sikkerhet for kritisk infrastruktur og kritiske samfunnsfunksjoner konkluderer FFI med at det er behov for et nasjonalt tverrsektorielt regelverk for utvelgelse av skjermingsverdige objekter, og at nasjonal kritisk infrastruktur og kritiske samfunnsfunksjoner bør inkluderes i regelverket.[28]

9.3.2 Identifisering av kritisk infrastruktur i henhold til KIKS

Direktoratet for samfunnssikkerhet og beredskap (DSB) har etablert en modell for sikkerhet i kritisk infrastruktur og kritiske samfunnsfunksjoner – KIKS-modellen.[29] Denne modellen er basert på

---

19 Herbjørn Andresen, *Kartlegging av sektorlovgivning som regulerer virksomheters tiltak mot tilsiktede hendelser*, Høgskolen i Oslo og Akershus, elektronisk vedlegg 1.

20 Forskrift 10. september 2012 om klassifisering og sikring av anlegg i elektroniske kommunikasjonsnett (klassifiseringsforskrifta).

21 Forskrift 18. desember 2009 nr. 1600 om sikkerhet ved vassdragsanlegg (damsikkerhetsforskriften).

22 Forskrift 7. desember 2012 om forebyggende sikkerhet og beredskap i energiforsyningen (beredskapsforskriften).

23 Forskrift 29. mai 2013 om sikring av havner.

24 Forskrift 29. mai 2013 om sikring av havneanlegg.

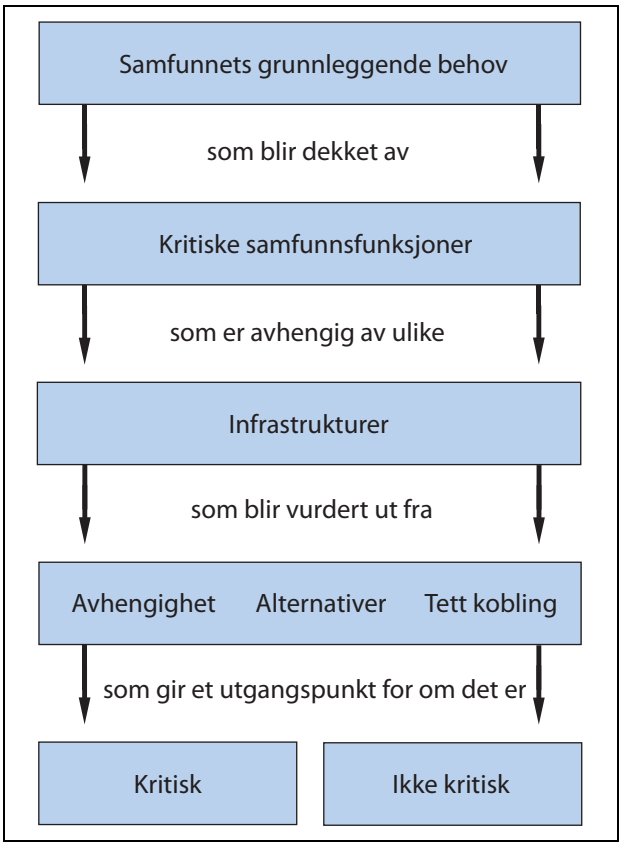
25 Forskrift 22. juni 2004 om sikkerhet, pirat- og terrorberedskapstiltak og bruk av maktmidler om bord på skip og flyttbare boreinnretninger (sikkerhetsforskriften).

26 Herbjørn Andresen, *Kartlegging av sektorlovgivning som regulerer virksomheters tiltak mot tilsiktede hendelser*, Høgskolen i Oslo og Akershus, elektronisk vedlegg 1.

27 Tor Jørgen Melien, *Våre hemmelige soldater: norske spesialstyrker 1940–2012* (Oslo: Spartacus, 2012).

28 Forsvarets forskningsinstitutt, *Vurdering av forebyggende sikkerhet innen kraft, petroleum og luftfart*, FFI-rapport 00702 (Kjeller: Forsvarets forskningsinstitutt 2016), elektronisk vedlegg nr. 3.

29 DSB, *Sikkerhet i kritisk infrastruktur og kritiske samfunnsfunksjoner – modell for overordnet risikostyring,* 2012.



Figur 9.2 Kritisk infrastruktur.

Infrastrukturutvalgets utledning av kritisk infrastruktur ut fra samfunnets grunnleggende behov.
Kilde: NOU 2006: 6, Når sikkerhet er viktigst.

Infrastrukturutvalgets rapport.[30] Basert på identifiseringen av kritiske samfunnsfunksjoner, kan det identifiseres hvilke systemer og anlegg som er helt nødvendige for opprettholdelse av de aktuelle funksjonene. Infrastrukturutvalget oppstilte i sin utredning følgende modell for identifisering av kritisk infrastruktur. I henhold til modellen over vil identifisering av kritisk infrastruktur avhenge av tre kriterier:

1. avhengighet
2. alternativer, og
3. tett kobling

Første trinn er å vurdere *avhengigheten* av den aktuelle infrastrukturen. Med vurdering av avhengighet menes en kartlegging av hvilke samfunnsfunksjoner som vil bli berørt av et bortfall av infrastrukturen, samt hvilke konsekvenser dette vil få for ivaretakelse av de verdiene som skal beskyttes. Desto større konsekvensene blir, desto mer kritisk vil infrastrukturen være. Ekom-infrastrukturen er et eksempel på en infrastruktur som en rekke kritiske samfunnsfunksjoner er avhengig av for å opprettholde funksjonalitet. DSB har i rapporten Risikoanalyse av cyberangrep mot ekom-infrastruktur[31] vurdert hvordan kritiske samfunnsfunksjoner påvirkes av et bortfall av ekom-nettet. Scenariet som ble lagt til grunn var at sentrale noder i det landsdekkende transportnettet ble satt ut av drift i en femdagersperiode. For en rekke samfunnsfunksjoner, herunder jernbane, luftfart, sentral kriseledelse og krisehåndtering, samt helse og omsorg, vil et utfall av ekom-nettet ha store konsekvenser. DSB vurderte videre at nettokostnaden for et slikt utfall ville overstige 10 milliarder kroner for de fem dagene.

Det andre trinnet vil være å vurdere *alternativer*. Med alternativer menes i henhold til DSBs rapport det som ofte kalles redundans i risikostyringssammenheng. Manglende alternativer tilsier en høy grad av kritikalitet. Et eksempel her kan være energiforsyning. Infrastrukturutvalget viste i sin utredning til at Norge har et stort antall kraftverk spredt over hele landet, og at dette medfører at bortfall av ett kraftproduserende anlegg ikke ville få store konsekvenser for kraftleveransen sett under ett. En infrastruktur med høy grad av redundans, vil således tale for en lavere grad av kritikalitet.

Det tredje trinnet vil være å vurdere grad av *tett kobling*. Et tett koblet system vil innebære at forstyrrelser ett sted i systemet får umiddelbare konsekvenser for systemet som helhet. Høy grad av tett kobling tilsier høy grad av kritikalitet. Eksempler kan her være jernbane og lufttrafikk, som er avhengig av sentralisert styring i sann tid for effektiv og sikker drift. Et annet eksempel er digitale verdikjeder, eksempelvis innenfor ekom. Økende grad av digitalisering gir en økt sårbarhet i denne forstand. I det digitale sårbarhetsutvalgets utredning vises det til at et av kjennetegnene ved digitale verdikjeder, er at feil *propagerer* momentant og noen ganger på uforutsigbare måter. Som eksempel nevnes at en feil hos en nettleverandør kan få hele betalingssystemet til å svikte umiddelbart.[32]

DSBs arbeid med å etablere et rammeverk for KIKS har fokusert på overordnede kriterier for identifisering av kritiske samfunnsfunksjoner og kritisk infrastruktur. DSB har i sine to KIKS-rap-

[30] NOU 2006: 6.

[31] Direktoratet for samfunnssikkerhet og beredskap, *Risikoanalyse av cyberangrep mot ekom-infrastruktur*, – delrapport til Nasjonalt risikobilde 2014.

[32] NOU 2015: 13.

porter ikke omtalt aktuelle løsninger for kategorisering av infrastruktur, hverken ut i fra type/funksjon eller ut i fra graden av kritikalitet.

9.3.3 Sivilbeskyttelsesloven og EPCIP

Sivilbeskyttelsesloven har til formål å beskytte liv, helse, miljø, materielle verdier og kritisk infrastruktur ved bruk av ikke-militær makt når Norge er i krig, når krig truer, når Norges selvstendighet eller sikkerhet er i fare, og ved uønskede hendelser i fredstid. Den nye sivilbeskyttelsesloven ble vedtatt i 2010. Den pålegger kommunene plikt til å lage helhetlige risiko- og sårbarhetsanalyser. På bakgrunn av analysene skal det lages beredskapsplaner og gjennomføres øvelser.

Sivilbeskyttelsesloven gir bestemmelser om Sivilforsvaret, tjenesteplikt i Sivilforsvaret, allmenhetens bistandsplikt i akuttsituasjoner, kommunal beredskapsplikt, rekvisisjon av eiendom og rettigheter, sivile beskyttelsestiltak og beskyttelse av kritisk infrastruktur. Kritisk infrastruktur defineres i loven som «de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner som igjen dekker samfunnet grunnleggende behov og befolkningens trygghetsfølelse». Definisjoner av kritisk infrastruktur og samfunnets kritiske funksjoner er ytterligere diskutert i kapittel 6.6 *Kritisk infrastruktur og kritiske samfunnsfunksjoner*.

Direktiv 2008/114/EF av 8. desember 2008 om identifisering og utpeking av europeisk kritisk infrastruktur og vurdering av behovet for å beskytte den bedre (EPCIP-direktivet), er implementert i sivilbeskyttelsesloven. Dette direktivet ivaretar beskyttelse av europeisk kritisk infrastruktur og har således en klar grenseflate mot dagens objektsikkerhetsregelverk.

Definisjonene som benyttes i direktivet er følgende:

> Med «kritisk infrastruktur» menes anlegg, systemer eller deler av slike som er nødvendige for å opprettholde sentrale funksjoner, menneskers helse, sikkerhet, trygghet og økonomiske eller sosiale velferd, og hvor driftsforstyrrelse eller ødeleggelse av disse vil kunne få betydelige konsekvenser.
>
> Med «europeisk kritisk infrastruktur» menes kritisk infrastruktur hvis driftsforstyrrelse eller ødeleggelse vil kunne få betydelige konsekvenser for to eller flere EØS-stater.

Direktivet stiller krav til medlemsstatene om identifisering og utpeking av europeisk kritisk infrastruktur (EKI), og krav til etablering av visse tiltak. Kriteriene for identifisering av Europeisk kritisk infrastruktur er spesifisert i direktivets artikkel 3. I tillegg til det grenseoverskridende kriteriet som fremkommer av definisjonen ovenfor, må europeisk kritisk infrastruktur oppfylle både sektorbaserte kriterier og sektorovergripende kriterier.

Det følger av endringer i sivilbeskyttelsesloven[33] at de sektorbaserte kriteriene tar hensyn til de særlige kjennetegn for de enkelte sektorer av europeisk kritisk infrastruktur. Disse kriteriene er graderte, men skal være tilgjengelige for den aktuelle sektor.

De sektorovergripende kriteriene som skal brukes for identifisering av europeisk kritisk infrastruktur omfatter følgende:

- Forulykkede-kriteriet: en vurdering av det potensielle antall omkomne eller sårede
- økonomisk effekt – kriteriet: en vurdering av størrelsen på det økonomiske tapet og/eller forringelse av varer og tjenester, herunder potensielle miljømessige konsekvenser
- allmenne konsekvenser – kriteriet: en vurdering av konsekvensene med hensyn til befolkningens tillit, fysiske lidelser og forstyrrelser av dagliglivet, herunder bortfall av vesentlige tjenester

Identifiseringsprosessen består av fire trinn. En mulig europeisk kritisk infrastruktur som ikke oppfyller kravene i ett av trinnene, anses ikke som europeisk kritisk infrastruktur. En infrastruktur som oppfyller kravene på ett trinn, skal gjennomgå de neste trinnene i fremgangsmåten.[34]

> Trinn 1: Hver EØS-stat skal anvende de sektorbaserte kriteriene for å foreta en første utvelgelse av kritisk infrastruktur i en sektor.
>
> Trinn 2: Hver EØS-stat skal anvende definisjonen av kritisk infrastruktur (se ovenfor) på en mulig europeisk kritisk infrastruktur identifisert i trinn 1. Betydningen av følgene vil bli fastslått enten ved hjelp av nasjonale metoder for å identifisere kritisk infrastruktur, eller ved henvisning til sektorovergripende kriterier, på et egnet nasjonalt plan. Når det gjelder infrastruktur som leverer en viktig tjeneste, vil det bli tatt

[33] Prop. 129 L (2011–2012), Endringer i sivilbeskyttelsesloven (gjennomføring av EPCIP-direktivet).

[34] Ibid.

hensyn til tilgjengelige alternativer og til varigheten av driftsavbruddet/gjenopprettingen.

Trinn 3: En EØS-stat som har utpekt kritisk infrastruktur som oppfyller kravene i de to første trinnene skal, videre vurdere om infrastrukturen imøtekommer kravet om at driftsforstyrrelser eller ødeleggelse vil kunne få betydelige konsekvenser for to eller flere EØS-stater. Hver EØS-stat skal anvende det grenseoverskridende elementet i definisjonen av europeisk kritisk infrastruktur (jf. definisjonen av EKI) som har oppfylt kravene i de første to trinnene i denne fremgangsmåten. En mulig europeisk kritisk infrastruktur som oppfyller definisjonen, skal gjennom det neste trinnet i fremgangsmåten. Når det gjelder infrastruktur som leverer en viktig tjeneste, skal det i vurderingen tas hensyn til tilgjengelige alternativer og til varigheten av driftsavbruddet/gjenopprettingen.

Trinn 4: Hver EØS-stat skal anvende de sektorovergripende kriteriene på gjenstående mulig europeisk kritisk infrastruktur. De sektorovergripende kriteriene skal ta hensyn til hvor alvorlig følgene er, og når det gjelder infrastruktur som leverer en viktig tjeneste skal det vurderes tilgjengelige alternativer samt varigheten av driftsavbruddet/gjenopprettingen. En mulig europeisk kritisk infrastruktur som ikke oppfyller de sektorovergripende kriteriene, skal ikke anses som europeisk kritisk infrastruktur. En mulig europeisk kritisk infrastruktur som har gjennomgått denne fremgangsmåten, skal bare meddeles til de EØS-stater som kan bli betydelig berørt av denne infrastrukturen.

Det følger videre av Prop. 129 L (2011–2012), at det er sannsynlig at EKI også vil kunne være utpekt som skjermingsverdig objekt etter objektsikkerhetsregelverket. Identifiserings- og utvelgelsesprosessen i henhold til objektsikkerhetsregelverket ligner i stor grad på den prosessen som foretas ved utpeking og identifisering av EKI etter EPCIP-direktivet.

En EØS-stat som har identifisert EKI skal underrette de andre EØS-statene som kan bli betydelig påvirket om infrastrukturens identitet, samt om årsakene til at denne utpekes som potensiell EKI. Videre skal EØS-staten innlede bilaterale og/eller multilaterale drøftelser med de berørte statene. Kommisjonen (ESA for Norges del) kan delta i disse diskusjonene, men har ikke tilgang til detaljerte opplysninger som vil muliggjøre en utvetydig identifisering av en bestemt infrastruktur.[35]

En EØS-stat som har grunn til å tro at den kan bli betydelig påvirket av en mulig EKI, men som ikke er identifisert som sådan av den EØS-stat på hvis territorium denne infrastrukturen befinner seg, kan underrette Kommisjonen/ESA om at den ønsker å delta i bilaterale og/eller multilaterale drøftinger om saken.[36]

Når det gjelder krav til tiltak, avviker objektsikkerhetsregelverket under sikkerhetsloven fra EPCIP-direktivet til en viss grad. EØS-statene skal vurdere om hver utpekt EKI innen deres territorium har en operatørsikkerhetsplan eller tilsvarende. En operatørsikkerhetsplan skal identifisere de kritiske aktiva innenfor infrastrukturen, samt presisere hvilke sikkerhetsløsninger som er eller skal bli iverksatt med henblikk på å beskytte den. Sikkerhetsplanen skal minst dekke følgende:

- Utpeking av viktige aktiva.
- Gjennomføring av en risikoanalyse med grunnlag i alvorlige trusselscenarier, hver aktivas sårbarhet og potensielle konsekvenser.
- Identifisering, utpeking og prioritering av mottiltak og prosedyrer med en sondering mellom grunnsikringstiltak (permanente) og ulike påbygningstiltak (graderte sikkerhetsforanstaltninger).

Grunnsikringstiltakene skal identifisere hvilke investeringer og midler som er nødvendige for sikkerheten, og som er relevante å bruke til enhver tid. Dette vil omfatte generelle tiltak, slik som tekniske sikkerhetstiltak (herunder installering av detektorer, adgangskontroll, samt beskyttelses- og forebyggelsestiltak), organisatoriske sikkerhetstiltak (herunder varslingsprosedyrer og krisestyring), kontroll- og verifiseringstiltak, kommunikasjon, bevisstgjøring og opplæring samt sikring av informasjonssystemer.[37]

Påbygningstiltakene kan aktiveres avhengig av risiko- og trusselnivået. Dersom det konstateres at det allerede eksisterer sikkerhetsplaner som oppfyller minimumsnivået og disse jevnlig ajourføres, er det ikke nødvendig å foreta seg noe ytterligere med hensyn til gjennomførelsen.[38]

Et viktig skille mellom sikkerhetsloven og EPCIP-direktivet, er at sikkerhetsloven kun regu-

[35] Ibid.
[36] Ibid.
[37] Ibid.
[38] Ibid.

lerer egenbeskyttelse mot tilsiktede uønskede hendelser, mens EPCIP-direktivet omfatter både tilsiktede og utilsiktede uønskede hendelser (*all hazards*-tilnærming). Justis- og beredskapsdepartementet er utpekt som kontaktpunkt for EKI i Norge (EPCIP Contact-point).

Sikkerhetsutvalget fikk presentert status for arbeidet med EPCIP på sin studiereise. Regelverket er nytt og det har vært tidkrevende å operasjonalisere direktivet. I 2012 var kun 20 objekter/infrastruktur identifisert som kritiske innen EU. Per oktober 2015 var ytterligere 76 objekter/infrastruktur identifisert. Utvelgelse og innrapportering av EKI har allikevel ikke skjedd i den utstrekning EU's DG Home Affairs mener er nødvendig for tilstrekkelig sikkerhet. Et av tiltakene som de vil iverksette for å bedre denne situasjonen er å tydeliggjøre den metodiske tilnærmingen for å kartlegge avhengigheter mellom ulike virksomheter. Som et ledd i dette har DG Home Affairs utarbeidet et verktøy for å kartlegge gjensidige avhengigheter (GRASP-tool). Videre understreket DG Home Affairs at de vil vektlegge krav til å inkludere forebyggende sikkerhetstiltak på et tidlig stadium av planleggingen og utformingen av ny infrastruktur.

EU programmet *Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks* (CIPS) har som formål å beskytte mennesker og kritisk infrastruktur fra blant annet terrorangrep gjennom å forbedre og styrke beskyttelsen av kritisk infrastruktur. CIPS bidrar med kompetanse og veiledning og gir også finansieringsmuligheter for CIP-tiltak. Mellom 2007 og 2012 ble over hundre ulike prosjekter finansiert gjennom CIPS.[39]

9.3.4 Instruks om sikring og beskyttelse av objekter ved bruk av sikringsstyrker

Instruks om sikring og beskyttelse av objekter ved bruk av sikringsstyrker fra Forsvaret og politiet i fred, krise og krig, fastsatt ved kongelig resolusjon 24. august 2012 fastsetter bestemmelser for ansvarsforhold og samarbeid om politiets og Forsvarets objektsikring ved bruk av sikringsstyrker. Formålet med objektsikring er at viktige objekter skal opprettholde sin virksomhet og funksjonalitet i kritiske situasjoner.

Sentrale begreper i instruksen er blant annet objekt, objektsikring, sikring og beskyttelse, nøkkelpunkter og sikringsstyrker. Definisjonene som legges til grunn er som følger:

> Med *objekter* menes ethvert fysisk objekt som krever sikring og beskyttelse ved bruk av sikringsstyrker fra politiet og Forsvaret i fred, krise og krig mot anslag og angrep av kriminell eller militær karakter. *Objekter* omfatter områder og fast og rørlig eiendom, uavhengig av om objektene er offentlige eller private eller sivile eller militære. Med *objektsikring* og *sikring og beskyttelse* menes aktive operative tiltak som potensielt kan innebære maktbruk ved bruk av styrker rettet mot en konkret trussel.
>
> Med *sikringsstyrker* menes personer og enheter fra politiet eller Forsvaret som har til oppgave å beskytte et objekt mot en mulig eller konkret trussel.
>
> Med *nøkkelpunkter* menes sivile og militære objekter og personer, som er av avgjørende betydning for forsvarsevnen og det militære forsvar i krig, og som er å anse som lovlige militære mål i krig, jf. artikkel 52 i Tilleggsprotokoll I av 1977 til Genèvekonvensjonene av 1949.

Forsvarets og politiets ansvar for objektsikring i henhold til instruksen er uavhengig av forebyggende sikkerhetstiltak som følger av sikkerhetslovens objektsikkerhetsregelverk. Forsvaret og politiet skal imidlertid ta hensyn til om objektene er underlagt forebyggende grunnsikringsregler etter annet regelverk.

Forsvaret har ansvar for utpeking av militære objekter og nøkkelpunkter. Nøkkelpunkter kan være både militære og sivile objekter. Videre har Forsvaret ansvar for sikring av alle nøkkelpunkter og relevante militære objekter og deres umiddelbare nærhet. Forsvaret foretar selv prioritering av sikringsstyrker til ulike objekter og nøkkelpunkter. Forsvarets operative hovedkvarter (FOH) skal ha total oversikt over nøkkelpunkter og objekter som er av særlig betydning for samfunnet, samt tilgjengelige sikringsstyrker innenfor eget ansvarsområde.

Politiet har ansvar for utpeking og sikring av sivile objekter. Det er det enkelte politidistrikt som skal utpeke og planlegge sikring av objekter innenfor sitt geografiske område. Politidirektoratet (POD) skal ha total oversikt over objekter som er av særlig betydning for samfunnet, samt tilgjengelige sikringsstyrker i sivil sektor.

---

[39] European Commission, Migration and Home Affairs, «Critical infrastructure», http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm (oppsøkt 14.09.2016).

Forsvaret, POD og NSM skal så langt det lar seg gjøre ha innsyn i hverandres objektlister.

9.4 Fremmed rett

I internasjonal rett, og da særlig innenfor Europa er sektoransvarsprinsippet det rådende. Sektoransvarsprinsippet gjelder også når det gjelder fastsettelse av bestemmelser for virksomheter med ansvar for ulike deler av samfunnskritisk infrastruktur.

Det er varierende i hvor stor grad det er etablert et overordnet, tverrsektorielt koordineringsansvar og regelverk. Flere europeiske land, samt EU, har imidlertid en tverrsektoriell tilnærming til arbeidet med objektsikkerhet.

9.4.1 Beskyttelse av kritisk infrastruktur i EU

Gjennom EPCIP-direktivet fastsetter EU kriteriene for identifisering og utpeking av europeisk kritisk infrastruktur. Denne utvelgelses- og identifiseringsprosessen starter med vurderinger av infrastruktur ut i fra sektorspesifikke og sektorovergripende nasjonale hensyn. På denne måten gir EPCIP-direktivet også føringer for hvorledes den enkelte EØS-stat skal vurdere kritikaliteten til egen infrastruktur.

EPCIP-direktivets viktigste funksjon er imidlertid å sikre at grenseoverskridende avhengigheter mellom infrastruktur og innsatsfaktorer blir ivaretatt, samt fastsette reglene for hvordan slike saker skal løses.

EU-direktiv om tiltak for et høyt felles sikkerhetsnivå i nettverks- og informasjonssystemer i EU (NIS-direktivet),[40] som er omtalt i kapittel 8.4.5.2, er nylig blitt vedtatt i EU. Direktivet er sannsynligvis relevant også for EØS-land, men det er ikke vedtatt at dette skal gjelde også for Norge. Formålet med direktivet er å forbedre det indre markeds funksjon, gjøre EU mer konkurransedyktig i en globalisert verden, skape tillit til digitale tjenester og bidra til økonomisk vekst i Europa.

Som et ledd i dette stilles det krav til medlemsstatene om å identifisere operatører av essensielle tjenester som opererer på deres territorium. Fremgangsmåten som medlemsstatene skal følge for å identifisere operatører av essensielle tjenester er beskrevet i direktivet. Alle virksomheter som inngår i en liste over typer av virksomheter skal vurderes. Listen angir virksomheter i følgende sektorer:

- Energi
- Transport
- Helse
- Bank
- Finansmarkedsinfrastruktur
- Drikkevannsforsyning og -distribusjon
- Digital infrastruktur

Den fullstendige listen er gjengitt i NIS-direktivets, vedlegg 2 (Annex II).[41] Medlemslandene kan også vurdere andre virksomheter enn de som er oppramset i listen.

Videre skal medlemslandene vurdere om følgende vilkår er oppfylt:

- Virksomheten må tilby en tjeneste som er essensiell for opprettholdelsen av kritiske samfunnsmessige og/eller økonomiske aktiviteter.
- Tjenesteleveransen må være avhengig av nettverk og informasjonssystemer, og en hendelse i tjenestens nettverk og informasjonssystemer vil få en vesentlig forstyrrende virkning på leveransen.

Ved vurderingen av hva som er «vesentlig forstyrrende virkning», skal både tverrsektorielle og sektorspesifikke momenter tas i betraktning. Som omtalt i kapittel 8.4.5.2, stilles det krav til virksomheter som er operatører av essensielle tjenester om å gjennomføre sikkerhetstiltak.

Dersom dette direktivet gjøres gjeldende for Norge vil det gi føringer for hvordan operatører av essensielle tjenester skal identifiseres. Dette må i så fall ses i sammenheng med identifisering og utpeking av kritisk infrastruktur og kritiske samfunnsfunksjoner.

9.4.2 Beskyttelse av kritisk infrastruktur i NATO

Dagens trussel-, risiko, og sårbarhetsbilde vitner om behovet for internasjonalt engasjement som et supplement til nasjonal beredskap. NATOs sivile beredskapssystem ble gjennom 1990-tallet gradvis styrket og omstrukturert. Fokuset på internasjonalt samarbeid vedrørende beskyttelse av kritisk infrastruktur har særlig økt etter 11. september 2001. Flere terroranslag mot tog- og undergrunns-

[40] «NIS-direktivet», http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2016:194:FULL&from=EN (oppsøkt 14.09.2016).

[41] Ibid.

systemer i Europa bidro videre til økt oppmerksomhet rundt behovet for internasjonalt samarbeid om sikring av kritisk infrastruktur. Både EU og OSSE har økt sitt arbeid på feltet. Selv om beskyttelse av kritisk infrastruktur (*critical infrastructure protection (CIP*)) tradisjonelt ikke er et kjerneområde for NATO, har det fått økt oppmerksomhet.[42]

NATOs arbeid med CIP inkluderer sikring av egne anlegg, og sikring for ivaretakelse av samfunnsfunksjoner og infrastruktur som alliansen er avhengige av for å gjennomføre operasjoner (for eksempel utløst av artikkel 5). Alliansens formål er å kunne gjennomføre militære operasjoner uten at det går på bekostning av befolkningens trygghet. Dette innebærer at sivilbefolkningens behov er dekket før en eventuell militær operasjon iverksettes. For å gjennomføre eventuelle operasjoner er NATO, på lik linje med nasjonalstater, avhengig av for eksempel kritisk energiinfrastruktur. Avhengigheten av eksterne fossile energikilder, gjør at redusert tilgjengelighet vil kunne føre til kollaps i kritisk infrastruktur. CIP spiller derfor en nøkkelrolle for NATOs energisikkerhet.

Norge følger NATOs krav til sikring av NATO-anlegg på norsk jord. Foruten sikring av NATOs egne anlegg i medlemsland, kan ikke alliansen pålegge sine medlemsland andre sikringstiltak. NATO har i motsetning til EU ikke som formål å regulere beskyttelse av kritisk infrastruktur, men støtter opp om nasjonale planer ved å promotere høye standarder for beredskap og konsekvenshåndtering. En målsetting er blant annet økt informasjonsdeling, økt trening og utdanning, samt bistand til utpeking av kritisk infrastruktur. NATOs arbeid med CIP har fått økt prioritet i alliansen. Under NATO-toppmøtet i Riga i 2006 ble NATOs rolle i CIP fremhevet, herunder arbeidet med å beskytte befolkning, territorium, infrastruktur og forsvarsevne mot konsekvensene av terrorangrep.[43]

NATOs arbeid med CIP behandles i *Civil Protection Group* (CPG), som er en av de fire faggruppene underlagt *Civil Emergency Planning Committee* (CEPC). CEPC er den øverste komiteen for det sivile beredskapsarbeidet i NATO, og rapporterer direkte til Atlanterhavsrådet. DSB er Norges representant i CPG, som holder to plenumsmøter årlig.[44]

CEPC vedtok i 2003 et *concept paper* vedrørende CIP, og et veikart for det videre arbeidet. Målsettingen er å utvikle virkemidler for bedre å kunne møte utfordringer knyttet til hendelser som rammer kritisk infrastruktur.[45]

Første steg i CIP er å definere hva som anses som kritisk infrastruktur. NATOs medlemsland har ulike definisjoner som ofte reflekterer landets prioriteter. Selv om det ikke finnes noen allmenn definisjon, er kritisk infrastruktur vanligvis anlegg og tjenester som er vitale for opprettholdelse av samfunnets grunnleggende funksjoner, eller infrastruktur hvor bortfall vil nedsette samfunnets funksjonsevne.[46]

I noen land vektlegges særlig en infrastrukturs kritikalitet basert på om de funksjonene den representerer er vitale for samfunnet, mens andre land fokuserer mest på hvilken rolle infrastrukturen har og hvor alvorlig bortfall eller ødeleggelse av infrastrukturen vil være for samfunnet. Sistnevnte tilnærming er mest vanlig, men land som Frankrike benytter den første tilnærmingen.[47]

I de fleste medlemsland har definisjonen utviklet seg til å inkludere et bredt spekter av infrastruktur på tvers av et økende antall sektorer, fra de mer tradisjonelle sektorer som forsvar, transport og energi, til også å inkludere bank og finans, helse og IKT. Også infrastruktur som ikke er kritisk for samfunnets funksjonsevne, men som har en viktig symbolsk effekt, blir i økende grad ansett som kritisk infrastruktur. Sektorer som i de fleste av NATOs medlemsland anses som kritiske, inkluderer:

- Transportsystemer (fly, tog, vei og sjø).
- Energiproduksjon og shipping.
- Offentlige instanser og tjenester, herunder forsvar, rettshåndhevelse og krisetjenester.
- Informasjons- og kommunikasjonsteknologi.
- Mat og vann.
- Helsevesen og helsetjenester.
- Finansielle institusjoner.[48]

Selv om det er stort sammenfall i hvilke sektorer som anses som kritiske, er det noen europeiske land, herunder Østerrike og Sverige, som ikke

---

42 NATO Parliamentary Assembly, «The protection of critical infrastructures, 162 CDS 07 E rev 1», http://www.nato-pa.int/default.asp?SHORTCUT=1165 (oppsøkt 04.04.2016).

43 Ibid.

44 Direktoratet for samfunnssikkerhet og beredskap, «Sivilt beredskapsarbeid i NATO», http://www.dsb.no/Global/Om%20DSB/Dokumenter/Vedlegg%20%C3%A5rsrapport%20DSB%202013%20-%20Internasjonalt%20engasjement.pdf (oppsøkt 01.04.2016).

45 Ibid.

46 Ibid.

47 Ibid.

48 Ibid.

har noen offisielle lister over hvilke sektorer de regner som kritiske. CIP er en oppgave i risikohåndtering hvor hovedmålet er å redusere risikoen infrastrukturen står overfor til et akseptabelt nivå. Hvordan risikoen analyseres varierer noe fra land til land. De fleste europeiske land har en *all-hazard* tilnærming. Samtidig er det flere europeiske land, særlig England og Frankrike som har økt fokus på tilsiktede uønskede hendelser, særlig terrorisme.[49]

Når man vurderer mulige konsekvenser av en hendelse, er det vanskelig å sikre at alle konsekvenser er inkludert i analysen. Avhengigheter både innad i en sektor og på tvers av sektorer kan være sterke, særlig innen cyber-området. Mange nasjonale og internasjonale CIP-strategier er i utvikling for å bedre imøtekomme disse utfordringene.

Ulike risikoreduserende tiltak kan enten være knyttet til grunnsikring (permanente tiltak) eller påbygningstiltak som iverksettes basert på trusselnivået. Beskyttelsestiltak i NATOs medlemsland kan kategoriseres i fire ulike kategorier:[50]

- Fysiske sikringstiltak
- Elektroniske/cyber-tiltak
- Personkontroll
- Organisatoriske tiltak

9.4.3 Danmark

Danmark har som tidligere diskutert ikke noen generell sektorovergripende lov om forebyggende sikkerhet, og heller ikke et sektorovergripende lovverk vedrørende beskyttelse av kritisk infrastruktur.

Sektoransvaret er styrende for beskyttelse av kritisk infrastruktur i Danmark. Dette innebærer at alle myndigheter har ansvaret for beredskap i egen sektor. De myndigheter som har ansvaret for kritiske samfunnsfunksjoner, som veier, jernbane, teleforbindelse, helsevesen, og andre anlegg og funksjoner som er nødvendige for at samfunnet kan fungere arbeider systematisk med beredskap. Sektoranavarsprinsippet og bestemmelser om sivile sektorers planleggingsforpliktelser er forankret i den danske beredskapslovens kapitel 5 (§§ 24-28).

Etter det utvalget har fått opplyst har Beredskapsstyrelsen (underlagt Forsvarsministeriet) en generell plikt til å veilede myndighetene om beredskapsplanleggingen, men har ikke et tverrsektorielt ansvar for myndighetenes virkemidler overfor eiere og operatører av kritisk infrastruktur. Beredskapsstyrelsen har en *all hazards* tilnærming til beskyttelse av kritisk infrastruktur. Den danske Beredskapsstyrelsen har mange likhetstrekk med norske DSB og har i tett samarbeid med direktoratet utviklet en metode for kartlegging av nasjonal kritisk infrastruktur. Modellen har samme tilnærming som DSBs KIKS-modell.

Beredskapsstyrelsen har utarbeidet seks prinsipper for sektoransvaret med utgangspunkt i beredskapslovens § 24, stk. 1., disse er:

1. Alle ministre skal sikre et forsvarligt beredskab inden for deres eget ressortområde.
2. Sektoransvaret omfatter alle kritiske funktioner og opgaver, som er pålagt lovgivningsmæssigt, politisk eller administrativt.
3. Myndighedernes beredskabsplanlægning skal bygge på en løbende og systematisk risikostyringsproces, som er forankret i ledelsen.
4. Myndighederne skal forebygge større ulykker og katastrofer, hvor det er muligt, håndtere dem, når det er nødvendigt, og genoprette samfundets funktioner så hurtigt som muligt.
5. Myndighederne skal løbende overvåge risikobilledet inden for egen sektor.
6. Myndighederne skal sammen med forsvaret fastlægge behovet for civil støtte til forsvaret.[51]

Utviklingen i det danske arbeidet tilpasses i takt med utviklingen av EUs program for beskyttelse av kritisk infrastruktur (EPCIP). EU-regelverk styrer i stor grad nasjonale krav, særlig når det gjelder EPCIP-direktivet som pålegger Danmark å identifisere og utpeke europeisk kritisk infrastruktur (grenseoverskridende infrastruktur). EPCIP-direktivet er innarbeidet i den danske beredskapsloven, likesom EPCIP-direktivet i Norge er implementert i sivilbeskyttelsesloven som beskrevet i kapittel 9.3.3. Den danske beredskapsloven har flere likheter med den norske sivilbeskyttelsesloven da begge legger rammene for lokale beredskapsplaner.

9.4.4 Sverige

Säkerhetsskyddslagen er Sveriges lov som regulerer forebyggende sikkerhet. Sverige har også en beskyttelseslov, *Skyddslagen,* som er relevant for objekt- og infrastruktursikkerhet.

[49] Ibid.
[50] Ibid.
[51] Beredskabsstyrelsen, «Beredskap i Danmark, Sektorenes beredskap», http://brs.dk/beredskab/idk/sektorernesberedskab/Pages/Sektorensberedskab.aspx (oppsøkt 14.09.2016).

Säkerhetsskyddslagen er i stor grad innrettet for å sikre konfidensialitet for informasjon av betydning for *säkerhetskänslig verksamhet*. Säkerhetsskyddslagen er som nevnt i kapittel 6.3.1 under revisjon, og det er utarbeidet en *Statens Offentlige Utredningar* (SOU) der nytt lovgrunnlag for forebyggende sikkerhet er utredet.[52] Denne utredningen er utvalgets primære kilde for omtale av Sveriges regulering på området.

Säkerhetsskyddslagen omtaler ikke objekt- og infrastruktursikkerhet som eget tema. Bestemmelser under andre tema regulerer imidlertid relevante forhold. Det er særlig de deler som omhandler adgangsbegrensning (tillträdesbegränsning) som er relevant og vil bli diskutert her. De andre delene av *säkerhetsskyddslagen*, særlig personellsikkerhet og informasjonssikkerhet, er også relevant, men disse blir omtalt i NOUens øvrige tematiske kapitler.

I SOU 2015:25 understrekes behovet for å beskytte informasjon som er av betydning for *säkerhetskänslig verksamhet* ut i fra flere aspekter enn konfidensialitet. Utvalget som har utarbeidet rapporten foreslår å erstatte begrepet *tillträdesbegränsning* med begrepet *fysisk säkerhet*. De beskriver formålet med regulering av fysisk sikkerhet slik:

> Med fysisk säkerhet ska avses sådana säkerhetsskyddsåtgärder som ska förebygga dels att obehöriga får tillträde till områden, byggnader och andra anläggningar eller objekt där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller där verksamhet som av annan anledning är säkerhetskänslig bedrivs, dels skadlig inverkan på sådana områden, byggnader, anläggningar eller objekt.[53]

Skyddslagen med tilhørende forskrifter og forordninger er innrettet for å beskytte *skyddsobjekter* mot sikkerhetstruende virksomhet, og fokuserer på samfunnsfunksjoner som er viktig i et samfunnssikkerhetsperspektiv i fredstid. *Skyddsobjekt* kan være bygninger, anlegg og områder, samt militære fartøy og luftfartøy. Disse skal beskyttes mot sabotasje, terrorisme, spionasje og andre trusler mot hemmelig virksomhet.

Formålet med *Skyddslagens* følger av 1 § *Lagens syfte och skyddsändamål*:

> Denna lag innehåller bestämmelser om vissa åtgärder till förstärkt skydd för byggnader, andra anläggningar, områden och andra objekt mot åtgärder till förstärkt skydd för byggnader, andra anläggningar, områden och andra objekt mot 1. sabotage, 2. terroristbrott enligt 2 § lagen (2003:148) om straff förterroristbrott, 3. spioneri samt röjande i andra fall av hemliga uppgifter som rör total-försvaret, och 4. grovt rån.
>
> Lagen innehåller också bestämmelser om skydd för allmänheten mot skada som kan uppkomma till följd av militär verksamhet. [54]

Beskyttelse av objekter og infrastruktur i svensk lovgivning er altså delt mellom disse to lovene, som til sammen dekker mange av de samme forhold som det norske objektsikkerhetsregelverket under dagens sikkerhetslov. Dette er omtalt i SOU 2015:25:

> Vi anser att den norska sikkerhetsloven innehåller bestämmelser om objektssäkerhet som på ett bra sätt skulle kunna tydliggöra förhållandet mellan skydds- och säkerhetsskyddslagen. Sådana bestämmelser skulle dock kunna utformas genom tillämpningsföreskrifter. Vi föreslår därför inte att någon bestämmelse om detta tas in i en ny lag. Däremot är den nuvarande hänvisningen till skyddslagen fortfarande relevant och bör därför kvarstå oförändrad i en ny säkerhetsskyddslag.[55]

Videre er Sverige gjennom sitt medlemskap i EU forpliktet til å følge EPCIP-direktivet. Det er Myndigheten for samhällsskydd ock beredskap (MSB) som er utpekt som nasjonalt kontaktpunkt for arbeidet med EPCIP. Dette innebærer at MSB skal samordne spørsmål om beskyttelse av kritisk infrastruktur i Sverige, med andre medlemsland og med EU-kommisjonen.

I henhold til MSBs nettsider legger MSB til grunn en bredere forsåelse av begrepet samfunnsviktig virksomhet enn det som ligger i definisjonen i EPCIP. Sverige har i likhet med Norge ennå ikke utpekt europeisk kritisk infrastruktur.

---

[52] SOU 2015:25, *Betänkande av Utredningen om säkerhetsskyddslagen.*

[53] Ibid., 361.

[54] Sveriges riksdag, Skyddslag (2010:305), http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/skyddslag-2010305_sfs-2010-305 (oppsøkt: 14.09.2016)

[55] SOU 2015:25, 365

9.4.5 Storbritannia

Arbeidet med beskyttelse av kritisk infrastruktur i Storbritannia er forankret i *Security Act* (1989), og ivaretas av *Centre for the Protection of National Infrastructure* (CPNI), underlagt MI5. Ved å være under MI5 besitter CPNI stor kunnskap om truslene Storbritannia står overfor. Deres jobb er å få implementert vedtatt forebyggende sikkerhetspolicy og sikkerhetsregimer både i offentlig og privat sektor, med målsetting om å minimere risiko og redusere sårbarhet med tanke på tilsiktede hendelser. Dette gjelder fysisk objektsikring, personellsikkerhet og informasjonssikkerhet, inkludert cyber.

Storbritannia omtaler nasjonal infrastruktur som *the national infrastructure* og er definert som:

> Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:
>
> a) major detrimental impact on the availability, integrity or delivery of essential services – including those services, whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or
>
> b) significant impact on national security, national defence, or the functioning of the state.[56]

Når det gjelder kritisk nasjonal infrastruktur defineres dette i Storbritania som følger:

> Critical National Infrastructure comprises «those assets, services and systems that support the economic, political and social life of the United Kingdom whose importance is such that loss could:
>
> – cause large-scale loss of life;
> – have a serious impact on the national economy;
> – have other grave social consequences for the community;
> – or be of immediate concern to the national government.»[57]

Ansvarlig departement utpeker kritisk infrastruktur innenfor sitt område. Imidlertid har CPNI oppsyn med at definisjonene og klassifikasjonen av infrastruktur er foretatt i henhold til gjeldende standarder og praksis.

Utpeking i den enkelte sektor starter altså med det enkelte fagdepartement. Deretter blir det dialog og forhandling mellom eier av infrastruktur, CPNI og departementet som leder ut i implementerte sikkerhetstiltak.

CPNI holder oversikt over kritisk nasjonal infrastruktur, og opererer med seks ulike nivåer av kritikalitet for infrastruktur basert på deres viktighetsgrad for samfunnet. De tre øverste nivåene anses som kritiske. De lavere nivåer benyttes først og fremst for å holde oversikt over kategorier av infrastruktur som det kan være aktuelt å flytte til en av de høyere kategoriene dersom det skjer relevante endringer i samfunnet. Tilsvarende kan også infrastruktur som vurderes å ha endret status til mindre kritisk flyttes ned under den kritiske terskelen.

CPNI driver utadrettet og aktiv rådgivningsvirksomhet overfor både offentlige myndigheter og selvstendige rettssubjekter som eier eller forvalter kritisk infrastruktur, men har ikke myndighet til å gi pålegg eller sette krav til sikringen av slik infrastruktur.

I noen tilfeller gir myndighetene økonomisk støtte for å få kostbare sikringstiltak på plass ved utsatte objekter. Normalt vil det gis økonomisk kompensasjon etter dokumentert gjennomført tiltak. Storbritannia har også en forordning der sektormyndigheter kan få godkjent ulike økonomiske virkemidler (eksempelvis skatter, avgifter og gebyrer) som flytter de økonomiske kostnadene over på forbrukerne gjennom høyere priser på tjenester.

9.5 Utvalgets vurderinger og forslag

9.5.1 Objekt- og infrastruktursikkerhet

Utvalget mener at objekter og infrastruktur som er av kritisk betydning *for grunnleggende nasjonale funksjoner* må beskyttes. Utvalget mener både begrepet *skjermingsverdig objekt og skjermingsverdig infrastruktur* bør benyttes.

Med begrepet skjermingsverdig objekt legges følgende definisjon til grunn:

> eiendom som må beskyttes mot tilsiktede uønskede hendelser av hensyn til opprettholdelse av grunnleggende nasjonale funksjoner. Eiendom omfatter områder, bygninger, anlegg,

---

[56] Center for the Protection of National Infrastructure (CPNI), «The national infrastructure», http://www.cpni.gov.uk/about/cni/ (Oppsøkt: 14.09.2016).

[57] NATO Parliamentary Assembly, «The protection of critical infrastructures», 2016.

> transportmidler eller annet materiell, eller deler av slik eiendom.

Utvalget mener at definisjonen av *skjermingsverdig objekt,* på samme måte som i dagens sikkerhetslov, under visse omstendigheter også skal dekke lokaliteter der aktiviteter finner sted og bestemte personer oppholder seg slik dette er omtalt i innledningen til kapittel 9.2 og i forarbeidene til sikkerhetsloven.[58]

Objekt slik det er benyttet i gjeldende sikkerhetslov dekker også infrastruktur. Utvalget ser likevel behov for å innføre begrepet *infrastruktur,* for å skape tydeligere skille mellom enkeltstående objekter og infrastruktur som del av et system som understøtter grunnleggende nasjonale funksjoner. Som tidligere omtalt, er det blitt fremhevet av en rekke instanser at det er behov for å utvikle objektsikkerhetsregelverket slik at det gir bedre fleksibilitet i hvordan (og med hvilken type tiltak) et gitt sikkerhetsnivå skal oppnås. Det har særlig blitt vektlagt behov for å stimulere til tiltak som øker redundans og resiliens for kritiske samfunnsfunksjoner. Utvalget har lagt disse synspunktene og argumentene til grunn for sin anbefaling om å innføre begrepet *skjermingsverdig infrastruktur*. Utvalget ser det også som naturlig å benytte dette begrepet for å skape en klarere sammenheng med DSBs KIKS-systematikk, samt for å etablere et begrepsapparat som samsvarer bedre med internasjonal begrepsbruk. Infrastruktur og kritisk infrastruktur går igjen som et offisielt begrep i EU, NATO og de fleste landene Norge har et sikkerhetssamarbeid med.

Utvalget legger følgende definisjon til grunn for skjermingsverdig infrastruktur:

> anlegg og systemer som må beskyttes mot tilsiktede uønskede hendelser av hensyn til opprettholdelse av grunnleggende nasjonale funksjoner.

Utvalget mener med dette at *skjermingsverdig infrastruktur* er *kritisk infrastruktur* som må beskyttes mot *tilsiktede uønskede hendelser* av hensyn til opprettholdelse av grunnleggende nasjonale funksjoner. Utvalget oppfatter altså s*kjermingsverdig infrastruktur* som en delmengde av *kritisk infrastruktur,* på samme måte som *grunnleggende nasjonale funksjoner* oppfattes som en delmengde av *kritiske samfunnsfunksjoner*, slik dette er beskrevet i kapittel 6.7.3. Kritisk infrastruktur er definert som følger:

> anlegg og systemer som er nødvendige for å opprettholde samfunnets grunnleggende behov og funksjoner.

Det er behov for å regulere både *skjermingsverdige objekter* og *skjermingsverdig infrastruktur*. Disse to begrepene er delvis overlappende, men ingen av dem anses som tilstrekkelig dekkende for det loven skal regulere. I forståelsen av begrepet *skjermingsverdig infrastruktur* skal det legges vekt på koblingene mellom relevante objekter og systemer som er nødvendig for å understøtte *grunnleggende nasjonale funksjoner.*

9.5.2 Fordeling av ansvar og myndighet

Utvalget har vurdert ulike modeller for å fordele myndighet og ansvar for ulike oppgaver. Utfordringen er å finne en løsning som både ivaretar ønsket om høy grad av sektorautonomi og samtidig sikrer god tversektoriell koordinering av forebyggende nasjonal sikkerhet.

I henhold til objektsikkerhetsregelverket under dagens sikkerhetslov skal departementene utpeke skjermingsverdige objekter på bakgrunn av objektenes: a) betydning for sikkerhetspolitisk krisehåndtering og forsvar av riket, b) betydning for kritiske funksjoner for det sivile samfunn, c) symbolverdi, og d) mulighet for å utgjøre en fare for miljøet eller befolkningens liv og helse. Dette innebærer at departementene er forpliktet til å holde oversikt over kritiske samfunnsfunksjoner og deres sårbarheter på sine myndighetsområder.

Departementene har også i henhold til samordningsresolusjonen omtalt i kapittel 3.4, ansvar for å holde oversikt over *kritiske samfunnsfunksjoner* og deres sårbarheter på sine myndighetsområder. Utvalget mener det vil være hensiktsmessig å videreføre denne praksis, men mener det er behov for at departementene bør ha et utvidet og konkretisert ansvar for å holde oversikt over objekter og infrastruktur som har betydning for *grunnleggende nasjonale funksjoner*, og ansvar for sikkerhetsnivået i egen sektor. Dette må ses i sammenheng med det ansvar og de oppgaver utvalget har anbefalt at departementene skal ha i det generelle sikkerhetsarbeidet, beskrevet i kapittel 7.7.1.

Samtidig ser utvalget behov for å styrke Sikkerhetsmyndighetens rolle som ansvarlig for å koordinere sikkerhetstiltak på tvers av sektorer. Tversektoriell koordinering er å sikre et harmonisert sikkerhetsnivå, samt å sikre at sårbarheter knyttet til tversektorielle avhengigheter blir godt ivaretatt. Samfunnsøkonomiske lønnsomhetsvur-

[58] Ot.prp. nr. 21 (2007–2008).

deringer bør vektlegges i NSMs arbeid på dette området. Denne tverrsektorielle koordineringen vil være viktig for å sikre at risikoreduserende tiltak iverksettes der hvor de gir mest nytte for samfunnet, sett i forhold til samfunnets kostander ved å iverksette tiltaket. Dette slik at sårbarheter knyttet til tverrsektorielle avhengigheter blir håndtert effektivt i et nasjonalt perspektiv.

For at Sikkerhetsmyndigheten skal settes i stand til å ivareta sin koordinerende og sektorovergripende rolle, mener utvalget at det er nødvendig å tydeliggjøre rapporteringsansvar og informasjonsbehov for ulike etater og virksomheter. Utvalget mener Sikkerhetsmyndigheten bør arbeide med å finne effektive løsninger for rapportering og informasjonsforvaltning omkring skjermingsverdige objekter og infrastruktur. Dette bør gjennomføres i nært samarbeid med DSBs arbeid med *kritiske samfunnsfunksjoner* og *kritisk infrastruktur*, samt med berørte sektorer for å sikre at eventuelle sammenfallende informasjons- og rapporteringsbehov blir godt koordinert.

9.5.3 Utpeking og klassifisering av skjermingsverdige objekter og infrastruktur

Utvalget mener en svakhet med dagens objektsikkerhetsregelverk er at det ikke hviler noen forpliktelse på departementer eller NSM om å holde oversikt over objekter som er av en type som er nødvendig for understøttelse av *kritiske samfunnsfunksjoner,* men som ikke er kritisk som enkeltobjekt. Dette kan for eksempel skyldes tilstrekkelig redundans. Disse objektene vil derfor ikke være underlagt sikkerhetsloven. Dette leder til sårbarhet ved endringer i trusselbildet, eller annen samfunnsutvikling, som fører til at objekter som faller i en slik gruppe sannsynligvis ikke raskt nok blir utpekt som skjermingsverdig etter dagens regelverk, og dermed ikke i tilstrekkelig grad beskyttes med forebyggende sikkerhetstiltak.

I Storbritannia er det, som tidligere nevnt, CPNI som holder oversikt over *kritisk infrastruktur.* Der opererer man med seks ulike nivåer av kritikalitet for infrastruktur basert på deres viktighetsgrad for samfunnet. De lavere nivåer medfører ikke eksplisitte krav til sikkerhetstiltak, men benyttes først og fremt for å holde oversikt over en kategori infrastruktur som er aktuell for å flyttes til en høyere kategori dersom det skjer relevante endringer i samfunnet. Tilsvarende kan også infrastruktur som endrer status til mindre kritisk flyttes under den kritiske terskelen. CPNI fremhevet nytten av denne forordningen overfor utvalget under utvalgets besøk i Storbritannia.

Utvalget mener at konseptet som CPNI benytter i klassifiseringssammenheng er interessant fordi det ser ut til å gi høy grad av dynamikk i utpeking og klassifisering av objekter. Etter utvalgets oppfatning vil det samme kunne oppnås gjennom det ansvar som anbefales gitt til departementene om å holde oversikt over hvilke virksomheter som understøtter *grunnleggende nasjonale funksjoner* og *kritisk infrastruktur*, samt deres avhengigheter av innsatsfaktorer fra andre virksomheter og andre sektorer. Dette betyr at departementene må ha oversikt over både infrastruktur og objekter som er utpekt som skjermingsverdige, samt virksomheter som leverer innsatsfaktorer som understøtter *grunnleggende nasjonale funksjoner,* men som ikke er utpekt som *skjermingsverdig objekt eller infrastruktur.*

Utvalget mener også at innføringen av begrepet *skjermingsverdig infrastruktur* i seg selv vil kunne bidra til å forbedre situasjonen, da summen av objekter som inngår i et system kan oppfattes å utgjøre en *skjermingsverdig infrastruktur*. Sikkerhetsmyndigheten vil ha en viktig rolle i den tverrsektorielle koordineringen. Det vil være behov for at prosessen med å kartlegge og utpeke *skjermingsverdige objekter og infrastruktur*, gis en mer detaljert regulering. Denne type prosessregler bør gis i forskrifts form, og eventuelt ytterligere forklares og utdypes i understøttende veiledninger.

Utvalget mener det vil være hensiktsmessig å klassifisere *skjermingsverdige objekter og infrastruktur* basert på hvilke samfunnsfunksjoner de understøtter, og en skadevurdering ved redusert funksjonalitet som grunnlag for fastsettelse av krav til sikkerhetsnivå. Dagens sikkerhetslov benytter klassifiseringsgradene MEGET KRITISK, KRITISK og VIKTIG. Utvalget mener disse begrepene og nivåene er hensiktsmessige da betegnelsene signaliserer skadepotensialet overfor myndigheter og andre med saklig behov for slik informasjon. Utvalget foreslår derfor å benytte de samme begrepene og nivåene for skjermingsverdige objekter og infrastruktur.

Utvalget mener at begrunnelsen for klassifiseringen vil inneholde viktig informasjon for sektormyndigheter og Sikkerhetsmyndigheten i forbindelse med tilsyn og kontroll med sikkerhetsnivå og gjennomførte sikkerhetstiltak. Utvalget mener derfor at denne informasjonen bør følge sektormyndigheters og Sikkerhetsmyndighetens oversikt over skjermingsverdige objekter og infrastruktur.

9.5.4 Gjennomføring av sikringstiltak

Utvalget mener at det i lovforslaget bør stilles funksjonelle krav til sikkerhetstiltak fremfor spesifikke krav. Det bør være opp til sektormyndighet å avgjøre i hvilke grad det skal spesifiseres hvilke tiltak som skal gjennomføres eller hvorvidt det først og fremst skal pekes på for lavt sikkerhetsnivå på spesifikke områder og la det være opp til virksomheten å velge hvilke tiltak som skal gjennomføres. Etter utvalgets syn vil dette være den beste løsningen for å bidra til at sikkerhetsnivået blir på riktig nivå med så lav kostnad som mulig. Som tidligere nevnt, er det en forutsetning at aktuelle sikkerhetstiltak mot objekter og infrastruktur i sum er samfunnsøkonomisk lønnsomme.

Virksomheter og myndigheter som skal vurdere ulike sikkerhetstiltak, gjennomføre tiltak eller føre tilsyn med sikkerhetstilstanden, har behov for tilgang til ekspertkunnskap. Dette vil være nødvendig for å sikre at de tiltak som blir valgt og iverksatt er effektive og tilpasset dagens trusselbilde. I denne sammenheng vil det være avgjørende å benytte seg av et bredt spekter av fagmiljøer med relevant kompetanse, nasjonalt og internasjonalt. Det bør imidlertid tillegges en sentralisert funksjon å holde oversikt over slike fagmiljøer, samt å bidra til informasjonsutveksling og samarbeid, og å identifisere kunnskapshull og behov. Disse oppgavene vil naturlig kunne legges til Sikkerhetsmyndigheten. Dette vil også være viktig for at Sikkerhetsmyndigheten skal opprettholde tilstrekkelig faglig tyngde, noe som vil være nødvendig for å ivareta det overordnede ansvaret for forebyggende nasjonal sikkerhet.

Utvalget mener det bør påhvile den enkelte virksomhet som omfattes av loven, gjennom å ha fått utpekt *skjermingsverdig infrastruktur eller objekter*, å gjennomføre sikkerhetstiltak. Virksomhetene må også ta kostnadene av sikkerhetstiltakene. Kostnader ved slike sikkerhetstiltak bør stå i et rimelig forhold til det som oppnås ved tiltaket.

I enkelte tilfeller vil det ut fra samfunnets behov for sikkerhet kunne være nødvendig å pålegge omfattende sikkerhetstiltak for en spesifikk virksomhet eller i en samfunnssektor. Dette vil gagne samfunnet som helhet og ofte være nyttig for virksomheten som får pålegg. Dersom slike pålegg likevel medfører uforholdsmessig stor belastning for den aktuelle virksomhet eller sektor, sett i forhold til den egenverdi tiltakene har for virksomheten/sektoren, kan det være behov for å vurdere kompensatoriske tiltak. Som nevnt i kapittel 4.5, har staten et bredt spekter av virkemidler som kan benyttes for å oppnå god nasjonal sikkerhet, hvor økonomiske virkemidler er et av flere virkemidler. Utvalget ser det imidlertid ikke som formålstjenlig å spesifisere eventuelle kompensatoriske tiltak i loven. For det tilfelle slike pålegg skulle bli nødvendig, bør dette så langt som mulig søkes løst gjennom tett dialog mellom NSM, aktuelle sektormyndigheter og berørte virksomheter.

Forebyggende sikkerhet omhandler både grunnsikring og forsterkningstiltak. Således er *Instruks om sikring og beskyttelse av objekter ved bruk av sikringsstyrker*, viktig å se i sammenheng med sikkerhetsloven.

Kapittel 10
Personellsikkerhet

10.1 Innledning

Personellsikkerhet er et administrativt sikkerhetstiltak som skal bidra til å sikre at personell som har tilgang til sensitiv informasjon og sensitive objekter/infrastruktur, har den nødvendige lojalitet, pålitelighet og tillit som er nødvendig i et sikkerhetsmessig perspektiv.

Personellsikkerhet er et område hvor myndighetene gis hjemmel til å innhente og behandle til dels meget sensitive opplysninger om den enkelte, i den hensikt å vurdere hvorvidt vedkommende har nødvendig lojalitet og pålitelighet. Personellsikkerhet har således klare grenseflater mot enkeltindividets rettssikkerhet og personvern, og er derfor også et område som Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget) følger nøye. Som nevnt i kapittel 5.6 har Evalueringsutvalget i sin utredning foreslått at EOS-utvalget, primært av kapasitetsmessige årsaker, ikke lenger bør føre kontroll med avgjørelser om sikkerhetsklarering. Denne oppgaven foreslås i stedet lagt til et annet organ, eksempelvis Sivilombudsmannen.[1]

Siden sikkerhetslovens ikrafttredelse har det vært en stor demografisk utvikling. Norge er i dag et mangfoldig samfunn, og det er et politisk ønske om at dette også gjenspeiles i offentlig forvaltning. Globaliseringen av samfunnet medfører også at norske virksomheter i økende grad er avhengig av å hente inn nøkkelkompetanse fra utlandet. Dette er en ønsket samfunnsutvikling. Samtidig kan dette også bidra til å skape nye sårbarheter.

Utvalgets målsetting med forslaget til regulering av personellsikkerhet er å legge forholdene til rette for å forebygge og eventuelt avdekke utro tjenere som får tilgang til informasjon eller områder der skadepotensialet er stort. Eksempelvis er utenlandsk etterretning mot norske interesser, og vil fortsette å være, en reell trussel mot grunnleggende nasjonale funksjoner. Personell med tilgang til sensitiv informasjon eller til sensitive områder, vil kunne bli satt under press for å misbruke slike tilganger. Det er i denne sammenheng helt avgjørende at myndighetene kan forsikre seg om at personell som gis slike tilganger har den nødvendige lojalitet og pålitelighet.

En annen målsetting med utvalgets forslag er at hensynet til den enkeltes rettssikkerhet og personvern ivaretas i klareringsprosessen. En rekke av hjemlene i dette regelverket er inngripende overfor den enkelte, og det er således sentralt at det er etablert tilstrekkelige og tilfredsstillende rettssikkerhetsgarantier der slike inngrep er nødvendige.

En grunnleggende problemstilling utvalget må ta stilling til, er om de senere års demografiske endringer medfører behov for justeringer av regelverket for personellsikkerhet.

En annen utfordring med dagens klareringsinstitutt, er at saksbehandlingstiden ved sikkerhetsklareringer i mange tilfeller er svært lang. Lang saksbehandlingstid, kombinert med klareringsinstituttets inngripende karakter overfor den enkelte, er i seg selv en rettssikkerhetsmessig utfordring. I tillegg er det økonomisk kostbart for de virksomheter som er avhengige av den enkeltes kompetanse i sitt daglige virke. En problemstilling i denne sammenheng er hvorvidt det er innretningen på dagens lovregulering som i seg selv har en negativ innvirkning på saksbehandlingstiden. I den utstrekning utfordringene knyttet til saksbehandlingstid skyldes regelverket, må utvalget vurdere hvorvidt det er mulig å innrette loven på en måte som understøtter behovet for effektivitet.

En annen grunnleggende problemstilling utvalget må ta stilling til, er hvorvidt personellsikkerhet bør reguleres i en sektorovergripende lov, eller om det er tilstrekkelig at regulering av dette fagfeltet overlates til de ulike sektorspesifikke regelverkene. Herunder må utvalget vurdere hvorvidt det eksisterer hjemler for personkontroll i aktuelt sektorregelverk, og hvorvidt disse i så fall vurderes som tilfredsstillende.

[1] Dok. 16 (2015–2016), 132 flg.

10.2 Gjeldende sikkerhetslovs regulering

10.2.1 Tidligere revisjoner av personellsikkerhet

Lov- og forskriftsverket om personellsikkerhet har blitt revidert to ganger siden det trådte i kraft i 2001, i henholdsvis 2006 og 2011. Formålet med endringene har vært å styrke enkeltindividets rettssikkerhet i klareringsprosessen, og å etablere mekanismer som sikrer at personer ikke sikkerhetsklareres i større utstrekning enn nødvendig.

Forsvarsdepartementet besluttet sommeren 2003 å opprette en arbeidsgruppe som skulle vurdere sikkerhetslovens kapittel om personellsikkerhet, samt personellsikkerhetsforskriften og praksis. Arbeidsgruppen fikk i oppdrag å fremme begrunnede forslag til endringer i dette regelverket med sikte på å styrke den enkeltes rettssikkerhet.

Arbeidsgruppen leverte sin rapport Grenseland mellom rettssikkerhet og personellsikkerhet, til Forsvarsdepartementet 1. mars 2004. I rapporten ble det foreslått flere lovendringer med sikte på styrking av rettssikkerheten i sikkerhetsklareringssaker. I tillegg foreslo arbeidsgruppen en reduksjon i antall klareringsmyndigheter. Arbeidsgruppen presenterte tre modeller for ny organisering av klareringsmyndighetene, som alle i forskjellig grad innebar en sentralisering av dem.

