FORSVARSDEPARTEMENTET

HØRINGSNOTAT

FORSLAG TIL NY LOV OM BESKYTTELSE AV NORSK FORSVARSTEKNOLOGI OG SIKKERHETSGRADERTE PATENTER

4. Januar 2023

Innhold

1 Hovedinnholdet i høringsnotatet

Verden er inne i «Den fjerde industrielle revolusjon» hvor teknologiutviklingen skjer raskere og på flere områder enn da lov om forsvarsviktige oppfinnelser[1] trådte i kraft for over 60 år siden. Sentrale kjennetegn ved utviklingen er vekst i omfanget og bruken av data, digitalisering, automatisering, utvikling av kunstig intelligens, autonomi, og kvanteberegning. Utviklingen påvirker alle sider ved Forsvarets virksomhet. Den har stor innflytelse på moderne våpen, informasjons- og overvåkningssystemer og andre militære kapasiteter, og fører til at vi står overfor den syvende generasjon militære revolusjon.[2] Utviklingen gir store muligheter, men innebærer også flere sårbarheter for Norges evne til å ivareta Forsvarets operative evne.

For å reduserer sårbarhetene, og legge til rett for tilstrekkelig nasjonal kontroll med sentrale innsatsfaktorer for Forsvaret, foreslår Forsvarsdepartementet en ny lov om beskyttelsesverdig forsvarsteknologi og sikkerhetsgraderte patenter. Lovforslaget bygger videre på gjeldende lov om forsvarsviktige oppfinnelser, men vil også kunne omfatte varer, tjenester og teknologi som kan brukes til forsvarsformål, uavhengig av utviklingsnivået til teknologien og uavhengig av om teknologien allerede er tilgjengelig på markedet.

For at teknologien skal omfattes av lovforslaget må det fattes vedtak om at den har vesentlig betydning for Forsvarets operative evne, og derfor er beskyttelsesverdig. Lovforslaget innebærer en ny metode for å kartlegge denne teknologien basert på en konkret helhetsvurdering. Sentrale momenter i vurderingen er hvilke konsekvenser tap av teknologien vil ha for operativ evne, om den er tilpasset norske forhold, om den gir forsvarspolitiske fordeler for Norge, om den er allment tilgjengelig på markedet og hvor stor betydning teknologien har for beskyttelse av sensitiv informasjon.

Et vedtak om at en teknologi er beskyttelsesverdig innebærer bl.a. at det kreves tillatelse fra departementet før teknologien kan deles, uavhengig av hvordan den deles, og om den deles innenfor eller utenfor norsk jurisdiksjon. Sentrale momenter i vurderingen av om det kan gis tillatelse er hvor stor risiko for tap av teknologien det er med delingen, hvilke konsekvenser vil et tap av teknologien få for operativ evne, holdt opp mot hvilke fordeler deling vil ha for Forsvarets operative evne og for Norges forsvarssamarbeid med andre stater.

Departementet vil i tillegg kunne pålegge eller forby bruk, utvikling eller produksjon av teknologien dersom det nødvendig å legge føringer for å ivareta Forsvarets operative evne. Dette vil eksempelvis være aktuelt der teknologien utvikles på en måte som reduserer Forsvarets operative evne, eller at det er en risiko for at den gjøres tilgjengelig for aktører som gjør teknologien mindre tilgjengelig for Forsvaret i en eventuell fremtidig konflikt. For å sikre at teknologien er tilstrekkelig tilgjengelig for Forsvaret kan det også være aktuelt å stille krav om at kompetanse på teknologien er tilgjengelig, og produksjon av den skjer, innenfor norsk jurisdiksjon.

Kongen vil også kunne ekspropriere og sikre seg rett til å utnytte en beskyttelsesverdig forsvarsteknologi, dersom krav om tillatelse, eller et pålegg eller forbud ikke gir tilstrekkelig kontroll med eller tilgang til teknologien. Eksempelvis der aktøren legger ned virksomheten

[1] Lov 26. juni 1953 nr. 8 om oppfinnelser av betydning for rikets forsvar, jf. Ot.prp. nr. 62 (1952) og Innst. O. VII (1953). Ikrafttredelse 1. januar 1956.

[2] Science & Technology Trends 2020-2014 – Exploring the S&T Edge, *NATO Science & Technology Organization (2020)*, side 7.

eller planlegger å flytte produksjonen helt ut av landet. Departementet legger opp til at et vedtak om ekspropriasjon eller rett til utnyttelse vil kunne gi rett til erstatning, mens rett til erstatning for øvrige vedtak vil avhenge av en konkret helhetsvurdering der utgangspunkt vil være at det ikke er en rett til erstatning.

Formålet med lovforslaget er å legge til rette for at forsvarssektoren har tilstrekkelig nasjonal kontroll med og tilgang til teknologi som har vesentlig betydning for Forsvarets operative evne, samtidig som industriaktørene skal fortsette å utvikle fremtidsrettede løsninger på dagens og fremtidens utfordringer. Det legges opp til at aktørene gjennom praktiseringen av regelverket så langt som mulig skal få eksportert produkter, og dratt nytte av samarbeidsmuligheter i det internasjonale markedet, på samme måte som i dag.

De gjeldende reglene om hemmelige patenter foreslås i all hovedsak videreført, herunder reglene om håndtering av hemmelige patenter og unntak fra kravene i patentloven til offentliggjøring og betaling av årsavgift, men med oppdateringer for å reflektere forpliktelsene etter de internasjonale patentkonvensjonene og kravene i sikkerhetsloven.

2 Bakgrunnen for lovforslaget

Lov 26. juni 1953 nr. 8 om oppfinnelser av betydning for rikets forsvar (lov om forsvarsviktige oppfinnelser) ble gitt for å sikre det offentlige hjemmel til enhver forføyning som er nødvendig for at en oppfinnelse av betydning for rikets sikkerhet skal komme rikets forsvar mest mulig til nytte. Lovens bestemmelser var i stor utstrekning nye i forhold til tidligere lovgivning, jf. Ot.prp. nr. 62 (1952) og Innst. O. VII (1953)[3], men har nå behov for oppdatering av både språk og lovgivningsteknikk for å bli mer tilgjengelig for brukerne, og for å tilpasses den teknologiske utviklingen.

Den teknologiske utviklingen gjør at moderne våpensystemer og militære kapasiteter i større grad er høyteknologiske, og består av et vidt spekter av materialer og enkeltkomponenter. Digitale komponenter kan relativt enkelt omprogrammeres og justeres slik at funksjonen endres. Både materialene, enkeltkomponentene og hele systemer er i større grad bare tilgjengelig hos private aktører, i motsetning til tidligere da utviklingen skjedd innenfor forsvarssektoren. Det er i stor grad sivil- og forsvarsindustrien som har rettighetene til og utvikler ny teknologi, sammen med militære og sivile forskningsmiljøer.[4] Denne utviklingen gjør at forsvarssektoren har tilgang til moderne teknologi av høy kvalitet, men den utgjør også en sårbarhet for sektoren. Når sentrale innsatsfaktorer er, og fremover i større grad vil være hos private aktører, har forsvarssektoren mindre kontroll med og tilgang til kapasiteter som er nødvendige for å ivareta Forsvarets operativ evne.

Samtidig skjer det en voldsom teknologisk utvikling på allerede etablerte og nye teknologiområder. NATO har klassifisert noen områder som «emerging, disruptive and covergent» (EDT), bl.a. stordata, kunstig intelligens, autonomi, kvanteteknologi. Alle disse vil potensielt få stor betydning for utviklingen av fremtidens militære kapasiteter, men hvordan er fremdeles uklart. Det er derfor viktig med et lovgrunnlag som gir muligheter til å føre kontroll

[3] Loven er senere endret som følge av endringer i andre lover ved lov 15. desember 1967 nr. 9 om patenter, ved lov 24. mai 1985 nr. 30, ved lov 22. desember 1995 nr. 82 om endringer i lovgivningen om industrielt rettsvern, ved lov 14. desember 2001 nr. 98 og ved lov 22. juni 2012 nr. 58.

[4] Se kapitel 5.2 og 5.3 for beskrivelse av den teknologiske utviklingen, og om forholdet mellom teknologi utviklet i og utenfor forsvarssektoren.

med den videre utvikling av disse kapasitetene, men også for videreutviklingen av allerede etablerte teknologiområder.

Norsk forsvarsindustri har i dag en betydelig eksport av en rekke teknologisk avanserte militære produkter. I 2020 ble det eksportert forsvarsmateriell og flerbruksvarer for militær sluttbruk til en verdi på ca. 6,7 milliarder kroner.[5] Både forsvarsindustrien og sivil industri er avhengig av tilgang til det internasjonale marked for å kunne forbedre eksisterende og utvikle nye produkter, ettersom hjemmemarkedet ofte er for lite til å drive kostnadskrevende utviklingsarbeid. Det er også helt avgjørende å delta i nasjonalt og internasjonalt forsknings- og utviklingssamarbeid for å finne løsninger på dagens og fremtidens utfordringer. Eksport, og deltakelse i internasjonale forsknings- og utviklingsprosjekter, er dessuten en sentral del av forsvarssamarbeidet mellom Norge og andre stater.

Samlet er det derfor et behov for et lovgrunnlag som legger til rette for prosesser som sikrer industriaktørene tilgang til eksportmarkeder og forskningsmiljøer innenfor og utenfor norsk jurisdiksjon, samtidig som det legges til rette for tilstrekkelig kontroll med og tilgang til teknologi som har vesentlig betydning for operativ evne. Eksport og deltakelse i internasjonale forskningsmiljøer styrker forsvarssamarbeidet mellom Norge og andre stater, samtidig som deling utgjør en risiko for tap av teknologien eller informasjon om teknologien. Tap av teknologien utgjør igjen en risiko for tap av operativ evne og at norsk industri mister konkurransefortrinn i det internasjonale markedet.

Det er også et behov for å oppdatere lovens bestemmelser om hemmelige patenter slik at loven er i tråd med utviklingen som har skjedd innenfor patentretten siden loven trådte i kraft. Særlig gjelder dette behovet for en klargjøring av forholdet mellom lovens regler og gjeldende internasjonale patentkonvensjoner på området som Norge er bundet av, herunder forholdet til Den europeiske patentkonvensjonen (EPC) og Patentsamarbeidskonvensjonen (PCT). Det er også et behov for å gjennomgå forholdet til sikkerhetsloven, som er ny siden gjeldende lov trådte i kraft.

3 Rettstilstanden i andre land

3.1 Sverige

Lag 17. desember 1971 om försvarsuppfinningar er Sveriges lov om forsvarsviktige oppfinnelser og inneholder i all hovedsak de samme bestemmelsene som den norske loven. Loven ble sist endret i 2016 og omfatter patenterte oppfinnelser og definerte forsvarsoppfinnelser som det ikke er søkt patent om.

Det følger av § 1 at det med «försvarsoppfinningar» menes «uppfinning som särskilt avser krigsmateriel», men at det er regjeringen som gjennom forskrift er delegert myndighet til å angi hva som «avses med krigsmateriel».

I förordning (1988:563) om vad om avses med krigsmateriel i lagen (1971:1078) om försvarsuppfinningar, anses følgende som «krigsmateriel»:

1) «varor som är upptagna i bilagan till förordningen (1992:1303) om krigsmateriel,
2) övrig för militärt bruk utformad materiel till skydd mot verkan av stridsmedel,

[5] Meld. St. 35 (2020-2021) Eksport av forsvarsmateriell fra Norge i 2020, eksportkontroll og internasjonalt ikke-spredningssamarbeid, s. 9.

3) övrig för militärt bruk utformad materiel till skydd mot spaning eller andra iakttagelser».

Loven har regler for svenske oppfinnelser i §§ 4-14. Svenske oppfinnelser er i § 4 definert som forsvarsoppfinnelser som har «tilkommet i Sverige eller tilhör en här bosatt fysisk person eller tilhör en svensk juridisk person».

Loven § 4 fastslår at svenske forsvarsoppfinnelser skal gi et rettslig grunnlag for å kunne beskytte («hållas hemlig») oppfinnelser som er innenfor begrepet «försvarsuppfinning». Dette presiseres i § 4 hvor en «försvarsuppfinning» ikke kan offentliggjøres før dette er vurdert. Det er Försvarets materiellverk (FMV) (tilsvarende Forsvarsmateriell) som på vegne av den svenske regjeringen utfører vurderingene på oppfinnelsene. Det er for svenske oppfinnelser gitt en tre måneders frist til FMV for å informere om hemmelighold, jf. § 7. Dersom fristen ikke overholdes vil ikke oppfinnelser være omfattet av hemmelighold.

Det stilles ingen krav i loven om at oppfinnere og selskaper som produserer forsvarsmateriell eller tilsvarende, selv skal ta kontakt og få vurdert oppfinnelsen. De oppfinnelser som blir grunnlag for prøvingen må da komme via Patent- och registreringsverket (§ 5), eller være kjent av FMV fra før.

I lovens §§ 5 til 7 angis regler for hvordan beslutninger om hemmelighold og tillatelse til offentliggjøring skal saksbehandles. I tillegg til FMV som saksbehandler oppfinnelsene, har regjeringen nedsatt en granskningsnemd som tar endelig beslutning om hemmelighold eller offentliggjøring ved klager.

Lovens § 8 angir at granskningsnemden skal vurdere hvert år om hemmelighold skal videreføres. I tillegg kan hemmelighold vurderes opphevet ved søknad eller andre forhold.

Lovens § 11 gir en oppfinner adgang til å søke at staten overtar en oppfinnelse om den holdes hemmelig. Staten har da fire måneder på å overta oppfinnelsen ellers opphører beslutning om hemmelighold.

Lovens § 13 åpner for at regjeringen kan beslutte at en oppfinnelse av vesentlig betydning for Forsvaret skal utnyttes for statens regning eller av en annen som regjeringen bestemmer. Regjeringen kan også beslutte at all rett til oppfinnelsen skal avgis til staten (ekspropriasjon).

I denne forbindelse gir loven § 14 rett til erstatning ved at en oppfinnelse holdes hemmelig. Det gis også rett til erstatning dersom regjeringen beslutter at oppfinnelsen skal avgis til staten.

Loven har straffebestemmelser i §§ 21 og 22. Paragraf 21 åpner for straffesanksjoner ved brudd på lovens § 10 dersom noen lar fremmede stater få informasjon om oppfinnelser uten tillatelse av regjeringen. Straffen er bøter eller fengsel inntil ett år. Paragraf 22 fastslår erstatningsplikt for den som ulovlig utnytter en forsvarsoppfinnelse og hvor vedkommende skal betale erstatning for bruken samt eventuelle skader det har medført.

3.2 Danmark

Lov om hemmelige patenter er Danmarks lov om forsvarsviktige oppfinnelser. Det følger av § 1 at loven gjelder oppfinnelser som angår «krigsmateriel eller fremgangsmåder til fremstilling af krigsmateriel». Videre skal regjeringen ved kgl. anordning utdype ytterligere hva som menes med krigsmateriell. Dette er gitt i Anordning nr. 21 af 30. januar 1960. Definisjonen av krigsmateriell er bred og omhandler foruten kampmidler også materiell til beskyttelse og bekjempning av kampmidler.

Loven er utarbeidet på bakgrunn av NATO-avtalen om oppfinnelser (signert 21. september 1960) og loven ble vedtatt 27. januar 1960. Den ble sist oppdatert 28. desember 2011.

Loven gir et rettslig grunnlag for å holde oppfinnelser som tilfredsstiller kravene i lov og anordning hemmelig. Det er den danske erhvervs- og vækstministeren som beslutter at et patent skal være hemmelig etter anmodning fra forsvarsministeren, jf. § 2.

Loven § 3 gir myndighetene en tidsfrist på tre måneder på å beslutte hemmelighold fra tidspunktet det søkes patent. Dersom fristen ikke overholdes er ikke oppfinnelsen å anse som hemmelig.

Loven omfatter kun patenterte oppfinnelser og oppfinnelser det søkes patent på. Det stilles ingen krav i loven om at oppfinnere og selskaper som produserer forsvarsmateriell eller tilsvarende, selv skal ta kontakt og få vurdert oppfinnelsen. Det medfører at det må være Patent- og Varemærkestyrelsen som skal informere forsvarsministeren dersom de blir kjent med en oppfinnelse som tilfredsstiller kravene.

Loven har ikke bestemmelser om erstatning dersom en oppfinnelse blir holdt hemmelig. Loven har heller ikke bestemmelser om at oppfinnelsen skal utnyttes for statens regning eller av en annen som regjeringen bestemmer.

Loven har straffebestemmelser § 11. Her gis straff ved offentliggjøring av patentet og dersom det søkes patent i en annen stat dersom hemmelighold er besluttet. Straffen er bøter eller fengsel i inntil ett år.

Det er ikke regulert i loven hvor lenge en oppfinnelse holdes hemmelig eller når den skal vurderes frigitt, men det er i § 8 angitt hva som skal skje når hemmelighold opphører. Her er også Forsvarsministeren gitt rom for å beslutte videre hemmelighold.

3.3 NATO

NATO-avtalen "Agreement for the mutual safeguarding of secrecy of inventions relating to defence and for which applications for patents have been made» ble vedtatt av NATO-rådet 16. juli 1959. Norge og USA ratifiserte avtalen 12. januar 1961 som første nasjoner.

Før avtalen ble etablert hadde flere NATO-land forbud mot eksport av patentert krigsmateriell til utlandet, inkludert NATO allierte. I tillegg var det NATO-land som ikke hadde en lov for hemmelighold av patenter, et av dem var Danmark. Denne avtalen åpner imidlertid for å dele patenter som var sikkerhetsgraderte med andre NATO-land, samt at avtalepartene har en plikt til å beskytte og sikkerhetsgradere patentene på samme måte som opprinnelseslandet.

Avtalen oppstiller krav til hvordan medlemslandene kan dele patenterte oppfinnelser samt krav til beskyttelse av patentene. Avtalen har blitt oppdatert flere ganger, herunder med standardiserte graderingsbetegnelser og regler for deling av sikkerhetsgraderte patenter.

Nærmere regler er også gitt i «Implementing procedures for the NATO Agreement for the mutual safeguarding of secrecy of inventions relating to defence and for which applications for patents have been made». Denne prosedyren angir at sikkerhetsgraderte patenter behandles i mottakerstaten med samme sikkerhetsgradering som opphavslandet og i henhold til mottakerstatens sikkerhetsregelverk. Patentet må sendes fra, eller godkjennes av, en statlig forsvarsetat og må sendes gjennom godkjente og sikre statlige eller diplomatiske kanaler.

3.4 USA

3.4.1 Generelt

The Invention Secrecy Act fra 1951 regulerer hemmelighold av patentsøkte oppfinnelser og teknologi som kan utgjøre en trussel mot nasjonal sikkerhet i USA. Loven omhandler ikke andre forsvarsviktige oppfinnelser eller teknologi. Loven er oppdatert flere ganger.

US Patent and Trademark Office (USPTO) tar beslutningen om hemmelighold på bakgrunn av «Patent Security Category Review List» (PSCRL), som lister sensitive teknologier som faller under loven. PSCRL ble etablert første gang i 1971. Dette er en svært omfattende liste som omfatter ulike våpenkategorier, romteknologi, datateknologi, ammunisjon m.m. Normalt er det US Army, US Navy, US Air Force, National Security Agency, the Atomic Energy Commission og NASA som utarbeider og endrer PSCRL. USPTO har besluttet hemmelighold for i overkant av 5000 patentsøkte oppfinnelser (2019).

I tillegg er Invention Secrecy Act en lov om hemmelige patenter som regulerer hvordan man skal gå frem ved eksport av hemmeligholdte patenterte oppfinnelser samt deres lisenser. Det er gjennom disse to regelsettene at NATO-avtalen "Agreement for the mutual safeguarding of secrecy of inventions relating to defence and for which applications for patents have been made", har blitt gjennomført i amerikansk rett, se punkt 3.3.

Invention Secrecy Act § 181 gir rett til hemmelighold. Når hemmelighold besluttes skal det også vurderes hvor lenge hemmelighold er påkrevd, samt informere patenthaver. Patenthaver har rett til å anke en beslutning om hemmelighold. Et patent kan ikke gis lenger hemmelighold enn ett år, men kan forlenges med ett år om gangen dersom den etaten som krevde hemmelighold første gang, mener det fortsatt er behov for hemmelighold. I krise eller krig gjelder ikke tidsfristene for hemmelighold.

Videre gir loven § 183 rett til erstatning. En patenthaver kan søke om erstatning for hemmelighold og for statens bruk av oppfinnelsen innen seks år fra hemmelighold er besluttet og patenthaver er informert:

> «An applicant […], whose patent is withheld as herein provided, shall have the right, beginning at the date the applicant is notified that, except for such order, his application is otherwise in condition for allowance,[…], and ending six years after a patent is issued thereon, to apply to the head of any department or agency who caused the order to be issued for compensation for the damage caused by the order of secrecy and/or for the use of the invention by the Government, resulting from his disclosure."

Paragraf 184 omhandler regler for å patentere oppfinnelser utenfor USA. Det er ikke tillatt å patentere i utenlandet før etter seks måneder fra oppfinnelsen ble patentert i USA. Det kan likevel gjøres dersom man får dette godkjent av USPTO etter søknad.

Paragraf 186 er straffebestemmelser. Ved brudd på loven kan man bøtelegges med inntil $10.000 og/eller opp til to år i fengsel. Det er i § 185 også lagt inn at dersom man har informert om oppfinnelsen i utlandet, herunder søkt patent eller bistått andre i å utnytte oppfinnelsen, vil man miste retten til patentet i USA.

3.4.2 International Traffic in Arms Regulation (ITAR)

International Traffic in Arms Regulation (ITAR) er en forskrift til Arms Export Control Act (AECA). ITAR er etablert for å begrense og kontrollere eksport av forsvarsteknologi. Forskriften sikrer kontroll med bl.a. ikke-patentert forsvarsteknologi. Det er Directorate of Defense Trade (DDTC) under Utenriksdepartementet (Department of State) som forvalter regelverket. I ITAR er det utarbeidet en liste over materiell, teknologi, tjenester og kompetanse i «The United States Munitions List» (USML) som spesifiserer hva som faller under ITAR.

Innslagspunktet for enhver amerikansk industri som ønsker å eksportere militært materiell, teknologi, kunnskap eller gjennomføre demonstrasjoner for utenlandsk personell, er DDTC. Industrien skal søke om eksport i hvert enkelt tilfelle. DDTC vil innhente påtegning/uttalelser fra 12 andre kontor i det amerikanske statsapparatet, herunder blant annet Forsvarsdepartementet ved US Army, US Navy, US Marine Corp, US Air Force, Department of Homeland Security, Department of Commerce.

Basert på uttalelsene fra de ulike myndighetene og egne vurderinger av den politiske situasjonen, trusselaktører, interne og eksterne situasjoner relatert til mottakerland og selskaper, samt den til enhver tid gjeldende liste over nasjoner/selskaper som kan godkjennes eller ikke, vil DDTC innvilge eller avslå en søknad om eksport/visning/demo.

Brudd på ITAR-regelverket kan medføre en administrativ sanksjon (civil penalties) på inntil $1 million for hvert brudd. Det kan også føre til straff (criminal penalties) på opp til 20 års fengsel.

3.4.3 Export Administration Regulations (EAR)

Export Administration Regulations (EAR) er en forskrift som bl.a skal sikre at varer, teknologi som har «dual use»-funksjoner holdes under kontroll med tanke på eksport. Bureau of Industry and Security (BIS) under Department of Commerce har forvaltningsansvaret for forskriften. Listen “Commerce Control List» (CCL) er utviklet for å gi kontrollrutiner for kjemiske og biologiske våpen, spredning av nukleær teknologi, nasjonal sikkerhet, missilteknologi, regional stabilitet, håndvåpen, kriminalitet og anti terrorisme. De selskapene som ønsker å eksportere varer og teknologi som angitt på CCL skal søke om dette til BIS.

Brudd på EAR-regelverket kan medføre administrativ sanksjon (civil penalties) på inntil $300.000 for hvert brudd og straff (criminal penalties) på inntil $1 million for hvert brudd med opp til 20 års fengsel.

4 Forholdet til andre lover

4.1 Sikkerhetsloven

Lov av 21. juni 2018 om nasjonal sikkerhet (sikkerhetsloven) har som formål «å trygge Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser», jf. sikkerhetsloven § 1-1 bokstav a.

Det følger av lovens § 1-5 nr. 1 bokstav b) at nasjonale sikkerhetsinteresser er «landets suverenitet, territorielle integritet og demokratiske styreform og overordnede sikkerhetspolitiske interesser knyttet til: (...) forsvar, sikkerhet og beredskap». Siden det vil være helt sentralt å opprettholde Forsvaret operative evne for å ivareta Norges suverenitet,

territorielle integritet og demokratiske styreform, er det å opprettholde Forsvarets operative evne en nasjonal sikkerhetsinteresse.

Sikkerhetsloven skal ivareta forsvarets operative evne gjennom å «forebygge, avdekke og motvirke sikkerhetstruende virksomhet», jf. § 1-1 bokstav b. Sikkerhetsloven stiller derfor krav om sikring av informasjon, informasjonssystem, infrastruktur og objekter som har avgjørende betydning for å opprettholde forsvarets operative evne.

Det følger av § 5-1 at «informasjon er skjermingsverdig dersom det kan skade nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig». Slik departementet ser det vil et vedtak om at forsvarsteknologi er «beskyttelsesverdig» innebære at informasjon om teknologien er skjermingsverdig. Dette følger av at teknologien må ha «vesentlig betydning» for forsvarets operative evne for å være beskyttelsesverdig. Dersom informasjonen om teknologien blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig, vil det etter departementets vurdering kunne skade forsvarets operative evne, og slik også kunne skade nasjonale sikkerhetsinteresser. Informasjonen må derfor graderes etter sikkerhetsloven § 5-3, og beskyttes i tråd med krav i sikkerhetsloven med tilhørende forskrifter.

Det følger av § 1-2 første ledd at loven gjelder for alle statlige, fylkeskommunale og kommunale organer. For at sikkerhetsloven skal kunne anvendes for en ikke-offentlig virksomhet følger det av § 1-3 første ledd bokstav a at et departement innenfor sitt ansvarsområde skal «fatte vedtak om at loven helt eller delvis skal gjelde for virksomheter som behandler (..) sikkerhetsgradert informasjon.».

Det innebærer at dersom det fattes vedtak om at en hele eller deler av en teknologi er beskyttelsesverdig, må Forsvarsdepartementet samtidig fatte vedtak om at bedriften skal underlegges sikkerhetsloven, siden virksomheten da har tilgang til, eller selv tilvirker sikkerhetsgradert informasjon. Dersom virksomheten hører til et annet departements ansvarsområde, vil Forsvarsdepartementet gi melding til det aktuelle departementet, jf. § 1-3 første ledd. Departementet bemerker at det følger av § 1-2 andre ledd at loven «gjelder for leverandører av varer eller tjenester i forbindelse med sikkerhetsgraderte anskaffelser(...)». Dersom teknologien utvikles på oppdrag fra forsvarssektoren vil leverandøren etter all sannsynlighet være underlagt sikkerhetsloven som leverandør i en sikkerhetsgradert anskaffelse.

4.1.1 Hva innebærer det for virksomheten å bli underlagt sikkerhetsloven?

Virksomheter som har beskyttelsesverdig forsvarsteknologi vil normalt ha sikkerhetsgradert informasjon, og skjermingsverdige informasjonssystemer hvor den sikkerhetsgraderte informasjonen behandles. Virksomheten skal da jevnlig vurdere risikoen den sikkerhetsgraderte informasjonen og informasjonssystemet er utsatt for, og vurdere hvilke sikkerhetstiltak som er nødvendig for å redusere risikoen til et forsvarlig nivå, jf. §§ 4-2 og 4-3. Hva som vil være et forsvarlig nivå avhenger av hvilket graderingsnivå informasjonen har, hvilke risiko disse verdiene er utsatt for, og hva som vil være kostnadseffektiv sikring, jf. § 4-3 og kapitel 3 i

virksomhetssikkerhetsforskriften.[6] Virksomhetens arbeid med forebyggende sikkerhet skal være en del av virksomhetens styringssystem, jf. § 4-1.[7]

Av virksomhetssikkerhetsforskriften § 22 følger det eksempelvis at BEGRENSET informasjon skal sikres på en slik måte at den ikke med enkle midle kan bli kjent for uautoriserte personer, i tillegg til krav til destruering, utlevering og kryptering. For informasjon gradert KONFIDENSIELT eller høyere stilles strengere krav, bl.a. krav om etablering av kontrollert, beskyttet og sperret sone, jf. § 37. Sikkerhetsloven stiller også krav om at det bare er personer med tjenstlig behov som kan gis tilgang til informasjonen, og at personene er autorisert og eventuelt sikkerhetsklarert for tilgangen, jf. §§ 5-4 og 8-1.

Sikkerhetsloven med forskrifter stiller også krav dersom virksomheten skal dele sikkerhetsgradert informasjon med myndigheter eller virksomheter i andre stater. Virksomhetssikkerhetsforskriften § 25 stiller krav om at delingen da må

a) være i samsvar med nasjonale sikkerhetsinteresser
b) ikke i strid med lovbestemt taushetsplikt, og
c) foreligge sikkerhetsavtale mellom Norge og den aktuelle staten.

Departementet legger opp til at deling av informasjon om beskyttelsesverdig forsvarsteknologi vil være i «samsvar med nasjonale sikkerhetsinteresser», jf. bokstav a, dersom departementet gir tillatelse til deling i tråd med vurderingen som beskrives i kapitel 9.2.2.1. Fordelen med å dele informasjon om teknologien vil da veie opp den eventuelle negative konsekvensen deling vil kunne ha for nasjonal sikkerhetsinteresser. Departementet legger også opp til at deling av informasjon om beskyttelsesverdig teknologi forutsetter at Norge har en tilstrekkelig sikkerhetsavtale med mottakerstaten, som sikrer at informasjonen på det aktuelle sikkerhetsnivået blir håndtert med et forsvarlig sikkerhetsnivå, jf. bokstav c. Det innebærer at Nasjonal sikkerhetsmyndighet (NSM) i hver sak må vurdere om det foreligger tilstrekkelig sikkerhetsavtale med mottakerstaten før informasjonen kan deles.

Departementet bemerker at kravene i sikkerhetsloven i utgangspunktet kun skal beskytte virksomhetens skjermingsverdige verdier. Det innebærer at kravene vil være tilpasset omfanget av, og graderingsnivået på informasjonen og informasjonssystemet, uten at det stilles krav til beskyttelse av virksomhetens øvrige aktiva.

4.1.2 Eierskapskontroll

Virksomheten vil også være underlagt reglene om eierskapskontroll i sikkerhetsloven kapittel 10. Den som vil erverve en «kvalifisert eierandel» i en virksomhet som er underlagt sikkerhetsloven, «skal sende melding til departementet om dette», jf. § 10-1. For at eierandelen skal være kvalifisert, må den omfatte «minst en tredjedel av aksjekapitalen, andelene eller stemmene i virksomheten», «rett til å bli eier av minst en tredjedel av aksjekapitalen eller andelene», eller innebærer «betydelig innflytelse over forvaltningen av selskapet på annen måte», jf. § 10-1 første ledd bokstav a-c. Dersom ervervet kan medføre en

[6] Forskrift 20. desember 2018 nr. 2053 om virksomheters arbeid med forebyggende sikkerhet
[7] Se kapitel 2 i Forskrift 20. desember 2018 nr. 2053 om virksomheters arbeid med forebyggende sikkerhet (virksomhetsikkerhetsforskriften) for nærmere krav til styringssystemet.

«ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet», kan Kongen i statsråd stanse ervervet, eller bestemme at det skal settes vilkår for gjennomføringen, jf. § 10-3.

I vurderingen av om ervervet skal stanses vil det være sentralt å vurdere erververens samlede innflytelse på virksomheten, hvilken tilknytning vedkommende har til andre stater og i hvilken grad Norge har et forsvars- og sikkerhetssamarbeid med staten vedkommende har tilknytning til.[8] Skal et erverv stanses må den samlede risikoen ervervet utgjør for nasjonale sikkerhetsinteresser, veie opp for de negative økonomiske konsekvensene av vedtaket for virksomheten.[9]

For en virksomhet som har rettigheter til beskyttelsesverdig forsvarsteknologi vil det være relevant å vurdere i hvilken grad ervervet innebærer en risiko for tap av teknologien. Det innebærer en vurdering av om det kan settes vilkår for ervervet som vil redusere risikoen for tap, f.eks. at erverver ikke får tilgang til teknologien. Det må også vurderes hvilke konsekvenser tap av teknologien vil ha for Forsvarets operative evne. Dette må holdes opp mot de negative økonomiske konsekvensene for virksomheten av å stanse ervervet, og hvilke eventuelle fordeler oppkjøpet vil ha, f.eks. i hvilken grad ervervet gir økonomiske fordeler eller tilgang til tekniske miljøer som kan bidra til videreutvikling av teknologien.

