Datum
2009-10-29

Dnr (åberopas vid korresp.)
AD001-8770-09

Er referens
Ju2009/5174/PO

Justitiedepartementet
103 33 Stockholm

Förstudierapport
Översyn av säkerhetsskyddslagen

Sammanfattning

Vid en allmän översyn av säkerhetsskyddslagen bör ett antal övergripande frågor behandlas. Som exempel kan anges följande.

Det finns behov av att klargöra syftet med säkerhetsskydds-lagstiftningen och utreda vad lagstiftningens fokus och inriktning bör vara. Det bör utredas om innebörden av begreppet rikets säkerhet kan tydliggöras eller om lagstiftningens tillämpningsområde ska knyta an också till andra begrepp.

En annan viktig fråga är hur säkerhetsskyddslagstiftningen kan anpassas till dagens teknik och informationssamhälle. Lagstiftningen fokuserar idag på konfidentialitet medan tillgänglighets- och riktighetsfrågor inte beaktas.

Vidare bör utredas om säkerhetsskyddslagstiftningens koppling till offentlighets- och sekretesslagen (2009:400) ska ändras så att lagen i större utsträckning kan omfatta verksamhet som bedrivs av enskilda och statligt ägda bolag.

Bestämmelserna om säkerhetsskyddad upphandling bör förenklas och anpassas till moderna förhållanden. Det bör också utredas om tillsynsverktyget behöver utvecklas,

Postadress
Box 12312
102 28 STOCKHOLM

Besöksadress
Polhemsgatan 30
STOCKHOLM

Telefon
010-568 70 00
08-568 81 83 (direkt)

Telefax
010-568 70 10

sakerhetspolisen@sakerhetspolisen.se
www.sakerhetspolisen.se
Org.nr 202100-0076

kompletteras med sanktionsmöjligheter eller andra instrument, eller om det bör ersättas med annat verktyg.

Det bör också utredas om möjligheterna till registerkontroll behöver utökas. Det bör även tydliggöras vad som avses med registerkontroll. Inom ramen för översynen bör också frågan om Personal Security Clearance (PSC) lösas.

Slutligen bör utredas hur frågan om en nationell säkerhetsmyndighet (NSA), verkställande säkerhetsmyndighet (DSA) och nationell signalskyddsmyndighet (NCSA) ska lösas i svensk lagstiftning.

I många av de ovan nämnda frågeställningarna torde en internationell jämförelse vara av värde.

1 Uppdraget

Regeringen har i beslut den 17 juni 2009 gett Säkerhetspolisen i uppdrag att göra en förstudie över de frågeställningar som myndigheten bedömer bör behandlas i en allmän översyn av säkerhetsskyddslagstiftningen och det behov av säkerhetsskydd som kan finnas i olika slags verksamheter. Enligt uppdraget ska Säkerhetspolisen vid utförande av uppdraget i den omfattning det behövs samråda med närmast berörda myndigheter och näringslivsorganisationer.

Uppdraget ska enligt beslutet redovisas senast den 1 november 2009.

2 Om förstudien

Säkerhetspolisen har inom ramen för förstudien samrått med Lantmäteriet, Transportstyrelsen, Åklagarmyndigheten, Skatteverket, Svenska Kraftnät, Myndigheten för samhällsskydd och beredskap (MSB), Strålsäkerhetsmyndigheten, Rikspolisstyrelsen, Försvarsmakten, Försvarets materielverk (FMV), Post- och telestyrelsen (PTS), Inspektionen för strategiska produkter (ISP), Livsmedelsverket, Göteborgs kommun, Länsstyrelsen i Stockholms län, Teracom, Vattenfall, Sveriges kommuner och landsting samt Stockholms stad och Säkerhets- och integritetsskyddsnämnden.

Samrådet har bl.a. bestått i en hearing med representanter för ovanstående myndigheter m.fl. där frågeställningar relevanta för en översyn av säkerhetsskyddslagen behandlats. Myndigheterna har också fått möjlighet att lämna synpunkter på ett utkast till förstudierapport.

3 Behovet av en översyn av säkerhetsskyddslagen

3.1 Säkerhetsskyddslagstiftningen idag

Säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordningen (1996:633) trädde i kraft den 1 juli 1996. Säkerhetsskyddet ska enligt 6 § säkerhetsskyddslagen omfatta
- skydd mot brott som kan hota rikets säkerhet,
- skydd för uppgifter som omfattas av sekretess och rör rikets säkerhet, samt
- skydd mot terroristbrott, även om de inte hotar rikets säkerhet.

Lagen gäller enligt 1 § vid verksamhet hos staten, kommunerna och landstingen samt hos juridiska personer över vilka staten, kommuner eller landsting utövar ett rättsligt bestämmande inflytande. Lagen ska vidare gälla hos enskilda, om verksamheten är av betydelse för rikets säkerhet eller särskilt behöver skyddas mot terrorism.

Säkerhetsskyddslagstiftningen är således, vid sidan av skyddet mot terrorism, koncentrerad till ett skydd mot hot mot rikets säkerhet (prop. 1995/96:129 s. 25). Utgångspunkten när lagstiftningen trädde i kraft var att de intressen som lagstiftningen slår vakt om ska ha samma skydd oavsett om verksamheten bedrivs av det allmänna eller av enskilda.

3.2 Förändrade förutsättningar för säkerhetsskyddet

Sedan lagstiftningen infördes har förutsättningarna för och behovet av säkerhetslösningar kommit att ändra karaktär. Detta beror bl.a. på teknikutveckling, avreglering av marknader för samhällsviktig infrastruktur, ökande internationell samverkan och nya hot mot samhället.