I Ot.prp. nr. 59 (2004–2005)[2] fremmet Forsvarsdepartementet forslag om flere endringer i sikkerhetslovens kapittel om personellsikkerhet:

- Lovfesting av at tilknytning til andre stater kan være relevant å legge vekt på i vurderingen av sikkerhetsmessig skikkethet.
- Hjemmel for å kunne sette vilkår for en sikkerhetsklarering i særlige tilfeller.
- Oppmyking av regelverket for klarering av utenlandske statsborgere.
- Nye saksbehandlingsregler knyttet til sikkerhetsklarering.

Forslaget ble vedtatt og lovendringene trådte i kraft 1. januar 2006.[3]

Enkelte av arbeidsgruppens forslag ble behandlet i Ot.prp. nr. 21 (2007–2008).[4] For å harmonisere regelverket med de nye bestemmelsene om objektsikkerhet, ble det fremmet forslag om at sikkerhetslovens bestemmelser om sikkerhetsklarering skulle gis anvendelse for personer som skal gis tilgang til skjermingsverdige objekter klassifisert MEGET KRITISK eller KRITISK, og at Kongen skulle gis fullmakt til å fastsette nærmere regler om hvem som skal avkreves sikkerhetsklarering for de nevnte skjermingsverdige objektene.

I tillegg ble det foreslått en innstramming i bruken av sikkerhetsklarering i forhold til skjermingsverdig informasjon, i den hensikt å redusere antallet klareringssaker. Tidligere ble det stilt krav om at personell som *ville kunne få* tilgang til skjermingsverdig informasjon skulle sikkerhetsklareres, noe som medførte at terskelen for å sikkerhetsklarere ble for lav. Departementet foreslo derfor en justering av ordlyden, som innebar at det som hovedregel bare skulle igangsettes sikkerhetsklarering for personell som *skulle* gis tilgang til skjermingsverdig informasjon. Disse lovendringene trådte i kraft 1. januar 2011.[5]

10.2.2 Tilgang til sikkerhetsgradert informasjon

Sikkerhetsloven § 19 omhandler vilkårene som skal være innfridd for at en person skal kunne få tilgang til skjermingsverdig/sikkerhetsgradert informasjon.

Det følger av bestemmelsens første ledd at en person som skal gis tilgang til skjermingsverdig informasjon, på forhånd skal autoriseres.

Personell som skal ha tilgang til skjermingsverdig informasjon gradert KONFIDENSIELT eller høyere, skal i tillegg sikkerhetsklareres før autorisering finner sted, jf. bestemmelsens annet ledd. For personell som kun trenger tilgang til informasjon gradert BEGRENSET, er det således ikke noe krav om sikkerhetsklarering.

Personell som gjennom sitt arbeid vil kunne få tilgang til skjermingsverdig informasjon gradert KONFIDENSIELT eller høyere, skal sikkerhetsklareres dersom andre risikoreduserende tiltak for å hindre at vedkommende ikke får tilgang til slik informasjon, ikke med rimelighet lar seg gjennomføre, jf. loven § 19 tredje ledd. Bestemmelsen

---

2 Ot.prp. nr. 59 (2004–2005) Om lov om endringar i lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven).

3 Fastsatt ved kgl.res. 21. desember 2005 med heimel i lov 17. juni 2005 nr. 81 om endringar i lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven).

4 Ot.prp. nr. 21 (2007–2008).

5 Fastsatt ved kgl.res. 22. oktober 2010 med hjemmel i lov 11. april 2008 nr. 9 om endringer i lov om forebyggende sikkerhetstjeneste (sikkerhetsloven).

Boks 10.1 Autorisasjon og sikkerhetsklarering

Med *autorisasjon* menes i sikkerhetslovens forstand en «avgjørelse, foretatt av autorisasjonsansvarlig, om at en person etter forutgående sikkerhetsklarering (med unntak for tilgang til informasjon sikkerhetsgradert BEGRENSET), bedømmelse av kunnskap om sikkerhetsbestemmelser, tjenstlig behov samt avlagt skriftlig taushetsløfte, gis tilgang til informasjon med angitt sikkerhetsgrad», jf. loven § 3 første ledd nr. 20.

Med *sikkerhetsklarering* menes «avgjørelse, foretatt av klareringsmyndighet og bygget på personkontroll, om en persons antatte sikkerhetsmessige skikkethet for angitt sikkerhetsgrad», jf. loven § 3 første ledd nr. 19.

åpner således for å sikkerhetsklarere personell som i utgangspunktet ikke skal ha tilgang til gradert informasjon, dersom vedkommende *kan* få slik tilgang. I forarbeidene nevnes vakter, rengjøringspersonell og andre som gjennom sitt arbeid er i en posisjon hvor en lett kan skaffe seg tilgang til informasjon – selv om dette vil innebære brudd på arbeidsinstruks eller lignende.[6] En forutsetning for at slikt personell skal sikkerhetsklareres, er at andre sikkerhetstiltak først skal være gjennomført for å redusere denne risikoen. Økonomiske og andre konsekvenser som en følge av gjennomføring av andre sikkerhetstiltak vil være av betydning for om personellet skal klareres. Det understrekes i forarbeidene at tredje ledd er ment som en snever unntaksregel, og at ikke enhver ekstrakostnad oppfyller kravet til «ikke med rimelighet lar seg gjennomføre».[7]

Av bestemmelsens fjerde ledd fremgår det hvilke sikkerhetsgrader det skal gjennomføres sikkerhetsklarering for nasjonalt, og eventuelt også for tilsvarende sikkerhetsgrader i NATO eller annen internasjonal organisasjon:

- KONFIDENSIELT (eventuelt NATO CONFIDENTIAL/tilsvarende)
- HEMMELIG (eventuelt NATO SECRET/tilsvarende)
- STRENGT HEMMELIG (eventuelt COSMIC TOP SECRET/tilsvarende)

I forarbeidene er det presisert at klarering for en nasjonal sikkerhetsgrad, ikke automatisk innebærer at vedkommende også er klarert for tilsvarende sikkerhetsgrad fastsatt av en internasjonal organisasjon, eksempelvis NATO. Dersom vedkommende skal klareres for tilgang til internasjonalt gradert informasjon, må klareringsmyndigheten treffe uttrykkelig avgjørelse om dette.[8] I praksis skjer dette ved at anmodende myndighet presiserer i klareringsanmodningen at vedkommende i sitt arbeid vil ha behov for tilgang til eksempelvis NATO-gradert informasjon.

10.2.3 Tilgang til skjermingsverdige objekter

I sikkerhetsloven § 17 b fjerde ledd er Kongen gitt myndighet til å bestemme hvorvidt det skal kreves sikkerhetsklarering etter reglene i loven kapittel 6 for den som skal gis tilgang til skjermingsverdig objekt klassifisert MEGET KRITISK eller KRITISK.

Rundt problemstillingen om sikkerhetsklarering for tilgang til skjermingsverdige objekter, uttales det i forarbeidene at:

> En avveining mot kostnadsmessige, sysselsettingsmessige og personvernmessige forhold, kan imidlertid tilsi at kravet i enkelttilfeller og innen enkelte sektorer vil medføre for inngripende konsekvenser, og av denne grunn ikke bør implementeres fullt ut. Sikkerhetsklarering vil heller ikke være et egnet virkemiddel for alle kategorier av objekter. Det framstår på denne bakgrunn som hensiktsmessig at det i loven kun etableres en forskriftshjemmel for å gjennomføre sikkerhetsklarering, og at de nærmere bestemmelser gis i forskrifts form.[9]

I objektssikkerhetsforskriften er myndigheten til å bestemme hvorvidt det skal kreves sikkerhetsklarering for personell som skal gis permanent tilgang til objekter klassifisert KRITISK eller MEGET KRITISK, tillagt det enkelte fagdepartement, jf. forskriften § 3-6 første ledd. Sikkerhetsklarering skal ikke foretas der dette ikke anses som et egnet virkemiddel, og objekter må begrunne behovet for klarering.

Dersom det kreves sikkerhetsklarering, skal tilgang til et objekt klassifisert KRITISK kreve sikkerhetsklarering for KONFIDENSIELT eller høyere. For tilgang til objekt klassifisert MEGET KRI-

6 Ot.prp. nr. 49 (1996–97), 70.
7 Ot.prp. nr. 21 (2007–2008), 46.
8 Ot.prp. nr. 49 (1996–97), 70.
9 Ot.prp. nr. 21 (2007–2008), 39.

TISK, kreves sikkerhetsklarering for HEMMELIG eller høyere.

For besøkende som ledsages av autorisert personell kreves det ikke sikkerhetsklarering, jf. bestemmelsens fjerde ledd. Det skal imidlertid kontrolleres at de besøkendes identitet er korrekt. For representanter for en annen stat, internasjonal organisasjon eller utenlandsk rettssubjekt, skal det i tillegg kontrolleres at vedkommende faktisk representerer vedkommende stat/organisasjon/rettssubjekt.

10.2.4 Gjennomføringen av personkontroll

Før klareringsmyndigheten kan treffe en avgjørelse om sikkerhetsklarering må det gjennomføres en personkontroll. Med personkontroll menes i denne sammenheng en innhenting av relevante opplysninger til vurdering for sikkerhetsklarering, jf. sikkerhetsloven § 3 første ledd nr. 18. Personkontrollen igangsettes ved at autorisasjonsansvarlig – normalt den enkelte virksomhet – sender en anmodning om sikkerhetsklarering til klareringsmyndigheten, jf. loven § 20 første ledd.

Igangsettelse av personkontroll forutsetter at den det gjelder er informert, og har samtykket til at en slik kontroll foretas, jf. bestemmelsens andre ledd. I praksis vil den enkelte bli bedt om å fylle ut et personopplysningsskjema som grunnlag for personkontrollen, som også gjelder som et samtykke for at informasjon innhentes fra en rekke ulike kilder. Vedkommende plikter i denne sammenheng å gi fullstendige opplysninger om forhold som antas å kunne være av betydning for vurdering av sikkerhetsmessig skikkethet.

Dersom anmodningen om sikkerhetsklarering gjelder for sikkerhetsgrad HEMMELIG/tilsvarende eller høyere, kan personkontrollen også omfatte kontroll av nærstående personer som er knyttet til vedkommende ved familiebånd, jf. bestemmelsens tredje ledd. Personkontroll av nærstående ved anmodning om klarering for KONFIDENSIELT/tilsvarende, kan bare skje i «andre særlige tilfeller». I følge forarbeidene omfatter «nærstående personer som er knyttet til vedkommende ved familiebånd» også ektefelle, samboer og registrert partner.[10]

Personkontrollen skal omfatte opplysninger som vedkommende klareringsmyndighet selv sitter inne med og opplysninger som fremgår ved avlesning av relevante offentlige registre, jf. bestemmelsens fjerde ledd første punktum. Kongen er gitt myndighet til å bestemme hvilke registre som er relevante for personkontroll, jf. femte ledd første punktum.

Boks 10.2 Registre for personkontroll

Med hjemmel i § 20 femte ledd har Kongen i personellsikkerhetsforskriften § 3-4 fastsatt at NSM i personkontrolløyemed kan kreve å få utlevert opplysninger fra:

1. Reaksjonsregisteret
2. Straffesaksregisteret
3. Registre ved Politiets sikkerhetstjeneste
4. Det sentrale folkeregister (DSF)
5. Registre ved Skattedirektoratet
6. Registre ved Statens innkrevingssentral
7. Registre ved Utlendingsdirektoratet
8. NSMs egne registre
9. Private kredittopplysningsregistre
10. Tilsvarende registre i fremmede stater.

Registeransvarlig for de ulike registrene plikter å utlevere registeropplysninger til NSM vederlagsfritt og uten hinder av lovbestemt taushetsplikt. Opplysningene skal meddeles skriftlig.

Personkontrollen kan også omfatte andre kilder, herunder uttalelser fra tjenestesteder eller arbeidsplasser, offentlige myndigheter eller oppgitte referanser, jf. bestemmelsens fjerde ledd fjerde punktum. I forarbeidene er det påpekt at opplysningsplikten for tidligere arbeidsgivere, offentlige myndigheter og oppgitte referanser, ikke går foran eventuell lovbestemt taushetsplikt. Normalt vil det imidlertid være en klar forutsetning at den det gjelder har gitt samtykke til å innhente enhver opplysning om vedkommende uten hinder av taushetsplikten, for eksempel fra referansepersoner som er ført opp i personopplysningsblanketten.[11]

Det er et totalforbud mot å innhente, registrere eller videreformidle opplysninger om vedkommendes politiske engasjement, jf. bestemmelsens femte ledd siste punktum.

I bestemmelsens sjette ledd slås det fast et strengt krav til formålsbestemthet knyttet til de opplysninger som innhentes som ledd i personkontrollen. Slike opplysninger skal ikke benyttes til andre formål enn vurdering av sikkerhetsklarering. Dersom det er påkrevet av hensyn til den

[10] Ot.prp. nr. 49 (1996–97), 70.

[11] Ibid.

Boks 10.3 Relevante forhold for personkontroll

Opplysninger om følgende forhold kan tillegges betydning:

a) Spionasje, planlegging eller gjennomføring av sabotasje, attentat eller lignende, og forsøk på slik virksomhet.
b) Straffbare handlinger eller forberedelser eller oppfordringer til slike.
c) Forhold som kan lede til at vedkommende selv eller nærstående personer som er knyttet til vedkommende ved familiebånd, utsettes for trusler som innebærer fare for liv, helse, frihet eller ære med risiko for å kunne presse vedkommende til å handle i strid med sikkerhetsmessige interesser.
d) Forfalskning av, eller feilaktig eller unnlatt fremstilling om, faktiske forhold som vedkommende måtte forstå er av betydning for sikkerhetsklareringen.
e) Misbruk av alkohol eller andre rusmidler.
f) Enhver sykdom som på medisinsk grunnlag anses å kunne medføre forbigående eller varig svekkelse av pålitelighet, lojalitet eller sunn dømmekraft.
g) Kompromittering av skjermingsverdig informasjon, brudd på gitte sikkerhetsbestemmelser, nektelse av å gi personopplysninger om seg selv, unnlatelse av å gi autorisasjonsansvarlig løpende underretning om egne forhold av betydning for sikkerheten, nektelse av å gi taushetsløfte, tilkjennegivelse av ikke å ville være bundet av taushetsløfte eller nektelse av å delta i sikkerhetssamtale.
h) Økonomiske forhold som kan friste til utroskap.
i) Forbindelse med innen- eller utenlandske organisasjoner som har ulovlig formål, som kan true den demokratiske samfunnsordenen eller som anser vold eller terrorhandlinger som akseptable virkemidler.
j) Manglende mulighet for gjennomføring av en tilfredsstillende personkontroll.
k) Tilknytning til andre stater.
l) Andre forhold som kan gi grunn til å frykte at vedkommende vil kunne opptre i strid med sikkerhetsmessige interesser.

sikkerhetsmessige ledelse og kontroll av vedkommende, kan imidlertid opplysninger som fremkommer under personkontrollen meddeles til autorisasjonsansvarlig.

10.2.5 Vurderingsgrunnlaget for sikkerhetsklarering

Vurderingen av om en person skal sikkerhetsklareres skal baseres på en konkret og individuell helhetsvurdering, der alle tilgjengelige opplysninger tas i betraktning. Klareringsmyndigheten plikter i denne forbindelse å sørge for at saken er så godt opplyst som mulig før avgjørelse fattes. Sikkerhetsklarering skal bare gis der det ikke foreligger rimelig tvil om vedkommendes sikkerhetsmessige skikkethet, jf. sikkerhetsloven § 20 tredje ledd første og annet punktum, jf. første ledd første punktum.

Ved avgjørelsen av vedkommendes sikkerhetsmessige skikkethet, skal det bare legges vekt på forhold som er relevante for å vurdere den aktuelle personens pålitelighet, lojalitet og sunne dømmekraft med hensyn til behandling av sikkerhetsgradert informasjon. Bestemmelsen har en opplisting av forhold som kan tillegges betydning for vurderingen i første ledd bokstav a til l.

Oppregningen i bestemmelsen er ifølge forarbeidene uttømmende, men bokstav l vil likevel fungere som en sikkerhetsventil for opplysninger av sikkerhetsmessig karakter som ikke lar seg henføre under de øvrige forhold som kan tillegges betydning.[12]

Det presiseres videre i forarbeidene at opplistingen ikke skal forstås som en prioritert rekkefølge av forhold som kan tillegges betydning.

Bokstav k om *tilknytning til andre stater*, kom inn ved lovendring som trådte i kraft 1. januar 2006. I forarbeidene beskrives endringen som en presisering av at tilknytningen norske statsborgere måtte ha til andre stater, kan bli lagt vekt på i en vurdering av sikkerhetsmessig skikkethet. Begrepet tilknytning bør tolkes vidt i den forstand at ulik art av tilknytning vil kunne være relevant. Det kan for eksempel dreie seg om økonomiske interesser i en stat eller det kan være tale om at vedkommende har familiær tilknytning til staten. Det er likevel bare den tilknytning som er relevant for den sikkerhetsmessige kvalifikasjonen til den

[12] Ibid.

enkelte, som det kan legges vekt på i vurderingen. Graden av tilknytning vil også være av betydning.[13]

NSM har i sin veileder til personellsikkerhet[14] utdypet hvilke vurderingstema som er relevante for bokstav a til l.

I bestemmelsens andre ledd slås det fast at politisk engasjement, herunder medlemskap i, sympati med eller aktivitet for lovlige politiske partier eller organisasjoner og annet lovlig samfunnsengasjement, ikke kan tillegges vekt ved vurderingen av den enkeltes sikkerhetsmessige skikkethet.

I henhold til bestemmelsens tredje ledd tredje punktum, skal sikkerhetssamtale gjennomføres der dette ikke anses som åpenbart unødvendig. Ved lovendringen som trådte i kraft 1. januar 2006 ble kravet til sikkerhetssamtale forsterket. Før lovendringen skulle klareringsmyndigheten «søke å avklare uklare forhold, eventuelt gjennom å avholde sikkerhetssamtale». Den forsterkede plikten til å avholde sikkerhetssamtale ble i forarbeidene begrunnet med en harmonisering med forvaltningsorganers utrednings- og informasjonsplikt i medhold av forvaltningsloven § 17, og innebærer at klareringsmyndigheten bør gjennomføre en slik samtale dersom det er tvil om vedkommende skal gis klarering.[15] Sikkerhetssamtale anses som en sentral rettssikkerhetsgaranti hvor den enkelte gis anledning til kontradiksjon. Samtidig kan en slik samtale oppleves ganske belastende for den enkelte. Disse forhold gjør at klareringsmyndighetens bruk av slike sikkerhetssamtaler følges tett av EOS-utvalget.

Negative opplysninger som innhentes som ledd i personkontrollen om en persons nærstående, skal bare tas i betraktning i den utstrekning det antas at disse forholdene vil kunne påvirke den sikkerhetsmessige skikketheten til den personen det søkes om sikkerhetsklarering for, jf. bestemmelsens fjerde ledd.

Etter bestemmelsens femte ledd kan det i særlige tilfeller settes vilkår for sikkerhetsklarering. Hjemmelen til å kunne sette vilkår for en klarering kom som følge av lovendringen som trådte i kraft 1. januar 2006. I forarbeidene vises det til at en sikkerhetsklarering på vilkår kan bidra til en forholdsmessig avgjørelse der alternativet ellers hadde vært å nekte klarering.[16] Arbeidsgrupperapporten som lå til grunn for departementets lovforslag sa følgende om forslaget:

> Et problem med at dagens klareringer kan nyttes for tjeneste ved flere forskjellige etater, er at de nødvendigvis vil måtte gis på et mer generelt grunnlag enn om klarering ble gitt for en bestemt stilling. Ved sistnevnte alternativ vil en risikovurdering kunne knyttes opp til den spesifikke stillingen eller oppdraget. Ettersom klareringsmyndigheten ikke kan vite i hvilken sammenheng klareringen kan tenkes benyttet i fremtiden, vil klareringsmyndigheten i sin vurdering muligens ta med en hypotetisk mulighet for at en person med spesielle bindinger kan utløse høy sikkerhetsmessig risiko i en gitt situasjon. Dette kan igjen medføre at klareringsmyndigheten nekter klarering selv om sannsynligheten for at risikosituasjonen skal oppstå, er liten. Et eksempel på dette kan være en person med slike økonomiske eller familiære bindinger til et land at vedkommende lettere kan bli utsatt for press til å handle i strid

Boks 10.4 EOS-utvalget om sikkerhetssamtaler

I EOS-utvalgets årsmelding for 2014 ga utvalget uttrykk for at det kunne være behov for en ekstern evaluering av gjennomføringen av sikkerhetssamtaler. EOS-utvalget hadde sett at kvaliteten på gjennomføringen av samtalene varierte i de ulike klareringsmyndighetene, og at enkelte samtaler kunne vært gjennomført på en mer tillitsskapende og målrettet måte. EOS-utvalget observerte blant annet at samtalene ofte er svært omfattende og kan ha en avhørslignende form, noe som kan oppfattes som belastende for den omspurte.

I 2015 har EOS-utvalget hatt en løpende dialog med NSM om gjennomføring av sikkerhetssamtaler, og NSM har opplyst at man ønsker å iverksette flere tiltak for å forbedre og videreutvikle klareringsmyndighetenes fagkompetanse på området. EOS-utvalget har i årsmeldingen for 2015 uttrykt at dette arbeidet vil følges tett, og at man i løpet av 2016 vil kontrollere flere sikkerhetssamtaler.

Kilde: EOS-utvalgets årsrapport for 2015 s. 24-26

[13] Ot.prp. nr. 59 (2004–2005), 32.

[14] Veiledning til sikkerhetslovens kapittel 6 og forskrift om personellsikkerhet, fastsatt av NSM med hjemmel i sikkerhetsloven § 26 annet ledd og forskrift om personellsikkerhet.

[15] Ot.prp. nr. 59 (2004–2005), 32.

[16] Ibid.

med Norges sikkerhetsmessige interesser hvis vedkommende skal gjøre tjeneste i det aktuelle landet.[17]

Av forarbeidene fremgår det videre at bestemmelsen ikke var tenkt brukt som en vanlig løsning. Regelen kunne tenkes brukt i situasjoner hvor en person har tilknytning til andre stater som kan gjøre det uheldig at vedkommende blir gitt en generell klarering, som også kan benyttes for eksempel til tjeneste i den staten vedkommende har tilknytning til. Bestemmelsen vil også kunne brukes der vedkommende som blir klarert har et utenlandsk statsborgerskap. I disse tilfellene kan det være aktuelt å sette som vilkår at klareringen bare kan benyttes for en bestemt stilling eller i et geografisk avgrenset område.[18]

10.2.6 Sikkerhetsklarering av utenlandske statsborgere

I medhold av sikkerhetsloven § 22 kan en utenlandsk statsborger gis sikkerhetsklarering etter en vurdering av hjemlandets sikkerhetsmessige betydning og vedkommendes tilknytning til hjemlandet og Norge. Frem til lovendringen i 2006 var hovedregelen at utenlandske statsborgere normalt ikke skulle gis sikkerhetsklarering, med mindre det forelå et særlig behov for å gi en utenlandsk statsborger tilgang til sikkerhetsgradert informasjon. I forarbeidene til lovendringen ble det foreslått en viss oppmyking av denne bestemmelsen. Det ble samtidig presisert at bestemmelsen fortsatt var en *kan*-regel, hvor de nærmere angitte vurderingstemaene er avgjørende for hvorvidt klarering gis.[19]

Vilkåret om vedkommendes tilknytning til hjemlandet blir i stor grad de samme vurderingene som for *tilknytning til en annen stat*, jf. loven § 21 første ledd bokstav k. Vilkåret om tilknytning til Norge må baseres på en bred konkret vurdering, hvor et relevant moment vil være hvor lenge vedkommende har bodd i Norge, og hvilke slektskapsforhold vedkommende har. I forarbeidene presiseres at det ikke er ønskelig å sette absolutte krav til oppholds- og arbeidstillatelse, men at dette kan være sentrale momenter i vurderingen av vedkommendes tilknytning til Norge.

Boks 10.5 Sikkerhetsavtale

Norge har sikkerhetsmessig samarbeid med en rekke andre stater, både allierte og andre stater. Som grunnlag for dette sikkerhetsmessige samarbeidet er det inngått sikkerhetsavtaler med de aktuelle statene. En sikkerhetsavtale omfatter alle relevante sikkerhetsmessige forhold knyttet til blant annet håndtering av sikkerhetsgradert informasjon og sikkerhetsklarering av personell.

Dersom utenlandske statsborgere innehar en sikkerhetsklarering fra et hjemland Norge har et sikkerhetsmessig samarbeid med, vil denne sikkerhetsklareringen som regel legges til grunn også for tilgang til norsk sikkerhetsgradert informasjon.

Dersom utenlandske statsborgere fra et land Norge har sikkerhetsmessig samarbeid med ikke har sikkerhetsklarering fra hjemlandet, vil Nasjonal sikkerhetsmyndighet innhente nødvendige personkontrollopplysninger via den aktuelle statens sikkerhetsmyndigheter.

10.2.7 Klareringsmyndighet og autorisasjonsansvarlig

Etter gjeldende sikkerhetslov § 23 (som er vedtatt endret, se under) er hvert enkelt departement klareringsmyndighet for personell på sitt myndighetsområde. Myndigheten kan delegeres, og dette er i stor utstrekning gjort. Etter flere reduksjonsprosesser, sist i 2006, er det i dag totalt 42 klareringsmyndigheter. Av disse er 5 innenfor forsvarssektoren (deriblant Etterretningstjenesten og Nasjonal sikkerhetsmyndighet), 7 innenfor den dømmende makt (Høyesterett og lagmannsrettene), samt 3 innenfor Stortingets organer (Stortingets presidentskap, Stortingets administrasjon og Riksrevisjonen). I tillegg er Politiets sikkerhetstjeneste egen klareringsmyndighet. For øvrig er det 26 ulike sivile klareringsmyndigheter, som utgjøres av de enkelte departementene og enheter disse har delegert klareringsmyndighet videre til.

Klareringsmyndighetsstrukturen ble vurdert ved revisjonen av sikkerhetsloven i 2006.[20] Arbeidsgruppen som den gang ble nedsatt for å se

[17] Arbeidsgrupperapport, *Grenseland mellom rettssikkerhet og personellsikkerhet*, avgitt til Forsvarsdepartementet 1. mars 2004, 69–70.

[18] Ot.prp. nr. 59 (2004–2005), 32.

[19] Ibid.

[20] Ibid, 29 flg.

på regelverket la fram tre forslag til klareringsmyndighetsstruktur:

1. en desentralisert modell med utgangspunkt i dagjeldende sikkerhetslov § 23,
2. to klareringsmyndigheter; en for sivil sektor og en for militær sektor,
3. en felles klareringsmyndighet.

Forsvarsdepartementet besluttet den gang å beholde eksisterende struktur. Det ble likevel gitt klare føringer for at delegasjonspraksisen skulle strammes inn:

> Departementet vil følgje med på den vidare utviklinga på dette feltet, og det vil bli ei sentral tilsynsoppgåve for Nasjonal sikkerhetsmyndigheit å følgje opp etterlevinga av regelen i § 23. Det er naudsynt at departementa i tida frametter strammar inn delegeringspraksisen. Dersom dette ikkje skjer, vil departementet eventuelt måtte sjå på andre strukturløysingar, også dei modellane om ei eller to klareringsstyringsmakter som er nemnde ovanfor.[21]

Forsvarsdepartementets oppfordring om å stramme inn delegasjonspraksisen har imidlertid hatt en begrenset virkning, og antallet klareringsmyndigheter har ikke blitt vesentlig redusert etter denne lovrevisjonen.

Forsvarsdepartementet har derfor i Prop. 97 L (2015–2016) – Endringer i sikkerhetsloven (reduksjon av antall klareringsmyndigheter mv.) foreslått at det opprettes to klareringsmyndigheter: én for forsvarssektoren og én for de sivile sektorene, hvor henholdsvis Forsvarsdepartementet og Justis- og beredskapsdepartementet har det overordnede ansvaret. Forslaget medfører en betydelig reduksjon av antall klareringsmyndigheter, hvor den vesentligste endringen er en sentralisering av klareringsmyndighetene i sivile sektorer. I forslaget ble det forutsatt at de tre EOS-tjenestene fortsetter å klarere eget personell, grunnet de særlige forhold som gjør seg gjeldende for disse tjenestene. Videre ble det åpnet for at andre enn EOS-tjenestene kan gis slik myndighet dersom særlige grunner tilsier det. Formålet med endringen var å øke kvaliteten og effektiviteten hos klareringsmyndighetene, noe som også vil bidra til økt rettssikkerhet for den enkelte gjennom en mer enhetlig praksis samt øke tilliten til klareringsinstituttet hos allmennheten generelt. Kompleksiteten i klareringssakene øker og det stilles stadig større krav til klareringsmyndighetenes kompetanse.

Det ble i tillegg forslått en strukturell endring av bestemmelsen, som ikke er ment å skulle innebære en realitetsendring.

Stortinget har i forbindelse med behandlingen av Innst. 352 L (2015–2016) til Prop. 97 L (2015–2016) om endringer i sikkerhetsloven, vedtatt regjeringens forslag om å redusere antall klareringsmyndigheter.

Boks 10.6 Forslag til ny § 23

§ 23 *Autorisasjonsansvarlig og klareringsmyndighet*

Autorisasjon kan gis dersom autorisasjonsansvarlig ikke har opplysninger som gjør det tvilsomt om vedkommende sikkerhetsmessig er til å stole på. Autorisasjon gis normalt av virksomhetens leder. Autorisasjon skal ikke gis før det foreligger melding om sikkerhetsklarering, med unntak for de tilfeller som er beskrevet i § 19 tredje ledd, og en autorisasjonssamtale er avholdt. Nasjonal sikkerhetsmyndighet gir nærmere regler om autorisasjon og om hvem som er autorisasjonsansvarlig.

Kongen utpeker en klareringsmyndighet for forsvarssektoren og en for den sivile sektoren. Kongen kan utpeke andre klareringsmyndigheter når særlige grunner taler for det. Etterretnings- og sikkerhetstjenestene klarerer eget personell.

10.2.8 Bortfall, tilbakekall, nedsettelse og suspensjon av sikkerhetsklarering og autorisasjon

Sikkerhetsklarert og autorisert personell har plikt til å holde autorisasjonsansvarlig orientert om forhold som antas å være av betydning for vedkommendes sikkerhetsmessige skikkethet, jf. sikkerhetsloven § 24 første ledd. Eksempelvis vil endringer i sivilstatus, ileggelse av straffereaksjoner fra politi- og påtalemyndighet eller vesentlige endringer i den enkeltes økonomiske situasjon, være forhold som den enkelte plikter å orientere autorisasjonsansvarlig om. I NSMs veiledning til personellsikkerhet uttrykkes det at endringer i de forhold som kan anses å gjelde § 21 første ledd bokstav a til j som i praksis innebærer endringer i

[21] Ibid.

forhold til det den enkelte har opplyst i personopplysningsblanketten, vil utløse en meldeplikt til autorisasjonsansvarlig.

Dersom det fremkommer opplysninger som reiser tvil om en sikkerhetsklarert persons sikkerhetsmessige skikkethet, plikter klareringsmyndigheten å vurdere hvorvidt klareringen skal tilbakekalles, nedsettes til et lavere klareringsnivå eller suspenderes, jf. bestemmelsens andre ledd. Klareringsmyndigheten skal også i slike situasjoner iverksette nærmere undersøkelser for å avklare forholdet. Forarbeidene gir ingen nærmere veiledning om hvilke undersøkelser klareringsmyndigheten kan iverksette med hjemmel i § 24.

Ved behandlingen av den såkalte FOST-saken uttalte EOS-utvalget seg om grensedragningen mellom den enkelte virksomhets undersøkelse av sikkerhetstruende hendelser og klareringsmyndighetens ansvar for å iverksette undersøkelser etter § 24:

> Grensen mellom virksomhetens generelle ansvar for forebyggende sikkerhetstjeneste, herunder undersøkelse av sikkerhetstruende hendelser, og klareringsmyndighetens ansvar for å iverksette undersøkelse av forhold som reiser tvil om en sikkerhetsklarert persons sikkerhetsmessige skikkethet kan være vanskelig å trekke. Men som et utgangspunkt må det kunne sies at jo mer undersøkelsene retter seg mot forhold rundt en person – og ikke undersøkelse av konkrete hendelser – vil det tilligge klareringsmyndigheten, dvs NSM i denne saken, å gjennomføre undersøkelsene etter sikkerhetsloven § 24.[22]

Heller ikke EOS-utvalget går nærmere inn på hvilke virkemidler klareringsmyndigheten kan benytte ved gjennomføring av undersøkelser etter sikkerhetsloven § 24. Det må antas at klareringsmyndigheten har den samme adgangen til å innhente personkontrollopplysninger som ved førstegangs- eller reklarering, herunder kontroll opp mot relevante registre, oppgitte referanser, samt gjennomføre nye sikkerhetssamtaler i den hensikt å avklare forholdene.

Dersom klareringsmyndigheten beslutter å tilbakekalle, nedsette eller suspendere en sikkerhetsklarering, skal en begrunnet melding om dette oversendes NSM. I tillegg skal klareringsmyndigheten varsle autorisasjonsansvarlig umiddelbart om at slik beslutning er fattet, jf. bestemmelsens tredje ledd.

Tre forhold medfører etter bestemmelsens fjerde ledd at en persons autorisasjon automatisk bortfaller:

a) når personen fratrer den stilling som autorisasjonen omfatter,
b) når behovet for autorisasjon av andre grunner ikke lenger er til stede, eller
c) når vedkommende ikke lenger har tilstrekkelig sikkerhetsklarering.

I tillegg skal autorisasjonsansvarlig vurdere å tilbakekalle, nedsette eller suspendere klareringen dersom han eller hun får opplysninger som gir grunn til tvil om den autoriserte personens sikkerhetsmessige skikkethet, jf. bestemmelsens femte ledd. Slik avgjørelse skal innberettes til klareringsmyndighet som har klarert vedkommende. Bestemmelsen gir etter sin ordlyd ikke autorisasjonsansvarlig hjemmel til å igangsette nærmere undersøkelser for å avklare forholdet. Det forutsettes da at vedkommendes klarering vurderes av klareringsmyndigheten uten ugrunnet opphold.[23]

Dersom klareringsmyndigheten opprettholder sikkerhetsklareringen, reises spørsmålet om autorisasjonsansvarlig likevel kan opprettholde beslutningen knyttet til vedkommendes autorisasjon. I følge forarbeidene må en eventuell enighet om dette løses gjennom dialog mellom klareringsmyndigheten og autorisasjonsansvarlig. I ytterste konsekvens må saken løses gjennom at den bringes opp på høyere nivå, i siste instans gjennom avgjørelse på regjeringsnivå. I følge forarbeidene viser imidlertid erfaring at slike konflikter ikke inntreffer i praksis.

Det følger av bestemmelsens sjette ledd at NSM fastsetter generell gyldighetstid for sikkerhetsklareringer. I forarbeidene uttrykkes det at en sikkerhetsklarering bør være tidsbegrenset, da det av sikkerhetsmessige hensyn vil være regelmessig behov for å undersøke om det er kommet til nye opplysninger, eller skjedd endringer, som medfører at klarering må revurderes. I personellsikkerhetsforskriften § 4-8 er den generelle gyldighetstiden for klarering satt til fem år. Vernepliktig personell i Forsvaret klareres normalt sett for to år.

---

[22] Dok. 18 S (2009–2010), Årsmelding til Stortinget fra Stortingets kontrollutvalg for etterretnings-, overvåkings- sikkerhetstjeneste (EOS-utvalget), 30.

[23] Ot.prp. nr. 49 (1996–97), 71.

10.2.9 Saksbehandlingsregler

Ved lovendringen i 2006 ble det innført en rekke nye saksbehandlingsregler med sikte på å bedre den enkeltes rettssikkerhet i klareringsprosessen.

Sikkerhetsloven § 25 første ledd slår fast at forvaltningsloven kapittel IV (om saksforberedelse) og V (om vedtaket) ikke gjelder for avgjørelser om sikkerhetsklarering eller autorisasjon.

Klareringsmyndigheten har en *underretningsplikt* etter bestemmelsens andre ledd. Den som har vært vurdert sikkerhetsklarert har rett til å bli gjort kjent med resultatet, og ved en negativ avgjørelse skal klareringsmyndigheten på eget initiativ underrette vedkommende om resultatet og opplyse om klageadgangen. Med *negativ avgjørelse* menes både der klarering nektes, og de tilfeller der klarering gis, men på et lavere nivå enn søkt om.[24] Negative avgjørelser i lovens forstand omfatter også de tilfeller der klareringsmyndigheten treffer avgjørelse om tilbakekallelse, nedsettelse og suspensjon av sikkerhetsklarering etter loven § 24.[25]

Begrunnelse for avgjørelsen skal som hovedregel gis samtidig med underretningen om utfallet av klareringssaken, jf. bestemmelsens tredje ledd. Det kan gjøres *unntak for retten til begrunnelse*, dersom dette vil innebære at det røpes opplysninger som:

a) er av betydning for Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser,
b) er av betydning for kildevern,
c) det av hensyn til vedkommendes helse eller hans forhold til personer som står denne nær, må anses utilrådelig at vedkommende får kjennskap til,
d) angår tekniske innretninger, produksjonsmetoder, forretningsmessige analyser og beregninger og forretningshemmeligheter ellers, når de er av en slik art at andre kan utnytte dem i sin næringsvirksomhet.

Opplysninger etter bokstav a vil typisk være informasjon som er sikkerhetsgradert av utsteder av informasjonen.[26]

I forarbeidene presiseres det at unntaket i bokstav b om kildevern etter omstendighetene også vil kunne bli omfattet av bokstav a, men at det likevel vil kunne være en selvstendig unntakshjemmel.[27] I NSMs veiledning nevnes som eksempel opplysninger fra oppgitte eller supplerende referanser, uttalelser fra tjenestesteder eller arbeidsplasser, samt etterretningsopplysninger fra norske og utenlandske samarbeidende tjenester, og opplysninger fra politiet om pågående etterforskning.

Eksempler på informasjon som kan unntas etter bokstav c er opplysninger om psykisk helse, rusmisbruk eller uttalelser der en nærstående person kommer med nedsettende uttalelser om den som søkes klarert.[28]

Bokstav d samsvarer i hovedsak med forvaltningslovens bestemmelse om taushetsplikt om bedriftshemmeligheter, jf. forvaltningsloven § 13 første ledd nr. 2.

Etter bestemmelsens fjerde ledd skal klareringsmyndigheten i tillegg utarbeide en intern samtidig begrunnelse for den avgjørelse som fattes, hvor alle relevante forhold inngår, inkludert eventuelle forhold som er nevnt i bestemmelsens tredje ledd.

Loven § 25 a gir nærmere regler om vedkommendes *innsynsrett* i sin egen klareringssak. Det fremgår av bestemmelsens første ledd at innsynsretten først inntrer etter at avgjørelse i klareringssaken er fattet. I forarbeidene begrunnes en slik etterfølgende innsynsrett med at innsyn på et tidligere tidspunkt i særlig grad vil kunne påvirke verdien av en sikkerhetssamtale for klareringsmyndigheten. Det legges til grunn at bestemmelsen gir hjemmel for innsyn i det faktum klareringsmyndigheten legger til grunn i referatet fra sikkerhetssamtalen. Innsynsretten gjelder også eventuelle audiovisuelle opptak fra sikkerhetssamtalen.[29]

Unntakene fra innsynsretten i bestemmelsens tredje ledd er harmonisert med de unntak som gjelder i § 25 tredje ledd bokstav a til c. Unntaket for interne dokumenter forutsettes i forarbeidene praktisert på samme måte som tilsvarende unntak i forvaltningsloven.

Bestemmelsens tredje ledd fastslår at den som har krav på innsyn etter anmodning skal gis en kopi av dokumentet. Når det gjelder gjennomsyn av audiovisuelle opptak av sikkerhetssamtalen, skal dette skje ved oppmøte hos den aktuelle klareringsmyndigheten.

Dersom klareringsmyndigheten nekter en person innsyn i sin egen sak etter § 25 tredje ledd

---

[24] Ot.prp. nr. 59 (2004–2005), 32.

[25] Ot.prp. nr. 49 (1996–97), 71.

[26] Veiledning til sikkerhetslovens kapittel 6 og forskrift om personellsikkerhet, 20.

[27] Ot.prp. nr. 59 (2004–2005), 33.

[28] Ibid.

[29] Ibid.

eller § 25 a annet ledd første punktum, har vedkommende *rett til å få oppnevnt en advokat* for å ivareta sine interesser i saken, jf. loven § 25 b annet ledd. Det er et vilkår for oppnevning av advokat at vedkommende har uttømt klageadgangen for innsynssaken, og at klagefristen på selve klareringsavgjørelsen ikke har løpt ut. I følge forarbeidene er det av hensyn til rettssikkerheten tilstrekkelig at retten til advokat gjelder ved førsteinstansbehandlingen. Det er videre presisert i forarbeidene at ordningen kun gjelder for de tilfeller der vedkommende ikke får klarering i samsvar med anmodningen.[30]

Forsvarsdepartementet skal i henhold til bestemmelsens første ledd oppnevne en gruppe advokater for dette formålet, som skal sikkerhetsklareres for tilgang til sikkerhetsgradert informasjon opp til og med STRENGT HEMMELIG.

Den oppnevnte advokaten skal gis tilgang til både de faktiske opplysningene og den begrunnelse som den som vurderes sikkerhetsklarert ikke får, jf. bestemmelsens tredje ledd. Dette gjelder imidlertid ikke for dokumenter som er utarbeidet for den interne saksforberedelsen ved klareringsmyndigheten eller klageinstansen.

Advokaten vil etter bestemmelsens fjerde ledd ha en rådgivende rolle i spørsmålet om hvorvidt vedkommende bør klage på en negativ avgjørelse om sikkerhetsklarering. I forarbeidene presiseres det at advokaten vil ha taushetsplikt overfor egen klient, slik at de opplysningene advokaten får tilgang til etter tredje ledd ikke kan videreformidles til den som skal klareres. Advokatens rolle er også avgrenset slik at han eller hun ikke vil kunne representere vedkommende i en eventuell klagesak.[31]

Loven § 25 c slår i første ledd fast at bestemmelsene i forvaltningsloven kapittel VI om klage på enkeltvedtak gjelder tilsvarende i klareringssaker med mindre annet følger av sikkerhetsloven eller forskrift om personellsikkerhet.

Bestemmelsens andre ledd presiserer at det bare er den personen en avgjørelse retter seg mot, som har klagerett. Videre presiseres hvilke avgjørelser som kan påklages. Både negative avgjørelser, vilkår for sikkerhetsklarering og observasjonstid ved negativ avgjørelse, kan påklages til klageinstansen. Det samme gjelder nektet begrunnelse og avslag på begjæring om innsyn.

Klagen skal i tråd med forvaltningslovens bestemmelser sendes til den som har fattet avgjørelsen i første omgang, jf. bestemmelsens tredje ledd. Nasjonal sikkerhetsmyndighet er klageinstans for avgjørelser som er truffet av andre klareringsmyndigheter. Dersom Nasjonal sikkerhetsmyndighet har behandlet saken i førsteinstans, vil Forsvarsdepartementet være klageinstans.

Klagefristen er i henhold til bestemmelsens fjerde ledd tre uker fra den dag underretning om avgjørelsen som kan påklages, har kommet frem til vedkommende. Dersom det klages på nektet begrunnelse eller avslag på begjæring om innsyn, så avbrytes også klagefristen for selve klareringssaken. Ny klagefrist vil da løpe fra det tidspunkt underretning om avgjørelse vedrørende begrunnelse eller innsyn er kommet frem til vedkommende, eller på annen måte er gjort kjent for denne. I saker der advokat har gjennomgått saken etter § 24 b løper ny klagefrist fra den dag rådet fra advokaten har kommet frem til vedkommende.

Loven § 26 gir Kongen og Nasjonal sikkerhetsmyndighet hjemmel til å gi forskrifter og utfyllende bestemmelser om personellsikkerhet. I første ledd gis Kongen myndighet til å gi forskrift om opprettelse av et sentralt register for klareringsavgjørelser. I medhold av bestemmelsens andre ledd gis Nasjonal sikkerhetsmyndighet myndighet til å fastsette nærmere bestemmelser om personellsikkerhet, herunder sikkerhetsklarering av bestemte kategorier personell, om arkivering, oppbevaring og forsendelse av dokumenter, samt om avholdelse av sikkerhetssamtaler.

10.3 Sektorregelverk

I sektorlovgivningen er det svært få eksempler på krav til klarering, vandelsdokumentasjon eller skikkethetsvurderinger for de som jobber med sikring av objekter og anlegg. Kravene til de som skal jobbe med sikkerhet er i de fleste tilfeller begrenset til krav om kunnskaper og ferdigheter, og i noen grad krav til helse.[32]

De eksemplene man kan finne er på samferdselsområdet.

10.3.1 Luftfartsloven

Personkontroll for personell i luftfarten reguleres i forskrift om sikkerhet i luftfarten.

Ansvarshavende for sikkerhet, deltakere i sikkerhetsutvalg og personell som er teknisk ansvarlig for sikkerhetsutstyr må inneha gyldig sikker-

[30] Ibid.
[31] Ibid.
[32] Herbjørn Andresen, *Kartlegging av sektorlovgivning som regulerer virksomheters tiltak mot tilsiktede hendelser*, Høgskolen i Oslo og Akershus, elektronisk vedlegg 1, 17.

hetsklarering etter sikkerhetsloven kapittel 6, jf. forskriften § 13 første ledd bokstav a. I tillegg må nevnte personell bestå bakgrunnssjekk for id-kort til lufthavn, jf. bestemmelsens bokstav c.

For personell som skal ha tilgang til sikkerhetsbegrensede områder ved norske lufthavner, er det et krav om at disse underlegges en bakgrunnssjekk. Formålet med slik bakgrunnssjekk er å hindre at personer som kan representere en risiko for sikkerheten i luftfarten gis adgang til landingsplasser og luftfartsanlegg, eller godkjennes for sentrale posisjoner i luftfarten for øvrig. Bestemmelsene om bakgrunnssjekk skal også bidra til å sikre allmennhetens tillit til sivil luftfart, jf. forskriften § 37.

Luftfartstilsynet foretar bakgrunnssjekk, jf. forskriften § 38 første ledd. Den gjelder for personellgrupper som:

- skal ha id-kort som gir adgang til norsk lufthavn,
- skal ha id-kort fra norsk flyselskap,
- er utpekt som sikkerhetsgodkjent fraktleverandør som er ansvarlig for stedlig gjennomføring av sikkerhetsprogrammet,
- er utpekt av en kjent avsender for flyfrakt som stedlig ansvarlig for håndhevelse og kontroll med gjennomføringen av sikkerhetskontrollen,
- skal være instruktør,
- skal være fraktkontrollant.

Bestemmelsene om bakgrunnssjekk er basert på Kommisjonsforordning (EU) nr. 185/2010, som fastsetter de detaljerte bestemmelsene for gjennomføring av felles grunnleggende securitystandarder for sivil luftfart i EØS-området. Forordningens punkt 11.1.3 fastsetter hva en bakgrunnssjekk skal inneholde. En bakgrunnssjekk skal:

- fastslå personens identitet på grunnlag av dokumentasjon,
- omfatte strafferegistre i alle bostedsstater de siste fem år,
- omfatte en oversikt over arbeid, utdanning og oppholdssted de siste fem år.

Krav til dokumentasjon av identitet, samt utdannelse og ansettelsesforhold fremgår av forskriften § 39. Søker må fremlegge kopi av gyldig legitimasjon utstedt av offentlig myndighet hvor fødselsnummer og bilde fremgår. Videre må søker opplyse om utdannelse og ansettelsesforhold de siste fem år. Hvis det foreligger udokumenterte perioder på mer enn 28 dager, kan dette etter en helhetsvurdering medføre at søker får avslag på søknaden. Dersom de fremlagte opplysningene gir grunn til å anta at søker kan representere en risiko for sikkerheten i luftfarten, skal søknaden avslås.

Etter forskriften § 40 stilles det krav om at det foretas en vandelskontroll på grunnlag av en uttømmende politiattest. Det er kun politiattester som er utstedt i Norge eller i et annet EØS-land som kan godtas, og attesten skal ikke være eldre enn 90 dager.

Dersom søker innehar gyldig sikkerhetsklarering etter sikkerhetsloven, skal denne anses for å oppfylle krav til vandel etter forskriften. Id-kort skal imidlertid ikke utstedes med lengre gyldighet enn sikkerhetsklareringens varighet. Ny vandelskontroll skal gjennomføres minst hvert femte år.

Forskriften gir i §§ 42-51 detaljerte bestemmelser om gjennomføringen av bakgrunnssjekk, herunder hvilke strafferettslige reaksjoner som skal medføre avslag, karantenetid ved rettskraftige avgjørelser et cetera.

10.3.2 Skipssikkerhetsloven med forskrifter

For å hindre eller beskytte fartøyet mot terrorhandlinger og piratvirksomhet, kan væpnet vakthold tas i bruk etter en risikovurdering og etter konsultasjon med skipsføreren, jf. sikkerhetsforskriften § 20 første ledd.[33] Sikkerhetsforskriften er fastsatt med hjemmel i skipssikkerhetsloven.[34]

Sikkerhetsforskriften stiller i § 20 annet ledd bokstav b nr. 4 krav til personkontroll av en særlig gruppe personell. Væpnede vakter må ha fylt 18 år, kunne identifisere seg samt fremlegge vandelsattest av nyere dato. Dersom vandelsattest ikke er mulig å fremskaffe burde annen lignende bekreftelse eller referanse innhentes.

10.3.3 Jernbaneloven

Jernbaneloven fastsetter i § 3 d nærmere krav til personell med oppgaver knyttet til sikkerheten ved jernbane, samt behandling av opplysninger.[35]

Etter bestemmelsens første ledd første punktum må «fører av rullende materiell og annet per-

---

[33] Forskrift 22. juni 2004 nr. 972 om sikkerhet, pirat- og terrorberedskapstiltak og bruk av maktmidler om bord på skip og flyttbare boreinnretninger (sikkerhetsforskriften).

[34] Lov 16. februar 2007 nr. 9 om skipssikkerhet (skipssikkerhetsloven).

[35] Lov 11. juni 1993 nr. 100 om anlegg og drift av jernbane, herunder sporvei, tunnelbane og forstadsbane m.m. (jernbaneloven).

sonell som skal utføre oppgaver knyttet til sikkerheten ved jernbane […] oppfylle de vilkår som tilsynsmyndigheten fastsetter om kvalifikasjoner, alder, helse, fysisk og psykisk skikkethet, vandel, edruskap, utdanning, opplæring og trening m.m.»

Kravene til kvalifikasjoner, helse, edruskap og opplæring er omfattende og detaljerte i underliggende forskrifter. Det er imidlertid ikke gitt nærmere regler som spesifiserer om, og i så fall i hvilke tilfeller, personkontroll, herunder eventuell vandelskontroll, skal gjennomføres.

10.4 Fremmed rett

10.4.1 NATO

Bestemmelser om beskyttelse av *NATO* sikkerhetsgradert informasjon er gitt i *NATO Security Policy (Council Memorandum, C-M(2002)49),* som sammen med flere understøttende direktiver er bindende for Norge og de andre medlemslandene.

I C-M(2002)49 Enclosure B punkt 11-13 fremgår det at personer kan gis varig tilgang til gradert informasjon etter en vurdering av en persons lojalitet og i hvilken grad man kan stole på vedkommende. For behandling av informasjon som er gradert RESTRICTED er det ikke nødvendig med sikkerhetsklarering, men det skal gis informasjon om hvilket ansvar som tilligger den enkelte. For øvrig vises det til Enclosure C.

Det følger av Enclosure C, punkt 3, at personell som skal ha tilgang til NATO-informasjon sikkerhetsgradert NATO CONFIDENTIAL eller høyere, på forhånd er sikkerhetsklarert for det aktuelle nivå. Det skal foreligge en standard for i hvilken grad man kan stole på personer som skal få tilgang til gradert informasjon, jf. punkt 1. Det er ikke krav til sikkerhetsklarering for NATO RESTRICTED og dermed heller ikke bakgrunnssjekk, jf. punkt 4. Imidlertid er det krav om at kun de som har tjenstlig behov for informasjonen, gis tilgang, jf. punkt 6. Dette gjelder uavhengig av en persons stilling eller rang. Videre er det krav om at alle orienteres om sikkerhetsprosedyrer og hvilket ansvar de har for å beskytte den graderte informasjonen. Nærmere om hvem som har myndighet til å autorisere er ikke regulert i verken Enclosure C eller det tilhørende *Directive on Personnel security* (AC/35-D/2000-REV7).

10.4.2 Sverige

I Sverige skal det etter *säkerhetsskyddslagen* 11 § gjøres en *säkerhetsprövning* av personer som deltar i virksomhet som er av betydning for rikets sikkerhet eller som får tilgang til opplysninger som er viktige for beskyttelsen mot terrorisme.

Boks 10.7 Säkerhetsskyddslagen 17 §

En anställning eller ett annat sådant deltagande i verksamhet som avses i 13 § första stycket skall placeras i säkerhetsklass, om den anställde eller den som annars deltar i verksamheten

1. i stor omfattning får del av uppgifter som omfattas av sekretess och är av synnerlig betydelse för rikets säkerhet (säkerhetsklass 1),
2. i en omfattning som inte är obetydlig får del av sådana uppgifter som avses i 1 (säkerhetsklass 2), eller
3. i övrigt får del av uppgifter som omfattas av sekretess och som är av betydelse för rikets säkerhet, om ett röjande av uppgifterna kan antas medföra men för rikets säkerhet som inte endast är ringa (säkerhetsklass 3).

Det tilligger den enkelte virksomhet som anmoder om personkontroll å fatte avgjørelse om en person skal sikkerhetsklareres. Den enkelte virksomhet skal gjennom en analyse kartlegge hvilke ansettelser som medfører behov for plassering i en *säkerhetsklass*. Ansvaret for sikkerhetsprøvningen tilligger som hovedregel den virksomheten som ansetter personen.

Sikkerhetsprøvning forutsetter ikke plassering i *säkerhetsklass* etter 17 § i *säkerhetsskyddslagen*. Registerkontroll og særskilt personutredning er imidlertid forbeholdt situasjoner der det er tale om en ansettelse eller annen deltakelse som skal plasseres i en sikkerhetsklasse. I tillegg skal det gjennomføres registerkontroll som ledd i sikkerhetsprøvningen for virksomheter som har et særlig beskyttelsesbehov mot terrorhandlinger.

Personer som skal sikkerhetsprøves skal på forhånd samtykke i at registerkontroll og særskilt personutredning foretas, jf. 19 §. Et slikt samtykke skal også anses for å gjelde fornyede kontroller og utredninger så lenge som den kontrollerte skal inneha den aktuelle stillingen.

Etter 7 § 3 skal den enkeltes pålitelighet vurderes ut fra et sikkerhetsmessig perspektiv. I medhold av loven 11 § skal prøvningen klarlegge om personen antas å være lojal mot de interessene

som skal beskyttes, og for øvrig pålitelig ut fra et sikkerhetsmessig perspektiv.

Registerkontroll innebærer at opplysninger fra en rekke nærmere angitte registre innhentes etter forutgående samtykke fra den som skal sikkerhetsprøves. Kun opplysninger som er relevante for vurderingen av den enkeltes pålitelighet, ut fra et sikkerhetsmessig perspektiv, kan utleveres. Bedømmingen av hvilke opplysninger som har slik relevans gjøres av *Säkerhets- og integritetsskyddsnämnden*. Som hovedregel skal den det gjelder få anledning til å uttale seg om opplysninger som fremkommer, før disse utleveres for sikkerhetsprøvning. Dette med unntak av opplysninger som er taushetsbelagte overfor den det gjelder.

En sikkerhetsklassifisert stilling i stat, kommune eller landsting kan, med visse unntak, bare innehas av personer med svensk statsborgerskap, jf. 29 §. Regjeringen kan i særlige tilfeller gjøre unntak fra kravet om svensk statsborgerskap.

I forslaget til ny sikkerhetslov foreslås det blant annet en tilpassing av sikkerhetsklassifisering av stillinger, slik at denne tilsvarer klassifiseringen av sikkerhetsgradert informasjon.[36]

I tillegg foreslås en bestemmelse om at sikkerhetsprøvning skal følges opp i den tiden vedkommende deltar i *säkerhetskänslig* virksomhet. Forslaget er ment å tydeliggjøre at sikkerhetsprøvning er en kontinuerlig prosess, som pågår helt frem til en avsluttende samtale i forbindelse med fratreden fra stillingen.[37] Som en forlengelse av dette, foreslås det også en tydeliggjøring av at det skal skje en løpende registerkontroll opp mot relevante registre så lenge vedkommende deltar i *säkerhetskänslig* virksomhet.[38]

10.4.3 Danmark

Personkontroll reguleres i Danmark av Sikkerhedscirkulæret.[39]

Det følger av *Sikkerhedscirkulæret* § 12 at sikkerhetsgradert informasjon kun må gis til personell som er *sikkerhetsgodkjent* for den aktuelle sikkerhetsgrad. Dette kravet gjelder på alle graderingsnivåer.

Enhver offentlig myndighet er klareringsmyndighet for eget personell og for ansatte i private selskaper som arbeider for den offentlige myndigheten. Sikkerhetsgodkjenningen er avgrenset til den konkrete stilling, og har kun gyldighet for den sikkerhetsgodkjente persons arbeid hos den aktuelle myndighet, jf. cirkulæret § 13 første ledd. Sikkerhetsgodkjenning skal kun gis til personer som gjennom sitt arbeid skal ha tilgang til sikkerhetsgradert informasjon eller der det er nødvendig med hensyn til de funksjoner vedkommende skal ivareta, jf. § 15 første ledd.

Politets Efterretningstjeneste (PET) gjennomfører en sikkerhetsundersøkelse av den enkelte, som grunnlag for myndighetenes sikkerhetsgodkjennelse for egne ansatte, jf. § 13 tredje ledd. PET følger seks spor i sine undersøkelser:[40]

- Personlig informasjon (tilgjengelige offentlige registre)
- Kriminelt (politiets registre)
- Sikkerhet (PETs interne register)
- Sosialt (åpne kilder, sosiale medier etc)
- Økonomisk (skatteopplysninger, kredittregister etc)
- Kompetanse (henvendelse til tidligere arbeidsgivere)

Hvilke registre og kilder PET sjekker opp mot avhenger av hvilket klareringsnivå det bes om. Ettersom PET har direkte tilgang til en rekke av de relevante registrene, er saksbehandlingstiden på sikkerhetsklareringer vesentlig kortere enn i Norge.

Avgjørelse om sikkerhetsgodkjennelse skal treffes på grunnlag av en konkret vurdering basert på alle foreliggende opplysninger om personen og dens nærstående, jf. § 14. Det skal i denne vurderingen særlig legges vekt på personens lojalitet og pålitelighet i forbindelse med håndtering av sikkerhetsgradert informasjon. Nektelse av sikkerhetsgodkjennelse kan påklages til Justisministeriet.[41]

Offentlige myndigheter plikter å ha en ajourført liste over medarbeidere som innehar gyldig sikkerhetsgodkjennelse, herunder opplysninger om klassifikasjonsgrad, utstedelsesdato og gyldighetstid, jf. § 15 andre ledd. Tilgang til sikkerhetsgradert informasjon skal baseres på *need-to-know*-prinsippet, og den enkelte plikter å sikre at uvedkommende ikke får tilgang til slik informasjon, jf. § 16.

Etter sikkerhetsgodkjennelse gjør PET fortløpende kontroller opp mot politiets straffesaksre-

---

36 SOU 2015:25, 539–540.

37 Ibid., 537–538.

38 Ibid., 541–542.

39 Cirkulære om sikkerhedsbeskyttelse af informationer af fælles interesse for landende i NATO eller EU, andre klassificerede informationer samt informationer af sikkerhetsmæssig beskyttelsesinteresse i øvrigt (Sikkerhedscirkulæret) (CIS nr 10338 af 17/12/2014).

40 Informasjon fra utvalgets studiebesøk i Danmark.

41 Ibid.

gistre og egne sikkerhetsregistre. Videre har den enkelte plikt til å opplyse om forhold av betydning for sikkerhetsgodkjennelsen.[42]

10.4.4 Storbritannia

10.4.4.1 Personkontroll

I Storbritannia er det fire forskjellige nivåer for personkontroll, avhengig av den enkeltes behov for tilgang til informasjon og/eller lokaliteter.[43] Formålet med personkontrollen er dels å få bekreftet den aktuelle personens identitet, og dels å gi tilstrekkelig grad av sikkerhet for personens sikkerhetsmessige tillit, integritet og pålitelighet.

Det laveste nivået for personkontroll er *Baseline Personell Security Standard* (PBSS). PBSS omfatter alle statsansatte, herunder midlertidig ansatte og innleid personell. Dette er ikke en sikkerhetsklarering, men en kontroll som omfatter identitetsbekreftelse, statsborgerskap og imigrasjonsstatus, arbeidshistorikk de siste tre år, samt en kontroll av strafferegisteret opp mot ferdigsonede straffer. I tillegg må det redegjøres for eventuelle utenlandsopphold på totalt mer enn seks måneder siste tre år.

I tillegg til PBSS finnes det tre nivåer for sikkerhetsklarering. Det laveste nivået er *Counter Terrorist Check* (CTC). CTC omfatter personell som enten har tilgang til personer som vurderes særlig utsatt for terrorhandlinger, personell som gis tilgang til informasjon eller materiell av verdi for terrorister, eller personell som gis ueskortert tilgang til visse militære, sivile, industrielle eller kommersielle områder som vurderes å ha en forhøyet risiko for terrorhandlinger. En forutsetning for CTC-klarering er at vedkommende har vært gjennom PBSS. Vedkommende må videre fylle ut en detaljert personopplysningsblankett. I tillegg blir det gjort en kontroll opp mot arbeidsgivers registre, strafferegistre for både oppgjorte og ikke-oppgjorte straffbare forhold, samt kontroll av MI5s registre. Dersom det er uavklarte sikkerhetsmessige forhold knyttet til den enkelte, eller hvis sikkerhetstjenesten anbefaler det, kan det også gjennomføres sikkerhetssamtale før avgjørelse fattes. Kontroll av tredjepersoner nevnt i personopplysningsblanketten kan også gjennomføres.

Det skal gjennomføres en *Security Check* (SC) for personell som skal ha, eller gjennom sitt arbeid kan få, tilgang til sikkerhetsgradert informasjon eller andre verdier (*assets*) på nivå UK SECRET eller høyere, eller en internasjonal organisasjon eller fremmed stats informasjon gradert KONFIDENSIELT eller høyere. I tillegg til de forhold som kontrolleres under CTC, skal den enkeltes kreditt- og finansielle forhold kontrolleres opp mot kredittopplysningsregistre. Også for dette nivået kan kontrollen omfatte tredjepersoner.

Det øverste klareringsnivået – *Developed Vetting* (DV) – omfatter personell som skal ha tilgang til sikkerhetsgradert informasjon eller andre verdier (*assets*) på nivå UK TOP SECRET, eller informasjon med tilsvarende gradering fra en internasjonal organisasjon eller fremmed stat. For DV skal den enkelte, i tillegg til ordinær personopplysningsblankett, fylle ut et eget tilleggskjema samt et skjema med økonomisk relaterte spørsmål. I tillegg til de undersøkelser som gjøres for SC, skal det gjennomføres en full revisjon av den enkeltes personlige økonomi, et detaljert intervju med *Investigating Officer*, samt ytterligere undersøkelser og samtaler med oppgitte referanser. Kontrollen for DV omfatter også tredjepersoner.

10.4.4.2 Beslutningsgrunnlag og prosedyrer

Sikkerhetsklarering kan gjennomføres ved rekruttering til en stilling som krever slik klarering, eller for allerede ansatt personell som får endrede arbeidsoppgaver som forutsetter klarering. Ingen er pålagt å underlegge seg en klareringsprosess, men for enkelte typer stillinger vil en gyldig sikkerhetsklarering være en forutsetning.

