Försvarets underrättelseverksamhet och säkerhetstjänst

Integritet – Effektivitet

Betänkande av Underrättelsedatautredningen

Stockholm 2003

STATENS OFFENTLIGA UTREDNINGAR

SOU 2003:34

SOU och Ds kan köpas från Fritzes kundtjänst. För remissutsändningar av SOU och Ds svarar Fritzes Offentliga Publikationer på uppdrag av Regeringskansliets förvaltningsavdelning.

Beställningsadress:
Fritzes kundtjänst
106 47 Stockholm
Orderfax: 08-690 91 91
Ordertel: 08-690 91 90
E-post: fritzes.order@liber.se
Internet: www.fritzes.se

Svara på remiss. Hur och varför. Statsrådsberedningen, 1993.
– En liten broschyr som underlättar arbetet för den som skall svara på remiss.

Broschyren kan beställas hos:
Information Rosenbad
Regeringskansliet
103 33 Stockholm
Fax: 08–405 42 95
Telefon: 08–405 47 29
www.regeringen.se/propositioner/sou/pdf/remiss.pdf

Omslaget pryds av Försvarsmaktens och Försvarets radioanstalts vapen.

Tryckt av Edita Norstedts Tryckeri AB
Stockholm 2003

ISBN 91-38-21986-7
ISSN 0375-250X

Till statsrådet och chefen för Försvarsdepartementet

Regeringen beslutade den 7 februari 2002 att tillkalla en särskild utredare för att göra en översyn av regleringen av behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet. Utredaren skulle kartlägga behandlingen av personuppgifter och analysera behovet av särskilda bestämmelser. Utgångspunkten var att myndigheternas verksamhet skall kunna bedrivas effektivt med rationellt datorstöd samtidigt som nödvändig respekt visas för enskildas personliga integritet. Utredaren fick i uppdrag att lämna förslag till reglering i lag.

Den 7 februari 2002 förordnade dåvarande statsrådet, numera riksdagens talman Björn von Sydow kammarrättslagmannen Sten Wahlqvist att från samma dag vara särskild utredare.

Som experter har från den 15 mars 2002 medverkat rättssakkunnige Clara Ahlqvist, rättssakkunnige Mikael Andersson, kammarrättsassessorn Peder Liljeqvist, verksjuristen Kjell Nyman, avdelningsdirektören Elisabeth Wallin och förste arkivarien Karin Åström. Försvarsjuristen Göran Olsson förordnades som expert från den 17 juni 2002.

Sekreterare åt utredningen har varit kammarrättsassessorn Lars Dahlström.

Utredningen har antagit namnet Underrättelsedatautredningen (Fö 2002:01)

Härmed överlämnar utredningen sitt betänkande FÖRSVARETS UNDERRÄTTELSEVERKSAMHET OCH SÄKERHETSTJÄNST Integritet – Effektivitet (SOU 2003:34).

Arbetet har bedrivits i nära samråd med berörda experter. Betänkandet är därför skrivet i vi-form.

Utredningens uppdrag är härmed slutfört.

Jönköping i mars 2003

Sten Wahlqvist

/Lars Dahlström

Innehåll

Sammanfattning 11

Författningsförslag 23

1 Förslag till lag om behandling av uppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten 23

2 Förslag till lag om behandling av uppgifter i Försvarets radioanstalts underrättelseverksamhet 29

3 Förslag till lag om ändring i sekretesslagen (1980:100) 34

4 Förslag till förordning om behandling av uppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten 35

5 Förslag till förordning om behandling av uppgifter i Försvarets radioanstalts underrättelseverksamhet 37

6 Förslag till förordning om ändring i förordningen (1988:552) med instruktion för Försvarets underrättelsenämnd 39

7 Förslag till förordning om upphävande av förordningen (2001:703) om viss behandling av personuppgifter inom Försvarsmakten och Försvarets radioanstalt 41

BAKGRUNDEN TILL VÅRA FÖRSLAG

1 Uppdraget 45

1.1 Utredningens direktiv 45

1.2 Utredningsarbetet ... 46

2 Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten ... 49

2.1 Försvarsmaktens organisation och verksamhet ... 49

2.2 Den militära underrättelse- och säkerhetstjänsten ... 52
2.2.1 MUST:s organisation ... 52
2.2.2 MUST:s uppgifter och verksamhet ... 57

2.3 Försvarsunderrättelseverksamhet ... 59
2.3.1 Underrättelseprocessen ... 62

2.4 Författningsreglering av försvarsunderrättelseverksamhet ... 63
2.4.1 Lagen om försvarsunderrättelseverksamhet ... 64

2.5 Militär säkerhetstjänst ... 68
2.5.1 Den militära säkerhetstjänstens uppgifter ... 68

2.6 Författningsreglering av säkerhetsskyddet inom Försvarsmakten ... 71
2.6.1 Säkerhetsskyddslagen ... 72

3 Försvarets radioanstalts underrättelseverksamhet ... 79

3.1 Försvarets radioanstalts organisation ... 80

3.2 Försvarets radioanstalts uppgifter och verksamhet ... 81

3.3 Signalspaning ... 83

3.4 Försvarets radioanstalts delgivning av underrättelser ... 86

4 Övergripande rättslig reglering av behandling av personuppgifter ... 89

4.1 Dataskyddskonventionen ... 89

4.2 Europarådets rekommendation om användning av personuppgifter inom polissektorn ... 91

4.3 Riktlinjer från OECD ... 92

4.4 Dataskyddsdirektivet 92
4.4.1 Tillämpningsområde 92
4.4.2 Bestämmelser om när personuppgifter får behandlas 93
4.4.3 Information och rättelse m.m. 94
4.4.4 Tillsynsmyndighet 94
4.4.5 Överföring av personuppgifter till tredje land 95

4.5 Europakonventionen 95

4.6 Europeiska unionens stadga om de grundläggande rättigheterna 96

4.7 Personuppgiftslagen 97
4.7.1 Allmänt om lagen och dess tillämpningsområde 98
4.7.2 Förutsättningar för behandling av personuppgifter 99
4.7.3 Information och rättelse m.m. 101
4.7.4 Säkerhet vid behandlingen 102
4.7.5 Överföring av personuppgifter till tredje land 103
4.7.6 Datainspektionens befogenheter som tillsynsmyndighet 103
4.7.7 Sanktioner 104

5 Försvarsmaktens informationshantering i militär underrättelse- och säkerhetstjänst 107

5.1 Rättslig reglering av behandling av personuppgifter i den militära underrättelse- och säkerhetstjänsten 108

5.2 Behandling av personuppgifter i den militära underrättelse- och säkerhetstjänsten 112

5.3 System för automatiserad behandling av personuppgifter m.m. 114
5.3.1 Informationsdatabasen – Sektionen för öppna källor 115
5.3.2 Informationssystem för den militära underrättelse- och säkerhetstjänsten (IS UNDSÄK) 118
5.3.3 MUST:s internationella sambands- och kryptosystem (MINSK) 121

5.3.4 Bearbetning Analys Internationella Operationer (BANIO) ... 121
5.3.5 Totalförsvarets signalskyddssamordning (TSA) ... 121
5.3.6 Övriga system för automatiserad behandling av personuppgifter ... 122

6 Försvarets radioanstalts informationshantering i underrättelseverksamheten ... 125

6.1 Rättslig reglering av behandling av personuppgifter i Försvarets radioanstalts underrättelseverksamhet ... 126

6.2 Behandling av personuppgifter i Försvarets radioanstalts underrättelseverksamhet ... 127

6.3 System för automatiserad behandling av personuppgifter m.m. ... 128
6.3.1 Urvalsdatabasen – planering och inriktning ... 129
6.3.2 Källdatabasen – inhämtning genom signalspaning ... 130
6.3.3 Databasen för öppna källor – inhämtning ... 130
6.3.4 Analysdatabasen – bearbetning och analys ... 132
6.3.5 Rapportdatabasen – delgivning ... 132

VÅRA ÖVERVÄGANDEN

7 Övergripande frågor och principer ... 137

7.1 Behovet av datorstöd ... 137

7.2 Skyddet för den personliga integriteten ... 137

7.3 Särskild författningsreglering ... 142

7.4 Lag, förordning eller myndighetsföreskrifter ... 144

7.5 Grundläggande begrepp – databas eller register ... 145

8 Författningsreglering ... 149

8.1 Lagstiftningens systematik och allmänna tillämpningsområde ... 149

8.2 Allmänna bestämmelser ... 151
8.2.1 Tillämpningsområde ... 151

8.2.2 Förhållandet till personuppgiftslagen 153
8.2.3 Personuppgiftsansvaret 160
8.2.4 Tillåtna ändamål för behandling av uppgifter 161
8.2.5 Behandling av känsliga personuppgifter 168
8.2.6 Överföring av personuppgifter till tredje land 171

8.3 Behandling av uppgifter i databaser 174
8.3.1 Begreppet databas 174
8.3.2 Försvarets radioanstalts databaser 177
8.3.3 Försvarsmaktens databaser 180
8.3.4 Uppgifter som får behandlas 183
8.3.5 Begränsningar vid sökning i databaserna 185
8.3.6 Direktåtkomst 186

8.4 Enskildas rättigheter 191
8.4.1 Information 192
8.4.2 Rättelse och skadestånd 193
8.4.3 Överklagande 196

8.5 Särskild granskning till skydd för den personliga integriteten 197
8.5.1 Försvarets underrättelsenämnd 199
8.5.2 Vårt förslag om särskild granskning 201

9 Särskilda frågor 203

9.1 Bevarande och gallring 203

9.2 Utlämnande av uppgifter 209
9.2.1 Sekretess och utlämnande av uppgifter till utländsk myndighet eller internationell organisation 209
9.2.2 Utlämnande av uppgifter på medium för automatiserad behandling 210

10 Sekretessfrågor 213

10.1 Sekretess till skydd för enskilds personliga eller ekonomiska förhållanden 213

11 Ikraftträdande- och övergångsbestämmelser 223

12 Konsekvenser av våra förslag 225

13 Författningskommentarer 229

13.1 Förslag till lag om behandling av uppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten 229

13.2 Förslag till lag om behandling av uppgifter i Försvarets radioanstalts underrättelseverksamhet 239

13.3 Förslag till lag om ändring i sekretesslagen (1980:100) 248

BILAGOR

Bilaga 1: Kommittédirektiv 2002:13 251

Bilaga 2: Försvarets radioanstalts underrättelseproduktion 257

Sammanfattning

Några allmänna utgångspunkter för uppdraget

Den 24 oktober 1998 trädde personuppgiftslagen (1998:204) i kraft. Genom lagen genomförde Sverige Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (dataskyddsdirektivet).

Vi har haft i uppdrag att göra en översyn av regleringen av behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet. Den närmare regleringen av behandlingen av personuppgifter inom dessa verksamheter finns i dag i förordningen (2001:703) om viss behandling av personuppgifter inom Försvarsmakten och Försvarets radioanstalt. Syftet med vårt uppdrag har varit att kartlägga behandlingen av personuppgifter och analysera behovet av särskilda bestämmelser samt lämna förslag till reglering i lag. I uppdraget har ingått att granska frågor som rör användning, inhämtande, utlämnande, gallring och arkivering av personuppgifter samt tillsyn över behandlingen. Vår utgångspunkt för uppdraget har varit att myndigheternas verksamhet skall kunna bedrivas effektivt och med ett rationellt datorstöd samtidigt som nödvändig respekt visas för enskildas personliga integritet. Vi har även haft att beakta det internationella inslaget i myndigheternas verksamheter.

Övergripande principer för ny lagstiftning

Lag, förordning och myndighetsföreskrifter

Utvecklingen inom datorområdet visar att lagstiftning som reglerar användningen av datorstöd måste vara teknikneutral och flexibel, för att inte hindra den effektivisering av verksamheterna som kontinuerligt pågår. Samtidigt är det mycket viktigt att det i lagstiftningen tas hänsyn till de registrerades personliga integritet.