3.2.1 Teknikutveckling

När den nuvarande lagstiftningen utarbetades i början av 1990-talet användes datorn främst som en skrivmaskin, dvs. för dokumentation. Den explosionsartade tekniska utvecklingen under de senaste decennierna har fått genomgripande konsekvenser i västvärlden. En övervägande del av befolkningen har idag tillgång till bredband och mobiltelefoni. Både det svenska näringslivet och den offentliga sektorn bedriver också alltmer av sin verksamhet med stöd av Internet. Datorn används till att producera, distribuera och konsumera information. I stor utsträckning görs detta över Internet och i många fall sker det automatiskt utan att någon människa hanterar informationen. Dagens datorer kopplas ihop genom omfattande nätverk och utbyter information i en betydligt större utsträckning än tidigare. De tjänster som datorer användes för vid lagens tillkomst är således väsensskilda från de tjänster som de används till idag; digitala ekonomitjänster för deklaration och bankärenden, kommunikationstjänster som Internet, fast och mobil telefoni samt möjligheter att fjärrstyra system för t.ex. el, och vattenförsörjning samt kommunikationer. Informationstekniken genomsyrar idag i stort sett alla aspekter av samhällsviktiga verksamheter och fungerande IT-system är nödvändiga för att verksamheterna i samhället ska fungera. I samma takt som teknikberoendet blivit större har komplexiteten i systemen och verksamheterna ökat.

Den tekniska utvecklingen har också medfört att ett antal samhällsviktiga verksamheter effektiviserats och att medborgarna blivit alltmer vana vid att kunna ställa höga krav på att elektronisk information är tillgänglig och riktig. Därmed har också kraven på säkerhetslösningar förändrats – de lösningar som tillgodoser kraven på tillgänglighet och riktighet skiljer sig många gånger från de lösningar som kan garantera att informationens konfidentialitet skyddas. Det omfattande IT-beroendet inom den samhällsviktiga infrastrukturen, t.ex. tele- och datakommunikation, elförsörjning och transporter, gör samtidigt dagens samhälle mer sårbart än det varit tidigare. Denna sårbarhet berör såväl myndigheter som organisationer, företag och enskilda. Störningar i viktiga IT-system kan snabbt ge omfattande konsekvenser för stora delar av samhället, vilket är en relativt ny företeelse.

De ovan nämnda faktorerna har ändrat förutsättningarna för och behovet av säkerhetslösningar jämfört med hur situationen var vid säkerhetsskyddslagens tillkomst. Det gäller såväl vilka uppgifter som måste betraktas som skyddsvärda idag som vilka aktörer som bör omfattas av säkerhetsskyddslagstiftningen.

3.2.2 Avreglering av marknader för samhällsviktig infrastruktur

Under 1990-talet avreglerades bl.a. el- och telekommunikationsmarknaderna, vilket ledde till förändrade ansvarsförhållanden för dessa samhällsviktiga verksamheter. Idag finns en övervägande del av de verksamheter som är viktiga för det svenska samhällets funktionalitet inte under direkt statligt inflytande. Verksamheten drivs och förvaltas istället av företag verksamma i näringslivet. Detta gäller bl.a. inom områdena elförsörjning och kommunikation. Denna avreglering hade ännu inte hunnit få något större genomslag vid utformandet av säkerhetsskyddslagstiftningen under mitten av 1990-talet.

Av ekonomiska skäl och effektivitetsskäl väljer många verksamheter idag att köpa in svenska eller utländska företag för att utveckla och/eller hantera säkerhetskänsliga IT-system via s.k. outsourcing och offshoring. Dessa faktorer försvårar arbetet med säkerhetsskydd eftersom det medför att säkerhetsskyddslagstiftningen endast är tillämplig i begränsade delar.

3.2.3 Ökande internationell samverkan

Ett fenomen som inte är nytt men som blivit alltmer påtagligt de senaste decennierna är den ökade internationella samverkan mellan stater och den allmänna globaliseringen. Sverige samverkar med andra länder både inom ramen för EU och andra internationella organisationer och samarbeten, som exempelvis Nato och Europeiska rymdorganet (ESA). Personer, varor, tjänster etc. rör sig över statsgränserna i en allt större utsträckning. Kommunikationen och informationsöverföringen mellan länder

ökar härtill ständigt till följd av möjligheten till elektronisk kommunikation (Internet och telefoni).

Globaliseringen har medfört att gråzonen mellan rikets inre och yttre säkerhet har ökat och att begreppet nationell säkerhet har utvidgats. Också detta är faktorer som har ändrat förutsättningarna för och behovet av säkerhetslösningar jämfört med hur det såg ut vid säkerhetsskyddslagens tillkomst.

3.2.4 Nya hot mot säkerheten

När säkerhetsskyddslagen infördes upplevdes fortfarande det största hotet mot Sverige vara risken för ett storkrig mellan maktblocken i Europa och försvaret inriktades därför på att möta en invasion av landets territorium.

Enligt propositionen Vårt framtida försvar (prop. 2004/05:5) bedöms ett enskilt militärt angrepp från en annan stat direkt mot Sverige som osannolikt under överskådlig tid. Istället utgörs de hot som bedöms kunna få säkerhetspolitiska konsekvenser i Sverige av internationell terrorism och andra typer av grov internationell kriminalitet, spridning av massförstörelsevapen samt framställning och transport av vapen, komponenter och teknologi (a. prop. s. 12).