Beslutninger om sikkerhetsklarering vil alltid bli tatt av et departement eller av politiet. Det overordnede formålet med personkontrollen er å få en forsikring om at den aktuelle personen er skikket til å sikkerhetsklareres, og at vedkommende ikke utgjør en sikkerhetsrisiko, herunder at det er lite sannsynlig at vedkommende vil kunne komme til å misbruke sin tilgang, gi etter for press eller på annen måte bli fristet til å kompromittere sikkerhetsgradert informasjon.

Avgjørelse om klarering skal baseres på en helhetlig vurdering av all informasjon som innhentes gjennom personkontrollen, både positive og negative forhold. Alle disse faktorene skal så vurderes opp mot sikkerhetsmessige krav til den aktuelle stillingen for å påse at vedkommende er sikkerhetsmessig skikket for det aktuelle klareringsnivået. Ved vurderingen av den sikkerhetsmessige betydningen av forhold som avdekkes gjennom personkontrollen, er det forbudt å la personlig eller kulturell forutinntatthet påvirke vurderingen.

---

42 Ibid.

43 Cabinet Office, *HMG Personnel Security Controls*, version 2.0 – April 2014.

Dersom klarering nektes eller tilbakekalles for allerede ansatt personell, plikter klareringsmyndigheten å informere om avgjørelsen. Vedkommende har også krav på begrunnelse for avgjørelsen, med mindre hensynet til nasjonal sikkerhet tilsier at slik begrunnelse ikke kan gis. Vedkommende skal også informeres om klagemulighetene.

For personer som er en del av en rekrutteringsprosess, er det ikke noen plikt til å begrunne hvorfor vedkommende ikke får jobben. Dersom denne avgjørelsen skyldes sikkerhetsmessige forhold, bør vedkommende imidlertid bli informert om dette med mindre hensynet til nasjonal sikkerhet tilsier at slik informasjon ikke kan gis.

10.4.4.3 Personhistorikk

For å ha et grunnlag for å kunne gjennomføre en tilfredsstillende personkontroll, er det krav om at den aktuelle personen har hatt bosted i UK over en tilstrekkelig lang tidsperiode. Avhengig av hvilket klareringsnivå det søkes om vil det være krav om 3 – 10 års personhistorikk. Manglende personhistorikk er ikke nødvendigvis i seg selv et hinder for sikkerhetsklarering. Avgjørelsen skal tas på bakgrunn av den informasjonen som er tilgjengelig på det aktuelle tidspunktet.

10.4.4.4 Klageadgang

Nektelse eller tilbakekalling av sikkerhetsklarering for allerede ansatt personell kan i første omgang påklages til et internt klageorgan. Det interne klageorganet, som består av personell som ikke tidligere har hatt befatning med saken, har myndighet til å overprøve den opprinnelige beslutningen.

Dersom den interne klagerunden ikke fører frem, vil vedkommende ha muligheten til å påklage avgjørelsen til et eksternt klageorgan – *the Security Vetting Appeals Panel*. Det eksterne klageorganet kan behandle klager fra personell som er ansatt i den aktuelle myndigheten eller andre underlagte organisasjoner, samt personell som er ansatt hos en leverandør til disse. Det eksterne klageorganet behandler ikke klager knyttet til avslag på sikkerhetsklareringer i rekrutteringsprosessen, det vil si før vedkommende er ansatt.

Både ansatt personell, og personer i rekrutteringsfasen, kan ta saken inn for arbeidsretten dersom de mener seg utsatt for ulovlig diskriminering.

10.4.4.5 Informasjonsdeling

Informasjon som innhentes som ledd i personkontroll skal oppbevares sikkert og ikke lengre enn nødvendig. Som grunnlag for innhenting av registeropplysninger i klareringssaker, kan relevant informasjon deles med aktører som forestår innhenting, eksempelvis sikkerhetstjenestene og kommersielle tilbydere av kredittsjekk.

Etater som forestår sikkerhetsklarering kan oppbevare resultatene fra personkontrollen for personell som har blitt sikkerhetsklarert, samt personell som har fått avslag på klarering eller fått denne inndratt. Dersom vedkommende skifter arbeidsgiver kan slike opplysninger deles med ny arbeidsgiver, forutsatt at det foreligger krav om sikkerhetsklarering for den nye stillingen.

Resultatene fra personkontrollen kan også benyttes i den videre sikkerhetsmessige oppfølgingen av den enkelte, for eksempel i forbindelse med fornyelse av sikkerhetsklarering eller i forbindelse med periodisk sjekk opp mot registre.

10.4.4.6 Jevnlig og periodisk kontroll

Gyldige sikkerhetsklareringer gjennomgås med jevne mellomrom for å sikre at eventuelle endringer av forutsetningene for klareringene fanges opp. Dette innebærer både at sikkerhetsklarert personell med jevne mellomrom bes om å fylle ut en oppdatert personopplysningsblankett, og at informasjonen som klareringsmyndigheten er i besittelse av blir sjekket opp mot oppdaterte registre. En slik gjennomgang kan også gjennomføres dersom det innrapporteres endringer i forutsetningene, eller slike endringer blir kjent for klareringsmyndigheten på annen måte.

10.5 Utvalgte tema

10.5.1 Innledning

Personellsikkerhet er det fagområdet innenfor sikkerhetsloven det knytter seg mest praksis til. På årlig basis sikkerhetsklareres og reklareres i overkant av 30 000 personer for stillinger som krever tilgang til sikkerhetsgradert informasjon. I tillegg er det en rekke klagesaker knyttet til personer som får avslag på anmodningen om sikkerhetsklarering, eller blir klarert for et lavere nivå enn det er søkt om.

Denne omfattende praksisen gjør også at mange av de virksomhetene som er underlagt loven, har oppfatninger om hvordan regelverket

fungerer i praksis og hvilke forhold det knytter seg størst utfordringer til.

Utvalget har gjennom sitt arbeid fått tilbakemeldinger om spesielt viktige forhold fra en rekke sentrale aktører, både i form av skriftlige innspill og gjennom møter utvalget har hatt. Noen av de forholdene som har blitt påpekt overfor utvalget er knyttet til hvordan regelverket praktiseres i dag, i større grad enn hvordan regelverket er utformet. Noen forhold er imidlertid av mer lovgivningsmessig art.

10.5.2 Utenlandsk statsborgerskap og tilknytning til andre nasjoner

Norge har de senere år endret seg på det demografiske området. Migrasjonsmønstrene endres, og samfunn som frem til nylig ble sett på som relativt homogene, fremstår i stadig større grad som mangfoldige, og ofte med familiebånd og/eller utdanningsløp på tvers av landegrenser. Integrering er både et samfunnspolitisk mål og et virkemiddel. Større mangfold i forvaltningen er også et uttalt politisk ønske.

I dag har både forvaltningen og privat virksomhet nye muligheter for rekruttering av personer med verdifull kompetanse om andre land, kulturer og språk. Ikke minst er dette viktig for utenrikstjenesten, hvis oppgaveløsning og analyse forutsetter kultur- og samfunnsforståelse, geopolitisk kompetanse og språkkunnskaper, som ofte oppnås gjennom tjenestegjøring eller studier i andre land.

Tradisjonelle norske næringer og virksomheter får utenlandske eiere, relokaliseres og endrer sammensetningen av personell, uavhengig av om virksomhetens hovedkontor er plassert i Norge. For blant annet den norske utenrikstjenesten er det av vesentlig betydning både å kunne representere bredden av mangfoldet i Norge og å kunne nyttiggjøre seg den unike kompetansen denne type personell har fra samfunn og kulturer, særlig de som i stor grad skiller seg fra det vi har i Norge i dag.

Disse trendene medfører at nye personellgrupper har behov for tilgang til sensitiv, og i enkelte tilfeller sikkerhetsgradert, informasjon både innenfor privat og offentlig sektor. Statistikk fra Nasjonal sikkerhetsmyndighet for perioden 2010–2012 viser at det behandles årlig ca. 2400–3200 saker hvor hoved- eller biperson har, eller har hatt, et utenlandsk statsborgerskap. Dette inkluderer også doble statsborgerskap.

Samtidig kan denne utviklingen også skape noen nye sikkerhetsmessige sårbarheter. Lojalitets- og tilknytningsforholdene hos ansatte blir stadig mer komplekse, noe som vanskeliggjør de vurderingene som klareringsmyndighetene må gjøre i klareringssaker hvor vedkommende er av utenlandsk opprinnelse eller på annen måte har tilknytning til en annen stat. Den økende grad av internasjonalisering fører også til at konflikter i andre deler av verden potensielt også kan få store konsekvenser nasjonalt, for eksempel gjennom radikalisering og fremmedkrigere, og en økt terrortrussel.[44]

I PSTs trusselvurdering for 2016, er PSTs vurdering at utenlandske etterretningstjenester vil fortsette sitt arbeid i og mot Norge. Deres mål er å få tilgang til sensitiv og skjermingsverdig informasjon, påvirke politiske, økonomiske og forvaltningsmessige beslutninger og undersøke muligheter for å kunne sabotere kritisk infrastruktur ved en eventuell fremtidig konflikt. Stadig flere borgere med opprinnelse fra stater som Norge ikke har et sikkerhetsmessig samarbeid med, arbeider i dag innenfor sektorer med tilgang til sensitiv og skjermingsverdig informasjon, for eksempel nasjonale datasystemer. PST opplyser at de har flere rapporteringer på at slike borgere blir utsatt for trusler og press om å inngå et samarbeid med hjemlandets sikkerhets- og etterretningstjenester. I den grad fremmede etterretningstjenester oppnår et slik samarbeid med personer på innsiden, vurderes dette å være en svært effektiv etterretningsmetode med et stort skadepotensial for Norge.[45]

10.5.3 Mangelfull personhistorikk

Enkelte personellkategorier, særlig i utenrikstjenesten og Forsvaret, har en tjeneste som innebærer kortere eller lengre stasjonering utenlands. Mange utenriksstasjoner, som ofte er store stasjoner med bistandsporteføljer, er lokalisert i land Norge ikke har et sikkerhetsmessig samarbeid med.

I lys av tjenestens natur og at mange ansatte har langvarige opphold i utlandet, er det et betydelig antall ansatte i norsk utenrikstjeneste som har en utenlandsk ektefelle. Utenriksdepartementet anslår at opp mot 30 % av deres personell har en ektefelle eller partner som enten har eller har hatt utenlandsk statsborgerskap.

I henhold til loven § 20 første ledd bokstav j, er manglende mulighet for å gjennomføre en tilfredsstillende personkontroll et forhold som kan tilleg-

[44] NSM, *Sikkerhetsfaglig råd,* 2015, 13.
[45] PST, *Trusselvurdering*, 2016.

ges betydning ved vurderingen av den enkeltes sikkerhetsmessige skikkethet. For personell som eksempelvis har tjenestegjort ved en utenriksstasjon i et land Norge ikke har sikkerhetsmessig samarbeid med, vil klareringsmyndigheten ikke kunne innhente opplysninger fra samarbeidende tjeneste i dette landet. Også for medfølgende til utsendt personell kan kravet til observasjonstid/personhistorikk skape utfordringer dersom vedkommende har, eller skal søke om, sikkerhetsklarering.

I personellsikkerhetsforskriften § 3-6 er det slått fast som hovedregel at sikkerhetsmessig relevant informasjon for de siste 10 år om personer som inngår i personkontrollen må være tilgjengelig for å kunne gjennomføre en tilfredsstillende kontroll. Etter bestemmelsens andre ledd kan imidlertid sikkerhetsklarering gis etter en individuell helhetsvurdering, selv om kravet til observasjonstid ikke er oppfylt. Klareringsmyndigheten skal i denne vurderingen legge vekt på om mangel på observasjonstid skyldes kortvarige avbrudd, tjeneste for den norske stat eller humanitære organisasjoner, lav alder eller forhold av liten betydning for sikkerhetsmessig skikkethet. Kravet til personhistorikk er ytterligere utdypet i sikkerhetsgraderte rundskriv utgitt av NSM.

10.5.4 Tverrsektoriell hjemmel for bakgrunnskontroll

Det er i dag ulike ordninger for bakgrunnskontroll av personell som innehar, eller skal inneha tilgang til informasjon og/eller områder av sensitiv karakter. Som redegjort for under kapittel 10.3, synes regelverk i de ulike sektorene i liten grad å gi hjemmel for å gjennomføre slik kontroll.

Forsvarets forskningsinstitutt (FFI) skriver i sin utredning til utvalget at:

> Utro tjenere på innsiden av barrierer kan påføre anlegget, øvrig personell og nasjonen store utfordringer ved tradisjonelle terrorhandlinger, eksempelvis bruk av eksplosiver. Samfunnskonsekvensen av en slik terrorhandling kan være meget stor, ikke minst økonomisk. Personell med tilgang til fysiske eller elektroniske komponenter innen kritisk infrastruktur bør derfor klareres for tilgang. Ved hendelser eller trussel om hendelser, vil den nasjonale sikkerhetsmyndigheten ha behov for nært samarbeid med berørt bransje, hvilket ofte involverer graderte opplysninger. Manglende sikkerhetsklarering vil hemme eller hindre et slikt samarbeid.
>
> Rutiner og ordninger for klarering av personell tilknyttet kritisk infrastruktur bør gjennomgås. Det er viktig å påpeke at dette ikke må påføre tilsynsmyndigheter og selskaper en uhensiktsmessig belastning. Det anbefales at et tverrsektorielt organ gjennomfører personklarering etter anmodning fra departementene, og at denne klareringen ikke bør være mer omfattende enn det den enkeltes stillingskategori krever.[46]

FFI anbefaler på denne bakgrunn at:

> Det bør pålegges bakgrunnssjekk av personell som er ansatt, eller har tilgang til objekter og/eller systemer knyttet til kritiske samfunnsfunksjoner. […] Klareringen bør gjennomføres etter samme kriterier for alle sektorer, og utføres av sentral klareringsmyndighet. Klarering bør skje for to hovedkategorier personell i) personell med tilgang til sikkerhetsgradert eller sensitiv informasjon (sikkerhetsklarering), og ii) personell med adgang til anleggene, men uten behov for tilgang til sensitiv informasjon (adgangsklarering).[47]

I følge NSMs sikkerhetsfaglige råd benyttes sikkerhetsklareringsinstituttet etter sikkerhetsloven, i mangel på andre muligheter til å få gjennomført en tilfredsstillende bakgrunnskontroll, også overfor personell som verken skal ha, eller vil kunne få, tilgang til sikkerhetsgradert informasjon eller skjermingsverdige objekter. Dette kan igjen føre til lengre saksbehandlingstid for personell som innehar arbeidsoppgaver hvor sikkerhetsklarering er et absolutt krav. I tillegg medfører dette at personell blir utsatt for et større inngrep, enn hva som er strengt nødvendig.

NSM har på denne bakgrunn anbefalt at det utredes en ny tverrsektoriell hjemmel og ordning for bakgrunnskontroll av personell med sikte på å ivareta legitime behov som vandelsattest ikke dekker eller alene er utilstrekkelig for.[48]

Justis- og beredskapsdepartementet har i samarbeid med Samferdselsdepartementet sett nærmere på behovet for å bedre kontroll av de personer som får tilgang til sikkerhetsbegrensede områder på flyplasser.

---

[46] Forsvarets forskningsinstitutt, Vurdering av forebyggende sikkerhet innen kraft, petroleum og luftfart, FFI-rapport 00702 (Kjeller: Forsvarets forskningsinstitutt 2016), elektronisk vedlegg nr. 3, 59.

[47] Ibid.

[48] NSM, *Sikkerhetsfaglig råd*, 2015, tiltak 55.

Boks 10.8 Personkontroll i luftfartssektoren

I februar 2014 nedsatte Justis- og beredskapsdepartementet og Samferdselsdepartementet en arbeidsgruppe bestående av de to departementene, Politidirektoratet (POD), Politiets sikkerhetstjeneste (PST), Nasjonal sikkerhetsmyndighet (NSM) og Luftfartstilsynet, for å se nærmere på behovet for å utvide bakgrunnssjekken av enkelte grupper personell.

Arbeidsgruppen anbefalte at flere elementer burde inngå i bakgrunnssjekken, inkludert en sjekk opp mot PSTs registre. Arbeidsgruppen anbefalte også at man burde kunne undersøke, og legge vekt på opplysninger om søkerens økonomi, helse og rusmisbruk i den grad det anses relevant. I visse tilfeller vil det kunne være behov for å bruke sikkerhetsgradert informasjon fra PST i saksbehandlingen.

På bakgrunn av arbeidsgrupperapporten skisserte Samferdselsdepartementet tre ulike alternativer:

1. Nullalternativet, det vil si å fortsette med dagens løsning med bakgrunnssjekk hvert femte år på bakgrunn av blant annet en uttømmende politiattest.
2. Gå videre med arbeidsgruppens forslag om å utvide informasjonsgrunnlaget for bakgrunnssjekken.
3. Etablere en enklere form for sikkerhetsklarering for personer som skal ha tilgang til områder eller objekter som er risikoutsatt.

Justis- og beredskapsdepartementet har overfor utvalget meddelt at det antakelig er flere sektorer enn luftfarten som kan ha behov for bedre kontroll av personer som får tilgang til områder innenfor kritisk infrastruktur eller kritiske samfunnsfunksjoner. Departementet har på denne bakgrunn anført at det er lite hensiktsmessig med en sektorbasert tilnærming til problemstillingen.

Justis- og beredskapsdepartementet har bedt utvalget vurdere hvorvidt det er behov for bedre kontroll av personer som skal ha tilgang til sperrede områder innenfor kritisk infrastruktur og kritiske samfunnsfunksjoner. Dette for å sikre at personene ikke utgjør en sikkerhetsrisiko. Departementet viser i sitt innspill til at de er kjent med at det i Storbritannia gjennomføres en såkalt *Counter Terrorist Check* for personer som skal ha tilgang til områder eller objekter som er risikoutsatt i terrorsammenheng. En tilsvarende ordning vil ifølge departementet kunne dekke behovet for en bedre og mer målrettet kontroll, med tilgang til et bredere informasjonsgrunnlag. Det vil også kunne sikre en løpende kontroll, og muligheten til å frata tilgang dersom det oppstår grunn til bekymring i godkjenningsperioden.

Forsvarsdepartementet har også i et skriftlig innspill bedt utvalget om å vurdere hensiktsmessigheten av og behovet for en forenklet sikkerhetserklæring, jf. henvendelsen fra Justis- og beredskapsdepartementet om *Counter Terrorist Check*.[49]

[49] E-post fra Forsvarsdepartementet til utvalget, «Henvendelse fra FD til sikkerhetsutvalget», 23.05.2016.

10.5.5 Digitalisert overføring av registeropplysninger

Innhenting av informasjon om personell som skal sikkerhetsklareres skjer i dag fra mange ulike registre. Sikkerhetsloven § 20 femte ledd første punktum gir Kongen myndighet til å fastsette hvilke registre som er relevante for personkontroll. Med hjemmel i denne bestemmelsen er det i personellsikkerhetsforskriften § 3-4 første ledd fastsatt hvilke registre NSM kan kreve å få utlevert opplysninger fra.

Det følger videre av forskriften § 3-4 fjerde ledd at registereier plikter å utlevere opplysningene uten unødig opphold, og at NSM kan avtale med den enkelte registereier hvordan utlevering skal skje.

Det er i praksis stor variasjon med tanke på hvordan den enkelte registereier har innrettet seg for å kunne utlevere informasjon til NSM i personkontrolløyemed. Prosessene er til dels manuelle og tidkrevende, noe som også får betydning for saksbehandlingstiden for klareringssaker generelt.

Lang saksbehandlingstid kan ha mange negative konsekvenser. Personell som ikke kan benyttes av arbeids- og oppdragsgivere grunnet manglende sikkerhetsklarering, kan utgjøre en økonomisk kostnad ved at den enkelte virksomhet i

Boks 10.9 Dagens system for innhenting av personkontrollopplysninger:

Nasjonal sikkerhetsmyndighet (NSM) har overfor utvalget meddelt at informasjonsinnhentingen i personkontrollprosessen er arbeidskrevende som følge av manuelle prosesser både hos NSM og hos de enkelte kildene.

NSM opplyser at det er stor variasjon mellom de ulike kildene. Enkelte tilbyr web-grensesnitt som gjør at NSM kan kjøre spørringer i større volum mot registeret fra egne lokaler. Dette gir svar mer eller mindre umiddelbart, og medfører at NSM selv kan kjøre spørringer på en enkel måte, og så ofte det er behov. Dette gir også stor forutsigbarhet.

For en del andre kilder er innhentingen basert på manuelle prosesser, hvor det fysisk må transporteres en spørrefil med kurér til registereier (eller den som på vegne av registereier utleverer). Spørringen fra NSM må deretter lastes inn og svarfil sendes tilbake med kurér påfølgende dag.

For å effektivisere innhentingen er det fra NSMs side ønskelig å kunne kjøre spørring mot alle kilder fra NSMs lokaler. Dette vil kunne bidra til større forutsigbarhet i forhold til leveranser, samt at kilderesultatene i prinsippet kan innhentes samme dag som forespørselen kommer.

Kilde: NSM.

ytterste konsekvens må leie inn annet og allerede sikkerhetsklarert personell for å utføre de aktuelle arbeidsoppgavene. Saksbehandlingstiden kan også få innvirkning på konkurranseevne. Det er også en personlig belastning for den enkelte at klareringssaken trekker ut i tid, med den påfølgende usikkerheten dette skaper.

NSM har i sitt sikkerhetsfaglige råd foreslått en lovfesting av at NSM som hovedregel skal kunne kreve automatisert innhenting av opplysninger fra de aktuelle kilderegistrene.[50] I utvalgets dialog med NSM har utvalget forstått at det med *automatisert kildeinnhenting* primært menes *digitalisert overføring av registeropplysninger*, i motsetning til de manuelle arbeidsprosessene beskrevet over. Utvalget har lagt denne forståelsen til grunn.

10.5.6 Personkontroll

Personkontroll opp mot aktuelle registre gir et øyeblikksbilde. En sikkerhetsklarering er normalt gyldig i 5 år, jf. personellsikkerhetsforskriften § 4-8 første ledd. Før utløpet av klareringens gyldighetstid må autorisasjonsansvarlig anmode om at vedkommende reklareres. I en reklareringssak vil NSM innhente oppdaterte opplysninger fra de aktuelle registrene, og eventuelle nye sårbarheter som fremgår av registeropplysningene til den enkelte vil kunne avdekkes.

Det foreligger i dag ingen hjemmel for klareringsmyndigheten til å foreta regelmessig kontroll av relevante registre, i den hensikt å avdekke hvorvidt det har skjedd endringer av betydning for den enkeltes sikkerhetsmessige skikkethet. NSM har i sitt sikkerhetsfaglige råd uttrykt at det i flere innsidesaker i forkant har vært tegn på at vedkommende har vært eller var i ferd med å bli en utro tjener.[51]

Sikkerhetsklarert og autorisert personell plikter å holde autorisasjonsansvarlig orientert om forhold som antas å kunne være av betydning for vedkommendes sikkerhetsmessige skikkethet, jf. sikkerhetsloven § 24 første ledd. Dersom det imidlertid er tale om en utro tjener, vil plikten til å opplyse om relevante forhold trolig brytes.

NSM har på denne bakgrunn anbefalt at klareringsmyndigheten gis hjemmel til å gjennomføre regelmessig kildekontroll i klareringens gyldighetstid.[52] Forsvarsdepartementet har i et innspill til utvalget også bedt utvalget om å vurdere muligheten for denne typen regelmessig kildekontroll.[53]

Både Danmark og Storbritannia har klareringsregimer som legger til rette for at klareringsmyndigheten kan foreta jevnlige kontroller opp mot relevante registre. I Danmark har PET mulighet til å legge inn en såkalt KR-sperring i systemet, som gjør at PET får varsel dersom det inntrer forhold som kan ha betydning for vurderingen av den enkeltes sikkerhetsmessige skikkethet.

I Sverige er det foreslått en eksplisitt hjemmel om at sikkerhetsprøvningen skal følges opp så

[50] NSM, *Sikkerhetsfaglig råd*, 2015, tiltak 53.

[51] NSM, *Sikkerhetsfaglig råd*, 2015, 29.

[52] NSM, *Sikkerhetsfaglig råd*, 2015, tiltak 53.

[53] E-post fra Forsvarsdepartementet til utvalget, 23.05.2016.

lenge den sikkerhetssensitive virksomheten pågår.[54] Formålet med dette forslaget har vært å tydeliggjøre at sikkerhetsprøvning er en kontinuerlig prosess. Kravet til oppfølging innebærer blant annet at opplysningene fra den opprinnelige sikkerhetsprøvningen skal holdes oppdatert. Det er videre foreslått at det skal skje en løpende kontroll av relevante registre så lenge sikkerhetssensitiv virksomhet pågår (forslag 7 § annet ledd).

10.5.7 Informasjonsdeling

Opplysninger som er gitt til klareringsmyndigheten, og som innhentes gjennom personkontroll opp mot relevante registre, er underlagt et strengt krav til formålsbestemthet. Det følger av sikkerhetsloven § 20 sjette ledd at opplysninger som er samlet inn som ledd i personkontrollen ikke kan eller skal benyttes til andre formål enn vurdering av sikkerhetsklarering. Unntak fra dette kan kun gjøres i de tilfeller det anses påkrevet å meddele slike opplysninger til autorisasjonsansvarlig av hensyn til den sikkerhetsmessige ledelse og kontroll av vedkommende. Kravet til formålsbestemthet er ikke begrunnet i forarbeidene til sikkerhetsloven ut over at dette burde lovfestes.

NSM påpeker i sitt sikkerhetsfaglige råd at risikoen for innsidere/utro tjenere har blitt mer kompleks, og at sikkerhetsklarert personell har blitt mer eksponert for trusselaktører med både evne og vilje til å utnytte sårbarheter. I følge NSM tas det i dag, enten bevisst eller ubevisst, større risiko enn tidligere ved at det klareres og autoriseres flere personer som kan ha lojaliteter eller sårbarheter som kan utnyttes.

Dagens begrensninger i regelverket for deling av informasjon som innhentes som ledd i personkontrollen, vanskeliggjør ifølge NSM muligheten for å kunne utveksle informasjon med PST og eventuelle andre relevante aktører, om enkeltsaker. Dette medfører blant annet at PST ikke vil ha tilstrekkelig evne til å gjøre målrettet oppfølging av den økte restrisikoen som oppstår ved at man tar større risiko i klarerings- og autoriseringsprosessen enn tidligere. Etter NSMs oppfatning, gjør denne situasjonen at det må tas stilling til hvor mye usikkerhet samfunnet aksepterer.

NSM har anbefalt at det bør fremmes forslag om endring av sikkerhetsloven § 20 sjette ledd, slik at NSM kan gi noe relevant informasjon fra klareringssaker til PST for at PST skal kunne ivareta sitt ansvar for å forebygge og motvirke trusler mot rikets sikkerhet eller andre grunnleggende nasjonale interesser.[55]

Justis- og beredskapsdepartementet har i et brev til utvalget uttrykt bekymring for at personer med bakgrunn fra eller tilknytning til stater som driver ulovlig etterretningsvirksomhet mot Norge eller norske interesser, har tilgang til informasjon som disse statene ikke bør få tilgang til. Behovet for informasjonsutveksling mellom PST og NSM har også blitt kommunisert til departementet fra begge disse myndighetene.[56] Departementet støtter på denne bakgrunn NSMs forslag om endring av sikkerhetsloven § 20 sjette ledd.

Formålet med en slik informasjonsutveksling vil være å forebygge at personer som er autorisert og klarert for sikkerhetsgradert informasjon, formidler informasjon til skade for grunnleggende nasjonale interesser.

PST skal i henhold til politiloven § 17 b blant annet forebygge og etterforske overtredelser av straffeloven kapittel 17 Vern av Norges selvstendighet og andre grunnleggende nasjonale interesser og overtredelser av sikkerhetsloven. En del av PSTs samfunnsoppdrag er å forebygge og motvirke trusler fra utro tjenere. For å kunne gjøre dette på en tilfredsstillende måte, er PST avhengig av å ha kunnskap om hvem som sikkerhetsklareres og hvilke stillinger disse til enhver tid har. Etter dagens sikkerhetslov foreligger det ikke hjemmel for å kunne dele slik informasjon til PST fra NSM og de enkelte klareringsmyndighetene.

I tillegg skal PST utarbeide trusselvurderinger til bruk for politiske myndigheter, jf. politiloven § 17 c nr. 1, og PST har behov for å kunne sammenstille informasjon for å kunne se og analysere trender og utviklingstrekk. Eksempelvis kan det være slik at selv om den enkelte klarering av personer for enkeltland ikke er bekymringsfull i seg selv, kan summen av enkeltpersoner i bestemte posisjoner med tilknytning til land av bekymring, gi grunnlag for ulike typer forebyggende tiltak innenfor rammene av gjeldende rettsgrunnlag.

En hjemmel for å kunne dele informasjon som fremkommer under personkontrollen og informasjon om hvem som blir klarert, og for hvilke stillinger, med PST, vil medføre et inngrep i den enkeltes personvern. I henhold til prinsippet om formålsbestemthet skal personopplysninger kun samles inn for bestemte formål, og skal i utgangspunktet kun behandles i samsvar med det formålet de i utgangspunktet ble samlet inn for. Behand-

[54] SOU 2015:25.

[55] NSM, *Sikkerhetsfaglig råd*, 2015, tiltak 57.

[56] Brev fra Justis- og beredskapsdepartementet til utvalget, 16.06.2016, gradert KONFIDENSIELT.

ling av opplysninger til andre formål enn det de ble samlet inn for, krever et selvstendig rettsgrunnlag.

10.6 Utvalgets vurderinger

Personellsikkerhet er et sentralt virkemiddel for å kunne forebygge, og eventuelt avdekke, at utro tjenere får tilgang til informasjon eller områder hvor skadepotensialet er stort.

Dette er også den delen av forebyggende sikkerhet som i størst grad gjør inngrep i den enkelte ansattes personvern. I saksbehandlingen av klareringssaker innhentes det til dels meget sensitive opplysninger om den personen som det søkes om klarering for, og det må stilles strenge krav til hvordan denne informasjonen behandles.

Utvalget har som gjennomgående prinsipp at forslag som innebærer inngrep i den enkeltes rettsikkerhet og personvern, skal være godt begrunnet, forholdsmessige og ha en sikkerhetsmessig effekt som overstiger personvernulempene.

Personellsikkerhet må være strengt regulert, både av hensyn til de krav legalitetsprinsippet stiller til klare hjemmelsgrunnlag og kravene til tilfredsstillende rettssikkerhetsgarantier der det gjøres inngrep i personvernet. Regelverket for personellsikkerhet har vært gjenstand for en grundig revisjon i 2006, hvor hensynet til å sikre den enkeltes rettssikkerhet var førende for revisjonsarbeidet. Utvalgets syn er at de saksbehandlingsreglene som er regulert i dagens sikkerhetslov inneholder de nødvendige rettssikkerhetsgarantiene for å sikre at den enkeltes rettigheter blir ivaretatt gjennom klareringsprosessen. Utvalget foreslår derfor å videreføre disse saksbehandlingsreglene relativt uendret.

Utvalget er videre opptatt av hvilke forhold som bør reguleres i et sektorovergripende regelverk, og hvilke som kan overlates til de enkelte samfunnssektorenes eget regelverk. Som et generelt utgangspunkt mener utvalget at personellsikkerhet fremdeles bør reguleres i et sektorovergripende regelverk. En slik tilnærming vil bidra til å sikre et enhetlig sikkerhetsnivå på tvers av samfunnssektorene, samtidig som det sikrer likebehandling av ansatte i stillinger som krever klarering – uavhengig av hvilken samfunnssektor de arbeider innenfor. At en klarering etter sikkerhetsloven som utgangspunkt ikke er knyttet til en konkret stilling, og at utvalget heller ikke foreslår at dette endres, taler også for å regulere personellsikkerhet i en sektorovergripende lov.

Et annet sentralt prinsipp for utvalgets forslag er å legge til rette for økt effektivitet i saksbehandlingen. Utvalget er kjent med at saksbehandlingstiden i klareringssaker er lang, noe EOS-utvalget også har påpekt i sine årsrapporter de senere år. EOS-utvalget påpekte i sin årsmelding for 2015 at saksbehandlingstiden i mange saker er så lang at den medfører en uforholdsmessig inngripen i enkeltpersoners liv fra myndighetenes side. Utvalget legger til grunn for lovforslaget at reguleringen skal bidra til en effektivisering av saksbehandlingen i klareringssaker.

10.6.1 Generelle betraktninger

På generelt grunnlag mener utvalget at dagens regelverk for personellsikkerhet i hovedsak klarer å balansere avveiningen mellom sikkerhetsmessige hensyn på den ene siden og hensynet til den enkeltes rettsikkerhet og personvern på den andre. Regelverket på lovs nivå har en fleksibel og dynamisk tilnærming, der klareringssaker skal avgjøres på bakgrunn av en konkret helhetsvurdering. Dette gir mulighet til å vurdere den enkelte sak individuelt ut fra de særegne hensyn som gjør seg gjeldende. En del av de utfordringene som er identifisert skyldes slik utvalget ser det, hvordan regelverket praktiseres. Den individuelle og konkrete helhetsvurderingen lovgivningen legger opp til, er i enkelte veiledninger og rundskriv erstattet med en mer skjematisk tilnærming til hvordan klareringssaker skal avgjøres. Utvalget har samtidig forståelse for at en slik praksis har utviklet seg, særlig sett hen til det høye antall klareringsmyndigheter som finnes, og hvor noen klareringsmyndigheter har et meget lavt antall klareringssaker på årlig basis. Dette, kombinert med at klareringssakene blir stadig mer komplekse, gjør det vanskelig å opprettholde den nødvendige kompetansen.

Utvalget støtter derfor den vedtatte endringen av klareringsmyndighetsstrukturen. En samling av kompetansen i to klareringsmyndigheter er slik utvalget ser det, et viktig og riktig grep. Utvalgets forslag til endringer av personellsikkerhetsregelverket må også sees i lys av denne vedtatte reduksjonen av klareringsmyndighetsstrukturen. Et avgjørende premiss for at utvalgets forslag skal få den intenderte effekt, er robuste og kompetente klareringsmyndigheter som har de nødvendige forutsetninger for å kunne gjøre en helhetlig og individuell vurdering i den enkelte sak.

Utvalget har i lovforslaget foreslått endringer av både materiell og strukturell art. Forslagene til

strukturelle endringer er ment å innebære materielle endringer fra dagens rettstilstand.

For å gjøre lovens kapittel om personellsikkerhet mer oversiktlig, har utvalget foreslått å samle bestemmelsene om autorisasjon og autorisasjonsansvarliges plikter i egne bestemmelser. Tilsvarende er foreslått for klarering og klareringsmyndighetenes plikter.

Utvalget foreslår videre å fjerne opplistingen av relevante forhold klareringsmyndighetene kan legge vekt på ved vurderingen av den enkeltes sikkerhetsmessige skikkethet (dagens lovs § 21 første ledd bokstav a til l). Opplistingen i dagens lov er etter utvalgets oppfatning for detaljert i en overordnet lov. Det sentrale vurderingskriteriet etter bestemmelsen er om vedkommende ut fra en konkret helhetsvurdering er sikkerhetsmessig skikket for tilgang til gradert informasjon eller skjermingsverdige objekter/infrastruktur. Vurderingen er avgrenset til de forhold som er relevante for å vurdere vedkommendes pålitelighet, lojalitet og sunne dømmekraft. For øvrig vil det generelle forvaltningsrettslige forbudet mot å ta utenforliggende hensyn, også gjelde for klareringsmyndighetens behandling av klareringssaker. Listen over forhold som kan tillegges vekt bør slik utvalget ser det i stedet legges på forskriftsnivå. En forskriftsregulering av slike detaljerte opplistinger vil også gjøre regelverket mer dynamisk og lettere å endre ved behov.

Utvalget foreslår at bestemmelsen om bruk av vilkår for klarering skilles ut som en egen bestemmelse og at det presiseres at dette også gir hjemmel for å kunne klarere en person for en konkret stilling. Muligheten for bruk av stillingsklarering følger i dag av forarbeidene til sikkerhetsloven. Utvalget mener at bruk av vilkår eller stillingsklarering i gitte tilfeller kan være viktige sårbarhetsreduserende tiltak, som bør brukes aktivt der alternativet vil være å gi avslag på klareringsanmodningen. Forslaget innebærer således ingen materiell endring av rettstilstanden, men en fremheving av muligheten til å kunne gjøre konkrete tilpasninger ut fra den sikkerhetsmessige situasjonen.

Den plikt som autorisert og klarert personell har til å varsle om forhold av betydning, er også foreslått skilt ut i en egen bestemmelse.

10.6.2 Utenlandske statsborgere og tilknytning til andre nasjoner

Norge har opplevd større demografiske endringer siden lovens ikrafttredelse. Som en konsekvens av dette ble det foretatt en viss oppmyking av sikkerhetslovens regulering av adgangen til å sikkerhetsklarere utenlandske statsborgere i 2006.

Utvalget mener det er viktig at det mangfoldige Norge også gjenspeiles i virksomheter som er av kritisk betydning for grunnleggende nasjonale funksjoner. Personer som har tilknytning til andre nasjoner besitter kompetanse om andre land, kulturer og språk, som er verdifull for en rekke virksomheter. Samtidig mener utvalget at en slik tilknytning potensielt også kan medføre en økt sikkerhetsmessig sårbarhet. PSTs trusselvurderinger fremhever utenlandske etterretningstjenesters mål om å få tilgang til sensitiv informasjon, blant annet for å undersøke mulighetene for å kunne sabotere kritisk infrastruktur ved en eventuell fremtidig konflikt. Tilknytningsforholdet til en nasjon med slike målsettinger vil kunne sette personer i nøkkelstillinger under press.

Utvalget har vurdert hvorvidt dagens regelverk er for restriktivt med tanke på klarering av utenlandske statsborgere eller norske statsborgere med tilknytning til andre nasjoner. I begge tilfeller legger lovens system opp til at avgjørelser om klarering skal baseres på en konkret helhetsvurdering der vedkommendes tilknytning til en annen nasjon, er et av flere relevante momenter i denne vurderingen. Tilknytning til en annen stat er slik utvalget ser det et helt selvsagt og nødvendig vurderingsmoment.

Utvalget vil derfor anbefale at tilknytning til andre stater, som et av flere vurderingsmomenter i en konkret helhetsvurdering, videreføres i ny sikkerhetslov. Utvalget erkjenner imidlertid at klareringssaker hvor vedkommende har tilknytning til en annen stat, spesielt de stater som potensielt utgjør en etterretningstrussel mot norske interesser, er meget komplekse saker som stiller høye krav til klareringsmyndighetenes kompetanse. Utvalget tror de vedtatte endringene i klareringsmyndighetsstrukturen kan bidra til å legge til rette for et høyt kompetansenivå hos klareringsmyndighetene. Forslaget må også sees i sammenheng med at utvalget foreslår å fremheve adgangen til å sette vilkår for en klarering eller innvilge en klarering avgrenset til en konkret stilling (stillingsklarering).

Etter utvalgets oppfatning vil det ikke innebære urimelig forskjellsbehandling å sette vilkår for en klarering, eller innvilge en stillingsklarering, der alternativet ville vært å avslå klareringsanmodningen. Det sikkerhetsmessige aspektet må imidlertid uansett være førende for hvorvidt en person innvilges sikkerhetsklarering eller ikke. Dersom klarering på vilkår, eller stillingsklarering, vurderes ikke å ha tilstrekkelig risikoredu-

serende effekt, må og skal klareringsanmodningen avslås.

Når det gjelder klarering av personell uten norsk statsborgerskap, foreslår utvalget en justering av bestemmelsen. Gjeldende bestemmelse har blitt forstått og praktisert slik at en eller annen form for tilknytning til Norge, har vært et avgjørende kriterium for å kunne innvilge klarering. Dette har i praksis ført til at personer har fått nektet klarering, selv om vurderingen for øvrig ikke gir grunn til å betvile vedkommendes sikkerhetsmessige skikkethet. Slik utvalget ser det, har dette vært en utilsiktet konsekvens av bestemmelsen, og det foreslås derfor en justering av bestemmelsen som åpner for å kunne klarere utenlandske statsborgere som ikke har en tilknytning til Norge.

10.6.3 Mangelfull personhistorikk

Avgjørelser om klarering skal baseres på en konkret helhetsvurdering av hvorvidt vedkommende er til å stole på. Slik utvalget ser det er muligheten for å gjennomføre en tilfredsstillende personkontroll et av flere relevante forhold som kan tillegges betydning ved denne vurderingen. Hovedregelen om 10 års personhistorikk er regulert i personellsikkerhetsforskriften § 3-6, hvor det også fremgår at det ut fra en individuell helhetsvurdering kan gjøres unntak fra dette kravet.

Slik utvalget ser det gir regelverket på lov- og forskriftsnivå tilstrekkelig fleksibilitet til å kunne gjøre unntak fra kravet til personhistorikk der gode grunner taler for dette. Det fremstår imidlertid som at praktiseringen av dette unntaket, herunder rundskrivene som beskriver hvordan dette skal forstås, har en mer restriktiv og skjematisk tilnærming enn lov- og forskriftsreguleringen skulle tilsi.

En individuell vurdering av om det er grunnlag for å gjøre unntak fra 10 års personhistorikk, forutsetter høy kompetanse hos de enkelte klareringsmyndighetene. Sett hen til dagens situasjon, hvor antallet klareringsmyndigheter er høyt og kompetansenivået varierende, har utvalget forståelse for at man i rundskrivene har lagt seg på en restriktiv linje. Både Utenriksdepartementet og Landsorganisasjonen har overfor utvalget påpekt at denne praksisen er problematisk, spesielt for personell i utenrikstjenesten.

Den vedtatte endringen av klareringsmyndighetsstrukturen bør, slik utvalget ser det, også gjenspeiles i de ulike rundskrivene vedrørende personellsikkerhet. Økt kompetanse hos de gjenværende klareringsmyndighetene innebærer også at disse vil være bedre rustet til å kunne gjøre konkrete og individuelle helhetsvurderinger.

10.6.4 Tverrsektoriell hjemmel for bakgrunnskontroll

Som beskrevet over har en rekke sentrale aktører påpekt behovet for en tverrsektoriell hjemmel for bakgrunnskontroll, ut over det som følger av dagens klareringsinstitutt. Basert på gjennomgangen av relevant sektorregelverk, er utvalget prinsipielt enig i at sektorregelverkene i liten grad regulerer personkontroll som et sikkerhetsmessig tiltak. Utvalget er også enig i at det på enkelte områder er behov for en hjemmel for personkontroll utover det som eksisterer i dag.

Utvalget har vurdert hvorvidt det vil være tilstrekkelig at det etableres en hjemmel for personkontroll i relevante sektorregelverk. En fordel med en slik tilnærming vil være at personkontrollen kan begrenses til det som er nødvendig i den aktuelle sektor. Det vil da kunne gjøres sektorspesifikke tilpasninger, både med hensyn til omfanget av personkontrollen og med hensyn til hvilke forhold som sjekkes. På den andre siden vil det være en risiko for at regelverket praktiseres ulikt i de ulike samfunnssektorene. Ut fra en sikkerhetsfaglig vurdering vil det være uheldig dersom det i enkelte sektorer legges opp til et liberalt regime for personkontroll, mens det i andre sektorer er streng personkontroll. Dette vil føre til en ubalanse mellom de ulike samfunnssektorene, som vil kunne øke sårbarheten. I tillegg vil det kunne innebære en forskjellsbehandling ved at det i enkelte sektorer stilles lavere krav til sikkerhetsmessig skikkethet enn i andre.

Utvalget anbefaler derfor at det i den nye sikkerhetsloven etableres en hjemmel for adgangsklarering for personell som skal ha tilgang til objekter eller infrastruktur, eller deler av disse, som er av kritisk betydning for grunnleggende nasjonale funksjoner. Det foreligger allerede i gjeldende sikkerhetslov en hjemmel for å kunne kreve sikkerhetsklarering for tilgang til skjermingsverdige objekter klassifisert KRITISK eller MEGET KRITISK.

På samme måte som etter dagens objektsikkerhetsforskrift, anbefaler utvalget at det enkelte fagdepartement gis hjemmel til å kunne fatte vedtak om krav til adgangsklarering for tilgang til nærmere angitte objekter eller infrastruktur. Dette er en naturlig konsekvens av utvalgets forslag om at fagdepartementene gis det overordnede ansvaret for forebyggende sikkerhet i egen sektor, og vil gi departementene anledning til å

gjøre nødvendige sektorspesifikke tilpasninger eller samfunnsøkonomisk lønnsomme prioriteringer innenfor eget myndighetsområde.

Utvalget har vurdert ulike alternativer for hvor omfattende en slik adgangsklarering bør gjøres. Det synes å være enighet om at en uttømmende politiattest ikke vil være tilstrekkelig ut fra et sikkerhetsmessig perspektiv. Samtidig mener utvalget at en like omfattende prosess som en ordinær sikkerhetsklarering, både vil utgjøre et stort inngrep i den enkeltes personvern og være meget ressurskrevende å administrere. Utvalget legger derfor til grunn for sitt forslag at personkontrollen for adgangsklarering skal gjøres mindre omfattende enn for dagens sikkerhetsklareringsregime for tilgang til gradert informasjon.

I tråd med Justis- og beredskapsdepartementets syn, er utvalget av den oppfatning at personkontrollen for adgangsklarering bør utformes etter de linjer man har i Storbritannia for en såkalt *Counter Terrorist Check*. En slik personkontroll gir et bredere informasjonstilfang enn en uttømmende politiattest, men er samtidig mindre omfattende enn en ordinær sikkerhetsklarering. Hvilke registre som er aktuelle for en slik personkontroll bør, på lik linje med det opprinnelige klareringsinstituttet, fastsettes på forskriftsnivå. Det vil imidlertid være naturlig at en slik registersjekk omfatter PSTs registre, i tillegg til de registre som sjekkes ved en uttømmende politiattest.

Når det gjelder gjennomføring av adgangsklarering, ser utvalget store fordeler ved å bygge på de allerede etablerte strukturene. Den vedtatte endringen i klareringsmyndighetsstrukturen, vil også gjøre dette mindre betenkelig. En slik løsning vil kunne gi økt effektivitet og høyere kompetanse hos klareringsmyndighetene, samtidig som det vil innebære økt rettssikkerhet for den enkelte. Det vil også være kostnadsbesparende sett opp mot alternativet – å etablere sektorvise regimer for personkontroll, hvor hver enkelt samfunnssektor vil måtte bygge opp tilstrekkelig kompetanse og ressurser.

Forslaget vil medføre økt ressursbruk. Antall klareringssaker vil øke, og for å kunne gjennomføre en effektiv klareringsprosess vil det sannsynligvis være behov for en økning i antall årsverk som skal behandle slike saker. En avgjørende forutsetning er at de aktuelle klareringsmyndighetene dimensjoneres slik at de kan saksbehandle både sikkerhets- og adgangsklareringer, uten at dette går på bekostning av saksbehandlingstiden. Ettersom det vil være opp til det enkelte fagdepartement å avgjøre hvorvidt det skal settes krav til adgangsklarering, er det vanskelig å si noe konkret om hvor mange stillinger dette vil gjelde. En rekke stillinger vil imidlertid allerede i dag ha krav om sikkerhetsklarering fordi vedkommende i kraft av sin stilling vil ha behov for tilgang til gradert informasjon. Utvalget antar likevel at det vil bli en økning av antall klareringer som konsekvens av at lovens virkeområde utvides.

Forslaget vil innebære personvernulemper for personell i stillinger hvor det settes krav til klarering. Klareringsinstituttet er i seg selv av inngripende karakter, hvor det blant annet innhentes personopplysninger fra en rekke relevante registre. Utvalget legger til grunn at det enkelte fagdepartement kun setter krav om adgangsklarering der dette er nødvendig og også har en reell sikkerhetsmessig effekt.

Utvalget mener imidlertid at den sikkerhetsmessige gevinsten ved å etablere en generell hjemmel for adgangsklarering, overstiger de ulempene dette vil medføre kostnadsmessig og for den enkeltes personvern. Forslaget vil være et viktig bidrag til utvalgets målsetting om å legge til rette for å kunne forebygge og eventuelt avdekke utro tjenere.

Utvalget har også vurdert hvorvidt forslaget kan være i strid med tilbakevirkningsforbudet i Grunnloven § 97, dersom krav til adgangsklarering gjøres gjeldende for personell som allerede er ansatt i en virksomhet som ikke tidligere har vært underlagt loven. Menneskerettighetsutvalget oppsummerte rettstilstanden for tilbakevirkningsforbudet utenfor strafferettens område på følgende måte:

> Utenfor strafferettens område er det alminnelig enighet om at § 97 ikke forbyr all tilbakevirkning. Et strengt tilbakevirkningsforbud vil være til hinder for at lovgivningen holder tritt med samfunnsutviklingen, og det vil legge alvorlige begrensninger på lovgivning som styringsinstrument. Hvorvidt den tilbakevirkende loven er rettsstridig, dvs. i strid med Grunnloven § 97, vil derfor måtte bero på en helhetsvurdering av situasjonen, jf. bl.a. plenumsavgjørelsene i Rt-1996-1415 (Borthen), Rt-2007-1281 (Ullern Terrasse) og Rt-2010-143 (rederiskattesaken). I denne helhetsvurderingen vil en rekke faktorer spille inn, herunder vurderinger av den enkeltes behov for å forutberegne sin rettsstilling og lovgivers formål med å endre rettstilstanden. I tillegg vil mer konkrete faktorer som inngrepets art og styrke, berettigede forventninger, behovet for lovendring, eventu-

elle overgangsregler, lovgivers egne vurderinger av grunnlovsmessighet m.m. spille inn ved vurderingen.[57]

De aktuelle vernede interessene med hensyn til utvalgets forslag vil være den enkelte ansattes arbeidsforhold og arbeidsoppgaver. En negativ klarering vil i ytterste konsekvens kunne medføre at vedkommende ikke vil kunne fortsette i sin jobb, dersom det ikke er mulig å omplassere vedkommende til en annen stilling i samme virksomhet, som ikke krever slik adgangsklarering. Den enkelte ansatte vil naturlig nok ha en berettiget forventning om at han eller hun kan beholde sin stilling og arbeidsoppgaver. På den annen side vil det faktum at det foreligger forhold ved den enkelte som medfører at vedkommende ikke er sikkerhetsmessig skikket til å inneha den aktuelle stillingen, etter utvalgets syn trekke i retning av at vedkommendes forventinger ikke bør tillegges vesentlig vekt.

Mot den enkeltes interesser i å beholde stillingen, står hensynet til nasjonal sikkerhet – å beskytte grunnleggende nasjonale funksjoner mot tilsiktede uønskede hendelser. Klareringsinstituttet er, som nevnt, et helt sentralt virkemiddel for å kunne beskytte grunnleggende nasjonale funksjoner mot utro tjenere og ivareta hensynet til nasjonal sikkerhet. Etter utvalgets vurdering må de samfunnsmessige hensynene som ligger bak forslaget om adgangsklarering, veie tyngre enn hensynet til å ivareta den enkeltes interesser. Utvalget har derfor kommet til at det ikke vil være sterkt urimelig å gi forslaget tilbakevirkende kraft. I motsatt fall vil lovforslaget få svært begrenset effekt for allerede tilsatt personell.

Den enkeltes rettssikkerhet i klareringsprosessen vil være ivaretatt gjennom de allerede etablerte rettssikkerhetsgarantiene, herunder retten til begrunnelse og til å påklage en negativ klareringsavgjørelse.

10.6.5 Digitalisert overføring av registeropplysninger

Basert på innspill fra NSM, har utvalget vurdert hvorvidt registereiere bør pålegges å tilrettelegge for det NSM kaller *automatisert kildeinnhenting*. I utvalgets dialog med NSM har utvalget fått forståelsen av at hovedutfordringen for NSM er at samhandlingen med enkelte registereiere er basert på en manuell og tidkrevende prosess for å få oversendt den aktuelle informasjonen som finnes i registrene. Dette har igjen betydning for saksbehandlingstiden i klareringssaker. Som nevnt i kapittel 10.5.5, har utvalget lagt til grunn at det NSM primært ønsker, er at de enkelte registereierne pålegges en plikt til å legge til rette for en digitalisert overføring av relevante registeropplysninger.

Utvalget mener generelt at det er viktig å legge forholdene til rette for at saksbehandlingen av klareringssaker kan gå så raskt som mulig. En sømløs samhandling mellom relevante aktører innen klareringsinstituttet, kan bidra til en slik effektivisering. Slik utvalget har forstått det, er denne manuelle og tidkrevende prosessen for innhenting av opplysninger fra relevante registre, en av flaskehalsene i systemet.

Utvalget mener en digitalisert overføring av relevante registeropplysninger vil kunne bidra til å effektivisere klareringsregimet. En slik digitalisert overføring vil også være mindre ressurskrevende, både for NSM og de ulike registereierne. En forutsetning for en slik løsning er at det etableres sikre kommunikasjonslinjer mellom NSM og de aktuelle registereierne, som tilfredsstiller kravene for digital behandling av slik informasjon. Utvalget går i lovforslaget inn for å lovfeste en plikt for registereierne til å legge til rette for en digitalisert overføring av registeropplysninger fra registereier til NSM.

Forslaget vil på kort sikt innebære økte investeringskostnader knyttet til å få etablert sikre kommunikasjonslinjer mellom NSM og de registereierne som i dag ikke har slike kommunikasjonslinjer med NSM, samt å tilrettelegge de aktuelle registrene for en slik overføring. På lengre sikt mener imidlertid utvalget at forslaget vil innebære en redusert ressursbruk knyttet til behandling av denne type saker, både hos NSM og de aktuelle registereierne. I et langsiktig samfunnsøkonomisk perspektiv mener således utvalget at fordelene ved en slik løsning vil overstige ulempene ved en kostnadsmessig økning på kort sikt.

10.6.6 Personkontroll

Både NSM og Forsvarsdepartementet har anmodet utvalget om å vurdere en hjemmel for ytterligere personkontroll ut over den personkontroll som gjennomføres ved førstegangsklarering og reklarering.

Utvalget har i sitt arbeid sett hen til hvordan dette er regulert i andre, sammenlignbare nasjoner. Både Danmark og Storbritannia har klareringsregimer som legger opp til at relevante registre kan kontrolleres når som helst i en klarerings

[57] Dok.16 (2011–2012), 137.

gyldighetstid, i den hensikt å avdekke hvorvidt det skjer endringer av betydning for den enkeltes sikkerhetsmessige skikkethet. I Sverige har ekspertgruppen som utredet forslag til ny sikkerhetslov, anbefalt at det innføres et tydelig hjemmelsgrunnlag for slik regelmessig kontroll.

Utvalget mener det er en svakhet ved dagens regelverk at det ikke foreligger hjemmel for å kunne gjennomføre personkontroll ut over førstegangs- og reklarering. Dagens system er lite egnet til å kunne fange opp endringer i klarert personells sikkerhetsmessige skikkethet, ut over den enkeltes opplysningsplikt til autorisasjonsansvarlig om slike forhold. Utvalget forslår derfor en hjemmel for å kunne iverksette ny personkontroll opp mot relevante registre når som helst innenfor en klarerings gyldighetstid. Hensikten er å kontrollere om det har skjedd endringer av betydning. Ny personkontroll kan i henhold til bestemmelsen både gjøres på regelmessig basis og ved konkret mistanke om at det har skjedd endringer som kan ha betydning for den enkeltes klarering.

Etter utvalgets oppfatning vil ikke forslaget ha vesentlige negative konsekvenser for den enkeltes personvern. Hjemmel for å innhente slike opplysninger i klareringsprosessen eksisterer allerede i dag og er godt begrunnet. Muligheten for å oppdatere denne informasjonen på regelmessig basis, eller ved mistanke om at det har skjedd endringer av betydning for den enkeltes sikkerhetsmessige skikkethet, vil dessuten være i tråd med personopplysningslovens krav om at personopplysninger skal være korrekte og oppdaterte. Dersom en slik personkontroll innebærer at det treffes en avgjørelse om suspensjon, nedsettelse eller tilbakekallelse av klareringen, vil den enkeltes rettssikkerhet bli ivaretatt gjennom den etablerte klageadgangen.

Kombinert med forslaget om plikt til å legge til rette for digitalisert overføring av kilderesultater, kan ikke utvalget se at forslaget vil ha store konsekvenser verken for NSM eller de berørte registereierne.

10.6.7 Informasjonsdeling

Utvalget har vurdert hvorvidt det bør etableres en hjemmel for å kunne dele informasjon mellom Sikkerhetsmyndigheten og Politiets sikkerhetstjeneste (PST). En slik hjemmel vil innebære et inngrep i den enkeltes personvern. Informasjon om den enkelte vil kunne bli brukt til andre formål enn de primært var innhentet for, nemlig å vurdere den enkeltes sikkerhetsmessige skikkethet knyttet til en konkret anmodning om klarering.

En slik hjemmel vil også kunne utfordre klareringsinstituttets grunnleggende innretning, hvor den enkeltes avgivelse av opplysninger til klareringsmyndigheten er tuftet på et prinsipp om at slike opplysninger behandles i fortrolighet. Det er imidlertid åpning allerede i dag for at klareringsmyndighetene kan dele informasjon med autorisasjonsansvarlig, der dette anses påkrevet av hensyn til den sikkerhetsmessige ledelse og kontroll av vedkommende.

Formålet med klareringsinstituttet er nettopp å redusere risikoen for at sikkerhetsgradert informasjon kompromitteres, eller at adgang til sensitive områder misbrukes på en måte som kan skade grunnleggende nasjonale funksjoner. Slik kompromittering eller misbruk av tilgang, vil i mange tilfeller være sammenfallende med overtredelse av de straffebud PST har som oppgave å forebygge og etterforske. Innsidetrusselen er slik utvalget ser det både reell og overhengende. Dette bekreftes av PSTs trusselvurderinger og de vurderinger som ligger til grunn for NSMs sikkerhetsfaglige råd. Formålet med en slik hjemmel for informasjonsdeling vil være hensynet til beskyttelse av grunnleggende nasjonale funksjoner.

Utvalget mener videre at en hjemmel til å dele slik informasjon vil kunne bidra til at PSTs forebyggende arbeid blir mer målrettet. Dette vil kunne gi en sikkerhetsmessig gevinst, og vil være et viktig virkemiddel for at PST skal kunne ivareta sine plikter.

Samlet sett mener utvalget at de sikkerhetsmessige gevinstene som oppnås ved at PST settes bedre i stand til å kunne målrette sitt forebyggende arbeid, overstiger de personvernmessige konsekvensene et slikt forslag medfører. En viktig rettssikkerhetsgaranti for den enkelte vil være EOS-utvalgets kontroll med EOS-tjenestene. Utvalget legger til grunn at praktiseringen av denne type informasjonsdeling mellom Sikkerhetsmyndigheten og PST, vil ha et særlig fokus fra EOS-utvalget.

Av personvernmessige hensyn mener utvalget at en slik hjemmel må avgrenses til det som er strengt nødvendig for at PST skal kunne ivareta sine oppgaver etter politiloven. Utvalget foreslår derfor en begrenset hjemmel til å kunne dele informasjon med PST, der dette er relevant og nødvendig etter politiloven § 17 b og § 17 c nr. 1.

Utvalget mener at prosedyren for deling av slik informasjon, bør være at PST initierer prosessen ved å anmode Sikkerhetsmyndigheten om nærmere angitt informasjon om klarert personell. Eksempelvis kan generelle trender i trusselbildet tilsi at PST har behov for en oversikt over klarert personell med tilknytning til en bestemt nasjon.

PST vil selv være best i stand til å vurdere hvilken informasjon som er nødvendig for å ivareta tjenestens oppgaver etter politiloven § 17 b og 17 c nr. 1. Dersom Sikkerhetsmyndigheten selv skal vurdere når det er relevant og nødvendig å dele informasjon med PST, vil informasjonsdelingen i mindre grad være knyttet opp til PSTs konkrete behov og vil kunne medføre at PST må håndtere større mengder overskuddsinformasjon.

Videre mener utvalget at informasjonsdelingen bør begrenses til de opplysninger som er nødvendige for at PST skal kunne ivareta sine oppgaver. Gjennom personkontrollen innhentes det en stor mengde opplysninger fra en rekke forskjellige registre. En generell hjemmel for deling av opplysninger som fremkommer under personkontrollen, vil slik utvalget ser det utgjøre et uforholdsmessig inngrep i personvernet.

Slik utvalget har forstått PSTs behov, er det særlig tre typer opplysninger som er relevante og nødvendige for at tjenesten skal kunne ivareta sine oppgaver. For det første gjelder dette informasjon om vedkommendes identitet og klareringsstatus. Personell som ikke får innvilget klarering, vil heller ikke få tilgang til sikkerhetsgradert informasjon eller til områder hvor det stilles krav om slik klarering.

For det andre vil opplysninger om vedkommendes tilknytning til andre nasjoner, enten direkte eller via nærstående, være relevant og nødvendig informasjon i denne sammenheng. Det er denne tilknytningen som kan danne grunnlaget for at vedkommende potensielt blir utsatt for press, og som således er inngangskriteriet for at PST skal kunne anmode om informasjon.

For det tredje bør opplysninger om vedkommendes tjenestested gjøres tilgjengelig for PST. Dette for å kunne målrette det forebyggende arbeidet, og å kunne kartlegge og analysere trender og utviklingstrekk. Eksempelvis vil en stat som kommer i søkelyset på grunn av atomkraft og reaktorteknologi kunne utgjøre en slik trend.

Utvalget har også vurdert hvorvidt PSTs anmodning bør kunne rettes mot de enkelte klareringsmyndighetene, eller mot Sikkerhetsmyndigheten som forvalter av det sentrale registeret for klareringsavgjørelser. Etter utvalgets vurdering vil det være mest hensiktsmessig at PST har ett enkelt kontaktpunkt inn mot klareringsinstituttet. Dette vil kunne bidra til å sikre en god samhandling og en ensartet praksis for deling av slik informasjon. Det vil også redusere behovet for å etablere saksbehandlerkapasitet hos de ulike klareringsmyndighetene til å håndtere slike anmodninger. Et annet forhold som taler for en slik løsning, er at informasjon om hvilke fokusområder PST har for sitt forebyggende arbeid i seg selv er sensitiv informasjon, hvor spredningen bør begrenses til et minimum.

En slik klart avgrenset hjemmel til å kunne dele informasjon med PST vil, slik utvalget ser det, ikke utgjøre et uforholdsmessig inngrep i den enkeltes personvern sett opp mot den sikkerhetsmessige gevinsten som oppnås ved tiltaket. At avgrensningen gjøres i loven, vil også gjøre det forutsigbart for den enkelte hvilken informasjon som kan deles med PST. For å ytterligere styrke forutsigbarheten for den enkelte, mener utvalget at det uttrykkelig bør fremgå av personopplysningsblanketten den enkelte fyller ut som grunnlag for klareringsprosessen, at nærmere angitt informasjon vil kunne deles med PST. For allerede klarert personell bør myndighetene orientere særskilt om at det gis anledning for å dele slik informasjon med PST. En måte dette kan gjøres på er at klareringsmyndighetene sender en generell orientering til aktuelle virksomheter, og ber om at denne informasjonen videreformidles til autorisert personell.

En slik lovhjemmel forutsetter også at NSMs sentrale klareringsregister innrettes på en slik måte at de aktuelle opplysningene fremgår, og at de enkelt kan hentes ut fra registeret. Det forutsetter også at de autorisasjonsansvarlige pålegges en plikt til å innrapportere til NSM hvilket personell som har blitt autorisert i den enkelte virksomhet, slik at opplysninger om dette kan legges inn i det sentrale klareringsregisteret. En slik rapporteringsplikt vil også medføre at endring av tjenestested vil fanges opp av NSM, ved at ny arbeidsgiver vil innrapportere at vedkommende har blitt autorisert for tilgang til sikkerhetsgradert informasjon i virksomheten.

Slik utvalget ser det, vil en slik innrapportering, uavhengig av PSTs behov for å benytte slik informasjon i sitt forebyggende arbeid, styrke personellsikkerheten i Norge gjennom en bedre oppfølging av, og kontroll med, klarert personells skifte av tjenestested. Utvalget mener uansett det er en svakhet med dagens klareringsinstitutt at det ikke eksisterer mekanismer som gjør at Sikkerhetsmyndigheten har en oppdatert oversikt over hvor klarert personell til enhver tid tjenestegjør.