I den militära underrättelse- och säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet hanteras stora mängder information som många gånger kan vara av känslig natur för de inblandade personerna. Hos båda myndigheterna pågår ständigt en teknisk utveckling av datorsystemen med ökade möjligheter att behandla och söka i stora uppgiftsmängder, vilket kan medföra en ökad risk för att enskilda drabbas av oacceptabla intrång i den personliga sfären. Det är viktigt att inte hamna i en situation där den tekniska utvecklingen styr den rättsliga regleringen, eller där den rättsliga regleringen onödigt hämmar effektiviseringen. Det är därför nödvändigt med en lagstiftning som enbart tar sikte på principiellt viktiga frågor och så långt som möjligt lämnar detaljregleringen därhän. Att beakta i sammanhanget är också att de aktuella verksamheterna är av sådan art att det inte är möjligt att i lagform reglera dem i detalj. Vi föreslår därför att de grundläggande principerna för behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet skall regleras särskilt i lag, medan kompletterande bestämmelser skall meddelas av regeringen eller den myndighet regeringen bestämmer.

För behandling av personuppgifter i myndigheternas administrativa verksamhet, t.ex. i arbetsgivarfrågor, anser vi det tillräckligt med personuppgiftslagens bestämmelser och föreslår därför ingen särskild reglering inom det området.

Integritet och effektivitet

Utgångspunkten för vårt uppdrag att reglera viss behandling av personuppgifter hos Försvarsmakten och Försvarets radioanstalt har varit att myndigheternas verksamheter skall kunna bedrivas effektivt samtidigt som nödvändig respekt visas för enskildas personliga integritet. Vid denna avvägning mellan integritet och

effektivitet är det enligt vår uppfattning två omständigheter som framstår som särskilt betydelsefulla. För det första är det de *ändamål* för vilka behandling av personuppgifter får ske och för det andra den *säkerhet och sekretess* som gäller i verksamheterna.

Försvarsunderrättelseverksamhet bedrivs dels för att kartlägga yttre militära hot mot landet, dels till stöd för svensk utrikes-, försvars- och säkerhetspolitik. Den militära säkerhetstjänsten har till uppgift att upptäcka, identifiera och möta säkerhetshot som riktas mot Försvarsmakten och dess intressen. Verksamheterna utgör grundläggande och viktiga samhällsfunktioner av stor betydelse för Sveriges yttre säkerhet och för att stärka samhället vid svåra påfrestningar i fred. Vi anser därför att en lagstiftning om behandling av personuppgifter måste ge Försvarsmakten och Försvarets radioanstalt möjlighet att bedriva de aktuella verksamheterna på ett ändamålsenligt och effektivt sätt, även om det av vissa personer kan uppfattas medföra ett visst intrång i den personliga integriteten.

Försvarsunderrättelseverksamhet och militär säkerhetstjänst är verksamheter som av naturliga skäl till stor del måste vara hemliga. Många uppgifter som hanteras är känsliga såväl med hänsyn till Sveriges förhållande till främmande makt som till skyddet för rikets säkerhet. Det är också viktigt att skydda uppgiftslämnare och arbetsmetoder. Den omfattande sekretess som omgärdar verksamheterna medför emellertid att det i jämförelse med annan verksamhet är mindre risk för att personuppgifter sprids till utomstående. Härmed är det i motsvarande mån mindre risk för att uppgifterna skall behandlas i strid med gällande ändamål, vilket i sig utgör ett skydd för den personliga integriteten.

Grundläggande för våra författningsförslag är att vi i lag anger tydliga och konkreta ändamål för behandling av personuppgifter. Behandling av personuppgifter som sker uteslutande enligt dessa särskilt fastlagda ändamål medför enligt vår uppfattning – med beaktande av den sekretess och säkerhet i övrigt som gäller i verksamheterna – inte någon påtaglig risk för *otillbörligt* intrång i registrerades personliga integritet. Vissa användningar, såsom t.ex. behandling av känsliga personuppgifter och annans direktåtkomst till elektroniskt lagrad information måste emellertid regleras särskilt. För att motverka den brist på insyn som följer av reglerna om sekretess bör vidare ett oberoende organ få till särskild uppgift att granska behandlingen av personuppgifter, för att ytterligare tillförsäkra att otillbörligt intrång i registrerades personliga integritet inte sker.

Lagstiftningens systematik och tillämpningsområde m.m.

Vi föreslår att den i dag gällande förordningen (2001:703) om viss behandling av personuppgifter inom Försvarsmakten och Försvarets radioanstalts skall ersättas av två nya lagar med tillhörande förordningar. Den ena lagen reglerar behandling av uppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten, medan den andra omfattar behandling av uppgifter i Försvarets radioanstalts underrättelseverksamhet.

De nya lagarna har samma inbördes systematik och delas in i tre kapitel. I ett första kapitel finns allmänna bestämmelser som i princip är tillämpliga på all behandling av uppgifter som omfattas av lagen. Det andra kapitlet innehåller särskilda bestämmelser som endast gäller automatiserad behandling av uppgifter i gemensamma databaser. I det avslutande kapitlet finns bestämmelser om enskildas rättigheter vid behandling av personuppgifter, nämligen om information, rättelse, skadestånd och överklagande samt bestämmelser om särskild granskning till skydd för registrerades personliga integritet.

Lagarna tillämpas vid behandling av personuppgifter som är helt eller delvis automatiserad. Även behandling av personuppgifter i vissa manuella register omfattas av lagarnas tillämpningsområde. Grundläggande bestämmelser i lagarna, t.ex. när det gäller ändamålen med och ansvaret för behandlingen, är tillämpliga även vid behandling av uppgifter om juridiska personer.

Lagarna gäller i stället för personuppgiftslagen, vars bestämmelser tillämpas på behandling av personuppgifter hos Försvarsmakten och Försvarets radioanstalt endast när det anges särskilt. De bestämmelser i personuppgiftslagen som är allmänt tillämpliga är de om definitioner, förhållandet till offentlighetsprincipen, grundläggande krav på behandling, säkerheten vid behandling, personuppgiftsombudets uppgifter samt tillsynsmyndighetens befogenheter och straff.

Försvarsmakten och Försvarets radioanstalt är personuppgiftsansvariga för den behandling som myndigheterna utför eller som det åligger dem att utföra.

Tillåtna ändamål för behandling av personuppgifter

Försvarsmaktens och Försvarets radioanstalts behandling av personuppgifter skall styras av särskilt angivna och tydliga ändamål, vilka skall framgå av lag.

Försvarsmakten får behandla personuppgifter för ändamålen försvarsunderrättelseverksamhet och militär säkerhetstjänst. Med *försvarsunderrättelseverksamhet* avses att inhämta, bearbeta och analysera samt delge information dels för att kartlägga yttre militära hot mot landet, dels till stöd för svensk utrikes-, försvars- och säkerhetspolitik. Uppgifter får behandlas för säkerhetspolitiska och militärstrategiska bedömningar, analys av pågående och bedömda framtida konflikter samt biografisk försvarsunderrättelseverksamhet. I den *militära säkerhetstjänsten* får uppgifter behandlas för att upptäcka, förebygga och avvärja säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess intressen. I verksamheten ingår *att* klarlägga verksamhet som innefattar hot mot rikets säkerhet och personer med anknytning till sådan verksamhet, *att* vidta åtgärder som hindrar eller försvårar säkerhetshotande verksamhet *och att* förhindra obehörig insyn i och påverkan av totalförsvarets telekommunikations- och informationssystem. I den militära säkerhetstjänsten får uppgifter om en person behandlas endast om personen har samband med säkerhetshotande verksamhet. Sådana uppgifter skall också förses med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Är personen inte misstänkt för att ha utövat eller komma att utöva säkerhetshotande verksamhet får uppgifter om denne behandlas endast om det klart framgår att sådan misstanke inte föreligger.

Försvarets radioanstalt får behandla uppgifter för att bedriva försvarsunderrättelseverksamhet samt för att i övrigt utföra de uppgifter som enligt instruktionen åligger myndigheten i dess *underrättelseverksamhet*. Med försvarsunderrättelseverksamhet avses här detsamma som ovan beskrivits för Försvarsmakten. Försvarets radioanstalt bedriver emellertid inte enbart militärt inriktad underrättelseverksamhet utan har också andra uppgifter som regeringens civila inhämtningsorgan i utrikes- och säkerhetspolitiska frågor. Försvarets radioanstalt skall även med sin tekniska expertis lämna stöd för annan myndighetsverksamhet än sådan som rör yttre hot mot rikets säkerhet.

Behandling av känsliga personuppgifter

Uppgifter om en person får inte behandlas enbart på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv (känsliga personuppgifter). Om uppgifter om en person behandlas på annan grund får de emellertid kompletteras med känsliga personuppgifter, när det är nödvändigt för syftet med behandlingen.

Vid sökning i Försvarsmaktens och Försvarets radioanstalts databaser får känsliga personuppgifter inte användas som sökbegrepp om det inte är nödvändigt. Sökning får inte ske enbart med en känslig personuppgift som grund utan måste även stödjas av ett för verksamheten annat berättigat skäl, och skall dessutom föregås av ett noggrant övervägande huruvida användningen av personuppgifterna tillför något av värde för verksamheten.

Utlämnande av uppgifter

Det internationella samarbetet inom underrättelse- och säkerhetstjänsten är av mycket stor betydelse för Sverige. Av gällande lagstiftning och regeringens regleringsbrev framgår att för såväl Försvarsmakten som Försvarets radioanstalt skall samarbete med andra länder och internationella organisationer vara en naturlig del av verksamheten. För att främja internationellt samarbete inom underrättelse- och säkerhetstjänsten anser vi att uppgifter för vilka sekretess gäller bör få lämnas ut till en utländsk myndighet eller en internationell organisation om utlämnandet tjänar den svenska statsledningen och det svenska totalförsvaret samt om lämnade uppgifter inte är till skada för svenska intressen.

Enligt vår uppfattning behöver utlämnande av uppgifter på medium för automatiserad behandling inte regleras särskilt. Sådant utlämnande kan förekomma till annan svensk myndighet och till annan stat eller internationell organisation. För svenska myndigheter finns ofta särskilda registerförfattningar som reglerar behandlingen av personuppgifter. Utlämnande till andra länder och internationella organisationer omfattas av höga krav på säkerhet och sekretess som betingas av ändamålet för verksamheten. Någon särskild integritetsskyddande regel är därför enligt vår mening inte nödvändig i dessa sammanhang.

På grund av Sveriges anslutning till Europarådets dataskyddskonvention är det emellertid nödvändigt med särskilda bestämmelser vid utlämnande av personuppgifter till andra länder. Vi föreslår därför att uppgifter som behandlas med stöd av de författningar vi föreslår får lämnas ut till andra länder om sekretess inte hindrar det och det behövs för att myndigheterna skall kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet eller det annars är nödvändigt för verksamheten. Bestämmelsen innebär inte i sig någon begränsning av myndigheternas möjlighet att lämna ut uppgifter, utan detta får i sin helhet avgöras efter försvars- och säkerhetspolitiska överväganden.

Behandling av uppgifter i databaser

Hos myndigheter behandlas i dag personuppgifter med datorstöd på i huvudsak två principiellt och tekniskt skilda sätt. För det första används persondatorer på så sätt att endast ett fåtal personer kan ta del av informationen, t.ex. enskilda tjänstemän som upprättar promemorior och beslutsunderlag m.m. samt skickar och tar emot e-post. För det andra används i stor utsträckning allmänt åtkomliga dataregister i form av gemensamma system med information som behövs i myndighetens verksamhet. Den senare formen av datorstöd anser vi bör omgärdas av särskilda skyddsregler, eftersom integritetsriskerna ökar när stora mängder information behandlas gemensamt. Vi föreslår att sådan behandling skall samlas under det rättsliga begreppet databas. Det rättsliga begreppet databas kan omfatta flera mindre register, databaser eller datorsystem.