4.1.3 Forholdet mellom sikkerhetstiltak etter sikkerhetsloven og vilkår for deling

I vurderingen av om teknologien er beskyttelsesverdig, må det også vurderes hvilke graderingsnivå som skal være på informasjonen om teknologien. Det innebærer at vilkår for deling av teknologien vil måtte ses i sammenheng med kravene som følger av sikkerhetsloven. Sikkerhetslovens krav til kontroll med hvem som får tilgang til informasjon, vil langt på vei kunne redusere risikoen for tap av informasjon om teknologien ved deling. Sikkerhetsloven har også begrensninger for deling av informasjon ut fra norsk jurisdiksjon. Det vil imidlertid være aktuelt å stille krav som kommer i tillegg til sikkerhetsloven, f.eks. der konsekvensen for operativ evne er svært stor om teknologien kommer uvedkommende i hende, eller der risikoen for tap av teknologien ikke kan ivaretas i tilstrekkelig grad gjennom kravene i sikkerhetsloven. Det vil f. eks kunne være aktuelt å stille krav om norsk statsborgerskap for tilgang til teknologien.

Selv om departementet legger opp til at det ikke vil være forskjellige nivå av beskyttelsesverdighet, vil graderingsnivået på informasjon om teknologien kunne variere, noe som i praksis vil ha betydning for hvilke vilkår som settes for deling av teknologien.

4.2 Eksportkontroll

Kontroll med eksport av forsvarsmateriell reguleres av lov 18. desember 1987 nr. 93 om kontroll med eksport av strategiske varer, tjenester og teknologi mv. (eksportkontrolloven), med tilhørende forskrift av 19. juni 2013 nr. 718 om eksport av forsvarsmateriell, flerbruksvarer, teknologi og tjenester (eksportkontrollforskriften).

Utenriksdepartementet er nasjonal eksportkontrollmyndighet og har ansvaret for ovennevnte lov og tilhørende forskrift. I tillegg til lov og forskrift foreligger det retningslinjer for Utenriksdepartementets behandling av søknader om eksport av forsvarsmateriell, samt

[8] Prop. 153 L (2016-2017), side 151-152 og 192
[9] Prop. 153 L (2016-2017), side 152 og 192.

teknologi og tjenester for militære formål av 28. februar 1992. Eksport av forsvarsmateriell samt flerbruksvarer til militær sluttbruk redegjøres for i en årlig melding til Stortinget.[10]

Eksportkontrolloven skal sikre at eksport av forsvarsmateriell fra Norge skjer i tråd med norske utenriks- og sikkerhetspolitiske interesser, og Stortingets forutsetninger. Loven sikrer også at eksporten av flerbruksvarer ikke bidrar til spredning av masseødeleggelsesvåpen (kjernefysiske, kjemiske og biologiske våpen), samt leveringsmidler for slike våpen.

Ny lov om beskyttelse av forsvarsteknologi (lovforslaget) skal sikre at Forsvaret har tilstrekkelig kontroll med og tilgang til teknologi som har vesentlig betydning for å ivareta Forsvarets operative evne.[11] Det innebærer i hovedsak å kunne føre kontroll med hvem som kan få tilgang til teknologien, hvor teknologien er tilgjengelig, hvem teknologien kan deles med, både innenfor og utenfor norsk jurisdiksjon, og mulighet til å legge føringer på bruk og utvikling av en teknologi.

Av eksportkontrolloven § 1 følger videre at Kongen kan bestemme at varer og teknologi som kan være av betydning for andre lands utvikling, produksjon eller anvendelse av produkter til militær bruk eller som direkte kan tjene til å utvikle et lands militære evne, samt varer og teknologi som kan benyttes til å utøve terrorhandlinger, jf. straffeloven § 131, ikke må utføres fra Norge uten særskilt tillatelse. En slik tillatelse gis i form av en eksportlisens fra Utenriksdepartementet basert på søknad fra norsk eksportør, som har ansvaret for å innhente eksportlisens før eksport finner sted.

Lovforslaget innebærer at eksportøren i tillegg må søke om tillatelse fra Forsvarsdepartement i forkant av eksporten.[12] Lovforslaget skal redusere risikoen for tap av beskyttelsesverdig forsvarsteknologi ved eksport, og innebærer at Forsvarsdepartement må vurdere risikoen for tap av teknologien opp mot fordelene ved eksport, før den eksporteres.[13]

Eksportkontrollforskriften gir også nærmere regler for hva som er lisenspliktig, adgangen til å sette vilkår for lisens, unntak fra lisensplikten, og adgangen til å trekke tilbake, suspendere eller endre tidligere innvilget lisens. Hvilke varer, teknologi og tjenester som er lisenspliktige, og som krever lisens for å eksportere, fremgår av to lister inntatt som vedlegg til forskriften. Liste I omfatter forsvarsrelaterte varer (våpen, ammunisjon og annet militært materiell, teknologi og tjenester) og liste II omfatter flerbruksvarer. Flerbruksvarer er sivile varer som er utviklet for sivile formål, men som også har militære anvendelsesområder. Forskriften regulerer også eksport av tjenester og teknologi relatert til varer på liste I og liste II, samt formidling av slike varer mellom to tredjeparter.

Innholdet i Utenriksdepartementets varelister fremforhandles internasjonalt, der Utenriksdepartementet deltar. Forhandlingene foregår i fire multilaterale eksportkontrollregimer; Australia-gruppen, som retter seg mot å hindre spredning av kjemiske og biologiske våpen, Missile Technology Control Regime (MTCR), som omfatter leveringsmidler for masseødeleggelsesvåpen, Nuclear Suppliers Group (NSG), som gjelder

[10] Siste stortingsmelding er Meld. St. 35 (2020-2021) Eksport av forsvarsmateriell fra Norge i 2020, eksportkontroll og internasjonalt ikke-spredningsarbeid

[11] Se kapitel 5 for beskrivelse av varer, tjenester og teknologi som kan omfattes av lovforslaget.

[12] Se kapitel 9.3.4 for saksbehandlingen og samhandlingen mellom UD og FD.

[13] SE kapitel 9.2 om tillatelse til deling av teknologi.

kjernefysiske våpen, samt Wassenaar-samarbeidet, som omfatter konvensjonelle våpen, militære varer og sensitiv høyteknologi.

Beskyttelsesverdig forsvarsteknologi vil i de aller fleste tilfellene være en vare, tjeneste eller teknologi som er omfattet av liste I eller II. Et vedtak om at en forsvarsteknologi er beskyttelsesverdig vil imidlertid rette seg mot en konkret teknologi.[14] F.eks kan to forskjellige typer raketter omfattes av liste I, men bare en av dem være beskyttelsesverdig, eller inneholde komponenter som er beskyttelsesverdige. For å tydeliggjøre sammenhengen mellom regelverkene er det tatt inn i definisjonen av forsvarsteknologi at begrepene varer, tjenester eller teknologi skal forstås på samme måte som begrepene er definert i eksportkontrollregelverket.[15]

Av Utenriksdepartementets retningslinjer[16] følger nærmere saksbehandlingsregler for behandlingen av søknader om eksport av forsvarsmateriell. Utgangspunktet for behandlingen fremgår av Stortingets vedtak av 11. mars 1959 som sier at «eksport av våpen og ammunisjon fra Norge bare må skje etter en omhyggelig vurdering av de uten- og innenrikspolitiske forhold i vedkommende område»[17], og hovedhensynet «at Norge ikke vil tillate salg av våpen og ammunisjon til områder hvor det er krig, krig truer eller til land hvor det er borgerkrig».[18]

Dette utgangspunktet er konkretisert i retningslinjene punkt 2.3 med «særlige avslagsgrunner», der det blant annet fremgår at søknader der «dette er uforenlig med Norges internasjonale forpliktelser», vil bli avslått.[19] Hva som er Norges internasjonale forpliktelser er konkretisert i vedlegg A, kriterium 1-4, bl.a. dersom eksport vil være uforenlig med «medlemstatenes internasjonale forpliktelser og deres plikt til å overholde våpenblokadene innført av De forente nasjoner (FN), Den europeiske union (EU) og organisasjonen for sikkerhet og samarbeid i Europa (OSSE)»[20] eller «der det er åpenbart at det militære utstyret som skal eksporteres kan bli brukt til intern undertrykking».[21]

I retningslinjene punkt 2.4 fremgår hensyn som det også skal tas særlig hensyn til i vurderinger av søknader om eksport, blant annet kriterium 5 om «den nasjonale sikkerheten i Norge, allierte og vennligsinnede land»[22]. Det vil bl.a. si «risikoen for at den militære teknologien eller det militære utstyret som skal eksporteres, kan bli brukt mot deres egne eller andre medlemsstaters styrker og mot styrkene til vennligsinnede og allierte land.»[23] I saksbehandlingen og helhetsvurderingen av kriterium 5 legger departementet til grunn at FDs vedtak om deling av en beskyttelsesverdig teknologi vil inngå som en del av vurderingen.[24]

---

[14] Se kapitel 5.2 og 5.3 for nærmere om begrepene «forsvarsteknologi» og «beskyttelsesverdig».
[15] Se kapitel 15 og merknaden til § 2.
[16] Retningslinjer for Utenriksdepartementets behandling av søknader om eksport av forsvarsmateriell, samt teknologi og tjenester for militære formål av 28. februar 1992.
[17] Retningslinjene punkt 2.2 bokstav b)
[18] Retningslinjene punkt 2.2 bokstav a)
[19] Retningslinjene punkt 2.3 bokstav a), se de påfølgende bokstavene for avslagsgrunner på bakgrunn av folkerett og humanitære hensyn
[20] Kriterium 1 bokstav a)
[21] Kriterium 2 bokstav a)
[22] Punkt 2.4 bokstav a)
[23] Kriterium 5 bokstav b, Retningslinjer for Utenriksdepartementets behandling av søknader om eksport av forsvarsmateriell, samt teknologi og tjenester for militære formål av 28. februar 1992.
[24] Se kapitel 9.2 for beskrivelse av vedtaket om tillatelse til deling.

I tillegg definerer retningslinjene forsvarsmateriell i henhold til varekategoriene A og B[25], fire landgrupper[26], og hvilken dokumentasjon som kreves i forbindelse med eksport. Varekategoriene og landgruppene angir hvilke varer som normalt kan eksporteres til hvilke land, og i hvilke tilfeller eksporten må underlegges en nærmere vurdering, jf. forrige avsnitt. Varekategori A omfatter våpen, ammunisjon og visse typer materiell, samt annet materiell med strategisk kapasitet som vesentlig kan påvirke de militære styrkeforhold utover nærområdet. Varekategori B omfatter øvrige forsvarsrelaterte varer som ikke har de egenskaper eller bruksområder som definert for varekategori A.[27] Eksempelvis følger det av retningslinjene at varer i varekategori A normalt bare kan eksporteres til forsvarsmyndigheter i landgruppe 1, dvs. «nordiske land og NATOs medlemsland, samt enkelte særskilt nærstående land.»[28]

Utenriksdepartementets vedtak om innvilgelse av lisens for eksport av forsvarsmateriell er utelukkende en politisk beslutning. Disse beslutningene har sitt grunnlag i norske utenriks- og sikkerhetspolitiske interesser, Stortingets forutsetninger og internasjonale forpliktelser.

Eksport av teknologi i form av kunnskap er omfattet av eksportkontroll. Dette fremgår i forarbeidene til eksportkontrolloven, Ot.prp. nr. 9 (1987-88) om lov om kontroll med eksport av strategiske varer, tjenester og teknologi. I forarbeidene til eksportkontrolloven § 1 fremgår det videre at «teknologi omfatter alle fremgangsmåter og hjelpemidler, uansett om dette er kommet til uttrykk i skriftlig materiale (…) eller formidles muntlig». Begrepet «teknologi» omfatter på eksportkontrollområdet også immateriell teknologi i form av kunnskapsoverføring. En slik fortolkning er i tråd med definisjonen av teknologi i eksportkontrollforskriftens vedlegg I og II. Etter gjeldende rett er det dermed hjemmel til å kontrollere kunnskapsoverføring innenfor eksportkontrollregelverkets virkeområde. Dette inkluderer også tilfeller der kunnskapsoverføringen skjer i Norge, dersom informasjonen vil bli brukt i utlandet.

Utenriksdepartementet gjennomførte våren 2022 en alminnelig høring av forslag til endringer i eksportkontrollforskriften for å tydeliggjøre at eksportkontrollregelverket også omfatter visse overføringer av kunnskap med militære anvendelser. I forslaget til eksportkontrollforskriften § 2 (10) er «kunnskapsoverføring» foreslått definert som «enhver form for muntlig eller skriftlig deling av kunnskap om varer og teknologi som kan tjene til å utvikle et lands militære evne.» Videre foreslås det å innføre lisensplikt for kunnskapsoverføring i forslag til ny § 5a i eksportkontrollforskriften: *«Kunnskapsoverføring om varer og teknolog oppført på liste I og II, samt kunnskapsoverføring for øvrig som skal tjene til å utvikle et lands militære evne, som ytes i utlandet eller her i landet for bruk i utlandet, krever lisens fra Utenriksdepartementet»*. Utenriksdepartementet arbeider høsten 2022 med gjennomgang av høringsinnspillene.

I lys av at den teknologiske utviklingen går raskt vil en sentral del av samarbeidet mellom Forsvarsdepartementet og Utenriksdepartementet i operasjonaliseringen av forslaget til ny lov, være å gjøre det klart for virksomhetene hva som på listene til eksportkontrollregelverket er beskyttelsesverdig forsvarsteknologi, og motsatt hvilke beskyttelsesverdig forsvarsteknologi som omfattes av hvilken av listene til eksportkontrollregelverket. Oversikten over

[25] Punkt 3.1
[26] Punkt 3.2
[27] Meld. St. 35 (2020-2021) Eksport av forsvarsmateriell fra Norge i 2020, eksportkontroll og internasjonalt ikke-spredningsarbeid.
[28] Punkt 4.2 bokstav a) og b).

beskyttelsesverdig forsvarsteknologi vil forvaltes av, og være tilgjengelig på nettsidene, til Forsvarsdepartementet.

4.3 Lov om forretningshemmeligheter

Lov 27. mars 2020 nr. 15 om vern av forretningshemmeligheter (forretningshemmelighetsloven) gjennomfører EU-direktiv 2016/943 om beskyttelse av fortrolig «knowhow» og forretningshemmeligheter. Loven trådte i kraft 1. januar 2021.

Loven er i all hovedsak en videreføring av gjeldende rett og innebærer en forenkling og samling av gjeldende regler om forretningshemmeligheter.

Loven har som formål å sikre at innehavere av forretningshemmeligheter får vern mot urettmessig tilegnelse, bruk og formidling av hemmeligheten, jf. loven. § 1.

«Forretningshemmeligheter» er i loven § 2 første ledd definert som «opplysninger som

a) er hemmelige i den forstand at opplysningene ikke som helhet, eller slik de er satt sammen eller ordnet, er allment kjent eller lett tilgjengelig
b) har kommersiell verdi fordi de er hemmelige
c) innehaveren har truffet rimelige tiltak for å holde hemmelig».

Loven § 3 forbyr inngrep i forretningshemmeligheter gjennom handlinger hvor en urettmessig tilegner seg, bruker eller formidler en forretningshemmelighet. Videre forbyr § 4 første ledd å «tilvirke, markedsføre eller bringe i omsetning varer som vedkommende visste eller burde ha visst utgjør inngrep i en forretningshemmelighet» Dette gjelder også «innførsel, utførsel eller lagring av varer som utgjør inngrep i en forretningshemmelighet, med sikte på å bringe varene i omsetning». Det vil utgjøre inngrep i en forretningshemmelighet når varen har en utforming, egenskap eller funksjon eller produseres eller markedsføres på en måte som «i vesentlig grad drar fordel av en forretningshemmelighet som er urettmessig tilegnet, brukt eller formidlet», jf, § 4 andre ledd.

I lovens forarbeider (Prop.5 L (2019-2020) s. 44) presiseres det at vurderingen av om en handling er «urettmessig» vil være sammensatt, men vil omfatte handlinger som er i strid med annen lovgivning, privatrettslige avtaler, instrukser eller andre normer på området. Formålet med loven er å verne mot annen kommersiell bruk. Etter departementets syn vil vilkår for deling, og krav til bruk av, ikke være et urettmessig inngrep. Det samme gjelder pålegg om å gi opplysninger om beskyttelsesverdig forsvarsteknologi. Etatene i forsvarssektoren vil dessuten ha taushetsplikt om «tekniske innretninger og fremgangsmåter samt drifts- eller forretningsforhold som det vil være av konkurransemessig betydning å hemmeligholde av hensyn til den som opplysningen angår», jf. forvaltningsloven § 13 første ledd nr. 2.

4.4 Lov om militære rekvisisjoner (rekvisisjonsloven)

Når riket er i krig gir lov 29. juni 1951 nr. 19 om militære rekvisisjoner § 1 første ledd hjemmel til å rekvirere «alt som er nødvendig for krigsmakten og institusjoner som er knyttet til den», herunder «varer og annet løsøre av enhver art».

Rekvisisjoner kan skje til både eie eller bruk, jf. § 2 første ledd, og ytelser og tap som følge av rekvisisjoner etter loven gir rett til godtgjørelse, jf. § 12 første ledd.

Videre følger det av § 1 andre ledd at Kongens rekvisisjonsadgang i § 1 helt eller delvis også skal gjelde utenfor krigstid når krigsmakten eller noen del av denne er beordret satt på krigsfot

i beredskapsøyemed, eller når det er nødvendig til fremme av beredskapstiltak, herunder større øvelser.

Nærmere regler om rekvisisjoner etter loven er gitt i forskrift 17. september 1999 nr. 1012 om militære rekvisisjoner. Forskriften kommer til anvendelse i «krig» og «utenfor krigstid» når «Forsvaret eller deler av dette er innkalt etter særskilt vedtak truffet av Kongen i statsråd, eller til fremme av nødvendige beredskapstiltak, herunder gjennomføring av større øvelser», jf. § 1 første ledd bokstav b.

Loven gir Forsvaret vide hjemler til å rekvirere varer og lignende i krigstid, forutsatt at det er truffet vedtak fra Kongen i statsråd, men også i forbindelse med beredskapstiltak og gjennomføring av større øvelser. Loven innebærer at Forsvaret også kan rekvirere beskyttelsesverdig forsvarsteknologi, forutsatt at vilkårene for rekvisisjon er tilstede. Rekvisisjonsloven vil imidlertid ikke oppstille vurderingsmomenter for hva som er beskyttelsesverdig. Regelverket vil heller ikke stanse, eller sette vilkår for deling og bruk av teknologi i fredstid, som er nødvendig for å ha tilstrekkelig kontroll med beskyttelsesverdig forsvarsteknologi, slik det legges opp til i kapitel 9.

4.5 EØS-regelverket

Gjennom avtalen om Det europeiske økonomiske samarbeidsområde (EØS-avtalen) er Norge gitt tilgang til EUs indre marked med fri flyt av varer, tjenester, arbeid og kapital, og med felles konkurransevilkår for næringslivet, jf. EØS-avtalen artikkel 1 og artikkel 8. EØS-avtalen er inntatt i norsk rett i lov av 27. november 1992 nr. 109 om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) mv. (EØS-loven) og trådte i kraft 1. januar 1994.

Artikkel 8 nr. 1 fastslår at det skal være fritt varebytte mellom EØS-landene. Eksportrestriksjoner og alle tiltak med tilsvarende virkning for det frie varebyttet er i utgangspunktet forbudt, jf. artikkel 12. Tilsvarende gjelder for adgangen til å yte tjenester i EØS-området, jf. artikkel 36. Det omfatter bl.a. adgangen til å yte konsulenttjenester.

EØS-avtalen gir ingen definisjon av hva som er å anse som «varer». EU-domstolen har lagt til grunn at varebegrepet tolkes vidt og omfatter alle produkter som har en pengeverdi og som er gjenstand for kommersielle transaksjoner.[29]

Departementet legger til grunn at beskyttelsesverdig forsvarsteknologi vil være varer i EØS-avtalens forstand, forutsatt at de har en pengeverdi og kan være gjenstand for kommersielle transaksjoner. Departementet legger også til grunn at tjenester knyttet til beskyttelsesverdig forsvarsteknologi vil være omfattet av tjenestebegrepet i EØS-avtalen. Eksempelvis vil konsulenttjenester fra en virksomhet som har kunnskap om hvordan en teknologi brukes eller kan utvikles være omfattet EØS-avtalen.

Et vedtak som setter begrensninger på deling av beskyttelsesverdig teknologi mellom virksomheter som holder til innenfor EØS-området vil i utgangspunktet være i strid med artikkel 12 og 36. Skal vedtaket være i tråd med EØS-retten må det derfor fattes innenfor rammene av unntaksbestemmelsen i EØS-avtalen. Departementet legger til grunn at både artikkel 123, artikkel 13 og artikkel 33, jf. artikkel 39, vil kunne gi tilstrekkelig hjemmel til å

[29] Sejersted m.fl., *EØS-rett* (2. Utgave, 2003) s. 283.

fatte vedtak om begrensninger på deling, produksjon, utvikling og annen utnyttelse av teknologien som ellers ville være i strid med EØS-avtalen.

Det følger av artikkel 123 bokstav b at EØS-avtalen ikke er til hinder for at en avtalepart kan treffe tiltak 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».

For beskyttelsesverdig forsvarsteknologi som er «våpen, ammunisjon og krigsmateriell, eller andre varer som er uunnværlige for forsvarsformål» vil artikkel 123 bokstav b kunne gi hjemmel for å gjøre unntak fra EØS-avtalen. Bruk av bestemmelsen forutsetter imidlertid at det er nødvendig å gjøre unntak for å ivareta vesentlige sikkerhetsinteresser, og at bruken av unntaket ikke går lenger enn det som er nødvendig for å ivareta den aktuelle interessen.[30]

Beskyttelsesverdig forsvarsteknologi er varer, tjenester og teknologi med vesentlig betydning for Norges forsvarsevne, se beskrivelsen i kapitel 5.2 og 5.3. Departementet legger derfor til grunn at teknologien normalt også har sentral betydning for Norges vesentlige sikkerhetsinteresser. Et vedtak som setter begrensninger på utnyttelse av teknologien for å beskytte denne, vil da normalt være begrunnet i behovet for å ivareta vesentlige sikkerhetsinteresser. Slik departementet ser vil det avgjørende for om et vedtak er innenfor EØS-retten da være om det finnes andre mindre inngripende alternativer til vedtaket for å oppnå det samme formålet. Det vil bero på en konkret vurdering i hver enkelt sak. Departementet legger imidlertid opp til at et vedtak om begrensninger skal være siste utvei for å redusere risikoen for tap av teknologien, slik at et vedtak om begrensninger normalt vil være proporsjonalt og forholdsmessig. Se kapitel 9-2 til 9.4 for beskrivelsen av hvilke begrensninger som er aktuelle.

Det er også et vilkår i artikkel 123 at tiltaket «ikke endrer konkurransevilkårene for varer som ikke er bestemt for direkte militært formål». Vilkåret innebærer bl.a. at bestemmelsen ikke kan brukes til å treffe vedtak for å beskytte teknologi som er bestemt for sivil bruk, men som også er direkte anvendbart militært. Slik departementet ser det må da et vedtak knyttet til beskyttelsesverdig teknologi som ikke har noen militære tilpasninger, normalt måtte begrunnes i en av de andre unntaksbestemmelsene i EØS-avtalen.

Det følger av artikkel 123 bokstav a at EØS-avtalen ikke er til hinder for at en avtalepart kan treffe tiltak som:

> «den anser nødvendig for å hindre spredning av opplysninger som er i strid med dens vesentlige sikkerhetsinteresser»

Departementet legger til grunn at et vedtak om begrensninger på utnyttelsen av beskyttelsesverdig forsvarsteknologi også vil kunne være egnet til å hindre spredning av opplysninger som er i strid med statens vesentlige sikkerhetsinteresser. Departementet viser til at informasjon om en beskyttelsesverdig teknologi er gradert, jf. kapitel 4.1, og at

[30] Vilkåret om at bruken av bestemmelsen må være forholdsmessig og proporsjonalt følger av praksis fra EU-domstolen om bruk av den tilsvarende bestemmelsen i EU-traktaten, artikkel 346, se bl.a. C-274/12 *Schiebel*, avsnitt 37.

informasjonen kan skade nasjonale sikkerhetsinteresser om den blir gjort kjent for uvedkommende, jf. sikkerhetsloven § 5-3. Sikkerhetsgradert informasjon vil imidlertid normalt kunne beskyttes i tilstrekkelig grad gjennom at det stilles krav om at virksomheten som håndterer informasjonen oppfyller kravene i sikkerhetsloven med forskriften for beskyttelse av informasjonen. Et vedtak om begrensninger utover disse kravene vil da normalt gå lenger enn det som er nødvendig for å beskytte informasjonen, og det vil da være tvilsomt om tiltaket er proporsjonalt og forholdsmessig.

Departementet legger til grunn at et vedtak knyttet til beskyttelsesverdig forsvarsteknologi som ikke har noen militære tilpasninger, vil normalt kunne hjemles i artikkel 13. Det følger av artikkel 13 at forbudet mot eksportrestriksjoner i artikkel 12 blant annet ikke er til hinder for forbud eller restriksjoner på eksport eller transitt som er begrunnet ut fra hensynet til «offentlig (...) orden og sikkerhet». Det følger videre av andre punktum at «[s]like forbud eller restriksjoner må dog ikke kunne brukes til vilkårlig forskjellsbehandling eller være en skjult hindring på handelen mellom avtalepartene». Tilsvarende unntak gjelder for tjenester, jf. artikkel 33, jf. artikkel 39.

«Offentlig sikkerhet» omfatter både den indre og ytre sikkerhet og kan hjemle krav om eksportlisens for varer av strategisk betydning til andre ikke-allierte land.[31] På grunn av teknologiens sentrale betydning for forsvarsevnen, jf. kapitel 5.2 og 5.3 legger departementet til grunn at et vedtak om begrensninger for å beskytte beskyttelsesverdig forsvarsteknologi vil kunne være begrunnet i «offentlig sikkerhet». Det gjelder imidlertid samme krav til at tiltaket må være proporsjonalt og forholdsmessig som for tiltak etter artikkel 123. Det avgjørende for om et vedtak er innenfor EØS-retten vil da være om det finnes andre mindre inngripende alternativer til vedtaket for å oppnå det samme formålet. Det vil bero på en konkret vurdering i hver enkelt sak. Departementet legger imidlertid opp til at et vedtak om begrensninger skal være siste utvei for å redusere risikoen for tap av teknologien, slik at et vedtak om begrensninger normalt vil være proporsjonalt og forholdsmessig. Se også her kapitel 9-2 til 9.4 for beskrivelsen av hvilke begrensninger som er aktuelle.

5 Virkeområde

5.1 Gjeldende rett

5.1.1 «Oppfinnelse»

Gjeldende lov om forsvarsviktige oppfinnelser § 1 gjelder for:

«oppfinnelser av betydning for rikets forsvar når oppfinnelsen er gjort her i riket, eller det er søkt om patent på den her, eller når noen som er bosatt her eier oppfinnelsen helt eller delvis eller har utnyttelsesrett i den.»

Dette innebærer at alle oppfinnelser som har betydning for Forsvaret omfattes av loven, forutsatt at:

- Varen, tjenesten eller teknologien er en oppfinnelse,
- som har betydning for rikets forsvar,
- oppfinnelsen er gjort i Norge, eller

[31] Sejersted m.fl., EØS-rett (2. Utgave, 2003) s. 316

- det er søkt om patent på oppfinnelsen i Norge, eller
- når noen som er bosatt i Norge eier oppfinnelsen helt eller delvis eller har utnyttelsesrett i den.

Departementet legger til grunn at det i de langt fleste tilfeller vil være klart om «oppfinnelsen er gjort i Norge», eller om «det er søkt om patent for oppfinnelsen i Norge». Førstnevnte tilfelle ville omfatte personer eller virksomheter hvor det kan dokumenteres at oppfinnelsen er gjort innenfor norsk jurisdiksjon. I sistnevnte tilfelle må det være levert en patentsøknad til et patentkontor i Norge. I vurderingen av om «noen som er bosatt i Norge eier oppfinnelsen helt eller delvis eller har utnyttelsesrett» vil det være avgjørende om vedkommende er avtalepart i en avtale som viser utnyttelsesretten til oppfinnelsen. Departementet legger imidlertid til grunn at det vil måtte gjøres en nærmere vurdering av om produktet er en «oppfinnelse», og om den «har betydning for rikets forsvar».

Begrepet «oppfinnelse» er verken definert i gjeldende lov eller i patentloven. Ordlyden tilsier at loven gjelder for et nytt produkt, i fasen fra idé til produktet er ferdigutviklet, det er satt i produksjon, er alminnelig kjent eller tilgjengelig på markedet.

I forarbeidene[32] til loven står det om begrepet oppfinnelse:

> «Utvalget mener at uttrykket «oppfinnelser» i denne loven ikke må være begrenset til patenterbare oppfinnelser. På den annen side bør det ikke omfatte sådant som på forhånd er alminnelig kjent, eller som for fagfolk på området vil være mer eller mindre selvfølgelig. Tekniske fremgangsmåter eller anordning som ikke kan betegnes som oppfinnelser kan utvalget ikke foreslå inntatt i loven.»

Uttalelsen i forarbeidene tilsier at det ikke er avgjørende om oppfinnelsen oppfyller patentlovens krav for å bli patentert, eller om den allerede er patentert, for at oppfinnelsen omfattes av loven. Det er i hvilken grad produktet er alminnelig kjent, eller om det er selvfølgelig for fagfolk på området som er avgjørende for om produktet er en «oppfinnelse» etter gjeldene lov. Det innebærer en vurdering av om produktet er nytt i forhold til andre produkter som allerede er tilgjengelig på markedet, og hvor tilgjengelig informasjonen om produktet er for aktører på markedet. Begrepet vil etter departementets syn omfatte produkter som befinner seg på ett av de teknologisk modenhetsnivået på TRL-skalaen[33], eller der produkter er satt i produksjon, men ikke kjent for markedet enda. Slik departementet ser det vil imidlertid ikke gjeldende lov omfatte varer, tjenester eller teknologi som er alminnelig kjent eller tilgjengelig på markedet.

5.1.2 Nærmere om betydning for rikets forsvar, direkte betydning for rikets forsvar og krigsmateriell

Etter departementets syn omfatter ordlyden «betydning for rikets forsvar» alle typer oppfinnelser som kan brukes til forsvaret av Norge. Ordlyden skiller ikke på om oppfinnelsen er laget med det som formål, eller på hvor stor betydning oppfinnelsen må ha for rikets forsvar, det avgjørende er om den kan brukes til forsvar av Norge. I forarbeidene fremgår det at loven

[32] Ot. prp. nr. 62 (1952) s. 14-15.
[33] https://www.innovasjonnorge.no/no/tjenester/innovasjon-og-utvikling/finansiering-for-innovasjon-og-utvikling/finansiering-av-innovasjonsprosjekt/technology-readiness-level-trl/

ble gitt for å sikre det offentlige hjemmel til enhver forføyning som er nødvendig for at en oppfinnelse av betydning for rikets sikkerhet skal komme rikets forsvar mest mulig til nytte.[34]

Taushetsplikten i § 2 er imidlertid begrenset til oppfinnelser som «gjelder krigsmateriell» eller oppfinnelser som har «direkte betydning for rikets forsvar». Det følger av § 2 at disse oppfinnelsene «må ikke gjøres kjent for andre» enn relevante myndigheter etter § 3. Ordlyden «krigsmateriell» omfatter oppfinnelser som er egnet til bruk i krig, eksempelvis våpen, ammunisjon, bomber, raketter, missiler etc. Ordlyden «direkte betydning for rikets forsvar» tilsier at oppfinnelsen må gjelde et produkt som ligger tett opp mot krigsmateriell, men som ikke er direkte egnet til å løse oppgaver for å påføre en motstander skade i krig, eller understøtte slikt materiell[35]. Eksempelvis vil oppfinnelser som ivaretar sentrale logistikk- eller kommunikasjonsoppgaver kunne være omfattet av vilkåret.