Forslaget vil ha noen kostnadsmessige konsekvenser for Sikkerhetsmyndigheten i form av behov for saksbehandlerkapasitet til å kunne håndtere anmodninger fra PST. I tillegg vil det sentrale registeret for klareringsavgjørelser måtte tilpasses slik at nødvendig og relevant informa-

sjon fremgår av registeret, og enkelt kan hentes ut av dette. Forslaget vil også ha noen kostnadsmessige konsekvenser for autorisasjonsansvarlig, knyttet til plikten til å innrapportere opplysninger. For PSTs vedkommende vil forslaget sannsynligvis ikke innebære slike kostnader.

Kapittel 11
Sikkerhetsgraderte anskaffelser

11.1 Innledning

Regelverket for sikkerhetsgraderte anskaffelser er et viktig verktøy for å kunne sikre at leverandører som gis tilgang til sikkerhetsgradert informasjon eller til skjermingsverdige objekter, er sikkerhetsmessig til å stole på. Dette både for å sikre at sikkerhetsgradert informasjon blir håndtert på en forsvarlig måte, og for å sikre at tilgang til skjermingsverdige objekter ikke misbrukes på en måte som kan ha alvorlige skadefølger.

Utvalgets målsetting med regelverket for sikkerhetsgraderte anskaffelser er å sikre at regelverket gir et tilstrekkelig hjemmelsgrunnlag til å kunne undersøke om leverandører til virksomheter av kritisk betydning for grunnleggende nasjonale funksjoner er sikkerhetsmessig skikket. Samtidig må regelverket ikke være innrettet på en slik måte at det i vesentlig grad kompliserer, forsinker eller fordyrer virksomhetenes anskaffelsesprosesser.

En grunnleggende problemstilling utvalget har måttet ta stilling til er om dagens regelverk, med de vedtatte endringene i henhold til Prop. 97 L (2015–2016), har en balansert og hensiktsmessig tilnærming når det gjelder sikkerhetshensyn på den ene siden og bedriftsøkonomiske hensyn på den andre.

En annen grunnleggende problemstilling utvalget har måttet ta stilling til er hvorvidt utvalgets innretning på den nye loven, herunder utvidelsen av lovens virkeområde, nødvendiggjør endringer i regelverket om sikkerhetsgraderte anskaffelser.

11.2 Gjeldende sikkerhetslovs regulering

Sikkerhetsloven kapittel 7 gir nærmere bestemmelser om sikkerhetsgraderte anskaffelser. En sikkerhetsgradert anskaffelse er i loven § 3 første ledd nr. 17 definert som en:

> anskaffelse, foretatt av anskaffelsesmyndighet som innebærer at leverandøren av varen eller tjenesten vil kunne få tilgang til skjermingsverdig informasjon eller objekt, eller som innebærer at anskaffelsen må sikkerhetsgraderes av andre årsaker.

Anskaffelsesmyndighet er definert som «et forvaltningsorgan som har til hensikt å anskaffe, eller har anskaffet, varer eller tjenester fra et rettssubjekt som ikke er et forvaltningsorgan», jf. loven § 3 første ledd nr. 16.

Leverandører i sikkerhetsgraderte anskaffelser blir automatisk underlagt sikkerhetslovens bestemmelser, jf. loven § 2 annet ledd. Regelverket om sikkerhetsgraderte anskaffelser berører derfor i stor grad selvstendige rettssubjekter. Regelverket etablerer de nødvendige sikkerhetsmekanismer når selvstendige rettssubjekter er leverandører av varer eller tjenester til et forvaltningsorgan eller en virksomhet som er underlagt sikkerhetsloven.

Nærmere bestemmelser om sikkerhetsgraderte anskaffelser er regulert i forskrift om sikkerhetsgraderte anskaffelser.[1]

11.2.1 Sikkerhetsavtale

Ved sikkerhetsgraderte anskaffelser skal det inngås en sikkerhetsavtale mellom anskaffelsesmyndigheten og leverandøren.

Sikkerhetsavtalen formaliserer sikkerhetsmessige aspekter i forbindelse med en sikkerhetsgradert anskaffelse, og skal legge til rette for at lokale forhold, praktisk gjennomføring og detaljer av betydning for sikkerheten, kan reguleres tilfredsstillende.[2]

Før en leverandør kan få tilgang til skjermingsverdig informasjon, må sikkerhetsavtale være inngått, jf. sikkerhetsloven § 27 første ledd. Ved til-

[1] Forskrift 1. juli 2001 nr. 753 om sikkerhetsgraderte anskaffelser.

[2] Nasjonal sikkerhetsmyndighets veileder, 6.

gang til skjermingsverdig objekt er det bare krav om sikkerhetsavtale dersom Nasjonal sikkerhetsmyndighet krever det eller det av andre grunner er nødvendig å sikkerhetsgradere anskaffelsen.

Dersom en oppdragsgiver skal inngå en sikkerhetsavtale med en utenlandsk leverandør, kan det først skje etter godkjenning fra Nasjonal sikkerhetsmyndighet, jf. § 27 første ledd tredje punktum. Hva sikkerhetsavtalen skal inneholde, følger av forskrift om sikkerhetsgraderte anskaffelser § 2-5. Leverandøren er omfattet av sikkerhetslovens bestemmelser uavhengig av om det inngås en sikkerhetsavtale, men sikkerhetsavtalen tydeliggjør og operasjonaliserer de sikkerhetskrav som gjelder for den enkelte anskaffelse.[3]

11.2.2 Leverandørklarering

Dersom leverandøren skal gis tilgang til skjermingsverdig informasjon gradert KONFIDENSIELT eller høyere, eller dersom det av andre grunner anses nødvendig, skal det gjennomføres en leverandørklarering for å vurdere leverandørens sikkerhetsmessige skikkethet, jf. loven § 28. Nasjonal sikkerhetsmyndighet er klareringsmyndighet for leverandørklareringer.

Leverandørklarering skal kun gis dersom det ikke foreligger rimelig tvil om leverandørens skikkethet. Ved avgjørelse om leverandøren anses sikkerhetsmessig skikket skal det bare legges vekt på forhold som er relevante for å vurdere leverandørens evne og vilje til å utøve forebyggende sikkerhetstjeneste etter bestemmelsene i eller i medhold av loven.[4]

I vurderingen skal også personkontroll av personer i leverandørens styre og ledelse inngå, jf. forskriften § 3-1 nr. 1. Leverandøren skal videre gi alle relevante opplysninger av betydning for klareringsspørsmålet, jf. § 28 tredje ledd. Opplysningsplikten er nærmere regulert i forskriften § 3-2.

En leverandør som innehar en leverandørklarering skal uten ugrunnet opphold orientere Nasjonal sikkerhetsmyndighet om endringer i styre eller ledelse, forandringer i eierstrukturen, flytting av lokaliteter og utstyr, åpning av gjeldsforhandlinger eller begjæring om konkurs, og om andre forhold som kan ha betydning for leverandørens sikkerhetsmessige skikkethet. Hvis forholdene anses å representere en sikkerhetsrisiko som ikke kan elimineres gjennom forebyggende sikkerhetstiltak, kan Nasjonal sikkerhetsmyndighet inndra leverandørklareringen, jf. § 28 fjerde ledd, jf. forskriften § 3-3.

Det følger videre av § 28 fjerde ledd siste punktum at skjermingsverdig informasjon eller objekt ikke kan overføres til ny eier eller inngå i bobehandling ved gjeldsforhandling eller konkurs, med mindre Nasjonal sikkerhetsmyndighet har samtykket til dette.[5]

Saksbehandlingsreglene i sikkerhetsloven kapittel 6 om personellsikkerhet, herunder bestemmelsen om begrunnelse og klage, gjelder så langt de passer for leverandørklaringer, jf. § 28 femte ledd.

11.2.3 Varighet av leverandørklarering

Regjeringen har i Prop. 97 L (2015–2016) foreslått at leverandørklarering gis etter anmodning fra en anskaffelsesmyndighet, men med en tidsbegrenset varighet. Forslaget innebar en endring fra oppdragsbasert til tidsbasert leverandørklarering. Systemet med klarering for hvert enkelt oppdrag var ifølge regjeringen for tungvint, og genererte et unødvendig høyt antall søknader om leverandørklarering. Leverandørklarering for det enkelte oppdrag var også i utakt med praksis i en del andre land, samt med internasjonalt regelverk.

Det nærmere tidsrommet leverandørklareringen skal gjelde er foreslått regulert som en forskriftshjemmel, som gir Kongen myndighet til å bestemme den generelle gyldighetstiden for slike klareringer. I forarbeidene antydes det en varighet på fem år, tilsvarende den generelle varighetstiden for personellklareringer.[6]

Stortinget har, i forbindelse med behandlingen av Innst. 352 L (2015–2016) til Prop. 97 L (2015–2016), vedtatt regjeringens forslag om tidsbasert leverandørklarering.

11.2.4 Anskaffelser til kritisk infrastruktur

Regjeringen har videre i Prop. 97 L (2015–2016) fremmet forslag om en ny lovbestemmelse (§ 29 a) som pålegger virksomheter som eier eller rår over kritisk infrastruktur en plikt til å gjøre en risikovurdering ved anskaffelser til slik infrastruktur, og en påfølgende myndighet for Kongen i statsråd til å treffe vedtak om å nekte anskaffelsen gjennomført eller sette nærmere vilkår for anskaffelsen.

Om begrunnelsen for forslaget skriver departementet følgende:

---

3 Ot.prp. nr. 49 (1996–97), 62.

4 Ibid., 63.

5 Ibid.

6 Prop. 97 L (2015–2016), 50.

> Globalisering og økt internasjonalisering av vare og tjenestehandelen har ført til at eiere av kritisk infrastruktur, i større utstrekning enn tidligere, bruker utenlandske selskaper som leverandører til norsk kritisk infrastruktur. Utstrakt bruk av utenlandske leverandører er potensielt problematisk fordi det kan medføre en forhøyet risiko for spionasje og sabotasje til skade for norske interesser. Samfunnets økte avhengighet av kritisk infrastruktur gjør at denne problemstillingen trolig vil få stadig større relevans framover.[7]

I det opprinnelige høringsforslaget foreslo Forsvarsdepartementet en absolutt varslingsplikt til ansvarlig fagdepartement dersom en anskaffelse til kritisk infrastruktur som virksomheten eier eller rår over kunne innebære en ikke ubetydelig risiko for rikets selvstendighet og sikkerhet eller andre vitale nasjonale sikkerhetsinteresser.

I høringen ble det også foreslått en ny bestemmelse i sikkerhetsloven § 2, for å kunne fange opp eiere av kritisk infrastruktur som ikke var underlagt sikkerhetsloven fra før.

På bakgrunn av høringsinnspillene foreslo departementet i Prop. 97 L (2015–2016) noen hovedendringer fra det opprinnelige lovforslaget.[8]

For det første ble det foreslått å lovfeste at den nye bestemmelsen skulle gjelde alle virksomheter som foretar anskaffelser til kritisk infrastruktur, uavhengig av om virksomheter er underlagt sikkerhetslovens øvrige bestemmelser.

Kritisk infrastruktur i sikkerhetslovens forstand ble foreslått definert som «anlegg og systemer som er nødvendige for å opprettholde samfunnets grunnleggende behov og funksjoner».[9]

For det andre ble den absolutte varslingsplikten, foreslått endret til en uttrykkelig plikt for virksomhetene til å foreta risikovurderinger ved anskaffelser til kritisk infrastruktur. Varslingsplikten til ansvarlig departement vil først inntre dersom virksomheten ønsker å gjennomføre en anskaffelse som innebærer en ikke ubetydelig risiko for sikkerhetstruende virksomhet.

I forlengelsen av endringen av den absolutte varslingsplikten foreslo også departementet en presisering om at virksomhetene ikke behøver å varsle myndighetene dersom virksomhetene selv iverksetter risikoreduserende tiltak som fjerner risikoen, eller gjør denne ubetydelig.

Ansvarlig fagdepartement som mottar et varsel, skal som utgangspunkt innhente rådgivende uttalelser fra relevante organer. I forarbeidene nevnes Politiets sikkerhetstjeneste, Etterretningstjenesten og Nasjonal sikkerhetsmyndighet som aktuelle organer. Etter å ha samlet inn nødvendig informasjon, kan saken avgjøres av departementet i dialog med den aktuelle virksomheten. For det tilfelle at departementet kommer til at anskaffelsen ikke bør gjennomføres, eller det bør stilles nærmere vilkår for gjennomførelsen, skal saken fremmes for Kongen i statsråd. Det presiseres at et vedtak fra Kongen i statsråd må være innrettet på en slik måte at lovens formål ivaretas. I forarbeidene presiseres det at formålsbegrensningen blant annet vil innebære at det ikke er hjemmel for å gripe inn ved risiko for industrispionasje som kun er egnet til å skade en enkeltbedrifts forretningsvirksomhet.[10]

Stortinget har, i forbindelse med behandlingen av Innst. 352 L (2015–2016) til Prop. 97 L (2015–2016), vedtatt regjeringens forslag om plikt til å gjennomføre en risikovurdering ved anskaffelser til kritisk infrastruktur og påfølgende vedtaksmyndighet for Kongen i statsråd.

11.3 Annet relevant regelverk

11.3.1 Lov om offentlige anskaffelser

Alle offentlige anskaffelser i Norge reguleres av anskaffelsesloven[11] med tilhørende forskrifter, herunder forskrift om offentlige anskaffelser[12] (FOA) og forskrift om forsvars- og sikkerhetsanskaffelser[13] (FOSA).

Formålet med regelverket er å bidra til økt verdiskapning i samfunnet ved å sikre mest mulig effektiv ressursbruk ved offentlige anskaffelser basert på forretningsmessighet og likebehandling, jf. anskaffelsesloven § 1.

FOSA gjennomfører EUs direktiv om forsvars og sikkerhetsanskaffelser i norsk rett. Direktivet har som formål å etablere en ny europeisk lovgivningsramme for inngåelse av sensitive offentlige kontrakter på forsvars- og sikkerhetsområdet. Direktivet er ment å skape mer åpenhet omkring anskaffelsene på dette området.

---

7 Ibid., 51.
8 Ibid., 63.
9 Ibid., 77.
10 Ibid., 65.
11 Lov 16. juli 1999 nr. 69 om offentlige anskaffelser (anskaffelsesloven).
12 Forskrift 7. april 2006 nr. 402 om offentlige anskaffelser (FOA).
13 Forskrift 4. oktober 2013 nr. 1185 om forsvars- og sikkerhetsanskaffelser (FOSA).

Felles for regelverket om offentlige anskaffelser er at det som utgangspunkt kun gjelder for statlige, kommunale og fylkeskommunale myndigheter og offentligrettslige organer, jf. loven § 2. Regelverket får således ikke anvendelse for selvstendige rettssubjekter, eksempelvis private virksomheter, som ikke omfattes av loven § 2.

Loven gjelder ikke for anskaffelser som kan unntas etter EØS-avtalen artikkel 123, jf. § 4.

Om forholdet mellom regelverket for offentlige anskaffelser og sikkerhetslovens bestemmelser om sikkerhetsgraderte anskaffelser, skriver Forsvarsdepartementet i Prop. 97 L (2015–2016) at:

> [f]or offentlige oppdragsgivere må regelverket om sikkerhetsgraderte anskaffelser sees i sammenheng med regelverket for offentlige anskaffelser. En sikkerhetsgradert anskaffelse er i utgangspunktet omfattet av [anskaffelsesloven] og [forskrift om forsvars- og sikkerhetsanskaffelser]. Nevnte lov og forskrift gjelder imidlertid ikke der en anskaffelse kan unntas med hjemmel i EØS-avtalen artikkel 123.[14]

11.3.2 Sektorspesifikt anskaffelsesregelverk

I *kraftsektoren* har energiloven og beredskapsforskriften egne bestemmelser om anskaffelser i energiforsyningen. Det følger av beredskapsforskriften § 6-5 at KBO-enheter som setter ut oppdrag til leverandører og andre med oppdrag for eller i energiforsyningen, skal påse at disse er forpliktet til å etterleve bestemmelsene om informasjonssikkerhet og taushetsplikt for sensitiv informasjon. Beredskapsmyndigheten[15] fører tilsyn med etterlevelsen av disse bestemmelsene også overfor leverandørene. I medhold av forskriften § 6-6 kan anbudsinnbydelser og lignende begrenses når det er nødvendig for å hindre at sikkerhetsgradert eller sensitiv informasjon om energiforsyningen blir offentlig tilgjengelig gjennom anbudsdokumentene.

I *finanssektoren* har finanstilsynsloven § 4 c nærmere bestemmelser om meldeplikt til Finanstilsynet ved utkontraktering av virksomhet. Finanstilsynet kan sette vilkår for utkontrakteringen eller gi foretaket pålegg om å ikke iverksette eller å avslutte oppdraget, dersom tilsynet finner at utkontraktering skjer i et omfang eller på en måte som ikke kan anses forsvarlig, vanskeliggjør tilsynet, eller for øvrig er i strid med bestemmelser gitt i eller i medhold av lov.

11.4 Utvalgets vurderinger

Etter utvalgets vurdering er det fortsatt behov for regelverk for sikkerhetsgraderte anskaffelser. Regelverket er et viktig virkemiddel for å kunne sikre at leverandører til virksomheter av kritisk betydning for *grunnleggende nasjonale funksjoner*, sikkerhetsmessig er til å stole på. Regelverket for sikkerhetsgraderte anskaffelser bør således gjelde for alle virksomheter som omfattes av loven.

Utvalget støtter det vedtatte lovforslaget med endring fra oppdragsbasert til tidsbasert leverandørklarering. Endringen vil, slik utvalget ser det, være et viktig bidrag for å effektivisere prosessene knyttet til sikkerhetsgraderte anskaffelser. Endringen medfører også at regelverket er mer i tråd med hvordan dette er regulert i andre sammenlignbare nasjoner. For norske leverandører vil en tidsbasert leverandørklarering også gjøre det lettere å konkurrere om oppdrag på det internasjonale markedet.

Utvalget støtter også innretningen på den foreslåtte bestemmelsen om anskaffelser til kritisk infrastruktur. Innretningen med at virksomhetene plikter å gjennomføre en risikovurdering ved anskaffelser er, slik utvalget ser det, også i tråd med den innretning utvalget har på forslaget til ny sikkerhetslov. De øvrige endringene utvalget foreslår, særlig når det gjelder de foreslåtte mekanismene om deling av trusselinformasjon, også sette virksomhetene i bedre stand til å kunne gjøre en forsvarlig risikovurdering ved slike anskaffelser.

Utvalget mener imidlertid at plikten til å gjøre risikovurderinger, må avgrenses til de virksomheter som faktisk omfattes av loven, det vil si de virksomheter som råder over *skjermingsverdige objekter* eller *skjermingsverdig infrastruktur*. Utvalgets forslag til utvidelse av lovens virkeområde, vil medføre at virksomheter som råder over infrastruktur av kritisk betydning for grunnleggende nasjonale funksjoner vil bli underlagt loven. Hvorvidt dette innebærer at alle virksomheter som er ment å omfattes av den foreslåtte § 29 a, også omfattes av bestemmelsen i utvalgets lovforslag, vil avhenge av hvilke vurderinger departementene og Sikkerhetsmyndigheten gjør når det gjelder vedtak overfor virksomheter som skal underlegges loven.

---

[14] Prop. 97 L (2015–2016), 48.

[15] Norges vassdrag- og energidirektorat (NVE).

Kapittel 12
Eierskapskontroll

12.1 Innledning

I henhold til utvalgets mandat skal utvalget:

> …vurdere behov for regulering/kontroll overfor selskaper som håndterer informasjon, teknologi og/eller fysiske aktiva av betydning for samfunnets sikkerhet, herunder håndteringen av endringer i statens eller andres eierskap i slike selskaper. Dette kan være selskaper innen forsvarssektoren eller i sivil sektor.

Stadig større deler av det som tradisjonelt utgjorde en integrert del av statens virksomhet, og som således lå innenfor alminnelig instruksjonsmyndighet og kontroll, ivaretas i dag av selvstendige rettssubjekter. Grunnleggende nasjonale funksjoner er derfor i økende grad avhengig av understøttelse fra private selskaper for å kunne opprettholde evnen til å ivareta sine oppgaver. Dette kan føre til en økt sårbarhet for grunnleggende nasjonale funksjoner. For private selskaper, hvor staten ikke har eierinteresser som sikrer en viss grad av kontroll, eksisterer det i dag ingen hjemmel for en generell kontroll med eierskapet i selskapene.

Utvalgets målsetting er å sikre at staten har tilstrekkelige og riktige virkemidler for å kunne regulere selskaper som håndterer informasjon, teknologi eller fysiske aktiva av kritisk betydning for grunnleggende nasjonale funksjoner. En grunnleggende forutsetning for utvalget i denne sammenheng, er at de virkemidler som gjøres tilgjengelig for staten ikke samtidig i vesentlig grad innskrenker selskapenes muligheter til å konkurrere i et globalt marked.

En grunnleggende problemstilling i denne sammenheng er hvorvidt eksisterende regelverk, både dagens sikkerhetslov og regelverk på tilgrensende områder, gir tilstrekkelige virkemidler for å kunne håndtere denne sårbarheten.

En annen grunnleggende problemstilling er hvorvidt en generell hjemmel for å kontrollere eierskapet i slike selskaper, vil få den tilsiktede effekt – uten at dette samtidig får uforholdsmessig store konsekvenser for selskapenes konkurransedyktighet.

12.2 Gjeldende rett

Det finnes en rekke regelverk som har til hensikt å kontrollere eierskapet i norske selskaper. Ingen av regelverkene har imidlertid som formål å hjemle en generell kontroll med eierskapet i strategisk viktige selskaper.

Konkurranseloven[1] har som formål å fremme konkurranse for derigjennom å bidra til effektiv bruk av samfunnets ressurser. Konkurransetilsynet kan i medhold av konkurranseloven § 16 forby foretakssammenslutninger som vil føre til eller forsterke en vesentlig begrensning av konkurransen i strid med lovens formål. Konkurranseloven § 17 gir nærmere bestemmelser om Konkurransetilsynets myndighet vedrørende fusjonskontroll gjennom å definere hva som utgjør en foretakssammenslutning. En av formene for foretakssammenslutning er gjennom et såkalt kontrollerverv, jf. § 17 annet ledd. Kontroll defineres i § 17 tredje ledd som «mulighet til å utøve avgjørende innflytelse over et foretaks virksomhet».

Børsloven[2] har som formål å legge til rette for effektive, velordnede og tillitvekkende markeder for finansielle instrumenter, jf. børsloven § 1. Loven § 17 gir nærmere bestemmelser om eierkontroll i regulert marked som ikke er børs. Erverv som fører til at erververen kan bli eier av en betydelig eierandel i slike markeder, kan bare gjennomføres etter at melding om dette på forhånd er sendt til Finanstilsynet. Med betydelig eierandel menes i denne sammenheng direkte eller indirekte eierandel som representerer minst

---

1 Lov 5. mars 2012 nr. 12 om konkurranse mellom foretak og kontroll med foretakssammenslutninger (konkurranseloven).

2 Lov 29. juni 2007 nr. 74 om regulerte markeder (børsloven).

Boks 12.1 Utstyrsdiversitet

Det digitale sårbarhetsutvalget har i sin utredning påpekt at manglende diversitet i utstyrsleverandørmarkedet innen ekominfrastrukturen er en kilde til sårbarhet. Konkurranselovgivningen vil i noen grad kunne bidra til å forhindre monopolleverandører, men Sårbarhetsutvalget mener at denne lovgivningen ikke i tilstrekkelig grad har klart å forhindre at det er en ensidighet i visse utstyrsleverandører.

Sårbarhetsutvalget har i denne forbindelse anbefalt at Nkom, i samråd med Konkurransetilsynet, bør ta initiativ til å utrede hvorvidt man i dag har tilstrekkelige virkemidler for å ivareta dette forholdet. Det blir også vist til at denne problemstillingen bør tas med i utformingen av ny sikkerhetslov.

Nkom har i sin høringsuttalelse, datert 15. mars 2016, uttalt at konkurranselovgivningen ikke er egnet til å oppnå formålet hva gjelder utstyrsdiversitet. Nkom støtter forslaget om at problemstillingen bør tas med i utformingen av ny sikkerhetslov.

Kilde: NOU 2015: 13, 115.

10 prosent av aksjekapitalen eller stemmene, eller på annen måte gjør det mulig å utøve betydelig innflytelse over forvaltningen av selskapet, jf. loven § 17 første ledd annet punktum. Finanstilsynet kan nekte slikt erverv dersom aksjeeier ikke anses egnet til å sikre en god og fornuftig forvaltning av foretaket, jf. § 17 tredje ledd.

Industrikonsesjonsloven[3] har som formål at landets vannkraftressurser skal forvaltes til beste for allmennheten. Dette skal sikres gjennom offentlig eierskap på statlig, fylkeskommunalt og kommunalt nivå, jf. industrikonsesjonsloven § 1 første ledd. Etter industrikonsesjonsloven § 2 kan private eie kraftproduksjon så lenge det offentlige «direkte eller indirekte innehar minst to tredeler av kapitalen og stemmene og organiseringen er slik at det åpenbart foreligger reelt offentlig eierskap» (konsolideringsmodellen). Industrikonsesjonslovens bestemmelser om åpenbart reelt offentlig eierskap legger en klar restriksjon på mulighetene for å selge kraftproduksjon til private (herunder utenlandske) eiere.

[3] Lov 14. desember 1917 nr. 16 om erverv av vannfall mv. (industrikonsesjonsloven).

Det finnes i tillegg regelverk av sektorovergripende karakter, som har elementer av kontroll med eierskap, men da knyttet til leverandører i konkrete anskaffelser og ikke til strategisk viktige selskaper som sådan.

Sikkerhetsloven kapittel 7 om sikkerhetsgraderte anskaffelser regulerer anskaffelser hvor leverandøren kan få tilgang til skjermingsverdig informasjon eller skjermingsverdig objekt, jf. sikkerhetsloven §§ 27 og 28. I forbindelse med en leverandørklarering plikter den aktuelle leverandøren å gi alle opplysninger som antas å være av betydning for klareringsspørsmålet. I dette ligger også et krav om at leverandøren plikter å opplyse om blant annet eierstruktur. Leverandøren skal også uten ugrunnet opphold orientere Nasjonal sikkerhetsmyndighet om endringer i styre eller ledelse, forandringer i eierstrukturen, flytting av lokaliteter og utstyr etc., jf. § 28 fjerde ledd. Regelverket er imidlertid avgrenset til konkrete anskaffelser, og er således mindre egnet for å ivareta mer generelle behov for kontroll med eierskapet i strategisk viktige selskaper. For en mer utførlig omtale av regelverket for sikkerhetsgraderte anskaffelser vises det til kapittel 11.

Regjeringens forslag til innføring av en lovbestemmelse om varslingsplikt og myndighet til å fatte vedtak ved anskaffelser til kritisk infrastruktur, se omtalen av § 29 a i kapittel 11.2.4, foreslås i det vesentlige videreført i utvalgets lovforslag.

Som nevnt i kapittel 11.3.2 har kraftsektoren en egen regulering av anskaffelser til energiforsyningen. Det følger av beredskapsforskriften § 6-6 at anbudsinnbydelser og lignende skal begrenses når det er nødvendig for å hindre at sikkerhetsgradert eller sensitiv informasjon om energiforsyningen blir offentlig tilgjengelig gjennom anbudsdokumentene.

12.2.1 Tidligere lov om erverv av næringsvirksomhet

12.2.1.1 Ervervsloven

Norge hadde frem til EØS-avtalens ikrafttredelse konsesjonslovgivning om godkjenning av eierskifte, som diskriminerte mellom norske og utenlandske statsborgere.

Etter at Norge sluttet seg til EØS-avtalen, var det ikke lenger lovlig å opprettholde et diskriminerende regelverk hvor bare utenlandske bedriftsoppkjøp i Norge krevde konsesjonsbehandling. Dette, i tillegg til at det gamle konsesjonsregelverket var blitt utdatert, medførte behov

Boks 12.2 Historikk

Frem til 1888 hadde både utlendinger og norske statsborger fri tilgang til å erverve eiendomsrett og bruksrett til fast eiendom i Norge. Fra 1888 kom den første konsesjonsloven – statsborgerrettsloven – som innførte en generell konsesjonsplikt for utenlandske personer og selskap som ervervet norsk eiendom. Loven var begrunnet i frykten for at fremmede land og statsborgere skulle kjøpe opp store områder i Norge. Etter hvert ble også ønsket om å bevare viktige naturressurser som vannfall, mineralforekomster og skogseiendommer en viktig motivasjon for lovgivningen.

Etter en omfattende lovrevisjonsprosess i 1917 ble konsesjonsreglene strammet inn gjennom en ny konsesjonslov (industrikonsesjonsloven). En viktig endring var at erverv av aksjer og andeler i selskap ble underlagt konsesjonsplikt dersom selskapene hadde eiendomsrett eller bruksrett som medførte konsesjonsplikt ved direkte erverv. Konsesjonsplikten gjaldt kun for utenlandske rettssubjekter som ervervet fast eiendom.

I 1974 ble industrikonsesjonsloven erstattet av en ny allmenn konsesjonslov.

for å utvikle et nytt og moderne regelverk som var bedre tilpasset reguleringsbehovet vedrørende eierskifte i næringslivet. Resultatet av denne prosessen var *ervervsloven*[4] som trådte i kraft 1. januar 1995.

Ervervsloven gjaldt for erverv av eiendeler i norske foretak, samt erverv av aktiva som innebar overtakelse av næringsvirksomhet i Norge, jf. loven § 1 første ledd. Ervervsloven har ikke et klart definert formål, verken i loven eller i forarbeidene. Det følger av forarbeidene at loven først og fremst var ment å dekke de behovene myndighetene hadde for kontroll på og styring med eierskifte i norsk næringsliv, være preventiv overfor useriøse investorer, bidra til å vedlikeholde sysselsetting og bosetting i distriktene, samt sikre informasjon om eierstrukturene i norsk næringsliv.[5]

Ervervsloven var basert på et meldepliktsystem, hvor de som ervervet eiendeler i et norsk foretak hadde meldeplikt avhengig av omfanget på oppkjøpet. Meldeplikten gjaldt både for nasjonale og utenlandske oppkjøpere. Meldeplikten inntrådte ved erverv som medførte at erververen ble innehaver av «mer enn en tredel eller minst en halvdel, eller minst to tredeler av samtlige eierandeler eller av stemmeberettigede eierandeler», jf. loven § 4 første ledd. Meldeplikten ble bare utløst i de tilfeller der foretaket hadde:

- over 50 tilsatte, eller
- en omsetning siste år på over 50 millioner kroner, eller
- mottatt offentlig støtte til forskning og utvikling på over 5 millioner kroner til minst et enkeltprosjekt gjennom de siste åtte årene.

Oppkjøpet skulle meldes til departementet innen 30 dager etter at bindende avtale om erverv var inngått, jf. loven § 9. Etter at oppkjøpet var meldt til departementet, hadde departementet en frist på 30 dager til å vurdere ervervet, jf. loven § 10. Dersom departementet ikke ga skriftlig melding om behov for ytterligere informasjon eller at oppkjøpet ville bli underlagt nærmere vurdering etter loven kapittel 6, innen fristen på 30 dager, ble oppkjøpet ansett som godkjent.

Dersom departementet hadde grunn til å anta at oppkjøpet kunne ha vesentlige negative virkninger for foretaket, bransjen eller samfunnet for øvrig, herunder sysselsettingsmessige virkninger, kunne oppkjøpet undergis nærmere vurdering, jf. § 13. Med mindre allmenne hensyn talte imot, skulle oppkjøpet godkjennes. Dersom godkjenning ikke ble gitt, kunne departementet pålegge oppkjøperen å avhende de eierandeler eller aktiva det meldepliktige oppkjøpet omhandlet innen en nærmere angitt frist, jf. § 17.

Etter loven kapittel 7 hadde departementet også hjemmel til å fastsette nærmere bestemte vilkår som av allmenne hensyn var nødvendig for at oppkjøpet skulle kunne godkjennes.

Brudd på de plikter som påhvilte erverver etter loven var sanksjons- og straffebelagt etter loven kapittel 8. Brudd på meldeplikten, fristoversittelse eller nekting av erverv kunne sanksjoneres etter loven § 19, herunder ileggelse av tvangsmulkt, pålegg om salg og gjennomføring av tvangssalg. Avgivelse av uriktige og/eller ufullstendige opplysninger kunne sanksjoneres etter § 20. Ved brudd på vilkår etter loven kapittel 7, kunne departementet ilegge tvangsmulkt inntil forholdet ble brakt i orden, jf. § 21. Forsettlig eller uaktsom overtredelse av loven var også straffbelagt med bøter, jf. loven § 22.

---

4 Lov 23. desember 1994 nr. 79 om erverv av næringsvirksomhet (ervervsloven).

5 Ot.prp. nr. 62 (2001–2002) om lov om oppheving av lov om erverv av næringsverksemd, 10.

12.2.1.2 Opphevelsen av ervervsloven

I Ot.prp. nr. 62 (2001–2002) fremmet Nærings- og fiskeridepartementet forslag om å oppheve ervervsloven. En forutgående evaluering av loven hadde vist at det reelle behovet for å kontrollere eierskifte var lite fordi det sjelden var knyttet dramatiske endringer til slike skifter. Det ble vist til at de strukturelle endringene i næringslivet først og fremst skjedde som følge av endringer i markedsforhold og lignende, og uavhengig av eierskifte.

Departementet hadde siden lovens ikrafttredelse og frem til 31. desember 2001 mottatt melding om til sammen 2147 erverv. Av disse meldepliktige ervervene hadde 13 erverv vært oppe til nærmere prøving etter loven kapittel 6. Ingen av disse hadde resultert i at godkjenning ble nektet. For åtte av sakene ble det stilt vilkår for godkjenningen.

Etter departementets vurdering var det ikke lenger et reelt behov for norske myndigheter å kontrollere eierskifte i norsk næringsliv. Loven hadde ikke vært et effektivt virkemiddel for å sikre næringsvirksomhet i Norge, slik intensjonen med loven var. Departementet pekte videre på at loven hadde utspilt sin rolle i dagens samfunn med fri flyt av både kapital, virksomhet og arbeidskraft på tvers av landegrensene. En særnorsk regulering på dette feltet kunne etter departementets oppfatning ikke sies å ha hatt de ønskede virkningene, verken for norske myndigheter eller for norsk næringsliv, inkludert norske arbeidstakere.

Departementet viste også til at loven hadde medført et unødvendig byråkrati, og at den skapte uforutsigbarhet for eventuelle investorer. I tillegg påførte loven norsk næringsliv både direkte og indirekte kostnader.

Departementet viste til at ervervsloven i noen utstrekning hadde blitt benyttet til å få informasjon om eierens planer med selskaper, og dermed beredskapssituasjonen. Det ble imidlertid lagt til grunn at loven primært ikke hadde dette formålet. Andre hensyn som loven delvis hadde dekket, mente departementet kunne ivaretas uten ervervsloven. Hva gjaldt hensynet til sikkerhet og beredskap, vurderte departementet at dette ikke var den avgjørende grunnen for å etablere ervervsloven:

> På bakgrunn av høyringssvara meiner departementet at det ut frå beredskaps- og tryggleiksomsyn ikkje er komme fram avgjerande grunnar som tilseier at ervervslova ikkje kan opphevast. Departementet viser til at beredskapsaspektet ikkje var den avgjerande grunnen til å etablere ervervslova. Ervervslova vil derfor langt frå vere noko fullgodt alternativ når ein skal løyse problematikken som høyringsinstansane peiker på. Slike omsyn bør, slik FO/S og DSB tek til orde for, i staden innarbeidast i og bli tatt omsyn til i samband med ein framtidig revisjon av tryggleiks- og beredskapsregelverket. Departementet meiner derfor at det ikkje føreligg tungtvegande grunnar til å avvente opphevinga av ervervslova til anna regelverk på området er komme til.[6]

Stortinget opphevet loven med virkning fra 1. juli 2002.[7]

Boks 12.3 EFTAs åpningsbrev til Norge

EFTAs overvåkningsorgan (EFTA Surveillance Authority (ESA)) sendte den 24. mars 2000 et såkalt åpningsbrev til Norge, hvor det ble hevdet at ervervsloven var i strid med EØS-avtalen. ESA hevdet at det hadde skjedd en utvikling innenfor EF-retten, og at det måtte innfortolkes et rent diskrimineringsforbud i EØS-avtalen artikkel 31 og 40. Et restriksjonsforbud omfattet også nasjonale, ikke-diskriminerende regler som hindret eller gjorde det vanskelig å utøve de grunnleggende frihetene, blant annet etablering og fri flyt av kapital. Slike nasjonale regler kunne etter ESAs oppfatning bare godtas dersom de var begrunnet med tvingende allmenne hensyn, og dersom de ikke var i strid med proporsjonalitetsprinsippet.

Norge hevdet i sitt svarbrev til ESA at EØS-reglene ikke forbød andre restriksjoner enn de som innebærer forskjellsbehandling på bakgrunn av nasjonalitet. Det ble videre hevdet at dersom det ble lagt til grunn at det forelå et restriksjonsforbud etter artikkel 31 og 40, så kunne ervervsloven begrunnes i tvingende allmenne hensyn.

Ervervsloven ble opphevet før ESA konkluderte i saken.

---

6 Ibid., 26.

7 Besl.O. nr. 80 (2001–2002), jf. Innst. O. nr. 72 (2001–2002) og Ot.prp. nr. 62 (2001–2002).

12.3 Fremmed rett

12.3.1 Innledning

En rekke nasjoner har regler om myndighetskontroll med investeringer i landet ut fra sikkerhetsmessige hensyn. Hvilke typer virksomheter som er gjenstand for kontroll er i varierende grad angitt i de enkelte nasjoners regelverk. Noen nasjoner praktiserer frivillig melding til myndighetene, mens andre pålegger erververen meldeplikt dersom nærmere vilkår er oppfylt.

I den videre fremstillingen gis en oversikt over relevant regelverk i USA, Storbritannia, Canada, Frankrike og Finland. Danmark og Sverige har ikke regelverk som regulerer denne type myndighetskontroll, men omtales kort nedenfor. Fremstillingen er basert på en rapport fra Advokatfirmaet Wikborg, Rein & Co til Sikkerhetsutvalget.[8]

12.3.2 USA

12.3.2.1 Kontroll av utenlandske investeringer i nasjonale virksomheter – CFIUS

I USA fører *Committe on Foreign Investment in the US* (CFIUS) (heretter også benevnt som Komiteen), kontroll med transaksjoner som medfører kontrollovertakelse. Lovgrunnlaget for CFIUS sin virksomhet består av *Defense Production Act (1950) Section 721, Executive Order 11858, Foreign Investment and National Security Act (FINSA)* og *CFR Part 800* (heretter kalt Part 800).

Komiteen vurderer om kontrollovertagelsen vil kunne true nasjonal sikkerhet. I den grad det er tilfellet, skal transaksjonen forbys med mindre det lar seg gjøre å fremforhandle en avtale med partene som løser problemet. Det er frivillig å inngi melding til Komiteen, men Komiteen kan gripe inn på eget initiativ og pålegge vilkår eller forby kontrollovertagelsen.

I de tilfellene der det ikke inngis frivillig melding er CFIUS avhengig av å få kunnskap om relevante transaksjoner på andre måter. Dette skjer ved at CFIUS sjekker pressemeldinger, meldinger til *Securities and Exchange Commission* og andre offentlige notifikasjoner og meldinger til offentlige myndigheter for å få en oversikt over transaksjoner som er gjennomført eller som planlegges.

12.3.2.2 Relevante transaksjoner

Hvilke typer transaksjoner som er gjenstand for kontroll er regulert i Part 800, Subpart C, § 800.301. Transaksjoner som rammes er:

a) en transaksjon som medfører eller kan medføre at en *U.S business* (heretter *nasjonal virksomhet*) blir kontrollert av en utenlandsk person,
b) en transaksjon som innebærer at en utenlandsk person overdrar sin kontroll over en nasjonal virksomhet til en annen utenlandsk person,
c) en transaksjon som medfører eller kan medføre at en utenlandsk person får kontroll over en del av en virksomhet (*entity*) eller av en eiendel (*assets*), så fremt denne utgjør en nasjonal virksomhet, og
d) et *joint venture* eller lignende, der en av partene kommer inn med en nasjonal virksomhet og en utenlandsk person kan kontrollere den nasjonale virksomheten gjennom *joint venturet*.

Lån eller lignende til en nasjonal virksomhet omfattes i utgangspunktet ikke, med mindre låneforholdet kan foranledige kontrollovertagelse, eksempelvis der lånet er konvertibelt eller der långiver vil kunne overta virksomheten/eiendeler ved mislighold, jf. §§ 800.303 og 800.304, jf. § 800.206.

En transaksjon er i § 800.224 definert som en foreslått eller gjennomført foretakssammenslutning, erververse eller overtakelse (*takeover*). Det kan gjelde eierskapsinteresser, erververse av stemmeandeler, fullmakt fra en person med stemmeandeler, foretakssammenslutning eller konsolidering, opprettelse av *joint venture* og langvarige leasingavtaler hvor leietaker i det vesentlige treffer alle forretningsmessige beslutninger som gjelder driften av den leasede enheten.

Det er *kontrollendringer* i nasjonal virksomhet som omfattes. Hva som utgjør en nasjonal virksomhet er definert i Part 800 § 800.226. Enhver *enhet* som er involvert i handel mellom statene i USA omfattes, men det gjelder kun den delen av virksomheten som er involvert i slik handel.

En *enhet* er nærmere definert som enhver filial, avdelingskontor eller underavdeling, kompaniskap, forening, eiendom/bo, fond, selskap eller del av et selskap eller organisasjon (uansett hvilket lands lov den er underlagt), jf. § 800.211. Videre omfattes aktiva, uavhengig av om det er skilt ut som egen juridisk enhet, som drives av en

[8] Wikborg, Rein & Co, *Oversikt over utenlandsk lovgivning om myndighetskontroll med endret eierskap over virksomheter som håndterer informasjon, teknologi og/eller fysiske aktiva av betydning for samfunnets sikkerhet; EØS-rettslige skranker for innføring av tilsvarende regler i Norge*, elektronisk vedlegg 2.

Boks 12.4 National Industrial Security Program

USA har også et nasjonalt sikkerhetsprogram (*National Industrial Security Program* (NISP)) som har til formål å beskytte hemmeligstemplet eller sensitiv informasjon som personell får tilgang til i sitt arbeid med kontrakter, programmer, anbud eller forsknings- og utviklingsprosjekter for amerikanske myndigheter. Programmet foreskriver et samarbeid mellom myndighetene og private aktører, og er etablert i medhold av Executive Order 12829 section 6. NISP forvaltes av *Defense Security Service* (DSS), en etat under USAs forsvarsdepartement. I vurderingen av om et selskap skal få tilgang til hemmeligstemplet eller sensitiv informasjon, foretar DSS en *Facility Security Clearance* (leverandørklarering).

Virksomheter der utenlandske personer har eierinteresser reguleres av FOCI-retningslinjene (*Foreign Ownership, Control or Influence*). Følgende virksomheter omfattes av regelverket:

a) nasjonale selskaper der en utenlandsk person har interesser (i form av eierskap eller på annen måte), og
b) vedkommende har direkte eller indirekte adgang til å bestemme eller styre et selskaps virksomhet på en måte som kan medføre at uvedkommende kan få tilgang til hemmeligstemplet informasjon, eller som kan påvirke utførelsen av en hemmeligstemplet kontrakt.

Selskaper som omfattes av regelverket får i utgangspunktet ikke sikkerhetsklarering og vil dermed ikke kunne inngå i NISP. Selskapet kan imidlertid treffe tiltak for likevel å få sikkerhetsklareringen, såkalte *mitigation instruments*, eksempelvis gjennom overføring av stemmeandeler til en amerikansk statsborger.

Det ovennevnte regelverk og prosedyrene for klarering foregår i utgangspunktet parallelt med kontrollen av utenlandske investeringer i nasjonale virksomheter, og det er tale om to separate regelverk med selvstendig og separat håndheving. Imidlertid vil CFIUS i praksis legge vekt på eventuelle tiltak som selskapet har iverksatt for å oppnå sikkerhetsklarering i sin vurdering. Tiltak som er godkjent under FOCI kan være avgjørende for om CFIUS klarerer transaksjonen, og det er anbefalt å gjennomgå NISP- og FOCI-prosessen før transaksjonen meldes til CFIUS.

av de forannevnte som et foretak på en bestemt lokalitet eller som leverer bestemte produkter eller tjenester. Som enhet regnes også enhver myndighet (herunder utenlandsk eller amerikansk myndighet eller lokale myndigheter og deres respektive departementer, etater og virksomheter).

Dette innebærer at reglene favner svært vidt, og det avgjørende er ikke virksomhetens organisering eller hvilket lands lover den er underlagt, men hvorvidt den driver handel eller virksomhet innenfor USA. Det er heller ikke noe krav at det gjelder virksomhet innenfor bestemte bransjer.

Det er kun transaksjoner der en utenlandsk person kan oppnå kontroll i den ovennevnte nasjonale virksomhet som omfattes.

Utenlandsk person er definert i § 800.216 som enhver utlending, utenlandsk myndighet eller utenlandsk enhet, eller enhver enhet som en utlending, utenlandsk myndighet eller utenlandsk enhet har kontroll over.

12.3.2.3 Kontrollbegrepet

Kontrollbegrepet reguleres nærmere i Part 800 § 800.204. Hvorvidt det foreligger kontroll beror ikke alene på eierandel eller antall styremedlemmer, men på om man har makt til å bestemme («*the power (…) to determine, direct, or decide*») i viktige saker (*important matters*), som nærmere eksemplifisert i bestemmelsen. Bestemmelsen lister også opp diverse vetorettigheter som i seg selv ikke vil være tilstrekkelig til å gi en mindretallsaksjonær kontroll, jf. bestemmelsens bokstav c. Andre former for minoritetsvern vil bli vurdert konkret (bokstav d).

Bestemmelsen minner mye om kontrollbegrepet i norsk konsernrett med den forskjellen at lovgiver, i stedet for å overlate til praksis og domstolene å fastlegge dens nærmere innhold, har tatt stilling til hvorvidt en rekke typeeksempler skal omfattes eller ikke.

12.3.2.4 Vurdering av inngrepsbehov: Momenter

De overordnede vurderingstemaene for hvorvidt en transaksjon bør vurderes nærmere og eventuelt forbys eller tillates på vilkår, er i henhold til § 800.501:

a) om en utenlandsk person kan komme til å overta kontrollen i en nasjonal virksomhet,
b) om det godtgjøres (*credible evidence*) at en utenlandsk person med kontroll over en slik nasjonal virksomhet kan tenkes å ville utføre handlinger som vil kunne true nasjonal sikkerhet, og
c) om nasjonal lovgivning, foruten Section 721 og *the International Emergency Economic Powers Act*, gir tilstrekkelig beskyttelse mot den potensielle trusselen/faren.

Det følger videre av § 800.503 at meldte transaksjoner skal undersøkes nærmere dersom de omfattes av § 800.301 (jf. kapittel 12.3.2.2), og et medlem av Komiteen mener de truer nasjonal sikkerhet, eller den aktuelle fagetaten (*lead agency*) anbefaler undersøkelse. Transaksjonen skal alltid undersøkes nærmere hvis den vil medføre at kontroll overtas av en utenlandsk myndighet eller dersom den vil medføre at en utenlandsk person får kontroll over kritisk infrastruktur (*critical infrastructure*).

Kritisk infrastruktur er definert i § 800.208 som et system eller eiendel (*asset*), fysisk eller virtuelt, som er så vesentlig eller nødvendig for USA at funksjonssvikt eller ødeleggelse vil svekke nasjonal sikkerhet.

Øvrige faktorer som *kan* tas i betraktning i vurderingen av om nasjonal sikkerhet trues, er detaljert opplistet i Section 721, (f) og omfatter blant annet produksjon i USA som er nødvendig for Forsvaret; nasjonal industris evne og kapasitet til å dekke Forsvarets behov; betydningen av utenlandske personers kontroll av nasjonal industri og kommersiell aktivitet for USAs evne og kapasitet til å ivareta nasjonal sikkerhet etc.

Ovennevnte regler suppleres av CFIUS' egne retningslinjer for saksbehandlingen. Av disse fremgår det at den *nasjonale virksomhetens art* og den *utenlandske personens identitet* skal tas i betraktning i vurderingen av hvorvidt nasjonal sikkerhet kan bli truet som følge av transaksjonen.

12.3.2.5 Saksbehandlingen

CFIUS vurderer hvorvidt en transaksjon omfattes av regelverket og hvorvidt det bør treffes tiltak, jf. § 800.501 og FINSA section 5. Det følger også av sistnevnte at en utpekt underenhet kan gjøre vurderingen på vegne av Komiteen. CFIUS hadde på et tidspunkt etter 2007 hele ni underliggende enheter. Komiteen ledes formelt av finansministeren, og består for øvrig av en rekke relevante ministre og etatsledere. Komiteen skal møtes i henhold til presidentens pålegg eller ved innkalling fra møteleder.

Presidenten skal forelegges en rapport dersom Komiteen mener at transaksjonen bør utsettes eller forbys, dersom Komiteen er i tvil eller ikke klarer å treffe en beslutning eller dersom Komiteen ønsker at presidenten tar beslutningen.

Selskaper som skal gjennomføre en transaksjon kan gi frivillig melding til Komiteen.

Transaksjoner som ikke notifiseres ved frivillig melding kan bli fanget opp gjennom Komiteens egne undersøkelser. Dersom Komiteen etter slike undersøkelser oppdager en transaksjon som Komiteen anser for å være omfattet av regelverket, og Komiteen har grunn til å tro at transaksjonen kan ha betydning for nasjonal sikkerhet, kan Komiteen kreve (*request*) nødvendig informasjon fra partene. Dersom Komiteen basert på mottatt informasjon kommer til at transaksjonen bør meldes, kan Komiteen kreve at det inngis melding, jf. § 800.401. Partene har da informasjonsplikt, jf. § 800.701, og dersom informasjonsplikten ikke overholdes, kan Komiteen innhente informasjonen ved stevning til retten eller med andre midler, jf. 50 U.S.C. App. 2155(a).

Det er klare regler for hva en melding skal inneholde for å kunne saksbehandles. Partene oppfordres til å kontakte Komiteen på forhånd, blant annet for å sørge for at meldingen inneholder all nødvendig informasjon, og for at Komiteen skal få oversikt over saken, jf. § 800.401. Innholdskravene er detaljerte og følger av § 800.402.

Fra og med beslutning om at meldingen oppfyller formkravene er tatt har Komiteen 30 dager på vurdere om transaksjonen skal undersøkes nærmere, jf. § 800.502 (b). Partene skal ha informasjon om at melding er inngitt og at undersøkelse er igangsatt, jf. § 800.503. Dersom Komiteen velger å undersøke transaksjonen nærmere, skal dette gjennomføres innen nye 45 dager, jf. § 800.506.

Komiteen kan i løpet av denne perioden fremforhandle avtale eller pålegge vilkår som partene i transaksjonen må oppfylle for å unngå svekkelse

av nasjonal sikkerhet. Avtale eller vilkår skal bygge på en risikobasert analyse foretatt av Komiteen, jf. Section 721 (I) (1) (A) og (B).

Presidenten skal forelegges en rapport dersom Komiteen mener at transaksjonen bør utsettes eller forbys, dersom Komiteen er i tvil eller ikke klarer å treffe en beslutning, eller dersom Komiteen for øvrig ønsker at presidenten tar beslutningen. Presidenten har 15 dager på å treffe en beslutning, jf. FINSA section 6.

Partene har anledning til å trekke meldingen etter nærmere bestemmelser i § 800.507. Det må blant annet søkes om Komiteens tillatelse til å trekke meldingen. Tillatelse kan gis på nærmere fastsatte vilkår etter Komiteens vurdering. Et eksempel er pålegg om prosedyrer som må gjennomføres for at Komiteen skal kunne følge med på sakens videre utvikling.

Ettersom det er frivillig å inngi melding, er det heller ikke noe formelt gjennomføringsforbud eller krav om forhåndsgodkjenning. Men ettersom myndighetene kan gripe inn på eget initiativ, må partene i en transaksjon selv vurdere risikoen for dette og planlegge transaksjonen deretter, herunder regulere risikoen for inngrep.

Det synes noe uklart i hvilken grad CFIUS' avgjørelser kan påklages. Regelverket gir ikke i seg selv anvisning på klagemuligheter. Men i en avgjørelse den 15. juli 2014 kom en domstol til at CFUIS' saksbehandling ikke ga partene tilstrekkelige kontradiksjonsmuligheter, og det ble da henvist til *5th Amendment* og dens bestemmelser om *due process*.

§ 800.801 gir CFIUS hjemmel for administrativ ileggelse av mulkt (*penalty*) ved grov uaktsom eller forsettlig inngivelse av uriktige eller mangelfulle opplysninger, og ved inngivelse av falsk fullmakt der dette er påkrevd. Brudd kan medføre bøter på opptil USD 250 000 per overtredelse.

Sanksjonene utelukker ikke at det i tillegg kan reageres etter andre sivile eller strafferettslige regler, jf. bestemmelsens bokstav g. Bøtene kan inndrives ved å reise sak for føderale domstoler, jf. bokstav f.

Etter Section 721 bokstav m er CFIUS pålagt å utgi en årlig rapport til Kongressen med statistikk og informasjon om hvem som har gitt melding, hvilke typer bransjer, meldinger som er trukket, vilkår og avtaler, samt en redegjørelse for pågående vurderinger av transaksjoner som kan ha betydning for utenlandske personers kontroll av nasjonale selskaper som driver med forskning og utvikling eller produserer kritisk teknologi.

Fra Komiteens årsrapport for 2013 følger det at det ble inngitt 97 meldinger som ble ansett som relevante transaksjoner og dermed gjenstand for nærmere vurdering. Av disse gjennomførte Komiteen etterfølgende undersøkelser i 48 av tilfellene. Fra 2011 til 2013 ble det avtalt eller pålagt vilkår i 27 av tilfellene.

Selskapenes overholdelse av avtaler og vilkår følges opp blant annet ved periodisk rapportering til myndighetene, besøk fra myndighetene, granskning gjennomført av tredjeparter, etterforskning og forebyggende tiltak ved mistanke om vilkårsbrudd.

12.3.3 Storbritannia

The Industry Act fra 1975 gir i Part II myndighetene hjemmel for å gripe inn ved utenlandsk kontrollovertagelse over viktige produksjonsvirksomheter (*important manufacturing undertakings*), forutsatt at overtakelsen er i strid med nasjonale interesser (Art. 13 (1) (b)). *Interesser* skal forstås som interesser knyttet til «*public policy, public security or public health*» (Art. 13 (7)).

Finner myndighetene grunn til å gripe inn, kan de forby, begrense eller fastsette vilkår for overtakelsen, jf. Art. 13 (1) (b) (i) og (ii), men i tillegg også selv overta eierskap til virksomheten (Art. 13 (2)). I sistnevnte tilfelle må det svares erstatning, jf. Art. 16 (6) og Art. 19. Avgjørelsen kan bringes inn for voldgift, jf. Art. 20.

Per oktober 2015 hadde myndighetene ennå ikke benyttet seg av muligheten til å gripe inn etter disse bestemmelsene.

The Enterprise Act fra 2002 angir i Part 3, Chapter 2, at myndighetene kan stoppe eller sette vilkår for sammenslåinger (*mergers*) og overtakelse av britiske selskaper, hvis transaksjonen må anses å stride mot offentlige interesser (*public interest consideration*), jf. Art. 42.

Slike offentlige interesser omfatter nasjonal sikkerhet, jf. Art. 42, jf. Art. 58, som igjen viser til *public security* som definert i EUs Fusjonsforordning (EC 139/2004) art. 21 (4).

Myndighetene kan videre gripe inn ved overtakelse av en enhet som har vært leverandør til myndighetene og som dermed er i besittelse av forsvarsrelatert informasjon, jf. Art 59 (1), jf. (2), (3) og (8). Ellers omfattes også tilfeller som etter myndighetenes egen oppfatning må anses å være en fare for offentlige interesser, jf. Art. 42 (3).

Bestemmelsen nevner ikke utenlandsk kontrollovertakelse spesifikt og tar i utgangspunktet sikte på å regulere foretakssammenslutninger utfra konkurranserettslige betraktninger. Men loven forstås slik at også utenlandske investerin-

ger i seg selv, kan utgjøre en trussel mot offentlige interesser.

Myndighetene har hittil grepet inn seks ganger med hjemmel i denne loven med henvisning til nasjonale sikkerhetsinteresser. Samtlige saker gjaldt hensynet til beskyttelse av militært sensitiv informasjon. Alle transaksjonene ble tillatt på vilkår, blant annet i form av krav knyttet til forsyningssikkerhet og beskyttelse av gradert informasjon.

Regelverket under *Entreprise Act 2002* forvaltes av *Competition and Markets Authority* (CMA) siden 2014 (før dette av *Office of Fair Trading (OFT)*). Transaksjoner som i beløp overstiger visse terskelverdier er meldepliktige. Men når det gjelder nasjonal sikkerhet, kan myndighetene gripe inn på eget initiativ mot transaksjoner uavhengig av transaksjonens størrelse.

Storbritannia praktiserer for øvrig kontroll over virksomheter gjennom *direkte eierskap av kontrollerende aksjeposter*, herunder såkalte *golden shares*, det vil si mindre aksjeposter med spesielle tilknyttede vedtektsfestede rettigheter. Gjennom slike poster kan myndighetene blant annet begrense størrelsen på andres aksjebeholdning i selskapet, blokkere utenlandsk overtakelse og kontrollere utnevnelsen av styremedlemmer. Praksisen med *golden shares* har vært kritisert og er redusert de siste årene.

12.3.4 Canada

Investment Canada Act (ICA) fra 1985 retter seg direkte mot utenlandske investeringer i Canada. Disse blir vurdert opp mot en generell *net benefit test*, og siden 2009 vurderes det i tillegg særskilt om investeringen kan være skadelig for nasjonal sikkerhet.

Reglene er inntatt i lovens Part IV.1 og får anvendelse når en investering gjøres av en *non-Canadian*, jf. definisjonen i lovens Art. 3. For selskaper synes essensen å være hvorvidt det er kontrollert (direkte eller indirekte) av kanadiske borgere. Det er således uten betydning at kjøperselskapet er et kanadisk selskap dersom det er eid av utlendinger. I tilfeller av spredt eierskap hvor det vil være vanskelig å fastslå fra hvilke land eierne kommer fra eller hvor virksomheten ikke kan sies å bli styrt av aksjonærene (eksempelvis børsnotert selskap uten noen dominerende aksjonærer), vil det være krav om at 2/3 av styremedlemmene må være kanadiske borgere for å gå klar av reglene.

Hvis investeringen gjøres av en *non-Canadian*, skal det sendes inn melding dersom det gjelder etablering av ny virksomhet eller ved overtakelse av kontroll over en kanadisk virksomhet, jf. lovens Art. 11. I sistnevnte tilfelle vil transaksjonen bli gjenstand for vurdering (*review*) dersom den beløpsmessig overstiger visse terskler. Terskelverdiene avhenger blant annet av om målselskapet er eller blir overtatt av en WTO-investor, eller av en statlig kontrollert investor, og av om det er en kulturrelatert virksomhet (*cultural business*), jf. loven Art. 14.

For så vidt gjelder utenlandsk statlig kontrollert investor er det gitt egne retningslinjer for saksbehandlingen. Det følger av disse at slike transaksjoner vil være gjenstand for visse tilleggsundersøkelser. Myndighetene vil således forsikre seg om at virksomheten vil bli drevet etter kommersielle prinsipper og basert på kanadiske prinsipper for god virksomhetsstyring (*corporate governance*).

Hva som utgjør kontrollovertakelse er utførlig regulert i Art. 28. Det er en presumsjon for kontrollovertakelse i tilfelle overtakelse av mellom 1/3 og 50 % av aksjene, med mindre det godtgjøres at dette ikke gir faktisk kontroll (*control-in-fact*). Dette vil være praktisk ved børsnoterte selskaper hvor største aksjonær har en slik aksjebeholdning. Indirekte kontrollovertakelse, herunder av utenlandsk morselskap, ser også ut til å være omfattet. Overtakelse av utenlandsk selskap med kanadisk avdeling som ikke er organisert som et selskap (muligens tilsvarende norsk NUF) rammes derimot ikke.

Hovedtema for vurderingen er hvorvidt investeringen vil være en *net benefit* for Canada, jf. Art. 16. Relevante momenter i den vurderingen er listet opp i Art. 20 og inkluderer blant annet effekten på (i) økonomisk aktivitet i Canada (herunder på sysselsetting), (ii) produktivitet, effektivitet, teknologisk utvikling mv. i Canada, (iii) konkurransen i Canada og (iv) Canadas evne til å konkurrere i globale markeder. Vurderingen kan slå ut forskjellig avhengig av politiske føringer knyttet til bestemte bransjer. Eksempelvis skal det ikke være adgang til utenlandske overtakelser innenfor film- og forlagsbransjen. Overtakelse innenfor andre bransjer kan tenkes begrenset med grunnlag i reglene om nasjonal sikkerhet.

Uavhengig av hvorvidt det skal gjøres en *review* som nevnt ovenfor, det vil si uansett transaksjonens størrelse, skal det vurderes om investeringen kan være skadelig for nasjonal sikkerhet. Dette er regulert særskilt i lovens Part IV.1. Senest innen 45 dager etter at melding eller søknad om *review* er mottatt, skal myndighetene varsle den utenlandske investoren om at transak-

sjonen eventuelt vil bli gjenstand for en slik vurdering. Transaksjonen skal deretter stilles i bero, jf. Art. 25.2 (2).

Også der transaksjonen allerede er gjennomført, for eksempel med bakgrunn i at det ikke var meldingsplikt i utgangspunktet, vil myndighetene kunne ta initiativ til kontroll ved å varsle partene om at det skal iverksettes en vurdering utfra hensynet til nasjonal sikkerhet. Melding om dette må i så fall gis innen 45 dager etter gjennomføring av transaksjonen.

Adgangen til å vurdere en transaksjon etter Part IV.1 gjelder også andre former for investeringer enn nyetablering og kontrollovertakelse, herunder erverv av ikke-kontrollerende eierandeler, se Art. 25.1 (c).

I vurderingen skal det tas stilling til hvorvidt investeringen «could be injurious to national security», jf. Art. 25.2 (1). Begrepet *national security* er ikke definert nærmere i loven, og det legges da opp til en bred skjønnsutøvelse i praktiseringen av reglene. Det gjelder heller ingen beløpsmessige terskelverdier når det gjøres en *national security review*.

Beslutningene treffes av den aktuelle fagstatsråden og/eller regjeringen (*Governor in Council*). I prinsippet kan enhver type beslutning som vurderes som tilrådelig for å beskytte nasjonale interesser treffes, i loven eksemplifisert som (i) forbud, (ii) tillatelse på vilkår og (iii) krav om nedsalg til en ikke-kontrollerende eierandel, jf. Art. 25.4 (1). Eksempler på vilkår kan være at en viss andel av styremedlemmene (vanligvis 25 %) og ledelsen må være kanadiske.

Avgjørelsene kan ikke påklages, men kan påankes etter reglene i *Federal Courts Act*, jf. Art. 25.6.

Så langt er få transaksjoner blitt stoppet i medhold av ICA med bakgrunn i hensynet til nasjonal sikkerhet, men det antas at flere er blitt avlyst underveis i saksbehandlingen.

I forlengelsen av ICA har Canada i tillegg visse sektorbaserte reguleringer som også gir anledning til å ta hensyn til nasjonal sikkerhet. Disse gjelder i all hovedsak skifte av eierskap eller lisensoverføringer innenfor blant annet uranproduksjon, transport, kulturvirksomhet, telekommunikasjon og kringkasting. Dessuten er den finansielle servicesektoren gjenstand for generelle eierskapsrestriksjoner som også kan berøre utenlandske transaksjoner. I tillegg er enkelte selskaper underlagt egne lover, eksempelvis *Air Canada* og *Canadian National Railway*.

12.3.5 Frankrike

Frankrike har detaljerte regler om myndighetskontroll med utenlandske investeringer i landet utfra hensynet til nasjonale interesser, herunder relatert til nasjonal sikkerhet. Reglene finnes i *Code Monétaire et Financier, Titre V* om finansielle relasjoner med utlandet, jf. første kapittel, Articles L151-1 til L151-4.