Elektroniska angrepp i olika former betraktas idag som ett av de allvarligare hoten. Elektroniska angrepp kan genomföras anonymt via Internet och från valfri geografisk plats vilket minimerar risken för att angriparen upptäcks och lagförs. Elektroniska angrepp kräver dessutom relativt begränsade resurser och kompetens, även om riktigt avancerade attacker kan vara resurskrävande. Konsekvenserna av en elektronisk attack kan bli allvarliga för vissa verksamheter och kan ibland även påverka rikets säkerhet, t.ex. inom finans-, telekommunikations- och energiförsörjningsområdet.

Att hotens karaktär är annorlunda idag jämfört med tidigare märks också i Säkerhetspolisens verksamhet. Från att tidigare i stor utsträckning ha fokuserat på försvarsindustri och försvarsförmåga har främmande staters underrättelseverksamhet de senaste decennierna dessutom breddats mot forskning och utveckling inom civila områden samt mot politiska frågor. Även information som rör samhällsviktiga system har varit föremål för underrättelse-inhämtning från främmande stat.

Sammanfattningsvis är hoten mot säkerheten i Sverige i vid mening av en delvis annan karaktär än de var vid säkerhetsskydds-lagstiftningens tillkomst.

4 Vilka frågor bör behandlas inom ramen för en allmän översyn av säkerhetsskyddslagstiftningen?

Som framgått ovan har utvecklingen medfört att det finns anledning att se över säkerhetsskyddslagstiftningens uppbyggnad och innehåll. I det följande diskuteras vilka punkter som bör behandlas inom ramen för en översyn av säkerhetsskydds-lagstiftningen.

4.1 Lagstiftningens fokus och uppbyggnad

Frågor som bör ingå i en översyn av säkerhetsskyddslagen:
* Vad är syftet med säkerhetsskyddslagstiftningen? Vad bör lagstiftningens fokus och inriktning vara?
* Kan innebörden av begreppet rikets säkerhet tydliggöras eller ska lagstiftningens tillämpningsområde även knyta an till andra begrepp? Hur förhåller sig begreppet rikets säkerhet till behovet av skydd mot terrorism?
* Bör lagstiftningens koppling till offentlighets- och sekretesslagen ändras så att lagen i större utsträckning kan omfatta verksamhet som bedrivs av enskilda och statligt ägda bolag? Bör lagen i större utsträckning gälla generellt ifråga om myndigheter?
* Hur ska de olika lagar som innehåller bestämmelser om skydd mot terrorism (t.ex. lagen [1990:217] om skydd för samhällsviktiga anläggningar, lagen [2006:1209] om hamnskydd samt lagen [2004:1100] om luftfartsskydd etc.) förhålla sig till säkerhetsskyddslagstiftningen?

Med säkerhetsskydd avses framför allt skydd mot brott som kan hota rikets säkerhet och skydd för uppgifter som omfattas av sekretess och rör rikets säkerhet. Säkerhetsskyddslagstiftningen är således främst fokuserad på *rikets säkerhet*.

Det finns inte någon legaldefinition av begreppet rikets säkerhet. I förarbetena till säkerhetsskyddslagen uttalas att rikets säkerhet i korthet kan sägas avse såväl den yttre säkerheten för det nationella oberoendet som den inre säkerheten för det demokratiska statsskicket (prop. 1995/96:129 s. 22). I förarbetena uttalas vidare bl.a. att skyddet för den yttre säkerheten i dag i första hand tar sikte på totalförsvaret. Ett hot mot rikets yttre säkerhet kan emellertid förekomma även om det inte utgör ett hot mot totalförsvaret. Vad gäller rikets inre säkerhet anförs i de ovan nämnda förarbetena till säkerhetsskyddslagen att den inre säkerheten kan vara hotad utan att totalförsvaret berörs. T.ex. kan angrepp mot rikets demokratiska statsskick förekomma från olika grupperingar utan förbindelse med främmande makt.

Säkerhetspolisens erfarenhet är att man inom många verksamheter förknippar begreppet rikets säkerhet med totalförsvaret och framförallt försvarshemligheter.

Som framgått ovan är dock de hot som idag finns mot Sverige av delvis en annan karaktär. Utöver internationell terrorism och andra typer av grov internationell kriminalitet, har elektroniska attacker i form av t.ex. skadlig kod blivit allt vanligare. Det finns ingen anledning att tro att den utvecklingen kommer att avstanna. När det gäller främmande staters underrättelseverksamhet är det numera forskning och utveckling inom civila områden (bl.a. företags-hemligheter), politiska frågor och information rörande samhällsviktiga system som framförallt är av intresse, inte, som förr, endast försvarsrelaterade hemligheter.

Lagstiftningens fokus på begreppet rikets säkerhet medför att myndigheter och företag i många fall inte uppfattar att säkerhetsskyddslagstiftningen är relevant för deras verksamhet. Detta bidrar till att urholka betydelsen av säkerhetsskydds-lagstiftningen. Att innebörden av begreppet rikets säkerhet inte uppfattas som relevant innebär också en konkret fara såtillvida att myndigheter m.fl. riskerar att misslyckas med att skydda verksamhet av betydelse för samhället som t.ex. verksamheter som ska förebygga och hantera allvarliga kriser.