Olika regler skall således gälla för Försvarsmaktens respektive Försvarets radioanstalts behandling av uppgifter beroende på om behandlingen utförs av enskilda tjänstemän och uppgifterna inte görs tillgängliga för gemensam användning i verksamheten, eller om behandlingen är automatiserad och utförs i en särskild samling av uppgifter som används gemensamt i verksamheten (databaser).

Försvarets radioanstalts databaser

Försvarets radioanstalt bedriver underrättelseverksamhet genom att inhämta information dels via signalspaning dels från öppna källor. Försvarets radioanstalts system för behandling av person-

uppgifter i dess underrättelseverksamhet är helt anpassat till underrättelseprocessens led med planering och inriktning, inhämtning, bearbetning och analys samt delgivning. I enlighet härmed skall det för uppgifter som används vid planering och inriktning av myndighetens underrättelseverksamhet på kort och på lång sikt finnas en urvalsdatabas. Information som hämtas in genom signalspaning skall lagras i en källdatabas medan övrig information lagras i en databas för öppna källor. Bearbetning och analys av inhämtad underrättelseinformation skall ske i en analysdatabas och de underrättelserapporter som är färdiga för delgivning skall slutligen lagras i en rapportdatabas.

Försvarsmaktens databaser

Inom den militära underrättelse- och säkerhetstjänsten finns det i dag två typer av register eller databaser, antingen för öppen eller för hemlig information. Enligt den reglering av Försvarsmaktens databaser som vi föreslår skall det finnas en informationsdatabas samt en underrättelse- och säkerhetsdatabas. I informationsdatabasen får Försvarsmakten behandla information som inte är hemlig och som hämtats in från allmänt tillgängliga öppna källor.

Hemliga uppgifter lagras hos Försvarsmakten i flera olika datorbaserade system anpassade till ändamålet med den särskilda behandlingen. Den viktigaste databasen är härvid Informationssystem för den militära underrättelse- och säkerhetstjänsten (IS UNDSÄK). I databasen behandlas uppgifter som rör hela den militära underrättelse- och säkerhetstjänstens ansvarsområde. Det finns även vissa andra databaser för behandling av hemlig information med mer begränsade användningsområden, som t.ex. bearbetning och analys av uppgifter i samband med Sveriges deltagande i internationella operationer eller för kommunikation med Sveriges försvarsattachéer. Underrättelse- och säkerhetsdatabasen är avsedd att vara ett samlande begrepp för de olika databaser i vilka Försvarsmakten behandlar hemliga uppgifter.

Innehåll

Det är inte möjligt att i detalj lagreglera vilka uppgifter som bör få behandlas i myndigheternas databaser. En noggrann reglering av vilka uppgifter som får behandlas måste även till viss del vara

hemlig. Vi föreslår därför att regeringen eller den myndighet som regeringen bestämmer skall meddela närmare föreskrifter eller beslut om vilka uppgifter som får behandlas i Försvarsmaktens och Försvarets radioanstalts databaser. I förordning införs emellertid av upplysningsskäl en bestämmelse om vilka uppgiftskategorier som får behandlas i databaserna. Även bestämmelserna om ändamål kan ge enskilda information om vilka uppgifter som registreras.

Direktåtkomst

Att tillåta direktåtkomst för myndigheter till information i andra myndigheters dataregister m.m. har länge ansetts särskilt integritetskänsligt. Vi delar den uppfattningen, men anser att det finns starka skäl för att tillåta sådan åtkomst. Vilka som får ha direktåtkomst till Försvarsmaktens och Försvarets radioanstalts databaser bestäms av regeringen i förordning eller beslut. Vi föreslår att direktåtkomst får förekomma mellan Försvarsmakten respektive Försvarets radioanstalt och i första hand Regeringskansliet. I viss utsträckning bör också de andra myndigheter som bedriver försvarsunderrättelseverksamhet eller i övrigt deltar i skyddet av rikets säkerhet ha direktåtkomst. Regeringen, eller den myndighet som regeringen bestämmer, bör meddela närmare föreskrifter eller beslut om omfattningen av direktåtkomsten.

Enskildas rättigheter

Fysiska personer bör av integritetsskäl ha vissa grundläggande rättigheter som rör behandlingen av uppgifter om dem. Förutom rätt till information, rättelse och skadestånd, anser vi att vissa beslut av Försvarsmakten och Försvarets radioanstalt bör kunna överklagas. Dessa rättigheter bör inte gälla för juridiska personer.

Således anser vi att personuppgiftslagens bestämmelser om information som skall lämnas självmant till den registrerade när uppgifter samlas in från denne själv och om information som skall lämnas efter ansökan av den registrerade, i huvudsak bör tillämpas vid behandling av personuppgifter i de aktuella verksamheterna. Vidare bör personuppgiftslagens bestämmelser om rättelse av personuppgifter och om skadestånd tillämpas. Försvarsmaktens och Försvarets radioanstalts beslut om rättelse och om information

som skall lämnas efter ansökan av en registrerad skall enligt vår mening kunna överklagas till allmän förvaltningsdomstol.

Särskild granskning till skydd för den personliga integriteten

Personuppgiftslagens regler om enskildas rätt till information är av stor betydelse för att personuppgifter inte skall behandlas på ett sätt som kan medföra att enskildas personliga integritet kränks. Den sekretess som gäller för uppgifter i de nu aktuella verksamheterna innebär emellertid att information i den mening som avses i personuppgiftslagen i praktiken aldrig kommer att lämnas av den personuppgiftsansvariga myndigheten. Av 27 § personuppgiftslagen följer nämligen att sekretess och tystnadsplikt alltid går före den i personuppgiftslagen föreskrivna informationsskyldigheten. Härigenom begränsas också de registrerades möjlighet att begära rättelse och skadestånd.

Det är enligt vår uppfattning nödvändigt att skyddet för registrerades personliga integritet kompletteras. Försvarets underrättelsenämnd bör därför få i uppdrag att särskilt granska den behandling av personuppgifter som sker i Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet.

Försvarets underrättelsenämnd har till uppgift att följa underrättelsetjänsten inom Försvarsmakten och de övriga myndigheter som bedriver försvarsunderrättelseverksamhet, bl.a. Försvarets radioanstalt. Härvid har nämnden redan i dag som särskild uppgift att granska hur de register som behövs för försvarsunderrättelseverksamhet läggs upp och förs. Försvarets underrättelsenämnd framstår med hänsyn härtill och till nämndens kunskaper om försvarsunderrättelseverksamhet som bäst lämpad att utföra granskning av behandlingen av personuppgifter enligt de författningar vi nu föreslår.

Förslaget om en särskild granskning syftar inte till att inskränka det övergripande tillsynsansvar som åligger Datainspektionen enligt personuppgiftslagen. Datainspektionen bör alltjämt ha huvudansvaret för tillsyn över behandlingen av personuppgifter hos Försvarsmakten och Försvarets radioanstalt. Försvarets underrättelsenämnds granskning skall vara en extra integritetsskyddskontroll som, utöver Datainspektionens tillsyn, skyddar de

registrerade mot kränkning av den personliga integriteten vid behandling av personuppgifter.

Försvarets underrättelsenämnd skall inte vara involverad i någon löpande ärendehantering hos de båda myndigheterna och enskilda skall inte kunna vända sig till nämnden med begäran om utlämnande av handlingar. En sådan begäran skall som i dag prövas av Försvarsmakten eller Försvarets radioanstalt.

Bevarande och gallring

Registerförfattningar innehåller av integritetsskäl ofta bestämmelser som innebär att uppgifter som huvudregel inte får bevaras utan tidsgräns. I många sådana författningar finns därför bestämmelser om gallring av uppgifter eller om överlämnande av uppgifter till en arkivmyndighet. I nya registerförfattningar tillämpas vanligen en metod som innebär att det i lag ställs upp huvudregler för när gallring av uppgifter skall ske, men med möjlighet för regeringen eller Riksarkivet att besluta eller meddela föreskrifter om att uppgifter skall bevaras.

När det gäller uppgifter i traditionella pappersbaserade allmänna handlingar är i stället huvudregeln att det inte finns några särbestämmelser utan arkivlagens regler gäller fullt ut. Det är också denna metod som vi anser bör gälla i fråga om bevarande och gallring av uppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet.

I de aktuella verksamheterna måste uppgifter kunna sparas under mycket lång tid, ofta i minst 30 år och ibland så länge som upp till 70 år. Gallring syftar som nämnts i första hand till att värna skyddet för den personliga integriteten. Med hänsyn till bl.a. offentlighetsprincipen bör emellertid krav på gallring inte gälla som huvudregel utan att starkt vägande integritetsskäl talar härför. När uppgifter har bevarats i 30 år eller längre har enligt vår uppfattning integritetsintressena till stor del spelat ut sin roll. Gallring är vidare inte den enda metoden för att tillgodose skyddet för den personliga integriteten. Framför allt den sekretess som gäller i verksamheterna fungerar som ett starkt skydd för den personliga integriteten och talar mot nödvändigheten av att ha särskilda gallringsregler. Samtidigt tjänas integritetsintresset inte alltid bäst av att så många uppgifter som möjligt gallras. I vissa fall har bevarandet av känsliga uppgifter visat sig vara till stor fördel för enskilda. Vidare utgör

offentlighetsintresset och den minskade möjligheten till insyn i myndigheternas verksamhet för bl.a. forskning skäl som talar mot omfattande gallring.

Mot bakgrund härav föreslår vi inte några särskilda gallringsbestämmelser för de aktuella verksamheterna. Det innebär att bestämmelserna i arkivlagen och personuppgiftslagen blir tillämpliga vad gäller frågor om bevarande och gallring, oavsett om uppgifterna behandlas i en databas eller inte. I praktiken innebär detta att allmänna handlingar som huvudregel skall bevaras och att handlingarna får gallras endast om Riksarkivet har tillåtit det. För andra uppgifter, dvs. sådana uppgifter som inte ingår i allmänna handlingar, gäller i stället att de skall rensas (förstöras) när de inte längre behövs för de ursprungliga ändamålen med registreringen.

Sekretess till skydd för enskilds personliga eller ekonomiska förhållanden

I Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten finns uppgifter som kan vara mycket integritetskänsliga för enskilda och deras närstående och som inte skyddas av gällande sekretessregler. Det kan t.ex. gälla uppgifter som avslöjar en persons fysiska eller psykiska hälsotillstånd. Den sekretess som i dag gäller för uppgifter i den militära underrättelse- och säkerhetstjänsten syftar endast till att skydda själva verksamheten hos myndigheten och utgör därmed inget skydd för enskilda individer och deras personliga eller ekonomiska intressen. Mot bakgrund härav föreslår vi att det i sekretesslagen (1980:100) införs en bestämmelse om sekretess hos Försvarsmakten i den militära underrättelse- och säkerhetstjänsten, till skydd för uppgift om enskilds personliga eller ekonomiska förhållanden. Sekretess för sådan uppgift skall enligt vår mening gälla om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon honom närstående lider skada eller men. Sekretess bör gälla i högst 70 år.

Författningsförslag

1 Förslag till lag om behandling av uppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten

Härigenom föreskrivs följande.

1 kap. Allmänna bestämmelser

Lagens tillämpningsområde m.m.

1 § Denna lag tillämpas vid behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten, om behandlingen är helt eller delvis automatiserad eller om uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Bestämmelserna i 4–6 §§ samt 2 kap. gäller även vid behandling av uppgifter om juridiska personer.

I 2 kap. finns särskilda bestämmelser om behandling av personuppgifter i den militära underrättelse- och säkerhetstjänstens databaser.