Dette underbygges av forskrift av 9. mars 2000 nr. 215 om behandling av saker etter lov om oppfinnelser av betydning for rikets sikkerhet, der begrepene er ytterligere konkretisert.

Det følger av forskriften § 2 at materiell eller en oppfinnelse er «krigsmateriell» eller ansett for å ha «direkte betydning for rikets forsvar» dersom det er «særskilt egnet for eller særskilt bestemt for bruk i krig», og faller inn under én av følgende kategorier:

a) Våpen med tilbehør av enhver art, herunder ammunisjon, og lignende materiell med sprengvirkning, brannstiftende virkning, varmevirkning, røykvirkning, lysvirkning, lydvirkning, radioaktiv virkning eller stridsgassvirkning.

b) Biologiske eller kjemiske stridsmidler, samt materiell for konstatering, identifisering eller måling av radioaktive, biologiske eller kjemiske stridsmidler.

c) Materiell for ildledning, observasjon (herunder fotomateriell mv.), beregning, oppklaring og varsling av mål, materiell for sikkerhetstjenesten i samband med dette.

d) Materiell til vern mot observasjon, oppklaring eller annen iakttakelse.

e) Navigasjonsmateriell og materiell til kontroll, målsøkning eller styring av hvilken som helst type våpen.

f) Materiell som kan nyttes av eller er av betydning for sambandstjenesten.

g) Anleggs-, brøyte- eller rydningsmaskiner samt oversettings- og brumateriell.

h) Transportmidler og anordninger av alle slags skip, fly eller biler, med eller uten stridsmidler.

i) Materiell og konstruksjoner til vern mot våpen og stridsmidler av alle slag.

j) Materiell for villedning.

k) Materiell for og mot forstyrrelse av sambandstjenesten, radar eller andre lokaliseringsmidler.

l) Materiell for og mot forstyrrelse av ildledning, varsling, navigering eller målsøking.

[34] Bl.a. Ot.prp. nr. 62 (1952) s.14
[35] Ot.prp. nr. 62 (1952) s. 5

Ordlyden «særskilt egnet for eller særskilt bestemt for bruk i krig» tilsier at oppfinnelsen enten må ha som formål å løse en oppgave i en krigssituasjon, eller ha egenskaper som gjør at den vil være egnet til å løse oppgaver i en krigssituasjon.

Sett i sammenheng med ordlyden «betydning for riktes forsvar» må det konstateres en sammenheng mellom det oppfinnelsen kan brukes til, og Forsvarets operative evne, skal oppfinnelsen omfattes av loven. Det må begrunnes hva oppfinnelsen kan brukes til og hvordan den kan understøtte Forsvarets operative evne. Departementet legger imidlertid til grunn at det ikke skal mye til for at kravet om sammenheng er oppfylt. Eksempelvis vil en brøytemaskin i utgangspunktet være like anvendelig i en fredssituasjon, som i en krigssituasjon. Den vil likevel kunne være omfattet av loven, ettersom en brøytemaskin ofte er en forutsetning for å gjennomføre sentrale logistikkoppgaver under strid om vinteren.

Slik departementet ser det vil oppfinnelser Forsvaret bare kan bruke til å løse oppgaver som ikke er forbundet med operativ evne falle utenfor gjeldende lovs virkeområde. Eksempelvis oppfinnelser som kun skal brukes ved bistand til sivilsamfunnet i forbindelse med naturkatastrofer, og kommunikasjon og logistikk som ikke har en link til operativ evne.

5.2 Forslaget i høringsnotatet

5.2.1 Generelt om forholdet mellom forsvarssektoren og industrien og den teknologiske utviklingen

For å løse sine oppgaver er Forsvaret avhengig av moderne varer, tjenester og teknologi. Slike varer, tjenester og teknologi leveres av forsvarsindustrien, men i større grad også sivil industri. I Meld. St. 17 (2020-2021) er det redegjort for hvilken rolle og betydning forsvarsindustrien har for ivaretakelse av Forsvarets operative evne. Det er særlig der industrien leverer løsninger som ivaretar Norges spesielle nasjonale behov, og der den leverer relevant materiell, tjenester og kompetanse som sikrer at Norge bidrar inn i byrdefordelingen i NATO, at Forsvaret er avhengig av industriens kompetanse og kapasitet.[36]

Av norsk forsvarsindustris bidrag er særlig luftvernsystemet NASAMS (Norwegian Advanced Surface-to-Air Missile System), fjernstyrte våpenstasjoner, missilsystemene NSM (Naval Strike Missile) og JSM (Joint Strike Missile) og rakettmotorer til missiler, eksempler på relevant materiell og løsninger som er tilpasset nasjonale behov, og som derfor har sentral betydning for Forsvarets operative evne. Disse systemene har høyt innslag av digitale løsninger og teknologi, som igjen krever komponenter og kompetanse som i stor grad bare er tilgjengelig hos industrien. Videre er moderne kryptoteknologi et område der forsvarsindustrien leverer helt sentrale bidrag for å ivareta nasjonalt behov for skjerming av sensitiv informasjon.[37]

Forsvaret baserer seg også i stor grad på tilgang til ressurser fra det sivile markedet for å sikre nødvendig beredskap og forsyningssikkerhet. Sivilt næringsliv spiller en betydelig rolle i å understøtte forsvarssektoren i fred, krise og væpnet konflikt, innenfor rammen av totalforsvaret. Forsvaret er i dag avhengig av tilgang til nødvendig teknologi, kapasitet og kompetanse, bl.a. på IKT-området og innenfor logistikk.[38] Særlig er IKT-området et eksempel på et

[36] Kap 4.1 i Meld. St. 17 (2020-2021) Samarbeid for sikkerhet – Nasjonal forsvarsindustriell strategi for et høyteknologisk og fremtidsrettet forsvar
[37] Bla. Kap 4.5 i Meld. St. 17 (2020-2021)
[38] Se særlig kapitel 3.3 og 4.1 i Meld. St. 17 (2020-2021) Samarbeid for sikkerhet – Nasjonal forsvarsindustriell strategi for et høyteknologisk og fremtidsrettet forsvar

innovasjonsorientert og teknologikrevende område, der Forsvaret i mindre grad enn tidligere besitter kompetanse.

I 2018 ga derfor Forsvaret ut en digitaliseringsstrategi som beskriver en ambisjon der forsvarssektoren i langt større grad må tilpasse seg den raske utviklingen av teknologi for å sikre nødvendig operativ evne. Et resultat av strategien er at det blant annet pågår IKT-programmer i forsvarssektoren for å anskaffe sikre plattformer og etablere skytjenester og «kampnær IKT» til styrker på taktisk nivå. Dette skal bl.a. bidra til å etablere moderne og sikre kommunikasjonsløsninger på alle nivå i sektoren.[39]

Videre er moderne våpensystemer og kapasiteter i større grad høyteknologiske enn tidligere. De har et høyt innslag av digitale komponenter og software, samtidig som materialteknologi utvikles på helt nye måter. Teknologien som Forsvarets materiell og tjenester bygger på, er i økende grad identisk med teknologi utviklet for bruk i sivil sektor, selv om det ikke nødvendigvis vil være fullstendig overlapp.[40] Komponentene kan relativt enkelt brukes på andre måter, eller omprogrammeres slik at ytelsen økes eller reduseres. Eksempelvis er navigasjonssystemer og undervannssensorer i utgangspunktet like anvendelig til sivilt som militær bruk, f. eks til fartøy og personnavigasjon, der forskjellen kun er hvordan teknologien er integrert i Forsvarets systemer, eller at sensorene har en deteksjonskapasitet spesielt tilpasset militær bruk.

Fremover vil teknologiske gjennombrudd i sivil sektor kunne gi våpenplattformer og systemer økt rekkevidde, større ødeleggelsespotensial og bedre presisjon.[41] Bl.a. vil den økende digitaliseringen og utbygging av 5G nettet, fremveksten av tingenes internett («Internet of Things) og komplekse analyser av stordata endre Forsvarets mulighet til å forstå og analysere kompliserte situasjoner. Additiv tilvirkning (3D-printing) vil kunne bidra til å redusere logistikk og vedlikeholdsbehov av Forsvarets materiell, og på sikt kunne endre hvordan produkter produseres. Videre vil autonome systemer, og neste generasjons sensorer også bidra på flere nivåer i Forsvarets operasjoner. Nye tekstiler, syntetisk biologi, kunstig intelligens, kvantemaskiner er andre eksempler på teknologier som vil kunne få økende betydning for Forsvarets operative evne gjennom nye måter å kunne gjennomføre både nye og etablerte former for krigføring.[42] I tillegg har NATO trukket frem romteknologi og hypersoniske våpensystemer[43] som områdene der den teknologiske utviklingen vil by på utfordringer, men også store mulighetsrom for operativ evne og kapasitetsbygging.

NATO klassifiserer disse teknologiområdene som «emerging, disruptive and covergent» (EDT), og er basert på en analyse av hvilke teknologiske områder det vil være mulig å bruke militært, som samtidig fundamentalt vil endre måten militæraktivitet drives på. Dette gjelder både konkrete kapabiliteter, men også hvordan krigføring gjennomføres. Det legges i NATO-

[39] Kapittel 3.4 i Meld. St. 17 (2020-2021)

[40] Kapittel 4.2 om forskning og utvikling i det forsvarsindustrielle samarbeidet i Meld. St. 17 (2020-2021) Samarbeid for sikkerhet – Nasjonal forsvarsindustriell strategi for et høyteknologisk og fremtidsrettet forsvar

[41] Se b.la. «Teknologiske trender – muligheter og utfordringer for fremtidens forsvar» FFI (2020).

[42] Kapittel 3.4 i Meld. St. 17 (2020-2021) Samarbeid for sikkerhet – Nasjonal forsvarsindustriell strategi for et høyteknologisk og fremtidsrettet forsvar, «Teknologiske trenger – muligheter og utfordringer for fremtidens forsvar» FFI (2020) og «Emerging technology trends for defence and security» (2020), 20/01050, av Harald Erik Andås ved FFI.

[43] Kapittel 4, Conclusion, i NATO Science&technology trends 2020-2040.

rapporten bl.a. til grunn at endringene i det teknologiske landskapet, og hvem som er aktører på den militære arenaen, gjør at vi står ovenfor den syvende generasjon militære revolusjon.[44]

Etter departementets syn er en konsekvens av det teknologiske utviklingsbildet at kapasiteter som er sentrale for Forsvarets operative evne i stor grad er høyteknologiske, og at Forsvarets kapasiteter består, og fremover vil bestå, av komponenter og kompetanse som i stor grad kun er tilgjengelig hos sivil- og forsvarsindustri. Dette gjør at Forsvaret i økende grad er avhengig av kapasitet og kompetanse fra eksterne aktører for å kunne levere operativ evne. I tillegg vil kompetanse og utvikling fra sivile forskningsmiljøer få økt betydning for operativ evne, ved siden av etablerte militære forskningsmiljøer.

5.2.1.1 Forsvarsteknologi – varer, tjenester og teknologi som kan brukes til forsvarsformål

For å sikre forsvarssektoren nødvendig kontroll med den teknologien som har betydning for vår forsvarsevne ser departementet behov for å videreføre terskelen fra gjeldende lov[45], slik at all type teknologi som kan brukes til forsvaret av Norge kan omfattes av loven. Departementet ser også behov for at ny lov omfatter teknologi som ikke er en «oppfinnelse».

Departementet viser til beskrivelsen i forrige kapittel, og særlig til at moderne våpensystemer og militære kapasiteter i større og større grad er høyteknologiske og består av komponenter som også kan anvendes og utvikles sivilt. Det vil også være svært krevende å ha tilstrekkelig oversikt over de militære bruksområdene for moderne teknologi allerede på oppfinnelsesstadiet. Det gjelder særlig for de fremvoksende teknologiene. Teknologi vil utvikles sivilt, til i utgangspunktet sivile formål, av aktører som er kjent eller ikke kjent av forsvarssektoren. Samtidig som teknologien kan være like anvendelig til militære formål. Allerede kjent teknologi kan også settes sammen, eller virke sammen med annen ny teknologi, på måte som gjør at den kan få stor betydning for Forsvarets operative evne etter at den har blitt gjort tilgjengelig på markedet.

Etter departementets syn er det heller ikke hensiktsmessig at Forsvarets behov for kontroll med teknologi som har vesentlig betydning for operativ evne er avhengig av om den tradisjonelt er kategorisert som sivil teknologi, eller om den kan klassifiseres som en oppfinnelse. Etter departementets syn bør vedtakskompetansen være avhengig av teknologiens betydning for vår operative evne, heller enn om produktet er under utvikling, hvem som utvikler den eller om en aktør har valgt å holde oppfinnelsen hemmelig av kommersielle grunner.

Departementet legger imidlertid opp til at vedtakskompetansen bør brukes så tidlig som mulig i utviklingsløpet til teknologien, for at vilkår om krav til tiltak i teknologien vil kunne bli implementert med så lave kostnader som mulig. Se kapitel 9.2 og 9.3 for nærmere om hvilke vilkår, påbud og forbud som er aktuelle. Departementet viser her særlig til dagens samspill mellom myndighetene og industrien i forbindelse med implementeringen og forvaltningen av Strategi for beskyttelses av norskutviklet teknologi.[46] Se nærmere omtale i kapitel 9.1.3.

[44] Kapittel 2, Science&Techonolgy trends
[45] Se kapittel 5.1.2
[46] Boks 7.4 og 7.5, Mld. St. 17 (2020-2021)

For å nærmere konkretisere hvilke produkter som kan brukes til forsvarsformål har departementet sett hen til eksportkontrollregelverkets liste I og II[47]. Departementet foreslår en begrepsharmonisering, slik at ny lov vil omfatte varer, tjenester og teknologi, slik begrepene er definert i eksportkontrollregelverket.[48][49]Forslaget til ny lov vil da som utgangspunkt kunne omfatte de samme varer, tjenester og teknologi som følger av liste I og II.[50] Departementet viser til den grundige prosessen som gjennomføres før et produkt føres opp på listen, og ser listene som et hensiktsmessig utgangspunkt for den videre vurderingen av om produktet skal omfattes av lovforslaget.[51] Departementet foreslår derfor at den nye loven gjelder for «forsvarsteknologi» definert som «varer, tjenester og teknologi som kan brukes til forsvarsformål».[52]

Departementet presiserer imidlertid at selv om en konkrete vare, tjeneste eller teknologier er beskyttelsesverdige, vil ikke det nødvendigvis innebærer at alle varene, tjenestene eller teknologiene innenfor samme kategori på liste I eller II er beskyttelsesverdige. Det innebærer eksempelvis at to forskjellige typer raketter vil kunne falle inn under samme kategori på liste I, mens bare en av dem er beskyttelsesverdige. Det kan også tenkes tilfeller der et produkt ennå ikke har kommet på liste I eller II, men der betydningen teknologien har for Forsvarets operative evne gjør at den bør underlegges loven.

Departementet presiserer at begrepet «forsvarsteknologi» med dette også vil kunne omfatte koder, algoritmer, informasjon om produksjonsprosesser, metoder og kunnskap og teori knyttet til en teknologi («know-how»). Det vil også omfatte kunnskap i form av algoritmer, programmer og lignende som kan ha verdi som forsvarsteknologi i seg selv.

Departementet vil også bemerke at selv om det legges opp til en definisjon som er vid, er ikke hensikten at Forsvaret skal kunne sette begrensninger på all teknologi som Forsvaret kan bruke i sin virksomhet for å løse sine oppdrag. Et slik virkeområde vil være praktisk uhåndterbart å holde kontroll på, og de negative konsekvensene av et eventuelt vedtak ville heller ikke stå i forhold til den aktuelle teknologiens betydning for operativ evne og nasjonale sikkerhetsinteresser. Departementet legger derfor opp til at en vare, tjeneste eller teknologi må være beskyttelsesverdig, før den skal kunne underlegges bestemmelsene i loven, se kapitel 5.3.

Departementet legger opp til at de øvrige vilkårene fra gjeldende lov videreføres, det vil si at varen, tjenesten eller teknologien må være utviklet i Norge, eies av en enkeltperson eller virksomhet som holder til innenfor norsk jurisdiksjon, det må ha blitt søkt patent i Norge, eller virksomheten eller enkeltpersonen må ha helt eller delvis utnyttelsesrett til teknologien.

5.3 Beskyttelsesverdig forsvarsteknologi

Etter departementets syn er det kun de varene, tjenestene og teknologien som har vesentlig betydning for at Forsvaret skal kunne løse sitt samfunnsoppdrag, som bør kunne underlegges

[47] Vedlegg I og II til Forskrift om eksport av forsvarsmateriell (FOR-2013-06-19-718). Liste I ;https://lovdata.no/static/SF/sf-20130619-0718-01-09.pdf?timestamp=1637103644000, Liste II: https://lovdata.no/static/SF/sf-20130619-0718-02-07.pdf?timestamp=1637103644000

[48] Forskrift om eksport av forsvarsmateriell, flerbruksvarer, teknologi og tjenester (FOR-2013-06-19-718) § 2.

[49] Punkt 7.1 i Retningslinjer for Utenriksdepartementets behandling av søknader om eksport av forsvarsmateriell, samt teknologi og tjenester for militære formål av 28. februar 1992. https://www.regjeringen.no/no/tema/utenrikssaker/Eksportkontroll/dok_kontroll/id2554749/

[50] Vareliste I – Forsvarsrelaterte varer, og Vareliste II – Flerbruksvarer

[51] Se kapitel 4.2 for beskrivelse av prosessen før en vare, tjeneste eller teknologi blir ført opp på en av listene.

[52] Lovutkastet § 2 bokstav a

loven. Dette vil være de varene, tjenestene eller teknologien som det vil få konsekvenser for Forsvarets operative evne av et visst omfang, dersom Forsvaret mister kontroll over teknologien eller uvedkommende får tilgang til den. I Forsvaret operative evne inngår også teknologiens betydning for Norges forsvars- og sikkerhetssamarbeid med andre stater. Disse produktene ser departementet et klart behov for å holde tilstrekkelig kontroll med, både i utviklingsfasen, men også i forbindelse med deling av teknologien mellom virksomheter innenfor og utenfor norsk jurisdiksjon. Departementet presiserer at det er en nasjonal sikkerhetsinteresse at Forsvaret har tilstrekkelig kontroll med de innsatsfaktorene Forsvaret er avhengig av for å kunne opprettholde operativ evne.

Departementet forslår derfor at det må gjøres en konkret helhetsvurdering av hvor viktig produktet er for Forsvarets operative evne før det kan treffes vedtak om at teknologien er beskyttelsesverdig. Slik departementet ser det vil hensynet til Norges nasjonale sikkerhetsinteresser veie tyngre enn de eventuelle negative konsekvensene for eieren eller rettighetshaveren til produktet, og for eventuelle begrensinger i markedsadgangen for det aktuelle produktet, for de varer, tjenester og teknologi som har vesentlig betydning for Forsvarets operative evne.

5.3.1 Teknologiske kompetanseområder og vurderingskriterier

Hvilke type teknologi dette kan være, er i Meld. St. 17 (2020-2021)[53] kategorisert i åtte teknologiske kompetanseområder (TKO). Områdene er bestemt ut i fra relevans for Forsvarets kapabiliteter, det vil si Forsvarets evne til å utføre bestemte handlinger. De teknologiske kompetanseområdene angir hvor Forsvaret ser et behov for kompetanse innenfor norsk forsvarsindustri og der kompetanse hos industrien er et viktig bidrag til Forsvarets operative evne:

Kompetanseområde	**Beskrivelse**
Kommando-, kontroll-, informasjons-, kommunikasjons- og kampledelsessystemer	Systemer som skal bidra til situasjonsforståelse og støtte militære styrker i planlegging, disponering og gjennomføring av en operasjon i alle domener (land, sjø, luft, cyber og rommet). I disse aktivitetene står sikker behandling og overføring av data sentralt. Det kreves kompetanse på brukerutstyr, applikasjoner og tjeneste- og kommunikasjonsinfrastruktur.
Systemintegrasjon	Forsvarets operative evne bygger på samvirke mellom ulike systemer som igjen er satt sammen av samvirkende delsystemer. Systemintegrasjon omfatter også evnen til å velge og kombinere delsystemer på en slik måte at produktene samlet ivaretar Forsvarets behov. På produktnivå må kompetansen ses i sammenheng med evnen til å ha systemansvar for et produkt.

[53] Kapittel 7.3 - Meld. St. 17 (2020-2021) Samarbeid for sikkerhet – Nasjonal forsvarsindustriell strategi for et høyteknologisk og fremtidsrettet forsvar

Autonome systemer og kunstig intelligens	Et systems evne til å utføre oppgaver på egen hånd. Kunstig intelligens vil i praksis si datamaskiner som utfører oppgaver som tradisjonelt er blitt utført av mennesker. Anvendelsesområdene for kunstig intelligens blir stadig flere, hvorav autonome systemer er ett. Samhandling mellom autonome systemer og menneske er en viktig del av dette teknologiområdet.
Missilteknologi	Teknologien som er nødvendig for å få et missil til å fly mot et mål. Det inkluderer blant annet teknologi for målsøker, stridshode med eksplosiver, aerodynamikk, styring, navigasjon, kommunikasjonssystemer og integrasjon av missil på plattform. Kompetanseområde 2, Systemintegrasjon, utgjør vesentlig grunnlagskompetanse for missilteknologi.
Undervannsteknologi	Teknologi som understøtter alle typer undervannsoperasjoner, fra beskyttelse mot trusler, til innsats. Kompetanse på undervannskommunikasjon faller både inn under dette området og område 1. Kompetanseområde 2, Systemintegrasjon, er en vesentlig del av nødvendig kompetanse for dette kompetanseområdet.
Ammunisjon, rakettmotorer og militært sprengstoff	Kompetanse om objekter som skytes fra forskjellige våpensystemer og får nødvendig fremdrift og virkning i målet, og omfatter blant annet granater, prosjektiler, stridshoder og missiler. Teknologiområdet fokuserer på kompetanse innenfor energetiske materialer, utvikling av kjemiske komposisjoner, ballistikk, design av komplette produkter, samt produksjonsteknikk for disse.
Materialteknologi spesielt utviklet eller bearbeidet for militære formål	Anskaffelse av materialer og produksjonsprosesser for militære formål. Flere militære kapabiliteter bygger på materialteknologi som ikke er kommersielt tilgjengelig, og teknologiområdet har potensial for teknologisk overlegenhet innenfor flere av de øvrige områdene.
Levetidsstøtte for militære systemer	Forsyninger, reparasjoner, vedlikehold, utvikling, levetidsoppdateringer, lagring og avhending av materiell og systemer i forsvarssektoren. Programvare og applikasjoner spiller en stadig viktigere rolle for militært materiell og tjenester. På enkelte

	områder innebærer dette et skifte fra typiske midtlivsoppdateringer til kontinuerlige oppgraderinger og forbedringer. For mange militære systemer utgjør nå programvare en større kostnadskomponent enn det fysiske materiellet, og utviklingen synes å fortsette i denne retningen. Evne til kontinuerlig levetidsoppgraderinger av anskaffede systemer vil sannsynligvis bli stadig viktigere, og dette kompetanseområdet er slik sett tett knyttet til område 2, Systemintegrasjon

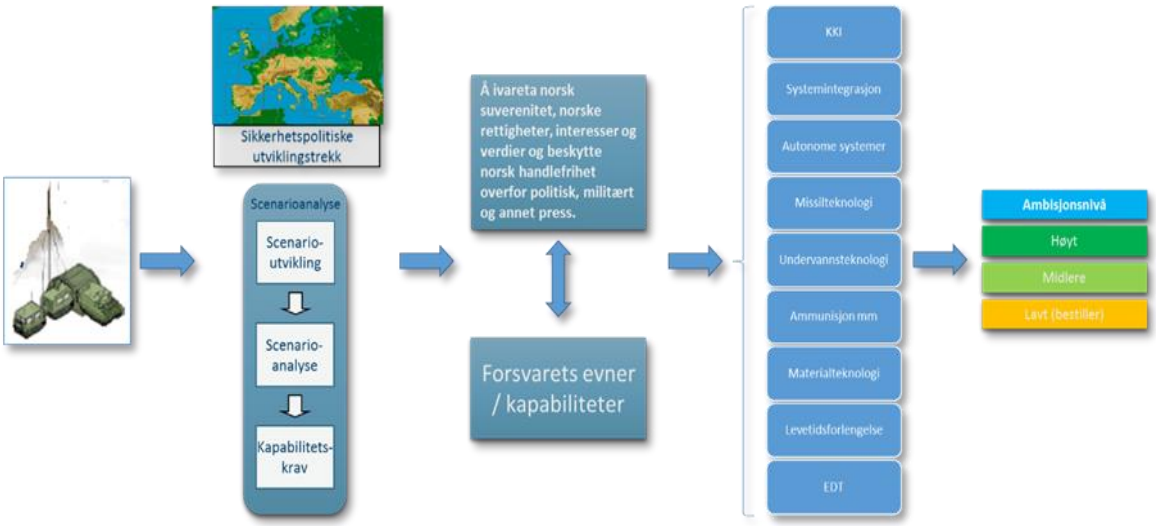
Departementet bemerker at som en naturlig følge av at de teknologiske kompetanseområdene er bestemt ut i fra relevans for Forsvarets kapabiliteter vil de være gjenstand for utvikling over tid.

I tillegg til teknologi som omfattes av de teknologiske kompetanseområdene, legger departementet til grunn at også teknologi som omfattes av begrepene «digital teknologi»[54] vil kunne omfattes av loven. Det vil bl.a. si stordata og analytiske verktøy, cyberteknologi, «edge»-prosessering, og ubemannede systemer, kunstig intelligens, autonomi, additiv tilvirkning, romteknologi, bioteknologi, og teknologi som omfatter bruken av det elektromagnetiske spekteret.[55] Disse teknologien vil fremover kunne få så stor betydning for Forsvarets operative evne at de må kunne underlegges ny lov. Departementet legger imidlertid opp til at det jevnlig skal gjøres en gjennomgang av de fremvoksende teknologien, for å vurdere om de teknologiske kompetanseområdene skal oppdateres.

Slik departementet ser det er det imidlertid ikke tilstrekkelig eller en forutsetning at en teknologi omfattes av et eller flere av kompetanseområdene. Det må også gjøres en vurdering av hvor viktig den aktuelle teknologien er innenfor et kompetanseområde. Eksempelvis vil beslutningsstøttesystemer, militær radiokommunikasjon og høygradert krypto være mye viktigere under *Kommando-, kontroll-, informasjons-, kommunikasjons- og kampledelsessystemer,* og derfor for operativ evne, enn eksempelvis fast kommunikasjonsinfrastruktur, «vanlige» kontorapplikasjoner, lavgradert krypto og forvaltningssystemer. Den første vurderingen kan illustreres slik:

[54] «Emerging technology trends for defence and security» (2020), 20/01050, av Harald Erik Andås ved FFI, og NATO-STO «Science and Technology Trends 2020-2040: Exploring the S&T Edge».

[55] «Emerging technology trends for defence and security» (2020), 20/01050, av Harald Erik Andås ved FFI, og NATO-STOrapporten «Science and Technology Trends 2020-2040: Exploring the S&T Edge».



Departementet legger videre opp til at det skal vurderes:

- I hvilken grad teknologien er tilpasset norske forhold
- Hvilke kapabiliteter teknologien understøtter og hvilken konsekvens tap av teknologien vil ha for operativ evne.
- I hvilken grad teknologien er tilgjengelig på markedet.
- I hvilken grad produktet gir forsvarspolitiske fordeler for Norge
- Hvor stor betydning teknologien har for beskyttelse av nasjonal sensitiv informasjon
- I hvilken grad teknologien gir kompetanse om hvordan komponenter virker sammen, og kan settes sammen til systemer, av betydning for operativ evne

I vurderingen av om produktet er *tilpasset norske forhold* må det vurderes om det gir Forsvaret operative kapasiteter som er unike eller svært fordelaktige. Det vil være relevant å se hen til om produktet er tilpasset norsk geografi, klima og topografi. Det vil også være relevant å vurdere om teknologien understøtter et annet produkt med disse egenskapene, eksempelvis gjennom vedlikehold og levetidsstøtte. Luftvernsystemet NASAMS, missilsystemene NSM og JSM, rakettmotorer til flere typer missiler og fjernstyrte våpenstasjoner er eksempler på teknologi som i dag ivaretar nasjonale behov, bl.a. som følge av styringssystemer tilpasset norske forhold.

Det må videre gjøres en vurdering av hvilke *konsekvenser tap av teknologien vil ha for operativ evne*. Det innebærer en vurdering av hvilke av Forsvarets kapabiliteter teknologien understøtter, og i hvilken grad tap av teknologien vil gi en potensiell motstander et overtak i en eventuell konflikt. Understøtter teknologien en sentral kapabilitet, samtidig som tap av teknologien vil kunne gi en motstander et overtak i en eventuell konflikt, taler det med tyngde for at teknologien er beskyttelsesverdig.

Departementet bemerker at det vil kunne være enkeltkomponenter eller deler av informasjon i teknologien som har så stor betydning for operativ evne at den er beskyttelsesverdig. Det må derfor tas stilling til om det er teknologien i seg selv eller deler av denne som har vesentlig

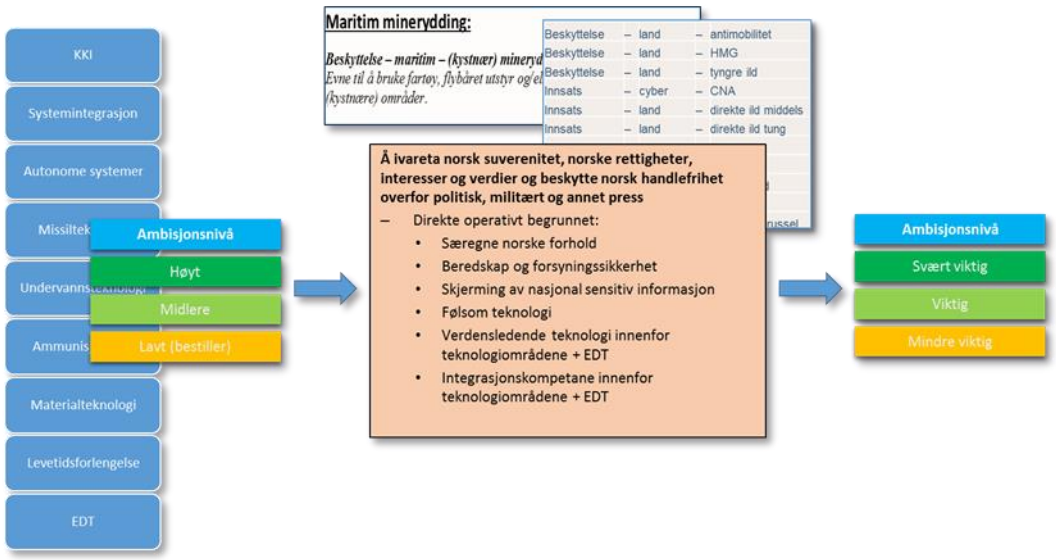
betydning, eller om betydningen for operativ evne er knyttet til algoritmer, software, teori, metoder eller en bestemt fremstillings eller produksjonsprosess.

Det er også relevant å se hen til i hvilken grad teknologien er *tilgjengelig på markedet*. Er teknologien ikke normalt tilgjengelig på markedet, eller kun i begrenset grad, kan det tilsi at det er behov for nasjonal kontroll med teknologien, og at teknologien derfor er beskyttelsesverdig.

Det må også vurderes om teknologien gir særlige *forsvarspolitiske fordeler*. I denne vurderingen inngår i hvilken grad det eksisterer tilsvarende løsninger på verdensmarkedet. Det er særlig der Norge har unik kompetanse og er verdensledende at det vil være forsvarspolitiske fordeler ved en teknologi.[56] Dette inkluderer en vurdering av i hvilken grad allierte bruker teknologien i sine kapabiliteter. Avhengig av hvilke forsvarspolitiske fordeler produktet gir, kan det tilsi at den bør underlegges nasjonal kontroll. Er produktet verdensledende vil det også potensielt kunne gi en motstander et overtak i en eventuell konflikt, dersom denne får kjennskap til teknologien. Motsetningsvis vil det at teknologien er lett tilgjengelig andre steder, eller at utvikling av teknologien er ivaretatt av det internasjonale markedet, være argumenter mot at teknologien gir oss forsvarspolitiske fordeler.