Begränsningen till uppgifter som rör rikets säkerhet utesluter vidare uppgifter som omfattas av sekretess men som *inte* rör rikets säkerhet. Detta innebär bl.a. att uppgifter som mottagits av svenska myndigheter etc. inom ramen för ett internationellt samarbete, riskerar att falla utanför säkerhetsskyddslagstiftningen. Sverige har i flera internationella sammanhang åtagit sig att uppfylla utländska säkerhetsskyddskrav. Detta gäller t.ex. inom ramen för samarbetet Partnerskap för fred i vilket Sverige ingått ett säkerhetsskyddsavtal med Nato. Vidare har Sverige till följd av medlemskapet i det Europeiska rymdorganet (ESA) åtagit sig att tillämpa ESA:s säkerhetsbestämmelser. Som medlem i Europeiska unionen föreligger också förpliktelser för Sverige i och med att medlemsstaterna är skyldiga att respektera Europeiska unionens råds säkerhetsbestämmelser (2001/264/EG). Vidare har Sverige ett flertal bilaterala överenskommelser där krav på säkerhetsskydd finns. Det är angeläget att säkerhetsskyddslagstiftningen utformas på ett sätt som säkerställer att dessa åtaganden kan uppfyllas.

Utgångspunkten för säkerhetsskyddslagstiftningen är att de intressen som lagstiftningen ska slå vakt om, t.ex. skyddet av uppgifter som rör rikets säkerhet, ska ha samma skydd oavsett om den verksamhet där uppgifterna förekommer bedrivs av det allmänna eller av enskilda rättssubjekt. Säkerhetsskyddslagens koppling till offentlighets- och sekretesslagen medför dock att enskilda rättssubjekt faller utanför säkerhetsskyddslagens tillämpningsområde i flera viktiga avseenden. Detta eftersom

offentlighets- och sekretesslagen bara är tillämplig på myndigheter, kommuner och landsting, och bolag m.fl. där kommun eller landsting har ett bestämmande inflytande samt vissa andra, särskilt angivna organ såvitt avser den verksamhet som anges (bl.a. AB Svensk Bilprovning såvitt avser fordonskontroll). Som exempel kan nämnas att ett privatägt elbolag inte kan underställas kravet på skydd för sekretessbelagda uppgifter rörande rikets säkerhet eftersom bolaget inte hanterar några uppgifter som omfattas av sekretess i deras verksamhet (7 § p. 2 säkerhetsskyddslagen). Ett annat exempel är att inplacering i säkerhetsklass inte kan ske hos ett sådant elbolag eftersom sådan inplacering förutsätter att den anställde eller den som annars deltar i verksamheten får del av viss mängd uppgifter som omfattas av sekretess (17 § säkerhetsskyddslagen). I takt med avregleringen av statlig verksamhet har det område inom vilket säkerhetsskyddsregelverket inte är tillämpbart kommit att öka alltmer. Det kan därför diskuteras om kopplingen till offentlighets- och sekretesslagen begränsar säkerhetsskyddslagens tillämpningsområde på ett sätt som inte var tänkt ursprungligen.

Vidare är det viktigt att vid en översyn av säkerhetsskydds-lagstiftningen klarlägga hur annan lagstiftning t.ex. lagen om skydd för samhällsviktiga anläggningar m.m., lagen om hamnskydd respektive luftfartsskydd ska förhålla sig till säkerhetsskydds-lagstiftningen.

4.2 Säkerhetsskydd och informations- och IT-säkerhet

Följande frågor bör ingå i en översyn av säkerhetsskyddslagen:
* Hur kan lagstiftningen anpassas till dagens teknik och informationssamhälle?
* Bör de svenska reglerna om klassificering av information anpassas till vad som gäller i Europa och annars internationellt?
* Hur ska säkerhetsgodkännande av informationssystem som ska anslutas till utländskt informationssystem hanteras i svensk lagstiftning?

När det gäller informationssäkerhetsområdet är dagens säkerhetsskydd inriktat på att förebygga att uppgifter som omfattas av sekretess och som rör rikets säkerhet obehörigen röjs, ändras eller förstörs (7 § säkerhetsskyddslagen).

Säkerhetsskyddslagen syftar alltså till att skydda sekretessbelagda uppgifter rörande rikets säkerhet från obehörig påverkan eller röjande. När säkerhetsskyddslagen infördes i mitten på 90-talet förekom sekretessbelagda uppgifter som rörde rikets säkerhet främst i pappersdokument.

Idag hanteras nästan all information, såväl hemlig som öppen, i IT-system. Även t.ex. produktion och distribution av dricksvatten och

elektricitet, är idag beroende av digitala system för styrning, reglering och övervakning (s.k. SCADA-system). Dessa system exponeras därmed för de hot som finns på Internet, däribland traditionella störningar i form av skadlig kod och risken för cyberattacker.

Nuvarande säkerhetsskyddslagstiftning reglerar endast skyddet mot att de (hemliga) uppgifter som finns i ett IT-system röjs. Däremot saknas regler om säkerhetsskydd avseende IT-systems övriga funktioner, t.ex. funktioner för tillgänglighet och riktighet.

Ett IT-systems funktion kan, sett tillsammans med de uppgifter som finns i systemet, vara av stor betydelse för rikets säkerhet. Exempel på detta finns bl.a. i de verksamheter som producerar/distribuerar drickvatten och elektricitet, men även i den verksamhet som bedrivs inom finanssektorn och av myndigheter som Skatteverket, Försäkringskassan och Riksgälden. De nämnda myndigheterna hanterar endast i mindre utsträckning hemliga uppgifter som rör rikets säkerhet. Däremot har myndigheterna det gemensamt att de har ett antal komplexa och centrala IT-system som måste vara tillgängliga och innehålla riktig information för att det svenska samhället ska fungera och medborgarnas förtroende för statens verksamhet bibehållas. IT-systemen är samhällsviktiga och av stor betydelse för rikets säkerhet.

I säkerhetsskyddsförordningen finns idag föreskrifter om att vissa typer av IT-system ska vara försedda med funktioner för behörighetskontroll och s.k. säkerhetsloggning. Med hänsyn till teknikutvecklingen bör övervägas om inte även andra säkerhetsfunktioner, såsom bl.a. skydd mot obehörig avlyssning och intrångsskydd, bör införas i säkerhetsskyddet.