Förhållandet till personuppgiftslagen

2 § Om inte annat anges i 3 § eller i 3 kap. gäller denna lag i stället för personuppgiftslagen (1998:204).

3 § När personuppgifter behandlas enligt denna lag eller enligt andra föreskrifter i det ämne som regleras i lagen gäller personuppgiftslagens (1998:204) bestämmelser om

1. definitioner i 3 §,
2. förhållandet till offentlighetsprincipen m.m. i 8 §,
3. grundläggande krav på behandling i 9 §,
4. säkerheten vid behandling i 30 och 31 §§,
5. personuppgiftsombud m.m. i 36 § andra stycket och 38–40 §§,
6. tillsynsmyndighetens befogenheter i 43 och 47 §§, och
7. straff i 49 §.

Personuppgiftsansvar

4 § Försvarsmakten är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför eller som det åligger myndigheten att utföra. Motsvarande ansvar gäller för behandling av uppgifter om juridiska personer.

Ändamål m.m.

Försvarsunderrättelseverksamhet

5 § Uppgifter får behandlas i försvarsunderrättelseverksamheten dels för att kartlägga yttre militära hot mot landet dels till stöd för svensk utrikes-, försvars- och säkerhetspolitik om det behövs för

1. säkerhetspolitiska och militärstrategiska bedömningar,
2. analyser av pågående och bedömda framtida konflikter, eller
3. biografisk försvarsunderrättelseverksamhet.

Militär säkerhetstjänst

6 § Uppgifter får behandlas i den militära säkerhetstjänsten för att upptäcka, förebygga och avvärja säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess intressen om det behövs för

1. att klarlägga verksamhet som innefattar hot mot rikets säkerhet och personer med anknytning till sådan verksamhet (säkerhetsunderrättelsetjänst),
2. åtgärder som hindrar eller försvårar säkerhetshotande verksamhet (säkerhetsskyddstjänst), eller
3. att förhindra obehörig insyn i och påverkan av totalförsvarets telekommunikations- och informationssystem (signalskyddstjänst).

7 § För de ändamål som anges i 6 § 1–2 får uppgifter om en person behandlas endast om

1. personen kan misstänkas för att ha utövat eller komma att utöva verksamhet som innefattar hot mot rikets säkerhet eller terrorism,
2. uppgifterna avser information som framkommit i samband med att en person har genomgått registerkontroll enligt säkerhetsskyddslagen (1996:627),
3. det kan antas att personen bedriver annan säkerhetshotande verksamhet än som avses i 1, och det finns särskilda skäl till att uppgiften skall behandlas, eller
4. personen har lämnat uppgifter om säkerhetshotande verksamhet.

Uppgifter om att en person kan antas ha samband med säkerhetshotande verksamhet skall förses med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

Uppgifter om en person som inte misstänks för att ha utövat eller komma att utöva säkerhetshotande verksamhet får behandlas endast om det genom särskild upplysning eller på annat sätt klart framgår att sådan misstanke inte föreligger.

Behandling av känsliga personuppgifter

8 § Uppgifter om en person får inte behandlas enbart på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv.

Om uppgifter om en person behandlas på annan grund får de kompletteras med sådana uppgifter som avses i första stycket när det är nödvändigt för syftet med behandlingen.

Överföring av personuppgifter till tredje land

9 § Personuppgifter som behandlas med stöd av denna lag får lämnas ut till andra länder om sekretess inte hindrar det och det behövs för att Försvarsmakten skall kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet eller det annars är nödvändigt för verksamheten.

2 kap. Försvarsmaktens databaser

Inledande bestämmelse

1 § I försvarsunderrättelseverksamheten och den militära säkerhetstjänsten skall det finnas ett antal skilda samlingar uppgifter, som med hjälp av automatiserad behandling används gemensamt i verksamheten för de i 1 kap. 5–7 §§ angivna ändamålen (databaser).

Informationsdatabasen

2 § Uppgifter som samlats in från öppna källor skall behandlas i en informationsdatabas för att göra insamlad information tillgänglig i verksamheten.

Uppgifter i databasen får utöver vad som framgår av första stycket behandlas endast genom att föras över till en underrättelse- och säkerhetsdatabas.

Underrättelse- och säkerhetsdatabasen

3 § Uppgifter som samlats in på annat sätt än från öppna källor skall lagras i en underrättelse- och säkerhetsdatabas.

I databasen får även lagras uppgifter som överförts från informationsdatabasen.

4 § Uppgifter får behandlas i databasen för analys och bearbetning av inhämtat underrättelsematerial samt för lagring och delgivning av underrättelserapporter.

Uppgifter som får behandlas

5 § Regeringen, eller den myndighet regeringen bestämmer, meddelar närmare föreskrifter eller beslut om vilka uppgifter som får behandlas i databaserna.

I 1 kap. 7 § finns vissa bestämmelser om innehåll som gäller för uppgifter som behandlas i den militära säkerhetstjänsten.

Sökbegrepp

6 § Vid sökning efter uppgifter i informationsdatabasen eller underrättelse- och säkerhetsdatabasen får uppgifter om ras eller etniskt ursprung, politisk åsikt, religiös eller filosofisk övertygelse,

medlemskap i fackförening, hälsa eller sexualliv användas som sökbegrepp endast om det är nödvändigt för syftet med behandlingen.

Direktåtkomst

7 § Vilka som får ha direktåtkomst till Försvarsmaktens informationsdatabas eller underrättelse- och säkerhetsdatabas bestäms av regeringen i förordning eller beslut.

Regeringen, eller den myndighet regeringen bestämmer, meddelar närmare föreskrifter eller beslut om omfattningen av direktåtkomsten.

3 kap. Enskildas rättigheter

Information till den registrerade

1 § Vid tillämpningen av denna lag gäller bestämmelserna om information till den registrerade i 23 och 25–27 §§ personuppgiftslagen (1998:204).

Rättelse och skadestånd

2 § Bestämmelserna i personuppgiftslagen (1998:204) om rättelse och skadestånd gäller vid behandling av personuppgifter enligt denna lag eller anslutande författningar.

Överklagande

3 § Försvarsmaktens beslut om rättelse och om information som skall lämnas enligt 26 § personuppgiftslagen (1998:204) får överklagas hos allmän förvaltningsdomstol. Andra beslut enligt denna lag får inte överklagas.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Särskild granskning till skydd för den personliga integriteten

4 § Den myndighet som regeringen bestämmer skall ha till särskild uppgift att granska att Försvarsmaktens behandling av personuppgifter i försvarsunderrättelseverksamheten och den militära säkerhetstjänsten sker i enlighet med bestämmelserna i denna lag.

---

1. Denna lag träder i kraft den 1 juli 2004.
2. Bestämmelser i lagen om grundläggande krav på behandling av personuppgifter samt behandling av känsliga personuppgifter skall inte börja tillämpas förrän den 1 oktober 2007 i fråga om sådan manuell behandling av personuppgifter som påbörjats före den 24 oktober 1998 eller manuell behandling som utförs för ett visst bestämt ändamål om manuell behandling för ändamålet påbörjats före den 24 oktober 1998.

2 Förslag till lag om behandling av uppgifter i Försvarets radioanstalts underrättelseverksamhet

Härigenom föreskrivs följande.

1 kap. Allmänna bestämmelser

Lagens tillämpningsområde m.m.

1 § Denna lag tillämpas vid behandling av personuppgifter i Försvarets radioanstalts underrättelseverksamhet, om behandlingen är helt eller delvis automatiserad eller om uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Bestämmelserna i 4–5 §§ samt 2 kap. gäller även vid behandling av uppgifter om juridiska personer.

I 2 kap. finns bestämmelser om behandling av personuppgifter i Försvarets radioanstalts databaser.

Förhållandet till personuppgiftslagen

2 § Om inte annat anges i 3 § eller i 3 kap. gäller denna lag i stället för personuppgiftslagen (1998:204).

3 § När personuppgifter behandlas enligt denna lag eller enligt andra föreskrifter i det ämne som regleras i lagen gäller personuppgiftslagens (1998:204) bestämmelser om

1. definitioner i 3 §,
2. förhållandet till offentlighetsprincipen m.m. i 8 §,
3. grundläggande krav på behandling i 9 §,
4. säkerheten vid behandling i 30 och 31 §§,
5. personuppgiftsombud m.m. i 36 § andra stycket och 38–40 §§,
6. tillsynsmyndighetens befogenheter i 43 och 47 §§, och
7. straff i 49 §.

Personuppgiftsansvar

4 § Försvarets radioanstalt är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför eller som det åligger myndigheten att utföra. Motsvarande ansvar gäller för behandling av uppgifter om juridiska personer.

Ändamål

5 § Uppgifter får behandlas i underrättelseverksamheten dels för att kartlägga yttre militära hot mot landet dels till stöd för svensk utrikes-, försvars- och säkerhetspolitik, om det behövs för

1. säkerhetspolitiska och militärstrategiska bedömningar,
2. analyser av pågående och bedömda framtida konflikter, eller
3. biografisk försvarsunderrättelseverksamhet.

Uppgifter får också behandlas om det behövs för myndighetens verksamhet med att

1. bedriva signalspaning enligt den inriktning som regeringen, Försvarsmakten och övriga uppdragsgivare anger,
2. följa förändringen av signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet,
3. fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten,
4. utföra matematiska bedömningar av kryptosystem för totalförsvaret, samt
5. biträda andra myndigheter vid värdering, utveckling, anskaffning och drift av signalspaningssystem.

Behandling av känsliga personuppgifter

6 § Uppgifter om en person får inte behandlas enbart på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv.

Om uppgifter om en person behandlas på annan grund får de kompletteras med sådana uppgifter som avses i första stycket om det är nödvändigt för syftet med behandlingen.

Överföring av personuppgifter till tredje land

7 § Personuppgifter som behandlas med stöd av denna lag får lämnas ut till andra länder om sekretess inte hindrar det och det

behövs för att Försvarets radioanstalt skall kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet eller det annars är nödvändigt för verksamheten.

2 kap. Försvarets radioanstalts databaser

Inledande bestämmelse

1 § I underrättelseverksamheten skall det finnas ett antal skilda samlingar uppgifter, som med hjälp av automatiserad behandling används gemensamt i verksamheten för de i 1 kap. 5 § angivna ändamålen (databaser).

Urvalsdatabasen

2 § Uppgifter som används för att bestämma planering och inriktning av inhämtning av information, genom signalspaning eller på annat sätt, skall behandlas i en urvalsdatabas.

Uppgifter i databasen får endast behandlas för tillhandahållande av nödvändig urvalsinformation.

Källdatabasen

3 § Uppgifter som har inhämtats genom signalspaning skall behandlas i en källdatabas för att göra inhämtad information tillgänglig i verksamheten.

Uppgifter i databasen får utöver vad som anges i första stycket behandlas endast genom att med hjälp av urvalskriterier föras över till analysdatabasen.

Databasen för öppna källor

4 § Uppgifter som har inhämtats på annat sätt än genom signalspaning skall behandlas i en databas för öppna källor för att göra inhämtad information tillgänglig i verksamheten.

Uppgifter i databasen får utöver vad som anges i första stycket behandlas endast genom att med hjälp av urvalskriterier föras över till analysdatabasen.

Analysdatabasen

5 § Uppgifter som lagras i källdatabasen och databasen för öppna källor får tillsammans med andra nödvändiga uppgifter behandlas i en analysdatabas för analys och annan bearbetning, såsom dekryptering och översättning.

Uppgifter i databasen får utöver vad som framgår av första stycket behandlas endast för utarbetande av underrättelserapporter och lagring av arbetsmaterial för sådana rapporter.

Rapportdatabasen

6 § Uppgifter i färdiga underrättelserapporter som har utarbetats i analysdatabasen skall behandlas i en rapportdatabas för att göra informationen i rapporterna tillgänglig i verksamheten.