Det vil også være relevant å vurdere om det er *komponentene eller systemene i seg selv, eller kun kompetansen* om hvordan disse kan utvikles og settes sammen som har vesentlig betydning for operativ evne. Det må da vurderes hvilken betydning kompetansen har for Forsvarets kapabiliteter, og hvilke konsekvenser det vil ha dersom vi ikke har nasjonal kontroll med den aktuelle kompetansen.

Departementet bemerker at vurderingene over til dels vil overlappe hverandre, men vil sammen gi tilstrekkelig grunnlag for et vedtak om at en teknologi er beskyttelsesverdig.



[56] Kap 4.2 i Meld. St. 17 (2020-2021) Samarbeid for sikkerhet – Nasjonal forsvarsindustriell strategi for et høyteknologisk og fremtidsrettet forsvar

Eksempel

Et informasjonssystem som skal sikre kommunikasjon mellom to enheter i Forsvaret vil kunne omfattes av teknologiområdet kommando, kontroll og informasjonssystemer. Er systemet et kampledelsessystem, vil det være svært viktig innenfor kompetanseområdet. Har systemet egenskaper som gjør det særlig egnet til å operere under norske forhold, og er det kryptert med høygraderte løsninger vil det være vektige argumenter for at systemet er beskyttelsesverdig. Dersom den operative evnen blir skadelidende dersom systemet faller bort, eller blir kjent for en uvedkommende, tilsier det at systemet er beskyttelsesverdig. Det må imidlertid tas stilling til om det bare er selve krypteringsløsningen og kompetanse på hvordan komponentene i systemet er satt sammen som har disse konsekvensene, eller som det er nødvendig å ha nasjonal kontroll over. Krypteringsteknologien vil normalt ikke være åpent tilgjengelig på markedet, noe som også kan tale for at teknologien er beskyttelsesverdig.

Departementet har vurdert om det skal være forskjellige grader av beskyttelsesverdighet, på samme måte som de forskjellige graderingsnivåene for sikkerhetsgradert informasjon. På den ene siden vil en gradering kunne si noe om hvor viktig en teknologi er, og sånn sett kunne utgjøre et godt utgangspunkt for vurderingen av hvilke vilkår som er nødvendige for å begrense tilgang på de forskjellige nivåene.

Samtidig er terskelen for hvilke teknologier som er beskyttelsesverdige satt relativt høyt, etter en sammensatt helhetsvurdering. Sammenholdt med at det er stor fleksibilitet i vilkårene som kan stilles for å ha tilstrekkelig kontroll med teknologien[57], og at det kan tas hensyn til hvor viktig teknologien er når det sette vilkår for deling mv., har departementet foreløpig kommet til at forskjellige graderinger har begrenset merverdi.

Departementet foreslår at det er et vilkår for at det kan treffes vedtak om at en forsvarsteknologi er beskyttelsesverdig, at teknologien er utviklet i Norge eller eies av en enkeltperson eller virksomhet som holder til innenfor norsk jurisdiksjon, eller at det har blitt søkt patent i Norge eller virksomheten eller enkeltpersonen har helt eller delvis utnyttelsesrett til teknologien. Avgrensningen forutsetter at loven anvendes innenfor rammene av norsk jurisdiksjonsmyndighet etter folkerettslige regler. For å presisere at loven ikke kan anvendes i strid med Norges folkerettslige regler, har departementet derfor foreslått å innta et folkerettsforbehold i lovutkastet § 3 første ledd. Dette vil forhindre spørsmål knyttet til folkerettslige regler for jurisdiksjon, eksempelvis spørsmål om hvor en teknologi er utviklet eller hvor et selskap holder til i tilfeller hvor det er sivilt utviklede teknologier i regi av et selskap med kontorer i ulike land.

Departementet ber om høringsinstansenes syn på departementets forslag til klargjøring av forholdet til folkeretten gjennom et folkerettsforbehold eller hvorvidt folkerettsreglene som

[57] Se kapitel 9 om vedtak om vilkår for deling, bruk, utvikling og produksjon av beskyttelsesverdig forsvarsteknologi.

begrenser norsk jurisdiksjonsmyndighet og forutsetningen om at loven forutsettes anvendt innenfor rammene av folkeretten, istedenfor bør beskrives i lovens forarbeider.

Departementet foreslår at forskriftshjemmelen legges til Kongen, og at det som en del av forskriftsarbeidet vurderes om virkeområdet skal ytterligere konkretiseres med kriterier for når en teknologi er beskyttelsesverdig. Eventuelle kriterier bør være dynamiske, slik at de er egnet til å fange opp den raske teknologiske utviklingen.

5.4 Formål

Gjeldende lov om forsvarsviktige oppfinnelser har ingen egen formålsbestemmelse. I følge lovens forarbeider ble loven gitt for å sikre det offentlige hjemmel til enhver forføyning som er nødvendig for at en oppfinnelse av betydning for rikets sikkerhet skal komme rikets forsvar mest mulig til nytte (Ot.prp. nr. 62 (1952) s. 14).

Departementets vurdering er at angivelsen av lovens formål i forarbeidene langt på vei er dekkende også for lovforslaget. Formålet med lovforslaget er å sikre at Forsvaret også fremover har tilstrekkelig tilgang til, og kontroll med, de sentrale innsatsfaktorene som er nødvendige for å ivareta operativ evne og løse Forsvarets oppgaver. I tillegg er det sentralt at Forsvaret har kontroll med hvordan teknologi utvikles, slik at denne ikke utvikles til skade for operativ evne. Det er også sentralt å sikre at potensielle motstandere ikke får tilgang til teknologien, slik at Forsvaret mister strategisk overtak i en eventuell fremtidig konflikt.

Departementet foreslår at det tas inn en bestemmelse som presiserer lovens formål i § 1. Den vil kunne gi retning mot hvilke teknologier som blir omfattet av loven, og for hvilke vilkår det er aktuelt å knytte til en konkret teknologi.

Departementet foreslår at en ny lov har som formål å sikre at

- Forsvaret har tilstrekkelig tilgang til og kontroll med teknologi som har vesentlig betydning for operativ evne
- uvedkommende ikke får tilgang til slik teknologi
- norske forsvars- og sikkerhetsinteresser blir ivaretatt ved deling, utvikling og produksjon av og internasjonalt samarbeid om slik teknologi

Departementet presiseres at det ikke vil kunne utledes noen rettigheter eller plikter av formålsbestemmelsen, men bestemmelsen vil kunne gi veiledning i tolkningen av lovens øvrige bestemmelser.

6 Roller, ansvar og myndighet

6.1 Gjeldende rett

Myndigheten som er tillagt «Kongen» etter lov om forsvarsviktige oppfinnelser er delegert til Forsvarsdepartementet (FD) gjennom kgl. res. av 12. mars 1999.[58] FD kan, med unntak av

[58] Forskrift 12. mars 1999 nr. 242 Delegering av myndighet etter lov om oppfinnelser av betydning for rikets forsvar.

myndigheten i loven § 2 første ledd tredje punktum om fastsettelse av forskrift om hva som er å anse som krigsmateriell, delegere myndigheten videre.

Departementets myndighet er delegert videre til Forsvarets overkommando, jf. forskrift 9. mars 2000 nr. 215 om behandling av saker etter lov om oppfinnelser av betydning for rikets forsvar § 3 (heretter forskrift om forsvarsviktige oppfinnelser). Forsvarets overkommando ble nedlagt 1. januar 2003. Fra samme dato ble Nasjonal Sikkerhetsmyndighet (NSM) etablert som et direktorat som i dag er administrativt Justis- og beredskapsdepartementet, samt faglig underlagt Forsvarsdepartementet i saker innenfor departementets ansvarsområde.

Forskrift om forsvarsviktige oppfinnelser ble ikke endret ved nedleggelsen av Forsvarets overkommando. Myndigheten forskriften legger til Forsvarets overkommando er imidlertid siden 2003 utøvd av NSM. Dette oppdraget fremgår i dag av Hovedinstruks for Nasjonal sikkerhetsmyndighet (NSM) fastsatt av Justis- og beredskapsdepartementet og Forsvarsdepartementet den 3. mai 2019.

Gjeldende forskrift § 3 slår fast at Forsvarets Overkommando har myndighet til å:

a) Beslutte at en oppfinnelse skal gjøres kjent, jf. lovens § 2 andre ledd, første punktum og tredje ledd.
b) Forlenge fristen etter lovens § 2 andre ledd, andre punktum.
c) Gi tillatelser som nevnt i lovens § 3 andre ledd, første punktum.
d) Gi bemyndigelser som nevnt i lovens § 3 andre ledd, andre punktum.
e) Avgjøre om en oppfinnelse kan antas å være av betydning for rikets forsvar og kreve opplysninger som nevnt i lovens § 4.
f) Foreta ettersyn som nevnt i lovens § 5.
g) Treffe vedtak om avståelse til eie eller bruk for det offentlige eller andre, samt treffe øvrige vedtak om forbud og påbud etter lovens § 6.
h) Treffe vedtak om hemmelighold av patentsøknad og patent etter lovens § 7 første ledd, sjette punktum.
i) Bestemme at oppfinnelsen skal holdes hemmelig etter at patentet er trådt ut av kraft, jf. lovens § 7 første ledd, første punktum.
j) Oppheve vedtak og bestemmelse som nevnt i bokstavene g og h, jf. lovens § 7 andre ledd, første punktum.

Forskriften gir Forsvarets Overkommando myndighet til å beslutte at en oppfinnelse kan gjøres kjent for andre enn myndighetene involvert i vurderingen av oppfinnelsen eller når oppfinnelsen er underlagt rådighetsbegrensninger eller hemmelig patent. Forsvarets Overkommando kan også forlenge perioden med tre måneder for når en oppfinnelse er underlagt taushetsplikt i forbindelse med foreleggelse av oppfinnelsen til myndighetene. Videre er Forsvarets Overkommando gitt myndighet til å gjøre unntak fra forbudet mot bekjentgjøring og gi tillatelse til at rettighetshaver til oppfinnelsen kan få bistand av andre for å utforme dokumentasjonen til myndighetene eller patentsøknaden. Forsvarets Overkommando kan også gi tillatelse til at andre bistår eller utfører eksperimenter eller utprøving av oppfinnelsen når det er ønskelig av hensyn til rikets forsvar.

Etter anmodning fra Forsvarets Overkommando skal FFI og Patentstyret bistå i behandling av saker etter forskriften, jf. forskriften § 8. Når det er påkrevd, kan Forsvarets Overkommando også henvende seg til andre myndigheter, institusjoner eller personer for bistand.

Den 1. januar 2016 ble Forsvarsmateriell (FMA) opprettet som en egen etat under Forsvarsdepartementet med ansvar for materiellforvaltning og materiellinvestering i forsvarssektoren. Etaten ble skilt ut fra Forsvaret, inkludert deler av Forsvarets logistikkorganisasjon (FLO). Naturlig nok angir verken loven eller forskriften myndighet FMA har i forbindelse med lov om forsvarsviktige oppfinnelser.

FMA utleder i dag sitt ansvar knyttet til beskyttelse av forsvarsteknologi ut fra *Strategi for beskyttelse av norskutviklet forsvarsteknologi* (2018). FMAs rolle begrenser seg til vurderinger av deling av teknologi. FMA er forvaltningsansvarlig etat og kontaktpunkt for industrien, samt koordinerer med de øvrige etatene i forsvarssektoren og fremmer nødvendige tilrådninger til departementet.

6.2 Forslaget i høringsnotatet

Gjennomgangen over av hvilke aktører som etter gjeldende rett er delegert myndighet etter loven, viser at det er behov for å klargjøre de involverte myndighetenes roller, ansvar og myndighet ved forvaltningen av loven. Gjennomgangen viser også at det er behov for å klargjøre hvilke oppgaver de ulike aktørene skal ivareta.

Det er FD som har vedtatt og har det overordnede ansvaret for *Strategi for beskyttelse av norskutviklet forsvarsteknologi*. Kompetansen til å fatte vedtak om at en teknologi er beskyttelsesverdig i forslag til lov § 3, er en sentral del av loven og et sentralt virkemiddel ved selve operasjonaliseringen av forsvarsindustriell strategi.

Samtidig kan både vedtak om beskyttelsesverdighet, ileggelse av begrensninger og ekspropriasjon være svært inngripende for den vedtaket retter seg mot. Det er derfor departementets vurdering at myndigheten til å fatte vedtak om at en teknologi er beskyttelsesverdig, vedtak om tillatelse, påbud eller forbud og vedtak om ekspropriasjon og rett til utnyttelse bør ligge hos FD, jf. forslag til ny lov §§ 3, 5, 6, 7 og 8.

Gjennom *Strategi for beskyttelse av norskutviklet forsvarsteknologi* er det etablert en praksis for deling av teknologi og informasjon. FMAs ansvar for forvaltningen og vurderinger etter denne strategien, er nært beslektet med vurderingene etter lov om forsvarsviktige oppfinnelser.

Gjennom forvaltningen av strategien har FMA nærhet til industrien og relevante forskningsmiljøer, samt tett dialog med Forsvaret og FFI. FMA har dermed god kompetanse til å vurdere teknologi og beskyttelsesbehov. Det er derfor etter departementets syn naturlig å bygge på FMAs kompetanse og erfaring fra forvaltning av strategien og dermed forankre den eksisterende rollefordelingen etter strategien. FD foreslår at FMA får en saksforberedende og rådgivende rolle overfor FD hvor etaten får ansvar for å koordinere innspill fra andre berørte aktører (FFI, NSM og Forsvaret), saksbehandling og sende frem sektorens anbefaling til FD. At hovedansvaret for koordinering og saksforberedelse gis til én aktør vil også føre til mer effektiv saksbehandling.

Forsvaret og FFI vil ikke gis formelt ansvar eller myndighet etter loven, men vil være sentrale aktører i forbindelse med FMAs anbefalinger av beskyttelsesverdighet og begrensninger gjennom å gi råd og veiledning om teknologi og operative behov. Samtidig vil NSM kunne gi FMA råd i vurderingen av om en teknologi kan deles med andre, hvilke eventuelle tiltak som kan bidra til å redusere risiko for tap og bidra til å belyse risiko for og konsekvenser av tap av teknologi og kompetanse. NSM vil også kunne bidra med tilgang til relevante registre for vurdering av om det skal gis tillatelse til deling. Departementet legger opp til at FMA har tett

dialog med Forsvaret, FFI og NSM i forbindelse med sine utredninger og anbefalinger til departementet. For å få informasjon om aktuelle teknologier som kan være beskyttelsesverdig, må FMA også ha god dialog med Patentstyret og Utenriksdepartementet i saker om henholdsvis hemmelige patenter og eksportkontroll.

Videre vil NSM fungere som rådgivende organ i sikkerhetsspørsmål, og bistå virksomhetene som skal dele sikkerhetsgradert informasjon til fremmede stater etter virksomhetssikkerhetsforskriften § 25. I henhold til § 25 kan sikkerhetsgradert informasjon bare deles med andre stater dersom det er i samsvar med nasjonale sikkerhetsinteresser, ikke er i strid med lovbestemt taushetsplikt og det foreligger en sikkerhetsavtale mellom Norge og den aktuelle staten. Sikkerhetsavtalene Norge har med andre stater forvaltes av NSM.

Kryptoteknologi og -materiell er underlagt et særskilt forvaltningsregime. Etter sikkerhetsloven § 5-6 skal NSM godkjenne kryptosystemer som skal brukes for å beskytte sikkerhetsgradert informasjon. NSM har også en nasjonal forvalterrolle for dette materiellet og godkjenner leverandører av kryptosikkerhetstjenester, herunder industrielle utviklere og leverandører av kryptoteknologi. NSM skal også «godkjenne kryptoalgoritmer som brukes i utstyr som tenkes eksportert», jf. § 5-6 tredje ledd. Det innebærer at NSM må godkjenne deling av denne type teknologi før det kan gis tillatelse til deling med virksomheter i andre stater.

Der FMA inngår utviklings- og anskaffelseskontrakter med industrien knyttet til kryptoteknologi vil dette skje i en nær dialog med NSM. Ved vurderinger av om kryptoteknologi skal anses som beskyttelsesverdig forsvarsteknologi, vil NSM være den som besitter den beste faglige kompetansen til å fremme anbefaling om beslutning til FD. Departementet foreslår likevel at NSM sin rolle er begrenset til vurderinger av beskyttelsesverdig kryptoteknologi gjennom å gi råd til FMA ved vurderingen av om en teknologi er beskyttelsesverdig og hvilke begrensninger som eventuelt bør ilegges.

I de tilfellene hvor kryptoteknologi er integrert i våpensystemer og annet forsvarsmateriell, må FMA sørge for et nært samarbeid og dialog med NSM ved deling av forsvarsteknologi med andre land. Dette innebærer å ha dialog i forbindelse med NSMs godkjenningsprosess for kryptoalgoritmer og dialog for å avklare hvor grensen mellom kryptoteknologi og kryptoteknologi som er integrert i en teknologi, går.

All kryptoteknologi og -materiell NSM godkjenner for bruk til beskyttelse av sikkerhetsgradert informasjon, vil etter sin natur være skjermingsverdig etter sikkerhetsloven, og vil måtte håndteres og beskyttes i samsvar med bestemmelser i, og i medhold av, sikkerhetsloven.

7 Opplysningsplikt

7.1 Gjeldende rett

Gjeldende lov om forsvarsviktige oppfinnelser § 4 fastslår at

> «såfremt Kongen antar at en oppfinnelse er av betydning for rikets forsvar, kan han kreve fullstendige opplysninger om den av enhver som sitter inne med slike opplysninger».

Den gjeldende opplysningsplikten er vid og vil gjelde alle typer opplysninger fra alle som har opplysninger om oppfinnelser som antas å ha betydning for rikets forsvar. Bestemmelsen

pålegger imidlertid ingen selvstendig plikt for oppfinneren eller andre til å gi opplysninger, men forutsetter at myndighetene kjenner til oppfinnelsen og ber om at opplysningene utleveres.

7.2 Forslaget i høringsnotatet

7.2.1 Opplysninger som er relevante for vurderingen av om en forsvarsteknologi er beskyttelsesverdig

For å vurdere om en teknologi er beskyttelsesverdig må departementet kunne kreve alle relevante opplysninger om teknologien, bl.a. informasjon om hva teknologien skal brukes til, hva den kan brukes til, hvordan må den brukes for å oppnå resultater, hvilke testresultater teknologien har oppnådd, teknologiens operative og tekniske ytelse og hvilke bestanddeler teknologien består av, samt om det er bakenforliggende kunnskap som metodikk, prosesser eller annen kompetanse som er relevant for vurdere om produktet eller kunnskapen er beskyttelsesverdig.

Det foreslås derfor at adgangen departementet har etter gjeldende lov § 4 videreføres i forslag til § 4, men at det presiseres fra hvem disse opplysningene kan kreves fra. Slik departementet ser det bør hensynet til å ivareta nasjonal sikkerhet gå foran annen taushetsplikt fastsatt gjennom konfidensialitetsklausuler i kontrakter eller i lovs form. Det foreslås derfor at opplysningsplikten skal gjelde uavhengig av annen taushetsplikt.

Departementet har vurdert å pålegge en aktiv opplysningsplikt til den som gjør oppfinnelsen eller som eier teknologien, uten at vedkommende har fått en forespørsel om å fremlegge opplysningene fra forsvarssektoren. Gjennom de mange og omfattende kontaktflatene sektoren har med industrien, er mulighetene for å fange opp informasjon om teknologier som kan antas å omfattes av loven store. Forsvarssektoren får også informasjon om teknologi som kan være aktuell for beskyttelse gjennom UDs eksportkontrollmyndighet og Patentstyrets behandling av hemmelige patenter. Det fremstår derfor ikke som nødvendig å foreslå noen aktiv opplysningsplikt som går lenger enn dagens regelverk. Forsvarsmateriell (FMA) må imidlertid sørge for at det etableres gode rutiner for dialog med Patentstyret og UD slik at FMA får informasjon og mulighet til å vurdere teknologier det er søkt om hemmelig patent eller eksportlisens for.

På bakgrunn av dette foreslås det at den som eier, utvikler, bruker eller har tilgang til teknologi som forsvarsektoren antar er beskyttelsesverdig pålegges en opplysningsplikt dersom departementet ber om det.

7.2.2 Når departementet kan be om opplysningene

Vilkåret for å kreve opplysninger fra en virksomhet eller enkeltpersoner er at det må være «grunn til å tro» at teknologien er beskyttelsesverdig. Dette innebærer at departementet må sitte på opplysninger om teknologien som gjør det rimelig å anta at teknologien har betydning for Forsvarets operative evne, før det kan kreves opplysninger om teknologien. Eksempelvis gjelder dette dersom det er sannsynlig at teknologien faller innunder de til enhver tid gjeldende vedtatte teknologiske kompetanseområdene og vurderes å ha betydning for en av de seks prioriteringskriteriene som er beskrevet nærmere i kapitel 5.3.

7.2.3 Opplysninger som er relevante for vurderingen av om det kan gis tillatelse til deling

For å kunne vurdere om det skal kunne gis tillatelse til deling av beskyttelsesverdig forsvarsteknologi må det etter departementets syn kunne kreves opplysninger som er relevante for vurderingen av tilknytningen mellom virksomhetene og andre stater. Før det kan gis

tillatelse til deling må det gjøres en vurdering i hvilken grad virksomheten som mottar teknologien har tilknytning til andre stater. For å kunne gjøre denne vurderingen er departementet avhengig av å kunne hente inn opplysninger om eierstrukturen i virksomheten, hvilke eiere virksomheten har med hvilken innflytelse, og hvilken tilknytning eierne har til andre stater. For å legge til rette for en så effektiv informasjonsinnhenting som mulig foreslå departementet at opplysningene kan kreves både fra den virksomheten som ønsker å dele teknologi, og den som skal være mottaker av teknologien.

Når det gjelder hvilke opplysninger som er relevante har departementet sett hen til de opplysningene det skal opplyses om ved gjennomføringen av eierskapskontroll etter sikkerhetsloven, jf. sikkerhetsloven kapitel 10 og virksomhetssikkerhetsforskriften § 93. Departementet foreslår at utgangspunktet for innhentingen vil være:

- Mottakers navn, adresse og organisasjonsnummer, fødselsnummer eller tilsvarende nummer
- Organisasjonsnummeret til virksomheten som skal være mottaker av teknologien
- Mottakers eierstruktur
- Hvem som sitter i mottakers styre
- Hvem som inngår i daglig ledelse

Departementet foreslår at tas inn en begrensning i bestemmelsen for å sikre at kravet om opplysninger ikke går lengre enn det som er nødvendig for å vurdere om en tillatelse kan gis etter §§ 5 eller 6.

8 Taushetsplikt

8.1 Gjeldende rett

Taushetsplikt er regulert i loven § 2 første ledd:

> «Oppfinnelse som gjelder krigsmateriell eller som for øvrig har direkte betydning for rikets forsvar må ikke gjøres kjent for andre enn de i § 3 nevnte myndigheter dersom oppfinnelsen ikke allerede er alminnelig kjent. Oppfinner eller rettighetshaver må ikke på annen måte enn nevnt i § 3 foreta seg noe i hensikt å utnytte oppfinnelsen, eller noe som kan vanskeliggjøre forføyninger i henhold til § 6 (...).»

Etter loven er det forbudt å gjøre en forsvarsviktig oppfinnelse kjent for andre enn de myndighetene som er involvert i foreleggelsen av en oppfinnelse etter § 3. Dette er i dag Forsvarsdepartementet, Nasjonal sikkerhetsmyndighet (NSM), Patentstyret, FFI, samt patentkontorer som er leverandørklarert og godkjent for å yte bistand knyttet til søknader om patenter av oppfinnelser som faller inn under loven. Formålet med taushetsplikten er å sikre at en oppfinnelse som er av betydning for rikets forsvar ikke blir kjent for uvedkommende.

Taushetsplikten etter loven inntrer imidlertid først for oppfinnelser som gjelder «krigsmateriell», eller som forøvrig har «direkte betydning» for Forsvaret. Basert på ordlyden omfatter derfor taushetsplikten en snevrere krets oppfinnelser enn hva som omfattet av virkeområdet til loven, og adgangen til å kreve opplysninger og til å fastsette rådighetsbegrensninger.

Den som vil nyttiggjøre seg av en forsvarsviktig oppfinnelse, har plikt til å gi en fullstendig skriftlig beskrivelse av oppfinnelsen til NSM, eller søke om patent til Patentstyret dersom oppfinneren ønsker industrielt rettsvern for oppfinnelsen, jf. § 3.

Loven åpner for at NSM kan gjøre unntak for forbudet mot bekjentgjøring og gi tillatelse til at rettighetshaver henvender seg til andre for utarbeidelse av beskrivelsen til myndighetene, patentsøknaden eller for eksperimentering eller prøving av oppfinnelsen. Det kan også gis tillatelse til at andre enn rettighetshaveren utfører eksperimenter eller tester oppfinnelsen når det er ønskelig av hensyn til rikets forsvar.

Forbudet mot bekjentgjøring av forsvarsviktige oppfinnelser opphører når NSM bestemmer det. For oppfinnelser som er lagt frem for NSM eller Patentstyret gjelder forbudet likevel ikke lenger enn fire måneder etter foreleggelsen, eller ytterligere tre måneder dersom det på bakgrunn av særlige forhold anses nødvendig. Ved slik forlengelse har NSM plikt til å varsle rettighetshaver straks.

8.2 Forholdet til taushetsplikt etter sikkerhetsloven

Som nevnt i kapittel 4.1 er det departementets vurdering at informasjon om en teknologi som identifiseres som «beskyttelsesverdig» også vil være skjermingsverdig informasjon da «det kan skade nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig», jf. sikkerhetsloven § 5-1.

Sikkerhetsgradert informasjon skal bare overlates til personer som har tjenstlig behov og er autorisert for tilgang til slik informasjon, jf. § 5-4 første ledd. Ved tilgang til informasjon sikkerhetsgradert KONFIDENSIELT eller høyere må personellet også ha gyldig sikkerhetsklarering for det aktuelle graderingsnivå, jf. sikkerhetsloven § 8-1 andre ledd. Alle som får tilgang til sikkerhetsgradert informasjon som ledd i arbeidet eller tjenesten for en virksomhet som omfattes av loven, har taushetsplikt om innholdet, jf. § 5-4 andre ledd. Taushetsplikten gjelder også etter at arbeidet eller tjenesten er avsluttet.

En forutsetning for at private virksomheter skal kunne gis tilgang til, eller selv tilvirke, sikkerhetsgradert informasjon er at de er underlagt sikkerhetsloven. Der hvor beskyttelsesverdig forsvarsteknologi utvikles etter oppdrag fra forsvarssektoren vil dette gjennomføres som en sikkerhetsgradert anskaffelse, og leverandøren vil være underlagt sikkerhetsloven etter § 1-2 andre ledd. Dersom det fattes vedtak om at en teknologi, som en bedrift har utviklet av eget tiltak eller utenfor rammene av en sikkerhetsgradert anskaffelse, er beskyttelsesverdig, må Forsvarsdepartementet samtidig vurdere å fatte vedtak om at bedriften skal underlegges sikkerhetsloven etter §1-3 første ledd bokstav a.

Sikkerhetsloven § 5-2 siste ledd gir hjemmel til å kunne dele sikkerhetsgradert informasjon med andre stater. Nærmere bestemmelser er gitt i virksomhetssikkerhetsforskriften § 25 som fastslår at en fremmed stat kan gis tilgang til norsk sikkerhetsgradert informasjon dersom det:

- Er i samsvar med nasjonale sikkerhetsinteresser
- Ikke er i strid med taushetsplikt
- Foreligger en sikkerhetsavtale mellom Norge og den aktuelle staten

En sikkerhetsavtale kan være folkerettslig bindene, men kan også være en avtale/fellesforståelse (MOU) uten slike rettsvirkninger. Sikkerhetsavtaler kan videre være inngått generelt for statsforvaltningen eller ha et snevrere virkeområde avgrenset til forsvarssektorene eller et

konkret prosjekt. Sikkerhetsavtalene forplikter partene til å beskytte den andre parts sikkerhetsgraderte informasjon som egen informasjon med tilsvarende graderingsnivå, og fastsetter også prosedyrer for gjennomføring av sikkerhetsgraderte anskaffelser hvor leverandøren er lokalisert i den andre staten.

Det stilles videre krav om teknologisikkerhetsavtaler mellom FMA og ikke-statlige aktører som vil være involvert i håndtering av teknologien i et mottakerland. Slike avtaler pålegger aktørene å følge bilaterale sikkerhetsavtaler, graderingsnivå og pålegg gitt i graderingsspesifikasjon for den aktuelle teknologien.

8.3 Forslaget i høringsnotatet

Departementet foreslår at det etter ny lov § 3 kan fattes vedtak om beskyttelsesverdighet overfor forsvarsteknologi som har vesentlig betydning for Forsvarets operative evne. På bakgrunn av det legger departementet til grunn at informasjonen om teknologien, eller den delen av teknologien, som anses å være beskyttelsesverdig som den klare hovedregel vil være å anse som sikkerhetsgradert informasjon.

Sikkerhetslovens regler gjelder imidlertid bare for virksomheter som er underlagt loven. Det innebærer at frem til det eventuelt er fattet vedtak om at virksomheten som eier teknologien skal underlegges loven, vil ikke kravene om taushetsplikt, autorisasjon og klarering etter sikkerhetsloven gjelde. For å unngå at informasjon om teknologien kan deles mens det vurderes om den er beskyttelsesverdig, foreslås det i § 3 andre ledd at det kreves tillatelse fra departementet dersom teknologien skal deles med andre utenfor virksomheten. Det foreslås i tredje ledd at det bare er personer internt i virksomheten med tjenstlig behov som skal ha tilgang til informasjon som omhandler forsvarsteknologi. På den måten sikrer man at informasjon ikke kommer på avveie frem til man har ferdigbehandlet saken. Departementet har vurdert om det er behov for å gjøre klareringsregimet i sikkerhetsloven gjeldende for informasjon om teknologi som er til vurdering for beskyttelsesverdighet, men har kommet til at mekanismene som foreslås ivaretar hensynet til konfidensialitet i tilstrekkelig grad.

Det er derfor departementets vurdering at behovet for skjerme opplysninger om teknologien er ivaretatt av sikkerhetslovens regler og forslaget til § 3 andre og tredje ledd. På bakgrunn av det anses det ikke nødvendig med en egen bestemmelse om taushetsplikt.

Departementet foreslår imidlertid at det i lovforslaget § 10 andre ledd presiseres at departementet kan gi den som utvikler, eier, bruker eller har tilgang til beskyttelsesverdig forsvarsteknologi tillatelse til å be andre om bistand til en hemmelig patentsøknad.

8.3.1 Lukkede dører ved domstolsbehandling

Det følger av gjeldende lov § 8 at «i saker angående oppfinnelser som går inn under denne lov, kan retten bestemme at saken skal behandles for lukkede dører».

Departementet foreslår imidlertid å ikke videreføre gjeldende lov § 8 i ny lov. Som beskrevet i henholdsvis kapittel 4.1 og i 9.2 vil informasjon knyttet til beskyttelsesverdig forsvarsteknologi være sikkerhetsgradert. Departementet ser ikke behov for å videreføre egne regler for domstolsbehandling av informasjon om beskyttelsesverdig forsvarsteknologi, utover de som følger for domstolens behandling av sikkerhetsgradert informasjon. Det følger av tvisteloven § 22-1 første ledd at det ikke kan «føres bevis om noe som holdes hemmelig av hensyn til rikets sikkerhet eller forholdet til fremmed stat». Det følger imidlertid av andre ledd at Kongen likevel kan samtykke til at beviset føres.

Reglene for lukkede dører i forbindelse med domstolsbehandling følger i dag av tvisteloven § 22-12. Det følger av første ledd at «når et bevis omhandlet i dette kapittel føres med vedkommendes samtykke, skal retten pålegge de tilstedeværende taushetsplikt, hvis ikke samtykket bestemmer noe annet. Har retten pålagt taushetsplikt, skjer muntlig forhandling om beviset for lukkede dører».

Tvistelovens regler om bevisforbud innebærer at det som hovedregel ikke skal føres bevis som er sikkerhetsgradert. I tilfeller hvor dette likevel føres vil det pålegges taushetsplikt og skje bak lukkede dører. På bakgrunn av det er det departementets vurdering at tvistelovens regler i tilstrekkelig grad ivaretar behovet for å behandle sak som omhandler beskyttelsesverdig forsvarsteknologi bak lukkede dører.