En annan fråga som behöver utredas är den samrådsskyldighet som föreskrivs i 12 § säkerhetsskyddsförordningen. Exempelvis bör det övervägas om kretsen av samrådsskyldiga ska utökas. Även formerna för samrådsförfarandet bör studeras.

En annan informationssäkerhetsrelaterad fråga som blivit alltmer aktuell i takt med samhällets utveckling är behovet av s.k. informationsklassificering. Den omfattande internationella samverkan som idag förekommer mellan Sverige å ena sidan och andra länder och mellanfolkliga organisationer å andra sidan har stor betydelse för frågan om informationsklassificering. I internationella säkerhetsbestämmelser, exempelvis inom EU och Nato samt flertalet länder i Europa, är skyddet för motsvarigheten till hemliga uppgifter indelat i fyra säkerhetsskyddsnivåer, restricted, confidential, secret och top secret. Avsaknaden av motsvarande svenska regler innebär problem i Sveriges relationer till andra länder och mellanfolkliga organisationer. Det kan i sammanhanget nämnas att hanteringen av nyssnämnda slag av uppgifter är reglerad i författning avseende vissa statliga

myndigheter inom försvarssektorn.[1] Förhållandet gör det svårt för myndigheter m.fl. utanför försvarssektorn att bedöma hur de utländska säkerhetsskyddsnivåerna ska förhålla sig till de svenska säkerhetsskyddsreglerna.

4.3 Säkerhetsprövning, säkerhetsklasser och registerkontroll

Följande frågor bör ingå i översynen av säkerhetsskyddslagen:
* Hur bör bestämmelserna om säkerhetsprövning utformas för att säkerställa en adekvat säkerhetsnivå i samhället?
* Bör systemet anpassas för att fungera även i internationella sammanhang?
* Bör fler myndigheter och organisationer (bolag, stiftelser m.fl.) ha möjlighet att besluta om placering i säkerhetsklass?
* Behöver möjligheterna till registerkontroll utökas, t.ex. vad avser registerkontroll till skydd mot terrorism? Det bör tydliggöras vad som avses med registerkontroll.
* Hur ska frågan om Personal Security Clearance (PSC) hanteras i Sverige?

Innan en person anställs eller på annat sätt får delta i verksamhet som är av betydelse för rikets säkerhet, eller anlitas för uppgifter som är viktiga för skyddet mot terrorism, ska en säkerhetsprövning göras. Prövningen ska klarlägga om personen kan antas vara lojal mot de intressen som skyddas i säkerhetsskyddslagen och om personen i övrigt är pålitlig från säkerhetssynpunkt. Prövningen ska också, under vissa förutsättningar, omfatta registerkontroll och särskild personutredning (11 § säkerhetsskyddslagen). Säkerhetsprövning kan sammanfattningsvis beskrivas som den sammanvägda bedömningen av en persons lojalitet och pålitlighet som en arbetsgivare gör för att avgöra om personen kan få en viss anställning eller ett visst uppdrag.

En person som har genomgått säkerhetsprövning kan få en anställning eller ett uppdrag som är placerat i säkerhetsklass. Som lagstiftningen är uppbyggd kan placeringen i säkerhetsklass endast ske i verksamheter som omfattas av offentlighets- och sekretesslagen. Det finns emellertid verksamheter som är skyddsvärda även om inte sekretessbelagda uppgifter hanteras i verksamheten. Detta gäller t.ex. inom kärnkraftsindustrin. Det är angeläget att också personer som arbetar med sådan samhällsviktig och skyddsvärd verksamhet kan bli föremål för säkerhetsprövning. Det bör därför utredas om reglerna om säkerhetsprövning bör förändras.

[1] Försvarsmaktens föreskrifter (FFS 2007:3) om säkerhetsskydd gäller numera för Fortifikationsverket och Försvarshögskolan samt de myndigheter som lyder under Försvarsdepartementet, utom Kustbevakningen, Myndigheten för samhällsskydd och beredskap och Statens haverikommission (jfr 39 § säkerhetsskyddsförordningen).

Det finns även andra skäl till att systemet med säkerhetsprövning bör ses över. Idag är det vanligt att myndigheter och företag vid tillsättning av anställningar placerade i säkerhetsklass lägger alltför stor vikt vid, och ibland till och med uteslutande förlitar sig på, resultatet av en utförd registerkontroll och därför underlåter att genomföra de ytterligare åtgärder som ska innefattas i en säkerhetsprövning. Detta är en brist eftersom en registerkontroll aldrig ger en helhetsbild av en person. För att få en tillfredsställande bild av en persons pålitlighet är det nödvändigt att också genomföra intervjuer och inhämta referenser rörande den potentiella arbetstagaren. Med tanke på de stora skyddsvärden som kan stå på spel vid tillsättning av en säkerhetsplacerad anställning är det en samhällelig angelägenhet att systemet med säkerhetsprövning fungerar på ett bra sätt. Frågan om hur systemet bör vara utformat för att uppnå detta bör belysas i översynen.

Det finns idag tre olika säkerhetsklasser (säkerhetsklass 1, 2 respektive 3). Vilken säkerhetsklass en person placeras i beror i huvudsak på vilken mängd hemliga uppgifter personen kommer att hantera i sin anställning. Detta är en skillnad i förhållande till vad som gäller internationellt, eftersom de flesta länder har ett system som bygger på vilken nivå av uppgifter personen kommer att hantera, dvs. på hur skyddsvärda de hemliga uppgifterna är. För att ytterligare belysa skillnaderna kan sägas att i Sverige analyseras befattningarna och åsätts en säkerhetsklass medan man i andra länder knyter säkerhetsklassen till en individ. Skillnaderna mellan de svenska och de internationella reglerna medför problem i internationella sammanhang då den svenska lagstiftningen inte kan översättas till och förstås av internationella organ, utländska arbetsgivare etc.