Article L151-1 fastslår innledningsvis et hovedprinsipp om at finansielle relasjoner mellom Frankrike og utlandet skal være uten restriksjoner.

Etter Article L151-2 gis myndighetene hjemmel til å gi nærmere bestemmelser om at det skal føres kontroll med visse typer transaksjoner utfra hensynet til nasjonale interesser:

a) valutatransaksjoner, overføring av kapital over landegrensen og alle typer oppgjør over grensen,
b) beføyelser over franske eiendeler i utlandet,
c) utenlandske investeringer i Frankrike (også nedsalg), og
d) import og eksport av gull og alle andre vesentlige overføringer av eiendeler inn til eller ut av Frankrike.

Kontroll kan utøves i form av krav om meldeplikt, krav om forhåndsgodkjennelse eller ved at transaksjonen undersøkes i ettertid.

Article L151-3 oppstiller krav om forhåndsgodkjennelse av visse utenlandske investeringer og må anses å være en særregulering av den tilsvarende henvisningen i L151-2. Formålet med kontrollen er å sikre beskyttelse av *nasjonale interesser*.

Etter Article L151-3 I, siste setning, skal det gis nærmere bestemmelser om hvilke virksomhetsområder som skal være gjenstand for obligatorisk forhåndsgodkjennelse. Slike bestemmelser er gitt i Dekret nr. 2005-1739 av 30. desember 2005 som endret ved Dekret nr. 2014-479 av 14. mai 2014. Endringsdekretet fra 2014 omtales gjerne som Alstomdekretet. I hovedsak omfattes nå sektorene/virksomhetsområdene pengespill, teknologi, forsvar/våpen, infrastruktur (energi, transport, telekom og vann) og helse, nærmere spesifisert i dekretets Article R153-2.

Der investoren har tilknytning til EU gjelder det tilleggsbestemmelser, se nedenfor i kapittel 12.3.5.1.

Hva som er relevante investeringer er angitt i R153-1 og omfatter:

Boks 12.5 Alsomdekretet Article R153-2:

1. Pengespill.
2. Privat sikkerhet.
3. Forskning, utvikling, eller produksjon av midler for å benyttes i ulovlig virksomhet; i terroristaktiviteter eller i patogener eller gift.
4. Utstyr for overvåkning av korrespondanse og samtaler.
5. Testing og sertifisering av sikkerheten for IT-produkter og -systemer.
6. Produksjon av varer eller tilførsel eller servicetilbud for å besørge sikkerheten i IT-systemer.
7. Gjenstander og teknologi med dobbelt bruksområde, både sivilt og militært.
8. Krypteringsverktøy og -tjenester.
9. Aktiviteter utført av firmaer som er betrodd nasjonale forsvarshemmeligheter, spesielt i forbindelse med forsvarskontrakter eller sikkerhetsklausuler.
10. Forskning, produksjon, eller handel med våpen, ammunisjon, krutt, og eksplosiver til militære- eller krigsformål.
11. Aktiviteter utført av virksomheter med kontrakter som angår design eller tilførsel av utstyr for Forsvarsdepartementet, enten direkte eller som underleverandør, for å produsere eller tilføre en tjeneste for en av sektorene referert til i punkt 7 til 10 ovenfor.
12. Andre aktiviteter knyttet til materiell, produkter eller tjenester essensielle for offentlig ro og orden, sikkerhet og forsvaret av landet, nemlig forsyning av elektrisitet, gass, hydrokarboner og andre energikilder, vann, transport, elektronisk kommunikasjon, militære anlegg og installasjoner, samt helsesektoren.

a) overtakelse av kontroll slik dette er definert i L233-3 i *Code de Commerce* over et fransk selskap (*entreprise*),
b) direkte eller indirekte overtakelse av hele eller deler av en fransk filial, eller
c) passering av 33,33 % direkte eller indirekte eierskap over egenkapitalen eller stemmerettighetene i et fransk selskap.

Alternativ c gjelder ikke for investeringer innenfor EU.

Etter loven er det departementet som fører kontroll med aktuelle investeringer (L151-3 I). Etter dekretets R153-7 kan investoren kontakte departementet med sikte på å få en forhåndsavklaring av hvorvidt den aktuelle investeringen er meldepliktig. Departementet skal da gi svar innen to måneder. Manglende svar på en slik forespørsel er ikke å anse som bekreftelse på at det ikke er meldeplikt.

Meldingen skal inneholde informasjon om blant annet investorens forretningssted, hvem som kontrollerer investoren, identiteten til aksjonærer med mer enn 5 % aksjer/stemmer, styremedlemmers navn og adresse etc.

Etter R153-8 skal meldingen besvares innen to måneder etter at fullstendig søknad er mottatt. Manglende svar er å anse som godkjennelse av transaksjonen. Fristen kan forlenges dersom det bes om supplerende informasjon. Det praktiseres en åpen dialog mellom investoren og myndighetene med uformelle konsultasjoner underveis i saksbehandlingen hvor investoren kan gis mulighet til å justere søknaden.

En eventuell godkjennelse kan gis på vilkår, jf. L151-3 II. Etter R153-9 kan det stilles som vilkår for tillatelsen at investoren må besørge virksomheten videreført, herunder industriell kapasitet, kapasitet knyttet til forskning og utvikling, *know-how*, forsyningssikkerhet med videre. Prinsippet om forholdsmessighet skal hensyntas ved fastsettelse av vilkårene. Overholdelse av vilkårene kontrolleres av det aktuelle fagdepartementet.

Etter R153-10 skal søknaden avslås hvis (i) det er sterke grunner til å anta at investoren vil kunne begå overtredelser av nærmere bestemte straffebud eller (ii) der aktuelle vilkår knyttet til en eventuell tillatelse anses utilstrekkelige til å ivareta hensynet til nasjonale interesser.

Avslag kan bringes inn for franske domstoler, men ikke direkte for EU-domstolen. Per 2008 var det ikke gitt avslag på noen søknader.

Der påkrevd forhåndsgodkjennelse ikke er innhentet, kan myndighetene stoppe eller reversere transaksjonen, jf. Article L151-3 III. Før slik beslutning treffes, skal den utenlandske investoren gis anledning til å uttale seg. Ved brudd på reglene eller pålegg kan det ilegges et gebyr på inntil det dobbelte av den ulovlige investeringen. Størrelsen på gebyret skal være proporsjonal med alvoret i overtredelsen.

Etter lovens Article L151-4 er enhver avtale eller forpliktelse som direkte eller indirekte gjennomfører (*réalise*) en utenlandsk investering der

påkrevd forhåndsgodkjennelse ikke er gitt å anse som en nullitet (*nul*).

12.3.5.1 Særlig om investeringer innenfor EU

I Alstom-dekretet fra 2014, sondres det mellom investorer med og uten tilknytning til EU. R153-3 til 153-5 gjelder de med, mens R153-2 gjelder de uten EU-tilknytning.

Det føres kontroll med overtakelser innenfor virksomhetsområdene som er listet i R153-2 nr. 8-12 (det vil si militært/våpen og viktig infrastruktur) for begge kategoriene av investorer, jf. R153-2 og R153-4. Det samme gjelder for nr. 2-7, men det gjelder da særskilte tilleggsvilkår når investoren har EU-tilknytning. Disse tilleggsvilkårene følger av R153-5. Terskelen for utøvelse av kontroll er dermed høyere for nr. 2-7 når det dreier seg om investorer med EU-tilknytning.

Særreglene for investeringer innenfor EU gjelder der den aktuelle investoren faller innenfor en av følgende tre kategorier (jf. R153-4 og 153-5):

a) fysisk person fra et EU-land eller fra et EØS-land med skatteavtale med Frankrike,
b) selskap (*entreprise*) med forretningssted (*siège social*) i et slikt land, eller
c) fysisk person med fransk statsborgerskap som bor i et slikt land.

Etter R153-3, som gjelder investorer med EU-tilknytning, er alternativet passering av 33,33 % i seg selv ikke å anse som en relevant investering i denne sammenheng. Investeringen må således enten innebære overtakelse av kontroll som definert i *Code de Commerce* eller overtakelse av filial.

12.3.6 Finland

Den finske *Lag om tillsyn över utlänningars företagsköp* fra 2012 regulerer utlendingers adgang til å overta innflytelse over visse finske foretak. Nasjonale sikkerhetsinteresser er et av grunnlagene for kontrollen. Loven hjemler kontroll med utlendingers overtakelse av finske foretak. Hensikten med kontrollen er å ivareta *ytterst viktige nasjonale interesser*, jf. § 1. I § 2 defineres dette nærmere slik:

> tryggande av landets försvar eller säkerställande av allmän ordning och allmän säkerhet i enlighet med artiklarna 52 och 65 i fördraget om Europeiska unionens funktionssätt när det föreligger ett verkligt och tillräckligt allvarligt hot mot ett grundläggande samhällsintresse.

Kontroll skal etter § 4 føres med overtakelse av *försvarsindustriföretag*. *Försvarsindustriföretag* er i § 2 nr. 4 definert som sammenslutning eller virksomhet som produserer eller leverer forsvarsmateriell eller andre tjenester eller produkter som er viktige for det militære forsvaret. I tillegg omfattes virksomheter eller sammenslutninger som i Finland tilvirker produkter med dobbelt anvendelsesområde (*dual use*), som omfattes av det finske eksportkontrollregelverket.

I tillegg føres kontroll med andre sammenslutninger eller virksomhet som av andre grunner anses å være en kritisk organisasjon med tanke på beskyttelse av samfunnets vitale funksjoner.

Kontroll er aktuelt der investoren faller innenfor en av følgende kategorier, jf. § 2 nr. 3:

a) en utlänning som inte har sin bosättningsort i en stat som hör till Europeiska unionen (EU) eller Europeiska frihandelssammanslutningen (EFTA),
b) en sammanslutning eller stiftelse som inte har sin hemort i någon av EU:s eller EFTA:s medlemsstater,
c) en sammanslutning eller stiftelse som har sin hemort i någon av EU:s eller EFTA:s medlemsstater men i vilken en utlänning som avses i a-punkten eller en sammanslutning eller stiftelse som avses i b-punkten innehar minst en tiondedel av det röstetal som samtliga aktier i ett aktiebolag medför eller som utövar motsvarande faktiskt inflytande i en annan sammanslutning eller rörelse.

Ved kjøp av en *försvarsindustriföretag*, omfattes i tillegg investorer innenfor EU, nærmere bestemt (§ 2 tredje avsnitt):

> sådana fysiska personer samt sammanslutningar och stiftelser som har sin bosättningsort eller hemort i någon annan av EU:s medlemsstater än Finland eller i någon av EFTA:s medlemsstater. Detsamma gäller sådana finländska sammanslutningar och stiftelser där en fysisk person eller en sammanslutning eller stiftelse som har sin bosättningsort eller hemort i någon annan av EU:s medlemsstater än Finland eller i någon av EFTA:s medlemsstater innehar minst en tiondedel av det röstetal som samtliga aktier i aktiebolaget medför eller som utövar motsvarande faktiskt inflytande i sammanslutningen eller rörelsen.

Loven regulerer *företagsköp* og omfatter transaksjoner som resulterer i passering av en tidel, en tredel eller halvparten av stemmene i det aktuelle selskapet. Loven har detaljerte regler om hvordan man beregner andelen stemmer som transaksjonen resulterer i, jf. § 2 nr. 5. Lovens § 6 oppstiller visse unntak.

Tilsynet føres av Arbeids- og næringsdepartementet, jf. § 3. Nødvendige opplysninger innhentes fra andre aktuelle myndigheter. Transaksjonen skal godkjennes så lenge den ikke anses å være i strid med *ytterst viktige nasjonale interesser*. Avgjørelsen treffes av departementet eller av statsrådet (regjeringen), jf. §§ 3 og 4.

Foretakskjøp innenfor forsvarssektoren er meldepliktige og må forhåndsgodkjennes, jf. § 4. Ved kjøp av foretak utenfor forsvarssektoren er det frivillig å melde, jf. § 5.

Søknaden skal i begge tilfeller inneholde alle nødvendige opplysninger om målselskapet, den utenlandske investoren og transaksjonen. Dette omfatter eierskapsstruktur i målselskapet før og etter gjennomføring, samt eierskap over investoren. Det skal også opplyses om investorens videre planer for målselskapet.

Etter § 5, andre avsnitt, er det hjemmel for å gi pålegg om at ikke meldte transaksjoner likevel må meldes. Myndighetene må da kreve fremlagt relevant informasjon senest tre måneder etter å ha fått kjennskap til transaksjonen.

Utenfor forsvarssektoren vil meldingen anses som automatisk godkjent dersom myndighetene ikke (i) innen seks måneder etter mottak av nødvendige opplysninger beslutter fortsatt utredning i saken eller (ii) innen tre måneder overfører saken til behandling i statsråd (det vil si i praksis innstiller på avslag), jf. § 5 siste avsnitt.

Ved avslag vil investoren bli pålagt å selge seg ned til under 10 % (eventuelt ned til en høyere eierandel som det tidligere er gitt tillatelse til). Etter dette kan investoren ikke stemme for en for større andel på selskapets generalforsamling (eller tilsvarende), og de overskytende aksjene skal heller ikke tas i betraktning når det for å treffe en gyldig beslutning kreves samtykke fra en viss andel av selskapets aksjer. Avslag kan påankes etter § 9.

12.3.7 Sverige og Danmark

Hverken Sverige eller Danmark ser ut til å ha regler om tilsyn med utenlandsk overtakelse av kontroll over virksomheter ut fra hensynet til å skulle ivareta nasjonale sikkerhetsinteresser.

Det disse landene har av regler på området er knyttet til konkurranserettslig kontroll med foretakssammenslutninger og kontroll med eierskap innenfor finanssektoren. Men som i Norge er dette styrt av andre hensyn enn hensynet til nasjonal sikkerhet, og hvorvidt eierne er utenlandske er i utgangspunktet i seg selv uten relevans.

12.4 EØS-rettslige forpliktelser

EØS-avtalen er en viktig rammefaktor for hvordan norsk regelverk knyttet til eierskapskontroll kan utformes.

Lovgivning som innebærer utøvelse av eierskapskontroll vil, avhengig av investeringen som skjer, kunne innebære inngripen enten i etableringsretten (EØS-avtalen artikkel 31[9]) eller den frie bevegelighet for kapital (EØS-avtalen artikkel 40). Dersom investeringen innebærer at eieren får kontroll over selskapet, er investeringen beskyttet av etableringsretten. Dersom investeringen ikke resulterer i kontroll, er investeringen beskyttet av retten til fri bevegelighet for kapital.

Utgangspunktet er at det vil være i strid med EØS-avtalen å diskriminere eiere fra andre EØS-stater. Dette forbudet gjelder også restriksjoner som rammer det å foreta investeringer i selskap, selv om regelen rammer likt for innenlandske og utenlandske eiere. Forbudet mot restriksjoner gjelder blant annet prosessuelle krav til meldeplikt, godkjenning etc.

Lovgivning som diskriminerer eiere fra andre EØS-stater må begrunnes i aktuelle unntaksbestemmelser i EØS-avtalen. Lovgivning som innebærer restriksjoner eller som rammer norske og utenlandske eiere likt vil kunne begrunnes i såkalte allmenne hensyn.

Selv om nasjonal lovgivning vil innebære en diskriminerende behandling av utenlandske EØS-eiere og dermed i utgangspunktet være ulovlig, vil det i helt spesielle tilfeller i medhold av unntakene i EØS-avtalens artikkel 123, artikkel 32 og artikkel 33 (og tilsvarende for den frie bevegelighet av kapital) kunne være anledning til å gripe inn og utøve kontroll med endringer i eierskap når dette er nødvendig av hensyn til sikkerhetsinteresser.

12.4.1 EØS-avtalen artikkel 123

EØS-avtalen har i likhet med Traktaten om den europeiske unions virkemåte (TEUV) en bestemmelse som gir unntak fra avtalens øvrige bestem-

[9] Agreement on the European Economic Area (EEA Agreement). Trådt i kraft 1. januar 1994.

melser dersom det er nødvendig av sikkerhetshensyn.

EØS-avtalen artikkel 123 lyder:

> Bestemmelsene i denne avtale skal ikke hindre en avtalepart i å treffe tiltak:
>
> a) som den anser nødvendig for å hindre spredning av opplysninger som er i strid med dens vesentlige sikkerhetsinteresser,
> b) som angår produksjon av eller handel med våpen, ammunisjon og krigsmateriell eller andre varer som er uunnværlige for forsvarsformål, eller forskning, utvikling eller produksjon som er uunnværlig for forsvarsformål, såfremt disse tiltak ikke endrer konkurransevilkårene for varer som ikke er bestemt for direkte militære formål,
> c) som den anser vesentlig for sin sikkerhet i tilfelle av alvorlig indre uro som truer den offentlige orden, i krigstid eller ved alvorlig internasjonal spenning som innebærer en fare for krig, eller for å oppfylle forpliktelser den har påtatt seg med sikte på å opprettholde fred og internasjonal sikkerhet.

Det kan være aktuelt å begrunne kontroll med eierskap i alle tre bokstavene. Bokstav a gir unntak fra EØS-avtalen for forhold hvor det vil være skadelig i seg selv at informasjon blir kjent. Dette vil eksempelvis kunne være aktuelt ved endringer i eierskapet til selskaper som har kontrakter med Forsvaret om kapasiteter som ikke er offentlig kjent. Inntreden av nye eiere vil da kunne medføre at det blir kjent at Forsvaret får levert en tjeneste eller en vare med visse kapabiliteter. Bokstav b kan være aktuell der det er nødvendig at det utøves eierskapskontroll med en av Forsvarets leverandører av våpen, ammunisjon, krigsmateriell, eller andre varer som er uunnværlig for forsvarsformål. Bokstav c vil kunne begrunne unntak for å ivareta andre vesentlige sikkerhetsinteresser.

Dersom det er aktuelt å anvende EØS-avtalen artikkel 123, må unntaket påberopes i det enkelte tilfellet, og det må begrunnes konkret.

Myndigheten som påberoper seg unntaket har bevisbyrden for at vilkårene i unntaksbestemmelsen er oppfylt, jf. EU-domstolens avgjørelse C-615/10.

I EU-domstolens avgjørelse C-414/97, Kommisjonen mot Spania, la EU-domstolen til grunn at det må foretas en konkret vurdering av om vesentlige sikkerhetsinteresser gjør det nødvendig med et unntak. Saken gjaldt offentlige anskaffelser, men tilsvarende vil gjelde ved kontroll av eierskap.

På bakgrunn av det som ble fastslått i den nevnte avgjørelsen, uttaler Kommisjonen i sin fortolkningsmeddelelse om anvendelsen av daværende artikkel 296 på offentlig innkjøp av forsvarsmateriell (tilsvarer nåværende TEUV artikkel 346):

> The Treaty therefore contains strict conditions for the use of this derogation, balancing Member States' interests in the field of defence and security against the fundamental principles and objectives of the Community. The aim of these conditions is to prevent possible misuse and to ensure that the derogation remains an exception limited to cases where Member States have no other choice than to protect their security interests nationally.
>
> The Court of Justice has consistently made it clear that any derogation from the rules intended to ensure the effectiveness of the rights conferred by the Treaty must be interpreted strictly. Moreover, it has confirmed that this is also the case for derogations applicable «in situations which may involve public safety». In Commission v Spain, the Court ruled that articles in which the Treaty provides for such derogations (including Article 296 TEC) «deal with exceptional and clearly defined cases. Because of their limited character, those articles do not lend themselves to a wide interpretation».

I følge Kommisjonens meddelelse skal unntaket som et utgangspunkt tolkes restriktivt. Samtidig understreker Kommisjonen også at det er «the Member States' prerogative to define their essential security interests and their duty to protect them». Likevel må medlemsstatene ikke «abuse this flexibility».

For å oppfylle vilkårene må behovet som skal beskyttes som nevnt gjelde «essential interests of (…) security». Det fremgår av meddelelsen at andre hensyn, særlig industrielle og økonomiske, ikke kan rettferdiggjøre bruk av artikkel 123, selv om de er forbundet med vesentlige sikkerhetsinteresser. Det må være hensyn til sikkerhetsinteresser og ikke norsk industri som kan begrunne inngripen.

Den konkrete vurderingen av dette (det vil si av behovene) må foretas nasjonalt, og ut fra nasjonale forhold. Likevel tilføyes det at «[a]t the same time, Member States' security interests should also be considered from a European perspective.

They may vary, e.g. for geographical or historical reasons».

Ved spørsmålet om anvendelsen av unntaket må det foretas en konkret vurdering i den enkelte sak. Det må vurderes hvilken sikkerhetsinteresse som skal beskyttes, hva som er sammenhengen mellom sikkerhetsinteressen og inngrepet i eierskapet for det relevante selskapet, og endelig hvorfor det er nødvendig å kontrollere eierskapet for å verne om sikkerhetsinteressen.

Som nevnt over, skal det ved denne vurderingen uansett også legges til grunn at det er opp til medlemsstatene å definere sine vesentlige sikkerhetsinteresser, og deres behov for å beskytte disse. Dette innebærer at statene har en relativt vid skjønnsmargin ved fastleggelsen av hva som ligger i sikkerhetsinteressen. Dette er blant annet lagt til grunn i sak C-252/01 premiss 30. Saken gjaldt anskaffelse av flyfotografering hvor EU-domstolen uttalte:

> It is not disputed that the Kingdom of Belgium is responsible for protecting the security not only of its national installations but also of the installations of international organisations within its territory, such as NATO. It is therefore for the Belgian authorities to lay down the security measures necessary for the protection of such installations.

EU-domstolen gikk så imidlertid i premiss 31-35 gjennom hvilke sikkerhetskrav som ble stilt og hvordan dette var egnet til å oppnå formålet, dog uten å foreta en særlig intensiv prøving.

EU-domstolens tidligere praksis, herunder C-252/01, som ga medlemsstatene svært stor skjønnsfrihet i anvendelsen av TEUV artikkel 346 (og tidligere tilsvarende bestemmelsene), er imidlertid i senere tid blitt skjerpet inn. EU-domstolen prøver nå i større utstrekning om bruk av unntaket er nødvendig og proporsjonalt. I C-615/10, Korkein, uttalte EU-domstolen i premiss 45:

> the Member State which seeks to take advantage of that Treaty provision can show that it is necessary to have recourse to the derogation provided for in that provision in order to protect its essential security interests (see, to that effect, inter alia, Commission v Finland, paragraph 49) and whether the need to protect those essential interests could not have been addressed within a competitive tendering procedure such as that specified by Directive 2004/18.

I en artikkel av Baudouin Heuninckx skriver forfatteren om sak C-252/01:[10]

> On the other hand, the ECJ ruled that the exemption cannot be invoked if less restrictive or disproportionate measures could be used to preserve the confidentiality of the information to be provided under the contract and still allow the use of competitive tendering. Such measures could include requirements for the tenderers to sign non-disclosure agreements and to comply with applicable security regulations.

Selv om det er statenes eget ansvar å definere hva som ligger i deres vesentlige sikkerhetsinteresser, kan unntaket altså kun anvendes hvis det er strengt nødvendig for å ivareta sikkerhetsinteressene, og sikkerhetsinteressen ikke kan vernes gjennom tiltak som ikke er i strid med EØS-avtalen, eller på mindre inngripende måte.

I EU-domstolens sak C-3/88, Re Data Processing, hadde Italia i en anskaffelse av IT-tjenester anført at det var nødvendig å kreve at tilbydere skulle ha italiensk offentlig eierskap fordi de ansatte hos leverandøren ville ha tilgang til straffesaksdata. EU-domstolen konkluderte med at dette ikke var nødvendig fordi dette kunne sikres ved å pålegge straffesanksjonert taushetsplikt for de ansatte hos leverandøren.

I sak C-324/93, Evans Medical, antydet EU-domstolen til at det kanskje ikke var nødvendig med begrensninger på import av narkotiske legemidler dersom man kunne oppnå betryggende forsyningssikkerhet gjennom å stille krav til leverandørene.

12.4.2 EØS-avtalen artikkel 32 og 39

EØS-avtalen artikkel 32 og 39 gir et unntak fra den frie etableringsretten og den frie bevegeligheten av tjenester for virksomhet som innebærer utøvelse av offentlig myndighet. Unntaket gjelder etter sin ordlyd selv om det private selskapet kun leilighetsvis utøver offentlig myndighet, men det går trolig en nedre grense. Unntaket innebærer at EØS-avtalen ikke får anvendelse for regulering av slik virksomhet. I motsetning til unntaket i EØS-avtalen artikkel 123 (nasjonal sikkerhet) og artikkel 33 (offentlig orden, folkehelse og offentlig sikkerhet) hvor unntaket kun kan påberopes dersom det er nødvendig og forholdsmessig, gjelder unn-

[10] Baudouin Heuninckx «Lurking at the Boundaries: Applicability of EU law to Defence and Security Procurement», *PPLR3* (2010), 97.

taket for utøvelse av offentlig myndighet uten noen slike krav.

Norge har i regelverket om offentlige anskaffelser innført et unntak fra plikten til å følge forskrift om offentlige anskaffelser ved tildeling av oppdrag som innebærer utøvelse av offentlig myndighet.

12.4.3 EØS-avtalen artikkel 33

EØS-avtalen artikkel 33 fastsetter at bestemmelse om etableringsretten:

> skal ikke hindre at bestemmelser om særbehandling av fremmede statsborgere får anvendelse når de er fastsatt ved lov eller forskrift og begrunnet med hensynet til offentlig orden, sikkerhet og folkehelsen.

Bestemmelsen har til en viss grad et overlappende anvendelsesområde med EØS-avtalen artikkel 123. Kontroll med eierskap i selskaper som håndterer informasjon, teknologi og/eller fysiske aktiva av betydning for samfunnets sikkerhet, spesielt i sivil sektor, vil dermed kunne være unntatt EØS-avtalen etter både artikkel 123 og 33.

EU-domstolen behandlet i sak C-54/99, Scientologikirken, et spørsmål om en fransk lovbestemmelse var forenlig med den frie bevegelighet av kapital. Frankrike hadde på det tidspunktet en lov som innebar en meldeplikt og krav om tillatelse for utenlandske investeringer som kunne utgjøre en fare for offentlig orden, folkehelsen og offentlig sikkerhet.

EU-domstolen uttalte at lovgivningen innebar en begrensning på samhandelen. Domstolen konstaterte at:

> selv om medlemsstaterne i det væsentlige har frihed til i overensstemmelse med deres nationale behov at bestemme, hvad hensynet til den offentlige orden og den offentlige sikkerhed kræver, må begrundelserne imidlertid i fællesskabsretlig sammenhæng og særligt i det omfang, de skal retfærdiggøre en fravigelse af det grundlæggende princip om frie kapitalbevægelser, fortolkes strengt, således at deres rækkevidde ikke ensidigt kan fastlægges af den enkelte medlemsstat uden fællesskabsinstitutionernes kontrol.

I forlengelsen ble det uttalt:

> Den offentlige orden og den offentlige sundhed kan således kun påberåbes, når der foreligger en virkelig og tilstrækkelig alvorlig trussel mod et grundlæggende samfundshensyn.

Det måtte foretas en nødvendighets- og forholdsmessighetsvurdering av behovet for reguleringen. Med henvisning til tidligere praksis viste EU-domstolen til at en må foreta en inngående vurdering av om det er nødvendig med forhåndsgodkjenning av investeringer, men påpekte at det kan tenkes tilfeller hvor dette vil være forenlig. Dette vil gjelde der etterfølgende mulighet for kontroll ikke er tilstrekkelig.

Den franske lovgivningen ble imidlertid felt da den var for vag. Kravet om forutgående tillatelse gjaldt helt generelt for enhver investering som kunne utgjøre en fare for den offentlige sunnhet og offentlige orden uten noen nærmere presisering. Dette innebar at det ikke var mulig å forutberegne sin rettsstilling, og dermed ikke mulig å vurdere når det måtte innhentes forutgående tillatelse. Frankrike har gjennom det såkalte Altstomdekretet revidert sin lovgivning til å bli vesentlig mer treffsikker.

Portugal ble i sak C-367/98, Kommisjonen mot Portugal, dømt for brudd mot EU-retten ved å ha en lovbestemmelse om krav til forhåndsgodkjenning ved kjøp av visse portugisiske selskaper. EU-domstolen uttalte i premiss 50:

> As regards a scheme of prior administrative authorisation of the kind at issue in the present case, the Court has previously held that such a scheme must be proportionate to the aim pursued, inasmuch as the same objective could not be attained by less restrictive measures, in particular a system of declarations ex post facto (see, to that effect, Sanz de Lera, paragraphs 23 to 28; Konle, paragraph 44; and Case C-205/99 Analir and Others [2001] ECR I-1271, paragraph 35). Such a scheme must be based on objective, non-discriminatory criteria which are known in advance to the undertakings concerned, and all persons affected by a restrictive measure of that type must have a legal remedy available to them (Analir, cited above, paragraph 38).

12.4.4 Rettighetshavere etter EØS-avtalen – forholdet til eiere fra tredjeland

Rettighetshavere for etableringsretten etter EØS-avtalen er både fysiske EØS-borgere og selskaper i andre EØS-stater, jf. EØS-avtalen artikkel 34. En juridisk person etablert i en annen EØS-stat regnes dermed i utgangspunktet som en EØS-borger

uavhengig av statsborgerskapet til eierne av selskapet. Dersom en skulle innføre lovgivning som skiller mellom eiere med og uten EØS statsborgerskap, vil selskaper i et annet EØS-land, som har eiere med ikke-EØS statsborgerskap, regnes som en eier innenfor EØS-området.

For kapital har TEUV artikkel 63 en revidert og oppdatert regulering sammenlignet med EØS-avtalen artikkel 40, hvor det oppstilles et forbud mot restriksjoner på kapitalbevegelser både mellom medlemsstatene, og mellom medlemsstatene og tredjestater. Her er det antatt å være en forskjell mellom EØS-avtalen og rettstilstanden for EU-medlemmer. I forhold til den frie bevegelighet av kapital, så er dermed EØS-avtalen, i motsetning til TEUV, ikke til hinder for å diskriminere mot eiere utenfor EØS-området.

12.4.5 Krav til utforming av lovgivningen

Inngripen i disse spesielle tilfellene vil kreve lovhjemmel. I kravet til nødvendighet ligger det at formålet ikke kan oppnås på mindre inngripende måte og dermed ikke går ut over det som er nødvendig for å oppnå formålet. Kravet til forholdsmessighet innebærer at interessene som inngrepet skal beskytte må stå i rimelig forhold til graden av forstyrrelse av det indre markedet.

Eksempelvis vil en meldeplikt, kombinert med et gjennomføringsforbud inntil godkjennelse er gitt, i seg selv ha en begrensende effekt på andre EØS-lands eieres investeringer i Norge. Tilsvarende vil en usikkerhet om hvilke selskaper som er underlagt kontroll med eierskapet eller usikkerhet om vilkårene for når det vil bli grepet inn kunne ha en begrensende effekt på investeringslysten i Norge.

Lovgivningen må dermed utformes slik at den kun rammer de tilfellene hvor unntakene fra EØS-avtalen gir adgang til inngripen, er tilstrekkelig presis om hvilke selskaper den rammer og hva som vil være vilkårene for når det vil skje inngripen slik at investorer kan forutberegne sin rettsstilling, og ikke unødvendig pålegger meldeplikt eller andre prosessuelle plikter på investeringer i selskaper hvor det ikke er adgang til å føre kontroll.

En slik lovhjemmel vil måtte fortolkes som en snever unntaksbestemmelse. Det vil måtte dokumenteres godt i den enkelte sak hvorfor det er nødvendig å gripe inn. Inngripen kan kun skje av hensyn til sikkerhetsinteresser. Det vil være et totalforbud mot å foreta inngripen for å ivareta næringspolitiske interesser.

12.5 Eierskapsmeldingen

12.5.1 Innledning

Gjennom Meld. St. 27 (2013–2014) Et mangfoldig og verdiskapende eierskap, har regjeringen fremlagt hovedretningen for regjeringens politikk for å fremme et mangfoldig eierskap i norsk næringsliv og for statens eierskap.

Eierskapet kan ha stor betydning for verdiskapningen og konkurransekraften i et selskap. Hva som utgjør en god eierskapssammensetning vil avhenge av en rekke faktorer, herunder markedsutviklingen, virksomhetenes utvikling og karakter, samt med eiernes forutsetninger og holdning til risiko. Ulike faser i et selskaps utvikling fordrer forskjellige behov, og ulike eiere har som regel ulike forutsetninger for å bidra til denne utviklingen.

Virksomheters evne til omstilling og innovasjon er en grunnleggende forutsetning for å kunne håndtere en økt endringstakt i næringslivet. Dette stiller også krav til eierne, som premissgivere for selskapenes virksomhet og som beslutningstakere ved større endringer.

Eierskap har betydning for hvordan selskaper styres og drives. I Eierskapsmeldingen beskrives utviklingen de siste tiår som en utvikling mot et mer fragmentert eierskap i børsnoterte selskaper. Dette, kombinert med blant annet høy endringstakt i markedet, gjør det mer krevende å opprettholde strategiske konkurranseposisjoner og evne til verdiskapning over tid. Oppmerksomheten mot eiernes og selskapenes samfunnsansvar har også økt, og i etterkant av finanskrisen har det også vært en utvikling mot økt bevissthet om den langsiktige verdiutviklingen av selskaper.

Den teknologiske utviklingen har også medført at selskaper i større grad må forholde seg til stadig raskere endringer i omgivelsene, noe som vil kunne være utfordrende med et tungt statlig eierskap.

12.5.2 Privat eierskap som hovedregel

Regjeringen Solberg har i Eierskapsmeldingen fremhevet at privat eierskap etter regjeringen syn er, og bør være hovedregelen i norsk næringsliv. Statlig eierskap bør begrunnes særskilt.

Privat eierskap omfatter alt eierskap som ikke er offentlig, det vil si der stat, fylkeskommune eller kommune ikke er den dominerende eier.

Offentlig eierskap inkluderer ifølge Eierskapsmeldingen både de tilfeller hvor det offentlige har direkte eierskap i norske selskaper og indirekte

eierskap i utenlandske og norske selskaper. Statens pensjonsfond utland og Statens pensjonsfond Norge er eksempler på indirekte statlig eierskap. I motsetning til direkte eierskap, forvaltes investeringene ut fra et finansielt porteføljeperspektiv, og ikke ut fra et strategisk eierperspektiv i det enkelte selskap.[11]

Det fremheves i meldingen at private eiere ofte kan ivareta egne preferanser og eiendom, og utøve et mer direkte personlig eierskap, enn staten som utøver eierrollen på vegne av fellesskapet. Det vil normalt også være færre beslutningsledd mellom eiere og ledelse i selskapet når eieren er privat. Private eiere vil også ofte ha en større nærhet til og kunnskap om det markedet selskapet opererer i, og vil gjerne ha sterkere insentiver for effektiv drift og høy avkastning, enn hva en statlig eier har.

I meldingen blir det også pekt på enkelte potensielle utfordringer knyttet til statlig eierskap. For det første kan et statlig eierskap innebære en potensiell konflikt mellom eierskapet og statens øvrige roller. For det andre vil et omfattende statlig eierskap kunne medføre fare for en maktkonsentrasjon, som igjen kan svekke privat sektor. Og for det tredje er det begrensninger i den industrielle kompetansen hos staten som eier. Alle disse forholdene taler etter regjeringens syn for å begrense det statlige eierskapet i kommersielle selskaper, og stryke det private eierskapet.

12.5.3 Begrunnelser for statlig eierskap

Staten forvalter i dag direkte eierskap i om lag 70 selskaper gjennom ti ulike departementer. Eierskapet varierer i størrelse, fra store børsnoterte selskaper til heleide selskaper med rene sektorpolitiske mål. Det er også stor variasjon når det gjelder hvilke sektorer disse selskapene opererer i. Selskapsrettslig er disse virksomhetene ulikt organisert, herunder aksjeselskap, allmennaksjeselskap, statsforetak, helseforetak eller andre typer særlovselskaper.

I Eierskapsmeldingen angis det fire forhold som etter regjeringens oppfatning kan begrunne statlig eierskap.

For det første vil hensynet til *korrigering av markedssvikt* kunne begrunne statlig eierskap. Med markedssvikt menes at det oppstår et avvik mellom privat- og samfunnsøkonomisk lønnsomhet. Enkelte varer og tjenester bør eller må, ut fra et samfunnsperspektiv, produseres på en annen måte enn gjennom et marked med fri konkurranse, eksempelvis ved produksjon av fellesgoder på områder hvor det er naturlige monopoler. Det norske strømnettet trekkes frem som eksempel på et område hvor det er betydelige stordriftsfordeler som medfører et naturlig monopol. Statlig kontroll med den nasjonale infrastrukturen som det sentrale strømnettet utgjør, trekkes også frem som et forhold som begrunner statlig eierskap.

Et annet forhold som kan begrunne statlig eierskap er hensynet til *nasjonal forankring av viktige selskaper, hovedkontorfunksjoner og nøkkelkompetanse*. Fra samfunnets side kan det være ønskelig å opprettholde visse typer virksomhet i Norge. Statlig eierskap trekkes frem som et virkemiddel for å opprettholde hovedkontor i Norge. Dette sikres ved å eie minimum en tredjedel av et selskap, som medfører at staten har negativt flertall med hensyn til endringer av selskapets vedtekter. Et annet mål som trekkes frem er å sikre kontroll med at det fortsatt foregår produksjon av varer og tjenester av betydning for nasjonal sikkerhet, leveringssikkerhet eller for å ivareta nasjonal suverenitet. Hensynet til slik strategisk produksjon har medført statlig eierengasjement ved flere ulike virksomheter, blant annet Kongsberg Gruppen ASA og Nammo AS.

Hensynet til å sikre en forsvarlig *forvaltning av felles naturressurser*, som fiskeri og havbruk, vannkraft og petroleum har tradisjonelt vært brukt som begrunnelse for statlig eierskap. I Eierskapsmeldingen diskuteres det hvorvidt statlig eierskap er et nødvendig virkemiddel for å oppnå målsettingene. Stedsspesifikke naturressurser kan vanskelig flyttes ut av landet, og staten vil således uavhengig av eierskap ha en viss kontroll med ressursene gjennom annen regulering. Statlig eierskap kan imidlertid benyttes som virkemiddel for å sikre at forvaltningen av ressursene skjer til fellesskapets beste, og for å sikre at inntektene knyttet til disse ressursene tilfaller fellesskapet og ikke få enkeltaktører.

En fjerde begrunnelse for statlig eierskap er *sektorpolitiske og samfunnsmessige hensyn*. På enkelte områder har staten et særskilt ønske om styring og kontroll, herunder muligheten til å endre vilkår raskt. Statens særskilte ansvar for å ivareta god nasjonal infrastruktur som blant annet flyplasser og strømnett trekkes frem som eksempler i denne sammenheng. Sektorpolitiske hensyn ligger også til grunn for statlige sykehus, blant annet for å sikre forsvarlige helsetjenester til hele befolkningen uavhengig av den enkeltes betalingsevne. Statlig eierskap kan også sees i lys av en målsetting om lik tilgang og sikker forsyning

[11] Meld. St. 27 (2013–2014), *Et mangfoldig og verdiskapende eierskap*, 36.

av visse basistjenester, uavhengig av etterspørsel, bosted, betalingsvilje og -evne og annen status.

I meldingen påpekes det at det bør vurderes for hvert enkelt tilfelle om eierskap er det mest effektive virkemidlet for å oppnå aktuelle mål, eller om man ved bruk av alternative virkemidler kan oppnå det samme. Bruk av rettslige reguleringsinstrumenter, som blant annet *konsesjonsregler*, *lover og forskrifter,* har gradvis erstattet statlig eierskap som virkemiddel for ivaretakelsen av definerte mål. Konsesjonsbestemmelser kan sikre at nødvendige tjenester er forsvarlige og tilgjengelige for allmennheten, uten at tjenestetilbyderne er offentlig eid. Andre alternativer er å knytte *subsidier* til bestemte handlingsmønstre, *kontraktsstyring* og *statlige anskaffelser* av varer og tjenester. Kontraktsstyring kan innebære kommersielle avtaler med private leverandører om produksjon av bestemte varer eller tjenester, eller fastsatt pris overfor brukerne, mot vederlag til staten. Gjennom anskaffelsesregelverket kan staten sette krav til tilbud og vilkår for gjennomføring av oppdraget, som også kan sikre måloppnåelse for blant annet sektorpolitiske målsettinger.

12.5.4 Kategorisering av selskapene i det direkte eierskapet

I Eierskapsmeldingen er de selskapene som staten eier direkte kategorisert i fire ulike kategorier. Utgangspunktet for kategoriseringen har vært statens begrunnelser og mål for det direkte statlige eierskapet.

1. *Selskaper med forretningsmessige mål* omhandler de selskapene hvor staten kun har forretningsmessige mål med eierskapet, og hvor eierforvaltningen har som eneste formål å maksimere statens investeringer. Innen kategori 1 har regjeringen blant annet kategorisert Flytoget AS, Mesta AS og SAS AB.
2. *Selskaper med forretningsmessige mål og nasjonal forankring av hovedkontor* omhandler selskaper hvor staten både har forretningsmessige mål med eierskapet, og et mål om å opprettholde norsk forankring av selskapenes hovedkontor og tilhørende hovedkontorfunksjoner. For å ivareta sistnevnte må vil det i utgangspunktet være tilstrekkelig at staten innehar en eierandel på over en tredjedel. Innen kategori 2 har regjeringen blant annet kategorisert Kongsberg Gruppen ASA, Nammom AS, Norsk Hydro ASA, Statoil ASA og Telenor ASA.

Boks 12.6 Stortingsbehandlingen av Eierskapsmeldingen

Vedtak X

Stortinget ber om at regjeringen, dersom staten som eier skulle forelegges og delta i en beslutning om en endring i Kongsberg Gruppen ASAs struktur (salg av deler av selskapet eller lignende), tar med i sine vurderinger hensynet til å ivareta forsvarsmessig kompetanse og virksomhet med tanke på nasjonal sikkerhet.

Kilde: Innst. 140 S (2014–2015).

3. *Selskaper med forretningsmessige mål og andre spesifikt definerte mål* omhandler selskaper hvor staten, i tillegg til forretningsmessige målsetninger, kan ha behov for å legge enkelte føringer for utøvelse av virksomheten. For at det ikke skal skapes tvil om at slike selskaper drives på forretningsmessig grunnlag, vil den sektorpolitiske styringen hovedsakelig ivaretas gjennom reguleringer, konsesjonsregler og forretningsmessig statlige kjøp fra selskapene. Innen kategori 3 har regjeringen blant annet kategorisert Aerospace Industrial Maintenance Norway SF[12], NSB AS, Posten Norge AS og Statkraft SF.
4. *Selskaper med sektorpolitiske målsettinger* omhandler selskaper hvor statens eierskap hovedsakelig har sektorpolitiske formål. Som eier vil staten vektlegge at de sektorpolitiske målene nås mest mulig effektivt. Innen kategori 4 har regjeringen blant annet kategorisert Andøya Space Center AS, Avinor AS, Gassco AS, Norsk Helsenett SF, Norsk Rikskringkasting AS, Petoro AS, Space Norway AS, Statnett SF, samt de regionale helseforetakene.

12.6 Nasjonal forsvarsindustriell strategi

Forsvarsdepartementet fremmet i Meld. St. 9 (2015–2016) Nasjonal forsvarsindustriell strategi, regjeringens politiske plattform for å bidra til å opprettholde og videreutvikle norsk forsvarsindustri.[13]

[12] Nå AIM Norway AS.

[13] Meld. St. 9 (2015–2016), *Melding til Stortinget – Nasjonal forsvarsindustriell strategi.*

Kapasitet innenfor viktige teknologiske kompetanseområder, er vesentlig for å kunne sikre forsvarssektoren riktig materiell og kompetanse til rett tid. En tilgjengelig norsk kapasitet på dette området øker Norges evne til å ivareta nasjonal sikkerhet på områder der særnorske forhold krever særlig kompetanse.

Ulike regjeringers strategi for forsvarsindustrien har variert gjennom tiden, men behovet for en norsk forsvarsindustri, med kompetanse innen strategisk viktige områder, har hele tiden ligget fast.

I meldingen beskrives sikkerhetssituasjonen på følgende måte:

> NATO er hjørnesteinen i norsk sikkerhetspolitikk. Alliansetilknytningen er viktig for avskrekkingsformål, og alliert medvirkning vil være særlig viktig i håndteringen av sikkerhetspolitiske kriser eller hvis det skulle inntreffe væpnet konflikt. Samtidig må Norge selv være i stand til å ivareta sine interesser i fredstid, hevde egen suverenitet, drive myndighetsutøvelse, utøve krisehåndtering og om nødvendig kunne håndtere innledende faser av en konflikt.[14]

Norsk forsvarsindustris betydning for ivaretakelse av nasjonale sikkerhetsinteresser, er i meldingen fremhevet på tre sentrale områder.

For det første er det viktig å *opprettholde kompetanse* på områder som er av sentral betydning for Norge. Norges topografi er vesensforskjellig fra andre nasjoner i Vest-Europa. Forsvarets evne til å operere i nærområdene, forutsetter en tilpasning til disse særegne forholdene. Det er derfor nødvendig å opprettholde og videreutvikle kompetansen innenfor norsk forsvarsindustri på disse områdene. I tillegg har Norge i den del tidligere situasjoner valgt nasjonale løsninger for anskaffelse av materiell. Vedlikehold og oppgradering av dette materiellet, forutsetter at norsk forsvarsindustri opprettholder relevant kompetanse.

Et annet forhold som er av betydning er *sårbarheten innenfor moderne kommunikasjonssystemer*. I meldingen vises det til de senere års overvåknings- og avlyttingsskandaler, og at det i denne sammenheng er viktig å ha nasjonal kontroll på enkelte kritiske kommunikasjonssystemer og kritisk teknologi, eksempelvis nasjonal høygradert krypteringsteknologi.

På områder som er kritiske i beredskapssammenheng, vil det være avgjørende å sikre en tilstrekkelig *materiell- og forsyningssikkerhet* for å kunne ivareta nasjonal sikkerhet i en krise-/krigssituasjon. Etter regjeringens syn vil det ikke være en tilfredsstillende løsning at slik forsyningssikkerhet, utelukkende baseres på en annen stats eller utenlandsk aktørs evne og vilje til å kunne levere de varer og tjenester som er nødvendige for å opprettholde et forsvarlig nivå på nasjonal sikkerhet og beredskap:

> Dersom nødvendig kompetanse, produksjons- og vedlikeholdskapasitet på enkelte spesielt kritiske områder ikke er tilgjengelig innenlands, kan resultatet – tross vårt NATO-medlemskap og nære tilknytning til enkelte allierte – bli en uakseptabel avhengighet av en annen stat eller utenlandsk leverandør. Dette vil kunne få konsekvenser for forsyningssikkerheten, og dermed medføre en innskrenkning av vår nasjonale handlefrihet.[15]

12.7 Sentrale eierandelsgrenser i aksjelovgivningen

12.7.1 Innledning

Forholdet mellom aksjeselskaper/allmennaksjeselskaper og selskapets eiere (aksjeeiere/aksjonærer) reguleres av henholdsvis aksjeloven[16] og allmennaksjeloven.[17]

Aksjelovgivningen bygger på en klar rolledeling mellom eierne og selskapsledelsen. Den alminnelige forvaltningen av selskapet hører under styret og selskapets daglige leder, jf. aksjeloven (asl)/allmennaksjeloven (asal) § 6-12.

Aksjeeierne utøver den øverste myndighet av selskapet gjennom generalforsamlingen, jf. asl/asal § 5-1 første ledd. Aksjeeiernes mulighet til å påvirke styringen av selskapet er således gjennom deltakelse i generalforsamlingen. Aksjelovgivningen legger imidlertid begrensninger på hva slags type beslutninger generalforsamlingen kan fatte, jf. asl/asal § 5-21 om misbruk av generalforsamlingens myndighet. Formålet med denne bestemmelsen er å sikre minoritetsaksjonærenes rettigheter overfor majoriteten. Generalforsamlingen kan etter § 5-21 ikke treffe noen beslutning som er egnet til å gi visse aksjeeiere eller andre en urimelig fordel på andre aksjeeieres eller selskapets bekostning.

[14] Ibid., 9.

[15] Ibid.

[16] Lov 13. juni 1997 nr. 44 om aksjeselskaper (aksjeloven).

[17] Lov 13. juni 1997 nr. 45 om allmennaksjeselskaper (allmennaksjeloven).

Utgangspunktet i aksjeretten er at hver aksje har en stemme, jf. asl § 5-2 første ledd første punktum (asal § 5-4 første ledd første punktum). Denne tilnærmingen er et utslag av likhetsgrunnsetningen, som er lovfestet i asl/asal § 4-1 første ledd første punktum. Selskapets vedtekter kan imidlertid inneholde bestemmelser om stemmerettsbegrensninger. I aksjelovgivningen godtas to typer stemmerettsbegrensninger. For det første kan stemmerettsbegrensninger knyttes til person, jf. asl § 5-3 første ledd annet punktum (asal § 5-4 første ledd annet punktum).[18] For det andre kan det i selskapets vedtekter fastsettes at aksjene i en aksjeklasse ikke skal gi stemmerett eller ha begrenset stemmevekt, jf. asl § 5-3 første ledd tredje punktum (asal § 5-4 første ledd tredje punktum).[19]

Gjennom generalforsamlingen vil aksjonærene kunne treffe en rekke sentrale og strategiske beslutninger med virkning for selskapet. I det følgende gjennomgås de eierandelsgrensene som er sentrale i aksjelovgivningen.

12.7.2 Eierandelsgrenser

Hovedregelen i aksjeselskapsretten er at beslutninger fra generalforsamlingen krever flertall (*alminnelig flertall*) av de avgitte stemmene, jf. asl/asal § 5-17 første ledd første punktum. Flertallet beregnes ut fra avgitte stemmer, det vil si ut fra antall aksjer representert på generalforsamlingen. Står stemmetallet likt, er møteleders stemme avgjørende. En eierandel på over halvparten av aksjekapitalen sikrer således normalt kontroll med beslutninger som krever alminnelig flertall av de avgitte stemmer. Dette er beslutninger som godkjenning av årsregnskap (asl § 5-5 og asal § 5-6) og beslutninger om utdeling av utbytte til aksjonærene (asl/asal § 8-2 første ledd). Også valg av medlemmer til selskapets styre krever alminnelig flertall på generalforsamlingen, jf. asl/asal § 6-3 første ledd. Selskapets styre har ansvaret for den alminnelige forvaltningen av selskapet, og kontroll på hvem som velges inn i styret vil således kunne være av stor betydning for en eier.

Fra hovedregelen om alminnelig flertall er det en rekke unntak. For en del viktige avgjørelser krever aksjelovgivningen *kvalifisert flertall*.

For endring av selskapets vedtekter kreves *to tredjedels flertall*, både av avgitte stemmer og av den aksjekapitalen som er representert på generalforsamlingen, jf. asl/asal § 5-18 første ledd annet punktum. I aksjeselskapslovgivningen er det fastsatt noen minstekrav til hva vedtektene må inneholde, herunder lokalisering av forretningskontor og selskapets virksomhet, jf. asl/asal § 2-2 første ledd. To tredjedels flertall kreves også ved beslutninger om fusjon eller fisjon, vedtak om forhøyelse og nedsettelse av aksjekapitalen, opptak av konvertible lån, vedtak om omdanning og vedtak om oppløsning.

En eierandel på over en tredjedel av aksjekapitalen og en tilsvarende andel av stemmene på generalforsamlingen vil således gi negativ kontroll med de beslutninger som krever to tredjedels flertall. Ved negativ kontroll vil eieren således kunne motsette seg vesentlige beslutninger som for eksempel flytting av hovedkontor, andre vedtektsendringer etc.

En annen gruppe beslutninger som krever kvalifisert flertall følger av asl/asal § 15-19. For disse beslutningene er kravet til kvalifisert flertall ytterligere skjerpet ved at det kreves tilslutning fra aksjeeiere som utgjør mer enn *ni tideler* av den aksjekapital som er representert på generalforsamlingen, i tillegg til flertall som for vedtektsendringer (to tredjedels flertall av avgitte stemmer). Dette gjelder blant annet beslutninger som innebærer at aksjeeiernes rett til utbytte eller til selskapets formue reduseres på annen måte enn ved bestemmelse som nevnt i § 2-2 annet ledd.[20]

Noen beslutninger krever *enstemmighet* fra samtlige fremmøtte aksjeeiere, jf. asl/asal § 5-20. Dette gjelder beslutninger som omhandler helt grunnleggende rettsposisjoner aksjeeierne har overfor selskapet, herunder kommer aksjeeiernes forpliktelser i forhold til selskapet, enkelte begrensninger i adgangen til å overdra eller erverve aksjer, beslutning om at aksjer kan være gjenstand for tvungen innløsning, at rettsforholdet mellom tidligere likestilte aksjer endres samt at aksjeeiernes rett til utbytte eller til selskapets formue reduseres.

---

[18] I praksis sondres det mellom tre typer stemmerettsbegrensninger knyttet til person: kvotebegrensninger, kvoteterskler og progressive stemmerettsbegrensninger.

[19] I praksis brukes ofte betegnelsen A-aksjer og B-aksjer om denne type stemmerettsbegrensninger. Det kan være flere grunner til at et selskap opererer med forskjellige aksjeklasser. En grunn kan være at man i et selskap ønsker en nasjonal kontroll med styringen, men tilførsel av utenlandsk kapital. Kilde: Geir Woxholth, *Selskapsrett 5. utgave* (Oslo: Gyldendal Norsk Forlag), 191.

[20] Asl/asal § 2-2 annet ledd omfatter tilfeller der selskapet ikke skal ha til formål å skaffe aksjeeiere økonomisk utbytte.

12.8 Utvalgets vurderinger

Globaliseringen av kapitalmarkedene medfører at utenlandske aktører i økende grad investerer i norske selskaper. Dette er også en konsekvens av Norges EØS-rettslige forpliktelser til å sikre fri bevegelighet for kapital (EØS-avtalen artikkel 40).

Utvalget har vurdert hvorvidt eksisterende regelverk gir tilstrekkelige virkemidler for å kunne ha kontroll med virksomheter som håndterer informasjon, teknologi og/eller fysiske aktiva av betydning for grunnleggende nasjonale funksjoner. Etter utvalgets vurdering gir regelverket for sikkerhetsgraderte anskaffelser i en viss utstrekning mulighet til å kunne ha kontroll. Gjennom leverandørklareringer, vil Sikkerhetsmyndigheten få innsikt i leverandørens eierstrukturer og vil kunne avslå klarering der disse eierstrukturene utgjør en risiko for at grunnleggende nasjonale funksjoner kan bli skadelidende. Leverandørene plikter også å opplyse om endringer i eierstrukturene i klareringens gyldighetstid, slik at Sikkerhetsmyndighetene vil kunne trekke tilbake en leverandørklarering der eierskapskonstellasjonene utvikler seg i en retning som utgjør en økt sikkerhetsmessig risiko. Sikkerhetsgraderte anskaffelser vil således kunne avbøte en del av utfordringene knyttet til bruk av utenlandske leverandører i understøttelsen av grunnleggende nasjonale funksjoner. At Stortinget også har vedtatt at slike leverandørklareringer skal kunne gis for en lengre tidsperiode, og ikke bare for den konkrete anskaffelsen, er også positivt i denne sammenheng. Når det gjelder håndtering av sensitiv og sikkerhetsgradert informasjon og/eller teknologi, vil dette regelverket kunne bidra til å redusere sårbarheten ved å bruke utenlandske aktører.

Likevel mener utvalget at dette regelverket ikke alene vil kunne sikre at grunnleggende nasjonale funksjoner ikke blir skadelidende ved at strategisk viktige selskaper helt eller delvis blir kjøpt opp av utenlandske aktører. Særlig gjelder dette hensynet til forsyningssikkerhet og beredskap. Selskaper som leverer varer eller tjenester av kritisk betydning for grunnleggende nasjonale funksjoner, vil som utgangspunkt kun ha en kontraktuell forpliktelse til slik levering. I en krise- eller krigssituasjon hvor det sannsynligvis vil være knapphet på tilgjengelige ressurser vil det, slik utvalget ser det, ikke være en tilfredsstillende løsning at Norge har basert nødvendig kompetanse, eller produksjons- og vedlikeholdskapasitet på enkelte spesielt kritiske områder, utelukkende på utenlandske leverandører. Ved knapphet på ressurser må man være forberedt på at en slik kontraktuell forpliktelse ikke vil bli overholdt. Behovet til leverandørens hjemstat kan i slike tilfeller bli prioritert. Særlig vil dette gjelde i de tilfeller selskapets hjemstat er en stat Norge ikke har et sikkerhetsmessig samarbeid med.

Utvalgets vurderinger er at myndighetene i dag ikke har tilstrekkelig virkemidler for å kunne sikre nasjonal kontroll med strategisk viktige selskaper. Regelverket for sikkerhetsgraderte anskaffelser, vil ikke alene kunne avbøte de utfordringene som ble skissert innledningsvis. Utvalget mener derfor det er behov for en mekanisme som setter myndighetene i stand til å kunne kontrollere eierskapet i slike selskaper.

Utvalget har vurdert ulike løsninger for hvordan en slik mekanisme bør innrettes. Både av hensyn til Norges EØS-rettslige forpliktelser, og av hensyn til det enkelte selskaps konkurranseevne i et globalt marked, mener utvalget at en mekanisme for å kunne kontrollere eierskapet må være en snever unntaksbestemmelse, som kun anvendes der dette er tvingende nødvendig for å kunne ivareta sikkerheten for grunnleggende nasjonale funksjoner. Utvalget har i denne sammenheng sett hen til hvordan dette er regulert i andre nasjoner vi vanligvis sammenligner oss med. Danmark og Sverige har ikke en slik type regulering. De fleste andre nasjoner utvalget har undersøkt, har imidlertid en eller annen form for mekanisme for å kunne kontrollere eierskapet i strategisk viktige selskaper. Praksis fra henholdsvis USA og Storbritannia viser også at slike mekanismer også blir benyttet, om enn i et meget begrenset omfang. I USA ble det i tidsperioden 2011–2013 satt nærmere vilkår i 27 av de sakene som ble undersøkt, jf. kapittel 12.3.2.5, og i Storbritannia har reguleringen i *The Enterprise Act* (2002) blitt benyttet til å sette nærmere vilkår for erverv i seks tilfeller, jf. kapittel 12.3.3.

Som nevnt innledningsvis er det særlig hensynet til forsyningssikkerhet og beredskap, behovet for å beholde og videreutvikle kritisk kompetanse og behovet for å beholde nasjonal kontroll på sikkerhetsgradert eller annen sensitiv informasjon, som kan begrunne en kontroll med eierskapet i enkelte selskaper. Utvalget mener derfor at en slik hjemmel bør være konkret avgrenset til å omfatte virksomheter som er *av kritisk betydning for grunnleggende nasjonale funksjoner,* jf. utvalgets lovforslag § 1-2 første ledd bokstav a til e. For en nærmere beskrivelse av hva som menes med grunnleggende nasjonale funksjoner, vises det til omtalen i kapittel 6.7.

I utgangspunktet vil det være i strid mot EØS-avtalen å diskriminere mot eiere fra andre EØS-stater. Selv om nasjonal lovgivning vil innebære en diskriminerende behandling av utenlandske EØS-eiere og dermed i utgangspunktet være ulovlig, vil det i helt spesielle tilfeller i medhold av unntakene i EØS-avtalen artikkel 123, artikkel 32 og artikkel 33 (og tilsvarende for den frie bevegelighet av kapital) kunne være anledning til å gripe inn og utøve kontroll med endringer i eierskap når dette er nødvendig av hensyn til sikkerhetsinteresser. Utvalget mener en slik klart avgrenset hjemmel for å utøve eierskapskontroll, kan begrunnes i EØS-avtalens artikkel 123.

Den konkrete avgrensningen til virksomheter av kritisk betydning for grunnleggende nasjonale funksjoner oppfyller, slik utvalget ser det, kravet til presisjon i lovgivningen. I tillegg ivaretas kravet til forholdsmessighet mellom interessene det tas sikte på å beskytte (grunnleggende nasjonale funksjoner) og den forstyrrende innvirkning en slik regulering kan få for det indre markedet i EU/EØS.

Bestemmelsen er ment å være en snever unntaksbestemmelse, og myndighetene vil måtte dokumentere godt i den enkelte sak hvorfor det er nødvendig å gripe inn. Inngripen kan kun skje av hensyn til sikkerhetsinteresser. Bestemmelse må ikke brukes for å ivareta andre interesser, herunder næringspolitiske interesser.

Av hensyn til bestemmelsens inngripende karakter, mener utvalget at vedtaksmyndigheten etter bestemmelsen bør legges til Kongen i statsråd. Dette vil også være i tråd med øvrige inngripende vedtaksbestemmelser som foreslås i loven. Utvalget mener videre at saksbehandlingen av slike saker bør baseres på de samme strukturene som øvrige inngripende vedtaksbestemmelsene, det vil si at det enkelte fagdepartement har ansvaret for å vurdere og eventuelt saksforberede for Kongen i statsråd.

I de tilfeller det fattes vedtak om å nekte eller stille vilkår for et erverv av eierandeler i virksomheten, kan dette få betydelige konsekvenser for selskapet og eierne. Utvalget mener imidlertid at den sikkerhetsmessige gevinsten som oppnås ved at staten har mulighet til å gripe inn i ekstraordinære tilfeller, i et bredere samfunnsperspektiv overstiger den ulempen dette vil ha for de virksomheter som rammes.

Del IV
Særlige merknader og lovforslag

Kapittel 13
Merknader til de enkelte bestemmelsene

Kapittel 1 – Formål og virkeområde

§ 1-1 Lovens formål

Bestemmelsen angir formålet med loven.

I bestemmelsens *første ledd* slås det for det første fast at den skal bidra til å trygge «Norges suverenitet, territorielle integritet og demokratiske styreform». Angivelsen av disse sikkerhetspolitiske interessene, er ikke en uttømmende oppregning av de grunnleggende nasjonale interessene loven tar sikte på å trygge, men er en fremheving av de interessene det er avgjørende å ivareta. Suverenitet og territoriell integritet skal per definisjon være uavkortet, med de begrensninger og tilpasninger som følger av Norges folkerettslige forpliktelser, herunder EØS-avtalen. Ingen andre land eller organisasjoner skal kunne frata Norge råderett over egne anliggender. Landets øverste statsorganer må ha handlefrihet og kontroll innen norsk territorium. Videre innebærer *suverenitet* evne til å hevde nasjonens interesser internasjonalt ved at Norge fører en selvstendig og egendefinert utenrikspolitikk. En forsvarlig beskyttelse vil være avgjørende for å opprettholde rettsstatens og demokratiets grunnleggende verdier.

Begrepet *tilsiktede uønskede hendelser* er nærmere forklart i kapittel 6.7.4. I likhet med dagens sikkerhetslov tar loven sikte på å beskytte grunnleggende nasjonale funksjoner mot terrorhandlinger, sabotasje og spionasje. Loven er imidlertid ikke avgrenset til å gjelde for bare disse truslene. Det er de tilsiktede uønskede hendelsene som kan utgjøre en trussel mot grunnleggende nasjonale funksjoner, det tas sikte på å beskytte mot. Denne avgrensningen vil i seg selv være styrende for hvilke typer tilsiktede hendelser som vil være aktuelle. Eksempelvis vil annen alvorlig kriminalitet, herunder organisert kriminalitet, også kunne ha store skadefølger for grunnleggende nasjonale funksjoner.

Begrepet *grunnleggende nasjonale funksjoner* er grundig behandlet i kapittel 6.7.2. Begrepet er ment å være en rettslig standard som vil bli endret i takt med den generelle samfunnsutviklingen, og formes i tråd med den systematikken loven for øvrig legger opp til når det gjelder identifisering av slike funksjoner og deres understøttende elementer.