Uppgifter som får behandlas

7 § Regeringen, eller den myndighet regeringen bestämmer, meddelar närmare föreskrifter eller beslut om vilka uppgifter som får behandlas i databaserna.

Sökbegrepp

8 § Vid sökning efter uppgifter i en databas får uppgifter om ras eller etniskt ursprung, politisk åsikt, religiös eller filosofisk övertygelse, medlemskap i fackförening, hälsa eller sexualliv användas som sökbegrepp endast om det är nödvändigt för syftet med behandlingen.

Direktåtkomst

9 § Direktåtkomst får förekomma endast till rapportdatabasen. Regeringen meddelar närmare föreskrifter eller beslut om vilka som får ha direktåtkomst till rapportdatabasen.

Regeringen, eller den myndighet regeringen bestämmer, meddelar närmare föreskrifter eller beslut om omfattningen av direktåtkomsten.

3 kap. Enskildas rättigheter m.m.

Information till den registrerade

1 § Vid tillämpningen av denna lag gäller bestämmelserna om information till den registrerade i 23 och 25–27 §§ personuppgiftslagen (1998:204).

Rättelse och skadestånd

2 § Bestämmelserna i personuppgiftslagen (1998:204) om rättelse och skadestånd gäller vid behandling av personuppgifter enligt denna lag eller anslutande författningar.

Överklagande

3 § Försvarets radioanstalts beslut om rättelse och om information som skall lämnas enligt 26 § personuppgiftslagen (1998:204) får överklagas hos allmän förvaltningsdomstol. Andra beslut enligt denna lag får inte överklagas.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Särskild granskning till skydd för den personliga integriteten

4 § Den myndighet som regeringen bestämmer skall ha till särskild uppgift att granska att Försvarets radioanstalts behandling av personuppgifter i underrättelseverksamheten sker i enlighet med bestämmelserna i denna lag.

---

1. Denna lag träder i kraft den 1 juli 2004.
2. Bestämmelser i lagen om grundläggande krav på behandling av personuppgifter samt behandling av känsliga personuppgifter skall inte börja tillämpas förrän den 1 oktober 2007 i fråga om sådan manuell behandling av personuppgifter som påbörjats före den 24 oktober 1998 eller manuell behandling som utförs för ett visst bestämt ändamål om manuell behandling för ändamålet påbörjats före den 24 oktober 1998.

3 Förslag till lag om ändring i sekretesslagen (1980:100)

Härigenom föreskrivs att det i sekretesslagen (1980:100) skall införas en ny paragraf, 9 kap. 27 §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	9 kap.
	27 §
	Sekretess gäller hos Försvarsmakten i den militära underrättelse- och säkerhetstjänsten för uppgift om enskilds personliga eller ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon honom närstående lider skada eller men.
	I fråga om uppgift i allmän handling gäller sekretessen i högst sjuttio år.

Denna lag träder i kraft den 1 juli 2004.

4 Förslag till förordning om behandling av uppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten

Härigenom föreskrivs följande.

Definitioner

1 § Termer och uttryck i denna förordning har samma betydelse och tillämpningsområde som i lagen (2004:000) om behandling av uppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten.

Uppgifter som får behandlas

2 § I informationsdatabasen och underrättelse- och säkerhetsdatabasen får behandlas uppgifter som avser

1. identifiering av enskilda,
2. de omständigheter och händelser som ger anledning att anta att den registrerade har betydelse för myndighetens försvarsunderrättelseverksamhet eller militära säkerhetstjänst,
3. upplysningar om varifrån den registrerade uppgiften kommer och om uppgiftslämnarens trovärdighet, och
4. hänvisningar till de ärenden där uppgifter om den registrerade behandlas.

Försvarsmakten får meddela närmare föreskrifter eller beslut om vilka uppgifter som får behandlas i myndighetens databaser.

Sekretess

3 § Utöver vad som framgår av 1 kap. 3 § tredje stycket sekretesslagen (1980:100) får uppgifter för vilka sekretess gäller enligt den lagen lämnas ut till en utländsk myndighet eller en internationell organisation om utlämnandet tjänar den svenska statsledningen och det svenska totalförsvaret samt om lämnade uppgifter inte är till skada för svenska intressen.

Direktåtkomst

4 § Regeringskansliet, Försvarets materielverk och Försvarets radioanstalt får ha direktåtkomst till informationsdatabasen.

Regeringskansliet, Försvarets materielverk, Försvarets radioanstalt, Totalförsvarets forskningsinstitut, Tullverket och Krisberedskapsmyndigheten får ha direktåtkomst till underrättelse- och säkerhetsdatabasen.

Försvarsmakten får bestämma omfattningen av den direktåtkomst som får förekomma enligt första och andra stycket.

Granskningsmyndighet

5 § Försvarets underrättelsenämnd är granskningsmyndighet enligt lagen (2004:000) om behandling av uppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten.

Verkställighetsföreskrifter

6 § Försvarsmakten får meddela närmare föreskrifter om verkställighet av bestämmelserna i lagen (2004:000) om behandling av uppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten.

Denna förordning träder i kraft den 1 juli 2004.

5 Förslag till förordning om behandling av uppgifter i Försvarets radioanstalts underrättelseverksamhet

Härigenom föreskrivs följande.

Definitioner

1 § Termer och uttryck i denna förordning har samma betydelse och tillämpningsområde som i lagen (2004:000) om behandling av uppgifter i Försvarets radioanstalts underrättelseverksamhet.

Uppgifter som får behandlas

2 § I urvalsdatabasen, källdatabasen, databasen för öppna källor, analysdatabasen och rapportdatabasen får behandlas uppgifter som avser

1. identifiering av enskilda,
2. de omständigheter och händelser som ger anledning att anta att den registrerade har betydelse för myndighetens försvarsunderrättelseverksamhet eller militära säkerhetstjänst,
3. upplysningar om varifrån den registrerade uppgiften kommer och om uppgiftslämnarens trovärdighet, och
4. hänvisningar till de ärenden där uppgifter om den registrerade behandlas.

Försvarets radioanstalt får meddela närmare föreskrifter eller beslut om vilka uppgifter som får behandlas i myndighetens databaser.

Sekretess

3 § Utöver vad som framgår av 1 kap. 3 § tredje stycket sekretesslagen (1980:100) får uppgifter för vilka sekretess gäller enligt den lagen lämnas ut till en utländsk myndighet eller en internationell organisation om utlämnandet tjänar den svenska statsledningen och det svenska totalförsvaret samt om lämnade uppgifter inte är till skada för svenska intressen.

Direktåtkomst

4 § Regeringskansliet och Försvarsmakten får ha direktåtkomst till rapportdatabasen.

Försvarets radioanstalt får bestämma omfattningen av den direktåtkomst som får förekomma enligt första stycket.

Granskningsmyndighet

5 § Försvarets underrättelsenämnd är granskningsmyndighet enligt lagen (2004:000) om behandling av uppgifter i Försvarets radioanstalts underrättelseverksamhet.

Verkställighetsföreskrifter

6 § Försvarets radioanstalt får meddela närmare föreskrifter om verkställighet av bestämmelserna i lagen (2004:000) om behandling av uppgifter i Försvarets radioanstalts underrättelseverksamhet.

Denna förordning träder i kraft den 1 juli 2004.

6 Förslag till förordning om ändring i förordningen (1988:552) med instruktion för Försvarets underrättelsenämnd

Härigenom föreskrivs att 1 och 2 §§ förordningen (1988:552) med instruktion för Försvarets underrättelsenämnd skall ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 §	
Försvarets underrättelsenämnd har till uppgift att följa underrättelsetjänsten inom Försvarsmakten och de övriga myndigheter som enligt förordningen (2000:131) om försvarsunderrättelseverksamhet bedriver försvarsunderrättelseverksamhet.	
	Nämnden har även till uppgift att följa den militära säkerhetstjänsten inom Försvarsmakten enligt säkerhetsskyddslagen (1996:627).
2 §	
Nämnden skall särskilt	
1. följa hur lagen (2000:130) om försvarsunderrättelseverksamhet och förordningen (2000:131) om försvarsunderrättelseverksamhet tillämpas,	
2. granska att försvarsunderrättelseverksamheten bedrivs i enlighet med den inriktning som är bestämd,	
3. ägna uppmärksamhet åt de enheter inom Försvarsmakten och Försvarets radioanstalt som inhämtar underrättelser med särskilda metoder,	

4. granska de medel och metoder för inhämtning av underrättelser som används,	
5. granska *hur de register som behövs för försvarsunderrättelseverksamheten läggs upp och förs samt*	5. granska *behandlingen av uppgifter enligt lagen (2004:000) om behandling av uppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt enligt lagen (2004:000) om behandling av uppgifter i Försvarets radioanstalts underrättelseverksamhet.*
6. granska principer för rekrytering och utbildning av personal.	

Denna förordning träder i kraft den 1 juli 2004.

7 Förslag till förordning om upphävande av förordningen (2001:703) om viss behandling av personuppgifter inom Försvarsmakten och Försvarets radioanstalt

Härigenom föreskrivs att förordningen (2001:703) om viss behandling av personuppgifter inom Försvarsmakten och Försvarets radioanstalt skall upphöra att gälla vid utgången av juni 2004.

BAKGRUNDEN TILL VÅRA FÖRSLAG

1 Uppdraget

1.1 Utredningens direktiv

Vårt uppdrag är att göra en översyn av regleringen av behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet. Syftet med uppdraget är att vi skall kartlägga behandlingen av personuppgifter och analysera behovet av särskilda bestämmelser samt lämna förslag till reglering i lag.

I vårt uppdrag ingår att granska frågor som rör användning, inhämtande, utlämnande, gallring och arkivering samt tillsyn. Utgångspunkten är att myndigheternas verksamhet skall kunna bedrivas effektivt och med ett rationellt datorstöd samtidigt som nödvändig respekt visas för enskildas personliga integritet. I arbetet skall också det internationella inslaget i myndigheternas verksamheter beaktas.

Bakgrunden till behovet av översyn utgörs av personuppgiftslagen (1998:204) som trädde i kraft den 24 oktober 1998 och som i fråga om automatiserad behandling av personuppgifter i princip gäller fullt ut från och med den 1 oktober 2001. Genom lagen genomförde Sverige Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (dataskyddsdirektivet). Enligt artikel 3.2 första strecksatsen gäller dataskyddsdirektivet inte för sådan behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av EG-rätten och inte under några omständligheter behandlingar som rör allmän säkerhet, försvar, statens säkerhet och statens verksamhet på straffrättens område. Den svenska personuppgiftslagen har däremot gjorts generellt tillämplig och omfattar även sådan verksamhet som faller utanför EG-rättens område, således även försvarsmyndigheternas underrättelseverk-

samhet och militär säkerhetstjänst. Enligt personuppgiftslagen gäller emellertid att avvikande bestämmelser i lag eller förordning har företräde framför personuppgiftslagen. Lagen innehåller i princip endast generella regler och behovet av undantag och särregler för mer speciella områden får tillgodoses genom andra författningar.

För närvarande regleras den aktuella behandlingen av personuppgifter i förordningen (2001:703) om viss behandling av personuppgifter inom Försvarsmakten och Försvarets radioanstalt samt i personuppgiftslagen (1998:204). Inom Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet behandlas i dag en stor mängd personuppgifter som dessutom kan vara av känslig natur. Såväl riksdagen som regeringen har vid upprepade tillfällen framhållit att sådan behandling av personuppgifter bör regleras särskilt i lag i stället för i förordning (se bl.a. bet. 1997/98:KU18 s. 43 och prop. 1997/98:44 s. 41). Vi har således i uppdrag att ersätta de bestämmelser som i dag finns i förordningen med lagregler anpassade för att tillgodose ifrågavarande myndigheters behov av att kunna bedriva sin verksamhet effektivt med ett rationellt datorstöd, samtidigt som nödvändiga integritetsaspekter beaktas.