9 Vedtak om tillatelse til deling, begrensninger på bruk, rett til utnyttelse og ekspropriasjon

9.1 Gjeldende rett

9.1.1 Vedtak om ekspropriasjon, rett til utnyttelse og begrensninger

Gjeldende lov om forsvarsviktige oppfinnelser § 6 gir hjemmel til å sette begrensinger på bruk, til å utnytte og til å overta eierskapet til en oppfinnelse. Det følger av bestemmelsen at:

> «Oppfinnelser som Kongen antar har betydning for rikets forsvar, kan etter bestemmelse av Kongen kreves avstått til det offentlige eller andre, når dette anses ønskelig for at oppfinnelsen kan komme forsvaret mest mulig til nytte. Det samme gjelder rett til å utnytte slik oppfinnelse for nærmere bestemt tid.
>
> I samme øyemed kan Kongen forby rettighetshaveren å råde over oppfinnelse som nevnt i første ledd på nærmere bestemt måte her i riket eller i utlandet, eller pålegge ham nærmere bestemte plikter i forbindelse med utnyttelsen. Forbud eller påbud etter dette ledd gjelder for den tid Kongen bestemmer.
>
> Forføyninger etter denne paragraf kan treffes også etter utløpet av den i § 2, annet ledd, nevnte frist. Avgjørelse om at det ikke vil bli truffet forføyninger, kan når som helst omgjøres.»

Det følger av lovens forarbeider (Ot.prp. nr. 62 (1952) s. 14) at bestemmelsen skal gi det offentlige hjemmel til enhver forføyning som er nødvendig for at en oppfinnelse som har betydning for rikets forsvar skal komme mest mulig til nytte for Forsvaret. Myndigheten som etter loven er tillagt «Kongen» er delegert til Forsvarsdepartementet, jf. forskrift 12. mars 1999 nr. 242 om delegering av myndighet etter lov om oppfinnelser av betydning for rikets forsvar.

Bestemmelsen første ledd gir departementet mulighet til å overta eierskapet til en oppfinnelse, og til å bestemme at oppfinnelsen skal kunne utnyttes av forsvaret i en avgrenset tidsperiode. Bestemmelsen annet ledd gir hjemmel til å forby visse former for bruk av oppfinnelsen, og pålegge plikter i forbindelse med bruken av oppfinnelsen. Forutsetningen for bruk av begge leddene er at det aktuelle tiltaket må anses ønskelig for at oppfinnelsen skal komme best mulig til nytte for forsvaret. Det innebærer slik departementet ser det at det er tilstrekkelig at tiltaket har som formål at oppfinnelsen skal komme best mulig til nytte for forsvaret.

Bestemmelsens innebærer at departementet bl.a. kan sette begrensninger på om en oppfinnelse kan deles med andre, hvem den kan deles med og hvordan den deles, bl.a. hvilke endringer som

må gjøres på oppfinnelsen før den kan deles. Det kan også stilles krav til hvordan oppfinnelsen kan brukes, utvikles eller produseres.

9.1.2 Avtale og eierskap

Forsvarssektoren har både rettigheter og eierskap til oppfinnelser og eksisterende teknologi gjennom avtaler med industriaktører. Avtalene inngås ved tildeling av økonomisk støtte til forsknings- og utviklingsprosjekter (FoU), gjennom utviklingskontrakter eller gjennom kjøp av ferdige varer og tjenester.

Støtten til FoU-prosjektene gis hovedsakelig gjennom rammetildelinger og gjennom brukerfinansiering. Gjennom avtalene om støtte stilles det vanligvis krav om royalties ved videresalg av sluttproduktet, full råderett over de immaterielle rettighetene eller andre tilsvarende gjenytelser for forsvarssektoren som skal sikre at forsvarssektoren får igjen for å sine investeringer.

I tillegg gir avtalene departementet mulighet til å bl.a. stille krav til hvilke formål en teknologi kan brukes, krav om taushetsplikt for deltakerne i utviklingsprosjektet, hvem som kan være deltakere i prosjektet og krav om at verken informasjon om teknologien eller selve teknologien kan deles uten samtykke fra departementet. Det kan også være aktuelt å sette vilkår for deling, og begrense hvem som kan være mottakere av teknologien.

De samme kravene kan stilles gjennom utviklingskontraktene med industrien. Dersom det er det økonomisk mest fordelaktige, og det beste for å ivareta forsvarssektorens behov, skal det inngås ikke-eksklusive lisensavtaler til produktene eller tjenesten som utvikles. Dette følger av Anskaffelsesregelverket for forsvarssektoren (ARF) kapitel 24 om rettigheter. Det kan også være aktuelt å erverve eiendomsretten eller inngå eksklusive lisensavtaler av samme hensyn, «eller det foreligger tungtveiende sikkerhetsbetraktninger, eksempelvis i henhold til lov og tilhørende forskrift om oppfinnelser av betydning for rikets forsvar, som utelukker at det inngås en ikke-eksklusiv lisensavtale.», jf. § 24-5.

Staten har eierandel i Kongsberg Gruppen og NAMMO med hhv. 50,001% og 50%. Det gjør at staten innenfor selskapsrettens rammer også har en viss kontroll over hvordan teknologien forvaltes, hvem som er eiere av teknologien og selskapet, og hvem som får utbytte fra salg av teknologien. Staten har også en viss kontroll med hvem som er eiere av selskapene gjennom sikkerhetslovens regler om eierskapskontroll.[59]

9.1.3 Strategi for beskyttelse av norskutviklet forsvarsteknologi (2018)

Forsvarsdepartementet fastsatte 21. november 2018 Strategi for beskyttelse av norskutviklet forsvarsteknologi. Hensikten med strategien er å bidra til nødvendig forvaltning og kontroll med utvikling, anvendelse og tilgang til teknologi som må beskyttes av hensyn til nasjonal sikkerhet og forsvarsmessige behov. Strategien er basert på forsvarssektorens eierskap og rettigheter til teknologi, og legges til grunn for vurderinger av hvem som kan få tilgang til teknologien og informasjon om denne, og eventuelt sette vilkår for slik tilgang. Begrensningene settes i dag i hovedsak ved eksport av teknologien. Forsvarsmateriell (FMA) forvalter strategien på vegne av Forsvarsdepartementet.

I vurderingen av hvilke land teknologien kan deles med, vektlegges flere forhold som:

[59] Kapitel 10 i Lov om nasjonal sikkerhet (sikkerhetsloven) av 1. juni 2018.

- I hvilken grad deling vil innebære risiko for å kompromittere vesentlige nasjonale eller allierte sikkerhetsinteresser.
- I hvilken grad deling vil kunne kompromittere Forsvarets operative evne.
- I hvilken grad deling vil medføre risiko for teknologilekkasje eller utvikling av motmidler.
- I hvilken grad deling vil kunne påvirke Norges sikkerhets- og forsvarspolitiske relasjoner til andre nasjoner, positivt eller negativt.
- I hvilken grad deling vil kunne gi Forsvaret operative fortrinn eller økonomiske gevinster.
- I hvilken grad deling vil kunne styrke Norges adgang til internasjonalt samarbeid om forskning, utvikling, produksjon og understøttelse av materiell og systemer.

Strategien legger til grunn at beskyttelsen av teknologien kan økes gjennom tiltak som begrenser tilgangen til og muligheten for uønsket utnyttelse av teknologien. Utover krav etter sikkerhetsloven kan det i tillegg stilles krav til at tilgang til teknologien, informasjon om teknologien, og hvilken informasjon som gis om funksjoner og bruksmåter, kan knyttes til konkrete virksomheter eller enheter.

Informasjon om teknologien som er sikkerhetsgradert skal beskyttes i tråd med kravene i sikkerhetsloven med forskrifter, jf. sikkerhetsloven §§ 5-3, 5-4 og virksomhetsikkerhetsforskriften kapittel 4. Graderingsnivået til teknologien er styrende for hvilke sikkerhetstiltak som skal implementeres. Begrensninger på tilgang ses i sammenheng med kravene i sikkerhetsloven, slik at disse virker samme på en hensiktsmessig måte. Graderingsnivået fastsettes i dag i dialog mellom industrien, FMA og NSM.

En forutsetning for at sikkerhetsgradert informasjon kan deles til andre stater eller til virksomheter i andre stater er også at vilkårene i virksomhetssikkerhetsforskriften § 25 er oppfylt. Bestemmelsen stiller bl.a. krav til at deling av sikkerhetsgradert informasjon ut av norsk jurisdiksjon er i samsvar med nasjonale sikkerhetsinteresser, og at det er inngått sikkerhetsavtale mellom Norge og den aktuelle staten. I tillegg må det inngås en sikkerhetsavtale for teknologien med virksomheten som skal motta den sikkerhetsgraderte informasjonen. Sikkerhetsavtalen for teknologien («teknologisikkerhetsavtalen») skal bl.a. inneholde hvilken informasjon som deles, graderingsnivået på informasjonen, hvilke krav som følger av den bilaterale sikkerhetsavtalen for beskyttelse av informasjonen, hvilke krav til sikkerhetstiltak som følger av sikkerhetsloven med forskrifter for det aktuelle graderingsnivået, og eventuelle krav som følger av graderingsspesifikasjon for den aktuelle teknologien. Avtalen regulerer normalt også hvem som skal føre tilsyn med at kravene er oppfylt. NSM er involvert i denne prosessen som forvalter av sikkerhetsavtalene Norge har med andre stater.

FMAs anbefaling vedrørende om en teknologi skal kunne deles i tråd med strategien oversendes FD for endelig avgjørelse. FDs svar på FMAs anbefaling videreformidles av FMA til industrien, med kopi til UD. Industrien legger ved FMAs svar når det søkes om eksportlisens til UD. FMA kontrollerer virksomheten har implementert nødvendige tiltak før eksport.

9.2 Forslaget i høringsnotatet

9.2.1 Behovet for videreføring av vedtakskompetansen fra gjeldende lov

Den teknologiske utviklingen gjør at moderne våpensystemer og militære kapasiteter i større grad er høyteknologiske, og at det i større grad er sivil- og forsvarsindustrien som har

rettighetene til og utvikler ny teknologi.[60] Det gjør at teknologi som har vesentlig betydning for operativ evne[61] helt eller delvis- kun er tilgjengelig hos private aktører. Med sikte på fortsatt utvikling eksporterer norsk forsvarsindustri i dag en rekke teknologisk avanserte produkter[62], og deltar på forsknings- og utviklingsprosjekter innenfor og utenfor Norges grenser.[63] Eksempelvis deltar norsk industri i flere initiativer i regi av det Europeiske forsvarsfondet (EDF).[64] Samtidig som dette bidrar til teknologisk utvikling, utgjør deling av teknologi, og informasjon om teknologien, en risiko for tap av teknologien. Tap av teknologien vil igjen kunne føre til at Forsvaret ikke lenger har tilgang til teknologien i samme grad, og at uvedkommende får tilgang til teknologien som gjør at den brukes eller utvikles på en måte som vil kunne skade Forsvarets operative evne.

Den teknologiske utviklingen gjør også at moderne våpen, informasjons- og overvåkningssystemer, og andre militære kapasiteter, i større grad enn tidligere består av komponenter som relativt enkelt kan settes sammen og justeres på for å påvirke systemenes yteevne. Det gjør at Forsvaret har økende behov for kontroll med hvordan teknologien brukes, utvikles, og produseres. For å sikre at teknologi er tilstrekkelig tilgjengelig for Forsvaret har det også betydning hvor produksjonen av teknologien skjer, og hvor kompetanse på utvikling av teknologien er tilgjengelig.

Sett i lys av at beskyttelsesverdig forsvarsteknologi har vesentlig betydning for Forsvarets operative evne, og for ivaretakelsen av Norges nasjonale sikkerhetsinteresser, ser departementet behov for å videreføre vedtakskompetansen som følger av gjeldende lov, men med noen presiseringer og endringer. Departementet har vurdert om det gir tilstrekkelig kontroll med teknologien at forsvarssektoren er medeier eller har rettigheter til teknologien. Slik departementet ser det vil det imidlertid være for stor usikkerhet knyttet til hva partene kan bli enige om gjennom avtalene til at avtale alene skal sikre ivaretakelsen av Forsvarets operative evne. Misligholdsbeføyelsene som er tilgjengelige ved avtalebrudd har heller ikke tilstrekkelig preventiv effekt, tatt i betraktning skadeomfanget for nasjonale sikkerhetsinteresser ved tap av teknologien, og at mulighetene til skadebegrensning er svært små.

Videre har erfaringene med begrensninger på deling og bruk med grunnlag i *Strategi for beskyttelse av norskutviklet forsvarsteknologi (2018*) vært gode. De vilkår som stilles hindrer at teknologien blir gjort tilgjengelig for uvedkommende, samtidig som forsvarsindustrien får eksportert produkter og dratt nytte av samarbeidsmuligheter i det internasjonale markedet. Det gir også en positiv markedsføringseffekt for industrien at teknologien er underlagt et strengt delingsregime, slik at risikoen for at uvedkommende har fått tilgang til teknologien er lav. Slik departementet ser det sikrer strategien en god balansegang mellom behovet for eksport og deling av teknologi, og behovet for å ha kontroll med at teknologi ikke kommer uvedkommende i hende. Strategien gir også kontroll med at teknologien deles og utvikles til det beste for operativ evne.

[60] Se kapitel 5.2 og 5.3 for beskrivelse av den teknologiske utviklingen, og om forholdet mellom teknologi utviklet i og utenfor forsvarssektoren.
[61] Se kapitel 5.3 om beskyttelsesverdig forsvarsteknologi.
[62] Meld. St. 35 (2020-2021) Eksport av forsvarsmateriell fra Norge i 2020, eksportkontroll og internasjonalt ikke-spredningssamarbeid, s. 9
[63] Bl.a. Meld. St. 17 (2020-2021) Samarbeid for sikkerhet – Nasjonal forsvarsindustriell strategi for et høyteknologisk og fremtidsrettet forsvar, kapitel 4.2.
[64] https://www.forsvarsfondet.no/

9.2.2 Tillatelse til deling av beskyttelsesverdig forsvarsteknologi

Etter departementets syn vil alle former for deling av teknologi og informasjon om teknologien medføre risiko for tap av teknologien. Størrelsen på risikoen, og konsekvensene av et tap av teknologien, vil avhenge av hvem teknologien deles med, og på hvilke vilkår. Samtidig kan deling av teknologi være en forutsetning for utvikling av teknologien. Eksport av teknologi, og deltakelse i internasjonale forsknings- og utviklingsprosjekter kan i tillegg bidra til påvirkning av Norges forsvars- og sikkerhetspolitiske forhold til andre stater.

9.2.2.1 Tillatelse til deling ved eksport

Departementet foreslår at vurderingen av om tillatelse til eksport bygger videre på dagens praksis etter strategi for beskyttelse av norskutviklet forsvarsteknologi, med noen justeringer. Departementet foreslår å tydeliggjøre at det skal gjøres en vurdering av risiko for tap av teknologien ved eksporten, hvilke tiltak som kan redusere risikoen for tap av teknologien, hvilke konsekvenser tap av teknologien vil ha for Forsvarets operative evne, og at disse vurderingene holdes opp mot fordelen eksport vil ha for Forsvarets operative evne. I vurderingen av fordeler for operativ evne inngår hvilke konsekvenser eksport vil ha for Norges forsvars- og sikkerhetspolitiske forhold til mottakerstaten eller andre stater.

For å vurdere risikoen for tap av teknologien ved eksport må det gjøres en sammensatt vurdering av mottakerstaten og virksomheten det skal eksporteres til. Departementet foreslår å tydeliggjøre at risikoen for tap av teknologien avhenger av:

- Etterretningstrussel
- Statlige styringsindikatorer
- Virksomheten i mottakerlandet
- Mottakerlandets og virksomhetens sikkerhetsmessige modenhetsnivå
- Forretningsstabilitet i mottakerlandet

Størrelsen på etterretningstrusselen avhenger graden av etterretningsvirksomhet fra andre stater mot mottakerstaten, og om eksporten vil føre til økt etterretningsvirksomhet mot norske interesser i mottakerstaten.

En vurdering av de statlige styringsindikatorene innebærer en vurdering av de politiske forholdene i staten, og i hvilken grad de politiske forholdene tilsier at det er en risiko for at teknologien blir gjort kjent for andre enn mottakeren av teknologien. Utgangspunktet for vurderingen er anbefalingene fra NSM[65], men med noen justeringer. Det vil være særlig relevant å se til hvilken tilknytning det er mellom staten og virksomheter i landet, f. eks om lovgivningen gir staten mulighet til å tilegne seg varer, tjenester og teknologi fra virksomhetene i staten. Det vil her være relevant å vurdere hvilke forsvars- og sikkerhetspolitiske samarbeid Norge har med den aktuelle mottakerstaten. Er samarbeidet med staten nært vil i utgangspunktet risikoen for tap av teknologien på grunn av de statlige styringsindikatorene være lav.

[65] Anbefaling om landvurdering ved tjenesteutsetting, Utgitt av Nasjonal sikkerhetsmyndighet (NSM) 11. september 2020. Tilgjengelig på nettsidene til NSM: https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/anbefaling-om-landvurdering-ved-tjenesteutsetting/statlige-styringsindikatorer/

Videre er det relevant å vurdere tilknytningen mellom virksomheten og styresmaktene i den aktuelle staten. Det innebærer en vurdering av eierforholdene i virksomheten som er mottaker av teknologien, hvilke styresammensetning og ledelse virksomheten har, hvilke personer som er ansatt i virksomheten og hvilke tilknytning det er mellom disse og styresmaktene i staten. I vurderingen av det sikkerhetsmessige modenhetsnivået vurderes cybersikkerhetstilstanden i mottakerstaten, og i virksomheten som er mottaker av teknologien.

Vurdering av forretningsstabilitet er en vurdering av i hvilken grad inngåtte avtaler respekteres i mottakerstaten, og hvor stor risiko det er for at teknologien blir delt med andre enn virksomheten i strid med gjeldende avtaler. Det innebærer bl.a. en vurdering av risikoen for korrupsjon, hvitvasking og habilitetsproblematikk.

Desto større risiko på et eller flere av disse punktene, jo større er risikoen for at teknologien kommer på avveie ved eksport til mottakerlandet. Departementet bemerker at dersom det kun er aktuelt å dele teknologi med en annen stats myndigheter, må vurderingen tilpasses deretter. Det vil fremdeles være relevant å vurdere etterretningstrusselen, de statlige styringsindikatorene, det sikkerhetsmessige modenhetsnivået, men ikke relevant å se hen til de øvrige momentene som går på vurderingen av virksomhetene som skal motta teknologien.

Risikoen for tap av teknologien eller uønsket utnyttelse kan reduseres gjennom at det settes vilkår om begrensninger på hvem informasjon om teknologien deles til, på hvilke tidspunkt og hvilken detaljeringsgrad det er på informasjonen det gis tilgang til. Det kan eksempelvis settes vilkår om at informasjonen kun kan gis til en eller flere personer i virksomheten, at det kun gis dokumentasjon eller opplæring som ikke opplyser om alle detaljene i teknologien. Det vil også kunne stilles vilkår om det kun gis begrenset tilgang til informasjon i markedsføring av et produkt, og at det kun gis full tilgang til kjøperen av produktet.

Det kan dessuten stilles vilkår om justeringer som skal begrense tilgang til informasjon om teknologien, f.eks krav til kryptering av programvare, krav om enkelte typer oppdateringer og konfigurasjoner, eller krav til bruk av konkrete komponenter. Det innebærer justeringer som gir varsler ved forsøk på å gjøre uautoriserte endringer i eller å dekonstruere teknologien

I vurderingen av den negative konsekvensen for Forsvarets operative evne foreslår departementet at det skal vurderes i hvilken grad Forsvaret mister operativ evne ved tap av teknologien, og da særlig om Forsvaret vil miste et strategisk overtak i strid. Det innebærer en vurdering av hvilke kapabiliteter teknologien understøtter, og hvilke konsekvenser det vil få for Forsvarets operative evne dersom en potensiell motstander får tilgang til teknologien. I vurderingen av negative konsekvenser må det også ses hen til om det kan settes vilkår om å gjøre justeringer som gjør det enklere å forsvare seg mot teknologien for Forsvaret.

Risikoen for tap av teknologien, og konsekvensen av et tap for operativ evne, må vurderes opp mot hvilke fordeler deling vil ha for operativ evne. I denne vurderingen vil det være relevant i hvilken grad deling vil gi mulighet til forbedring av teknologien, eksempelvis om deling vil kunne gi en styrket tilgang til internasjonalt forskning, utvikling, produksjon og understøttelse av materiell og/eller systemer. Det vil også være relevant om eksport vil bidra til interoperabilitet med allierte, og/eller vil utløse et markedspotensial for teknologien. Et stort markedspotensial vil kunne innebære økonomiske fordeler, som igjen kan bidra til utvikling av teknologien eller av ny og forbedret teknologi.

I vurderingen av fordeler ved delingen inngår også hvilke konsekvenser eksport vil ha for Norges forsvars- og sikkerhetspolitiske forhold til mottakerstaten eller andre stater. Det innebærer en vurdering av om eksport vil styrke eller svekke vårt forhold til mottakerstaten og/eller andre stater. Eksport til en stat vil kunne styrke forholdet til mottakerstaten, men samtidig svekke Norges forhold til andre stater.

Samlet er dette en kompleks helhetsvurdering, der det er utfordrende å si noe konkret om når tillatelse til eksport kan gis. Tillatelse vil avhenge av om fordelen med eksporten veier opp for risikoen for tap av teknologien og konsekvensene for operativ evne dersom teknologien likevel går tap. Generelt vil teknologi med høyt skadepotensiale for Forsvarets operative evne bare kunne deles der risikoen for tap av teknologi er lav, og fordelen for operativ evne eller samarbeid med andre nasjoner er høy. Dersom eksporten ikke gir fordeler for operativ evne, eller kun svært begrensede fordeler, vil det kun være aktuelt å akseptere lav risiko for tap av teknologien.

Departementet foreslår at utfyllende bestemmelser om tillatelse til å dele beskyttelsesverdig forsvarsteknologi ut fra norsk jurisdiksjon kan gis i forskrift, jf. lovforslaget § 5 siste ledd. Det innebærer bl.a. bestemmelser om vilkår for tillatelsen. Det vises til at den teknologiske utviklingen kan gjøre det nødvendig med detaljert regulering av deling av enkelte teknologier, f. eks detaljerte krav til justeringer av en konkret teknologi, eller andre typer vilkår, for enkelte mottakere. Denne type bestemmelser egner seg bedre i forskrift siden de sannsynligvis vil måtte endres med jevne mellomrom for å holdes oppdatert i takt med den teknologiske utviklingen.

9.2.2.2 Tillatelse til deling innenfor norsk jurisdiksjon

Departementet foreslår at det også kreves tillatelse for deling av beskyttelsesverdig forsvarsteknologi mellom virksomheter innenfor norsk jurisdiksjon. Departementet viser til at flere virksomheter med høy teknologisk kompetanse har bånd til stater som innebærer en risiko for at sensitiv informasjon og teknologi i praksis blir overført ut av norsk jurisdiksjon, uten at det gjøres en formell avtale om deling av teknologien. Eksempelvis der en virksomhet i Norge har et morselskap i en annen stat. Norske myndigheter vil i disse tilfellene ha svært begrenset mulighet til å få innsikt i overførselen. Delingen til virksomheter med bånd til andre stater vil særlig kunne være problematisk i de tilfellene båndet er til stater Norge ikke har et forvars- eller sikkerhetsmessig samarbeid med.

Departementet mener derfor at bør gjøres en samlet vurdering av risikoen for tap av teknologien, konsekvensene for operativ evne ved tap og hvilke fordeler overføring vil ha for operativ evne før det gis tillatelse til deling mellom virksomheter innenfor norsk jurisdiksjon.

Vurderingen av hvilken konsekvens et eventuelt tap av teknologien vil ha for Forsvarets operative evne vil være lik som gjennom deling ved eksport, se kapitel 9.2.2.1. I vurderingen av hvilken fordeler deling av teknologien vil ha for Forsvarets operative evne vil det i utgangspunktet ikke være relevant å vurdere om delingen styrker eller svekker vårt forhold til andre stater, ettersom andre stater ikke får tilgang til teknologien. Det kan tenkes unntak, der teknologien deles med et norsk datterselskap av et utenlandsk selskap, der teknologien som en del av den aktuelle transaksjonen blir gjort tilgjengelig for myndighetene i hjemstaten til selskapet.

I vurderingen av risikoen for tap av teknologien må det gjøres en vurdering av i hvilken grad virksomheten som skal motta teknologien har tilknytning til andre stater. Det innebærer en

vurdering av eierstrukturen i virksomheten, hvilke eiere virksomheten har med hvilken innflytelse, og hvilken tilknytning eierne har til andre stater. Vurderingen bør etter departementets syn bygge på de samme opplysningene det skal opplyses om ved gjennomføring av eierskapskontroll etter sikkerhetsloven, jf. sikkerhetsloven kapitel 10 og virksomhetssikkerhetsforskriften § 93. Det vil særlig være relevant å vurdere den samlede innflytelse personer i styret og ledelse har på driften av virksomheten, hvilken tilgang disse eventuelt vil ha til den beskyttelsesverdige teknologien, og i hvilken grad de har tilknytning til andre stater. I vurderingen av tilknytning er nasjonalitet og næringsinteresser i andre stater sentralt, og da særlig om disse båndene utgjør en risiko for at andre stater vil kunne få tilgang til teknologien.

Størrelsen på risikoen vil i stor grad avhenge av hvilken stat virksomheten har tilknytning til, og graden av etterretningsvirksomhet mot den aktuelle type virksomhet, og ansatte i virksomheten. Det vil være relevant å se hen til hvilke statsborgerskap de ansatte, og eventuelle konsulenter, i virksomheten har, og hvilken bakgrunnssjekk som allerede er gjort av disse. Normalt vil risikoen være mindre enn i motsatt tilfelle dersom Norge har et tett forsvars- og sikkerhetspolitisk samarbeid med staten.

Departementet legger også til grunn at det vil innebære en lavere risiko for tap av teknologien ved deling til en virksomheten med sterke bånd til norske myndigheter, eksempelvis der den norske stat har eierinteresser i virksomheten, eller der styret og daglig ledelse er norske statsborgere og/eller disse er sikkerhetsklarert.

På samme måte som ved eksport må det i vurderingen av risiko ses hen til hvilke vilkår som kan settes for delingen, som vil redusere risikoen for at teknologien går tapt. De samme vilkårene som fremgår av kapitel 9.2.2.1 vil kunne være aktuelle også når det deles innenfor norsk jurisdiksjon.

I vurderingen av fordelene ved deling vil det være særlig relevant å vurdere om overføringen vil kunne gi en styrket tilgang til forsknings-, utviklings- eller produksjonsmiljøer, eller føre til understøttelse av materiell og/eller systemer som vil kunne gi økt operativ evne. Det vil også være relevant å se hen til om overføringen vil bidra til interoperabilitet med allierte, og/eller vil utløse et markedspotensial for teknologien. Som ved eksport vil et stort markedspotensial kunne innebære økonomiske fordeler, som igjen kan bidra til utvikling av teknologien eller av ny og forbedret teknologi.

Samlet er også dette en kompleks helhetsvurdering, der det er utfordrende å si noe helt konkret om når det kan gis tillatelse til deling. Det avgjørende vil være om fordelen med delingen veier opp for risikoen for tap av teknologien, og negative konsekvenser for operativ evne ved tap av teknologien. Generelt vil teknologi med høyt skadepotensiale bare kunne deles der risikoen for tap av teknologi er lav, og fordelen for operativ evne er høy. Dersom overføringen ikke gir fordeler for operativ evne, eller kun i begrenset grad, vil det bare være aktuelt å tillate overføringen dersom risikoen for tap av teknologien er lav.

Departementet foreslår at utfyllende bestemmelser om adgangen til å dele beskyttelsesverdig forsvarsteknologi innenfor norsk jurisdiksjon kan gis i forskrift, jf. lovforslaget § 5 siste ledd. Det innebærer bl.a. bestemmelser om vilkår for tillatelsen. Det vises til at den teknologiske utviklingen kan gjøre det nødvendig med detaljert regulering av deling av enkelte teknologier, f. eks detaljerte krav til justeringer av en konkret teknologi, eller andre typer vilkår, for enkelte

mottakere. Denne type bestemmelser egner seg bedre i forskrift siden de sannsynligvis vil måtte endres med jevne mellomrom for å holdes oppdatert i takt med den teknologiske utviklingen.

9.2.3 Pålegg om eller forbud mot bruk, utvikling eller produksjon av beskyttelsesverdig forsvarsteknologi.

Moderne våpen, informasjons- og overvåkningssystemer, og andre militære kapasiteter, består i større grad enn tidligere av komponenter som relativt enkelt kan settes sammen og justeres på nye måter som kan påvirke systemenes yteevne. Software kan også relativt enkelt omprogrammeres slik at en bruksmåte eller utvikling av en teknologi reduserer effekten av Forsvarets våpensystemer, eller redusere yteevnene til sentrale informasjonssystemer.[66] Særlig er potensialet for utvikling, og skadepotensialet av utviklingen, stort og uavklart for de fremvoksende teknologiene.[67]

Dette gjør at Forsvaret har økende behov for kontroll med hvordan teknologien brukes, utvikles, og produseres, og hvem som får tilgang til teknologien. For å sikre at teknologi er tilstrekkelig tilgjengelig for Forsvaret har det også betydning hvor produksjonen av teknologien skjer, og hvor kompetanse på utvikling av teknologien er tilgjengelig. Departementet foreslår derfor å videreføre adgangen til å legge føringer på bruk og utvikling av beskyttelsesverdig forsvarsteknologi.

Departementets forslag innebærer en tydeliggjøring av at det kan settes begrensninger på hvor teknologien skal kunne brukes, utvikles eller produseres. Det vises til at beskyttelsesverdig forsvarsteknologi har vesentlig betydning for operative evne, jf. kapitel 5.3, og at det derfor vil kunne oppstå behov for å legge føringer som sikrer at teknologien i tilstrekkelig grad er tilgjengelig for Forsvaret, eller som sikrer at teknologien ikke blir tilgjengelig for potensielle motstandere i en eventuell fremtidig konflikt. Departementet legger til grunn at det vil kunne bli aktuelt å stille krav om at hele eller deler av kompetansen om eller utviklingskapasiteten av en teknologi er tilgjengelig innenfor norsk jurisdiksjon, selv om en industriaktør ønsker å flytte hele eller deler av produksjonen ut av landet. Departementet legger også til grunn at det vil kunne være aktuelt å sette denne type begrensninger for å oppfylle internasjonale- eller folkerettslige forpliktelser.

For å minske risikoen for at uvedkommende får tilgang til teknologien foreslår departementet at det også tydeliggjøres at det kan legges føringer på hvem som kan få tilgang til teknologien hos virksomheten. Departementet viser til at risikoen for tap av teknologien kan reduseres i betydelig grad dersom det stilles krav om at teknologien kun kan gjøres tilgjengelig hos en avdeling i virksomheten, eller at en virksomhet bare kan få tilgang til en delmengde av informasjonen, eller om at teknologien bare er tilgjengelig for personer med norsk statsborgerskap. Forutsetningen for at det sette begrensninger på tilgang er at de er nødvendige for å redusere risikoen for tap av teknologien, og at kravene ikke går lengre enn det som er nødvendig for å oppnå en akseptabel restrisiko.

Departementet foreslår at bruk av bestemmelsen er avhengig av om føringene er nødvendig for å ivareta Forsvarets operative evne eller hindre at utvikling eller bruk skjer i strid med Norges internasjonale- eller folkerettslige forpliktelser. Departementet vil understreke at bestemmelsen er ment som en «sikkerhetsventil», og at det må fremgå av begrunnelsen for å bruke

[66] Se kapitel 5.2.1 for en nærmere beskrivelse av det teknologiske utviklingsbildet.
[67] Se kapitel 5.2.1 for en nærmere beskrivelse av det teknologiske utviklingsbildet.

bestemmelsen at bruken er helt nødvendig for å ivareta disse hensynene. Det foreslås derfor at det følger av bestemmelsen at plikter eller forbud ikke kan gå lenger enn det som er nødvendig for å ivareta operativ evne eller internasjonale- eller folkerettslige forpliktelser. Departementet presiserer at en ønsket utvikling av en kapasitet først og fremst skal skje gjennom forsknings- og utviklingskontrakter.[68]

Departementet foreslår at utfyllende bestemmelser kan gis i forskrift. Den teknologiske utviklingen kan gjøre det nødvendig med detaljert regulering av enkelte teknologier. Denne type bestemmelser egner seg bedre i forskrift siden de sannsynligvis vil måtte endres med jevne mellomrom for å holdes oppdatert i takt med den teknologiske utviklingen.