För befattningar som placerats i säkerhetsklass krävs enligt huvudregeln att den anställde innehar svenskt medborgarskap, även om regeringen i ett enskilt fall kan medge undantag. Inom vissa verksamheter är det emellertid nödvändigt att ha tillgång till kompetens som inte finns att tillgå i Sverige, eller kompetens från flera länder. Mot bakgrund av den alltmer integrerade europeiska arbetsmarknaden kan diskuteras om kravet i säkerhetsskyddslagen på svenskt medborgarskap i alla situationer är relevant. Detta gäller naturligtvis endast sådana befattningar som inte kräver svenskt medborgarskap enligt 11 kap. 9 § regeringsformen.

Om en anställning eller ett deltagande i verksamheten har placerats i säkerhetsklass, eller om det behövs för skyddet mot terrorism, får s.k. registerkontroll utföras. Den aktuella personen kontrolleras då gentemot bl.a. belastningsregistret, misstankeregistret och Säpo-registret (12 § säkerhetsskyddslagen). Säkerhetspolisen genomför registerkontroll efter ansökan från behörig myndighet och samtycke från den person som ska kontrolleras. Om registerkontrollen resulterar i en träff, dvs. om uppgifter om personen finns i något av registren, är det registerkontroll-

delegationen inom Säkerhets- och integritetsskyddsnämnden som avgör om uppgiften ska lämnas ut till arbetsgivaren.

De nuvarande reglerna om registerkontroll inrymmer flera dilemman som bör lösas vid en översyn av säkerhetsskydds-lagstiftningen.

Möjligheterna att utföra registerkontroll till skydd mot terrorism är mer begränsade än möjligheterna till registerkontroll i andra fall eftersom registerkontroll till skydd mot terrorism enligt huvudregeln endast får göras ifråga om den som ska anställas eller delta i verksamhet vid vissa särskilt angivna anläggningar, t.ex. flygplatser, anläggningar som förklarats som skyddsobjekt etc. (26-27 §§ säkerhetsskyddsförordningen). I och med att möjligheten till registerkontroll är begränsad till särskilt angivna anläggningar, saknas grund för att utföra registerkontroll till skydd mot terrorism t.ex. i fråga om transporter av kärnämnen och kärnavfall.

När det gäller skydd mot terrorism bör reglerna om s.k. spontanuppföljning förtydligas. Det kan ifrågasättas om det finns skäl att göra skillnad mellan registerkontroll till skydd mot terrorism och registerkontroll i andra syften.

I detta sammanhang noteras att det bör tydliggöras vad som avses med registerkontroll. En ren bokstavstolkning av aktuell bestämmelse tyder på att registerkontrollen endast ska omfatta sådana register till vilka Säkerhetspolisen har direktåtkomst, vilket möjligen inte torde vara avsikten.

Det nuvarande systemet med en fristående delegation som ska avgöra om uppgifter som framkommer vid registerkontroll ska lämnas ut ska tillgodose behovet av att känsliga uppgifter inte sprids i onödan. Det har dock framförts uppfattningar om att systemet är opraktiskt och i vissa avseenden till och med olämpligt. Det kan till exempel vara svårt för registerkontrolldelegationen att avgöra vilka uppgifter som faktiskt är relevanta att lämna ut. Några av de myndigheter Säkerhetspolisen har varit i kontakt med upplever också att nämnden har blivit mer restriktiv i fråga om vilka uppgifter som lämnas ut. Vidare har det lämpliga i att en arbetsgivare får kännedom om vilka uppgifter som finns registrerade rörande en person, som arbetsgivaren kanske inte ens kommer att anställa, ifrågasatts. Slutligen är det motsägelsefullt att om Säkerhetspolisen i sin brottsförebyggande verksamhet får kännedom om att en person med anställning placerad i säkerhetsklass agerar på ett sätt som inte är lämpligt ur säkerhetssynpunkt, så kan myndigheten inte vidta brottsförebyggande åtgärder om det innebär att arbetsgivaren måste informeras. Istället måste Säkerhets- och integritetsskyddsnämnden avgöra om informationen får lämnas vidare. Om personen istället arbetar hos en privat arbetsgivare, och alltså inte har en

säkerhetsklassad anställning, finns det inte samma hinder för Säkerhetspolisen att vidta brottsförebyggande åtgärder.

Myndigheter och andra som säkerhetsskyddsförordningen gäller för och som har beslutat om registerkontroll ska dokumentera resultatet av säkerhetsprövningen när det gäller en person som bedömts vara pålitlig från säkerhetssynpunkt. Vilka krav på dokumentation av den säkerhetsprövning som skett utan att registerkontroll utförts är oklart med dagens lagstiftning. Vidare finns inte något krav på dokumentation av säkerhetsprövning när en person bedömts inte vara pålitlig från säkerhetssynpunkt. Frågorna rörande dokumentation bör behandlas inom ramen för en översyn av säkerhetsskyddslagstiftningen.

Som nämnts ovan (4.1) kan inplacering i säkerhetsklass inte ske hos ett privat bolag, t.ex. ett elbolag eller kärnkraftverk, eftersom sådan inplacering förutsätter att offentlighets- och sekretesslagen är tillämplig. Det kan diskuteras om inte fler myndigheter och organisationer (bolag, stiftelser m.fl.) bör får möjlighet att besluta om placering i säkerhetsklass.