Direktiven i sin helhet framgår av *bilaga 1*.

1.2 Utredningsarbetet

Vårt arbete har bedrivits med målsättningen att anpassa bestämmelserna om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet till personuppgiftslagens rättsliga ramar och till behovet av ett regelverk som främjar effektiviteten i dessa verksamheter. Härvid har även dataskyddsdirektivet beaktats, som utan att vara direkt tillämpligt ändå utgör den grundläggande rättsliga regleringen av skyddet för den personliga integriteten med avseende på behandling av personuppgifter. Europarådets dataskyddskonvention, som utan undantag är tillämplig på verksamheterna, har beaktats fullt ut.

En av de grundläggande utgångspunkterna för vårt arbete har varit att föreslå moderna, teknikneutrala och allmänt ändamålsenliga och flexibla regler. I detta ligger att vi inte i första hand haft som målsättning att enbart skräddarsy regleringen för redan

befintliga eller kända och planerade datorsystem. Avsikten har varit att lägga fast vissa grundläggande principer och bestämmelser vilka skall gälla för all helt eller delvis automatiserad behandling av personuppgifter oavsett i vilken form denna sker. Dessa bestämmelser kompletteras med särskilda regler för myndigheternas databaser, utan att reglerna hindrar nya tekniska lösningar som kan möjliggöra nödvändig framtida teknisk utveckling och effektivisering.

Den andra viktiga utgångspunkten för arbetet har varit att ta hänsyn till de integritetsaspekter som följer av användningen av omfattande automatiserade uppgiftssamlingar i den militära underrättelse- och säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet. Särskild vikt har härvid lagts vid att anpassa de integritetsskyddande reglerna till de särskilda sekretesskrav som gäller för försvarsunderrättelseverksamhet och militär säkerhetstjänst.

Vårt arbete har bedrivits i nära samråd med företrädare för den militära underrättelse- och säkerhetstjänsten samt Försvarets radioanstalt. Utredningen har besökt både Försvarets radioanstalt och Försvarsmaktens högkvarter och i samband härmed sammanträffat med företrädare för myndigheternas olika verksamheter inom ramen för utredningsuppdraget. Därutöver har utredningens sekreterare träffat företrädare för den militära underrättelse- och säkerhetstjänsten för att på plats studera verksamheten. Utredaren och sekreteraren har vidare sammanträffat med ordföranden för Försvarets underrättelsenämnd och utredningen har fortlöpande samrått med företrädare för nämnden. Vi har sammanträffat med Samordningssekretariatet för säkerhetspolitiska underrättelsefrågor i Regeringskansliet. Vidare har samrått skett med Utredningen om översyn av Försvarets radioanstalt (Dir. 2001:66) samt Utredningen om översyn av personuppgiftslagen (Dir. 2002:31).

Det ligger i sakens natur att vi under arbetets gång har tagit del av uppgifter av hemlig och kvalificerat hemlig natur. Vi har emellertid inriktat utredningens arbete på att lämna ett betänkande som i sin helhet kan läggas fram offentligt.

2 Försvarsmaktens försvars-underrättelseverksamhet och den militära säkerhetstjänsten

Utredningen har i uppdrag att göra en översyn av regleringen av behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet. Försvarsunderrättelseverksamhet skall bedrivas för att kartlägga yttre militära hot mot landet och till stöd för svensk utrikes-, försvars- och säkerhetspolitik. Den militära säkerhetstjänsten syftar till att tillgodose det långsiktiga säkerhetsskyddet för Försvarsmakten och dess intressen. Försvarsunderrättelseverksamhet bedrivs av Försvarsmakten samt de andra myndigheter som regeringen bestämmer. Försvarets radioanstalt är en av de myndigheter som utöver Försvarsmakten skall bedriva försvarsunderrättelseverksamhet. Den militära säkerhetstjänsten bedrivs av Försvarsmakten.

I detta och följande kapitel beskriver vi Försvarsmaktens och Försvarets radioanstalts uppgifter och organisation såvitt avser de aktuella verksamheterna. I detta kapitel lämnas också en redogörelse för innebörden av begreppen försvarsunderrättelseverksamhet och militär säkerhetstjänst samt för hur dessa verksamheter regleras genom lag och annan författning.

2.1 Försvarsmaktens organisation och verksamhet

Försvarsmaktens organisation

Försvarsmakten är en myndighet under regeringen med överbefälhavaren (ÖB) som chef. Försvarsmakten består i princip av två, organisatoriskt delvis sammanfallande, delar. Den ena är grundorganisationen i vilken Försvarsmaktens resurser fortlöpande utvecklas, vidmakthålls och – vid behov – avvecklas. Den andra är insatsorganisationen, i vilken resurserna används.

Grundorganisationen indelas i organisationsenheter (förband, skolor och centra). Den upprätthåller den beredskap som krävs för att sätta upp de krigsförband som behövs i insatsorganisationen. *Insatsorganisationen* utgörs av Högkvarteret med operativa insatsledningen (OPIL), militärdistrikten, de operativa insatsförbanden, och de nationella skyddsstyrkorna. Insatsorganisationen tillförs resurser antingen från grundorganisationen – t.ex. förband under utbildning, hemvärn eller förband som upprätthåller beredskap – eller genom att förband mobiliseras.

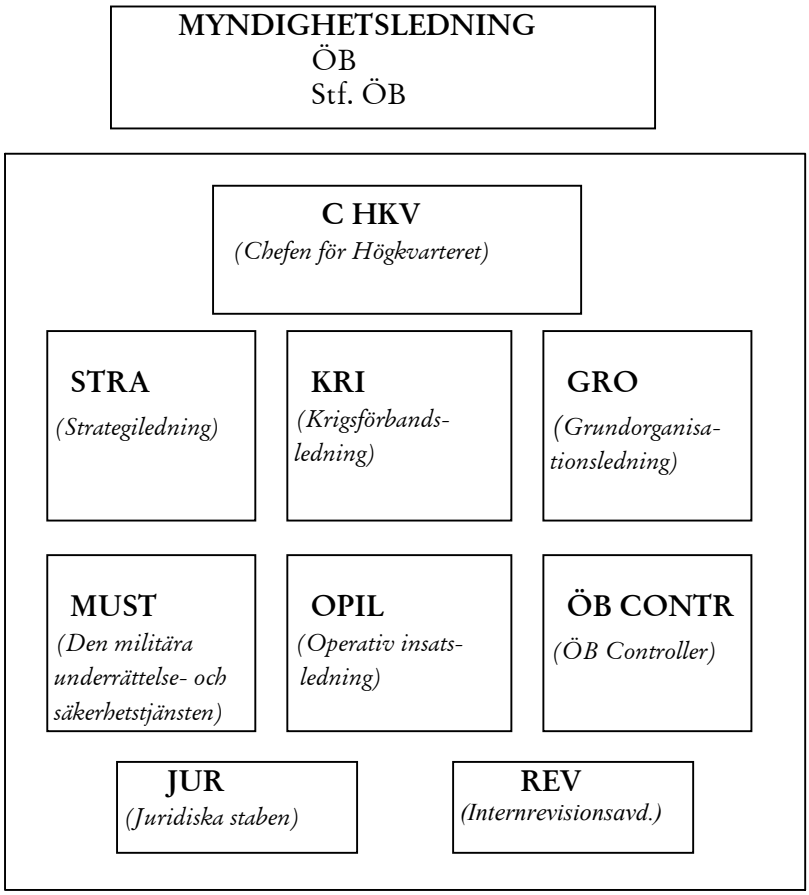
Högkvarterets främsta uppgift är verksamhetsledning och insatsledning med tillhörande militärstrategiska frågor, Försvarsmaktens utveckling och att vara kontaktyta mot regeringen. Högkvarteret leds av en chef (C HKV). I Högkvarteret återfinns funktioner för bl.a. militärstrategisk och territoriell ledning, samt verksamhetsledning, planering, försvarsmaktsstudier, informationstjänst, personalförsörjning samt underrättelse- och säkerhetstjänst.

För operativ och taktisk ledning finns OPIL som innehåller operationsledning och tre taktiska kommandon (armé, marin och flyg). Cheferna för operationsledningen och de tre taktiska kommandona är underställda chefen för OPIL.

Militärdistriktens uppgift är att leda territoriell verksamhet, som bl.a. innebär samverkan med totalförsvarets civila delar på regional och lokal nivå. Militärdistrikten leder och genomför också utbildning av hemvärnet och stödjer de frivilliga försvarsorganisationerna.

Uppdrag till organisationsenheterna ges av grundorganisationsledningen (GRO). Strategiledningen (STRA) leder Försvarsmaktens långsiktiga utveckling, planering och avvägning, militärstrategiska inriktning och planering i fred, kris och krig. Krigsförbandsledningen (KRI) är ansvarig för krigsförbanden. Chefen för KRI leder och samordnar utveckling, vidmakthållanden och avveckling av krigsförband samt genomför materiel- och anläggningsförsörjning.

Högkvarterets organisation ser sedan den 1 januari 2002 ut som följer.



Försvarsmaktens verksamhet

De grundläggande uppgifterna för Försvarsmakten framgår av bestämmelserna i 1–3 §§ förordningen (2000:555) med instruktion för Försvarsmakten. Enligt dessa bestämmelser är myndighetens uppgift att försvara hela Sverige mot väpnat angrepp var det än kommer ifrån, och hävda Sveriges territoriella integritet. Grunden för Försvarsmaktens verksamhet skall vara förmågan till väpnad strid. Försvarsmakten skall bidra till fred och säkerhet i omvärlden genom att kunna genomföra och lämna stöd till fredsfrämjande operationer och säkerhetsfrämjande samarbete samt kunna lämna stöd till humanitär verksamhet. Försvarsmakten skall bidra till att stärka det svenska samhället vid svåra påfrestningar i fred genom att kunna samverka med andra myndigheter och kunna ställa

resurser till förfogande. Försvarsmakten skall ha den operativa förmåga, de kompetenser och den insatsorganisation som regeringen beslutar. Försvarsmakten skall även upprätthålla den beredskap som regeringen beslutar. Försvarsmaktens beredskap, organisation och planläggning skall medge att Försvarsmaktens förmåga kan anpassas för att motsvara förändrade krav och behov. Försvarsmakten skall genomföra den planläggning och vidta de förberedelser som behövs för att kunna lösa myndighetens uppgifter.

Utöver dessa grundläggande uppgifter har Försvarsmakten vissa särskilda uppgifter. Av 4 § 1–3 i myndighetens instruktion framgår de särskilda uppgifter som är av intresse för utredningens uppdrag. Enligt nämnda bestämmelser skall Försvarsmakten särskilt leda och bedriva försvarsunderrättelseverksamhet och militär säkerhetstjänst samt leda och samordna signalskyddstjänsten inom totalförsvaret.