9.2.4 Ekspropriasjon og utnyttelse i en avgrenset tidsperiode

Departementet foreslår å videreføre adgangen i gjeldende rett til å ekspropriere og til å utnytte en beskyttelsesverdig forsvarsteknologi i en avgrenset tidsperiode. Både ekspropriasjon og rett til å utnytte teknologien vil kunne være aktuelt der aktøren som har rettighetene til teknologien vil disponere over den på en måte som gjør at Forsvaret ikke lenger vil ha tilgang til teknologien i samme grad, eller det oppstår risiko for at uvedkommende kan ta i bruk teknologien på en måte som vil skade Forsvarets operative evne. En forutsetning for et vedtak om ekspropriasjon eller rett til å unytte teknologien bør imidlertid være at de øvrige virkemidlene beskrevet i kapittel 9.2.2 og 9.2.3 ikke reduserer risiko i stor nok grad, eller gir tilstrekkelig tilgang til teknologien.

Det kan for eksempel være aktuelt der rettighetene til teknologien, eller hele eller deler av en virksomhet, ønskes solgt til en utenlandsk aktør, og der salget medfører en betydelig svekkelse av aktørens kompetanse på teknologien. Det kan videre være aktuelt når et norsk firma legger ned virksomheten, og det er risiko for at teknologien overføres til uvedkommende mottakere i forbindelse med behandlingen av konkursboet. Det kan også være aktuelt når en bedrift overdras til utenlandske eiere, uten at ervervet stanses etter sikkerhetslovens regler om eierskapskontroll, eller der hvor en norsk eller utenlandsk eier planlegger å flytte produksjonen helt eller delvis til utlandet.

I disse tilfellene kan det bli aktuelt å overføre teknologien til en annen leverandør som kan videreføre produksjonen for å opprettholde Forsvarets operative evne. Det kan være en annen industriaktør eller en aktør i forsvarssektoren som gjennom ekspropriasjon eller rett til utnyttelse av teknologien i en avgrenset tidsperiode gis tilgang til teknologien.

Ettersom ekspropriasjon er et sterkt inngripende for rettighetshaver foreslår departementet å heve terskelen for å kunne gjøre inngrep fra «når dette anses ønskelig» i gjeldende rett, til når det er «nødvendig av hensyn til Forsvarets operative evne». Det innebærer at det må være en risiko for at teknologien eller kompetanse om denne ikke lenger vil være tilgjengelig for Forsvaret i tilstrekkelig grad, dersom teknologien ikke eksproprieres eller det gis en rett til å utnytte teknologien. Det foreslås også at vedtakskompetansen legges til Kongen.

9.3 Saksbehandling

9.3.1 Generelt

Departementet foreslår at myndigheten til å fatte vedtak om at en teknologi er beskyttelsesverdig legges til Forsvarsdepartementet (FD). Det foreslås også at FD tillegges

[68] Se kapitel 9.1.2 for en nærmere beskrivelse av forsknings og utviklingskontrakter.

myndighet til å fatte vedtak om tillatelse til deling av teknologien og om påbud eller forbud mot bruk, utvikling og tilgang til teknologien. Det foreslås at Kongen får myndigheten til å fatte vedtak om ekspropriasjon og rett til å utnytte en teknologi i en begrenset tidsperiode.

Det foreslås videre at Forsvarsmateriell (FMA) skal forberede saker og være rådgiver for FD i saker etter loven. FMA vil da ha ansvaret for å koordinere innspill fra berørte aktører og etater i forsvarssektoren, og fremme anbefaling til vedtak til FD. Departementet legger til grunn at FMA i denne rollen kan bygge videre på den tette dialogen med etatene i forsvarssektoren og industrien, som FMA har i rollen som forvalter av Strategi for beskyttelse av norskutviklet forsvarsteknologi.

Departementet foreslår at saksbehandling av saker etter lov om beskyttelsesverdig forsvarsteknologi i utgangspunktet gjøres i en todelt prosess. Først vurderes det om en teknologi er beskyttelsesverdig (trinn 1), deretter hvilke begrensninger som skal gjelde for håndteringen av teknologien (trinn 2).

For ferdigutviklet teknologi vil vurderingene normalt resultere i ett samlet vedtak, der det fremgår at en teknologi er beskyttelsesverdig og hvilke begrensninger som eventuelt gjelder for håndteringen av teknologien. For teknologier som er under utvikling vil vedtak om restriksjoner ofte måtte fattes etter vedtaket om at en teknologi er beskyttelsesverdig. Det kan være at ikke alle bruksområdene til teknologien er fullstendig kartlagt eller at det er for tidlig å beslutte hvordan risikoen for tap av teknologien bør reduseres når den deles. Dette kan også gjøre seg gjeldende for ferdigutviklet teknologi, f. eks der komponenter utvikles slik at funksjonaliteten til teknologien endres. I begge tilfeller vil det fattes ett nytt enkeltvedtak som må saksbehandles i tråd med prosessen skissert nedenfor i kapittel 9.3.2.

Det vil følge av vedtaket om at en teknologi er beskyttelsesverdig at det er forbudt å dele den uten tillatelse fra FD. Virksomheten må derfor søke om tillatelse fra FD uavhengig av hvem teknologien skal deles med, og om det skal deles til en virksomhet innenfor eller utenfor norsk jurisdiksjon.

Departementet legger til grunn at vedtak om at en teknologi er beskyttelsesverdig, og vedtak om tillatelse til deling eller pålegg eller forbud er å anse som enkeltvedtak etter forvaltningsloven § 2 første ledd bokstav b. Forvaltningslovens krav til saksforberedelse ved enkeltvedtak etter kapittel IV og krav til vedtaket etter kapittel V kommer derfor til anvendelse på saksforberedelsen av vedtakene, jf. forvaltningsloven § 3 første ledd.

At forvaltningslovens regler for enkeltvedtak kommer til anvendelse medfører blant annet at parten skal forhåndsvarsles før vedtak fattes (§ 16), at forvaltningsorganet har utrednings- og informasjonsplikt (§ 17) og at parten har partsinnsyn (§ 18). Videre skal enkeltvedtak som hovedregel være skriftlig og begrunnes, jf. §§ 23 og 24. Som en konsekvens av at informasjon om beskyttelsesverdig forsvarsteknologi vil være gradert etter sikkerhetsloven § 5-3, jf. § 5-4, vil dette medføre at hele eller deler av vedtaket graderes, avhengig av skjermingsbehovet for den enkelte teknologien.

Enkeltvedtak om at en teknologi er beskyttelsesverdig og vedtak om tillatelse til deling eller pålegg eller forbud, kan påklages til Kongen i statsråd av en part eller annen med rettslig klageinteresse, jf. forvaltningsloven § 28 første ledd.

9.3.2 Saksbehandling - vedtak om at en forsvarsteknologi er beskyttelsesverdig

Når det vurderes om en forsvarsteknologi er beskyttelsesverdig foreslår departementet at det skal gis melding til rettighetshaveren om at teknologien er til vurdering, jf. forslag til ny lov § 3 andre ledd. Vurderingen forutsetter tett dialog med den som eier eller er rettighetshaver til teknologien. Et krav om at det skal gis melding legger til rette for dialog samtidig som det sikrer muligheten for kontradiksjon for rettighetshaveren.

Meldingen skal inneholde en beskrivelse av hvilken teknologi som er til vurdering, og eventuelt en nærmere angivelse av hvilken del av teknologien som er omfattet av vurderingen (delkomponenter, prosessbeskrivelser, metodikk, «know how»). Meldingen bør også angi tidsfristen som ligger til grunn for vurderingen, at eier og rettighetshaver har opplysningsplikt om forhold som er relevante for vurderingen og hvilke midlertidige begrensninger som gjelder for teknologien mens den er til vurdering.

Etter at melding er sendt vil FMA vurdere hvorvidt teknologien er beskyttelsesverdig i tråd med de angitte vurderingskriteriene i lovforslaget § 3. Vurderingen innebærer koordinering med relevante aktører i sektoren som FFI, Forsvaret og NSM, som besitter nødvendig kompetanse om henholdsvis teknologi, Forsvarets operative evne og sikkerhetsgradert informasjon. For at FMA og departementet skal ha tilstrekkelig tid til å vurdere om forsvarsteknologien er beskyttelsesverdig foreslår departementet at saksbehandlingstiden for et vedtak om at teknologien er beskyttelsesverdig utvides til seks måneder med mulighet til å forlenge fristen med ytterligere seks måneder i særlige tilfeller.

Dersom FMA vurderer at det er grunnlag for å fatte vedtak om at en teknologi er beskyttelsesverdig, fremmer FMA anbefaling om at FD fatter vedtak i saken.

Dersom departementet har behov for tilleggsopplysninger for å vurdere om teknologien er beskyttelsesverdig, må det innen fem måneder fra melding er sendt fremsettes skriftlig krav om ytterligere opplysninger. Fristen avbrytes inntil svaret er mottatt.

Departementets forslag innebærer at det i utgangspunktet ikke er adgang til å dele teknologien med andre mens teknologien er til vurdering, og at det ikke gis tilgang til teknologien for andre enn de med tjenstlig behov for tilgangen, jf. § 3 andre og tredje ledd. Det innebærer at teknologien kan videreutvikles og brukes hos virksomheten i denne perioden. Deling av teknologien krever imidlertid tillatelse, og at hvem som får tilgang til teknologien skal begrenses i så stor grad som mulig. Departementet vil legge til rette for en prosess som i størst mulig grad av sikrer forutsigbarhet for virksomhetene involvert i vurderinger som gjøres etter loven.

Departementet foreslår at det av vedtaket om at en teknologi er beskyttelsesverdighet skal fremgå:

- hvilken teknologi, eventuelt hvilke deler av en teknologi, som er beskyttelsesverdig
- informasjon om at teknologien kan bli ekspropriert, eller utnyttet i et nærmere bestemt periode
- hvilke restriksjoner på bruk, utvikling eller deling av teknologien som gjelder for teknologien.
- rettighetshavers rettigheter og plikter, bl.a. klageadgang, erstatning og straffansvar.

9.3.3 Saksbehandling - vedtak om tillatelse til deling og vedtak om pålegg eller forbud

Når det er fattet vedtak om at en teknologi er beskyttelsesverdig kan den ikke deles uten tillatelse, jf. forslag til ny lov §§ 5 og 6. Departement legger opp til at FMA vil være kontaktpunkt også for søknader om tillatelse til deling, og at FMA fremmer anbefaling til FD om tillatelse kan gis, eventuelt på hvilke vilkår. FMA vil hente inn opplysninger fra åpne kilder, fra Etterretningstjenesten, FST, FFI og NSM til bruk i vurdering av om tillatelse kan gis. Det vil også være aktuelt å hente inn opplysninger fra virksomheten det skal deles til for å vurdere eierforhold og tilknytning virksomheten har til andre stater. Deling forutsetter at Norge har sikkerhetsavtale med mottakerstaten som dekker graderingsnivået på den sikkerhetsgradert informasjonen, og at NSM godkjenner sikkerhetsavtalen for den konkrete teknologien, jf. sikkerhetsloven § 9-2.

Et vedtak om tillatelse til deling skal opplyse om hvilke vilkår som er satt for delingen, og hvordan FMA skal involveres for å vurdere om vilkårene i tillatelsen er oppfylt. Det kan også gis tillatelse til deling samtidig som det treffes vedtak om at en teknologi er beskyttelsesverdig, forutsatt at det foreligger tilstrekkelig informasjon til å gjøre vurderingene beskrevet i 9.2.2.

Forøvrig gjelder saksbehandlingsreglene i forvaltningsloven for vedtak om tillatelse til deling, forbud eller påbud eller utnyttelse over en viss tid og ekspropriasjon. Det innebærer bl.a. at saken skal forberedes og behandles «uten ugrunnet opphold» og at saksbehandlingstiden tilpasses sakens kompleksitet, jf. forvaltningsloven § 11a. Det innebærer også at vedtak kan påklages til Kongen i statsråd, jf. forvaltningsloven § 28 første ledd.

9.3.4 Forholdet til Utenriksdepartementets behandling av søknader om eksport etter eksportkontrollregelverket

Departementet bemerker at Forsvarsdepartementets behandling av en søknad om tillatelse til deling etter forslag til ny lov, og Utenriksdepartementets behandling av søknader om eksport av forsvarsmateriell etter eksportkontrollregelverket, er ulike og selvstendige vurderinger som foretas på grunnlag av ulike kriterier, hensyn og regelverk. Lovforslaget endrer ikke at Utenriksdepartementet har det konstitusjonelle ansvaret for eksportkontrollen, og at det er Utenriksdepartementet som avgjør søknader om eksportlisens.

Den som skal eksportere beskyttelsesverdig forsvarsteknologi vil derfor ha et selvstendig ansvar for å innhente tillatelse fra Utenriksdepartementet etter eksportkontrollregelverket og tillatelse til deling[69] fra Forsvarsdepartementet. Forsvarsdepartementet vil i vedtaket om tillatelse til deling ta inn en henvisning til Utenriksdepartementet, og informasjon om å søke om eksportlisens før eksport. Utenriksdepartementet vil i sin saksbehandling ta inn at søkere skal opplyse om hvorvidt varen, teknologien eller tjenesten er beskyttelsesverdig og omfattet av lovforslaget, og hvorvidt det er fattet vedtak om tillatelse til deling.

Dette innebærer at virksomheten som ønsker å dele beskyttelsesverdig forsvarsteknologi med myndigheter eller virksomheter i en annen stat bør sende søknad om tillatelse fra FD så tidlig som mulig, og senest samtidig som søknad om eksportlisens sendes til UD. FDs vedtak om tillatelse til deling videreformidles av FMA til søker, med kopi til UD, slik at industriaktøren kan legge ved vedtaket i søknaden om eksportlisens til UD. Dersom FD kommer til at deling

[69] Se kapitel 9.2.2 om tillatelse til deling.

ikke kan tillates etter vurderingen beskrevet i kapittel 9, vil vurderingen foretatt av FD bli sett hen til i UDs behandling av søknaden om eksportlisens, slik beskrevet i kapittel 4.2.[70]

Departementet legger også til grunn at det vil kunne være tilfelle der FMA eller FD ikke har fanget opp en teknologi som det er grunn til å tro at vil være beskyttelsesverdig, og der FMA blir gjort oppmerksom på denne av UD gjennom behandlingen av en søknad om eksportlisens. Vurderingen av om teknologien er beskyttelsesverdig må da skje parallelt med at søknad om lisens behandles av UD, i tråd med saksbehandlingen beskrevet i kapittel 9.3.

For å sikre en mest mulig ryddig og forutsigbar saksbehandling vil det legges opp til tett koordinering og informasjonsflyt mellom UD og FD. Dette skal bl.a. bidra til mest mulig lik tilnærming til hvilke varer, tjenester og teknologi som omfattes av regelverkene, og til hvilke restriksjoner eller vilkår som er aktuelle for eksport til hvilke land.

Departementet vil også vurdere å lage en egen veileder til lov om beskyttelsesverdig forsvarsteknologi for å bl.a. tydeliggjøre virkeområdet til regelverket og forholdet mellom regelverkene dersom det viser seg å være nødvendig.

10 Erstatning

10.1 Gjeldende rett

10.1.1 Lov om forsvarsviktige oppfinnelser

Retten til erstatning ved ekspropriasjon og rådighetsbegrensninger etter gjeldende lov § 6, er regulert i § 9:

> «For forføyninger i henhold til § 6 betales erstatning som i mangel av minnelig overenskomst fastsettes ved skjønn. Skjønnet holdes av Oslo tingrett. Erstatningen kan fastsettes til en årlig avgift eller til en sum engang for alle. Skjønnet bestemmer hvor mange år avgift i tilfelle skal betales. Forføyningene kan iverksettes før erstatning er fastsatt eller betalt. Staten innestår for at erstatningen blir betalt selv om avståing kreves til andre.
>
> Erstatningen fastsettes ved skjønn også i den utstrekning rettighetshaveren etter alminnelige rettsgrunnsetninger måtte ha krav på erstatning for andre forføyninger etter denne lov.»

Rettighetshaver har etter ordlyden rett til erstatning for alle forføyninger i henhold til § 6. Det vil si at rettighetshaver har rett til erstatning dersom staten overtar eierskap til oppfinnelsen, dersom oppfinnelsen utnyttes av Forsvaret i en avgrenset tidsperiode, dersom noen former for bruk av oppfinnelsen blir forbudt og dersom det pålegges plikter i forbindelse med bruken av oppfinnelsen.[71]

Erstatning etter § 9 forutsetter imidlertid også at de øvrige alminnelige ulovfestede vilkårene for erstatning er oppfylt. For å få erstatning må rettighetshaver påvise at forføyningene etter loven § 6 har påført et økonomisk tap og at det er årsakssammenheng mellom forføyningene og det økonomiske tapet.

[70] Se kapitel 4.2 for beskrivelse av eksportkontrollregelverket og forholdet mellom regelverket og lovforslaget.
[71] Se kapitel 9.1.1 for en nærmere beskrivelse av hvilke forføyninger som er aktuelle etter gjeldende lov § 6.

Etter andre ledd kan rettighetshaveren også få erstatning for andre forføyninger etter gjeldende lov, dersom rettighetshaveren har krav på det etter alminnelige erstatningsrettslige regler. I forarbeidene vises det til forføyninger etter §§ 2, 3 og 7, dvs. tap som oppstår i forbindelse med krav om hemmelighold av oppfinnelsen og foreleggelsen for myndighetene. [72]

Erstatningens størrelse skal i begge tilfeller fastsettes enten gjennom avtale mellom partene eller ved skjønn. Departementet bemerker at det per i dag ikke er truffet vedtak med hjemmel i § 6, eller de øvrige bestemmelsene i loven, og det er derfor heller ikke utbetalt erstatning etter § 9.

10.1.2 Grunnloven § 105 og ekspropriasjonserstatningsloven

Retten til erstatning når staten overtar eiendomsretten til fast eiendom eller gjenstander følger av Grunnloven. Det følger av § 105 at «krev omsyn til samfunnet at nokon må gje frå seg sin faste eller rørlege eigedom til offentleg bruk, skal ho eller han få fullt vederlag av statskassa.». Bestemmelsen gir eier rett til full erstatning der staten overtar eiendomsretten til, eller bruker, en fast eiendom eller gjenstand.

I rettspraksis er det lagt til grunn at den økonomiske stillingen til den som må avstå eiendom ikke skal svekkes som følge av inngrepet. I Rt. 1976 s. 1 (Kløfta-dommen) la Høyesterett til grunn at «som utgangspunkt må budet om full erstatning innebære at en ekspropriat ikke skal stilles dårligere økonomisk ved at de beføyelser han som eier disponerer over, må avgis til eksproprianten.» (side 7).

Dette prinsippet ligger til grunn for bestemmelsene om utmåling av erstatningen ved ekspropriasjon i ekspropriasjonserstatningsloven.[73] Det følger av § 4 at ekspropriaten normalt skal ha erstattet den høyeste verdien av salgs- og bruksverdi. Beregningen av salgs- og bruksverdi følger av §§ 5 og 6. Salgsverdien beregnes med utgangspunkt i hva «vanlege kjøparar ville gje for eigedomen ved frivillig sal.», mens bruksverdi fastsettes med utgangspunkt i «avkastningen av eigedomen ved slik påreknelig utnytting som det er røynleg er grunnlag for etter tilhøva på staden.»

Det skal mye til før rådighetsbegrensinger gir rett til erstatning. Grunnloven § 105 gir i utgangspunktet kun rett til erstatning der staten overtar eierskapet, eller bruker, eiendommen eller gjenstanden. Basert på en analogisk anvendelse av Grunnloven § 105 er det i høyesterettspraksis (bla. Rt. 2005 s. 469) lagt til grunn at rådighetsbegrensninger kun i særlige tilfeller gir rett til erstatning, der rådighetsbegrensningen har klare likhetstrekk med ekspropriasjon. En rett til erstatning forutsetter at rådighetsbegrensningen har «en slik karakter at det ut fra en helhetsvurdering fremstår som sterkt urimelig om det skal tåles» (avsnitt 29).

Inngrepet i eiendomsretten må i denne sammenheng være *vesentlig* sett i forhold til gjenstandens utnyttelsesmuligheter. Det legges vekt på størrelsen av det økonomiske tapet til eier, i hvilken grad det fortsatt er praktisk og rettslig mulig å bruke gjenstanden for eier, og inngrepets størrelse og virkning i forhold til utnyttelsesmulighetene til den berørte eiendommen eller gjenstanden. Andre momenter i helhetsvurderingen er formålet med begrensningene, om inngrepet skjer i etablert eller planlagt bruk, og i hvilken grad det er foretatt investeringer på eiendommen eller i gjenstanden.

[72] Ot.prp.nr. 62 (1952) s. 6.
[73] Lov 6. april 1984 nr. 17 om vederlag ved oreigning av fast eigedom [ekspropriasjonserstatningslova].

10.2 Forslaget i høringsnotatet

10.2.1 Erstatning ved ekspropriasjon og ved vedtak om rett til utnyttelse i en nærmere bestemt periode

Departementet foreslår å videreføre retten til erstatning ved ekspropriasjon og ved rett til utnyttelse av beskyttelsesverdig forsvarsteknologi, for å tydeliggjøre eiers grunnlovfestede rett til erstatning for beskyttelsesverdig forsvarsteknologi, jf. Grunnloven § 105. Departementet foreslår at utmålingen tar utgangspunkt i de samme prinsippene som følger av ekspropriasjonsretten, slik at ikke ekspropriaten stilles i en dårligere økonomisk stilling ved avgivelse av teknologien. Det innebærer at den høyeste verdien av bruks og salgsverdien legges til grunn for utmålingen, i tråd med prinsippene i ekspropriasjonserstatningslova §§ 5 og 6.

Størrelsen på salgs- og bruksverdien må avgjøres etter en konkret helhetsvurdering. For fastsettelse av salgsverdien må det ses hen til hva tilsvarende teknologi selges for. Det må bl.a. tas høyde for hvilke utviklingstrinn teknologien er på og hva som gjenstår før teknologien er salgbar. Utmåling av bruksverdi vil måtte ta utgangspunkt i hva som er en påregnelig utnyttelse av teknologien for virksomheten. Det innebærer en vurdering av utnyttelsespotensialet til de immaterielle rettighetene til produktet, inkludert verdien av eventuelle royalties til teknologien. Der det fattes vedtak om rett til å utnytte en teknologi i en nærmere bestemt periode vil det på samme måte som over gjøres en konkret helhetsvurdering for å komme frem til hva som er markedsverdien for tilsvarende utnyttelsesrett for sammenlignbar teknologi.

Departementet foreslår at erstatningens størrelse fastsettes enten ved avtale eller ved skjønn ved Oslo tingrett hvis det ikke oppnås enighet mellom partene.

10.2.2 Erstatning når det ikke gis tillatelse til deling, legges begrensninger på bruk eller legges føringer for tilgang til og utvikling av teknologi

Departementet foreslår at det bare gis rett til erstatning for vedtak om å ikke gi tillatelse til deling, eller vedtak om pålegg eller forbud, der rett til erstatning følger av den alminnelige læren om erstatning for rådighetsbegrensninger i ekspropriasjonsretten. Etter departementets syn vil dette tilpasse retten til erstatning til den rettsutvikling som har vært siden gjeldende lov trådte i kraft, i tillegg til at det vil harmonisere retten til erstatning med regelverket til de andre nordiske landene. Det innebærer at virksomhetene bare har rett til erstatning der vedtaket vil kunne likestilles med ekspropriasjon. Det vil kunne være tilfelle der det vil være sterkt urimelig at den aktuelle begrensningen skal tåles.[74] Det vil bero på en konkret helhetsvurdering av om den aktuelle begrensingen gir en vesentlig reduksjon i virksomhetens mulighet til å utnytte teknologien.

Etter departementets syn vil det i vurderingen være relevant å se hen til størrelsen av det økonomiske tapet som følge av begrensningen, og i hvilken grad det fortsatt er praktisk og rettslig mulig for virksomheten å utnytte teknologien. Det vil også måtte ses hen til inngrepets størrelse og virkning i forhold til utnyttelsesmulighetene til teknologien. Hva som er formålet med begrensningene, i hvilken grad begrensingene gjør inngrep i planlagt eller etablert bruk, og i hvilken grad det er gjort investeringer i teknologien, vil også være relevant i vurderingen.

[74] Se beskrivelsen av rettstilstanden i kapitel 10.1.2.

Departementet legger imidlertid til grunn at det i de langt fleste tilfeller ikke vil bli tilkjent erstatning for disse vedtakene. Dersom departementet avslår en søknad om å dele teknologien vil det normalt fremdeles eksistere et restmarked for teknologien, slik at vedtaket vanskelig vil kunne likestilles med ekspropriasjon i tråd med momentene over. Der vedtaket innebærer at det ikke eksisterer noe restmarked kan erstatning likevel være aktuelt, basert på en konkret vurdering etter momentene over.

Det vil heller ikke normalt gis erstatning der det legges begrensninger på bruk av, tilgang til eller utvikling og produksjon av teknologien. Etter departementets syn vil rett til erstatning kunne være aktuelt der teknologien ikke lenger kan brukes til det den var utviklet for, med tilhørende økonomisk tap for virksomheten. Rett til erstatning vil også kunne være aktuelt dersom begrensninger på utvikling eller produksjon fører til et så varig og stort økonomisk tap at videre utnyttelse av teknologien ikke er mulig, eksempelvis der krav om at produksjonen må skje innenfor norsk jurisdiksjon fører til et stort økonomisk tap for virksomheten. Departementet understreker imidlertid at rett til erstatning i tilfellene avhenger av en konkret helhetsvurdering i tråd med momentene skissert over.

Departementet bemerker at et vedtak etter dette lovforslaget har klare likhetstrekk med et vedtak etter sikkerhetsloven. Departementet viser i den forbindelse til sikkerhetsutvalgets vurdering i utredningen av ny sikkerhetslov i NOU 2016:19 i kap 7.7.8 på s. 143:

> «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 fremstå som sterkt urimelig verken overfor allmennheten eller for den vedtaket retter seg mot. (...) Forholdet til Grunnloven, den europeiske menneskerettighetskonvensjonen (EMK) med videre, bør vurderes konkret i det enkelte tilfelle der det blir aktuelt å bruke bestemmelsen.»

Etter departementets syn er formålet med et vedtak om pålegge begrensinger på utnyttelse av teknologi det samme som et vedtak etter sikkerhetsloven. Et vedtak om å pålegge begrensninger vil være begrunnet i behovet for beskyttelse av Forsvarets operative evne, som igjen er en av våre nasjonale sikkerhetsinteresser. Slik departementet ser det vil et vedtak som er begrunnet i hensynet til nasjonal sikkerhet kun helt unntaksvis være sterkt urimelig for den det retter seg mot. Dersom virksomheten nektes å dele teknologien vil hensynet til nasjonal sikkerhet normalt gå foran utnyttelsen av virksomhetens kommersielle rettigheter.

11 Hemmelige patenter

11.1 Gjeldende rett

Lov 15. desember 1967 nr. 9 om patenter (patentloven) og lov om forsvarsviktige oppfinnelser gjennomfører de internasjonale forpliktelsene og gir utfyllende regler om saksbehandlingen.

Norsk patentrett er harmonisert internasjonalt og basert på flere internasjonale konvensjoner vedtatt av Verdens immaterialrettsorganisasjon (WIPO), Verdens handelsorganisasjon (WTO), Den europeiske patentorganisasjonen og NATO. De viktigste internasjonale konvensjonene Norge er bundet av på patentområdet er Den europeiske patentkonvensjonen (EPC) og Patentsamarbeidskonvensjonen (PCT), som er implementert i norsk rett i henholdsvis patentloven kapittel 10a og kapittel 3, og WTOs avtale om handelsrelaterte sider ved immaterielle rettigheter (TRIPS-avtalen). TRIPS-avtalen stiller visse minimumskrav til det

vern av immaterielle rettigheter som medlemsstatene plikter å innarbeide i sin lovgivning og beskytter blant annet patenter, varemerker og åndsverk mot bruk eller kopiering uten tillatelse.

Gjennom WIPO har 153 medlemsland tilsluttet seg PCT. Konvensjonen gir statene som har tilsluttet seg avtalen rett til å inngi internasjonal patentsøknad som gjelder tilsvarende i alle statene som har sluttet seg til konvensjonen, jf. artikkel 3. Videre gir konvensjonen felles regler om søknadens utforming og håndtering.

Videre er Norge og 37 andre land medlemmer av Den europeiske patentorganisasjonen som har grunnlag i Den europeiske patentkonvensjonen (EPC). Konvensjonen gir rett til søknad om og meddelelse av europeiske patenter som har samme virkning i alle medlemsland, herunder Norge, jf. artikkel 2.

Både etter PCT og EPC har medlemsstatene likevel adgang til å gjøre unntak for patentsøknader av hensyn til nasjonale sikkerhetsinteresser. PCT artikkel 27 slår blant annet fast at avtalen ikke begrenser medlemsstatenes adgang til å "apply measures deemed necessary for the preservation of its national security". Tilsvarende sikkerhetsunntak er fastslått i EPC artikkel 21 som gir medlemsstatene rett til å ta «alle precautions necessary in the interests of its security».

Samtidig er Norge gjennom EØS-avtalen forpliktet av EU-forordningene 469/2009 og 1610/96 om forlenget beskyttelse og direktiv 98/44/EU om bioteknologiske oppfinnelser. I bilaterale frihandelsavtaler der Norge er part, er patentrett også en sentral del av bestemmelsene om immaterialrett.

Som nevnt i kapittel 3.3. åpner NATO-avtalen "Agreement for the mutual safeguarding of secrecy of inventions relating to defence and for which applications for patents have been made" (1960) for deling av sikkerhetsgraderte patenter mellom NATO-land. I henhold til avtalen er Norge forpliktet til å beskytte og sikkerhetsgradere patenter på samme måte som opprinnelseslandet. Videre gjelder også hemmeligholdelse av informasjonen i patentet i Norge. På samme måte skal Norge sørge for at patenter om forsvarsteknologi utviklet her har riktig graderingsnivå, og sørge for at slike patentsøknader kan, etter samtykke fra Forsvarsdepartementet, videreføres til andre NATO-land.

Vilkårene for patentbeskyttelse er fastsatt i patentloven §§ 1 til 2. For at en oppfinnelse skal ha patentbeskyttelse må det leveres en søknad på oppfinnelse som kan anvendes industrielt, jf. patentloven § 1 første ledd. Videre må oppfinnelsen være ny og skille seg vesentlig fra det som er kjent, jf. § 2 første ledd, og ikke være utelukket fra beskyttelse, jf. § 1 fjerde til sjette ledd og §§ 1 a og 1 b.

En patentsøknad offentliggjøres i Norsk Patenttidende 18 måneder etter at søknaden er levert eller fra prioritetsdagen for søknaden, jf. patentloven § 22 andre ledd første punktum. Dette skal tilrettelegge for at allmennheten kan skaffe seg kunnskap om hva som er patentsøkt, unngå å gjøre inngrep i andres teknologi, men også kan lære av og utvikle teknologien videre. Patentstyret foretar en omfattende saksbehandling og gransker søknaden mot tilgjengelig teknikk.

Hvis vilkårene for patentbeskyttelse foreligger, meddeles patent og ukentlig publiseres nye patenter i Norsk Patenttidende. Etter publisering av meddelt patent, kan det leveres innsigelse mot meddelelsen av enhver med klageinteresse. Patentstyrets avgjørelse av innsigelsen kan påklages til Klagenemnda for industrielt rettsvern. Gyldigheten av et meddelt patent kan alltid

prøves av domstolene. Oslo tingrett er særskilt verneting, både for gyldighet og inngrep i patent, jf. patentloven § 63. Videre skal det betales årsavgift for å opprettholde patentbeskyttelse, jf. patentloven §§ 8 og 40.

Eneretten som patenthaveren får etter patentloven innebærer at vedkommende kan nekte andre å utnytte oppfinnelsen i næring. Eventuelle begrensninger på utnyttelsen av oppfinnelsen vil imidlertid følge av annen lovgivning.