Virkemidler som er tilgjengelige for å sikre grunnleggende nasjonale funksjoner, kan på samme tid gjøre at de samme interessene og verdiene det tas sikte på å beskytte kommer under press. I bestemmelsens *andre ledd* er det derfor presisert at sikkerhetstiltak som iverksettes for å ivareta lovens formål, skal gjennomføres på en måte som er «forenlig med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn». Med *grunnleggende rettsprinsipper og verdier* menes blant annet hensynet til den enkeltes personvern og rettssikkerhet. I dette ligger en presiseringen av at det kun er de sikkerhetsmessige tiltakene som er nødvendige og forholdsmessige, og har en dokumentert effekt, som skal iverksettes. Det ligger også en plikt til å vurdere alternative og mindre inngripende tilnærminger til å oppnå samme effekt.

§ 1-2 Lovens virkeområde

Bestemmelsen angir lovens saklige virkeområde.

Virksomhetsbegrepet i loven, jf. bestemmelsens *første ledd*, omfatter alle former for virksomhet, uavhengig av eierskap og organisasjonsform, og er således en videreføring av gjeldende sikkerhetslovs virksomhetsbegrep. Ved vurderingen av om en *virksomhet* omfattes av loven er det uten betydning om det er tale om et privat selskap, foretak, forvaltningsorgan, forvaltningsbedrift, et hel- eller deleid statlig selskap, statsforetak, ideell organisasjon, stiftelse eller annet.

Et vilkår for at virksomheter omfattes av loven er at disse *råder over* nærmere angitt informasjon, informasjonssystemer objekter eller infrastruktur. Det avgjørende for hvorvidt en virksomhet *råder over* vil måtte avgjøres konkret i hvert enkelt tilfelle, ut fra en vurdering av om virksomheten har en faktisk og reell innflytelse/påvirkningsmulig-

het over informasjonen, informasjonssystemet, objektet eller infrastrukturen.

Hva som menes med *informasjon* er nærmere omtalt i merknaden til § 5-1.

Hva som menes med *informasjonssystem* er nærmere omtalt i merknaden til § 6-1.

Hva som menes med *objekt* og *infrastruktur* er nærmere omtalt i kapittel 9.5.1.

Også virksomheter som *driver aktivitet* av kritisk betydning for grunnleggende nasjonale funksjoner vil være omfattet av loven. Eksempelvis vil selskaper som har en nøkkelkompetanse som er av betydning for slike kunne tenkes å bli omfattet av loven. Normalt vil virksomheter som driver slik aktivitet, også ha en eller annen form for råderett over informasjon, informasjonssystemer, objekter eller infrastruktur, slik at de uansett vil falle inn under lovens virkeområde.

I begrepet *kritisk for* grunnleggende nasjonale funksjoner ligger et kvalitetskrav. Det er ikke tilstrekkelig at virksomheter leverer innsatsfaktorer for grunnleggende nasjonale funksjoner, for at de skal falle inn under loven. Det er kun de aktørene som har en så sentral rolle for funksjonene at de må anses som avgjørende for evnen til å opprettholdelse av funksjonsdyktighet, som vil omfattes. Avgjørende for vurderingen er hvilken betydning bortfall eller svekkelse av virksomheten har for den funksjonen som virksomheten understøtter. Den nærmere vurderingen av hvilke virksomheter som konkret vil falle inn under lovens virkeområdet må gjøres konkret, jf. loven § 2-1 om departementenes plikter. Se for øvrig kapittel 6.7.5 og 7.7.1.

For en nærmere omtale av de interessene som er listet opp i *første ledd bokstav a til e*, vises det til kapittel 6.7.2.

Bokstav a til c er identisk med straffeloven § 121 første ledd bokstav a til c. Praksis knyttet til forståelsen av de ulike forholdene i straffeloven, vil således også være relevante for forståelsen av tilsvarende forholdene i sikkerhetsloven.

Kongen i statsråd er i bestemmelsens andre ledd gitt myndighet til å gi nærmere forskrifter om lovens virkeområde. Myndigheten kan ikke delegeres, jf. den nærmere omtalen av dette i kapittel 7.7.10.

§ 1-3 Særbestemmelser om lovens virkeområde

I motsetning til gjeldende sikkerhetslov § 2 femte ledd, gjøres det ikke direkte unntak for Stortinget og dets organer. Bestemmelsens *første ledd* slår i stedet fast at loven gjelder for Stortinget og dets organer i den utstrekning Stortinget bestemmer det. Det forutsettes at Stortinget gjør et formelt vedtak om spørsmålet.

Bestemmelsens *andre ledd* er en videreføring av det vedtatte forslaget i Prop. 97 L (2015–2016) om en lovfesting av en langvarig og fast praksis om at det ikke stilles krav om sikkerhetsklarering og autorisasjon for regjeringens medlemmer og dommere i Høyesterett.

Bestemmelsens *tredje ledd* er en videreføring av gjeldende lov § 2 fjerde ledd om særregler for sikkerhetsklarering etter domstolloven og straffeprosessloven.

Bestemmelsens *fjerde ledd* er en videreføring av gjeldende lov § 2 andre ledd om at leverandører til sikkerhetsgraderte anskaffelser automatisk er omfattet av loven.

Bestemmelsens *femte ledd* er i hovedsak en videreføring av gjeldende lov § 2 sjette ledd, med de tilpasninger som er nødvendige i en modernisert lov. Med *bilandene* menes Bouvet-øya, Peter I's øy og Dronning Maud Land, jf. lov 27. februar 1930 nr. 3 § 1.

Kapittel 2 – Myndigheter etter loven

§ 2-1 Departementenes ansvar og myndighet etter loven

Bestemmelsen etablerer lovens systematikk for å identifisere hvilke grunnleggende nasjonale funksjoner som omfattes av loven og en systematikk for å kartlegge virksomheter som har en sentral rolle i understøttelsen av slike funksjoner.

Bestemmelsens *første ledd* slår fast at hvert enkelt departement er ansvarlig for forebyggende sikkerhet innenfor sitt myndighetsområde. Departementenes *myndighetsområde* vil følge den til enhver tid sittende regjerings fordeling av ansvar mellom statsrådene og de ulike departementene. Dette innebærer både at de ansvarlige departementene gis myndighet til å fatte vedtak overfor virksomheter i egen sektor, og et særlig ansvar for å følge opp at det skjer et forsvarlig forebyggende sikkerhetsarbeid i sektoren. Ved endring av departementsstrukturen, forutsettes det at regjeringen tar stilling til mulige konsekvenser for fordeling av myndighetsområder etter loven.

Første ledd bokstav a til c slår fast departementenes fremgangsmåte for å identifisere og fatte vedtak overfor de virksomheter som skal omfattes av loven. Det foreslås her en modell som består av tre trinn.

Departementene skal i henhold til *bokstav a*, først identifisere hvilke grunnleggende nasjonale funksjoner som finnes innenfor eget myndighetsområde. Med *holde oversikt over* menes at departe-

mentenes identifisering skal være en dynamisk prosess som må oppdateres ved behov.

På bakgrunn av departementenes oversikt over grunnleggende nasjonale funksjoner, plikter departementene etter *bokstav b*, å identifisere og holde oversikt over virksomheter som er av vesentlig betydning for understøttelsen av slike funksjoner.

Det at en virksomhet identifiseres som en virksomhet av *vesentlig betydning* innebærer ikke at det påhviler virksomheten plikter etter loven. Det er imidlertid viktig at departementene til enhver tid har en oversikt over hvilke innsatsfaktorer grunnleggende nasjonale funksjonene er avhengige av for å kunne opprettholde sin funksjonalitet. Generelle samfunnsmessige endringer, eller endringer i det gjeldende trusselbildet, kan også medføre at virksomheter som tidligere ikke har blitt ansett som kritiske, blir det. Systematikken det legges opp til i bestemmelsen er ment å skulle legge til rette for at slike endringer blir fanget opp.

Ut fra den totale oversikten over grunnleggende nasjonale funksjoner og virksomheter av vesentlig betydning for disse, skal departementet treffe enkeltvedtak overfor de virksomheter som er av kritisk betydning for de aktuelle funksjonene, jf. bestemmelsen første ledd *bokstav c*. Ved vurderingen av om en virksomhet er av *kritisk betydning* må det sees hen til virkeområdebestemmelsen i § 1-2, herunder om den aktuelle virksomheten råder over informasjon, informasjonssystemer, objekter eller infrastruktur, eller driver aktivitet, av slik betydning for grunnleggende nasjonale funksjoner.

I bestemmelsens *andre ledd første punktum* pålegges departementene en varslingsplikt til de virksomheter departementet har til hensikt å treffe vedtak overfor, jf. forvaltningsloven § 16. En slik forutgående varsling vil gi den aktuelle virksomheten mulighet til å kunne fremme sine synspunkter, før vedtak treffes. Bestemmelsens *andre ledd andre punktum*, slår fast at selvstendige rettssubjekter har rett til å påklage departementets vedtak etter første ledd bokstav c. Med *selvstendige rettssubjekter* menes enhver virksomhet som et departement ikke innehar alminnelig instruksjons-, organisasjons- og kontrollmyndighet overfor, i praksis alle virksomheter som ikke er en del av staten som rettssubjekt. For selvstendige rettssubjekters klageadgang, gjelder forvaltningslovens kapittel VI.

I bestemmelsens *tredje ledd* pålegges departementene å holde Sikkerhetsmyndigheten orientert om oversikter og vedtak som fattes etter første ledd bokstav a til c. Formålet med denne bestemmelsen er å legge til rette for at Sikkerhetsmyndigheten skal kunne ivareta sitt ansvar etter § 2-2.

I bestemmelsens *fjerde ledd første punktum* gis Sikkerhetsmyndigheten en forslagsrett overfor ansvarlig departement. Sikkerhetsmyndigheten har et sektorovergripende ansvar etter § 2-2, og vil kunne se gjensidige avhengigheter på tvers av samfunnssektorene, som det enkelte departement ikke nødvendigvis har forutsetninger for å identifisere. I tillegg vil Sikkerhetsmyndigheten kunne påpeke mangler i departementenes identifisering av, og vedtak overfor, virksomheter.

Dersom det aktuelle departement velger å ikke følge de forslag Sikkerhetsmyndigheten kommer med, gis Sikkerhetsmyndigheten i *fjerde ledd andre punktum* rett til å bringe saken inn for Tvisteorganet dersom Sikkerhetsmyndigheten vurderer departementets unnlatelse som uforsvarlig. At departementets unnlatelser må være *uforsvarlig* innebærer at terskelen for hvilke unnlatelser som kan bringes inn for Tvisteorganet, vil være høy. Hva som vil være *uforsvarlig* i den konkrete sak, må også ses i sammenheng med den rettslige standarden i § 4-1 tredje ledd, se merknad til denne.

I bestemmelsens *femte ledd* gis Kongen i statsråd myndighet til å fastsette nærmere bestemmelser om departementenes ansvar og myndighet. At myndigheten legges til *Kongen i statsråd* innebærer at forskriftsmyndigheten etter bestemmelsen, ikke kan delegeres.

§ 2-2 Sikkerhetsmyndigheten

Bestemmelsen angir Sikkerhetsmyndighetens ansvar og myndighet etter loven. I praksis vil funksjonen som sikkerhetsmyndighet ivaretas av den aktøren som får delegert myndigheten fra forvaltningsansvarlig departement.

I *bestemmelsens første ledd første punktum* slås det fast at Sikkerhetsmyndigheten har det sektorovergripende ansvaret for forebyggende sikkerhetsarbeid i medhold av loven. Sikkerhetsmyndighetens ansvar griper ikke inn i de enkelte departementenes ansvar innen eget myndighetsområde. Med *sektorovergripende ansvar* menes i første rekke ansvaret for at forebyggende sikkerhetsarbeid etter loven har en helhetlig tilnærming og ansvaret for å koordinere sikkerhetsarbeidet mellom ulike departementer og ulike relevante sektormyndigheter. Sikkerhetsmyndighetens ansvar er nærmere konkretisert i *første ledd bokstav a til e*.

Etter *bokstav a* plikter Sikkerhetsmyndigheten å påse at det føres tilsyn med de virksomheter som er underlagt loven. De nærmere reglene om tilsyn følger av loven kapittel 3.

Bokstav b regulerer Sikkerhetsmyndighetens råd- og veiledningsansvar etter loven. Sikkerhetsmyndigheten skal ha en aktiv rolle når det gjelder konkret rådgivning overfor virksomhetene. For en nærmere omtale av råd- og veiledningsplikten vises det til kapittel 7.7.3.

Bokstav c omhandler Sikkerhetsmyndighetens ansvar for å utarbeide generelle veiledninger og rundskriv innen de ulike fagområdene loven omfatter. Plikten til å utarbeide denne type informasjon er en sentral fagmyndighetsoppgave.

I *bokstav d* pålegges Sikkerhetsmyndigheten å holde en tverrsektoriell og nasjonal oversikt over de funksjoner og virksomheter som er blitt identifisert av departementene etter § 2-1 første ledd bokstav a til c. Plikten til å holde en slik tverrsektoriell oversikt er en sentral del av Sikkerhetsmyndighetens sektorovergripende ansvar, og vil også danne grunnlaget for Sikkerhetsmyndighetens forslagsrett overfor departementene når det gjelder virksomheter som bør underlegges loven.

Den tverrsektorielle oversikten innbefatter også et særskilt ansvar for å identifisere gjensidige avhengigheter på tvers av samfunnssektorer og på tvers av virksomheter, slik at denne type avhengigheter kan synliggjøres overfor de ansvarlige departementene.

I *bokstav e* er Sikkerhetsmyndigheten gitt myndighet til å kunne treffe enkeltvedtak overfor virksomheter som ikke anses å falle inn under et departements ansvarsområde. Myndigheten korresponderer med departementenes myndighet etter § 1-2 første ledd bokstav c, og skal fange opp de virksomheter som ikke naturlig tilhører en klart definert samfunnssektor. Et eksempel her vil kunne være virksomheter innen satellittbaserte tjenester, hvor det i dag er til dels uoversiktlige ansvarslinjer, se kapittel 7.4.8.

Bestemmelsens *andre ledd* slår fast at varslingsplikten og klageretten etter § 2-1 andre ledd gjelder tilsvarende for Sikkerhetsmyndighetens vedtak overfor virksomheter.

§ 2-3 Informasjon om trusselvurderinger og risikohåndtering

Bestemmelsen omhandler Sikkerhetsmyndighetens ansvar for å legge til rette for, og koordinere, informasjon om trusselvurderinger. At bestemmelsen er innrettet som en tilretteleggings- og koordineringsplikt, skyldes primært at Sikkerhetsmyndigheten ikke vil ha full råderett over all trussel- og sikkerhetsinformasjon. For informasjon som utarbeides av andre relevante aktører, herunder Politiets sikkerhetstjeneste og Etterretningstjenesten, vil det i siste instans være opp til disse tjenestene hvorvidt de har anledning til å dele denne informasjonen. All informasjonsutveksling etter denne bestemmelsen må skje innenfor rammene av lovbestemt taushetsplikt og innenfor rammene av den enkelte aktørs lovmessige adgang til å dele slik informasjon.

Etter bestemmelsens *første ledd* plikter Sikkerhetsmyndigheten å legge til rette for at sektormyndigheter og virksomheter som er underlagt loven, får tilgang til informasjon som er nødvendig for å sette disse i stand til å etterleve sine plikter etter loven, eksempelvis virksomhetenes plikt til å gjennomføre risiko- og sårbarhetsanalyse, jf. § 4-3.

Som nevnt ovenfor er det flere aktører som har ansvar for å utarbeide ulike former for trusselvurderinger og annen sikkerhetsrelevant informasjon. Etter bestemmelsens *andre ledd* pålegges Sikkerhetsmyndigheten å koordinere tilgjengeliggjøring av slik informasjon. I tillegg skal Sikkerhetsmyndigheten påse at det etableres nødvendige arenaer for informasjons- og erfaringsutveksling. Av hensyn til de ulike samfunnssektorenes særegenheter og ulike behov, kan det være hensiktsmessig å ha sektorvise fora for slik erfarings- og informasjonsutveksling.

§ 2-4 Nasjonal responsfunksjon for alvorlige dataangrep

Bestemmelsen er en videreføring av det vedtatte forslaget i Prop. 97 L (2015–2016) til lovfesting av NorCERT og varslingssystemet for digital infrastruktur, jf. lovforslaget § 9 første ledd bokstav e og § 10a.

Bestemmelsen er ikke ment å innebære noen materiell endring fra det opprinnelige lovforslaget, se kapittel 7.3.3 og 7.7.6.

§ 2-5 Vedtaksmyndighet for Kongen i statsråd

Bestemmelsen er i det vesentlige en videreføring av det vedtatte forslaget om vedtaksmyndighet for Kongen i statsråd i Prop. 97 L (2015–2016), jf. lovforslaget § 5a andre ledd. Bestemmelsen gir Kongen i statsråd myndighet til å fatte vedtak om å stanse, begrense eller endre aktiviteter som medfører skadevirkninger på grunnleggende nasjonale funksjoner. Med *stor grad av sannsynlighet* menes at det må foreligge mer enn alminnelig sannsynlighetsovervekt for at den aktuelle aktivi-

teten kan medføre slik skade. Hvorvidt sannsynlighetskravet er oppfylt må vurderes konkret.

I bestemmelsens *andre ledd* slås det fast at vedtak etter bestemmelsen skal være proporsjonalt med den risiko som aktiviteten utgjør.

Dersom saken av hensyn til potensielle skadevirkninger ikke kan utredes tilstrekkelig før vedtak treffes, skal det i medhold av bestemmelsens *fjerde ledd* gjennomføres en etterfølgende saksbehandling med sikte på å rette slik mangler.

For en nærmere omtale av bestemmelsen, vises det til kapittel 7.7.8.

Bestemmelsen må også sees i sammenheng med virksomhetenes varslingsplikt etter § 4-6 første ledd bokstav c, jf. tredje ledd.

§ 2-6 Klage og tvisteløsning

Bestemmelsen gir nærmere anvisning på hvordan klager og tvister etter loven skal behandles.

I bestemmelsens *første ledd første punktum* slås det fast at vedtak som fattes med hjemmel i loven som hovedregel kan bringes inn for Tvisteorganet for forebyggende sikkerhet. Tvisteorganet er nærmere omtalt i merknaden til § 2-7. I første ledd andre punktum gjøres det for det første unntak for de vedtak som fattes med hjemmel i §§ 2-5, 9-4 eller 10-1. Felles for de opplistede vedtakshjemlene er at myndighet til å fatte vedtak er lagt til Kongen i statsråd. Disse vedtakene kan ikke påklages, men tvister kan på vanlig måte bringes inn for domstolene for overprøving. I tillegg gjøres det unntak for vedtak som nevnt i andre ledd.

I bestemmelsens *andre ledd* slås det fast at vedtak fattet i medhold av lovens kapittel 8 om personellsikkerhet, kan påklages til Sikkerhetsmyndigheten, og til departementet der Sikkerhetsmyndigheten er klareringsmyndighet. Dette er en videreføring av gjeldende sikkerhetslovs regulering av klagemuligheten for klareringssaker, se de særlige merknadene til lovens kapittel 8.

I bestemmelsens *tredje ledd* slås det fast at forvaltningslovens kapittel VI gjelder for selvstendige rettssubjekter klageadgang etter loven. Det følger av bestemmelsens første og andre ledd at klageinstansen er henholdsvis Tvisteorganet og Sikkerhetsmyndigheten. Dette er unntak fra hovedregelen i forvaltningsloven § 28 første ledd. For virksomheter som er underlagt departementenes alminnelige instruksjons- og kontrollmyndighet gjelder ikke klageadgangen.

§ 2-7 Tvisteorgan for forebyggende nasjonal sikkerhet

I bestemmelsen gis det nærmere prosedyreregler for utpeking av Tvisteorganet og for oppnevning av organets medlemmer. Tvisteorganets organisering og myndighet er nærmere omtalt i kapittel 7.7.7.

I bestemmelsens *andre ledd* slås det fast at det ved oppnevning av medlemmer til tvisteorganet, også skal legges vekt på kompetanse innen *personvern* og *rettssikkerhet*. Tvisteorganet er en sentral rettssikkerhetsgaranti for selvstendige rettssubjekter som blir underlagt loven ved enkeltvedtak, og det er derfor viktig at tvisteorganet består av medlemmer som besitter kompetanse som er relevant for selvstendige rettssubjekter, i tillegg til sikkerhetsfaglig kompetanse.

Av bestemmelsens *fjerde ledd* fremgår det at tvisteorganet skal avgi en årlig rapport. Formålet med slik rapportering er dels å gi allmennheten informasjon om Tvisteorganets virke og dels å gi relevante aktører mer konkret informasjon om praksis av betydning. Rapporteringen bør derfor innrettes slik at i hvert fall deler av innholdet er egnet for offentliggjøring.

Kapittel 3 – Tilsyn etter loven

§ 3-1 Tilsyn med virksomheter

Bestemmelsen regulerer fordeling av tilsynsansvar etter loven.

I bestemmelsens *første ledd* slås det fast at Sikkerhetsmyndigheten skal føre tilsyn med departementenes gjennomføring av loven.

I bestemmelsens *andre ledd* gis ansvarlig departement myndighet til å bestemme at tilsynsfunksjonen etter loven kan ivaretas av en sektormyndighet. Med *ansvarlig departement* menes i denne sammenheng det departement som i medhold av § 2-1 har det overordnede ansvaret for forebyggende sikkerhet i den aktuelle samfunnssektoren. Et vilkår for at departementet kan treffe en slik beslutning er at det finnes en sektormyndighet i den aktuelle samfunnssektoren som har en tilsynsfunksjon «som omfatter beskyttelse av informasjon, informasjonssystemer, objekter eller infrastruktur». At oppregningen er alternativ, innebærer at tilsynsfunksjonen ikke trenger å omfatte alle elementer. Hvorvidt tilsynsmyndigheten skal tillegges en sektormyndighet beror på en helhetsvurdering, hvor det blant annet må tas stilling til om den aktuelle sektormyndigheten har nødvendig sikkerhetsfaglig kompetanse til å ivareta tilsynsansvaret på en forsvarlig måte.

I bestemmelsens *tredje ledd* slås det fast at Sikkerhetsmyndigheten skal ha tilsynsansvaret i samfunnssektorer der det ikke finnes sektormyndigheter som nevnt i andre ledd. Denne tilsynsfunksjonen er basert på samarbeidsmodellen i § 3-2.

Sikkerhetsmyndigheten skal i henhold til bestemmelsens *fjerde ledd* føre tilsyn med de sektormyndighetene som er tillagt tilsynsansvar i medhold av andre ledd. Tilsynsansvaret overfor sektormyndighetene må sees i sammenheng med Sikkerhetsmyndighetens sektorovergripende ansvar og ansvaret for å påse at det føres tilsyn med gjennomføringen av lovens bestemmelser, jf. § 2-2 første ledd bokstav a.

§ 3-2 Sikkerhetsmyndighetens samarbeid med sektormyndigheter

Bestemmelsen regulerer samhandlings- og koordineringsplikten mellom Sikkerhetsmyndigheten og relevante sektormyndigheter innen de ulike samfunnssektorene. Bestemmelsen må sees i sammenheng med fordeling av tilsynsansvaret etter § 3-1.

Bestemmelsens *første ledd* slår fast en samarbeidsplikt mellom Sikkerhetsmyndigheten, sektormyndigheter tillagt tilsynsansvar etter loven og andre relevante myndigheter som har tilsynsfunksjoner etter annet regelverk.

Bestemmelsens *andre ledd* slår fast et prinsipp om at gjennomføring av tilsyn, så langt det er mulig, skal samordnes og koordineres mellom Sikkerhetsmyndighet og aktuelle tilsynsmyndigheter. Dette gjelder både i forhold til tilsynsmyndigheter med oppgaver som nevnt i § 3-1 andre ledd, og for andre tilsynsmyndigheter som fører tilsyn på andre områder. Formålet med bestemmelsen er å etablere en koordineringsplikt mellom tilsynsorganer, slik at den totale belastningen for tilsynsobjektene ikke blir høyere enn strengt nødvendig. En slik koordinering kan skje på flere måter, enten ved at tilsyn samordnes slik at det gjennomføres felles samtidige tilsyn eller ved at det avtales hvilke tidspunkter tilsyn skal skje på, slik at tilsynsobjektene ikke blir utsatt for to ulike tilsyn over en kort tidsperiode.

Etter bestemmelsens *tredje ledd* skal samarbeidet mellom Sikkerhetsmyndigheten og sektormyndighet tillagt tilsynsansvar etter § 3-1, formaliseres gjennom en samarbeidsavtale. En slik samarbeidsavtale bør som minimum omhandle ansvarsfordelingen mellom partene og hvordan den konkrete samhandlingen mellom dem skal skje.

I bestemmelsens *fjerde ledd* gis Sikkerhetsmyndigheten myndighet til å utarbeide og vedlikeholde grunnleggende kriterier for tilsyn etter loven (*bokstav a*) og forestå opplæring av sektormyndighetenes tilsynspersonell (*bokstav b*). En forutsetning for at Sikkerhetsmyndigheten skal kunne ivareta sitt sektorovergripende ansvar etter § 2-2, er at myndigheten gis en mulighet til å påvirke hva det skal føres tilsyn med, hvordan dette skal gjøres, samt mulighet til å sikre at tilsynspersonellet har den nødvendige kompetansen. Med «grunnleggende kriterier for tilsyn etter loven» menes overordnede føringer som sikrer at lovens formål ivaretas på en forsvarlig måte, også der tilsynsansvaret er delegert til aktuelle sektormyndigheter. Sektormyndighetene vil samtidig ha adgang til å supplere disse overordnede føringene med spesifikke kriterier som er tilpasset den enkelte samfunnssektor.

Bestemmelsens *femte ledd første punktum* regulerer Sikkerhetsmyndighetens adgang til å delta i forberedelse og gjennomføring av sektormyndighetenes tilsyn. Sikkerhetsmyndighetens rett til å delta er dels begrunnet i det sektorovergripende ansvaret, og dels Sikkerhetsmyndighetens behov for innsikt i den enkelte samfunnssektor. Gjennom deltakelse på tilsyn vil Sikkerhetsmyndigheten både kunne kvalitetssikre at tilsyn skjer på en sikkerhetsmessig forsvarlig måte og kunne bidra med sin sikkerhetsfaglige kompetanse. Etter *femte ledd andre punktum* kan sektormyndigheten anmode Sikkerhetsmyndigheten om bistand til forberedelser og/eller gjennomføring av tilsyn. Samhandlingen mellom Sikkerhetsmyndigheten og sektormyndighetene, herunder eventuell deltakelse på tilsyn, bør fortrinnsvis reguleres i samarbeidsavtalen mellom partene, jf. bestemmelsens tredje ledd. Sikkerhetsmyndighetens adgang til å kreve å delta, vil således fungere som en sikkerhetsventil for de tilfeller der det ut fra sikkerhetsfaglige hensyn anses nødvendig.

Bestemmelsen *sjette ledd* regulerer sektormyndighetenes rapporteringsplikt til Sikkerhetsmyndigheten. Formålet med rapporteringsplikten er å sikre at Sikkerhetsmyndigheten får tilgang til nødvendig informasjon for å kunne ivareta sitt sektorovergripende ansvar. Noen tilsynsaktiviteter vil være løpende, andre periodiske og atter andre hendelsesbaserte. I tillegg vil det kunne være tale om både stedlige tilsyn og dokumentbaserte tilsyn, muligens også maskinelt baserte tilsyn (testing). Det vil ikke foreligge noen rapporteringsplikt i alle slike tilfeller, derav henvisningen til at plikten er begrenset til rapportering av *hovedfunn*. De nærmere reglene for hvilke typer tilsyns-

aktiviteter som skal rapporteres bør konkretiseres på forskriftsnivå, jf. bestemmelsens *sjuende ledd*.

§ 3-3 Generelle prinsipper for tilsyn

Bestemmelsen angir de generelle prinsippene for gjennomføring av tilsyn etter loven. Bestemmelsen gjelder både for Sikkerhetsmyndigheten og for sektormyndigheter tillagt tilsynsansvar etter loven.

I bestemmelsens *første ledd* slås det fast at tilsyn etter loven skal skje på en slik måte at det virker minst mulig forstyrrende på daglig drift. Tilsyn kan være en belastning for de virksomheter som utsettes for dette, både ved at det er ressurskrevende for tilsynsobjektene å forberede tilsyn og ved at stedlig tilsyn potensielt kan medføre at den daglige drift blir redusert i den tidsperioden tilsynet pågår. En god forutgående dialog, der dette er mulig uten å undergrave formålet med tilsynet, vil i de fleste tilfeller kunne redusere unødvendig merarbeid og potensiell negativ innvirkning på daglig drift.

Bestemmelsens *andre ledd* angir en formålsavgrensning for bruk av opplysninger som tilsynsmyndigheten innhenter som ledd i tilsynet.

Tredje ledd er en presisering av at forvaltningslovens bestemmelser om taushetsplikt gjelder for tilsynspersonellet. I den utstrekning personellet får informasjon som er sikkerhetsgradert etter sikkerhetsloven, vil personellet også ha taushetsplikt om slik informasjon, jf. § 5-3 andre ledd.

§ 3-4 Stedlig tilsyn

Gjennomføring av stedlige tilsyn forutsetter at tilsynsmyndigheten får tilgang til tilsynsobjektet, enten det er informasjon, objekt eller infrastruktur.

Bestemmelsens *første ledd* fastslår at tilsynsmyndigheten kan kreve å få tilgang der dette er nødvendig for en forsvarlig gjennomføring av tilsynet.

Bestemmelsens *andre ledd* slår fast at tilsyn som hovedregel skal varsles skriftlig. Med *normalt varsles* tas det forbehold om at forutgående varsel i enkelte tilfeller ikke vil være mulig eller ønskelig, da dette vil kunne undergrave formålet med tilsynet.

§ 3-5 Tilsynsmyndighetens behandling av personopplysninger

Bestemmelsen inneholder særlige bestemmelser om tilsynsmyndighetens behandling av personopplysninger. Bestemmelsen i § 4-7 om personopplysningsvern gjelder generelt for all behandling av personopplysninger etter loven.

Som ledd i tilsynsvirksomheten vil tilsynsmyndigheten kunne få tilgang til personopplysninger, enten fordi det er behov for å behandle slike opplysninger eller som overskuddsinformasjon sammen med annen informasjon som er relevant for gjennomføring av tilsyn.

Bestemmelsens *første ledd* etablerer et generelt hjemmelsgrunnlag for behandling av personopplysninger der dette er nødvendig for å utføre tilsynsoppgavene etter loven.

I bestemmelsens *andre ledd* slås det fast at tilsynsmyndighetens behandling av personopplysninger kun kan skje der dette etter konkret vurdering fremstår som nødvendig og proporsjonalt i forhold til det inngrepet behandlingen representerer. Bestemmelsen er en lovfesting av nødvendighets- og proporsjonalitetsprinsippet.

I *tredje ledd* gis det nærmere prosedyreregler for tilsynsmyndighetenes behandling av personopplysninger. Som hovedregel skal personopplysninger kun behandles ved hjelp av virksomhetens egne informasjonssystemer. Tilsynsmyndigheten kan kun kreve kopi av personopplysninger i den utstrekning dette er nødvendig for å påvise eller avkrefte lovbrudd. Dersom det tas slik kopi av personopplysninger plikter tilsynsmyndigheten å varsle virksomheten om at dette er gjort.

§ 3-6 Pålegg

Bestemmelsen regulerer vilkårene for at det skal kunne ilegges pålegg etter loven, samt hvordan påleggsmyndigheten er fordelt.

I bestemmelsens *første ledd* slås det fast at to vilkår må være oppfylt for at det skal kunne ilegges pålegg etter loven. For det første må det være «utvilsomt at tiltaket er nødvendig» for å ivareta lovens formål. Med dette menes at den sikkerhetsmessige effekten ved pålegg om å iverksette sikkerhetstiltak må kunne dokumenteres med høy grad av sannsynlighet. For det andre må de kostnadene som påføres virksomheten som følge av pålegget «stå i et rimelig forhold til det som kan oppnås». Med dette menes at det må foretas en konkret vurdering av om nytten som kan oppnås for samfunnet, står i et rimelig forhold til de kostnadene pålegget fører med seg. Dette slik at sik-

kerhetstiltakene som pålegges ikke antas å bli uforholdsmessig kostbare for den enkelte virksomhet. Vilkåret må sees i sammenheng med § 4-1 andre ledd.

Bestemmelsens *andre ledd* fordeler påleggsmyndigheten mellom Sikkerhetsmyndigheten og relevante sektormyndigheter, hvor påleggsmyndigheten tilligger den aktøren som er tillagt tilsynsansvaret i medhold av § 3-1.

I medhold av bestemmelsen *tredje ledd* er Sikkerhetsmyndigheten gitt myndighet til å ilegge sektormyndigheter pålegg. Et vilkår for å kunne ilegge slike pålegg er at det vurderes som nødvendige å sikre at lovens formål ivaretas.

I bestemmelsens *fjerde ledd første punktum* slås det fast at pålegg kan påklages til Tvisteorganet. Dette gjelder også når Sikkerhetsmyndigheten har gitt pålegg til en sektormyndighet. For selvstendige rettssubjekter gjelder forvaltningsloven kapittel VI, jf. *fjerde ledd andre punktum*.

Kapittel 4 – Generelle krav til forebyggende sikkerhet

§ 4-1 Plikt til å gjennomføre sikkerhetstiltak

Bestemmelsen regulerer de generelle pliktene til å gjennomføre sikkerhetstiltak for virksomheter som er underlagt loven ved enkeltvedtak, jf. §§ 2-1 første ledd bokstav c og 2-2 første ledd bokstav e.

Bestemmelsens *første ledd* understreker at forebyggende risikoreduserende tiltak mot tilsiktede uønskede hendelser omfatter både tiltak som reduserer sannsynligheten for at hendelsen inntreffer (*bokstav a*) og tiltak som reduserer konsekvensene av hendelsen ved å redusere skadeomfanget (bokstav b). Nødvendig reduksjon av risiko oppnås ved å vurdere og iverksette enkeltstående tiltak eller kombinasjoner av flere typer tiltak. Kombinasjoner av tiltak vil ofte være aktuelt. Tiltak kan være av en art som direkte reduserer sannsynligheten for at hendelser rammer et spesifikt objekt eller en infrastruktur. Eksempler på dette er ulike former for barrierer, systemer for tidlig deteksjon av uønskede hendelser, verifikasjonssystemer og ulike former for reaksjon for å stoppe eller redusere omfanget av slike hendelser. Reduksjon av risiko kan også bestå av tiltak som reduserer skadevirkningene dersom en hendelse inntreffer. Dette kan enten være tiltak som baseres på økt redundans eller økt resiliens, eller kombinasjon av slike tiltak. Høy redundans innebærer at det er flere enheter eller delsystemer som bidrar til å opprettholde funksjonen. Dersom noen av enhetene eller delsystemene mister sin funksjon vil de øvrige kunne fylle funksjonen til den eller de som er falt ut, og dermed forhindre alvorlige konsekvenser. Høy resiliens betyr at funksjonen har stor evne til å raskt gjenopprette normaltilstand dersom hele eller deler av funksjonen blir påvirket av en hendelse. Summen av tiltak som forhindrer at hendelser inntreffer, gir redundans og resiliens, er det som gjør et system robust.

Som grunnlag for virksomhetens sikkerhetstiltak skal virksomheten gjøre en risiko- og sårbarhetsanalyse, jf. bestemmelsen *første ledd første punktum* og § 4-3.

Begrepet *forsvarlig sikkerhetsnivå* er en rettslig standard som trekker opp de ytre rammene for hvilket handlingsrom virksomheten har når det gjelder etablering av sikkerhetstiltak. Innholdet i den rettslige standarden er nærmere omtalt i kapittel 7.7.9.

Sikkerhetstiltakene for å oppnå et forsvarlig sikkerhetsnivå skal inkludere alle tiltak for å ivareta lovens formål, herunder informasjonssikkerhet, fysisk sikkerhet og personellsikkerhet, samt andre relevante sikkerhetstiltak. Det er kombinasjonen av relevante tiltak som er avgjørende for om virksomheten kan sies å ha et forsvarlig sikkerhetsnivå, ikke de ulike tiltakene vurdert hver for seg. For enkelte virksomheter vil det være umulig, eller uforholdsmessig kostbart, å etablere sikkerhetstiltak som gjør at tilsiktede uønskede hendelser blir forhindret. Redundante systemer vil imidlertid kunne redusere risikoen for at slike hendelser får kritiske konsekvenser, slik at kravet til forsvarlig sikkerhetsnivå er oppfylt.

I bestemmelsens *andre ledd* slås det fast at virksomheten, ved vurderingen av hvilke sikkerhetstiltak som skal gjennomføres, skal foreta en forholdsmessighetsvurdering mellom kostnadene ved tiltakene og den sikkerhetsmessige effekten som oppnås. Slike vurderinger må imidlertid gjøres innenfor rammen av det som skal til for å oppnå et *forsvarlig sikkerhetsnivå* etter første ledd.

Bestemmelsens *tredje ledd* presiserer at de risiko- og konsekvensreduserende tiltakene som iverksettes for å motvirke tilsiktede uønskede hendelser, kan sees i sammenheng med behov for tiltak for å håndtere annen type risiko. Med dette menes i første rekke at virksomheten bør ha en helhetlig tilnærming til forebyggende sikkerhet ved operasjonaliseringen av krav som følger av sikkerhetsloven og annet regelverk som stiller krav til sikkerhet generelt eller innen en sektor. Tiltak for å forebygge tilsiktede uønskede hendelser (*security*) og tiltak for å forebygge mot uhell og skadelige naturhendelser (*safety*), bør med andre ord så langt som mulig sees i sammenheng

med hverandre. Et vilkår for at slik planlegging og gjennomføring kan sees i sammenheng, er at kravene etter sikkerhetsloven oppfylles.

§ 4-2 Sikkerhetsstyring

Bestemmelsens *første ledd første punktum* slår fast at forebyggende sikkerhet er et ledelsesansvar. Myndigheten til å følge opp det forebyggende sikkerhetsarbeidet bør kunne delegeres, men en god forankring hos ledelsen er avgjørende for et godt og tilstrekkelig prioritert sikkerhetsarbeid.

Bestemmelsens *andre ledd* presiserer at virksomheten har et ansvar for opplæring av eget personell, og en påseplikt overfor underleverandører og andre oppdragstakere. Formålet med bestemmelsen er å uttrykkelig slå fast at en virksomhet ikke kan utkontraktere ansvaret for det forebyggende sikkerhetsarbeidet. Leverandører til sikkerhetsgraderte anskaffelser vil ha en selvstendig plikt til å iverksette forebyggende sikkerhetstiltak, jf. § 1-3 fjerde ledd og loven kapittel 9.

§ 4-3 Risiko- og sårbarhetsanalyse

Bestemmelsens *første ledd* regulerer virksomhetens plikt til å gjennomføre en risiko- og sårbarhetsanalyse (ROS-analyse) som grunnlag for virksomhetens forebyggende sikkerhetstiltak etter loven. ROS-analysen er et godt verktøy for en systematisk kartlegging av en virksomhets risiko og sårbarhet. ROS-analysen skaper bevissthet og kunnskap om risiko- og sårbarhetsnivået og danner grunnlaget for målrettet å kunne unngå/redusere risiko og sårbarhet mot tilsiktede uønskede hendelser. Analysen gir også grunnlag for prioriteringer og en vurdering av hvilke tiltak som bør iverksettes.

ROS-analysen danner med andre ord fundamentet for virksomhetens gjennomføring av sikkerhetstiltak og sikkerhetsstyring for øvrig. En forutsetning for å kunne gjøre en tilfredsstillende ROS-analyse er at de ulike virksomhetene blir satt i stand til å forstå hvilket trusselbilde som til enhver tid er gjeldende. Bestemmelsen må således sees i sammenheng med Sikkerhetsmyndighetens plikt til aktiv rådgivning og veiledning, jf. § 2-2 første ledd bokstav b og Sikkerhetsmyndighetens plikt til å tilrettelegge og koordinere tilgjengeliggjøring av trusselinformasjon og annen sikkerhetsrelevant informasjon, jf. § 2-3.

I bestemmelsens *andre ledd* pålegges virksomheten å gjennomgå, og om nødvendig revidere, ROS-analysen på jevnlig basis. Arbeidet med ROS-analysen skal være en dynamisk prosess, som skal ta høyde for endringer i gjeldende trusselsituasjon, virksomhetens sårbarheter eller andre sikkerhetsrelevante endringer. Når, og hvor ofte, en virksomhet må gjennomgå ROS-analysen vil i stor grad være situasjonsbetinget.

Sikkerhetsmyndigheten, eller den sektormyndighet som er gitt tilsynsansvar etter loven, plikter etter bestemmelsens *tredje ledd*, å bistå virksomheten med råd og veiledning dersom det anmodes om dette, jf. også § 2-2 første ledd bokstav b. Som hovedregel vil plikten til å gi råd og veiledning etter bestemmelsen følge fordelingen av tilsynsansvaret etter § 3-1. Det vil imidlertid kunne være forhold som gjør at ansvarsfordeling bør eller må være annerledes. For enkelte sektormyndigheter vil eksempelvis EØS-rettslige forpliktelser sette begrensninger for hvor langt sektormyndigheten kan gå i forhold til konkret rådgivning overfor virksomheter i egen sektor. Hvorvidt det er Sikkerhetsmyndigheten eller aktuelle sektormyndigheter som skal bistå virksomheten i slike situasjoner, bør fastlegges i samarbeidsavtalen mellom dem, jf. § 3-2 tredje ledd.

§ 4-4 Krav til dokumentasjon

Bestemmelsen regulerer virksomhetens plikt til å dokumentere det forebyggende sikkerhetsarbeidet. Formålet med bestemmelsen er å legge til rette for at tilsyn med virksomhetene etter loven kapittel 3 kan gjennomføres på en effektiv og hensiktsmessig måte.

I *bestemmelsens første ledd bokstav a* pålegges virksomheten å dokumentere at risiko- og sårbarhetsanalyse, jf. § 4-3, er gjennomført. I henhold til bestemmelsens *første ledd bokstav b* skal virksomheten også dokumentere at nødvendige tiltak er iverksatt med sikte på å redusere sannsynligheten for, og konsekvensene av, tilsiktede uønskede hendelser. Omfanget av dokumentasjon som er nødvendig for å ivareta formålet med bestemmelsen, bør fastsettes i forskrift, jf. bestemmelsens andre ledd.

Virksomhetens dokumentasjon etter bokstav a og b, vil være sensitiv og sannsynligvis sikkerhetsgradert informasjon, og må behandles deretter både av virksomheten selv og av tilsynsmyndighetene, jf. loven kapittel 5.

§ 4-5 Øvelser

Bestemmelsen regulere virksomhetenes plikt til å gjennomføre øvelser etter loven.

I *første ledd* slås det fast at slike øvelser skal gjennomføres regelmessig. Med *regelmessig* menes

at øvelser skal gjennomføres med en slik frekvens at formålet med bestemmelsen ivaretas. Formålet med å gjennomføre øvelser er dels å teste om etablerte sikkerhetstiltak fungerer etter hensikten. Dels er formålet å vedlikeholde og videreutvikle kompetansen til virksomhetens personell i håndteringen av tilsiktede uønskede hendelser mot virksomheten. Evaluering etter gjennomført øvelse skal gi et grunnlag for å vurdere behovet for å gjøre nødvendige endringer i virksomhetenes sikkerhetstiltak, og for å vurdere behovet for å styrke personellets kompetanse.

§ 4-6 Varsling

Bestemmelsen regulerer virksomhetenes varslingsplikt til tilsynsmyndighetene. En forutsetning for at myndighetene skal kunne ha oversikt over sikkerhetstilstanden i de ulike samfunnssektorene, og om nødvendig iverksette tiltak for å redusere risikoen, er at myndighetene får rettidig og tilstrekkelig informasjon om hendelser av betydning. Formålet med bestemmelsen er å legge til rette for at myndighetene kan ivareta sitt overordnede ansvar.

I bestemmelsens *første ledd* slås det fast at virksomhetene plikter å varsle tilsynsmyndighetene omgående i fire tilfeller. Med *omgående* menes i denne sammenheng at virksomhetene skal sende varsel så raskt det lar seg gjøre.

Første ledd bokstav a regulerer de tilfeller der det er klarlagt at en tilsiktet uønsket hendelse faktisk er gjennomført. Et første vilkår for at varslingsplikten skal inntre er at den aktuelle hendelsen er rettet mot den aktuelle virksomheten. I tillegg er det et vilkår at hendelsen kan ha betydning for virksomhetens «evne til å ivareta sine oppgaver knyttet til grunnleggende nasjonale funksjoner». Det vil således kun være de hendelsene som kan få negativ innvirkning på virksomhetens evne til å understøtte de aktuelle funksjonene, som det skal varsles om.

Etter *første ledd bokstav b* inntrer varslingsplikten også der det er en *begrunnet mistanke* om at hendelser som nevnt i bokstav a, er gjennomført eller planlagt. I begrepet *begrunnet mistanke* ligger et krav om at det må være en viss grad av sannsynlighet før varslingsplikten inntrer. Der det foreligger en mistanke om at en slik hendelse er planlagt, vil virksomheten uansett ha en egeninteresse i å varsle myndighetene slik at nødvendige tiltak for å avverge hendelsen kan iverksettes.

Første *ledd bokstav c* regulerer varslingsplikten for de situasjonene som kan utløse Kongen i statsråds vedtaksmyndighet etter § 2-5. For en nærmere omtale av hvilke situasjoner bestemmelsen tar sikte på å regulere vises det til merknaden til § 2-5, samt den nærmere omtalen i kapittel 7.2.3 og 7.7.8.

I *første ledd bokstav d* pålegges virksomhetene en varslingsplikt der det har skjedd brudd på krav til sikkerhet i loven kapittel 5, 6 eller 7, med tilhørende forskrifter. Varslingsplikten inntrer uavhengig av årsaken til at sikkerhetsbruddet har skjedd.

I bestemmelsens *andre ledd* slås det fast at virksomhetens varsel etter første ledd skal sendes både til sektormyndigheter som er tillagt tilsynsansvar, jf. § 3-1, og til Sikkerhetsmyndigheten. For at Sikkerhetsmyndigheten skal kunne ivareta sitt sektorovergripende ansvar, er det nødvendig at denne har en tilstrekkelig informasjonstilgang om relevante hendelser også i samfunnssektorer der den ikke har et direkte tilsynsansvar. Ved at Sikkerhetsmyndigheten får tilgang til varsel fra alle samfunnssektorer, vil denne også ha muligheten til å kartlegge og holde oversikt over trusler som rammer flere samfunnssektorer parallelt, samt gi nødvendig råd, veiledning og tidlig varsling til samfunnssektorer som enda ikke er berørt av de aktuelle truslene. Det vil imidlertid være sektormyndighetene med tilsynsansvar etter § 3-1 som har det primære ansvaret for å følge opp de varsler som kommer fra virksomheter i egen sektor.

Etter *bestemmelsens tredje ledd* skal tilsynsmyndighetene som mottar varsel etter første ledd bokstav c, *uten ugrunnet opphold* videresende slike varsel til ansvarlig departement for vurdering av enkeltvedtak etter § 2-5. Hva som ligger i *uten ugrunnet opphold* må avgjøres konkret. Et varsel etter første ledd bokstav c, skal videresendes så snart som mulig etter at tilsynsmyndigheten har tilstrekkelig informasjon om saken. Det kan tenkes situasjoner der tilsynsmyndigheten har behov for ytterligere informasjon fra virksomheten, før de har et tilstrekkelig informasjonsgrunnlag til å formidle videre.

I bestemmelsens *fjerde ledd* slås det fast at varslingsplikten skal etterleves, selv om dette innebærer videreformidling av opplysninger som i utgangspunktet er omfattet av lovbestemt taushetsplikt. Sett hen til de funksjoner og interesser loven tar sikte på å beskytte, er det avgjørende at taushetsplikt etter annet regelverk ikke er til hinder for varsling om slike tilsiktede uønskede hendelser.

§ 4-7 Behandling av personopplysninger

Bestemmelsen slår fast at behandling av personopplysninger som ledd i forebyggende sikkerhetsarbeid, skal skje i samsvar med prinsippene i personvernforordningen art. 5, med de unntak som følger av forordningen art. 23. Bestemmelsen gjelder for all behandling av personopplysninger, slik dette er definert i art. 4 (1) og (2) i nevnte forordning. Bestemmelsen forutsetter at de som er ansvarlige for behandling av personopplysninger (*behandlingsansvarlig*), jf. art. 4 (7), som ledd i etterlevelse av loven setter seg inn i og bruker nevnte bestemmelser aktivt.

For en nærmere omtale av personvernforordningen vises det til kapittel 5.3.2.

Kapittel 5 – Informasjonssikkerhet

§ 5-1 Sikkerhetsgradert informasjon

Bestemmelsen er i stor grad en videreføring av tidligere lov § 11. Den grunnleggende systematikken med skadevurdering, sikkerhetsgradering og merking er den samme.

Første ledd fastslår hvem som har plikt til å foreta skadevurdering, sikkerhetsgradering og merking av informasjon.

Skadevurderingen, som angis i bestemmelsen bokstav a til d, er bestemmende for hvilken informasjon som skal sikkerhetsgraderes og dermed beskyttes etter loven.

Innholdet i begrepet *informasjon* videreføres, slik dette er definert i dagens sikkerhets lov § 3 første ledd nr. 3, og nærmere forklart i forarbeidene.[1]

Begrepet *informasjon* skal forstås vidt. Måten informasjonen er tilvirket på og hvilken form informasjonen har er ikke relevante momenter i vurderingen av om noe er informasjon. Begrepet omfatter for eksempel informasjon i form av fysiske dokumenter, digitale og maskinlesbare signaler, film, lydopptak og muntlige opplysninger. I vurderingen av om noe skal anses som informasjon skal det legges vekt på om det er egnet til å tilføre en trusselaktør kunnskap som denne direkte eller indirekte kan benytte til å skade grunnleggende nasjonale funksjoner.

Plikten til å merke sikkerhetsgradert informasjon gjelder ikke der merking i praksis er umulig. Det gjelder for eksempel for informasjon som ikke har en fysisk tilstand, slik som muntlige opplysninger. Merkingsplikt inntrer imidlertid for den som bringer informasjonen over i et format der merking er mulig.

Ordlyden i bestemmelsen skiller seg noe fra tidligere lov. Endringen innebærer at man ved skadevurderingen må ta hensyn til skadepotensialet for hele lovens virkeområde, se nærmere i merknad til § 1-2. Tidligere lov nevnte eksplisitt hensynene til vitale sikkerhetsinteresser og alliertes sikkerhet. Slike hensyn er fortsatt relevante, jf. § 1-2.

Tema for skadevurderingen og dermed om informasjonen skal sikkerhetsgraderes, er i hvilken grad en trusselaktør, dersom denne blir kjent med informasjonen, kan påføre grunnleggende nasjonale funksjoner skade. Vurderingen vil være bestemmende for i hvilken grad informasjonens konfidensialitet må beskyttes. Er konklusjonen at konfidensialitetsbrudd ikke i noen grad kan få skadefølger, jf. bokstav d, for grunnleggende nasjonale funksjoner, skal informasjonen ikke sikkerhetsgraderes. Informasjonen skal dermed heller ikke beskyttes etter bestemmelsene i sikkerhetsloven kapittel 5. Dette utelukker ikke at informasjonen ikke skal beskyttes etter andre regler, for eksempel personopplysningsloven eller beredskapsforskriften.

Innholdet i og forholdet mellom de ulike sikkerhetsgradene for øvrig videreføres, herunder tilknytningen til NATO-systemet. Forarbeidene til tidligere lov er fortsatt relevante. Endringen fra *skade* i tidligere lov bokstav b og c til *skadefølge* i ny lov, er kun en språklig justering som ikke innebærer realitetsendring. Det samme gjelder endringen i bokstav d) fra *medføre* i tidligere lov til *få* i ny lov. Se også kapittel 8.2.1 som beskriver nærmere området for BEGRENSET.

Sondringen mellom skjermingsverdig og sikkerhetsgradert informasjon videreføres ikke.

Sikkerhetshensyn skal være styrende for nødvendighetsvurderingen etter *andre ledd første punktum*. Bestemmelsen skal sikre at det faktisk foretas en grundig vurdering av beskyttelsesbehovet og at andre relevante hensyn, slik som offentlighetsprinsippet, tas i betraktning.

Fjerde ledd er en videreføring av gjeldende rett.

Se for øvrig kapittel 8.5.1, 8.6.1 og 8.6.2.

§ 5-2 Beskyttelse av sikkerhetsgradert informasjon

Bestemmelsen fastsetter en beskyttelsesplikt for den virksomhet som rår over informasjonen. Denne plikten er noe annet og mer enn det som følger av § 5-4 om taushetsplikt, som retter seg mot enkeltpersoner med tilgang til informasjonen.

[1] Ot.prp. nr. 49 (1996–97), 66 og 68.

Bestemmelsen gjelder kun for sikkerhetsgradert informasjon, jf. § 5-1. Sikkerhetstiltakene skal ivareta både konfidensialiteten (bokstav a), integriteten (bokstav b) og tilgjengeligheten (bokstav c) til informasjonen. En konkret helhetsvurdering av behovet for beskyttelse av det enkelte element, må ligge til grunn for å kunne iverksette passende sikkerhetstiltak.

Nødvendighetsvurderingen vil i stor grad avhenge av de nærmere bestemmelser om beskyttelse som blir fastsatt i forskrift. NATO-reglene setter minstekrav for beskyttelse av informasjon innen de enkelte sikkerhetsgradene, som vil måtte være felles for alle som behandler sikkerhetsgradert informasjon. Utover dette er det opp til Kongen å avgjøre om og eventuelt i hvilken utstrekning sikkerhetskravene skal gjelde nasjonalt og tverrsektorielt. Se nærmere om dette i kapittel 7.7.10.

Ivaretakelse av tilgjengelighet skal i første rekke vurderes opp mot virksomhetens eget behov. Bestemmelsen må imidlertid ses i sammenheng med lovens system for øvrig og samfunnssikkerhetsprinsippet om samvirke. Det følger av dette en plikt til å vurdere om andre virksomheter har behov for den informasjonen som virksomheten besitter – også kalt *responsibility to share*.

§ 5-3 Tilgang til og taushetsplikt for sikkerhetsgradert informasjon

Første ledd fastsetter uttømmende og absolutte vilkår for å kunne overlate sikkerhetsgradert informasjon til en annen. Nærmere om autorisasjon følger av § 8-1.

Etter *andre ledd* plikter man å opprettholde taushet når det gjelder sikkerhetsgradert informasjon i alle andre tilfeller enn det som følger av første ledd. Den som skal overlate sikkerhetsgraderte informasjon til en annen må forvisse seg om at vilkårene er oppfylt.

«Enhver som får tilgang til» i andre ledd omfatter også den som har utstedt eller på annen måte tilvirket informasjonen. Oppregningen «arbeid, oppdrag, verv eller aktivitet» skal omfatte alle relasjoner til virksomheten som i noen grad er formalisert, der noen gjør noe på vegne av virksomheten.

Bestemmelsen er en videreføring av gjeldende rett og forarbeidene til tidligere lov er relevante. Endringene innebærer ikke realitetsforskjell fra tidligere sikkerhetslov.

§ 5-4 Tekniske sikkerhetsundersøkelser

Bestemmelsen er en videreføring av gjeldende rett. Begrepet *avtitting* er erstattet med *innsyn*, uten at det er ment å utgjøre en realitetsforskjell.

Kapittel 6 – Informasjonssystemsikkerhet

Kapittel 6 inneholder regler om hvilke informasjonssystemer som skal beskyttes etter loven, hvem som har ansvar for beskyttelsen og hvilke sikkerhetstiltak som kan og hvilke som skal iverksettes. Det legges også enkelte føringer for gjennomføringen av sikkerhetstiltakene. Loven regulerer kun forhold som er felles for alle skjermingsverdige informasjonssystemer. Forskriftshjemlene åpner for at Kongen kan gi både sektor- og systemtilpassede bestemmelser.

Mens informasjonssikkerhet handler om å beskytte den verdien som informasjonen representerer, handler informasjons*system*sikkerhet om å beskytte den funksjonen eller oppgaven som systemet skal ivareta. For å oppnå et forsvarlig nivå for informasjons*system*sikkerheten må også verdien av informasjonen som behandles i systemet vurderes.

§ 6-1 Skjermingsverdige informasjonssystemer

Bestemmelsen innfører begrepet skjermingsverdige informasjonssystemer som en samlebetegnelse for alle informasjonssystemer som omfattes av og skal beskyttes etter sikkerhetsloven.

Med begrepet *informasjonssystem* menes systemer som anvendes for å løse en oppgave eller utføre en funksjon i en organisasjon. Det omfatter menneskelige, organisatoriske og tekniske ressurser, metoder og teknikker.[2]

Informasjonssystem skal i sikkerhetsloven forstand forstås vidt. Begrepet omfatter både manuelle og digitale informasjonssystemer, og favner alt fra saksbehandlingssystemer, kontorstøttesystemer og rene kommunikasjonssystemer til kontroll- og styringssystemer.[3]

---

[2] Arild Jansen og Dag Wiese Schartum (red.), *Informasjonssikkerhet: Rettslige krav til sikker bruk av IKT* (Bergen: Fagbokforlaget 2005), 62.

[3] Jf. også lov 21. juni 2013 nr. 61 om forbud mot diskriminering på grunn av nedsatt funksjonsevne (diskriminerings- og tilgjengelighetsloven) § 14 første ledd: «Med informasjons- og kommunikasjonsteknologi (IKT) menes teknologi og systemer av teknologi som anvendes til å uttrykke, skape, omdanne, utveksle, lagre, mangfoldiggjøre og publisere informasjon, eller som på annen måte gjør informasjon anvendbar».

Bokstav a gjelder alle informasjonssystemer som, hvis de slutter å fungere eller får redusert funksjonalitet, har en negativ innvirkning på virksomhetens evne til å levere sine kritiske tjenester eller funksjoner. Avgjørende for om et system skal beskyttes etter loven er hvilken rolle systemet har ved virksomhetens produksjon av tjenester som er av kritisk betydning for grunnleggende nasjonale funksjoner. Hvilke typer oppgaver systemet utfører er også relevant, men ikke avgjørende.

Bokstav b omfatter informasjonssystemer som behandler sikkerhetsgradert informasjon. Dermed videreføres beskyttelsen av de systemer som per i dag kalles *godkjente informasjonssystemer*. Selve begrepet videreføres ikke.

Med begrepet *behandler* menes alle former for behandling av informasjon i et informasjonssystem, herunder transport, lagring og prosessering.

Ett system kan falle inn under både bokstav a og b. Se kapittel 8.5.2, 8.6.1 og 8.6.2 for nærmere omtale av skjermingsverdige informasjonssystemer.

§ 6-2 Beskyttelse av skjermingsverdige informasjonssystemer

Bestemmelsen fastsetter en plikt for virksomheten til å beskytte virksomhetens skjermingsverdige informasjonssystemer. Virksomhetens ROS-analyse, jf. § 4-3, vil danne grunnlaget for å angi hvilke informasjonssystemer som skal beskyttes etter sikkerhetsloven.

Virksomheten plikter å oppnå et forsvarlig sikkerhetsnivå for informasjonssystemene. *Bokstav a og b* konkretiserer hva som ligger i begrepet ved å angi hovedmålene for sikkerhetstiltakene. Ivaretakelse av a og b må ses i sammenheng. Eksempelvis er det ikke tilstrekkelig å bare se på graderingsnivået for et sikkerhetsgradert informasjonssystem, se kapittel 8.6.2. ROS-analysen vil danne grunnlaget for iverksettelse av de sikkerhetstiltak som er mest hensiktsmessige for det enkelte system. Det vil kunne variere fra system til system hva som skal til for å oppnå et forsvarlig sikkerhetsnivå.

§ 6-3 Godkjenning av skjermingsverdige informasjonssystemer

Bestemmelsen fastsetter at alle skjermingsverdige informasjonssystemer, jf. § 6-1, må sikkerhetsgodkjennes. For informasjonssystemer, jf. § 6-1 bokstav a setter loven ikke krav om forhåndsgodkjenning.

For informasjonssystemer som skal behandle sikkerhetsgradert informasjon, jf. § 6-1 b, videreføres gjeldende rett. Slike systemer må godkjennes før de kan behandle sikkerhetsgradert informasjon.

Forskriftshjemmelen i *tredje ledd* åpner for å etablere flere ulike godkjenningsprosesser og godkjenningsmyndigheter.

§ 6-4 Overvåking av skjermingsverdige informasjonssystemer

Sikkerhetsmessig overvåkning kan innebære mange former for sikkerhetstiltak. Særlig aktuelle tiltak er logging av aktivitet i systemet, automatiserte alarmer og manuell sammenstilling og analyse av innhentet data.

Som redegjort for i kapittel 8.6.4 er bestemmelsen i hovedsak en videreføring av gjeldende sikkerhetslov § 13a.

Første ledd oppstiller en plikt for virksomheten til å foreta sikkerhetsmessig overvåkning av virksomhetens skjermingsverdige informasjonssystemer, jf. § 6-1. Første ledd fastsetter dessuten formålet med overvåkningen. Med begrepene *forebygge og håndtere* menes sikkerhetstiltak som omfatter hele livssyklusen til en tilsiktet uønsket hendelse, herunder evne til å oppdage (detektere) og gjenopprette sikker tilstand etter hendelsen. Med *tilsiktet uønsket hendelse* menes forsøk på eller faktisk kompromittering av systemet. Bestemmelsens *siste punktum* erstatter gjeldende lov § 13a *sikkerhetsrelevante hendelser* uten at det innebærer en realitetsendring.

Andre ledd gir dels en hjemmel og dels en plikt til lagring, registrering og analyse av ulike former for utveksling av informasjon.

For at ikke tiltaket skal bli uforholdsmessig byrdefullt må omfanget av overvåkningen, herunder lagring og registrering, forankres i en nærmere vurdering av det enkelte systems særegenheter. Etter at behovet er kartlagt, trer plikten inn til å overvåke systemet i det omfang det er nødvendig for å oppnå formålet med tiltaket. For nærmere omtale av andre ledd, se kapittel 8.6.4.

Ved overvåkning av systemer som behandler personopplysninger må andre og tredje ledd ses i sammenheng. *Tredje ledd* stiller ytterligere krav til at virksomheten foretar grundige vurderinger før tiltaket iverksettes.

For det første stilles det strengere krav til vurderingen av formålsmessighet enn det som følger av andre ledd. Videre må virksomheten i hvert enkelt tilfelle foreta en forholdsmessighetsvurdering der behovet for overvåkning ses i sammen-

heng med eventuelle personvernulemper av behovet for overvåkning. Omfanget av overvåkningen må være begrunnet og nødvendig. Virksomheten må dessuten – der det er valgmuligheter – velge den metoden som er minst inngripende for personvernet til brukerne av systemet. I noen tilfeller kan for eksempel automatisert overvåkning med et innhold som er utilgjengelig for mennesker være mindre inngripende enn manuell overvåkning.

Etter *fjerde ledd* gis det hjemmel for å lagre informasjon som er resultat av overvåkningen i inntil 5 år. Loven setter ikke begrensninger for bruken av informasjon som ikke er personopplysninger.

Femte ledd er med ett unntak en videreføring av gjeldende sikkerhetslov § 13a tredje ledd. § 6-4 femte ledd inneholder også et *andre punktum*, der det ilegges en plikt for den som overvåker til å beskytte den informasjonen som blir kjent gjennom overvåkningsavtalen.

Sjette ledd er en videreføring av gjeldende sikkerhetslov § 13a femte ledd. Her pålegges virksomheten en informasjonsplikt i samsvar med personopplysningsloven § 19.

Sjuende ledd er en videreføring av gjeldende sikkerhetslov § 13a sjette ledd, men med noen presiseringer.

§ 6-5 Kommunikasjons- og innholdskontroll av informasjonssystemer

Bestemmelsen er i all hovedsak en videreføring av gjeldende sikkerhetslov § 15 om monitoring.

Bestemmelsen pålegger ingen plikt for virksomheten til å få gjennomført denne type kontroll. Ordningen skal kun være et supplement til øvrige relevante sikkerhetstiltak, og et tilbud til de virksomheter som ser behov for slik kontroll av sine informasjonssystemer, jf. *første ledd*.

Andre ledd setter rammene for hvilke metoder som kan inngå i kontrollen. Både avlytting og avlesing av informasjon tillates.