2.2 Den militära underrättelse- och säkerhetstjänsten

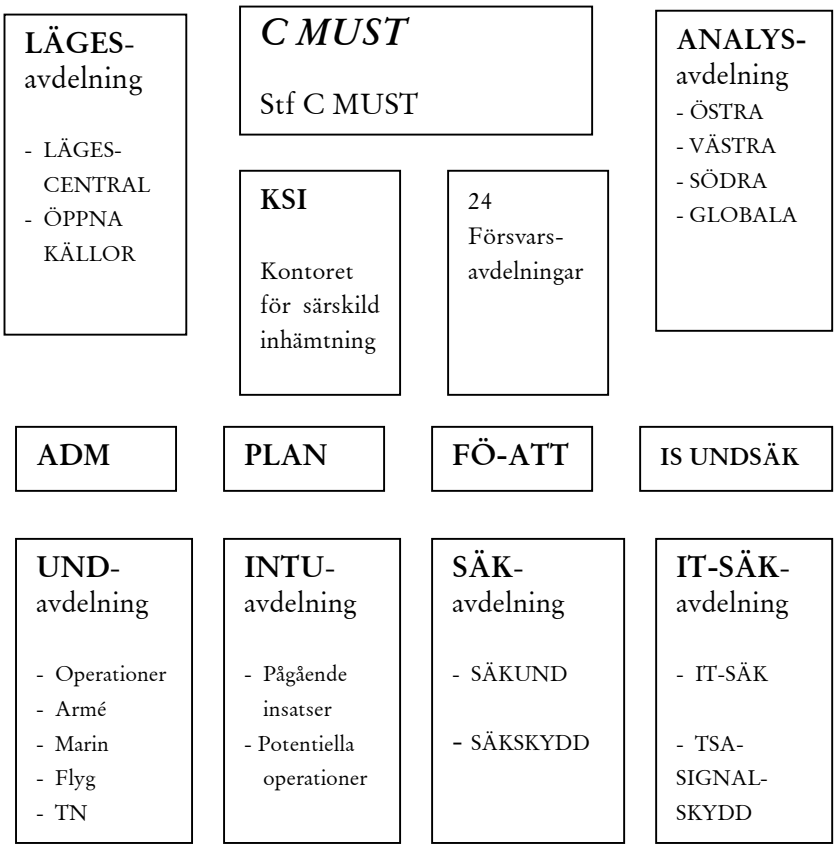
Försvarsmaktens ansvar när det gäller försvarsunderrättelseverksamhet och militär säkerhetstjänst utövas av den militära underrättelse- och säkerhetstjänsten (MUST). MUST är organisatoriskt en enhet inom Försvarsmaktens högkvarter. MUST leder inhämtning, bearbetning och delgivning av militära underrättelser samt samordnar och inriktar underrättelseproduktionen vid Försvarets radioanstalt och andra myndigheter som bedriver försvarsunderrättelseverksamhet. Den militära underrättelse- och säkerhetstjänsten leder även säkerhetstjänsten inom Försvarsmakten samt signalskyddstjänsten inom hela totalförsvaret.

I direkt samverkan med bl.a. försvars- och utrikesdepartementet medverkar MUST i den av statsmakterna ledda strategiska underrättelsetjänsten. MUST stödjer med underrättelser, planering för och genomförande av svenska internationella insatser.

2.2.1 MUST:s organisation

MUST är således den enhet inom Försvarsmaktens högkvarter som har till uppgift att leda den militära underrättelse- och säkerhetstjänsten. MUST:s verksamhet är organiserad på sex olika avdelningar samt en speciell enhet för särskild inhämtning av underrättelser. Därutöver finns fyra sektioner med framför allt

administrativ inriktning. Nedan följer en skiss över MUST:s organisation som den såg ut per den 1 december 2002.



Verksamheten leds av chefen för MUST och dennes ställföreträdare. *Administrativa sektionen (ADM)* svarar för administrativt stöd inom MUST.

Planeringssektionen (PLAN) utgör chefens för MUST ledningsfunktion. Sektionen samordnar inriktningen, inhämtningen och delgivningen av underrättelser inom Försvarsmakten samt ger förslag om inriktning och samordning av underrättelseverksamheten vid de övriga försvarsunderrättelsemyndigheterna. Sektionen leder funktionsutvecklingen för såväl underrättelse- som säkerhetstjänsten. Sektionen utarbetar också allmänna råd och föreskrifter beträffande underrättelsetjänsten inom Försvarsmakten.

Under chefen för MUST lyder *24 försvarsavdelningar* vilka vardera förestås av en försvarsattaché. *Försvarsattachésektionen (FÖ-ATT)* stödjer Sveriges försvarsattachéer administrativt med bl.a. samordning, organisation och utbildning. Försvarsattachéernas verksamhet vid olika svenska beskickningar är reglerad i förordningen (FFS 1985:20) om Sveriges försvarsattachéer. Enligt 4 § i förordningen är attachéerna underställda Försvarsmakten, men lyder under beskickningschefen i vissa avseenden. Det ankommer på chefen för MUST att leda verksamheten för attachéerna. Försvarsattachéerna verkar hos aktuella ambassader vid försvarsavdelningar som utgör enheter inom MUST. Försvarsattachéerna är avsedda att utgöra en förbindelselänk mellan värdlandet och den svenska försvarsmakten. De har att på öppen väg inhämta information om militärpolitiska förhållanden och om den militära och militärtekniska utvecklingen i värdlandet. De skall även följa och bedöma utvecklingen och de säkerhetspolitiska förhållanden i värdlandet, som kan få konsekvenser för totalförsvaret i hemlandet. Härutöver har attachéerna vissa uppgifter, som inte direkt anknyter till underrättelseverksamheten.

Ledningssektionen för IS UNDSÄK har i huvudsak till uppgift att utveckla, anskaffa, driftsätta och förvalta Informationssystem för den militära underrättelse- och säkerhetstjänsten (IS UNDSÄK), se avsnitt 5.3.2.

Lägesavdelningen hanterar all ingående och utgående information inom MUST. Detta innebär att avdelningen mottar och lagrar all inkommande information samt delger uppgifter om MUST:s analyser av det säkerhetspolitiska, militära och säkerhetshotande läget. Lägesavdelningen samordnar utarbetandet av regelbundna och särskilda rapporteringar om aktuella händelser som påverkar Försvarsmakten eller är av säkerhetspolitiskt eller i övrigt av stort intresse. Vid en särskild sektion inom avdelningen, Sektionen för Öppna Källor (SÖK), inhämtas, bearbetas och delges information som är allmänt tillgänglig, bl.a. från internationella databaser via Internet. Vidare biträder avdelningen säkerhetstjänsten med uppföljning av aktuella säkerhetsrapporter. Avdelningen leder också MUST:s arkivtjänst och den interna signalskyddsverksamheten.

Analysavdelningen genomför inhämtning, bearbetning och analys samt delgivning av underrättelser rörande säkerhetspolitisk, ekonomisk och militärstrategisk utveckling. Inom avdelningen utarbetas säkerhetspolitiskt, militärstrategiskt och operativt beslutsunderlag för Regeringskansliet och Högkvarteret. Vidare

utarbetar avdelningen kontinuerligt underrättelser om det aktuella säkerhetspolitiska, militära och säkerhetshotande läget. Avdelningen utarbetar beslutsunderlag inom Försvarsmakten och till Regeringskansliet avseende sådana säkerhetspolitiska utvecklingstendenser i omvärlden, som kan medföra krav på svenska internationella insatser. Avdelningen stödjer också INTU-avdelningen med säkerhetspolitiska och militärstrategiska bedömningar under en pågående svensk internationell insats. Vidare utarbetar avdelningen säkerhetspolitiskt underlag för underrättelsesamarbete med andra länder.

Underrättelseavdelningen genomför bearbetning och analys av grundläggande underrättelser om främst vissa andra länders militära stridskrafter. Verksamheten utgör stöd för strategisk underrättelsetjänst, operativ verksamhet, planering och förbandsproduktion. Avdelningen svarar för produktionen av hotbildsunderlag och fakta beträffande stridskrafter och övrigt stöd. Avdelningen inhämtar, bearbetar och delger även biografiska underrättelser avseende militära chefer. Avdelningen inhämtar, bearbetar och delger också underrättelser avseende informationskrigföring, spridning av massförstörelsevapen, terrorism, främmande undervattensverksamhet samt stödjer inriktningen av Sveriges försvarsattachéer. Underrättelseavdelningen är indelad i fem sektioner, en för respektive Operationer, Armé, Marin och Flyg samt i den Transnationella sektionen.

Avdelningen för internationella underrättelser (INTU-avdelningen) utarbetar underlag avseende det militära läget i konfliktområden där svensk internationell insats är eller kan komma att bli aktuell. Avdelningen ansvarar för underrättelser till stöd för svenska förband och enheter som deltar i internationella fredsbevarande och humanitära insatser. Verksamheten är inriktad på såväl pågående insatser som potentiella operationer och syftar till att skydda den svenska personalen som deltar i de olika missionerna. Avdelningen stödjer också analysavdelningen med operativa bedömningar i potentiella konfliktområden.

Säkerhetsavdelningen leder under chefen för MUST säkerhetstjänsten inom Försvarsmakten och planerar, inhämtar, bearbetar och delger säkerhetsunderrättelser. Avdelningen har tillsynsansvar för säkerhetstjänsten inom Försvarsmakten, men även för de flesta övriga myndigheter under Försvarsdepartementet samt Fortifikationsverket. Avdelningen utarbetar föreskrifter och allmänna råd för Försvarsmakten och nämnda myndigheter samt förslag till åtgärder för att utveckla den militära säkerhetstjänsten.

Säkerhetsavdelningen leder MUST:s samverkan med Rikspolisstyrelsen och Säkerhetspolisen. Inom säkerhetsavdelningen finns sektioner för säkerhetsunderrättelser och säkerhetsskydd.

Försvarsmakten och Rikspolisstyrelsen (Säkerhetspolisen) är de två myndigheter som leder säkerhetstjänsten inom Sverige. Försvarsmakten och Säkerhetspolisen är tillsynsmyndigheter och får enligt 44 § säkerhetsskyddsförordningen (1996:633) meddela ytterligare föreskrifter för verkställigheten av säkerhetsskyddslagen (1996:627) för sina respektive tillsynsområden. Vid Försvarsmaktens organisationsenheter skall det finnas en säkerhetschef. Chefen för MUST är Försvarsmaktens säkerhetsskyddschef. Han samordnar och kontrollerar den övergripande utvecklingen av underrättelse- och säkerhetstjänsten och samordnar den med totalförsvaret i övrigt.

IT-säkerhetsavdelningen leder under chefen för MUST IT-säkerhetsarbetet inom Försvarsmakten och signalskyddsarbetet inom hela totalförsvaret. I avdelningen ingår Totalförsvarets signalskyddssamordning (TSA). Avdelningen genomför bl.a. utbildningsinsatser och utarbetar regelverk inom IT-säkerhetsområdet. Inom TSA sker signalkontroll av radio- och trådbefordrad information eller annan informationsöverföring. Signalkontrollen syftar till att ge en bild av vad främmande signalspaning kan ha uppfattat av befordrad information samt att kontrollera att egna signalskyddssystem används och fungerar på önskat sätt. Inom IT-säkerhetsområdet har avdelningen motsvarande tillsynsansvar och uppgifter som säkerhetsavdelningen.

Kontoret för särskild inhämtning (KSI) arbetar enbart med inhämtning av underrättelser. Inhämtat material sammanställs i allmänhet till rapporter som överlämnas för vidare bearbetning inom MUST tillsammans med annat underrättelsematerial. KSI har till uppgift att inhämta information med särskilda metoder, dvs. genom förfaringssätt som det inte ankommer på andra underrättelseorgan att använda. KSI:s roll är därvid att ge Försvarsmakten möjlighet att ta till vara tillfällen till underrättelseinhämtning som andra organ inte kan utnyttja därför att de inte har ett säkerhetsskydd som är tillräckligt för situationen. KSI ingår i MUST och är underställd chefen för MUST, men lyder direkt under ÖB i vissa frågor.

2.2.2 MUST:s uppgifter och verksamhet

Försvarsmaktens grundläggande ansvar när det gäller att bedriva militär underrättelse- och säkerhetstjänst framgår som ovan nämnts av 4 § 1–3 förordningen (2000:555) med instruktion för Försvarsmakten. Här anges att Försvarsmakten skall leda och bedriva försvarsunderrättelseverksamhet och militär säkerhetstjänst samt leda och samordna signalskyddstjänsten inom totalförsvaret.