Den som ønsker å utnytte en oppfinnelse av betydning for rikets sikkerhet plikter å forelegge og inngi en fullstendig skriftlig fremstilling av produktet til NSM dersom patentsøknad ikke er inngitt til Patentstyret, jf. forskrift om forsvarsviktige oppfinnelser § 6. Dersom det ønskes industrielt rettsvern for oppfinnelsen, må patentsøknad leveres til Patentstyret, jf. loven § 3 første ledd. Patentstyret plikter å underrette NSM om innkomne patentsøknader for oppfinnelser som anses å være av betydning for rikets forsvar. Søknad om hemmeligholdelse sendes til NSM.

I henhold til gjeldende lov om forsvarsviktige oppfinnelser § 7 første ledd første punktum kan departementet bestemme at en patentsøknad eller et patent omfattet av loven skal holdes hemmelig. Loven gir også hjemmel til å beslutte at oppfinnelsen skal holdes hemmelig også for en nærmere fastsatt tid etter at patentet er trådt ut av kraft, jf. første ledd siste punktum.

Hemmeligholdelsen skiller slike patentsøknader fra andre patentsøknader som leveres til Patentstyret og innføres i det ordinære patentregisteret. Istedenfor innføres patentet eller søknaden i et eget register som er unntatt offentlighet, jf. loven § 7 første ledd andre og tredje punktum. Det betales ikke årsavgift til Patentstyret for patenter som er hemmelige etter loven, jf. § 7 første ledd femte punktum. Når det er besluttet at et patent skal hemmeligholdes, kan ikke oppfinnelsen gjøres kjent så lenge Kongen ikke bestemmer noe annet, jf. § 2 tredje ledd.

Videre er NSM delegert myndighet til å ha tilgang til, og føre tilsyn med, patentsøknader som er inngitt til Patentstyret, jf. loven § 5.

Dersom et vedtak om hemmeligholdelse oppheves, vil patentet behandles som vanlig i Patentstyret og omfattes av de ordinære kravene til offentliggjøring og betaling av årsgebyr og avgifter, jf. § 7 andre ledd.

I henhold til loven § 7 tredje ledd kan Kongen

> «under forutsetning av gjensidighet treffe overenskomst med fremmed stat om at patentsøknader på oppfinnelser som er av betydning for vedkommende stats forsvar og som inngis i Norge av noen bosatt i den fremmede stat, på anmodning i hvert tilfelle fra kompetent myndighet i denne stat skal holdes hemmelig, og at patent i tilfelle meddeles som hemmelig patent.»

Det er fastsatt nærmere saksbehandlingsrutiner knyttet til håndtering av søknader om hemmelig patent i «Rutiner mellom NSM, Patentstyret og Forsvarets Forskningsinstitutt (FFI) angående patentsøknader om oppfinnelser av betydning for rikets forsvar» datert 19. desember 2008.

11.2 Forslaget i høringsnotatet

Det er departementets vurdering at gjeldende regler om hemmelige patenter i all hovedsak bør videreføres, men at enkelte endringer bør foretas for å forenkle regelverket og klargjøre Norges folkerettslige forpliktelser.

Departementet foreslår å videreføre departementets hjemmel til å bestemme at et patent eller en patentsøknad skal holdes hemmelig. Departementet foreslår en forenkling som består i at Forsvarsdepartementet bestemmer om et patent eller en patentsøknad skal være hemmelig, det vil si sikkerhetsgradert, jf. lovforslaget § 9 første ledd første punktum. Departementet foreslår derfor at begrepet «hemmelig patent» som benyttes i gjeldende lov endres til «sikkerhetsgradert patent» og defineres i loven § 3 bokstav c som «søknader og meddelte patenter som er graderte etter sikkerhetsloven».

Departementet foreslår å videreføre gjeldende lov § 2 tredje ledd som fastslår at et hemmelig patent ikke kan gjøres kjent med andre uten tillatelse fra departementet, jf. lovforslaget § 9 andre ledd. Når rettighetshaver ber om bistand fra andre til en sikkerhetsgradert patentsøknad, må informasjonsoverføringen behandles etter kravene i sikkerhetsloven og virksomhetsikkerhetsforskriften. Se også kapittel 4.1.1.

Departementet foreslår å videreføre unntak fra reglene om allmenn tilgjengelighet, kunngjøring og innsigelse i patentloven §§ 19 til 25, jf. forslaget til ny lov § 11 første ledd. På samme måte skal det heller ikke betales årsavgifter for hemmelige patenter, jf. §§ 8 og 40, jf. forslaget til ny lov § 11 andre ledd. Departementet foreslår også å videreføre plikten etter gjeldende lov § 7 andre ledd femte og sjette punktum til å betale årsavgift for patenter som avgraderes. Årsavgiften tilsvarer avgiftsåret etter at Patentstyret har mottatt melding om at patentet er avgradert. Hvis Patentstyret for eksempel mottar melding om at et patent er avgradert i patentets syvende år, skal årsavgift betales tilsvarende patentets åttende år. Likevel forfaller årsavgiften i noe tilfelle før to måneder etter at Patentstyret har informert patentsøkeren eller patenthaveren om at patentet er avgradert, jf. lovforslaget § 10 fjerde ledd.

Videre vil innlevering av en sikkerhetsgradert patentsøknad til patentfullmektig eller myndighet utenfor, innebære informasjonsoverføring av sikkerhetsgradert informasjon. Departementet foreslår derfor å videreføre at departementet kan gi samtykke til at en hemmelig patentsøknad kan leveres til en patentfullmektig eller myndighet utenfor Norge, jf. lovutkastet § 9 tredje ledd første punktum. Slik overføring må være i tråd med norske sikkerhetsinteresser og oppfylle de øvrige kravene til utlevering av sikkerhetshetsgradert informasjon etter virksomhetsikkerhetsforskriften § 25, se også kapittel 4.1.1.

Videre foreslås det at departementets adgang til å avgradere hemmelige patenter videreføres, slik at Patentstyret på alminnelig måte kan behandle patentsøknaden etter patentloven. Samtidig foreslår departementet å videreføre Forsvarsdepartementets adgang til å gi nærmere regler om saksbehandlingen av hemmelige patenter og søknader fra fremmede stater etter internasjonal overenskomst i forskrift.

Videre foreslås det at fristen for når departementet skal avgjøre om et patent er sikkerhetsgradert utvides fra fire til seks måneder, jf. lovutkastet § 9 første ledd andre punktum. Forslaget vil medføre at saksbehandlingsfristene i loven harmoniseres. I særlige tilfeller foreslås det at fristen kan forlenges med inntil tre måneder, jf. lovutkastet § 9 første ledd tredje punktum. Dette vil typisk være hvor vurderingen av patentet er særlig komplisert og departementet har behov for mer tid til å vurdere patentet.

Etter at lov om forsvarsviktige oppfinnelser trådte i kraft i 1956, har Norge tiltrådt internasjonale patentrettslige avtaler, blant annet Den europeiske patentkonvensjonen (EPC), Patentsamarbeidskonvensjonen (PCT) og WTOs avtale om handelsrelaterte sider ved

immaterielle rettigheter (TRIPS-avtalen). Gjeldende lov § 7 tredje ledd om forholdet til registrering patenter i og fra fremmede stater er derfor utdatert. For å sikre at loven er oppdatert i henhold til Norges folkerettslige forpliktelser, foreslås det at dagens praksis om at en hemmelig patentsøknad ikke kan leveres gjennom PCT og EPC presiseres. Begrunnelsen for dette er at disse internasjonale ordningene ikke har tilsvarende regler om hemmeligholdelse som loven her krever og at ordningene har svært mange medlemsland som innleverte patentsøknader kan videreføres i. Muligheten for hemmeligholdelse vil være tapt i slike tilfeller.

Departementer foreslår på denne bakgrunn at det i ny lov § 9 tredje ledd andre punktum presiseres at en søknad om sikkerhetsgradert patent ikke kan inngis gjennom Patentsamarbeidskonvensjonen eller Den europeiske patentkonvensjonen.

TRIPS-avtalen har et sikkerhetsunntak i artikkel 73 som i bokstav a slår fast at ingen bestemmelse i avtalen skal fortolkes slik at et medlem «pålegges å legge fram opplysninger hvis offentliggjøring etter medlemmets mening ville være i strid med vesentlige sikkerhetsinteresser.» Når det gjelder sikkerhetsgraderte patenter i lovforslaget legger departementet til grunn at dette vil omfattes av unntaket i TRIPS-avtalen bokstav a.

I tillegg til oppdatering av selve lovgrunnlaget, bemerker departementet at det også er behov for å oppdatere gjeldende rutiner mellom NSM, Patentstyret og Forsvarets Forskningsinstitutt (FFI) angående patentsøknader om oppfinnelser av betydning for rikets forsvar slik at instruksen også gjenspeiler FMAs rolle i disse sakene. Per i dag er det kun fastsatt nærmere saksbehandlingsrutiner knyttet til håndtering av søknader om hemmelig patent i «Rutiner mellom NSM, Patentstyret og Forsvarets Forskningsinstitutt (FFI) angående patentsøknader om oppfinnelser av betydning for rikets forsvar» datert 19. desember 2008. Rutiner for øvrige områder er ikke formalisert og fastsatt.

NSM har kompetanse om både sikkerhetsgradering av patenter og teknologi og departementet foreslår derfor å videreføre NSMs ansvar for vurdering av sikkerhetsgraderte patenter. Samtidig innebærer forslaget om at FMA skal være forberedende etat for vurdering av om en forsvarsteknologi er beskyttelsesverdig, at etaten også vil vurdere teknologiens betydning for norsk forsvarsevne og andre nasjonale sikkerhetsinteresser. Dette er vurderinger som langt på vei er sammenfallende med vurderinger av om informasjon om en teknologi skal sikkerhetsgraderes. Det foreslås derfor at FMA også involveres tett i forbindelse med vurderingen av sikkerhetsgraderte patenter.

12 Straff

12.1 Gjeldende rett

Det følger av gjeldende lov § 10 at

> «Den som forsettlig eller uaktsomt overtreder denne lovs § 2, første eller tredje ledd, [eller § 12, annet ledd, annet punktum,] eller unnlater å gi opplysninger som kreves etter § 4, eller gir ufullstendige eller uriktige opplysninger, eller som overtrer bestemmelser utferdiget med hjemmel i § 6, annet ledd, eller § 7, første ledd, straffes med bøter eller fengsel inntil 1 år hvis ikke forholdet rammes av et strengere straffebud. Medvirkning straffes ikke.»

Bestemmelsen innebærer at forsettlige eller uaktsomme overtredelser av kravet til hemmelighold eller et hemmelig patent etter loven §§ 2 første og tredje ledd og 7 første ledd,

kan ilegges bøter eller fengsel inntil 1 år. Det samme gjelder for brudd på opplysningsplikten etter § 4 og rådighetsbegrensninger fastsatt med hjemmel i § 6 andre ledd, eller § 7 første ledd. Medvirkning straffes ikke.

Det er per i dag ikke er ilagt noen begrensninger med hjemmel i gjeldende lov, og det er da heller ikke ilagt noen straffereaksjoner med hjemmel i loven § 10.

12.2 Forslaget i høringsnotatet

Departementet foreslår å videreføre straffebestemmelsen etter gjeldende rett. Etter departementets syn vil ikke forvaltningsrettslige sanksjoner, som for eksempel et overtredelsesgebyr, ha tilstrekkelig preventiv effekt. Departementet viser til at en overtredelse av kravet til tillatelse, eventuelle vilkår til tillatelsen, opplysningsplikten og eventuelle påbud eller forbud vil kunne få svært alvorlige skadefølger for nasjonale sikkerhetsinteresser, og bør derfor kunne straffesanksjoner for å i tilstrekkelig grad sikre etterlevelse av lovforslaget. En videreføring av straffebestemmelsen fra gjeldende rett vil også sikre samme straffenivå som etter sikkerhetsloven for overtredelse av taushetsplikten,[75] som også har til formål å beskytte nasjonale sikkerhetsinteresser. En videreføring vil også sikre tilsvarende straffenivå som etter det danske og svenske regelverket.

Informasjon om beskyttelsesverdig forsvarsteknologi vil normalt være sikkerhetsgradert, jf. kapitel 4.1, og derfor taushetsbelagt, jf. sikkerhetsloven § 5-4 andre ledd. Både forsettlige og grovt uaktsomme overtredelser av taushetsplikten for sikkerhetsgradert informasjon kan straffes med bøter eller fengsel i inntil 1 år, eller begge deler, så lenge ikke forholdet går inn under en strengere straffebestemmelse, jf. sikkerhetsloven § 11-4.

Straffebestemmelsen i gjeldende lov omfatter ikke medvirkning, jf. § 10 siste setning. I forslag til ny lov foreslår departementet imidlertid at også medvirkning kan straffes etter lovforslaget, jf. straffeloven § 15. Slik departementet ser det vil det potensielt være mange involverte i utviklingen av beskyttelsesverdig forsvarsteknologi, der flere vil ha en posisjon som kan tilrettelegge for overtredelser av regelverket, for eksempel gjennom å kunne gi tilganger som kan gjøre informasjon om teknologien kjent for uvedkommende. Departementet ser derfor ikke noe grunnlag for å videreføre unntaket etter gjeldende rett.

Det følger av straffeloven § 1 at straffelovens alminnelige bestemmelser også gjelder for spesiallovgivningen, med mindre annet er bestemt i eller i medhold av lov eller følger av tolkning, jf. straffeloven § 1. Det er derfor ikke behov for at lovens straffebestemmelse angir at også medvirkning er straffbart.

13 Økonomiske og administrative konsekvenser

Det er per i dag ikke truffet vedtak med hjemmel i gjeldende lov. Det foreligger derfor ingen praksis knyttet til kompensasjonsreglene i loven § 9, og heller ikke noe empirisk grunnlag for å si noe om hvor stort et krav om kompensasjon etter lovforslaget vil være. Departementet legger imidlertid til grunn at ekspropriasjon eller rett til å utnytte en teknologien potensielt vil kunne føre til relativt høye erstatningsbeløp, anslagsvis fra noen hundre tusen til flere millioner kroner, avhengig av hva som er salgs- eller bruksverdien til teknologien, jf. kapitel 10.

[75] Sikkerhetsloven § 5-4 andre ledd, jf. § 11-4 andre ledd

Departementet legger imidlertid opp til at det svært sjeldent vil være aktuelt å ekspropriere eller sikre en rett til utnyttelse av teknologien, ettersom bestemmelsene om deling av teknologi og pålegg og forbud i de aller fleste tilfeller vil gi tilstrekkelig tilgang og kontroll med teknologien. Departementet legger til grunn at vedtak etter sistnevnte bestemmelser svært sjeldent vil medføre rett til erstatning, se kapitel 10.2.2 for nærmere om rett til erstatning ved rådighetsbegrensinger.

Slik departementet ser det vil de økonomiske konsekvensene for industriaktørene i hovedsak vil knytte seg til begrensninger på deling av teknologi ved eksport. Størrelsen på tapet avhenger av om eksporten nektes, eller hvilke vilkår som stilles før eksport tillates. Erfaringer basert på Strategi for norskutviklet forsvarsteknologi (2018), viser at industriens kostnader i hovedsak knytter seg til testing av teknologien etter at eventuelle justeringer i teknologien er implementert. Avhengig av hvor omfattende krav som stilles, og størrelsen på den aktuelle kontrakten, utgjør kostnaden anslagsvis ca. 0,02% av kontraktens verdi – noe som innebærer normalt ca. 5 % av aktørenes overskudd. Kostnadene vil i hovedsak være en engangskostnad, knyttet til implementering av tiltak og verifisering av at vilkår i vedtaket er oppfylt. Etter implementeringen og verifisering vil det for fremtidige leveranser i hovedsak være snakk om noe økt produksjonskostnad, som virksomheten vil kunne kompensere for i kontrakten med kunden.

Departementet legger imidlertid til grunn at dersom virksomhetene nektes eksport, og eksportmarkedet blir begrenset, vil de økonomiske konsekvensene for industriaktørene potensielt være større. Beskyttelsesverdig teknologi vil imidlertid ha så stor betydning for Forsvarets operativ evne, at hensynet til nasjonal sikkerhet etter departementets syn veier tyngre enn eventuelle negative økonomiske konsekvenser for industriaktørene. Departementet legger opp til at i de fleste tilfellene vil eksporten tillates mot at det settes vilkår som vil beskytte teknologien ved eksporten, og at industrien gjennom praktiseringen av regelverket så langt som mulig skal få eksportert produkter, og dratt nytte av samarbeidsmuligheter i det internasjonale markedet, på samme måte som i dag. Slik departementet ser det vil det dessuten gi en positiv markedsføringseffekt for industrien at teknologien er underlagt et strengt delingsregime, som reduserer risikoen for at uvedkommende får tilgang til teknologien.

Departementet bemerker at det bare vil være i de tilfellene hvor eksport nektes av Forsvarsdepartementet (FD), men ville blitt tillatt av Utenriksdepartementet (UD), at det er eksportnekten fra FD som gir et økonomisk tap for aktørene.

Når det gjelder nedslagsfelt til loven anslår departementet at det vil kunne dreie seg om 10-15 saker i året, der ikke alle sakene vil nå opp til terskelen for å være beskyttelsesverdig teknologi. Departementet legger opp til at dialogen mellom Forsvarsmateriell (FMA) og industrien opprettes så tidlig som mulig slik at eventuelle konsekvenser av vedtaket kan tas høyde for i forbindelse med søknad om eksportlisens, eller så tidlig som mulig ved utvikling av ny teknologi.

For de aktørene som blir omfattet av loven vil det også bli en kostnad knyttet til at informasjon om teknologien skal beskyttes etter kravene i sikkerhetsloven med forskrifter. Departementet legger imidlertid til grunn at de aller fleste av disse virksomhetene har tilstrekkelig god grunnsikkerhet i sine informasjonssystemer, gjennom at sensitiv informasjon behandles i tråd med krav til konfidensialitet, slik at merkostnader ved å bli underlagt

sikkerhetsloven vil bli begrenset. Departementet viser for øvrig til omtalen av økonomiske og administrative konsekvenser i forarbeidene til sikkerhetsloven.[76]

Når det gjelder administrative kostnader for industrien vil disse knyttes seg til en ekstra søknadsprosess i tillegg til UDs søknadsprosess om eksportlisens etter eksportkontrollregelverket. Departementet legger opp til en så smidig søknadsprosess som mulig, som går i forkant av eller parallelt med søknaden til UD. Slik departementet ser det vil prosessen innebære helt begrensede merkostnader for industrien sammenlignet med de kostnader som allerede påløper for behandling av søknad om eksportlisens. Det vises særlig til saksbehandlingsreglene for behandling av søknader om tillatelse, der en søknad skal behandles så snart som mulig, se kapitel 9.3.3.

Når det gjelder administrative kostnader for de berørte myndighetene vil lovforslaget innebære en klargjøring av ansvarsområdene til de forskjellige aktørene. Departementet legger opp til forvaltningsansvaret for loven overføres til FMA. Dette vil ikke umiddelbart medføre større administrative konsekvenser ettersom FMA allerede i dag forvalter strategi for beskyttelse av forsvarsteknologi. Samtidig forventes det at FMA på sikt vil ha behov for tilførte ressurser, avhengig av hvor stort sakstilfanget viser seg å bli. Det vil først og fremst gi utslag i økt kontakt med industrien om vilkår og utfordringer i mottakerland, i tillegg til å inngå og forvalte teknologisikkerhetsavtaler. FMA anslår at det kan dreie seg om behov for et ekstra årsverk, men det vil likevel avhenge av det konkrete antallet saker. De konkrete økonomiske og administrative konsekvensene av forslaget vil medføre for FMA, vil måtte vurderes etterhvert som praksisen utvikler seg og vil følges opp i den ordinære styringsdialogen til FD.

14 Ikrafttredelse

Ikrafttredelse forutsetter at saksbehandlingsrutiner oppdateres og samhandlingen mellom involverte myndigheter klargjøres. Departementet foreslår derfor at loven trer i kraft fra det tidspunktet Kongen bestemmer.

Gjeldende lov om forsvarsviktige oppfinnelser er i all hovedsak en rammelov hvor det er nærmere fastsatt i forskrift hva som er å anse som krigsmateriell eller for å ha direkte betydning for rikets forsvar, i tillegg til nærmere saksbehandlingsregler. Etter departementets vurdering forutsetter ikke den foreslåtte loven at det fastsettes forskrifter før loven kan tre i kraft. Vurderingsmomentene for når en teknologi er å anse som beskyttelsesverdig og hvilke momenter det skal legges vekt på ved tillatelse til deling innenfor norsk jurisdiksjon og ved eksport, fremgår istedenfor av den nye loven. Departementet legger opp til at forskrift først er aktuelt når loven har virket over noe tid for å nærmere regulere hvilke teknologier som skal omfattes av loven, samt eventuelle detaljkrav for enkelte teknologier. Siden det ikke er behov for å utarbeide nye forskrifter til ny lov, er det departementets vurdering at det ikke er behov for loven kan tre i kraft på ulike tidspunkter etter at lovforslaget er vedtatt av Stortinget.

Fra det tidspunkt som ny lov trer i kraft, vil gjeldende lov bli opphevet, jf. § 13. Det vil ikke være behov for å foreta endringer i andre lover som følge av ny lov om beskyttelsesverdig forsvarsteknologi.

[76] Prop. 153 L (2016-2017) Lov om nasjonal sikkerhet (sikkerhetsloven) s. 160.

15 Merknader til bestemmelsene

Til § 1 *Formål*

Bestemmelsen er ny og setter en overordnet ramme for hvilke formål loven skal ivareta. I *bokstav a* slås det fast at loven skal sikre at Forsvaret har tilstrekkelig tilgang til og kontroll med teknologi som har vesentlig betydning for operativ evne. Dette innebærer å sikre at Forsvaret har kontroll og innflytelse med innsatsfaktorer som er vesentlige for å ivareta operativ evne.

I *bokstav b* slås det fast at loven skal bidra til at uvedkommende ikke får tilgang til teknologi som har vesentlig betydning for operativ evne. Lovens tillatelsesregime skal bidra til å forhindre at Forsvaret mister operative fortrinn gjennom tap av teknologi og informasjon om teknologien.

Bokstav c slår fast at loven skal sikre at nasjonale forsvars- og sikkerhetsinteresser blir ivaretatt ved deling, utvikling og produksjon av slik teknologi. Nasjonale forsvarsinteresser omfatter bl.a. Forsvarets operative evne og forsvarssamarbeid med andre stater. Eksport og samarbeid om forsvarsmateriell er en viktig del av Norges forsvarssamarbeid med andre stater.

Til § 2 *Definisjoner*

Bestemmelsen er ny. Bestemmelsen definerer sentrale begreper i loven. I *bokstav a* defineres *forsvarsteknologi som, varer, tjenester og teknologi som kan brukes til forsvarsformål.* Begrepet er nærmere beskrevet i kapittel 6.2.2. Begrepet er en utvidelse av gjeldene lovs *oppfinnelser av betydning for rikets forsvar* og er brukt for å omfatte varer, tjenester og teknologi som allerede er på markedet, i tillegg til oppfinnelser og teknologi som fortsatt er under utvikling. Begrepene «varer, tjenester og teknologi» skal forstås på samme måte som begrepene er definert i eksportkontrollregelverket. Begrepene vil omfatte de forsvarsrelaterte varer som er oppført på liste 1, og de flerbruksvarer som er oppført på liste II. Med teknologi menes også her innsikt som er avgjørende for å utvikle, produsere, vedlikeholde eller bruke en vare.

Forsvarsteknologi kan imidlertid også omfatte produkter og teknologi som ikke står på liste I og II, så lenge produktet eller teknologien kan brukes til forsvarsformål. Forsvarsformål vil si at produktet eller teknologien kan påføre en fiende tap eller skade i strid eller på annen måte sikre Forsvaret en operativ fordel. Begrepet vil omfatte koder, algoritmer, informasjon om produksjonsprosesser, metoder og kunnskap og teori knyttet til en teknologi («know-how»). Det vil også omfatte kunnskap i form av algoritmer, programmer og lignende.

evnen til å forsvare norsk territorium, landets suverenitet, territorielle integritet og demokratiske styreform.

Bokstav b definerer *nasjonale forsvars- og sikkerhetsinteresser* som «evnen til å forsvare norsk territorium, landets suverenitet, territorielle integritet og demokratiske styreform». Bestemmelsen angir interessene som loven skal beskytte. Dette innebærer å sikre Forsvaret tilstrekkelig kontroll med de innsatsfaktorene som er nødvendig for å ivareta operativ evne.

Videre er forsvarssamarbeid med andre stater en viktig del av det å ivareta operativ evne, og forsvarsinteressene loven skal ivareta.

I *bokstav* c er begrepet *sikkerhetsgraderte patenter* definert. Begrepet *patent* sammenfaller med begrepet slik det er brukt i patentloven § 1 første ledd og henviser til bekreftelse på oppnådd enerett til utnyttelse i nærings- og driftsøyemed av en oppfinnelse som kan utnyttes industrielt innenfor ethvert teknisk område. Med *sikkerhetsgradert* menes patenter som omfatter informasjon som kan skade nasjonale sikkerhetsinteresser om den blir kjent for uvedkommende etter sikkerhetsloven § 5-3.

Til § 3 *Beskyttelsesverdig forsvarsteknologi*

Bestemmelsen er en delvis videreføring av gjeldende lov § 1, men med presiseringer av saksbehandlingsregler og nye vurderingskriterier for hvilken teknologier som kan omfattes av loven. Bestemmelsens *første ledd første punktum* gir departementet myndighet til å fatte vedtak om at forsvarsteknologi er beskyttelsesverdig. Av *første ledd andre punktum* følger at forsvarsteknologien må være utviklet i Norge, eies av en enkeltperson eller virksomhet som holder til innenfor norsk jurisdiksjon, det må ha blitt søkt patent i Norge, eller virksomheten eller enkeltpersonen har helt eller delvis utnyttelsesrett til teknologien for at det kan fattes vedta etter *første punktum*. Det må kunne dokumenteres at enkeltpersonen eller virksomheten holder til innenfor norsk jurisdiksjon, f.eks. ved å vise til registrering i Brønnøysundregisteret eller folkeregistret adresse. Det må kunne dokumenteres til at enkeltpersonen eller virksomheten har eierskapet eller utnyttelsesretten til teknologien, f.eks. gjennom en skriftlig avtale. Med utviklet i Norge må det kunne vises til at teknologien har blitt utviklet innenfor norsk jurisdiksjon, f.eks. i et norsk lokale og/eller på en norsk server.

Det følger av *første ledd første punktum* at forsvarsteknologi som har vesentlig betydning for Forsvarets operative evne er beskyttelsesverdig. Det innebærer at det må få konsekvenser av et visst omfang for Forsvarets operative evne, dersom Forsvaret mister kontroll over teknologien eller uvedkommende får tilgang til den. I Forsvarets operative evne inngår også teknologiens betydning for Norges forsvars- og sikkerhetssamarbeid med andre stater. Av *første ledd tredje punktum* følger momenter som er relevante for vurderingen av om teknologien har vesentlig betydning for Forsvaret operative evne.

Av *bokstav a* fremgår det at det skal legges vekt på i hvilke grad teknologien er tilpasset norske forhold. Det innebærer en vurdering av om det gir Forsvaret operative kapasiteter som er unike eller svært fordelaktige eller forhindrer andre i å få tilsvarende kapasiteter. Det vil være relevant å se hen til om produktet er tilpasset norsk geografi, klima og topografi. Det vil også være relevant å vurdere om teknologien understøtter et annet produkt med disse egenskapene, eksempelvis gjennom vedlikehold og levetidsstøtte.

Det skal etter *bokstav b* vurderes hvilke kapabiliteter teknologien understøtter og hvilken konsekvens et eventuelt tap av eller andres tilgang til teknologien vil ha for operativ evne. Det innebærer en vurdering av om tap av teknologien vil gi en potensiell motstander et overtak i en eventuell fremtidig konflikt. Understøtter teknologien en sentral kapabilitet, samtidig som tap av teknologien vil kunne gi et overtak i fremtidig konflikt, taler det med tyngde for at teknologien er beskyttelsesverdig. Det kan være teknologien i seg selv, eller enkeltkomponenter i denne som har vesentlig betydning for operativ evne.

Av *bokstav c* fremgår at i hvilken grad teknologien er tilgjengelig på markedet er et relevant moment. Er som teknologien ikke normalt er tilgjengelig på markedet, eller kun er det i begrenset grad, kan det tilsi at Forsvaret har behov for kontroll med teknologien for å ivareta operativ evne.

Etter *bokstav d* inngår det i vurderingen i hvilken grad teknologien gir forsvarspolitiske fordeler. I denne vurderingen inngår i hvilken grad det eksisterer tilsvarende løsninger på verdensmarkedet, og i hvilken grad allierte bruker teknologien i sine kapabiliteter. Er teknologien lett tilgjengelig andre steder, eller utvikling av teknologien er ivaretatt av det internasjonale markedet, tilsier det at teknologien ikke gir oss forsvarspolitiske fordeler.

Det følger av *bokstav e* at det også skal vurderes i hvor stor grad teknologien har betydning for beskyttelse av nasjonal sensitiv informasjon. Sensitiv informasjon kan være både sikkerhetsgradert eller Fortrolig. Hvilket graderingsnivå informasjonen har, i hvilket omfang, vil være sentralt. Det skal også ses hen til hvilken funksjon det aktuelle kommunikasjonssystemet har.

Bokstav f sier at det skal vurderes om Forsvaret har kompetanse på hvordan komponentene virker sammen, og kan settes sammen til systemer av betydning for operativ evne. Hvor stor betydning komponentene og systemene har må ses i sammenheng med hvile konsekvenser det vil ha dersom uvedkommende får tilgang til den aktuelle kompetansen.

Bokstav g åpner for at det kan legges vekt på andre forhold som kan medføre at forsvarsteknologien vil ha vesentlig betydning for operativ evne.

Av bestemmelsens *andre ledd* pålegges departementet en plikt om å sende melding til eier av forsvarsteknologien om at den er til vurdering etter loven. Meldingen skal inneholde en beskrivelse av hvilken teknolog som er til vurdering, og eventuelt en nærmere angivelse av hvilken del av teknologien som er omfattet av vurderingen (delkomponenter, prosessbeskrivelser, metodikk «know how»). Meldingen skal angi tidsfristen som ligger til grunn for vurderingen, opplysningsplikten til eier og rettighetshaver og hvilke midlertidige begrensninger som gjelder for teknologien mens den er til vurdering. Den skal også angi hvorvidt det er behov for ytterligere opplysninger fra eier eller rettighetshaver om teknologien.

Av bestemmelsen *andre ledd andre punktum* følger at teknologien ikke kan deles uten tillatelse fra departementet etter §§ 5 og 6. Det innebærer bl.a. at teknologien bare kan utvikles internt i en virksomhet så lenge teknologien er til vurdering, med mindre det gis tillatelse til deling fra departementet.

Av *tredje ledd* følger at det bare kan gis tilgang til teknologi og informasjon om teknologien til personer med tjenstlig behov for tilgang. Begrepet skal forstås på samme måte som i sikkerhetsloven § 5-4, og innebærer bl.a. at det bare er personer som har behov for tilgang for å utføre sine arbeidsoppgaver som kan få tilgang til teknologien, eller informasjon om denne.

Et vedtak om at en forsvarsteknologi er beskyttelsesverdig skal angi hvilken teknologi, og eventuelt hvilke deler av teknologien som er beskyttelsesverdig, hva vedtaket vil innebære for eier av teknologien (eier av immaterielle rettigheter), informasjon om at teknologien kan bli ekspropriert, virksomhetens opplysningsplikt og straffansvar ved brudd på loven. Det skal videre oppgi klageadgangen etter forvaltningsloven.

Det følger av *fjerde ledd* at departementet kan gi forskrift om hvilke teknologier som anses å være beskyttelsesverdige, og nærmere kriterier for vurderingen av når en teknologi er beskyttelsesverdig. Bestemmelsen skal ta høyde for at den teknologiske utviklingen kan gjøre det nødvendig med detaljert regulering av enkelte teknologier, og at det kan være andre relevante momenter for vurderingen enn de som fremgår av første ledd i bestemmelsen.