Med anledning av den alltmer internationaliserade arbetsmarknaden uppkommer också frågan om hur man i Sverige ska hantera de intyg över säkerhetsprövning som numera är vanligt förekommande i andra länder, s.k. Personal Security Clearance (PSC). I dagens internationaliserade samhälle med affärsverksamhet över landgränserna är sådana intyg mycket viktiga eftersom de visar att en person är godkänd för att hantera hemliga uppgifter. Med dagens regler kan ett PSC i praktiken endast utfärdas i de fall personen i fråga innehar en anställning som är placerad i säkerhetsklass. Det kan diskuteras om detta innebär en diskriminering eller i vart fall ett hinder mot den fria rörligheten.

Frågan om hur systemet med PSC ska lösas i svensk lagstiftning innefattar flera rättsliga och organisatoriska aspekter, t.ex. vad som ska omfattas av och ligga till grund för ett PSC, om utfallet av kontrollen ska vara absolut eller endast vägledande för arbetsgivaren vid dennes beslut om anställning, vilken instans som ska utfärda PSC etc.

4.4 Säkerhetsskyddad upphandling

Följande frågor bör ingå i en översyn av säkerhetsskyddslagen:
* Bör tillämpningsområdet för reglerna om säkerhetsskyddad upphandling utökas?
* Hur kan reglerna förenklas och anpassas till moderna förhållanden?

När staten, kommuner och landsting avser att begära in anbud eller träffa avtal om upphandling där det förekommer uppgifter som med hänsyn till rikets säkerhet omfattas av sekretess ska de träffa säkerhetsskyddsavtal med den aktuella leverantören.

Reglerna om säkerhetsskyddad upphandling har sin bakgrund i en tid då statligt och kommunalt ägda bolag inte var lika vanligt förekommande som idag och då myndigheter ofta drev projekt i egen regi och endast i vissa fall använde sig av externa leverantörer. I dag har situationen på flera sätt förändrats. Reglerna rörande säkerhetsskyddad upphandling har dock inte anpassats, varför de framstår som både ofullständiga och svårtillämpbara.

Ett exempel på att det finns luckor i regelverket rörande säkerhetsskyddad upphandling är att skyldigheten att upprätta säkerhetsskyddsavtal vid upphandling enligt ordalydelsen i 8 § säkerhetsskyddslagen inte omfattar enskilda eller rättssubjekt över vilka staten, kommunen eller landstinget utövar ett rättsligt bestämmande inflytande. Det gäller även om de bedriver verksamhet som är av betydelse för rikets säkerhet eller som särskilt behöver skyddas mot terrorism. Det saknas således regler om hur säkerhetsskyddsfrågan ska hanteras när sådana rättssubjekt gör upphandlingar där hemliga uppgifter förekommer. Detta är en brist, särskilt med tanke på den ökade försäljningen och bolagiseringen av statlig verksamhet som ägt rum de senaste åren. Som framgått ovan är det inte ovanligt att sådan försäljning och bolagisering omfattar verksamhet som är känslig ur säkerhetssynpunkt, t.ex. produktion och distribution av elkraft och telekommunikation (jfr avsnitt 3.2.2 och 4.1).

En annan situation som regelverket inte omfattar är upphandling när det visserligen inte kan sägas förekomma uppgifter som med hänsyn till rikets säkerhet omfattas av sekretess men när upphandlingen likaväl berör en känslig verksamhet som exempelvis bör skyddas mot terrorism (t.ex. elproduktion, jfr avsnitt 4.1). Det bör utredas om inte reglerna om säkerhetsskyddad upphandling bör omfatta även sådana upphandlingar.

Ett exempel på att utvecklingen gjort regelverket svårtillämpbart är att det idag är en regel snarare än ett undantag att myndigheter i stora projekt tar hjälp av externa leverantörer. Dessa anlitar i sin tur ofta flera underleverantörer för att fullgöra olika delar av projektet. Den nuvarande lagstiftningen är bristfällig i det avseendet att den

inte innehåller några regler om hur säkerhetsskyddsfrågan ska hanteras i dessa fall.

Det finns således behov av tydligare regler rörande säkerhetsskyddad upphandling. I detta sammanhang bör också övervägas hur regelverket kan förenklas och göras mer flexibelt eftersom myndigheter och företag tenderar att bortse från reglerna om de är för komplicerade och tids- och kostnadskrävande. Exempel på områden som eventuellt skulle kunna förenklas är kravet på säkerhetsskyddsavtal i de fall uppgifterna inte kommer att lämna den upphandlande partens lokaler när man avser att begära in anbud eller träffa avtal om upphandling. I dessa fall skulle säkerhetsprövning inklusive registerkontroll av de personer som ska ta del av sådana uppgifter som rör rikets säkerhet kanske kunna vara tillräcklig.

Även när det gäller säkerhetsskyddsavtal bör beaktas i vilken utsträckning internationella förhållanden kan påverka den svenska lagstiftningen. Som exempel kan nämnas förekomsten av utländska leverantörer och entreprenörer vid säkerhetsskyddade upphandlingar samt att s.k. Facility Security Clearance (FSC), som är vanligt förekommande internationellt, i Sverige i de flesta fall endast kan utfärdas om företaget redan har ett befintligt säkerhetsskyddsavtal där en kontroll av företagets säkerhetsskydd har genomförts.

4.5 Tillsyn, sanktioner m.m.

Följande frågor bör ingå i en översyn av säkerhetsskyddslagen:
* Behöver tillsynsverktyget utvecklas, kompletteras med sanktionsmöjligheter eller andra instrument, eller bör verktyget ersättas med ett annat verktyg?
* Hur ska tillsynsansvaret enligt säkerhetsskyddslagstiftningen fördelas mellan myndigheterna och hur ska det förhålla sig till tillsynsansvar enligt annan lagstiftning?