Bestemmelsen viderefører forbudet mot å kontrollere privat kommunikasjon og kommunikasjon med virksomheter som ikke omfattes av sikkerhetsloven, jf. *fjerde ledd*. Kontroll av kommunikasjon mellom skjermingsverdige informasjonssystemer i ulike virksomheter som er omfattet av sikkerhetsloven er tillatt.

Tredje ledd skal sikre at virksomhetens ledelse kan foreta en grundig vurdering av behovet for kontrollen. I vurderingen må det tas hensyn både til sikkerhet og personvern.

Sjette ledd begrenser Sikkerhetsmyndighetens behandling av informasjon som den blir kjent med gjennom kontrollen.

Se for øvrig kapittel 8.6.4

§ 6-6 Inntrengningstesting av skjermingsverdige informasjonssystemer

Bestemmelsen er i all hovedsak en videreføring av gjeldende sikkerhetslov § 15 om inntrengningstesting.

Virksomheten plikter ikke å få gjennomført inntrengningstesting. Ordningen skal være et tilbud til virksomheter som er omfattet av sikkerhetsloven. Det er opp til den enkelte virksomhet å vurdere behovet for tiltaket.

Virksomhetens orienteringsplikt etter *første ledd andre punktum* er generelt utformet og innebærer at det er tilstrekkelig at de ansatte er klar over at slike kontroller tidvis kan forekomme.

Det følger av *andre ledd* en plikt til både å gjennomføre en vurdering av formålsmessigheten og av forholdsmessigheten av sikkerhetstiltaket i de tilfeller testingen gjelder informasjonssystemer som behandler personopplysninger.

Tredje ledd er en videreføring av gjeldende § 15 tredje ledd, men inneholder også en presisering av hva informasjonen som kontrollinstansen blir kjent med, kan brukes til.

Bestemmelsens *fjerde ledd* skal sikre at de erfaringer Sikkerhetsmyndigheten gjør seg gjennom kontrollen blir dokumentert og videreført.

Femte ledd tilsvarer deler av dagens § 11-8 i informasjonssikkerhetsforskriften. Rapporteringen må ses i sammenheng med Sikkerhetsmyndighetens plikter, jf. § 2-2. Hovedformålet er å forbedre virksomhetens sikkerhet.

Forskriftsmyndigheten i *sjette ledd* fastslår at andre enn Sikkerhetsmyndigheten kan gjennomføre inntrengningstesting.

Se for øvrig kapittel 8.6.4

Kapittel 7 – Objekt- og infrastruktursikkerhet

§ 7-1 Skjermingsverdige objekter og infrastruktur

Bestemmelsen regulerer departementenes, og Sikkerhetsmyndighetens, ansvar og myndighet til å utpeke, klassifisere og holde oversikt over skjermingsverdige objekter og infrastruktur. Begrepene *skjermingsverdig objekt* og *skjermingsverdig infrastruktur* er nærmere omtalt i kapittel 9.5.1.

Bestemmelsen må sees i forlengelsen av departementenes, og Sikkerhetsmyndighetens, myndighet til å treffe enkeltvedtak etter § 2-1 første ledd bokstav c og § 2-2 første ledd bokstav e.

Etter bestemmelsens *første ledd* gis departementene myndighet til å utpeke og klassifisere skjermingsverdige objekter og infrastruktur innen eget myndighetsområde. Hva gjelder skjermingsverdige objekter, er dette en videreføring av departementenes myndighet etter gjeldende sikkerhetslov kapittel 5. Departementene pålegges også en plikt til å holde oversikt over slike objekter og slik infrastruktur. Plikten må sees i sammenheng med departementenes overordnede ansvar for forebyggende sikkerhet i egen sektor, jf. § 2-1 første ledd.

I bestemmelsens *andre ledd* gis Sikkerhetsmyndigheten tilsvarende myndighet og plikt overfor objekter og infrastruktur som ikke ligger innenfor et departements myndighetsområde, se også merknad til § 2-2 første ledd bokstav e.

Etter *tredje ledd* har virksomheter som råder over objekter eller infrastruktur som blir utpekt og klassifisert, de samme rettigheter til forutgående varsling og klage, som for enkeltvedtak etter §§ 2-1 og 2-2, se merknad til disse bestemmelsene.

Fjerde ledd korresponderer med Sikkerhetsmyndighetens forslags- og klagerett etter § 2-1 fjerde ledd, se merknad til denne bestemmelsen.

§ 7-2 Klassifisering

Bestemmelsen regulerer hvordan skjermingsverdige objekter og infrastruktur skal klassifiseres. Myndighet til å klassifisere objekter og infrastruktur tilligger ansvarlig departement eller Sikkerhetsmyndighet, jf. § 7-1 første og andre ledd. Formålet med klassifisering av objekter og infrastruktur er dels at det er styrende for hvilke sikkerhetstiltak som skal iverksettes, jf. § 7-3, og dels at det gir myndighetene anledning til å kunne prioritere mellom ulike objekt eller infrastruktur avhengig av graden av kritikalitet ved redusert funksjonalitet.

Første ledd fastslår at klassifisering skal skje på bakgrunn av en skadevurdering der skadefølgene som følge av redusert funksjonalitet skal være styrende for hvilket klassifiseringsnivå objektet eller infrastrukturen skal ha. Systematikken for klassifisering etter første ledd bokstav a til c bygger i stor utstrekning på systematikken i gjeldende sikkerhetslov § 17a, med de tilpasninger som er nødvendige av hensyn til lovforslaget for øvrig.

Etter første *ledd bokstav a* skal MEGET KRITISK benyttes dersom redusert funksjonalitet kan få *helt avgjørende skadefølger* for grunnleggende nasjonale funksjoner. Med *redusert funksjonalitet* menes objektet eller infrastrukturens evne til å understøtte den aktuelle funksjonen. Begrepet *helt avgjørende skadefølger* skal forstås på samme måte som i § 5-1 første ledd bokstav a.

Etter *første ledd bokstav b* skal KRITISK benyttes dersom redusert funksjonalitet *alvorlig kan skade* grunnleggende nasjonale funksjoner. Begrepet *alvorlig kan skade* skal forstås på samme måte som i § 5-1 første ledd bokstav b.

Etter *første ledd bokstav c* skal VIKTIG benyttes dersom redusert funksjonalitet *kan skade* grunnleggende nasjonale funksjoner. Begrepet *kan skade* skal forstås på samme måte som i § 5-1 første ledd bokstav c.

Bestemmelsens *andre ledd første punktum* slår fast at klassifiseringen skal skje på bakgrunn av virksomhetens ROS-analyse, jf. §4-3. Som en konsekvens av dette er det nødvendig at ansvarlig departement eller Sikkerhetsmyndigheten får tilgang til virksomhetens ROS-analyse i klassifiseringsarbeidet. Departementene og Sikkerhetsmyndigheten plikter videre å begrunne klassifisering ut fra hvilke funksjoner som understøttes og konsekvensene for disse funksjonene dersom det aktuelle objektet eller infrastrukturen får redusert funksjonalitet.

I *andre ledd andre punktum* slås det fast at begrunnelsen etter første punktum skal inngå i departementenes og Sikkerhetsmyndighetens totale oversikt over objekter og infrastruktur. Disse begrunnelsene vil være av sentral betydning for Sikkerhetsmyndighetens mulighet til å kunne kvalitetssikre departementenes klassifisering av objekter og infrastruktur i medhold av bestemmelsen. Selve begrunnelsen vil i seg selv være meget sensitiv informasjon, og vil måtte behandles deretter, jf. informasjonssikkerhetsbestemmelsene i loven kapittel 5.

I bestemmelsens *tredje ledd* presiseres det at klassifiseringsnivået kan være forskjellig for ulike deler av et objekt eller en infrastruktur. I den utstrekning dette er tilfelle skal slike deler defineres som selvstendige objekter eller infrastruktur. Det er altså mulig å definere «objekt i objekt», «infrastruktur i infrastruktur», «infrastruktur i objekt» og «objekt i infrastruktur». Dette innebærer at det kan være ulike klassifiseringsnivåer for ulike deler innad i samme objekt eller infrastruktur, med ulike beskyttelsesbehov. Sikkerhetstiltakene, jf. § 7-3, vil da også kunne differensieres avhengig av de ulike delenes klassifisering.

§ 7-3 Beskyttelse av objekter og infrastruktur

Bestemmelsen regulerer virksomhetenes plikt til å iverksette sikkerhetstiltak for utpekt og klassifisert objekt eller infrastruktur. Bestemmelsen må

sees i sammenheng med de generelle kravene til forebyggende sikkerhet etter § 4-1.

I henhold til bestemmelsens *første ledd* plikter virksomheten å iverksette de sikkerhetstiltak som er nødvendige for å opprettholde et forsvarlig sikkerhetsnivå. Begrepet *forsvarlig sikkerhetsnivå* viser tilbake på den rettslige standarden i § 4-1 første ledd, og skal forstås på samme måte.

I bestemmelsens *andre ledd første punktum* presiseres at det skal ses hen til det aktuelle klassifiseringsnivået og konsekvensene ved bortfall eller reduksjon av funksjonalitet. *Andre ledd andre punktum* fastslår at sikkerhetstiltakene skal sees i sammenheng og tilpasses det konkrete beskyttelsesbehovet.

I bestemmelsens *tredje ledd* gis departementene og Sikkerhetsmyndigheten myndighet til å treffe vedtak om krav til adgangsklarering for tilgang til hele eller deler av objekt eller infrastruktur som er utpekt og klassifisert etter §§ 7-1 og 7-2. Hva som menes med *adgangsklarering* er nærmere omtalt i merknaden til § 8-1 første ledd andre punktum. Med *tilgang* menes i denne sammenheng både fysisk og logisk tilgang til objekt eller infrastruktur. For enkelte typer objekt eller infrastruktur vil det ikke være nødvendig med fysisk tilgang for å kunne gjøre skade, en logisk (digital) tilgang kan i noen tilfeller gi like gode muligheter til å gjøre skade av betydning for objektets eller infrastrukturens funksjonalitet.

Hvorvidt det skal fastsettes krav om adgangsklarering for tilgang, må vurderes konkret for det enkelte objekt eller infrastruktur. I den konkrete vurderingen må det særlig tas hensyn til den sikkerhetsmessige effekten som oppnås, sett opp mot hvor inngripende tiltaket vil være overfor den aktuelle virksomheten og dens ansatte. Vedtak som nevnt i tredje ledd, som berører selvstendige rettssubjekter, kan i medhold av *fjerde ledd* påklages til Tvisteorganet.

§ 7-4 Testing av sikkerhetssystemer

Bestemmelsen regulerer virksomhetens adgang til å anmode Sikkerhetsmyndigheten om å gjøre forsøk på å forsere virksomhetens etablerte sikkerhetstiltak for tilgang til skjermingsverdig objekt eller infrastruktur. Bestemmelsen korresponderer med hjemmelen for inntregningstesting av informasjonssystemer, jf. § 6-6.

Slik testing er et frivillig tilbud til den enkelte virksomhet, og kan kun gjøres på anmodning fra ledelsen i den aktuelle virksomheten. Formålet med denne type testing er å forsøke å avdekke svakheter ved de tiltak en virksomhet har iverksatt for å forhindre uvedkommendes tilgang til objektet eller infrastrukturen. Virksomhetens orienteringsplikt etter *første ledd tredje punktum* er generelt utformet og innebærer at det er tilstrekkelig at de ansatte er klar over at slike kontroller tidvis kan forekomme.

Med *tilgang* menes i denne sammenheng både fysisk og logisk (digital) tilgang til objektet eller infrastrukturen, jf. også merknaden til § 7-3 tredje ledd.

Bestemmelsens *andre ledd* hjemler behandling av personopplysninger ved testing, men fastslår samtidig at det skal gjøres en nødvendighets- og forholdsmessighetsvurdering av behovet for slik behandling.

Bestemmelsens *tredje ledd* angir en formålsavgrensing for bruk av informasjon som testingen gir tilgang til. Med *informasjon* menes i denne sammenheng både personopplysninger og opplysninger om virksomheten. Bestemmelsens formål – å forbedre virksomhetens sikkerhetsnivå – vil være styrende for hva informasjonen kan benyttes til.

Etter bestemmelsens *fjerde ledd* plikter Sikkerhetsmyndigheten å avslutte operasjonen, dersom den lykkes i å forsere etablerte sikkerhetstiltak.

§ 7-5 Adgang til steder og områder

Bestemmelsen viderefører gjeldende sikkerhetslov § 18a første ledd bokstav b og c, men i en modernisert språkdrakt – og tilpasset den øvrige innretning på lovforslaget.

Gjeldende sikkerhetslov § 18a første ledd bokstav a om forbud mot adgang til «forsvarsbygg og -anlegg hvor gjenstander av interesse for rikets forsvar fremstilles, istandsettes eller oppbevares» foreslås ikke videreført, da adgangen til å fastsette slike forbud ivaretas av de øvrige delene av lovforslaget.

Endringene er ikke ment å gjøre realitetsendringer i dagens rettstilstand på området.

Kapittel 8 – Personellsikkerhet

§ 8-1 Når klarering og autorisasjon skal gjennomføres

Bestemmelsen regulerer når *sikkerhetsklarering*, *adgangsklarering* og *sikkerhetsautorisasjon* skal gjennomføres.

Med *sikkerhetsklarering* menes en avgjørelse fra klareringsmyndigheten om en persons antatte sikkerhetsmessige skikkethet til å kunne håndtere sikkerhetsgradert informasjon opp til et gitt sikkerhetsnivå.

Med *adgangsklarering* menes en avgjørelse fra klareringsmyndigheten om en persons antatte sikkerhetsmessige skikkethet for tilgang til klassifiserte områder innenfor skjermingsverdige objekter eller infrastruktur, jf. § 7-3 tredje ledd.

Med *sikkerhetsautorisasjon* menes avgjørelse fra autorisasjonsansvarlig i den enkelte virksomhet om at en person, etter en konkret helhetsvurdering, gis tilgang til sikkerhetsgradert informasjon eller tilgang til klassifiserte områder innen objekter eller infrastruktur.

Bestemmelsens *første ledd* slår fast at autorisasjon i medhold av § 8-2 skal gjennomføres for to kategorier personell. For det første gjelder dette for personer som skal gis tilgang til sikkerhetsgradert informasjon, jf. *første ledd første punktum*. «Skal gis tilgang til» indikerer at vedkommende gjennom sitt arbeid har tjenstlig behov for tilgang til slik informasjon. For det andre gjelder kravet til sikkerhetsautorisasjon, i henhold til *første ledd andre punktum*, personer som skal ha tilgang til klassifiserte områder innen objekter og infrastruktur, der det er truffet vedtak etter § 7-3 tredje ledd. Med *adgang* menes både fysisk og logisk tilgang til slike objekter eller infrastruktur, se merknad til § 7-3. Adgangsklarering er ment å være en mindre omfattende klareringsprosess enn sikkerhetsklarering for tilgang til sikkerhetsgradert informasjon, men samtidig mer omfattende enn en ordinær vandelskontroll.

Bestemmelsens *andre ledd* er en videreføring av gjeldende sikkerhetslov § 19 andre ledd, og slår fast at personer som skal autoriseres for tilgang til sikkerhetsgradert informasjon gradert KONFIDENSIELT eller høyere, på forhånd skal sikkerhetsklareres.

I bestemmelsens *tredje ledd* slås det fast at personell som innehar gyldig sikkerhetsklarering etter § 8-5, også skal anses adgangsklarert. Adgangsklarering er ment å være en mindre omfattende prosess enn sikkerhetsklarering, se merknad til § 8-5, og dersom sikkerhetsklarering allerede foreligger skal det legges til grunn at vedkommende er sikkerhetsmessig skikket også for adgang til objekt eller infrastruktur.

Fjerde ledd gjelder personer som «vil kunne få» tilgang til sikkerhetsgradert informasjon. Bestemmelsen er en videreføring av gjeldende sikkerhetslov § 19 tredje ledd. Det er ikke et vilkår for sikkerhetsklarering at vedkommende faktisk vil få tilgang til slik informasjon. I forarbeidene til gjeldende sikkerhetslov vises det som eksempel til vakter, rengjøringspersonell og andre som forutsetningsvis ikke skal ha tilgang til slik informasjon, men som gjennom sitt arbeid er i en posisjon hvor en lett kan skaffe seg slik tilgang. Et vilkår for sikkerhetsklarering av slikt personell er at andre risikoreduserende tiltak, eksempelvis adgangskontroll til lokaler der slik informasjon oppbevares, kan fjerne risikoen for at personellet kommer i en slik posisjon, jf. *fjerde ledd andre punktum*.

Femte ledd er en videreføring av gjeldende lov § 19 fjerde ledd, og skal forstås på samme måte. At en person sikkerhetsklareres for en nasjonal sikkerhetsgrad innebærer ikke at vedkommende automatisk er klarert for tilsvarende sikkerhetsgrader fastsatt av internasjonale organisasjoner, jf. begrepet *eventuelt* i bokstav a til c.

§ 8-2 Sikkerhetsautorisasjon

Bestemmelsen regulerer hvem som har ansvaret for autorisasjon etter loven, og det nærmere vurderingstemaet for om personer kan gis autorisasjon.

Første ledd slår fast at virksomhetens leder er ansvarlig for autorisasjon. Dette henger sammen med at forebyggende sikkerhet er et ledelsesansvar, jf. § 4-2 første ledd første punktum. Myndigheten til å gi autorisasjon kan ved behov delegeres.

Bestemmelsens *andre ledd* slår fast at *autorisasjonsansvarlig* også har ansvaret for daglig sikkerhetsmessig ledelse og kontroll av autorisert personell i virksomheten. Autorisasjonsansvarlig vil som nevnt ovenfor normalt være virksomhetens leder. Myndigheten til å ha daglig sikkerhetsmessig ledelse og kontroll av personellet, vil i praksis følges opp av den som har fått delegert myndighet etter første ledd, eksempelvis autorisert personells nærmeste foresatte. Med *sikkerhetsmessig ledelse og kontroll* menes blant annet ansvaret for å påse at autorisert personell har tilstrekkelig opplæring og kompetanse på forebyggende sikkerhet, og å påse at personellet faktisk etterlever sikkerhetsbestemmelsene i sitt daglige virke.

Bestemmelsens *tredje ledd* angir vurderingstemaet for avgjørelser om autorisasjon. Hvorvidt vedkommende er *sikkerhetsmessig til å stole på*, må baseres på en konkret helhetsvurdering av de opplysninger autorisasjonsansvarlig har tilgjengelig, og på det inntrykket som gis i autorisasjonssamtalen. Det kan heller ikke gis autorisasjon før det foreligger melding om klarering der dette er påkrevd etter § 8-1 andre ledd, det vil si ved autorisasjon for tilgang til sikkerhetsgradert informasjon gradert KONFIDENSIELT eller høyere. I *tredje ledd siste punktum* presiseres det at autorisa-

sjon ikke kan gis før det er avholdt en autorisasjonssamtale.

I bestemmelsens *fjerde ledd* pålegges virksomheten å løpende orientere Sikkerhetsmyndigheten om hvilke personer som er autorisert. Formålet med bestemmelsen er dels å sette Sikkerhetsmyndigheten i stand til å ha oversikt over hvor sikkerhetsklarert personell til enhver tid tjenestegjør, og dels å legge til rette for informasjonsdeling med Politiets sikkerhetstjeneste etter § 8-12.

§ 8-3 Nedsettelse, suspensjon og tilbakekallelse av autorisasjon

Bestemmelsen regulerer i hvilke tilfeller autorisasjonsansvarlig plikter å vurdere autorisasjonen tilbakekalt, nedsatt eller suspendert. Bestemmelsen regulerer også i hvilke tilfeller autorisasjon automatisk bortfaller.

Bestemmelsen er en videreføring av gjeldende sikkerhetslov § 24 andre og fjerde ledd, og skal forstås på samme måte.

§ 8-4 Klareringsmyndigheter etter loven

Bestemmelsen viderefører det vedtatte forslaget i Prop. 97 L (2015–2016) om endring av klareringsmyndighetsstrukturen.

I bestemmelsens *første ledd andre punktum* angis klareringsmyndighetenes myndighet til å avgjøre om en person er sikkerhetsmessig skikket for håndtering av sikkerhetsgradert informasjon, eller for adgang til klassifiserte områder innen objekter eller infrastruktur.

§ 8-5 Sikkerhets- og adgangsklarering

Bestemmelsen angir det nærmere vurderingstemaet for når klarering skal gis eller opprettholdes.

Etter *første ledd* skal klarering bare gis eller opprettholdes dersom det ikke foreligger rimelig tvil om vedkommendes sikkerhetsmessige skikkethet. Vurderingen av *rimelig tvil* må ses i sammenheng med det nivå vedkommende skal klareres for. Desto høyere klareringsnivå, desto mindre grad av tvil kan aksepteres. Vurderingstemaet for om vedkommendes *sikkerhetsmessige skikkethet* må baseres på en konkret helhetsvurdering av de foreliggende opplysningene. *Første ledd andre punktum* slår fast at det skal gjennomføres en personkontroll, jf. § 8-7, som grunnlag for denne vurderingen.

Bestemmelsen *tredje ledd* angir skrankene for hvilke forhold som kan vektlegges ved vurderingen av sikkerhetsmessig skikkethet. Det er kun forhold som er relevant for vedkommendes pålitelighet, lojalitet og sunne dømmekraft vedrørende behandling av gradert informasjon og tilgang til klassifiserte områder, som kan tillegges vekt i vurderingen. I *tredje ledd siste punktum* er det også et totalforbud mot å legge vekt på lovlig politisk engasjement. For en nærmere omtale av hvilke forhold som relevante å vektlegge, vises det til omtalen i kapittel 10.6.1.

I *bestemmelsens fjerde ledd* avgrenses klareringsmyndighetens anledning til å vektlegge negative opplysninger om nærstående personer til tilfeller der det antas at disse forholdene vil kunne påvirke vedkommendes sikkerhetsmessige skikkethet. Begrepet *nærstående personer* er nærmere omtalt i merknaden til § 8-7.

§ 8-6 Nedsettelse, suspensjon og tilbakekallelse av klarering

Bestemmelsen regulerer i hvilke tilfeller klareringsmyndigheten plikter å vurdere klareringen tilbakekalt, nedsatt eller suspendert, samt klareringsmyndighetens plikt til å varsle Sikkerhetsmyndigheten og autorisasjonsansvarlig. Bestemmelsen er en videreføring av gjeldende sikkerhetslov § 24 andre og tredje ledd og skal forstås på samme måte.

§ 8-7 Gjennomføring av personkontroll

Bestemmelsen gir nærmere regler for gjennomføring av personkontroll som grunnlag for klareringsmyndighetens vurdering av den enkeltes sikkerhetsmessige skikkethet etter § 8-5, og er i stor grad en videreføring av gjeldende sikkerhetslov § 20.

Med *personkontroll* menes i denne sammenheng både opplysninger fra vedkommende selv og de opplysninger klareringsmyndigheten selv besitter eller innhenter fra relevante registre eller andre kilder.

Etter bestemmelsens *første ledd tredje punktum* er det et vilkår for å igangsette personkontroll at den aktuelle personen er gjort oppmerksom på, og har *akseptert*, at slik kontroll igangsettes. Personer som søkes klarert er i de fleste tilfeller i en arbeidsgiver-/arbeidstakerrelasjon til autorisasjonsansvarlig, noe som gjør det vanskelig å oppfylle kravene til et informert og frivillig samtykke. Aksept av at slik kontroll gjennomføres er således tilstrekkelig. I første ledd siste punktum slås det fast at aksepten også skal omfatte muligheten for personkontroll av nærstående, jf. tredje ledd, og muligheten for fornyet personkontroll etter § 8-8.

Etter bestemmelsens *tredje ledd* kan det gjennomføres personkontroll for nærstående personer dersom det søkes om sikkerhetsklarering for HEMMELIG/tilsvarende eller høyere sikkerhetsgrader. Med begrepet *nærstående* menes i første rekke vedkommendes ektefelle, partner, samboer, barn, foreldre og søsken og andre personer vedkommende er knyttet til ved familiebånd. Nærståendebegrepet bør imidlertid ikke bare omfatte de personer vedkommende har en familiær tilknytning til. Det avgjørende bør være hvorvidt den aktuelle personen har en relasjon med vedkommende av en slik art at den har en reell påvirkningsmulighet på vedkommendes sikkerhetsmessige skikkethet.

Etter bestemmelsens *femte ledd* plikter behandlingsansvarlige (jf. merknadene til § 4-7) for relevante registre å legge til rette for en digitalisert overføring av personkontrollopplysningen til Sikkerhetsmyndigheten. *Behandlingsansvarlig* skal forstås på samme måte som *registereier* i gjeldende sikkerhetslov § 20 fjerde ledd andre punktum. Det vil være Sikkerhetsmyndigheten som forestår personkontrollen på vegne av de ulike klareringsmyndighetene. For en nærmere omtale av hva som menes med *digital overføring* vises det til kapittel 10.5.5 og 10.6.5.

§ 8-8 Fornyet personkontroll

Bestemmelsen regulerer klareringsmyndighetens adgang til å kunne anmode om fornyet personkontroll, jf. § 8-7, for klarert personell når som helst i klareringens gyldighetstid. Retten til å anmode om slik fornyet personkontroll gjelder både ved mistanke om nye forhold av betydning for vedkommende sikkerhetsmessige skikkethet, og som et ledd i regelmessig oppfølging av klarert personell.

§ 8-9 Bruk av vilkår og stillingsklarering

Bestemmelsen er i utgangspunktet en videreføring av dagens lov § 21 siste ledd.

Med begrepet *særlige tilfeller* menes at det skal være en viss tilbakeholdenhet med å gi klarering på vilkår eller stillingsklarering, blant annet av likebehandlingshensyn. Men i de tilfeller der alternativet er å avslå klareringsanmodningen, vil bruk av vilkår kunne benyttes dersom dette vurderes som et tilstrekkelig risikoreduserende tiltak. Bruk av vilkår for klarering, herunder stillingsklarering, vil blant annet kunne bidra til et mer fleksibelt system hvor verdifull kompetanse kan rekrutteres, uten at dette innebærer en uakseptabel høy risiko.

§ 8-10 Klarering av personer som ikke er norske statsborgere

Bestemmelsen er i hovedsak en videreføring av gjeldende lov § 22.

Begrepet *eventuelle tilknytning* til Norge indikerer at tilknytning til Norge ikke er et absolutt vilkår for å kunne innvilge klarering. Vurderingen skal baseres på en konkret helhetsvurdering, der tilknytning til Norge er ett av flere momenter som skal vektlegges i vurderingen. Hjemlandets sikkerhetsmessige betydning for Norge og vedkommendes tilknytning til dette, skal være tungtveiende momenter i vurderingen av sikkerhetsmessig skikkethet. Hva som menes med *tilknytning til en annen stat* er nærmere omtalt i merknaden til § 8-12.

I *første ledd tredje punktum* er det presisert at bruk av vilkår eller stillingsklarering skal vurderes særskilt ved klarering av utenlandske statsborgere. Denne type tiltak vil, sammen med autorisasjonsansvarliges sikkerhetsmessige ledelse og kontroll, kunne redusere en eventuell risiko til et akseptabelt nivå. Presisering gir således mulighet til å gjøre individuelle tilpasninger der dette er sikkerhetsmessig forsvarlig.

I bestemmelsens *andre ledd* er Kongen gitt myndighet til å gi nærmere bestemmelser om klarering av utenlandske statsborgere.

§ 8-11 Varslingsplikt

Bestemmelsen regulerer varslingsplikt for autorisert og klarert personell, samt autorisasjonsansvarliges varslingsplikt til den aktuelle klareringsmyndigheten.

Bestemmelsens *første ledd* er en videreføring av gjeldende lov § 24 første ledd om klarert og autorisert personells plikt til å varsle autorisasjonsansvarlig om forhold som antas å kunne innvirke på vurderingen av den enkeltes sikkerhetsmessige skikkethet.

Etter bestemmelsens *andre ledd* plikter autorisasjonsansvarlig som blir varslet, å varsle videre til vedkommende klareringsmyndighet dersom det innrapporterte forholdet antas også å kunne få betydning for vedkommendes klarering.

§ 8-12 Informasjonstilgang for Politiets sikkerhetstjeneste

Bestemmelsen regulerer Sikkerhetsmyndighetens adgang til, i nærmere angitte tilfeller, å utlevere opplysninger fra klareringssaker til Politiets sikkerhetstjeneste. Formålet med bestemmelsen er nærmere omtalt i kapittel 10.6.7.

Etter bestemmelsens *første ledd* er det et vilkår for utlevering av informasjon at det foreligger en forutgående *anmodning* fra Politiets sikkerhetstjeneste. Anmodningen må i en viss utstrekning ha et presist innhold, slik at utleveringen av informasjon begrenses til det som er nødvendig. Anmodningen kan eksempelvis være avgrenset til å gjelde informasjon om personer som har tilknytning til en bestemt nasjon, eller personer med utenlandsk tilknytning som tjenestegjør innen nærmere definerte virksomheter. Anmodningen bør normalt være avgrenset til å gjelde en nærmere avgrenset tidsperiode. Sikkerhetsmyndigheten vil kunne oppdatere informasjonsgrunnlaget dersom det skjer endringer innenfor den angitte tidsperioden. Anmodningene vil uansett måtte tilpasses det konkrete informasjonsbehovet Politiets sikkerhetstjeneste har på tidspunktet for anmodningen.

Begrepet *nærstående* skal forstås på samme måte som etter § 8-7 tredje ledd.

I bestemmelsens *første ledd bokstav a til c* er det nærmere angitt hvilke opplysninger Sikkerhetsmyndigheten kan utlevere med hjemmel i bestemmelsen.

Med *klareringsstatus* menes både hvilket nivå de aktuelle personene er klarert for og klareringens gyldighetstid.

Begrepet *tilknytning til andre stater* skal forstås vidt i den forstand at ulike slags tilknytninger vil kunne være relevante. Det kan for eksempel dreie seg om økonomiske interesser i en stat eller om vedkommende har familiær tilknytning i staten. Samtidig vil ikke enhver tilknytning til en annen stat være tilstrekkelig til å oppfylle kravet. Det avgjørende for vurderingen vil være om personen har en slik tilknytning til en annen stat, at denne vil kunne utgjøre et effektivt pressmiddel overfor vedkommende eller på annen måte ha betydning for vedkommendes lojalitet til Norge. Praksis vedrørende forståelsen av tilknytningskriteriet etter gjeldende sikkerhetslov 21 første ledd bokstav k, vil være relevant i denne sammenheng.

Med *tjenestested* menes hvor de aktuelle personene arbeider, herunder i hvilken virksomhet og hvilken stilling personene innehar i denne virksomheten.

Etter *bestemmelsens andre ledd* er det et vilkår for utlevering av informasjon som nevnt i første ledd bokstav a til c, at Politiets sikkerhetstjeneste *anfører at det er nødvendig* for å ivareta tjenestens oppgaver etter politiloven §§ 17b og 17c nr. 1. Begrunnelsen for hvorfor utlevering er *nødvendig* i de enkelte tilfellene vil ofte være av en slik karakter at Politiets sikkerhetstjeneste ikke kan, eller ikke ønsker, å dele denne begrunnelsen med andre. Når Politiets sikkerhetstjeneste anfører at slik informasjon er nødvendig, skal derfor Sikkerhetsmyndigheten legge til grunn at vilkårene for utlevering av informasjon er oppfylt. Begrunnelsen vil i ettertid kunne kontrolleres av EOS-utvalget.

§ 8-13 Begrunnelse og underretning

Bestemmelsene er en videreføring av gjeldende sikkerhetslov § 25, med de tilpasninger som er nødvendige for innretningen på lovforslaget for øvrig, og skal forstås på samme måte.

§ 8-14 Innsyn

Bestemmelsene er en videreføring av gjeldende sikkerhetslov § 25a, med de tilpasninger som er nødvendige for innretningen på lovforslaget for øvrig, og skal forstås på samme måte.

Begrepet *sakens dokumenter* skal forstås på samme måte som offentleglovas sakdokumentbegrep, jf. offentleglova § 4 første ledd, jf. andre ledd.

Et *dokument* er i offentleglova § 4 første ledd definert som «ei logisk avgrensa informasjonsmengd som er lagra på eit medium for seinare lesing, lytting, framsyning, overføring eller liknande».

Et *saksdokument* er et dokument som er kommet inn til eller lagt frem for et organ, eller som organet selv har opprettet, og som gjelder ansvarsområdet eller virksomheten til organet. Et dokument er opprettet når det er sendt ut av organet. Dersom dette ikke skjer, skal dokumentet regnes som opprettet når det er ferdigstilt.

Henvisningen i gjeldende lov til «audiovisuelt opptak av egen sikkerhetssamtale», jf. § 19 første ledd andre punktum og tredje ledd andre punktum, er ikke videreført. Audiovisuelle opptak omfattes av offentleglovas dokumentbegrep, og nærmere regler om fremgangsmåten for gjennomsyn av slike opptak bør fastsettes i forskrift.

§ 8-15 Oversendelse av sak til særskilt oppnevnt advokat

Bestemmelsen er en videreføring av gjeldende sikkerhetslov § 25b, med de tilpasninger som er nødvendige for innretning på lovforslaget for øvrig, og skal forstås på samme måte.

§ 8-16 Klage

Bestemmelsen er en videreføring av gjeldende sikkerhetslov § 25c, med de tilpasninger som er nødvendige for innretning på lovforslaget for øvrig, og skal forstås på samme måte.

§ 8-17 Utfyllende bestemmelser

Bestemmelsen er en videreføring av gjeldende sikkerhetslov § 26, med de tilpasninger som er nødvendige for innretning på lovforslaget for øvrig, og skal forstås på samme måte.

Kapittel 9 – Sikkerhetsgraderte anskaffelser mv.

§ 9-1 Sikkerhetsgradert anskaffelse

Bestemmelsen regulerer hva som skal anses som en sikkerhetsgradert anskaffelse. Bestemmelsen er en videreføring av gjeldende sikkerhetslov § 3 nr. 17, med de tilpasninger som er nødvendige i lys av innretningen på det nye lovforslaget.

§ 9-2 Inngåelse av sikkerhetsavtale

Bestemmelsen er i hovedsak en videreføring av gjeldende sikkerhetslov § 27.

Med *anskaffelsesmyndigheten* i *første ledd første punktum* menes den virksomhet som forestår anskaffelsen. Virksomhetsbegrepet er nærmere omtalt i merknaden til § 1-2.

I bestemmelsens *første ledd andre punktum* slås det fast at det skal inngås sikkerhetsavtale både før leverandøren kan få tilgang til gradert informasjon og før leverandøren får tilgang til skjermingsverdig objekt eller infrastruktur. Begrepet *tilgang til* objekt eller infrastruktur skal forstås på samme måte som i § 7-3 tredje ledd.

Hvilke leverandører som i medhold av *første ledd tredje punktum* er *utenlandske* må avgjøres konkret. Som et generelt utgangspunkt vil en leverandør anses som *utenlandsk*, dersom den driver sin virksomhet fra et annet land og under et annet lands jurisdiksjon, og hvor den sikkerhetsmessige oppfølging av leverandøren vil måtte forestås av et annet lands sikkerhetsmyndigheter. Det avgjørende for om leverandøren skal anses utenlandsk eller ikke, vil være hvorvidt Sikkerhetsmyndigheten har faktisk og rettslig anledning til å forestå sikkerhetsmessig oppfølging og kontroll av leverandøren.

Bestemmelsens *andre og tredje ledd* er en videreføring av gjeldende sikkerhetslov § 27 andre og tredje ledd, og skal forstås på samme måte.

§ 9-3 Leverandørklarering

Bestemmelsen er en videreføring av gjeldende sikkerhetslov § 28, med de tilpasninger som er nødvendig i lys av innretningen på det nye lovforslaget, og skal forstås på samme måte.

Med «dersom det av andre grunner anses nødvendig», jf. bestemmelses *første ledd første punktum*, menes i første rekke de tilfeller der leverandøren vil få tilgang til klassifiserte områder innen skjermingsverdig objekt eller infrastruktur, hvor ansvarlig departement har truffet vedtak om krav til adgangsklarering, jf. § 7-3 tredje ledd. Hvorvidt det kreves leverandørklarering for anskaffelser til skjermingsverdig objekt eller infrastruktur, må avgjøres konkret. I vurderingen bør det særlig tas hensyn til hvorvidt leverandørens personell får tilgang til deler av objektet eller infrastrukturen som har et høyt skadepotensial.

Første ledd andre punktum er en videreføring av det vedtatte forslaget i Prop. 97 L (2015–2016) om å gå fra oppdragsbaserte til tidsbaserte leverandørklareringer.

Bestemmelsens *andre til og med femte ledd* er en videreføring av gjeldende sikkerhetslov § 28 andre til og med femte ledd, og skal forstås på samme måte.

§ 9-4 Varslingsplikt og myndighet til å fatte vedtak ved anskaffelser til skjermingsverdig objekt og infrastruktur

Bestemmelsen er en videreføring av det vedtatte forslaget i Prop. 97 L (2015–2016) om anskaffelser til kritisk infrastruktur, med de tilpasninger som er nødvendige i lys av det øvrige lovforslaget. For en nærmere omtale av det vedtatte forslaget og hvilke justeringer som er foreslått, vises det til kapittel 11.2.4 og 11.4.

Bestemmelsen er avgrenset mot sikkerhetsgraderte anskaffelser. Virksomhetenes plikt til å foreta en risikovurdering ved anskaffelsen vil således gjelde alle anskaffelser som ikke er å anse som en sikkerhetsgradert anskaffelse etter §§ 9-2 og 9-3.

§ 9-5 Utfyllende bestemmelser mv.

Bestemmelsen er en videreføring av gjeldende sikkerhetslov § 29, og skal forstås på samme måte.

Kapittel 10 – Eierskapskontroll

§ 10-1 Eierskapskontroll

Etter bestemmelsen *første ledd* pålegges utenlandske erververe en meldeplikt ved erverv av eierandeler i nærmere angitte virksomheter.

Med *erverver* menes både fysiske og juridiske personer. Ved vurderingen av om erververen er *utenlandsk* vil det for fysiske personer måtte sees hen til statsborgerskap og bosted. For juridiske personer vil det måtte gjøres en konkret vurdering. Lokalisering av hovedkontor vil være et moment i denne vurderingen. I henhold til foretaksregistreringsloven § 1-2 regnes ethvert foretak med hovedkontor i Norge eller på norsk kontinentalsokkel, som et norsk foretak. Andre foretak er utenlandske.

Det vil imidlertid også være nødvendig å se hen til det aktuelle foretakets bakenforliggende eierstrukturer. Dersom en utenlandsk person (fysisk eller juridisk) innehar betydelige eierandeler i et norsk foretak, eller på annen måte har betydelig innflytelse over forvaltningen av selskapet, vil foretaket i seg selv måtte sees på som utenlandsk i relasjon til denne bestemmelsen. Med betydelig eierandel menes i utgangspunktet mer enn en tredjedel av aksjekapitalen eller av andelene eller stemmene på selskapets generalforsamling. Hvorvidt erverver kommer fra et annet EU-/EØS-land vil ikke ha betydning for om meldeplikten inntrer.

Virksomhet «av kritisk betydning for grunnleggende nasjonale funksjoner» skal forstås på samme måte som i loven § 1-2. Virksomheter av slik betydning vil være underlagt sikkerhetsloven ved enkeltvedtak etter §§ 2-1 første ledd bokstav c og 2-2 første ledd bokstav e.

Etter *første ledd bokstav a*, inntrer meldeplikt dersom erververen oppnår minst en tredjedel av aksjekapitalen, andelene eller stemmene i virksomheten. Begrepet *minst en tredjedel* viser til aksjelovgivningens bestemmelser om negativ kontroll ved avgjørelser som krever kvalifisert flertall, jf. blant annet aksjeselskapsloven/allmennaksjeselskapsloven § 5-18 første ledd andre punktum og § 2-2 første ledd.

Etter *første ledd bokstav b*, likestilles erverv av aksjer og andeler med erverv av rett til å bli eier når dette må ansees som reelt aksjeeie/andelseie. Et eksempel på erverv av rett til å bli eier kan være såkalte konvertible lån, hvor investor/långiver senere kan innløse gjelden i aksjer eller andeler. Slike konvertible lån innebærer i prinsippet at noen som ikke har skutt inn risikokapital, kan få innflytelse over selskapets beslutninger, og vil etter omstendighetene kunne omfattes av meldeplikten.

Etter *første ledd bokstav c*, inntrer også meldeplikt i de tilfeller erververen oppnår *betydelig innflytelse* over forvaltningen av selskapet på annen måte. Både juridiske og faktiske omstendigheter vil være relevante. Eksempelvis vil underliggende aksjonæravtaler som sikrer erververen kontroll ved strategisk viktige beslutninger i selskapet, være av betydning for vurderingen. Ved vurderingen vil det være naturlig å se hen til det selskapsrettslige kontrollbegrepet, slik dette er utviklet i norsk rettspraksis.

Etter bestemmelsens *andre ledd* skal aksjer som eies eller overtas av aksjeeierens nærstående likestilles med aksjeeierens egne aksjer ved vurderingen av om meldeplikt etter første ledd inntrer. Begrepet *nærstående*, skal forsås på samme måte som legaldefinisjonen av nærstående i relasjon til handel i finansielle instrumenter i verdipapirloven § 2-5.

Bestemmelsens *fjerde ledd* angir det nærmere vurderingstemaet for om Kongen i statsråd kan fatte vedtak etter bestemmelsen. En avgjørelse om å nekte godkjennelse av et slikt erverv skal baseres på en konkret og individuell helhetsvurdering, hvor inngripen kun kan skje av hensyn til sikkerhetsinteresser. Relevante sikkerhetsmessige hensyn kan være hensynet til forsyningssikkerhet og strategisk produksjon av varer og tjenester for grunnleggende nasjonale funksjoner, behovet for å beholde kritisk nøkkelkompetanse av betydning for slike funksjoner eller av hensyn til beskyttelse av sensitiv og/eller sikkerhetsgradert informasjon.

Begrepet *ikke ubetydelig risiko* innebærer at det er erverv med risiko ut over det normale som kvalifiserer for slike vedtak. Vurderingen vil måtte omfatte både sannsynlighet, sårbarhet og mulige konsekvenser ved at ervervet gjennomføres. På sannsynlighetssiden innebærer kriteriet at det ikke skal fattes vedtak dersom det kun foreligger en helt fjerntliggende eller rent teoretisk mulighet for at ervervet kan ha skadevirkninger for grunnleggende nasjonale funksjoner. Det bør være noe konkret med den aktuelle erververen som tilsier at risikoen er høyere enn for andre erververe. Bestemmelsen innebærer imidlertid ikke et krav

om sannsynlighetsovervekt. For øvrig vises det til omtalen av bestemmelsen i kapittel 12.8.

Etter *fjerde ledd* gis det også hjemmel for å sette vilkår ved en godkjenning av ervervet. Fastsetting av vilkår etter denne bestemmelse skal gjøres på bakgrunn av en konkret helhetsvurdering hvor blant annet vilkårets inngripende karakter, hensynet til ivaretakelse av grunnleggende nasjonale funksjoner og erververens forhold tas i betraktning. De vilkår som settes for godkjenning av ervervet må ha en saklige sammenheng med vedtaket og hensynet til ivaretakelse av grunnleggende nasjonale funksjoner.

Kapittel 11 – Kontroll- og tilsynsordninger. Tvangsmulkt, overtredelsesgebyr og straff

§ 11-1 Kontroll- og tilsynsordninger

Bestemmelsen viderefører gjeldende sikkerhetslov § 30.

Første ledd fastslår gjennom begrepet *underlagt* at forebyggende sikkerhetsarbeid etter sikkerhetsloven kan bli gjenstand for kontroll og tilsyn av EOS-utvalget. Bestemmelsen gir ikke direkte føringer for verken organiseringen, gjennomføringen eller omfanget av EOS-utvalgets kontroll.

Med *forebyggende sikkerhetsarbeid* etter loven i første ledd menes planlegging, tilrettelegging, gjennomføring og kontroll av forebyggende sikkerhetstiltak som søker å fjerne eller redusere risiko som følge av tilsiktede uønskede hendelser. Begrepet tilsvarer i all hovedsak begrepet *forebyggende sikkerhetstjeneste* slik det er definert i gjeldende sikkerhetslov § 3 første ledd nr. 1. For en nærmere omtale av forholdet mellom *tilsiktede uønskede hendelser* og *sikkerhetstruende virksomhet*, vises det til kapittel 6.7.4.

Bestemmelsen må ses i sammenheng med EOS-kontrolloven, herunder § 1, som angir EOS-utvalgets kontrollområde til «etterretnings-, overvåknings- og sikkerhetstjeneste som utføres av den offentlige forvaltning eller under styring eller på oppdrag av denne». Kontrollområdet er funksjonelt og ikke organisatorisk definert, se nærmere Dokument 16 (2015–2016) Rapport til Stortinget fra Evalueringsutvalget for Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste, kapittel 17.3.

Andre ledd tilsvarer dagens sikkerhetslov § 30 andre ledd.

§ 11-2 Tvangsmulkt

Bestemmelsen gir hjemmel til å ilegge en virksomhet som har overtrådt loven, løpende mulkt for å tvinge virksomheten til å rette opp i forholdet. Tvangsmulkt forutsetter at det er truffet gyldig enkeltvedtak som pålegger virksomheten å endre sin praksis, jf. § 3-6. Vedtaket må være rettskraftig før mulkten kan begynne å løpe. Mulighetene for å angripe vedtaket ved klage eller rettslige skritt, må altså være uttømt. Med *tilsynsmyndigheten* menes i denne sammenheng Sikkerhetsmyndigheten eller den sektormyndighet som har fått tildelt tilsynsansvaret etter § 3-1.

Tvangsmiddelet må være forholdsmessig, jf. blant annet § 1-1 andre ledd. Vedtaket må ikke være mer tyngende enn det som er nødvendig for å oppnå formålet med mulkten, og må dessuten være egnet til å oppnå formålet.

Vedtak om tvangsmulkt kan påklages, se nærmere i merknadene til § 2-6.

§ 11-3 Overtredelsesgebyr

Bestemmelsen gir tilsynsmyndigheten hjemmel til å ilegge overtredelsesgebyr ved overtredelse av de i første ledd angitte lovbestemmelsene.

Begrepet «noen som handler på dennes vegne» i *første ledd*, angir virksomhetens ansvar utover egen organisasjon. Det må være en viss tilknytning mellom virksomheten og den som har overtrådt bestemmelsen, jf. også § 5-3.

Oppregningen av lovens bestemmelser der overtredelsesgebyr er aktuelt omfatter de bestemmelser i loven som anses særlig viktig å overholde og som dessuten er tilstrekkelig klart formulert til at denne type sanksjon lar seg forsvare.

Ileggelse av gebyr er inngripende og må være forholdsmessig, jf. blant annet § 1-1 andre ledd. Bestemmelsens *andre ledd* angir relevante momenter som skal tas i betraktning ved fastsettelse av gebyrets størrelse. Momentene er relevante også ved vurderingen av om gebyr skal ilegges.

Bestemmelsens *tredje ledd* fastsetter foreldelsesfristen for adgangen til å pålegge overtredelsesgebyr. Utover det som er regulert i tredje ledd gjelder alminnelige regler om foreldelse.

§ 11-4 Straff

Bestemmelsens *første ledd* fastslår at overtredelse av nærmere angitt bestemmelser – de samme som i § 11-3 første ledd bokstav a og b – er straffbart, se merknadene til denne bestemmelsen. *Før-*

ste ledd retter seg i første rekke mot virksomheter som er ansvarlig for overholdelse av de enkelte bestemmelsene.

Bestemmelsens *andre* og *tredje ledd* retter seg mot enkeltpersoner som ikke overholder § 5-3 andre ledd eller forbud gitt i medhold av § 7-5.

Kapittel 12 – Ikrafttredelse og endringer i andre lover

§ 12-1 Ikrafttredelse

Ikrafttredelse av loven forutsetter en omfattende revisjon det det underliggende forskriftsverket til dagens sikkerhetslov. Myndighet til å fatte vedtak om når loven trer i kraft er derfor lagt til Kongen.

Kapittel 14
Lovforslag

Forslag til ny lov om forebyggende nasjonal sikkerhet (sikkerhetsloven)

Kapittel 1. Formål og virkeområde

§ 1-1 *Lovens formål*

Loven skal bidra til å trygge Norges suverenitet, territorielle integritet og demokratiske styreform ved å motvirke tilsiktede uønskede hendelser som kan skade grunnleggende nasjonale funksjoner.

Loven skal sikre at tiltak som iverksettes for å ivareta lovens formål, gjennomføres på en måte som er forenlig med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn.

§ 1-2 *Lovens virkeområde*

Loven gjelder for virksomheter som alene eller sammen med andre råder over informasjon, informasjonssystemer, objekter eller infrastruktur, eller som driver aktivitet, som er av kritisk betydning for grunnleggende nasjonale funksjoner knyttet til

a) de øverste statsorganers virksomhet, sikkerhet eller handlefrihet
b) forsvars-, sikkerhets- og beredskapsmessige forhold
c) forholdet til andre stater
d) landets økonomiske trygghet og velferd
e) befolkningens grunnleggende sikkerhet og overlevelse.

Kongen i statsråd kan gi forskrift om lovens virkeområde og kan herunder helt eller delvis unnta bestemte rettssubjekter eller visse typer informasjon, informasjonssystemer, objekter og infrastruktur.

§ 1-3 *Særbestemmelser om lovens virkeområde*

Loven gjelder for Stortinget og Stortingets organer i den utstrekning Stortinget bestemmer det.

Bestemmelsene gitt i og i medhold av kapittel 8 om personellsikkerhet gjelder ikke for regjeringens medlemmer og dommere i Høyesterett.

Loven gjelder for domstolene med de særregler som følger av bestemmelsene om sikkerhetsklarering og autorisasjon i og i medhold av domstolloven og straffeprosessloven. Kongen kan fastsette ytterligere særregler.

Loven gjelder for leverandører av varer eller tjenester i forbindelse med en sikkerhetsgradert anskaffelse etter loven kapittel 9.

For virksomheter på Svalbard, Jan Mayen og i bilandene gjelder loven i det omfang og med de stedlige tilpasninger Kongen bestemmer.

Kapittel 2. Myndigheter etter loven

§ 2-1 *Departementenes ansvar og myndighet etter loven*

Hvert enkelt departement er ansvarlig for forebyggende sikkerhet innenfor sitt myndighetsområde, og skal

a) identifisere og holde oversikt over grunnleggende nasjonale funksjoner innenfor sitt myndighetsområde
b) identifisere og holde oversikt over virksomheter som direkte eller indirekte er av vesentlig betydning for opprettholdelse av grunnleggende nasjonale funksjoner
c) treffe enkeltvedtak om at virksomheter er av kritisk betydning for grunnleggende nasjonale funksjoner, jf. § 1-2, slik at loven gjelder for dem.

Virksomheter som vurderes å være av kritisk betydning for grunnleggende nasjonale funksjoner, jf. første ledd bokstav c, skal forhåndsvarsles, jf. forvaltningsloven § 16. Selvstendige rettssubjekter kan påklage vedtaket til Tvisteorganet etter reglene i forvaltningsloven kapittel VI.

Ansvarlig departement skal holde Sikkerhetsmyndigheten orientert om oversikter og vedtak etter første ledd bokstav a til c.

Sikkerhetsmyndigheten kan på eget initiativ fremme forslag overfor ansvarlig departement om at det bør treffes vedtak etter første ledd bokstav c. Dersom Sikkerhetsmyndigheten finner at et departements unnlatelse av å treffe slikt vedtak er

uforsvarlig, kan departementets avgjørelse bringes inn for Tvisteorganet.

Kongen i statsråd kan gi forskrift om departementenes ansvar og myndighet etter loven.

§ 2-2 *Sikkerhetsmyndigheten*

Sikkerhetsmyndigheten har det sektorovergripende ansvaret for at gjennomføring av forebyggende sikkerhet i virksomhetene skjer i samsvar med denne loven. Sikkerhetsmyndigheten skal herunder

a) påse at det føres tilsyn med virksomheters gjennomføring av de kravene til forebyggende sikkerhet som følger av loven
b) gi informasjon, råd og veiledning til virksomheter om forebyggende sikkerhet og aktuelle tiltak for å gjennomføre de kravene som følger av loven
c) utarbeide og gjøre tilgjengelig generell informasjon om loven og praktiseringen av den
d) holde en tverrsektoriell oversikt over departementenes identifisering og enkeltvedtak etter § 2-1 første ledd bokstav a til c
e) treffe enkeltvedtak, jf. § 2-1 første ledd bokstav c, overfor virksomheter som ikke anses å falle innenfor et departements myndighetsområde.

For vedtak etter første ledd bokstav e gjelder § 2-1 andre ledd tilsvarende.

Kongen kan gi forskrift om Sikkerhetsmyndighetens ansvar etter loven.

§ 2-3 *Informasjon om trusselvurderinger og risikohåndtering*

Sikkerhetsmyndigheten skal legge til rette for at sektormyndigheter og virksomheter omfattet av loven får informasjon om trusselvurderinger og annen sikkerhetsinformasjon som er av betydning for myndighetenes og virksomhetenes gjennomføring av loven.

Sikkerhetsmyndigheten skal koordinere tilgjengeliggjøring av informasjon som nevnt i første ledd, og i samråd med sektormyndigheter og andre relevante myndigheter påse at det etableres nødvendige arenaer for informasjons- og erfaringsutveksling.

Kongen kan gi forskrift om utveksling av informasjon etter denne bestemmelsen.

§ 2-4 *Nasjonal responsfunksjon for alvorlige dataangrep*

Kongen utpeker en nasjonal responsfunksjon for alvorlige dataangrep mot skjermingsverdig infrastruktur og et nasjonalt varslingssystem for digital infrastruktur.

Når det er nødvendig for å beskytte grunnleggende nasjonale funksjoner, kan den nasjonale responsfunksjonen behandle personopplysninger i form av

a) metadata om IKT-trafikk til og fra virksomheter som er knyttet til det nasjonale varslingssystemet for digital infrastruktur
b) informasjon som er nødvendig for å analysere utløste alarmer i varslingssystemet
c) IP-adresser mottatt fra nasjonale og internasjonale samarbeidspartnere
d) logger og infisert maskinvare, etter samtykke fra en virksomhet der dette er nødvendig i forbindelse med bistand til håndtering av alvorlige dataangrep.

Behandling av andre former for personopplysninger er kun tillatt når det er strengt nødvendig for å beskytte grunnleggende nasjonale funksjoner.

Behandlingen skal i alle tilfeller være proporsjonal med det inngrepet den representerer i personvernet.

Kongen kan gi forskrift om den nasjonale responsfunksjonens behandling av personopplysninger.

§ 2-5 *Vedtaksmyndighet for Kongen i statsråd*

Kongen i statsråd kan fatte enkeltvedtak som er nødvendig for å stanse, begrense eller endre en planlagt eller pågående aktivitet, dersom denne aktiviteten med stor grad av sannsynlighet kan få kritiske skadevirkninger for grunnleggende nasjonale funksjoner. Vedtaket kan fattes uten hensyn til begrensningene i forvaltningsloven § 35 om adgangen til å omgjøre tidligere fattede vedtak, og uavhengig av om aktiviteten ellers er tillatt etter lov eller annet vedtak.

Vedtak etter første ledd skal om mulig være midlertidig og skal ikke ha lengre varighet enn hva som er strengt nødvendig. Vedtaket skal stå i rimelig forhold til den risiko aktiviteten utgjør. Det skal ikke fattes vedtak som er mer inngripende enn det som er strengt nødvendig for å redusere risikoen ved den aktuelle aktiviteten til et akseptabelt nivå.

Før vedtak etter første ledd treffes skal saken utredes så godt som tiden og situasjonen tillater. Berørte parter skal om mulig få anledning til å uttale seg. Den risikoreduserende effekten av vedtaket skal kunne dokumenteres.

Blir vedtak etter første ledd truffet i en situasjon der det ikke er mulig å gjennomføre fullt ut tilfredsstillende saksbehandling, skal slike mangler så snart som mulig rettes. Fremkommer det nye og vesentlige opplysninger i saken, skal det

første vedtaket vurderes på nytt, og nytt enkeltvedtak eventuelt treffes.

Vedtak etter første ledd er særlig tvangsgrunnlag etter tvangsfullbyrdelsesloven kapittel 13.

Kongen i statsråd skal gi forskrift om vedtak etter første ledd, herunder om eventuell kompensasjon til personer og virksomheter som får sin rettslige posisjon svekket som følge av Kongens vedtak.

§ 2-6 *Klage og tvisteløsning*

Vedtak etter loven kan bringes inn for Tvisteorganet for forebyggende nasjonal sikkerhet, jf. § 2-7. Dette gjelder ikke vedtak fattet av Kongen i statsråd med hjemmel i §§ 2-5, 9-4 eller 10-1, og vedtak som nevnt i andre ledd.

Vedtak etter loven kapittel 8 kan påklages til Sikkerhetsmyndigheten. I saker der Sikkerhetsmyndigheten er klareringsmyndighet, kan vedtak påklages til departementet.

Reglene i forvaltningsloven kapittel VI gjelder for selvstendige rettssubjekters klageadgang etter denne loven.

§ 2-7 *Tvisteorgan for forebyggende nasjonal sikkerhet*

Kongen utpeker et kollegialt organ med fem medlemmer som oppnevnes for fire år med adgang til gjenoppnevning for ytterligere fire år.

Ved oppnevning av organets medlemmer skal det, i tillegg til sikkerhetsfaglig kompetanse, også legges vekt på kompetanse innen personvern og selvstendige rettssubjekters rettssikkerhet.

Tvisteorganet kan bestemme at leder eller nestleder, sammen med to andre medlemmer, kan treffe midlertidige vedtak i saker som må avgjøres uten opphold.

Tvisteorganet skal avgi en årlig rapport om sin virksomhet.

Kongen i statsråd kan i forskrift gi nærmere bestemmelser om Tvisteorganets organisering og saksbehandling.

Kapittel 3. Tilsyn etter loven

§ 3-1 *Tilsyn med virksomheter*

Sikkerhetsmyndigheten skal føre tilsyn med departementenes gjennomføring av loven.

Innenfor samfunnssektorer der det finnes andre offentlige myndigheter som har tilsynsfunksjoner som omfatter beskyttelse av informasjon, informasjonssystemer, objekter eller infrastruktur, kan ansvarlig departement, jf. § 2-1, bestemme at disse sektormyndighetene skal føre tilsyn med virksomheter omfattet av loven.

Innenfor samfunnssektorer der det ikke finnes myndigheter med tilsynsfunksjoner som nevnt i andre ledd, skal Sikkerhetsmyndigheten føre tilsyn med virksomheter omfattet av loven.

Sikkerhetsmyndigheten skal føre tilsyn med sektormyndigheter som er tillagt tilsynsansvar etter andre ledd.

Kongen kan gi forskrift om fordeling av tilsynsansvaret mellom Sikkerhetsmyndigheten og aktuelle sektormyndigheter.

§ 3-2 *Sikkerhetsmyndighetens samarbeid med sektormyndigheter*

Sikkerhetsmyndigheten skal samarbeide med andre offentlige myndigheter som i medhold av lov har tilsynsfunksjoner innenfor sin samfunnssektor som omfatter beskyttelse av informasjon, informasjonssystemer, objekter eller infrastruktur.

Gjennomføring av tilsyn skal i størst mulig grad samordnes med andre tilsynsmyndigheter.

For områder der sektormyndigheter har tilsynsansvar etter § 3-1, skal det inngås samarbeidsavtaler mellom Sikkerhetsmyndigheten og sektormyndighetene.

Som grunnlag for sektormyndighetenes tilsyn etter loven, skal Sikkerhetsmyndigheten

a) utarbeide og vedlikeholde grunnleggende kriterier for tilsyn etter loven med forskrifter
b) forestå felles opplæring av tilsynspersonell.

Sikkerhetsmyndigheten kan, dersom den anser det nødvendig, medvirke til forberedelse og gjennomføring av tilsyn. Sektormyndighetene kan anmode Sikkerhetsmyndigheten om slik bistand.

Sektormyndigheter som har tilsynsansvar etter loven, jf. § 3-1, skal orientere Sikkerhetsmyndigheten om hovedfunn.

Kongen kan gi forskrift om samarbeidet mellom Sikkerhetsmyndigheten og sektormyndighetene.

§ 3-3 *Generelle prinsipper for tilsyn*

Tilsyn etter loven skal planlegges og gjennomføres på en slik måte at tilsynet virker minst mulig forstyrrende på tilsynsobjektenes daglige drift.

Opplysninger som tilsynsmyndigheten innhenter som ledd i tilsynsvirksomheten skal bare nyttes i direkte forbindelse med tilsynet.

Forvaltningslovens bestemmelser om taushetsplikt gjelder for personell som på vegne av tilsynsmyndigheten gjennomfører tilsyn etter loven.

§ 3-4 *Stedlig tilsyn*

I den grad det er nødvendig for å gjennomføre tilsyn etter loven, kan tilsynsmyndigheten kreve

nødvendig adgang til virksomhetens informasjon, informasjonssystemer, objekter og infrastruktur.

Stedlig tilsyn som nevnt i første ledd skal normalt varsles skriftlig. Forvaltningsloven § 15 gjelder tilsvarende.

Kongen kan gi forskrift om tilsynsmyndighetens stedlige tilsyn.

§ 3-5 *Tilsynsmyndighetens behandling av personopplysninger*

Når det er nødvendig for å utføre oppgavene etter loven, kan tilsynsmyndigheten behandle opplysninger som direkte eller indirekte kan knyttes til en fysisk enkeltperson (personopplysninger).

Behandlingen av personopplysninger etter første ledd må være proporsjonal med det inngrepet den representerer i personvernet.

Behandlingen av personopplysninger etter første ledd skal om mulig skje ved hjelp av virksomhetens informasjonssystem, og uten at personopplysninger blir kopiert eller overført til tilsynsmyndigheten. Tilsynsmyndigheten kan likevel kreve kopi av personopplysninger som er nødvendige for å bekrefte, avkrefte eller dokumentere at bestemmelser i loven er brutt. Virksomheten skal varsles om hvilke opplysninger det blir tatt kopi av.

Kongen kan gi forskrift om tilsynsmyndighetens behandling av personopplysninger.

§ 3-6 *Pålegg*

Pålegg etter loven kan bare gis dersom det er utvilsomt at tiltaket er nødvendig for å ivareta lovens formål, og de kostnadene som påføres virksomheten, står i et rimelig forhold til det som kan oppnås ved tiltaket.

Sektormyndighet med tilsynsansvar etter loven kan gi pålegg om gjennomføring av tiltak innenfor sin sektor. Sikkerhetsmyndigheten kan gi virksomheter som ikke er underlagt tilsyn fra en sektormyndighet, pålegg om gjennomføring av tiltak.

Sikkerhetsmyndigheten kan gi en sektormyndighet med tilsynsansvar etter loven nødvendige pålegg for å sikre at lovens formål ivaretas.

Pålegg kan påklages til Tvisteorganet. Reglene i forvaltningsloven kapittel VI gjelder for selvstendige rettssubjekters klageadgang.

Kapittel 4. Generelle krav til forebyggende sikkerhet

§ 4-1 *Plikt til å gjennomføre sikkerhetstiltak*

Virksomheten skal, på grunnlag av risiko- og sårbarhetsanalysen, jf. § 4-3, gjennomføre forebyggende sikkerhetstiltak. Tiltakene skal gi et forsvarlig sikkerhetsnivå, og

a) bidra til å hindre tilsiktede uønskede hendelser som kan skade informasjon, informasjonssystemer, objekter, infrastruktur eller aktivitet av kritisk betydning for grunnleggende nasjonale funksjoner
b) redusere skadevirkningene dersom slike hendelser inntreffer

Kostnader ved sikkerhetstiltak etter loven skal stå i et rimelig forhold til det som oppnås ved tiltaket.

Forutsatt at kravene som følger av første ledd og loven for øvrig oppfylles, kan planlegging og gjennomføring av forebyggende tiltak mot tilsiktede uønskede hendelser skje i sammenheng med forebyggende tiltak mot annen risiko som foreligger for virksomheten.