Til § 4 *Plikt til å gi opplysninger til departementet*

Bestemmelsen er i all hovedsak en videreføring av gjeldende lov § 4 om opplysningsplikt. Plikten gjelder for virksomheten som eier, utvikler, bruker eller har tilgang til forsvarsteknologi som det er grunn til å tro at kan være beskyttelsesverdig. Departementet kan kreve alle relevante opplysninger som er nødvendig for å vurdere om teknologien er beskyttelsesverdig eller for å vurdere hvilke rådighetsbegrensninger som skal ilegges. Det kan dreie seg om informasjon om hva teknologien skal brukes til, hva den kan brukes til, hvordan må den brukes for å oppnå resultater, hvilke testresultater teknologien har oppnådd, teknologiens operative og tekniske ytelse og hvilke bestanddeler teknologien består av, samt om det er bakenforliggende kunnskap som metodikk, prosesser eller annen kompetanse som er relevant.

Opplysningsplikten gjelder uten hinder av eventuell lovbestemt taushetsplikt.

Vilkåret *grunn til å tro* innebærer at departementet ikke uten videre kan be om opplysninger knyttet til en forsvarsteknologi. Departementet må sitte på tilstrekkelig opplysninger om teknologien som gjør det rimelig å anta at den kan ha betydning for Forsvaret. Dette vil kunne være tilfelle dersom det foreligger indikasjoner på at teknologien faller innenfor de til enhver tid gjeldende teknologiske kompetanseområdene.

Bestemmelsen i a*ndre ledd* er ny. Bestemmelsen skal gi tilgang til opplysninger som har betydning for vurderingen av mottakers tilknytning til andre stater i vurderingen av om det kan gis tillatelse til deling etter §§ 5 og 6. Det vil i utgangspunktet være:

- Mottakers navn, adresse og organisasjonsnummer, fødselsnummer eller tilsvarende nummer
- Organisasjonsnummeret til virksomheten som skal være mottaker av teknologien
- Mottakers eierstruktur
- Hvem som sitter i mottakers styre
- Hvem som inngår i daglig ledelse

Kravet om opplysninger kan ikke gå lengre enn det som er nødvendig for å vurdere om en tillatelse kan gis etter §§ 5 og 6.

Til § 5 Tillatelse til å dele beskyttelsesverdig forsvarsteknologi ut av norsk jurisdiksjon

Bestemmelsens er ny. *Første ledd første punktum* innebærer at beskyttelsesverdig forsvarsteknologi ikke kan deles med andre utenfor norsk jurisdiksjon uten tillatelse fra departementet. Det gjelder uavhengig av hvordan delingen skjer, f. eks. gjennom et salg eller som en del av et samarbeid om utvikling av teknologi. Bestemmelsen omfatter all form for eksport av teknologien.

Av *andre punktum* følger hvilke vurderingskriterier som inngår i den konkrete helhetsvurderingen av om tillatelse kan gis. Det avgjørende vil være om fordelen ved delingen

veier opp for risikoen for tap og konsekvensene for operativ evne ved tap av teknologien. I vurderingen av konsekvenser for Forsvarets operative evne inngår hvilke kapabiliteter teknologien understøtter og hvilke konsekvenser det vil få om en potensiell motstander for tilgang til teknologien. I vurderingen av fordeler for operativ evne er det relevant i hvilken grad deling vil gi mulighet til forbedring av teknologien, og i hvilken grad deling vil gi positive konsekvenser for Norges forsvars- og sikkerhetspolitiske forhold til mottakerstaten eller andre stater.

Av *tredje punktum* følger at departementet kan stille vilkår for tillatelsen. Formålet med vilkårene skal normalt være å redusere risikoen for tap av teknologien, og konsekvensene dersom teknologien likevel går tapt. Vilkårene kan være å begrense tilgang til informasjon om teknologien og tilpasninger som reduserer muligheter for å utnytte teknologien. Det kan stilles krav til hvem som skal få tilgang til informasjon om teknologien på hvilke tidspunkt og med hvilken detaljeringsgrad. Krav til tiltak kan knytte seg til kryptering av programvare, krav om enkelte typer oppdateringer og konfigurasjoner, eller krav til bruk av konkrete komponenter. Det kan være aktuelt å stille krav om «anti-tampering» tiltak, dvs. tiltak som varsler ved forsøk på å gjøre uautoriserte endringer i eller dekonstruere teknologien. Det kan settes krav om å gjøre tiltak som gjør det enklere å forsvare seg mot teknologien.

Andre ledd bokstavene a til g gir kriteriene for å vurdere risikoen for tap av teknologien ved eksport til det aktuelle mottakerlandet. Etterretningstrusselen (bokstav a) avhenger graden av etterretningsvirksomhet fra andre stater mot mottakerstaten, og om eksporten vil føre til økt etterretningsvirksomhet mot norske interesser i mottakerstaten. De statlige styringsindikatorene (bokstav b) er en vurdering av i hvilken grad de politiske forholdene tilsier at det er en risiko for at teknologien blir gjort kjent for andre enn mottakeren av teknologien. Det vil være særlig relevant å se til hvilken tilknytning det er mellom staten og virksomheter i landet, f. eks om lovgivningen gir staten mulighet til å tilegne seg varer, tjenester og teknologi fra virksomhetene i staten. Det vil også være relevant å vurdere hvilke forsvars- og sikkerhetspolitiske samarbeid Norge har med den aktuelle mottakerstaten. Er samarbeidet med staten nært vil i utgangspunktet risikoen for tap av teknologien på grunn av de statlige styringsindikatorene være lav.

Hvilken tilknytning i mottakerlandet har til det aktuelle landet (bokstav c) er en vurdering av eierforholdene i virksomheten som er mottaker av teknologien, hvilke styresammensetning og ledelse virksomheten har, hvilke personer som er ansatt i virksomheten og hvilke tilknytning det er mellom disse og styresmaktene i staten. Sikkerhetsmessig modenhetsnivået (bokstav d) er en vurdering av cybersikkerhetstilstanden i mottakerstaten, og i virksomheten som er mottaker av teknologien. Forretningsstabilitet (bokstav e) er en vurdering av i hvilken grad inngåtte avtaler respekteres i mottakerstaten, og hvor stor risiko det er for at teknologien blir delt med andre enn virksomheten i strid med gjeldende avtaler. Det innebærer bl.a. en vurdering av risikoen for korrupsjon, hvitvasking og habilitetsproblematikk.

Av *tredje ledd* følger at i vurdering av fordelen med eksporten inngår i hvilken grad det er sannsynlig at deling vil gi mulighet til forbedring av teknologien. Det vil eksempelvis være relevant om deling gir en styrket tilgang til internasjonalt forskning, utvikling, produksjon og understøttelse av materiell og/eller systemer. Det vil også være relevant å vurdere om eksport vil bidra til interoperabilitet med allierte, og/eller vil utløse et markedspotensial for teknologien. I vurderingen av konsekvenser deling av teknologien vil ha for Norges forsvars-

og sikkerhetspolitiske forhold til mottaker landet og andre stater inngår om eksport vil styrke eller svekke vårt forhold til mottakerstaten og/eller andre stater.

Av *fjerde ledd* følger at departementet kan gi forskrift om tillatelsen. Det innebærer bestemmelser om vilkår for tillatelsen. Bestemmelsen skal ta høyde for at den teknologiske utviklingen kan gjøre det nødvendig med detaljert regulering av enkelte teknologier og vilkår for deling av teknologien til enkelte mottakere.

Til § 6 *Tillatelse til deling innenfor norsk jurisdiksjon*

Bestemmelsen er ny. *Første ledd første punktum innebærer* at beskyttelsesverdig forsvarsteknologi ikke kan deles med andre innenfor norsk jurisdiksjon uten tillatelse fra departementet. Dette gjelder uavhengig av hvordan delingen skjer, f. eks. gjennom et salg eller som en del av et samarbeid om utvikling av teknologien. Av *andre punktum* følger hvilke vurderingskriterier som inngår i den konkrete helhetsvurderingen av om tillatelse kan gis. Det avgjørende vil være om fordelen ved delingen veier opp for risikoen for tap av teknologien og konsekvensene for operativ evne ved tap av teknologien. I vurderingen av hvilke konsekvenser tap av teknologien vil få for Forsvarets operative evne inngår hvilke kapabiliteter teknologien understøtter og hvilke konsekvenser det vil få om en potensiell motstander for tilgang til teknologien. I vurderingen av fordeler for operativ evne vil det være relevant i hvilken grad deling vil gi mulighet til forbedring av teknologien.

Av *andre ledd* følger at risikoen for tap av teknologien er avhengig av i hvilken grad virksomheten som skal motta teknologien har tilknytning til andre stater. Det innebærer en vurdering av eierstrukturen i virksomheten, hvilke eiere virksomheten har med hvilken innflytelse, og hvilken tilknytning eierne har til andre stater. Vurderingen vil bygge på de opplysningene som kan hentes inn etter lovforslaget § 4. Det vil særlig være relevant å vurdere den samlede innflytelse personer i styret og ledelse har på driften av virksomheten, hvilken tilgang disse eventuelt vil ha til den beskyttelsesverdige teknologien, og i hvilken grad de har tilknytning til andre stater. I vurderingen av tilknytning er nasjonalitet og næringsinteresser i andre stater sentralt, og da særlig om disse båndene utgjør en risiko for at andre stater vil kunne få tilgang til teknologien.

Størrelsen på risikoen vil i stor grad avhenge av hvilken stat virksomheten har tilknytning til, og graden av etterretningsvirksomhet mot den aktuelle type virksomhet, og ansatte i virksomheten. Det vil være relevant å se hen til hvilke statsborgerskap de ansatte, og eventuelle konsulenter, i virksomheten har, og hvilken bakgrunnssjekk som allerede er gjort av disse. Normalt vil risikoen være mindre dersom Norge har et tett forsvars- og sikkerhetspolitisk samarbeid med staten.

Av *tredje punktum* følger at det kan stilles vilkår for tillatelsen. Formålet med vilkårene skal normalt være å redusere risikoen for tap av teknologien, og konsekvensene dersom teknologien likevel går tapt. De vilkår som er aktuelle ved eksport er også aktuelle ved deling innenfor norsk jurisdiksjon. Det vil være særlig aktuelt å stille vilkår om at det bare skal gis tilgang til teknologien hos enkeltavdelinger eller grupper av personer hos virksomheten, eller at det ilegges begrensninger på hvilke personer utenfor virksomheten som gis tilgang til teknologien. Sistnevnte tilfelle vil være særlig relevant i forsknings- og utviklingsprosjekter hvor teknologi deles med forskere eller konsulenter som engasjeres utenfra. Det vil også være aktuelt å

begrense tilgang på detaljer om teknologien, og sette krav om at tilgang krever visse typer statsborgerskap.

Av *tredje ledd* følger at departementet kan gi forskrift om tillatelsen. Det innebærer bestemmelser om vilkår for tillatelsen. Bestemmelsen skal ta høyde for at den teknologiske utviklingen kan gjøre det nødvendig med detaljert regulering av enkelte teknologier og vilkår for deling av teknologien til enkelte mottakere.

Til § 7 *Pålegg eller forbud mot bruk, utvikling og tilgang til beskyttelsesverdig forsvarsteknologi*

Bestemmelsen er i hovedsak en videreføring av gjeldende lov § 6 andre ledd om adgangen til å sette forbud og påbud i forbindelse med utnyttelse av en oppfinnelse. Det følger av *første ledd første punktum* at departementet kan pålegge eller sette forbud mot enhver form for bruk, utvikling eller produksjon av beskyttelsesverdig forsvarsteknologi. Med *for å ivareta* menes at pålegget eller forbudet må ha som formål å beskytte forsvarets operative evne eller sikre at bruk, utvikling eller produksjon av en teknologi er i tråd med Norges internasjonale- eller folkerettslige forpliktelser.

Av *første ledd andre punktum* følger at *forbud* omfatter begrensninger på tilgang til teknologien og på hvor teknologien kan brukes, utvikles eller produserer. Bestemmelsen tydeliggjør at det kan sette begrensninger som sikrer at teknologien i tilstrekkelig grad er tilgjengelig for Forsvaret, eller som sikrer at teknologien ikke blir tilgjengelig for potensielle motstandere i en eventuell fremtidig konflikt. F.eks krav om at hele eller deler av kompetansen om eller utviklingskapasiteten av en teknologi er tilgjengelig innenfor norsk jurisdiksjon, selv om en industriaktør ønsker å flytte hele eller deler av produksjonen ut av landet. Bestemmelsen tydeliggjør også at det kan legges føringer på hvem som kan få tilgang til teknologien hos virksomheten. F.eks krav om at teknologien kun kan gjøres tilgjengelig hos en avdeling i virksomheten, eller at en virksomhet bare kan få tilgang til en delmengde av informasjonen, eller om at teknologien bare er tilgjengelig for personer med norsk statsborgerskap. Bestemmelsen gir hjemmel til å sette begrensninger på hvilke opplysninger det gis tilgang til og hvordan tilgangen gis. En forutsetning for at det stilles begrensninger på tilgang er at det er nødvendig for å redusere risikoen for tap av teknologien, og at kravene ikke går lengre enn det som er nødvendig for å oppnå en akseptabel restrisiko

Det følger av *andre ledd* at pålegget eller forbudet må være nødvendig for å oppnå formålet og ikke gå lenger enn det som er nødvendig for å oppnå formålet.

Til § 8 *Ekspropriasjon av beskyttelsesverdig forsvarsteknologi*

Bestemmelsens *første ledd* viderefører i hovedsak gjeldende lov § 6 første ledd som gir staten hjemmel til å kreve at teknologi blir avstått til det offentlige eller andre. Det følger av bestemmelsen at terskelen for å kunne fatte vedtak er «dersom det er nødvendig for å ivareta Forsvarets operative evne». Det innebærer at det må være en risiko for at teknologien eller kompetanse om denne ikke lenger vil være tilgjengelig for Forsvaret i tilstrekkelig grad til å ivareta operativ evne dersom teknologien ikke eksproprieres eller det gis en rett til å utnytte teknologien. En forutsetning for at et vedtak er nødvendig er imidlertid at et vedtak etter § 7 ikke reduserer risikoen i stor nok grad eller gir tilstrekkelig tilgang til teknologien.

Bestemmelsens *andre ledd* fastsetter rett til full erstatning for rettighetshaver ved ekspropriasjon eller der staten eller andre gis rett til å utnytte teknologien i en avgrenset tidsperiode. Utmåling av *full erstatning* skal basere seg på en konkret helhetsvurdering, der ekspropriaten ikke skal stilles i en dårligere økonomisk stilling ved avgivelse av teknologien. Den høyeste verdien av bruks og salgsverdien skal legges til grunn for utmålingen.

For fastsettelse av salgsverdien må det ses hen til hva tilsvarende teknologi selges for. Hvilke utviklingstrinn teknologien er på og hva som gjenstår før teknologien er salgbar vil være sentralt i vurderingen. Ved utmåling av bruksverdi skal det ta utgangspunkt i hva som er en påregnelig utnyttelse av teknologien for virksomheten. Det innebærer en vurdering av utnyttelsespotensialet til de immaterielle rettighetene til produktet, inkludert verdien av eventuelle royalties til teknologien. Ved rett til å utnytte en teknologi skal det ses hen til hva som er markedsverdien for tilsvarende utnyttelsesrett for sammenlignbar teknologi.

Bestemmelsen gir bare rett til erstatning for vedtak om å ikke gi tillatelse til deling, eller vedtak om pålegg eller forbud, der rett til erstatning følger av den alminnelige læren om erstatning for rådighetsbegrensninger i ekspropriasjonsretten. Det innebærer at virksomhetene bare har rett til erstatning der vedtaket vil kunne likestilles med ekspropriasjon. Det vil kunne være tilfelle der det vil være sterkt urimelig at den aktuelle begrensningen skal tåles.[77] Det vil bero på en konkret helhetsvurdering av om den aktuelle begrensingen gir en vesentlig reduksjon i virksomhetens mulighet til å utnytte teknologien.

I vurderingen vil relevante momenter være størrelsen på det økonomiske tapet som følge av vedtaket, og i hvilken grad det fortsatt er praktisk og rettslig mulig for virksomheten å utnytte teknologien. Det vil også måtte ses hen til inngrepets størrelse og virkning i forhold til utnyttelsesmulighetene til teknologien. Hva som er formålet med begrensningene, i hvilken grad begrensingene gjør inngrep i planlagt eller etablert bruk, og i hvilken grad det er gjort investeringer i teknologien, vil også være relevant i vurderingen.

Utmåling av erstatningen vil i disse tilfellene avhenge av det økonomiske tapet som følger av vedtaket.

Til § 9 *Sikkerhetsgraderte patenter*

Bestemmelsen er i all hovedsak en videreføring av gjeldende lov § 7.

Første ledd fastsetter at departementet avgjør saker om sikkerhetsgraderte patenter og hvorvidt et patent skal sikkerhetsgraderes, jf. sikkerhetsloven § 5-3, jf. § 5-4. Avgjørelsen skal tas innen seks måneder fra foreleggelsen, men saksbehandlingstiden kan i særlige tilfeller kan forlenges med inntil tre måneder. *Særlige tilfeller* kan for eksempel være hvor vurderingene er svært kompliserte, det må innhentes innspill fra flere aktører eller hvor informasjonsinnhentingen er av et betydelig omfang. Dersom saksbehandlingstiden forlenges, slår bestemmelsen fast at rettighetshaveren straks skal varsles. At rettighetshaveren skal varsles *straks* innebærer at departementet skal varsle uten ugrunnet opphold. Patentstyrets innføring av sikkerhetsgraderte patenter i et eget register som ikke er tilgjengelig for allmenheten er en videreføring av gjeldende lov § 7 første ledd tredje punktum.

Andre ledd viderefører gjeldende lov § 3 andre ledd første punktum og gir departementet hjemmel til å gi tillatelse til at rettighetshaver innhenter bistand fra andre ved utarbeidelsen av

[77] Se beskrivelsen av rettstilstanden i kapitel 10.1.2.

søknad om sikkerhetsgradert patent. *Andre* enn rettighetshaver kan for eksempel være patentkonsulenter, advokater eller teknologer som kan bistå med råd i forbindelse med patentsøknaden.

Hovedregelen etter loven er at søknader om sikkerhetsgraderte patenter skal innleveres til Patentstyret i Norge. *Tredje ledd* gir departementet likevel adgang til å gi samtykke til at en søknad om sikkerhetsgradert patent leveres til en patentfullmektig eller myndighet utenfor Norge. Det må foretas en konkret vurdering av om tillatelse skal gis og hvorvidt overføringen er i samsvar med nasjonale sikkerhetsinteresser. Overføringen av sikkerhetsgradert informasjon må for øvrig oppfylle kravene i sikkerhetsloven og virksomhetsikkerhetsforskriften. Bestemmelsen fastslår også at en søknad om sikkerhetsgradert patent ikke kan inngis gjennom Patentsamarbeidskonvensjonen eller Den europeiske patentkonvensjonen slik at et inngitt patent ikke har gjensidig virkning i alle medlemsland.

Fjerde ledd fastslår at departementet kan gi forskrift om behandling av hemmelige patentsøknader, meddelte patenter og slike søknader fra fremmede stater.

Til § 10 *Unntak fra patentloven for hemmelige søknader og patenter. Avgradering*

Første ledd viderefører gjeldende lov § 7 første ledd som fastslår unntak fra reglene om allmenn tilgjengelighet, kunngjøring og innsigelse i patentloven §§ 19 til 25.

Andre ledd fastslår unntak fra kravet om betaling av årsavgift for hemmelige patenter etter patentloven §§ 8 og 40.

I henhold til *tredje ledd* kan departementet avgradere hemmelige patenter. Avgjørelsen om avgradering av hemmelige patenter foretas i henhold til reglene i sikkerhetsloven § 5-3 og virksomhetsikkerhetsforskriften. Med mindre departementet bestemmer noe annet, avgraderes hemmelige patenter automatisk ved utløpet av vernetiden. Bestemmelsen fastslår at reglene i patentloven kommer til anvendelse for avgraderte patentsøknader eller patenter.

Fjerde ledd er en videreføring av gjeldende lov § 7 andre ledd femte og sjette punktum. Første punktum fastslår forpliktelsen til å betale årsavgift når Patentstyret har informert patentsøkeren eller patenthaveren om avgraderingen. Det vises forøvrig til bestemmelsen i sin helhet.

Til § 11 *Straff*

Bestemmelsen er i hovedsak en videreføring av gjeldende lov § 10. Bestemmelsen fastslår at forsettlig og uaktsom overtredelse av bestemmelsene om tilgang til beskyttelsesverdig forsvarsteknologi mens den er til vurdering, opplysningsplikt, kravet til tillatelse, påbud eller forbud og sikkerhetsgraderte patenter er straffbart. Bestemmelsene retter seg både mot virksomheter og enkeltpersoner som er rettighetshaver til teknologien eller som på annen måte er pliktsubjektet for bestemmelsene. Strafferammen er bot eller fengsel inntil 1 år med mindre forholdet rammes av et strengere straffebud.

Til § 12 *Ikrafttredelse*

Bestemmelsen slår fast at loven trer i kraft fra det tidspunkt Kongen bestemmer. Ikrafttredelse forutsetter at saksbehandlingsrutinene oppdateres og samhandlingen mellom involverte myndigheter klargjøres.

Til § 13 *Opphevelse*

Når den nye loven trer i kraft oppheves lov av 26. juni 1953 nr. 8 om oppfinnelser av betydning for rikets forsvar.

Forslag til lov om beskyttelse av norsk forsvarsteknologi og sikkerhetsgraderte patenter

§ 1 *Formål*

Loven skal

a) sikre at Forsvaret har tilstrekkelig tilgang til og kontroll med forsvarsteknologi som har vesentlig betydning for operativ evne
b) bidra til at uvedkommende ikke får tilgang slik teknologi
c) sikre at nasjonale forsvars- og sikkerhetsinteresser blir ivaretatt ved deling, utvikling og produksjon av slik teknologi.

§ 2 *Definisjoner*

I loven menes med

a) *forsvarsteknologi*: varer, tjenester og teknologi som kan brukes til forsvarsformål.
b) *nasjonale forsvars- og sikkerhetsinteresser*: evnen til å forsvare norsk territorium, landets suverenitet, territorielle integritet og demokratiske styreform.
c) *sikkerhetsgraderte patenter:* søknader og meddelte patenter som er graderte etter sikkerhetsloven.

§ 3 Beskyttelsesverdig forsvarsteknologi

Departementet kan, med de begrensninger som for følger av folkeretten, fatte vedtak om at forsvarsteknologi som har vesentlig betydning for forsvarets operative evne er beskyttelsesverdig. For at det kan treffes vedtak etter første punktum må forsvarsteknologien være utviklet i Norge, eies av en enkeltperson eller virksomhet som holder til innenfor norsk jurisdiksjon, det må ha blitt søkt patent i Norge, eller virksomheten eller enkeltpersonen har helt eller delvis utnyttelsesrett til teknologien. I vurderingen av om forsvarsteknologi har vesentlig betydning for forsvarets operative evne skal det legges vekt på:

a) I hvilken grad teknologien er tilpasset norske forhold
b) Hvilke kapabiliteter teknologien understøtter og hvilken konsekvens tap av teknologien vil ha for operativ evne
c) I hvilken grad teknologien er tilgjengelig på markedet

d) I hvilken grad teknologien gir forsvarspolitiske fordeler
e) Hvor stor betydning teknologien har for beskyttelses av nasjonal sensitiv informasjon
f) I hvilken grad forsvarsteknologien gir forsvarssektoren kompetanse om hvordan komponenter virker sammen, og kan settes sammen til systemer av betydning for operativ evne
g) Andre forhold som gjør at teknologien har vesentlig betydning for operativ evne

Departementet skal sende melding til eier om at teknologien er til vurdering etter første ledd. Når teknologien er til vurdering kan den ikke deles uten tillatelse fra departementet etter §§ 5 og 6. Forbudet mot deling gjelder ikke lenger enn seks måneder. Har departementet innen fem måneder fremsatt et skriftlig krav om ytterligere opplysninger, avbrytes fristen inntil svaret er mottatt. I særlige tilfeller kan departementet forlenge fristen inntil seks måneder.

Det kan bare gis tilgang til beskyttelsesverdig forsvarsteknologi eller informasjon om teknologien til personer som har tjenstlig behov for tilgang. Dette gjelder også mens teknologien er til vurdering etter første ledd.

Departementet kan gi forskrift om hvilke teknologier som er beskyttelsesverdige og kriterier for når en teknologi er beskyttelsesverdig.

§ 4 *Plikt til å gi opplysninger til departementet*

Når det er grunn til å tro at en forsvarsteknologi er beskyttelsesverdig kan departementet kreve at den som eier, utvikler, bruker eller har tilgang til teknologien gir alle opplysninger som er nødvendig for å vurdere om teknologien er beskyttelsesverdig etter § 3. Opplysningsplikten gjelder uten hinder av lovbestemt eller annen taushetsplikt.

Når departementet krever det skal den som skal dele eller motta beskyttelsesverdig forsvarsteknologi gi alle opplysninger som er nødvendige for å vurdere om tillatelse kan gis etter §§ 5 og 6.

Departementet kan gi forskrift om hvilke opplysninger som kan kreves fra den som eier, utvikler, bruker eller har tilgang til forsvarsteknologi. Departementet kan gi forskrift om hvilke opplysninger som kan kreves fra den som ønsker å dele og mottakeren av beskyttelsesverdig forsvarsteknologi.

§ 5 *Tillatelse til å dele beskyttelsesverdig forsvarsteknologi ut av norsk jurisdiksjon*

Beskyttelsesverdig forsvarsteknologi kan ikke deles med andre utenfor norsk jurisdiksjon uten tillatelse fra departementet. I vurderingen av om tillatelse kan gis skal departementet vurdere risikoen for tap av teknologien, konsekvensene for Forsvarets operative evne ved tap av teknologien, og hvilke fordeler deling av teknologien vil ha for Forsvarets operative evne. Departementet kan sette vilkår for tillatelsen.

I vurderingen av risiko for tap av teknologien skal det legges vekt på:

a) Etterretningstrussel

b) Statlige styringsindikatorer

c) Hvilken tilknytning virksomheten i mottakerlandet har til det aktuelle landet.

d) Mottakerlandets og virksomhetens sikkerhetsmessige modenhetsnivå

e) Forretningsstabilitet.

f) I hvilken grad det kan settes vilkår som reduserer risiko for og konsekvensen av et tap av teknologien.

g) Andre forhold som tilsier at det er risiko for tap av teknologien.

I vurderingen av fordeler for operativ evne skal det legges vekt på om deling vil bidra til forbedring av teknologien, og hvilke konsekvenser deling av teknologien vil ha for Norges forsvars- og sikkerhetspolitiske forhold til mottakerlandet og andre stater.

Kongen kan gi forskrift om tillatelse til deling av beskyttelsesverdig forsvarsteknologi ut fra norsk jurisdiksjon.

§ 6 Tillatelse til å dele beskyttelsesverdig forsvarsteknologi innenfor norsk jurisdiksjon

Beskyttelsesverdig forsvarsteknologi kan ikke deles med andre innenfor norsk jurisdiksjon uten tillatelse fra departementet. I vurderingen av om tillatelse kan gis skal departementet vurdere risikoen for tap av teknologien, konsekvensene for Forsvarets operative evne ved tap av teknologien, og hvilke fordeler deling av teknologien vil ha for Forsvarets operative evne. Departementet kan sette vilkår for tillatelsen.

I vurderingen av risiko for tap skal det legges vekt på mottakerens tilknytning til andre stater, og graden av forsvars- og sikkerhetssamarbeid mellom Norge og de statene mottakeren har tilknytning til. I vurderingen av fordeler for operativ evne skal det legges vekt på om deling vil bidra til forbedring av teknologien.

Kongen kan gi forskrift om tillatelse til deling av beskyttelsesverdig forsvarsteknologi innenfor norsk jurisdiksjon.

§ 7 *Pålegg om eller forbud mot bruk, utvikling eller produksjon av beskyttelsesverdig forsvarsteknologi*

For å ivareta Forsvarets operative evne eller Norges internasjonale eller folkerettslige forpliktelser, kan departementet pålegge eller sette forbud mot en bestemt bruk, utvikling eller produksjon av beskyttelsesverdig forsvarsteknologi. Forbud etter første punktum omfatter begrensninger på tilgang til teknologien og på hvor teknologien kan brukes, utvikles eller produseres.

Pålegg eller forbud kan ikke gå lenger enn det som er nødvendig for å ivareta operativ evne eller Norges internasjonale eller folkerettslige forpliktelser.

Departementet kan gi forskrift om pålegg eller forbud om bruk eller utvikling av beskyttelsesverdig forsvarsteknologi.

§ 8 *Ekspropriasjon av beskyttelsesverdig forsvarsteknologi og rett til utnyttelse av teknologien i en avgrenset tidsperiode*

Dersom det er nødvendig for å ivareta Forsvarets operative evne kan Kongen bestemme at beskyttelsesverdig forsvarsteknologi skal eksproprieres av staten eller andre, eller bestemme at teknologien skal kunne utnyttes i en avgrenset tidsperiode.

Eksproprierer staten beskyttelsesverdig forsvarsteknologi, eller gis staten eller andre rett til å utnytte teknologien i en avgrenset tidsperiode, skal staten betale full erstatning til rettighetshaveren.

Erstatning fastsettes gjennom avtale mellom staten og rettighetshaveren. Dersom staten og rettighetshaveren ikke blir enige, fastsettes erstatningen ved skjønn ved Oslo tingrett.

Erstatning kan betales som en engangssum eller en årlig utbetaling. Fastsettes erstatningen som en årlig utbetaling, skal det fastsettes i skjønnet hvor mange år utbetalingen skal betales. Skal en beskyttelsesverdig forsvarsteknologi avstås til andre enn staten, er staten garantist for at erstatningen blir betalt.

Ekspropriasjon eller rett til å utnytte teknologien etter § 8 kan gjennomføres før erstatningen er fastsatt eller betalt til rettighetshaveren.

Kongen kan gi forskrift om erstatning ved ekspropriasjon og rett til å utnytte teknologien i en avgrenset periode.

§ 9 *Sikkerhetsgraderte patenter*

Departementet avgjør om et patent skal sikkerhetsgraderes etter sikkerhetsloven. Avgjørelsen skal tas innen seks måneder fra foreleggelsen. Før fristen utløper kan den forlenges med inntil tre måneder dersom det foreligger særlige grunner. Rettighetshaveren skal straks varsles om forlengelsen. Patentstyret innfører sikkerhetsgraderte patenter i et eget register som ikke er tilgjengelig for allmenheten.

Departementet kan gi tillatelse til å be andre om bistand til en sikkerhetsgradert patentsøknad.

En søknad om sikkerhetsgradert patent kan bare leveres til en patentfullmektig eller myndighet utenfor Norge etter samtykke fra departementet. En søknad om sikkerhetsgradert patent kan ikke inngis gjennom Patentsamarbeidskonvensjonen eller Den europeiske patentkonvensjonen.

Departementet kan gi forskrift om behandlingen av sikkerhetsgraderte patentsøknader, meddelte patenter og slike søknader fra fremmede stater.

§ 10 *Unntak fra patentloven for sikkerhetsgraderte søknader og patenter. Avgradering*

Patentloven §§ 19 til 25 gjelder ikke for sikkerhetsgraderte patenter.

Kravene om årsavgifter etter patentloven §§ 8 og 40 gjelder ikke for sikkerhetsgraderte patenter.

Departementet kan avgradere sikkerhetsgraderte patenter. Med mindre departementet bestemmer annet, avgraderes sikkerhetsgraderte patenter automatisk ved utløpet av vernetiden. Er en patentsøknad eller et patent avgradert, gjelder reglene i patentloven.

Når Patentstyret har informert patentsøkeren eller patenthaveren om at et patent er avgradert, skal patentsøkeren eller patenthaveren betale årsavgift etter patentloven. Årsavgiften svarer til avgiftsåret etter at Patentstyret har mottatt vedtaket om avgradering. Årsavgiften forfaller ikke i noe tilfelle før to måneder etter at Patentstyret har informert patentsøkeren eller patenthaveren om avgraderingen.

§ 11 *Straff*

Den som forsettlig eller uaktsomt overtrer bestemmelser gitt i eller i medhold av §§ 3, 4, 5, 6, 7 og 9, straffes med bot eller fengsel inntil 1 år, eller begge deler, hvis forholdet ikke går inn under en strengere straffebestemmelse.

§ 12 *Ikrafttredelse*

Loven trer i kraft fra det tidspunktet Kongen bestemmer.

§ 13 *Opphevelse*

Fra det tidspunktet loven trer i kraft, oppheves lov av 26. juni 1953 nr. 8 om oppfinnelser av betydning for rikets forsvar.