Säkerhetsskyddslagstiftningen syftar till att säkerställa ett väl anpassat säkerhetsskydd i samhällsviktiga verksamheter. Tillsyn enligt säkerhetsskyddslagen syftar till att kontrollera att lagen efterföljs.

Säkerhetspolisen och Försvarsmakten har huvudansvaret för tillsyn på säkerhetsskyddsområdet men även andra myndigheter har ett visst tillsynsansvar. Tillsynsansvaret omfattar myndigheter och andra som säkerhetsskyddslagen gäller för, samt anbudsgivare och leverantörer som ingått säkerhetsskyddsavtal. Tillsyn sker genom besök och inspektion av skyddet och innefattar kontroll av att de berörda följer de lagar och regler som finns samt att säkerhetsskyddet är tillräckligt för den verksamhet som bedrivs. Tillsynen görs i en anda av samverkan och många myndigheter uppger att de uppskattar tillsynsverksamheten. Eventuella brister

påtalas både vid besöken och i en skriftlig rapport. Om brister inte rättas till, kan tillsynsmyndigheten anmäla detta till regeringen. I övrigt finns inga möjligheter till sanktioner enligt den nuvarande säkerhetsskyddslagstiftningen.

I säkerhetsskyddsförordningen föreskrivs en anmälningsskyldighet till Rikspolisstyrelsen när en hemlig uppgift kan ha röjts, om röjandet kan antas medföra ett men för rikets säkerhet som inte endast är ringa. Det finns inget krav enligt förordningen att rapportera andra säkerhetsincidenter eller verksamhet som kan hota rikets säkerhet. En sådan rapportering skulle ge bättre möjligheter att bedöma den säkerhetshotande verksamheten, minska sårbarheter i säkerhetsskyddet och förbättra föreskrifter samt tillsyn.

Säkerhetsskydd kan vara kostnadskrävande och det är ibland svårt för den säkerhetsskyddsansvarige, särskilt på företag, att få gehör för synpunkter och förslag på säkerhetshöjande åtgärder. Säkerhetspolisen har också erfarit att myndigheter m.fl. upplever eventuella straffpåföljder enligt 19 kap. brottsbalken som avlägsna. Det bör därför utredas om det finns anledning att införa sanktioner mot den som åsidosätter bestämmelser i säkerhetsskydds-lagstiftningen eller i ett säkerhetsskyddsavtal, eller om reglerna om tillsyn bör förtydligas vad avser metoder och omfattning för att kunna utgöra ett bättre stöd för såväl tillsynsmyndigheterna som de myndigheter och företag som är aktuella för tillsyn. Alternativ som kan utredas är om tillsynsverktyget bör utvecklas eller kompletteras med ett annat instrument, exempelvis ett auktorisations- eller certifieringssystem, ett självskattningssystem med olika säkerhetsnivåer, ett vitessystem eller om tillsynsverktyget bör ersättas med ett annat verktyg. Det är viktigt att utredaren vid en översyn av säkerhetsskyddslagen tar ställning till dessa frågor. Ett system med sanktioner måste dock ställas mot risken för en minskad öppenhet i dialogen mellan tillsynsmyndigheterna och de som kontrolleras.

I detta sammanhang bör också tillsynen och kontrollen enligt säkerhetsskyddslagstiftningen granskas i förhållande till sådan tillsyn som utförs enligt annan lagstiftning. Det finns andra myndigheter som har tillsynsansvar som tangerar Säkerhetspolisens tillsynsansvar och i vissa sammanhang föreligger en dubbelreglering. Som exempel kan nämnas att såväl affärsverket Svenska Kraftnät som länsstyrelserna har tillsynsansvar över anläggningar som samtidigt är föremål för tillsyn av Strålsäkerhetsmyndigheten enligt lagen (1984:3) om kärnteknisk verksamhet.

4.6 Övrigt

Följande frågor bör ingå i en översyn av säkerhetsskyddslagen:
* Hur ska frågan om en nationell säkerhetsmyndighet (NSA) och Nationell signalskyddsmyndighet (NSCA) lösas i Sverige?

I dagsläget är det inte klart vilken myndighet som representerar Sverige i internationella säkerhetsskyddssammanhang (jfr. Nationell säkerhetsmyndighet, NSA, Verkställande säkerhets-myndighet, DSA, och Nationell signalskyddsmyndighet, NSCA). För närvarande är UD utsedd som NSA gentemot bl.a. EU och Nato, medan Försvarsmakten har denna uppgift enligt ett flertal bilaterala internationella överenskommelser. FMV är i samma typ av överenskommelser angiven som DSA, medan rollen av NSCA i praktiken utövas av Försvarsmakten genom den rättsliga och faktiska signalskyddskompetens som finns vid myndigheten. Denna fråga bör lösas i samband med en allmän översyn av säkerhetsskyddslagstiftningen. I anslutning till överväganden om NSCA bör även ställning tas till om signalskyddstjänsten ska regleras i säkerhetsskyddsförordningen.

Denna rapport har beslutats av säkerhetspolischefen Anders Danielsson. I den slutliga handläggningen har säkerhetsrådet Jan Garton, polisöverintendenterna Doris Högne Rydheim, Anders Thornberg och Peter Waldenström, chefsjuristen Lars-Åke Johansson samt polisintendenten Per Kihlström deltagit. Föredragande har varit verksjuristen Pia Cedermark.

Anders Danielsson

Pia Cedermark