Kongen kan gi forskrift om plikter for virksomheter som omfattes av loven.

§ 4-2 *Sikkerhetsstyring*

Ansvaret for forebyggende sikkerhet etter loven påhviler leder for virksomheten. Forebyggende sikkerhet skal innarbeides som en del av virksomhetens styringssystem.

Virksomheten skal påse at dens ansatte, leverandører og oppdragstakere har tilstrekkelig opplæring i sikkerhetsspørsmål, og skal regelmessig kontrollere sikkerhetstilstanden i virksomheten. For leverandører til sikkerhetsgraderte anskaffelser gjelder loven kapittel 9.

Kongen kan gi forskrift om sikkerhetsstyring, herunder om bruk av standarder.

§ 4-3 *Risiko- og sårbarhetsanalyse*

Som grunnlag for virksomhetens forebyggende sikkerhetstiltak skal det gjennomføres en risiko- og sårbarhetsanalyse. Virksomheten skal herunder kartlegge hvilke andre virksomheter den er avhengig av for å opprettholde sin funksjonalitet.

Risiko- og sårbarhetsanalysen skal jevnlig gjennomgås, og om nødvendig revideres.

Sikkerhetsmyndigheten, eller sektormyndighet som er gitt tilsynsansvar etter loven, skal på anmodning rådgi og veilede virksomheten ved gjennomføring av risiko- og sårbarhetsanalyser.

Kongen kan gi forskrift om risiko- og sårbarhetsanalyse, herunder om bruk av standarder.

§ 4-4 *Krav til dokumentasjon*

Virksomheten skal dokumentere at

a) risiko- og sårbarhetsanalyse er gjennomført

b) nødvendige sikkerhetstiltak for å redusere risikoen for og konsekvensene av tilsiktede uønskede hendelser er iverksatt.

Kongen kan gi forskrift om krav til dokumentasjon.

§ 4-5 *Øvelser*

Virksomheten skal gjennomføre regelmessige øvelser for å sikre at kompetansen til å forebygge og håndtere tilsiktede uønskede hendelser vedlikeholdes og utvikles.

Kongen kan gi forskrift om øvelser.

§ 4-6 *Varsling*

Virksomheten skal omgående varsle tilsynsmyndigheten dersom

a) en tilsiktet uønsket hendelse har rammet virksomheten, som kan ha betydning for virksomhetens evne til å ivareta oppgaver knyttet til grunnleggende nasjonale funksjoner
b) det er begrunnet mistanke om at det har inntruffet eller er fare for at det vil inntreffe en hendelse som nevnt i bokstav a
c) det er begrunnet mistanke om at det har inntruffet eller er fare for at det vil inntreffe en tilsiktet uønsket hendelse som kan ha kritiske skadevirkninger for grunnleggende nasjonale funksjoner, selv om dette ikke er rettet mot virksomheten
d) det har skjedd brudd på krav til sikkerhet i kapittel 5, 6 eller 7, med forskrifter.

I samfunnssektorer der sektormyndigheter er gitt tilsynsansvar i medhold av § 3-1, skal Sikkerhetsmyndigheten varsles parallelt.

Tilsynsmyndigheten skal uten ugrunnet opphold videresende varsel etter første ledd bokstav c til ansvarlig departement for vurdering av enkeltvedtak etter § 2-5. Der Sikkerhetsmyndigheten er tilsynsmyndighet skal varsel uten ugrunnet opphold videresendes til departementet.

Varslingsplikten etter denne bestemmelsen gjelder uten hinder av lovbestemt taushetsplikt.

Kongen kan gi forskrift om virksomhetenes varslingsplikt etter loven.

§ 4-7 *Behandling av personopplysninger*

Behandling av personopplysninger som skjer med det formål å etterleve bestemmelsene i denne loven, skal skje i samsvar med prinsippene i Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 artikkel 5, jf. artikkel 23.

Kapittel 5. Informasjonssikkerhet

§ 5-1 *Sikkerhetsgradert informasjon*

Den som utsteder eller på annen måte tilvirker informasjon skal, på bakgrunn av en skadevurdering, sikkerhetsgradere og merke informasjonen på følgende måte:

a) STRENGT HEMMELIG benyttes dersom det kan få helt avgjørende skadefølger for grunnleggende nasjonale funksjoner, jf. § 1-2, om informasjonen blir kjent for uvedkommende
b) HEMMELIG benyttes dersom det kan få alvorlige skadefølger for grunnleggende nasjonale funksjoner, jf. § 1-2, om informasjonen blir kjent for uvedkommende
c) KONFIDENSIELT benyttes dersom det kan få skadefølger for grunnleggende nasjonale funksjoner, jf. § 1-2, om informasjonen blir kjent for uvedkommende
d) BEGRENSET benyttes dersom det i noen grad kan få skadefølger for grunnleggende nasjonale funksjoner, jf. § 1-2, om informasjonen blir kjent for uvedkommende.

Sikkerhetsgradering skal ikke skje i større utstrekning eller for lengre tid enn nødvendig. Sikkerhetsgraderingen skal bortfalle senest etter 30 år. I særskilte tilfeller kan Kongen beslutte unntak fra 30-års-regelen i andre punktum.

Kongen kan gi forskrift om sikkerhetsgradering.

Innenfor rammen av gjensidig overenskomst med fremmed stat eller internasjonal organisasjon kan Kongen i forskrift gi nærmere bestemmelser om sikkerhetsgradering og beskyttelse av informasjon som mottas fra eller avgis til vedkommende stat eller internasjonale organisasjon.

§ 5-2 *Beskyttelse av sikkerhetsgradert informasjon*

Virksomheten skal iverksette nødvendige sikkerhetstiltak slik at sikkerhetsgradert informasjon

a) ikke blir kjent for uvedkommende
b) ikke går tapt eller blir endret uten at dette er autorisert
c) er tilgjengelig for autoriserte personer der tjenstlige behov tilsier dette.

Kongen kan gi forskrift om minstekrav for beskyttelse av sikkerhetsgradert informasjon.

§ 5-3 *Tilgang til og taushetsplikt for sikkerhetsgradert informasjon*

Sikkerhetsgradert informasjon skal bare overlates til personer som har tjenstlig behov og er autorisert for slik tilgang.

Enhver som får tilgang til sikkerhetsgradert informasjon som ledd i arbeid, oppdrag, verv eller

aktivitet for en virksomhet som omfattes av loven har taushetsplikt om innholdet. Taushetsplikten gjelder også etter at vedkommende har avsluttet arbeidet, oppdraget, vervet eller aktiviteten.

§ 5-4 *Tekniske sikkerhetsundersøkelser*

Sikkerhetsmyndigheten, eller den Sikkerhetsmyndigheten bemyndiger, kan foreta undersøkelser av lokaler, bygninger og andre objekter som en virksomhet alene eller sammen med andre råder over, i den hensikt å fastslå om uvedkommende med eller uten tekniske hjelpemidler kan skaffe seg tilgang til sikkerhetsgradert informasjon ved avlytting av tale, avlesning av signaler eller ved innsyn.

Kongen kan gi forskrift om tekniske sikkerhetsundersøkelser.

Kapittel 6. Informasjonssystemsikkerhet

§ 6-1 *Skjermingsverdige informasjonssystemer*

Med skjermingsverdige informasjonssystemer menes

a) informasjonssystemer som er av kritisk betydning for grunnleggende nasjonale funksjoner
b) informasjonssystemer som behandler sikkerhetsgradert informasjon.

§ 6-2 *Beskyttelse av skjermingsverdige informasjonssystemer*

Virksomheten skal gjennomføre nødvendige tiltak for å oppnå et forsvarlig sikkerhetsnivå for skjermingsverdige informasjonssystemer. Tiltakene skal sikre at

a) informasjonssystemene opprettholder sin funksjonalitet
b) konfidensialiteten, integriteten og tilgjengeligheten til informasjon som behandles, ivaretas.

Kongen kan gi forskrift om beskyttelse av skjermingsverdige informasjonssystemer.

§ 6-3 *Godkjenning av skjermingsverdige informasjonssystemer*

Skjermingsverdige informasjonssystemer skal godkjennes av en ansvarlig godkjenningsmyndighet.

Informasjonssystemer som skal behandle sikkerhetsgradert informasjon skal forhåndsgodkjennes.

Kongen kan gi forskrift om godkjenning av skjermingsverdige informasjonssystemer, herunder utpeking av ansvarlige godkjenningsmyndigheter og krav til leverandører.

§ 6-4 *Overvåking av skjermingsverdige informasjonssystemer*

Virksomheten skal kontinuerlig overvåke sine skjermingsverdige informasjonssystemer for å forebygge og håndtere tilsiktede uønskede hendelser som kan skade informasjonssystemet. Hendelser som er relevante for sikkerhetsarbeidet skal registreres.

I den grad det er nødvendig for å ivareta formålet med overvåkningen skal utveksling av informasjon til, fra og i skjermingsverdige informasjonssystemer registreres, lagres og analyseres.

Overvåkning av informasjonssystemer som behandler personopplysninger skal begrenses til de metoder og det omfang som er strengt nødvendig for å ivareta formålet med overvåkningen.

Informasjon etter første og andre ledd kan lagres i inntil fem år. Lagrede personopplysninger kan kun benyttes i den utstrekning det er nødvendig for å ivareta formålet med overvåkningen.

Flere virksomheter som er tilknyttet samme informasjonssystem, kan avtale at en av virksomhetene skal forestå overvåkningen etter første og andre ledd på vegne av de øvrige virksomhetene. Den virksomheten som forestår overvåkningen plikter å sikre at kravene til informasjonssikkerhet i § 5-2 etterleves også for den informasjon den blir kjent med som følge av avtalen om felles overvåkning.

Virksomheten skal påse at autoriserte brukere av informasjonssystemer som overvåkes i henhold til denne bestemmelse, får informasjon om formålet med behandlingen, om de tiltak som er iverksatt, herunder metode og omfang, om informasjonen blir utlevert og eventuelt om hvem som er mottaker.

Kongen kan i forskrift gi nærmere bestemmelser om overvåkning av skjermingsverdige informasjonssystemer, herunder

a) hvilke typer informasjon som kan eller skal registreres, lagres og analyseres i forbindelse med eller som resultat av overvåkningen
b) hvem som skal ha tilgang til informasjon som er registrert og lagret i forbindelse med eller som resultat av overvåkningen
c) hvordan tilgang til registrert eller lagret informasjon skal gis
d) unntak fra lagringstid på fem år, jf. fjerde ledd.

§ 6-5 *Kommunikasjons- og innholdskontroll av informasjonssystemer*

Ledelsen i virksomheten kan anmode Sikkerhetsmyndigheten om å kontrollere om virksomhetens informasjonssystemer kun behandler slik informasjon som sikkerhetsgodkjenningen tilla-

ter. Virksomhetens ansatte skal orienteres om at slike kontroller kan forekomme.

Kontrollen kan gjennomføres ved å avlytte og avlese informasjon som behandles i eller kommuniseres mellom informasjonssystemer.

Iverksettelse av kontrollen kan ikke skje før virksomhetens ledelse har godtatt metodene som tenkes benyttet og Sikkerhetsmyndighetens vurdering av faren for at kontrollen kan fange opp kommunikasjon som nevnt i fjerde ledd.

Kontrollen skal ikke omfatte privat kommunikasjon eller kommunikasjon med virksomheter som ikke er omfattet av loven. Avdekker kontrollen at slik kommunikasjon likevel fanges opp skal kontrollen straks opphøre og informasjon som kontrollen har gitt tilgang til slettes.

Det er forbudt for tjenestepersoner som får tilgang til informasjon som nevnt i fjerde ledd, å bringe informasjonen videre til andre tjenestepersoner. For øvrig gjelder taushetsplikt etter § 5-3.

Når informasjon som er samlet inn i samsvar med første ledd ikke lenger har betydning for det angitte kontrollformålet, skal Sikkerhetsmyndigheten straks slette informasjonen.

Kongen kan i forskrift gi nærmere bestemmelser om kommunikasjons- og innholdskontroll av informasjonssystemer.

§ 6-6 *Inntrengningstesting av skjermingsverdige informasjonssystemer*

Ledelsen i virksomheten kan anmode Sikkerhetsmyndigheten om å forsøke å trenge inn i virksomhetens skjermingsverdige informasjonssystemer. Formålet kan bare være å kontrollere om motstandskraften til etablerte sikkerhetstiltak er tilfredsstillende, i den hensikt å forbedre sikkerheten. Virksomhetens ansatte skal orienteres om at slike kontroller kan forekomme.

Dersom kontrollen innebærer behandling av personopplysninger skal den begrenses til de metoder og det omfang som er strengt nødvendig for å ivareta formålet med kontrollen.

Informasjon som kontrollen gir tilgang til kan kun benyttes til å ivareta formålet med kontrollen. Når det ikke lenger er behov for informasjonen skal den slettes.

Dersom Sikkerhetsmyndigheten klarer å trenge inn i informasjonssystemet, skal fremgangsmåte og resultat dokumenteres, og operasjonen avsluttes.

Sikkerhetsmyndigheten skal gi rapport om resultatet av kontrollen til virksomheten. Rapporten skal kun inneholde informasjon som er av betydning for forbedring av virksomhetens sikkerhet.

Kongen kan gi nærmere forskrifter om inntrengning i skjermingsverdige informasjonssystemer, herunder gjennomføring av inntrengningstesting av andre enn Sikkerhetsmyndigheten.

Kapittel 7. Objekt- og infrastruktursikkerhet

§ 7-1 *Skjermingsverdige objekter og infrastruktur*

Hver enkelt departement skal innen sitt myndighetsområde utpeke, klassifisere og holde oversikt over objekter og infrastruktur av kritisk betydning for grunnleggende nasjonale funksjoner.

Sikkerhetsmyndigheten skal utpeke, klassifisere og holde oversikt over objekter og infrastruktur som ikke ligger innenfor et departements myndighetsområde.

Virksomheter som råder over objekter eller infrastruktur som utpekes etter første eller andre ledd, skal varsles om dette. Avgjørelse om utpeking som berører selvstendige rettssubjekter kan påklages til Tvisteorganet etter reglene i forvaltningsloven kapittel VI.

Sikkerhetsmyndigheten kan på eget initiativ foreslå utpeking av objekter og infrastruktur overfor ansvarlig departement. Dersom Sikkerhetsmyndigheten finner at et departements unnlatelse av å utpeke objekter eller infrastruktur er uforsvarlig, kan departementets avgjørelse bringes inn for Tvisteorganet for endelig avgjørelse.

Kongen kan gi forskrift om identifisering og utpeking av objekter og infrastruktur.

§ 7-2 *Klassifisering*

Skjermingsverdige objekter og infrastruktur skal klassifiseres i en av følgende klassifiseringsgrader:

a) MEGET KRITISK nyttes dersom det kan få helt avgjørende skadefølger for grunnleggende nasjonale funksjoner, jf. § 1-2, om objektet eller infrastrukturen får redusert funksjonalitet
b) KRITISK nyttes dersom det kan få alvorlige skadefølger for grunnleggende nasjonale funksjoner, jf. § 1-2, om objektet eller infrastrukturen får redusert funksjonalitet
c) VIKTIG nyttes dersom det kan få skadefølger for grunnleggende nasjonale funksjoner, jf. § 1-2, om objektet eller infrastrukturen får redusert funksjonalitet.

Klassifiseringen skal skje på grunnlag av virksomhetens risiko- og sårbarhetsanalyse, jf. § 4-3, og skal begrunnes ut ifra hvilke grunnleggende nasjonale funksjoner objektet eller infrastrukturen understøtter og konsekvensene av redusert funk-

sjonalitet. Begrunnelsen skal inngå i departementenes og Sikkerhetsmyndighetens oversikt over skjermingsverdige objekter og infrastruktur.

Dersom en del av et objekt eller infrastruktur har en høyere klassifisering enn objektet eller infrastrukturen for øvrig, skal denne defineres som selvstendig objekt eller infrastruktur.

Kongen kan gi forskrift om klassifisering av skjermingsverdige objekter og infrastruktur.

§ 7-3 *Beskyttelse av objekter og infrastruktur*

Virksomheten skal iverksette nødvendige sikkerhetstiltak for å opprettholde et forsvarlig sikkerhetsnivå.

Ved vurderingen av hva som er nødvendig skal virksomheten ta hensyn til klassifiseringsnivået på objektet eller infrastrukturen, og konsekvensen ved bortfall eller reduksjon av funksjonalitet. Sikkerhetstiltakene skal ses i sammenheng og tilpasses det enkelte objekts, eller den enkelte infrastrukturs, konkrete beskyttelsesbehov.

Ansvarlig departement kan treffe enkeltvedtak om krav til adgangsklarering etter loven kapittel 8, for tilgang til hele eller deler av skjermingsverdige objekter eller infrastruktur, innen sitt myndighetsområde. Sikkerhetsmyndigheten kan treffe slike vedtak overfor virksomheter som ikke ligger innenfor et departements myndighetsområde.

Avgjørelse om adgangsklarering etter tredje ledd som berører selvstendige rettssubjekter, kan påklages til Tvisteorganet etter reglene i forvaltningsloven kapittel VI.

Kongen kan gi forskrift om beskyttelse av objekter og infrastruktur innenfor hvert klassifiseringsnivå.

§ 7-4 *Testing av sikkerhetssystemer*

Ledelsen i virksomheten kan anmode Sikkerhetsmyndigheten om å forsøke å forsere etablerte sikkerhetstiltak for tilgang til skjermingsverdige objekter eller infrastruktur. Formålet kan bare være å forbedre sikkerhetsnivået gjennom å kontrollere motstandskraften til sikkerhetstiltakene. Virksomhetens ansatte skal orienteres om at slike kontroller kan forekomme.

Dersom kontrollen innebærer behandling av personopplysninger skal den begrenses til de metoder og det omfang som er strengt nødvendig for å ivareta formålet med kontrollen.

Informasjon som kontrollen gir tilgang til kan kun benyttes til å ivareta formålet med kontrollen. Når det ikke lenger er behov for informasjonen skal den slettes.

Dersom Sikkerhetsmyndigheten klarer å forsere sikkerhetstiltakene for tilgang til objekt eller infrastruktur, skal operasjonen avsluttes.

Kongen kan gi forskrift om testing av sikkerhetssystemer for skjermingsverdige objekter og infrastruktur, herunder gjennomføring av slik testing av andre enn Sikkerhetsmyndigheten.

§ 7-5 *Adgang til steder og områder*

Kongen kan av hensyn til forsvars-, sikkerhets- og beredskapsmessige forhold, jf. § 1-2 første ledd bokstav b, forby uvedkommende adgang til bestemt angitte områder og å overvære militære øvelser eller forsøk.

Kapittel 8. Personellsikkerhet

§ 8-1 *Når klarering og autorisasjon skal gjennomføres*

Person som skal gis tilgang til sikkerhetsgradert informasjon, skal ha autorisasjon i samsvar med § 8-2. Det samme gjelder person som skal ha adgang til klassifiserte områder innen objekter eller infrastruktur som er av kritisk betydning for grunnleggende nasjonale funksjoner, og det er truffet vedtak etter § 7-3 tredje ledd.

Person som skal autoriseres for tilgang til informasjon gradert KONFIDENSIELT eller høyere, skal på forhånd sikkerhetsklareres, jf. § 8-5. Sikkerhetsklarering må foreligge før autorisasjon kan gis.

Person som har gyldig sikkerhetsklarering skal også anses adgangsklarert.

Person som gjennom sitt arbeid vil kunne få tilgang til sikkerhetsgradert informasjon gradert KONFIDENSIELT eller høyere, skal sikkerhetsklareres. Dette gjelder likevel ikke dersom risikoen for slik tilgang kan fjernes ved å iverksette sikkerhetstiltak.

Sikkerhetsklarering gis for følgende nasjonale sikkerhetsgrader, eventuelt også for tilsvarende sikkerhetsgrader i NATO eller annen internasjonal organisasjon:

a) STRENGT HEMMELIG (eventuelt COSMIC TOP SECRET/tilsvarende)
b) HEMMELIG (eventuelt NATO SECRET/ tilsvarende)
c) KONFIDENSIELT (eventuelt NATO CONFIDENTIAL/tilsvarende).

§ 8-2 *Sikkerhetsautorisasjon*

Virksomhetens leder er ansvarlig for autorisasjon.

Autorisasjonsansvarlig har ansvaret for den daglige sikkerhetsmessige ledelse og kontroll av autorisert personell i egen virksomhet.

Autorisasjon kan gis dersom autorisasjonsansvarlig etter en konkret helhetsvurdering ikke har opplysninger som gjør det tvilsomt om vedkommende sikkerhetsmessig er til å stole på. Autorisasjon skal ikke gis før det foreligger melding om klarering, der dette er påkrevd etter § 8-1 andre ledd. Autorisasjonssamtale skal i alle tilfeller avholdes før autorisasjon gis.

Virksomheten skal løpende orientere Sikkerhetsmyndigheten om hvilke personer som er autorisert.

Kongen kan gi forskrift om autorisasjon og autorisasjonsansvarliges plikter etter loven.

§ 8-3 *Nedsettelse, suspensjon og tilbakekallelse av autorisasjon*

Får autorisasjonsansvarlig opplysninger som gir grunn til tvil om en autorisert person fortsatt kan anses sikkerhetsmessig skikket, skal autorisasjonen vurderes tilbakekalt, nedsatt eller suspendert. Avgjørelse om dette skal innberettes til vedkommende klareringsmyndighet.

Autorisasjon bortfaller automatisk når

a) personen fratrer den stilling som autorisasjonen er knyttet til
b) behovet for autorisasjon ikke lenger er til stede
c) personen ikke lenger har tilstrekkelig klarering.

§ 8-4 *Klareringsmyndigheter etter loven*

Kongen utpeker én klareringsmyndighet for forsvarssektoren og én for sivile sektorer. Klareringsmyndighetene avgjør om det er grunn til å anta at en person er sikkerhetsmessig skikket til å håndtere sikkerhetsgradert informasjon opp til et gitt sikkerhetsnivå eller for adgang til klassifiserte områder innen objekter eller infrastruktur som er av kritisk betydning for grunnleggende nasjonale funksjoner. Etterretnings- og sikkerhetstjenestene klarerer eget personell.

Når særlige grunner taler for det kan Kongen utpeke andre klareringsmyndigheter enn de som er nevnt i første ledd.

§ 8-5 *Sikkerhets- og adgangsklarering*

Klarering skal bare gis eller opprettholdes dersom det ikke foreligger rimelig tvil om vedkommendes sikkerhetsmessige skikkethet. Som grunnlag for vurderingen av en persons sikkerhetsmessige skikkethet skal det gjennomføres en personkontroll, jf. § 8-7.

Klareringsavgjørelser skal baseres på en konkret og individuell helhetsvurdering av de foreliggende opplysninger. Klareringsmyndigheten skal påse at klareringssaken er så godt opplyst som mulig før avgjørelse fattes. Sikkerhetssamtale skal gjennomføres der dette ikke anses som åpenbart unødvendig

I vurderingen skal det bare legges vekt på forhold som er relevante for vedkommendes pålitelighet, lojalitet og sunne dømmekraft med hensyn til behandling av gradert informasjon, og tilgang til skjermingsverdige objekter og infrastruktur. Politisk engasjement og annet lovlig samfunnsengasjement, herunder medlemskap i, sympati med eller aktivitet for lovlige politiske partier eller organisasjoner, skal ikke ha betydning for vurderingen av en persons sikkerhetsmessige skikkethet.

Negative opplysninger om nærstående personer, jf. § 8-7 tredje ledd, skal bare tas i betraktning dersom det antas at nærståendes forhold vil kunne påvirke vedkommendes sikkerhetsmessige skikkethet.

Kongen kan gi forskrift om hvilke forhold som kan tillegges betydning for vurderingen av sikkerhetsmessig skikkethet.

§ 8-6 *Nedsettelse, suspensjon og tilbakekallelse av klarering*

Får klareringsmyndigheten opplysninger som gir grunn til tvil om en sikkerhetsklarert persons sikkerhetsmessige skikkethet, skal klareringsmyndigheten vurdere å tilbakekalle eller nedsette klareringen, eller suspendere klareringen og iverksette nærmere undersøkelser for å avklare forholdet.

Er en sikkerhets- eller adgangsklarering besluttet tilbakekalt, nedsatt eller suspendert, skal begrunnet melding om dette sendes til Sikkerhetsmyndigheten. Autorisasjonsansvarlig skal varsles umiddelbart.

§ 8-7 *Gjennomføring av personkontroll*

Personkontroll skal gjennomføres som grunnlag for sikkerhets- eller adgangsklarering. Med mindre annet er bestemt av Sikkerhetsmyndigheten, skal personkontroll iverksettes etter anmodning fra autorisasjonsansvarlig. Før personkontroll igangsettes skal den som klareres motta informasjon om at slik kontroll vil bli foretatt, og skal ha akseptert dette. Aksepten skal også omfatte muligheten for personkontroll av nærstående personer etter tredje ledd, og fornyet kontroll etter § 8-8.

Personkontroll skal alltid omfatte opplysninger gitt av vedkommende selv. Vedkommende plikter å gi fullstendige opplysninger om forhold som den antar vil kunne være av betydning for

vurderingen av sikkerhetsmessig skikkethet etter § 8-5.

Ved sikkerhetsklarering for HEMMELIG/tilsvarende eller høyere sikkerhetsgrader, og i andre særlige tilfeller, kan det gjennomføres personkontroll av nærstående personer.

I tillegg til opplysninger som personen gir, skal kontrollen omfatte opplysninger som vedkommende klareringsmyndighet selv har, samt opplysninger fra offentlige registre, jf. åttende ledd. Behandlingsansvarlig plikter å utlevere registeropplysninger uten hinder av taushetsplikt. Registeropplysninger skal meddeles skriftlig. Kontrollen kan også omfatte andre kilder, herunder uttalelser fra tjenestesteder eller arbeidsplasser, offentlige myndigheter eller oppgitte eller supplerende referanser. Opplysninger som gis i forbindelse med personkontroll skal gis vederlagsfritt til klareringsmyndigheten.

Behandlingsansvarlige for relevante registre plikter å legge til rette for digitalisert overføring av personkontrollopplysningene til Sikkerhetsmyndigheten.

Opplysninger som er gitt klareringsmyndigheten i forbindelse med personkontroll, skal ikke benyttes til andre formål enn vurdering av klarering. Autorisasjonsansvarlig kan likevel meddeles opplysninger dersom dette anses påkrevet av hensyn til den sikkerhetsmessige ledelse og kontroll av vedkommende.

Personkontroll etter denne bestemmelsen skal for øvrig skje i samsvar med § 4-7.

Kongen gir forskrift om hvilke registre som er relevante for personkontroll for henholdsvis sikkerhetsklarering og adgangsklarering, samt fastsetter nærmere bestemmelser for digitalisert overføring av personkontrollopplysninger.

Kongen kan gi forskrift om fremgangsmåten ved registerundersøkelser i utlandet og om utlevering av opplysninger i forbindelse med andre lands myndigheters tilsvarende personkontroll. Under ingen omstendighet skal det innhentes, registreres eller videreformidles opplysninger om politisk engasjement som omfattes av § 8-5 andre ledd.

§ 8-8 *Fornyet personkontroll*

Klareringsmyndigheten kan be Sikkerhetsmyndigheten om å iverksette ny personkontroll, jf. § 8-7, av klarert personell når som helst innenfor en klarerings gyldighetstid, i den hensikt å kontrollere om det har skjedd endringer av betydning for vedkommendes sikkerhetsmessige skikkethet.

§ 8-9 *Bruk av vilkår og stillingsklarering*

En klarering kan i særlige tilfeller gis på nærmere angitte vilkår, og kan herunder være avgrenset til å kun gjelde en konkret stilling. Ved vurderingen av om det skal settes vilkår for klareringen, skal det særlig tas stilling til om andre tiltak vil kunne ha tilsvarende risikoreduserende effekt.

Kongen kan gi forskrift om bruk av vilkår og stillingsklarering.

§ 8-10 *Klarering av personer som ikke er norske statsborgere*

En person som ikke er norsk statsborger kan etter en konkret helhetsvurdering gis klarering. Klarering skal bare gis eller opprettholdes dersom det ikke foreligger rimelig tvil om vedkommendes sikkerhetsmessige skikkethet. I vurderingen skal det legges vekt på hjemlandets sikkerhetsmessige betydning og vedkommendes tilknytning til hjemlandet, samt vedkommendes eventuelle tilknytning til Norge. Ved klarering av personer som ikke er norske statsborgere skal det vurderes særskilt om bruk av vilkår eller stillingsklarering kan være risikoreduserende tiltak, jf. § 8-9.

Kongen kan gi forskrift om klarering av personer som ikke er norske statsborgere.

§ 8-11 *Varslingsplikt*

Klarert og autorisert person skal umiddelbart varsle autorisasjonsansvarlig om forhold som antas å kunne være av betydning for vedkommendes sikkerhetsmessige skikkethet.

Autorisasjonsansvarlig skal orientere vedkommende klareringsmyndighet dersom forholdet antas å kunne få betydning for vedkommendes klarering.

§ 8-12 *Informasjonstilgang for Politiets sikkerhetstjeneste*

I klareringssaker hvor personen eller nærstående har tilknytning til andre stater, kan Sikkerhetsmyndigheten på anmodning fra Politiets sikkerhetstjeneste gi informasjon om aktuelle personers

a) klareringsstatus
b) tilknytning til andre stater
c) tjenestested.

Utlevering av informasjon etter første ledd kan kun skje der Politiets sikkerhetstjeneste anfører at dette er nødvendig for å ivareta tjenestens oppgaver etter politiloven §§ 17 b og 17 c nr. 1.

Kongen kan gi forskrift om informasjonstilgang for Politiets sikkerhetstjeneste.

§ 8-13 *Begrunnelse og underretning*

Forvaltningsloven kapittel IV og V gjelder ikke for avgjørelser om klarering eller autorisasjon.

Den som har vært vurdert klarert, har rett til å bli gjort kjent med resultatet. Ved negativ avgjørelse skal vedkommende uoppfordret underrettes om resultatet og opplyses om klageadgangen.

Begrunnelse for en avgjørelse skal gis samtidig med underretningen om utfallet av klareringssaken. Vedkommende har ikke krav på begrunnelse dersom den ikke kan gis uten å røpe opplysninger som

a) er av betydning for grunnleggende nasjonale funksjoner, jf. § 5-1
b) er av betydning for kildevern
c) det av hensyn til vedkommendes helse eller dennes forhold til personer som står denne nær, må anses utilrådelig at vedkommende får kjennskap til
d) angår tekniske innretninger, produksjonsmetoder, forretningsmessige analyser og beregninger og forretningshemmeligheter ellers, når de er av en slik art at andre kan utnytte dem i sin næringsvirksomhet.

Klareringsmyndigheten skal i tillegg utarbeide en intern samtidig begrunnelse hvor alle relevante forhold inngår, herunder forhold som nevnt i tredje ledd.

§ 8-14 *Innsyn*

Etter at avgjørelse om klarering er fattet, har den som har vært vurdert klarert rett til å gjøre seg kjent med sakens dokumenter.

Vedkommende har ikke krav på innsyn i de deler av et dokument som inneholder opplysninger som nevnt i § 8-13 tredje ledd. Vedkommende har heller ikke krav på innsyn i et dokument som er utarbeidet for den interne saksforberedelsen ved klareringsmyndigheten eller klageinstansen, med unntak av faktiske opplysninger eller sammendrag eller annen bearbeidelse av faktum.

Den som har krav på innsyn skal på anmodning gis kopi av dokumentet.

§ 8-15 *Oversendelse av sak til særskilt oppnevnt advokat*

Departementet oppnevner en gruppe advokater som skal sikkerhetsklareres for høyeste nivå, og som skal gi råd i samsvar denne bestemmelsen.

Dersom begrunnelse ikke gis, jf. § 8-13 tredje ledd, eller avslag er gitt på begjæring om innsyn, jf. § 8-14 andre ledd første punktum, og den som har vært gjenstand for vurdering begjærer det, skal klareringsmyndigheten gjøre sakens dokumenter tilgjengelig for en advokat som nevnt i første ledd. Før retten til advokat inntrer må vedkommende ha benyttet retten til klage på nektet begrunnelse eller avslag på begjæring om innsyn, jf. § 8-16. Advokaten gir råd til personen som er vurdert klarert om hvorvidt personen bør klage.

Advokaten skal ha tilgang til faktiske opplysninger og begrunnelser i saken, herunder begrunnelser som er ukjente for den som har vært vurdert klarert. Dokument som er utarbeidet for den interne saksforberedelsen ved klareringsmyndigheten eller klageinstansen, jf. § 8-14 andre ledd siste punktum, skal ikke gis advokaten.

§ 8-16 *Klage*

Forvaltningsloven kapittel VI gjelder tilsvarende i klareringssaker om ikke annet følger av denne lov eller forskrift om personellsikkerhet.

Negativ avgjørelse om klarering, herunder om vilkår og om når klareringssaken tidligst kan tas opp på nytt, kan påklages av den avgjørelsen retter seg mot. Det samme gjelder nektet begrunnelse og avslag på begjæring om innsyn.

Klagen sendes vedkommende klareringsmyndighet. Sikkerhetsmyndigheten er klageinstans. Departementet er klageinstans for klareringsavgjørelser truffet av Sikkerhetsmyndigheten i første instans.

Fristen for å klage er tre uker fra den dag underretningen om avgjørelsen, nektet begrunnelse eller avslag på begjæring om innsyn har kommet frem til vedkommende. Dersom det klages på nektet begrunnelse eller avslag på begjæring om innsyn, avbrytes klagefristen. Ny klagefrist løper fra det tidspunkt underretning om begrunnelse eller innsyn er kommet frem eller vedkommende på annen måte er gjort kjent med den. I saker der advokat har gjennomgått saken etter § 8-15, løper ny klagefrist fra den dag rådet fra advokaten har kommet frem til vedkommende.

§ 8-17 *Utfyllende bestemmelser*

Kongen kan gi forskrift om opprettelse av et sentralt register for klareringsavgjørelser.

Kongen kan gi forskrift om personellsikkerhet, herunder om

a) klarering av bestemte kategorier personell, bl.a. vernepliktige mannskaper i Forsvaret
b) arkivering, oppbevaring og forsendelse av dokumenter i klarerings- og personkontrollsaker
c) avholdelse av sikkerhetssamtaler.

Kapittel 9. Sikkerhetsgraderte anskaffelser mv.

§ 9-1 *Sikkerhetsgradert anskaffelse*

Med sikkerhetsgradert anskaffelse menes en anskaffelse som innebærer at leverandøren av varen eller tjenesten vil kunne få tilgang til sikkerhetsgradert informasjon, jf. § 5-1, eller til et skjermingsverdig objekt eller infrastruktur, jf. § 7-1.

§ 9-2 *Inngåelse av sikkerhetsavtale*

Ved sikkerhetsgraderte anskaffelser skal det inngås en sikkerhetsavtale mellom anskaffelsesmyndigheten og leverandøren. Sikkerhetsavtale skal være inngått før leverandøren kan få tilgang til gradert informasjon eller et skjermingsverdig objekt eller infrastruktur. Sikkerhetsavtale med utenlandske leverandører kan bare inngås etter godkjenning av Sikkerhetsmyndigheten.

Sikkerhetsavtalen skal fastsette nærmere regler om ansvar og plikter etter bestemmelsene i og i medhold av loven her, herunder om

a) anskaffelsens sikkerhetsgrad, jf. §§ 5-1 og 7-2, spesifisert for de enkelte deler av oppdraget
b) undersøkelser hos leverandøren og annen kontroll med denne for å vurdere sikkerhetstilstanden og om leverandøren overholder sikkerhetsbestemmelsene og øvrige plikter etter loven
c) konsekvenser ved brudd på sikkerhetsavtalen.

Utgifter eller krav leverandøren måtte ha for å oppfylle bestemmelsene i eller i medhold av loven her og inngått sikkerhetsavtale, er anskaffelsesmyndigheten og Sikkerhetsmyndigheten uvedkommende, med mindre annet er uttrykkelig avtalt i sikkerhetsavtalen.

§ 9-3 *Leverandørklarering*

Før en leverandør kan få tilgang til sikkerhetsgradert informasjon gradert KONFIDENSIELT eller høyere, eller dersom det av andre grunner anses nødvendig, skal leverandøren ha gyldig leverandørklarering for angitt sikkerhetsgrad. Kongen gir forskrift om gyldighetstiden for leverandørklareringer. Sikkerhetsmyndigheten er klareringsmyndighet.

Leverandørklarering skal bare gis dersom det ikke foreligger rimelig tvil om leverandørens sikkerhetsmessige skikkethet. I vurderingen skal det bare legges vekt på forhold som er relevante for leverandørens evne og vilje til å utøve forebyggende sikkerhetstjeneste etter bestemmelsene i eller i medhold av loven. I vurderingen skal inngå personkontroll av personer i leverandørens styre og ledelse.

Leverandøren skal gi alle opplysninger som antas å kunne være av betydning for klareringsspørsmålet.

Leverandøren skal uten ugrunnet opphold orientere Sikkerhetsmyndigheten om endringer i styre eller ledelse, forandringer i eierstrukturen, flytting av lokaliteter og utstyr, åpning av gjeldsforhandling eller begjæring om konkurs og andre forhold som kan ha betydning for leverandørens sikkerhetsmessige skikkethet. Anses slike forhold å representere en sikkerhetsrisiko og risikoen ikke kan elimineres gjennom forebyggende sikkerhetstiltak, kan Sikkerhetsmyndigheten inndra leverandørklareringen. Sikkerhetsgradert informasjon eller skjermingsverdig objekt eller infrastruktur kan ikke overføres til ny eier eller inngå i bobehandling ved gjeldsforhandling eller konkurs, med mindre Sikkerhetsmyndigheten har samtykket til dette.

For øvrig gjelder reglene i kapittel 8, herunder reglene om begrunnelse og klage, så langt de passer.

§ 9-4 *Varslingsplikt og myndighet til å fatte vedtak ved anskaffelser til skjermingsverdig objekt og infrastruktur*

Ved anskaffelser til skjermingsverdig objekt eller infrastruktur skal virksomheten foreta en risikovurdering. Det skal tas stilling til om anskaffelsen medfører en ikke ubetydelig risiko for at tilsiktede uønskede hendelser kan inntreffe mot eller ved bruk av objektet eller infrastrukturen. Plikten til å foreta en risikovurdering gjelder ikke dersom det framstår som åpenbart at anskaffelsen ikke kan innebære slik risiko.

Virksomheten skal varsle ansvarlig departement dersom risikovurderingen konkluderer med at anskaffelsen innebærer en risiko som nevnt i første ledd. Virksomheter som ikke er underlagt noe departement, skal varsle Sikkerhetsmyndigheten. Varslingsplikten gjelder uten hinder av taushetsplikt. Plikten gjelder ikke dersom virksomheten selv iverksetter risikoreduserende tiltak som fjerner risikoen eller gjør den ubetydelig.

Et departement som mottar varsel etter andre ledd, bør innhente en rådgivende uttalelse fra relevante organer om anskaffelsens risikopotensiale og leverandørens sikkerhetsmessige pålitelighet.

Dersom en anskaffelse til skjermingsverdig objekt eller infrastruktur kan medføre en ikke ubetydelig risiko for at tilsiktede uønskede hendelser inntreffer, kan Kongen i statsråd fatte enkeltvedtak om at anskaffelsen nektes gjennomført, eller om at det settes vilkår for gjennomføringen. Dette gjelder også dersom det allerede er

inngått avtale om anskaffelsen. Dersom det ikke fattes vedtak etter første punktum, skal departementet underrette virksomheten om dette. Vedtak etter første punktum er særlig tvangsgrunnlag etter tvangsfullbyrdelsesloven kapittel 13.

Kongen i statsråd kan gi forskrift om varslingsplikt og myndighet til å fatte vedtak.

§ 9-5 *Utfyllende bestemmelser mv.*

Kongen kan gi forskrift om sikkerhetsgraderte anskaffelser, samt fastsette særskilte regler for gjennomføring av internasjonale sikkerhetsgraderte anskaffelser.

Kapittel 10. Eierskapskontroll

§ 10-1 *Eierskapskontroll*

Utenlandske rettssubjekter som ønsker å erverve eierandel i en virksomhet som er av kritisk betydning for grunnleggende nasjonale funksjoner som nevnt i § 1-2, skal sende melding til ansvarlig departement om dette. For virksomheter som ikke ligger innenfor et departements myndighetsområde, skal melding sendes til Sikkerhetsmyndigheten. Meldeplikten gjelder når ervervet direkte eller indirekte samlet gjør at erververen oppnår

a) minst en tredjedel av aksjekapitalen, andelene eller stemmene i virksomheten
b) rett til å bli eier av minst en tredjedel av aksjekapitalen eller andelene når dette må anses som reelt aksjeeie eller andelseie
c) betydelig innflytelse over forvaltningen av selskapet på annen måte.

Likt med aksjeeierens egne aksjer regnes de aksjer som eies eller overtas av aksjeeierens nærstående, jf. verdipapirhandelloven § 2-5. Det samme gjelder for andeler som eies eller overtas av andelseierens nærstående.

Et departement som mottar melding etter første ledd, bør innhente en rådgivende uttalelse fra relevante organer om ervervets risikopotensiale og erververens sikkerhetsmessige pålitelighet.

Dersom et erverv som nevnt i første ledd kan medføre en ikke ubetydelig risiko for skade på grunnleggende nasjonale funksjoner, kan Kongen i statsråd fatte enkeltvedtak om at ervervet nektes gjennomført, eller om at det settes vilkår for gjennomføringen. Dette gjelder også dersom det allerede er inngått avtale om ervervet. Dersom det ikke fattes vedtak etter første punktum, skal departementet underrette erververen om dette. Vedtak etter første punktum er særlig tvangsgrunnlag etter tvangsfullbyrdelsesloven kapittel 13.

Kongen kan gi forskrift om erverv av virksomheter omfattet av loven.

Kapittel 11. Kontroll- og tilsynsordninger. Tvangsmulkt, overtredelsesgebyr og straff

§ 11-1 *Kontroll- og tilsynsordninger*

Forebyggende sikkerhetsarbeid i medhold av loven er underlagt kontroll og tilsyn av Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste, i samsvar med bestemmelsene i og i medhold EOS-kontrolloven.

Kongen kan i tillegg etablere særskilte ordninger for å kontrollere og føre tilsyn med Sikkerhetsmyndigheten og andre virksomheters arbeid med forebyggende sikkerhet, i den hensikt å påse at utøvelsen holdes innen rammen av gjeldende lov, administrative eller militære direktiver og ulovfestet rett, eller for å sørge for at rettssikkerhetsmessige og andre hensyn ivaretas.

§ 11-2 *Tvangsmulkt*

Ved overtredelse av bestemmelser gitt i eller i medhold av denne loven, kan tilsynsmyndigheten fastsettes en tvangsmulkt som løper inntil forholdet er brakt i orden. Det samme gjelder for pålegg gitt i medhold av § 3-6.

Vedtak etter første ledd er særlig tvangsgrunnlag etter tvangsfullbyrdelsesloven kapittel 13.

Kongen kan gi forskrift om tvangsmulkt etter loven.

§ 11-3 *Overtredelsesgebyr*

Tilsynsmyndigheten kan pålegge en virksomhet overtredelsesgebyr dersom virksomheten eller noen som handler på dennes vegne, forsettlig eller uaktsomt:

a) overtrer bestemmelser gitt i eller i medhold av §§ 3-4, 4-1, 4-4, 4-6, 5-2, 6-2, 6-3, 7-3, 9-2 første ledd, 9-4 første ledd første og andre punktum eller 9-4 andre ledd første eller andre punktum
b) overtrer pålegg gitt med hjemmel i § 3-6
c) gir uriktige eller ufullstendige opplysninger til tilsynsmyndigheten
d) medvirker til overtredelser som nevnt i bokstav a til c.

Ved fastsettelse av overtredelsesgebyrets størrelse skal det særlig legges vekt på overtredelsens grovhet, overtredelsens varighet, utvist skyld og virksomhetens omsetning. Vedtak om overtredelsesgebyr er særlig tvangsgrunnlag etter tvangsfullbyrdelsesloven kapittel 13.

Adgangen til å pålegge overtredelsesgebyr foreldes etter fem år. Fristen avbrytes når tilsynsmyndigheten meddeler virksomheten at denne er

mistenkt for overtredelse av loven eller vedtak fastsatt med hjemmel i loven.

Kongen kan gi forskrift om overtredelsesgebyr.

§ 11-4 *Straff*

Den som forsettlig eller uaktsomt overtrer bestemmelser gitt i eller i medhold av §§ 3-4, 4-1, 5-1 første ledd, 5-2, 6-2, 6-3, 7-3, 9-2 første ledd, 9-4 første ledd første og andre punktum eller 9-4 andre ledd første eller andre punktum, eller overtrer pålegg gitt av tilsynsmyndigheten i medhold av § 3-6, straffes med bot eller fengsel inntil 6 måneder, hvis ikke forholdet går inn under en strengere straffebestemmelse.

Den som forsettlig eller grovt uaktsomt krenker taushetsplikt etter § 5-3 andre ledd, straffes med bot eller fengsel inntil 1 år, hvis ikke forholdet går inn under en strengere straffebestemmelse.

Den som overtrer forbud med hjemmel i § 7-5 straffes med bot eller fengsel inntil 1 år, hvis ikke forholdet går inn under en strengere straffebestemmelse.

Forsøk på overtredelser som nevnt i første til tredje ledd straffes på samme måte.

Kapittel 12. Ikrafttredelse og endringer i andre lover

§ 12-1 *Ikrafttredelse*

Loven trer i kraft fra den tid Kongen bestemmer.

§ 12-2 *Opphevelse av lov*

Fra den tid loven trer i kraft, oppheves lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste.

Del V
Vedlegg

Vedlegg 1

Begreper

En rekke begreper er sentrale i utvalgets arbeid. Nedenfor er en ikke uttømmende liste over sentrale begreper med tilhørende forklaringer. De fleste forklaringene er ikke ment som entydige definisjoner, men snarere en utdypning av hvilken forståelse utvalget har lagt til grunn i sitt arbeid.

Beredskap	Forberedt evne til på kort varsel å kunne øke sikkerhetsnivået, håndtere en uønsket hendelse eller tilstand, eller evne til å gjenopprette tilfredsstillende tilstand etter en uønsket hendelse. Beredskap forebygger ikke at en uønsket hendelse finner sted, men er en forberedelse til hendelses- og krisehåndtering.
Forebyggende sikkerhet	Tiltak som skal hindre at tilsiktete uønskede hendelser inntreffer, eller som skal redusere konsekvensene av slike dersom de inntreffer.
Grunnleggende nasjonale funksjoner	En funksjon er å anse som grunnleggende for Norge dersom bortfall av denne får konsekvenser som truer statens sikkerhetspolitiske ansvar for å ivareta Norges suverenitet, territorielle integritet og demokratiske styreform. Grunnleggende nasjonale funksjoner er knyttet til: a) de øverste statsorganers virksomhet, sikkerhet eller handlefrihet b) forsvars-, sikkerhets- og beredskapsmessige forhold c) forholdet til andre stater d) landets økonomiske trygghet og velferd e) befolkningens grunnleggende sikkerhet og overlevelse.
Hybrid krigføring	Kombinasjonen av fordekte forsøk på destabilisering ved bruk av indirekte og ikke-militære verktøy sammen med konvensjonell krigføring.
Informasjonssystem	System som anvendes for å løse en oppgave eller utføre en funksjon i en organisasjon. Det omfatter menneskelige, organisatoriske og tekniske ressurser, metoder og teknikker. Informasjonssystem omfatter både manuelle og digitale informasjonssystemer, og favner alt fra saksbehandlingssystemer, kontorstøttesystemer og rene kommunikasjonssystemer til kontroll- og styringssystemer.
Kritisk infrastruktur	Anlegg og systemer som er nødvendige for å opprettholde samfunnets grunnleggende behov og funksjoner.
Kritiske samfunnsfunksjoner	En samfunnsfunksjon defineres som kritisk hvis bortfall av den truer samfunnets og befolkningens grunnleggende behov. De grunnleggende behovene er definert som mat, vann, varme, trygghet og lignende.
Risiko	Er et produkt av sannsynligheten for at en hendelse inntreffer og konsekvensen dersom den inntreffer. Det vil være usikkerhet knyttet til både sannsynligheten og vurderingen av mulig konsekvens.

Sabotasje	Tilsiktet ødeleggelse, lammelse eller driftsstopp av utstyr, materiell, anlegg, eller funksjon, utført av eller for en fremmed stat, organisasjon, gruppering eller enkeltperson.
Samfunnssikkerhet	Vern av samfunnet mot hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare. Slike hendelser kan være utløst av naturen, være et utslag av tekniske eller menneskelige feil eller av bevisste handlinger.
Skjermingsverdig infrastruktur	Anlegg og systemer som må beskyttes mot tilsiktede uønskede hendelser av hensyn til opprettholdelse av grunnleggende nasjonale funksjoner.
Skjermingsverdig objekt	Eiendom som må beskyttes mot tilsiktede uønskede hendelser av hensyn til opprettholdelse av grunnleggende nasjonale funksjoner.
Spionasje	Innsamling av informasjon ved hjelp av fordekte midler i etterretningsmessig hensikt.
Terrorhandling	Ulovlig bruk av, eller trussel om bruk av, makt eller vold mot personer og eiendom, i et forsøk på å legge press på landets myndigheter eller befolkning eller samfunnet for øvrig for å oppnå politiske, religiøse eller ideologiske mål.
Tilsiktede uønskede hendelser	En hendelse forårsaket av en aktør med intensjon om å påføre en eller annen form for skade. I praksis betyr dette at den eller de som utfører eller planlegger å utføre handlingen vil kunne tilpasse handlingen til de sikkerhets- og beredskapstiltak som de har kjennskap til, eller som de forventer skal finnes.
Trussel	En mulig tilsiktet uønsket hendelse som kan gi en negativ konsekvens for den som rammes.

Vedlegg 2

Utvalgets møter

Sikkerhetsutvalget har hatt jevnlige arbeidsmøter. Møtene har dels bestått av orienteringer fra eksterne, interne diskusjoner og bearbeidelse av tekst til utredningen.

I forbindelse med behandlingen av noen utvalgte tema har utvalget nedsatt arbeidsgrupper, bestående av medlemmer av utvalget med støtte fra sekretariatet. Arbeidsgruppene har rapportert til utvalget.

Utvalget har også gjennomført et åpent arrangement for å belyse problemstillinger relatert til «sikkerhet og personvern i den digitale tidsalder». Det var stor interesse for arrangementet og omtrent 180 deltagere møtte opp.

Sikkerhetsutvalgets arbeidsmøter

- 20. april 2015
- 21. mai 2015
- 22. juni 2015
- 28. august 2015
- 1. oktober 2015
- 28. og 29. oktober 2015 (i forbindelse med studietur til NATO og EU i Brussel)
- 24. og 25. november 2015 (i forbindelse med studietur til Sverige og Danmark)
- 16. desember 2015
- 13. januar 2016
- 8. og 9. februar 2016 (i forbindelse med studietur til London)
- 15. mars 2016
- 13. april 2016
- 11. mai 2016
- 7. og 8. juni 2016
- 20. og 21. juni 2016
- 15. og 16. august 2016
- 29. og 30. august 2016
- 12. og 13. september 2016
- 21. september 2016

Møter i arbeidsgrupper nedsatt av utvalget

- 26. april 2016 (Lovstruktur)
- 25. mai 2016 (Objekt- og infrastruktursikkerhet)
- 15. juni 2016 (Samfunnsøkonomi)
- 26. august 2016 (Eierskapskontroll)

Konferanse – Sikkerhet og personvern i den digitale tidsalder

28. april 2016 09:30 – 14:00

Sted: Oslo Militære Samfund

Ordstyrer: Christian Borch

Formålet med konferansen var å skape debatt rundt sentrale tema for utvalgets arbeid, for å ivareta at relevante perspektiver og innspill ble ivaretatt i utvalgets utredningsarbeid. Samfunnets sikkerhet og den enkeltes personvern er grunnleggende verdier i en demokratisk rettsstat. Spørsmål som ble reist på konferansen var hvordan disse verdiene kan beskyttes og ivaretas parallelt? Er det en motsetning mellom å ivareta sikkerhet og individets frihet? Hvor går grensen for hva staten kan foreta seg med nasjonal sikkerhet som begrunnelse?

Konferansens program:

Del 1: Kritiske samfunnsfunksjoner – trusler, sårbarheter og beskyttelsestiltak

Innledere:
- Kjetil Nilsen, direktør Nasjonal sikkerhetsmyndighet
- Per Sanderud, direktør Norges vassdrags- og energidirektorat

Del 2: IKT-sikkerhet og personvern

Innledere:
- Eva Jarbekk, advokat Føyen Torkildsen AS (leder Personvernnemnda)
- Bjørn Erik Thon, direktør Datatilsynet

Paneldebatt: IKT-sikkerhet og personvern

Deltakere:
- Gjermund Hagesæter (Frp), statssekretær i Justis- og beredskapsdepartementet

- Bård Vegar Solhjell (SV), utenriks- og forsvarskomiteen
- Sveinung Rotevatn (V), sentralstyremedlem
- Jorodd Asphjell (A), justiskomiteen
- Anders Werp (H), nestleder av justiskomiteen

Mer informasjon om arrangementet finnes på Sikkerhetsutvalgets hjemmesider: https://nettsteder.regjeringen.no/sikkerhetsutvalget/arrangement/sikkerhet-og-personvern-i-den-digitale-tidsalder/

Vedlegg 3

Utvalgets informasjonsgrunnlag

Til støtte for sitt arbeid har utvalget innhentet informasjon og vurderinger fra et bredt spekter av kilder og aktører. Ved siden av skriftlige kilder har utvalget bedt om innspill på spesifikke tema fra ulike aktører og invitert bredt til å fremsende skriftlige innspill.

Aktører som har holdt orienteringer for utvalget

Norge:

- Datatilsynet
- Det digitale sårbarhetsutvalget (Lysne-utvalget)
- DNB ASA
- Direktoratet for samfunnssikkerhet og beredskap
- EOS-utvalget
- Etterretningstjenesten
- Forsvarets forskningsinstitutt
- Forsvarets logistikkorganisasjon
- Forsvarets sikkerhetsavdeling
- Forsvarsdepartementet
- Forsvarssjefen
- Førsteamanuensis Herbjørn Andresen, Høgskolen i Oslo og Akershus
- Gassco AS
- Justis- og beredskapsdepartementet
- Kongsberg Gruppen ASA
- Nasjonal kommunikasjonsmyndighet
- Nasjonal sikkerhetsmyndighet
- NorCERT (NSM)
- Norges- vassdrags og energidirektorat
- Olje- og energidepartementet
- Telenor Norge AS
- Telia AS
- Politiets sikkerhetstjeneste
- Professor Terje Aven, Universitetet i Stavanger
- Wikborg, Rein & Co, Advokatfirma DA

Sverige:

- Justitiedepartementet
- Myndigheten för samhällsskydd och beredskap
- Säkerhetspolisen

Danmark:

- Beredskabsstyrelsen
- Dr. Manni Crone, Danish Institute for International Studies
- Forsvarets Efterretningstjeneste
- Forsvarsministeriet
- Justisministeriet
- Politiets Efterretningstjeneste

Storbritannia:

- Cabinet Office
- Home Office
- MI-5: Center for the Protection of National Infrastructure (CPNI)
- Members of Home Affairs Select Committee
- Professor Sir David Omand, King's College
- Royal United Services Institute (RUSI)
- Sir David Anderson QC, Independent Reviewer of Terrorism Legislation

EU:

- Ambassadør Oda Sletnes
- Den norske EU-delegasjonen
- European Data Protection Supervisor
- Nederlands EU-delegasjon
- Storbritannias EU-delegasjon
- Terrorism and Crisis Management, DG Home Affairs, Europakommisjonen
- Trust and Security, DG for Communications Networks, Content and Technology (CNECT)

NATO:

- Ambassadør Knut Hauge, Norges faste representant til NATOs råd
- Den norske NATO-delegasjonen
- NATOs seksjon for etterretning, overvåkning og rekognosering (ISR). Divisjonen for forsvarsinvesteringer (DI)
- NATOs seksjon for tilsyn av sikkerhetspolicy (Policy Oversight Branch). NATOs kontor for sikkerhet (NATO Office of Security)

- NATOs seksjon for analyse av strategiske kapabiliter (ESC-SAC). Divisjonen for nye sikkerhetsutfordringer (ESC)
- NATOs seksjon for sivil beredskap, Divisjonen for operasjoner (OPS)
- NATOs seksjon for cyberforsvar. Divisjonen for nye sikkerhetsutfordringer (ESC)

Internasjonale selskaper:

- Apple Corporation, London
- Ernst and Young LLP, London
- Google, Brussels

Sekretariatets møter med relevante aktører

- Direktoratet for samfunnssikkerhet og beredskap
- Direktoratet for økonomistyring
- Forsvarets forskningsinstitutt
- Forsvarets logistikkorganisasjon
- Forsvarsbygg, Nasjonalt kompetansesenter for sikring av bygg
- Forsvarsdepartementet
- Justis- og beredskapsdepartementet
- Nasjonal Sikkerhetsmyndighet
- Politidirektoratet
- Politiets sikkerhetstjeneste
- Utenriksdepartementet

Skriftlige innspill til utvalget

Utvalget har mottatt skriftlige innspill fra følgende aktører:

- Direktoratet for samfunnssikkerhet og beredskap
- Etterretningstjenesten
- Forsvarsbygg
- Forsvarets sikkerhetsavdeling
- Forsvarsdepartementet
- Helse- og omsorgsdepartementet
- Justis- og beredskapsdepartementet
- Klima- og miljødepartementet
- Kongsberg Gruppen ASA
- Landbruks- og matdepartementet
- Landsorganisasjonen
- Nasjonal sikkerhetsmyndighet
- Norges vassdrags- og energidirektorat
- Nærings- og fiskeridepartementet
- Petroleumstilsynet
- Politidirektoratet
- Politiets sikkerhetstjeneste
- Utenriksdepartementet

Konferanser og seminarer

Utvalgsmedlemmer og/eller sekretariatsmedlemmer har deltatt på følgende konferanser og seminarer av relevans for utvalgsarbeidet:

- 16. juni 2015, FFI-forum: Tilnærminger til risikovurderinger for tilsiktede, uønskede handlinger, Forsvarets forskningsinstitutt
- 18. juni 2015, Konferanse om ekstremisme og terrorisme, Norges forskningsråd
- 8. september 2015, Møte i nettverk for samfunnsøkonomisk analyse, Direktoratet for økonomistyring
- 14. oktober 2015, Sårbarhetskonferansen 2015, Norges forsvars forening og Kvinners frivillige beredskap
- 30. november 2015, Pressekonferanse – utredning fra det digitale sårbarhetsutvalget
- 2. desember 2015, Digitale sårbarheter – Internasjonale løsninger, Norsk utenrikspolitisk institutt
- 6. januar 2016, Samfunnssikkerhetskonferansen, Universitetet i Stavanger
- 1. og 2. februar 2016, Samfunnssikkerhetskonferansen 2016, Direktoratet for samfunnssikkerhet og beredskap
- 16. og 17. mars 2016, Sikkerhetskonferansen 2016, Nasjonal sikkerhetsmyndighet
- 30. mars 2016, Nasjonalt beredskapssystem, Forsvarsdepartementet og Justis- og beredskapsdepartementet
- 10. mai 2016, MR-forum, Terror og rettsstaten, Norsk senter for menneskerettigheter

Vedlegg 4

Utvalgets referansegruppe

Til støtte for sitt arbeid har Sikkerhetsutvalget etablert en referansegruppe bestående av et representativt utvalg av berørte aktører.

Referansegruppen har vært et konsultativt organ og en arena for toveis kommunikasjon. Sikkerhetsutvalget har informert om sitt arbeid, og referansegruppens medlemmer har fremmet synspunkter og kommet med innspill i forbindelse med behandlingen av aktuelle problemstillinger.

Deltakerorganisasjoner til Sikkerhetsutvalgets referansegruppe

Referansegruppen har bestått av følgende instanser:

- Datatilsynet
- Direktorat for samfunnssikkerhet og beredskap
- Etterretningstjenesten
- Finanstilsynet
- Forsvarsstaben
- Helsedirektoratet
- Kommunenes sentralforbund
- Landsorganisasjonen
- Nasjonal kommunikasjonsmyndighet
- Nasjonal sikkerhetsmyndighet
- Norges vassdrags- og energidirektorat
- Næringslivets hovedorganisasjon
- Petroleumstilsynet
- Politidirektoratet
- Politiets sikkerhetstjeneste

Møter med referansegruppen:

- 6. november 2015
- 11. februar 2016
- 17. juni 2016
- 19. september 2016

Norges offentlige utredninger 2015 og 2016

Statsministeren:

Arbeids- og sosialdepartementet:
NOU 2015: 6 Grunnlaget for inntektsoppgjørene 2015
NOU 2016: 1 Arbeidstidsutvalget
NOU 2016: 6 Grunnlaget for inntektsoppgjørene 2016
NOU 2016: 13 Samvittighetsfrihet i arbeidslivet

Barne-, likestillings- og inkluderingsdepartementet
NOU 2015: 4 Tap av norsk statsborgerskap

Barne- og likestillingsdepartementet
NOU 2016: 16 Ny barnevernslov
NOU 2016: 17 På lik linje

Finansdepartementet:
NOU 2015: 1 Produktivitet – grunnlag for vekst og velferd
NOU 2015: 5 Pensjonslovene og folketrygdreformen IV NOU 2015: 9 Finanspolitikk i en oljeøkonomi
NOU 2015: 10 Lov om regnskapsplikt
NOU 2015: 12 Ny lovgivning om tiltak mot hvitvasking og terrorfinansiering
NOU 2015: 14 Bedre beslutningsgrunnlag, bedre styring
NOU 2015: 15 Sett pris på miljøet
NOU 2016: 2 Endringer i verdipapirhandelloven – flagging og periodisk rapportering
NOU 2016: 3 Ved et vendepunkt: Fra ressursøkonomi til kunnskapsøkonomi
NOU 2016: 5 Omgåelsesregel i skatteretten
NOU 2016: 11 Regnskapslovens bestemmeler om årsberetning mv.
NOU 2016: 15 Lønnsdannelsen i lys av nye økonomiske utviklingstrekk

Forsvarsdepartementet:
NOU 2016: 8 En god alliert – Norge i Afghanistan 2001–2014
NOU 2016: 19 Samhandling for sikkerhet

Helse- og omsorgsdepartementet:
NOU 2015: 11 Med åpne kort
NOU 2015: 17 Først og fremst

Justis- og beredskapsdepartementet:
NOU 2015: 3 Advokaten i samfunnet
NOU 2015: 13 Digital sårbarhet – sikkert samfunn
NOU: 2016: 9 Rettferdig og forutsigbar – voldsskadeerstatning
NOU 2016: 10 Evaluering av garantireglene i bustadoppføringslova

Klima- og miljødepartementet:
NOU 2015: 16 Overvann i byer og tettsteder

Kommunal- og moderniseringsdepartementet:
NOU 2015: 7 Assimilering og motstand
NOU 2016: 4 Ny kommunelov
NOU 2016: 18 Hjertespråket

Kulturdepartementet:
NOU 2016: 12 Ideell opprydding

Kunnskapsdepartementet:
NOU 2015: 2 Å høre til
NOU 2015: 8 Fremtidens skole
NOU 2016: 7 Norge i omstilling – karriereveiledning for individ og samfunn
NOU 2016: 14 Mer å hente

Landbruks- og matdepartementet:

Nærings- og fiskeridepartementet:

Olje- og energidepartementet:

Samferdselsdepartementet:

Utenriksdepartementet:
NOU 2016: 8 En god alliert – Norge i Afghanistan 2001–2014

Bestilling av publikasjoner

Offentlige institusjoner:
Departementenes sikkerhets- og serviceorganisasjon
Internett: www.publikasjoner.dep.no
E-post: publikasjonsbestilling@dss.dep.no
Telefon: 22 24 00 00

Privat sektor:
Internett: www.fagbokforlaget.no/offpub
E-post: offpub@fagbokforlaget.no
Telefon: 55 38 66 00

Publikasjonene er også tilgjengelige på
www.regjeringen.no

Trykk: 07 PrintMedia – 10/2016