De närmare riktlinjerna för försvarsunderrättelseverksamheten och säkerhetstjänsten vid Försvarsmakten läggs varje år fast i regeringens regleringsbrev för myndigheten. I regleringsbrevet för budgetåret 2003 avseende Försvarsmakten anger regeringen att för myndigheter som bedriver försvarsunderrättelseverksamhet skall gälla bl.a. följande. *Försvarsunderrättelseverksamhet* skall bedrivas för att kartlägga yttre militära hot mot landet och till stöd för svensk utrikes-, försvars- och säkerhetspolitik. Försvarsunderrättelseverksamhetens inriktning mot en vidgad säkerhetspolitisk hotbild skall fortsätta. Detta ställer, enligt regeringen, krav på samverkan med andra myndigheter, och en nära kontakt med myndigheternas avnämare. Samarbete med andra länder och internationella organisationer skall vara en naturlig del av verksamheten. Underrättelseverksamhet till stöd för Sveriges allt bredare medverkan i det internationella säkerhetssamarbetet skall ha hög prioritet. Inom ramen för EU:s krishanteringsförmåga skall Försvarsmakten bidra till ett stärkt europeiskt underrättelsesamarbete. Försvarsmakten skall förse regeringen med uppgifter om den militära verksamheten i vår omvärld och ge underlag för bedömningar av den utrikes- och säkerhetspolitiska utvecklingen. Rapporteringen skall anpassas till regeringens behov i enlighet med vad som anges i den särskilda inriktningen.

Enligt regleringsbrevet är *den militära säkerhetstjänstens* uppgift att tillvarata de säkerhetsintressen som främst berör Försvarsmakten och att bl.a. biträda polisen i dess ansvar beträffande skydd av rikets säkerhet. Den militära säkerhetstjänsten i fred syftar till att tillgodose det långsiktiga säkerhetsskyddet inom Försvarsmakten. Även för den militära säkerhetstjänsten skall samarbete med andra länder och internationella organisationer vara en naturlig del av verksamheten. Ett utbyte av information anses nödvändigt för att Sverige skall kunna få del av sådan information som landet behöver men som kräver resurser som saknas.

Den militära säkerhetstjänsten omfattar säkerhetsunderrättelsetjänst och säkerhetsskyddstjänst. Vidare är också signalskydds-

tjänsten en säkerhetsskyddsangelägenhet. Säkerhetsunderrättelsetjänsten skall klarlägga den säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess intressen såväl inom som utom landet. Säkerhetsskyddstjänsten skall ta fram åtgärder som syftar till att hindra eller försvåra säkerhetshotande verksamhet. Den skall också förebygga att hemliga uppgifter som rör rikets säkerhet obehörigen röjs, ändras eller förstörs. Signalskyddstjänsten syftar till att minska verkan av signalspaning, falsk signalering och störsändning mot totalförsvarets telekommunikations- och informationssystem. Den skall förhindra obehörig insyn i och påverkan av totalförsvarets telekommunikationer. Detta uppnås bl.a. genom användning av kryptografiska funktioner i informationssystemen.

Försvarsunderrättelseverksamhet och militär säkerhetstjänst bedrivs av olika organisationsenheter och på olika nivåer inom Försvarsmakten. Således åligger det varje enhet eller förband att ha det säkerhetsskydd som verksamheten kräver samt att registrera och rapportera säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess intressen. För en enskild organisationsenhet, inklusive förband i utlandsstyrkan, kan det också finnas behov av att t.ex. följa upp olika personers förehavanden som ett led i myndighetens försvarsunderrättelseverksamhet. Ansvaret för ledning och samordning av försvarsunderrättelseverksamhet och militär säkerhetstjänst inom Försvarsmakten och totalförsvaret i övrigt sköts dock av enheten vid Högkvarteret, MUST. Det är också inom MUST som den största delen av den aktuella verksamheten faktiskt bedrivs.

Den närmare innebörden av begreppen försvarsunderrättelseverksamhet och militär säkerhetstjänst beskrivs i avsnitt 2.3 och 2.5.

Chefen för MUST har i verksamhetsledningen för år 2003 sammanfattat den militära underrättelse- och säkerhetstjänstens uppgifter. Enligt detta dokument gäller i huvudsak att MUST

- leder inhämtning, bearbetning och delgivning av militära underrättelser och säkerhetsunderrättelser inom Försvarsmakten samt inriktning och samordning av verksamheten vid stödmyndigheter,
- utarbetar underlag för eventuella beslut om svenska internationella insatser samt ger stöd med resurser, underlag och underrättelser under genomförandet av dessa,

- leder, samordnar och kontrollerar säkerhetsskyddstjänsten vid vissa myndigheter under Försvarsdepartementet, och lämnar utbildningsstöd inom och utom Försvarsmakten,
- leder, samordnar och kontrollerar signalskyddstjänsten inom totalförsvaret,
- utvecklar säkerhetsskyddsförmågan inom IT-området och metoder för aktiv IT-kontroll inom Försvarsmakten,
- leder försvarsattachéverksamheten inom Försvarsmakten,
- lämnar stöd till Humanistisk- Samhällsvetenskapliga forskningsrådet och andra statligt utsedda utredningar och kommissioner så att relevant arkivmaterial hos Försvarsmakten för forskningsprojekt om militär underrättelse- och säkerhetstjänst skyndsamt kan tas fram,
- leder den militära underrättelse- och säkerhetstjänsten.

2.3 Försvarsunderrättelseverksamhet

Sedan lång tid tillbaka har nationer ansett sig ha ett behov av att skaffa information om främmande staters resurser och möjligheter i krig, bl.a. som underlag för militära operationer. Samtidigt har det i fredstid funnits ett motsvarande behov av information för att få besked om den säkerhetspolitiska situationen och om denna kräver mobilisering av landets försvarsmakt eller andra åtgärder vid kriser eller i händelse av krig. Av dessa skäl bedrivs försvarsunderrättelseverksamhet för att kartlägga främmande makters militära och politiska förhållanden och handlingsmöjligheter.

Med försvarsunderrättelseverksamhet avses en verksamhet eller en process för att hämta in, bearbeta och delge underrättelser och information. Begreppet försvarsunderrättelseverksamhet, som avser både militärt och civilt försvar, syftar till att göra åtskillnad till andra begrepp som t.ex. kriminalunderrättelseverksamhet. Försvarsunderrättelseverksamhet bedrivs för att kartlägga yttre militära hot mot landet och till stöd för svensk utrikes-, försvars- och säkerhetspolitik.

Säkerhetspolitik är en sammanfattande benämning på de åtgärder som landets regering vidtar inom ramen för utrikes- och försvarspolitiken till skydd mot yttre hot mot landet och för att bevara landets fred och självständighet. Sveriges säkerhetspolitiska mål är att i alla lägen och i former som vi själva väljer trygga en handlingsfrihet att, såsom enskild nation och i samverkan, kunna utveckla vårt samhälle. Den svenska säkerhetspolitikens mål och

inriktning blir på så sätt avgörande även för den grundläggande inriktningen av Försvarsmaktens försvarsunderrättelseverksamhet och Försvarets radioanstalts uppgifter som underrättelseorgan (jfr. prop. 2001/02:158 s. 19, SOU 1999:37 s. 169ff.).

Det övergripande ansvaret för under vilka former underrättelseverksamheten skall bedrivas ankommer ytterst på statsmakterna. Det är regering och riksdag som anger riktlinjerna för verksamheten och som bevakar att inte rättsstatens krav åsidosätts. I de senaste försvarsbesluten har det framhållits att omvälvningarna i den internationella miljön under 1990-talet med det kalla krigets slut och ett slut på de tidigare stormaktsmotsättningarna har lett till omfattande förändringar i den säkerhetspolitiska omvärldssituationen. Även om risken för krig mellan stater numera framstår som avlägsen så har inte konflikter och kriser försvunnit ens från vårt närområde. Nya säkerhetshot har uppstått vilket medfört att det svenska säkerhetsbegreppet måst vidgas. Som nya säkerhetshot har bl.a. angivits terrorism, spridning av massförstörelsevapen (proliferation), internationell kriminalitet, migrationstryck, etniska och kulturella konflikter samt hot mot den tekniska infrastrukturen i form av bl.a. sabotage m.m. mot tele- och datasystem (jfr. prop. 2001/02:10 s. 242f. och prop. 2001/02:158 s. 17ff.).

Det nya säkerhetspolitiska läget och ett vidgat säkerhetsbegrepp har inneburit nya förutsättningar för den svenska försvarsunderrättelseverksamheten. Således behöver Sverige en underrättelseverksamhet som mer än tidigare är inriktad mot att ge underlag för att belysa en vidgad säkerhetspolitisk hotbild. Samtidigt måste en sammanvägning av militär och civil underrättelseinformation alltid ske för att det skall föreligga ett mera fullständigt underlag för beslut och åtgärder i ett vidgat säkerhetspolitiskt perspektiv. Krav ställs därför på samordning mellan myndigheterna inom försvarsunderrättelseverksamheten och andra myndigheter för att hantera en bredare säkerhetspolitisk bild (se bl.a. prop. 2001/02:10 s. 242ff.).

I det senaste försvarsbeslutet, som omfattar perioden 2002–2004, har regeringen som en följd av den internationella utvecklingen dragit fyra slutsatser rörande mål och inriktning för svensk säkerhetspolitik. En första slutsats är att den grundläggande positiva säkerhetspolitiska situationen består, men att andra säkerhetspolitiska hot t.ex. terroristhot, IT-relaterade hot och hot med nukleära, biologiska och kemiska stridsmedel måste kunna bemötas. Den andra är att det även i framtiden ligger i Sveriges intresse att delta, civilt och militärt, vid internationell krishantering

i samband med olika kriser och konflikter. Den tredje slutsatsen sammanhänger med den tekniska infrastrukturens fundamentala betydelse för medborgarnas livsbetingelser och ett fungerande samhälle. Hot mot tekniska infrastruktursystem kan få mycket allvarliga konsekvenser. Slutligen är den fjärde slutsatsen att totalförsvarets förmåga till anpassning är en fortsatt viktig del av försvarspolitiken (jfr. prop. 2001/02:10 s. 34ff och prop. 2001/02:158 s. 19).

I den senaste försvarsbeslutspropositionen (prop. 2001/02:10 s. 42ff. bet. 2001/02:FöU9) har regeringen förklarat vad de säkerhetspolitiska förhållandena och det vidgade säkerhetsbegreppet medför för konsekvenser för den militära underrättelsetjänsten samt vilka krav som kan ställas på den framtida försvarsunderrättelseverksamheten. I försvarsbeslutet anges att en viktig uppgift för den militära underrättelsetjänsten är att på grundval av i första hand militära och politiska indikationer i tid kunna ge statsmakterna och försvarsledningen en förvarning om krigshot. Denna grundläggande uppgift kvarstår trots den förändrade militära hotbilden. Den säkerhetspolitiska utvecklingen ställer enligt försvarsbeslutet nya krav på den militära underrättelsetjänsten i bl.a. följande hänseenden.

- Underrättelsetjänsten skall utvecklas mot att kunna möta anpassningsprincipens krav på att kunna ge tidig förvarning och för att skapa förutsättningar för en operativ förmåga hos de militära förbanden.
- Utvecklingen när det gäller massförstörelsevapen och deras vapenbärare skall ha fortsatt hög aktualitet och inom den vidgade hotbilden utgör terrorism och den organiserade brottsligheten ett viktigt område för underrättelsetjänst.
- Underrättelsefunktionen inom ramen för de internationella organisationernas krishanteringsförmåga bör utvecklas bl.a. genom en utvecklad skicklighet hos de svenska underrättelseorganen i att inhämta och analysera underrättelseinformation inför och i samband med internationella insatser.
- Underrättelseverksamheten skall inriktas mot att säkerställa statsmakternas behov av information och regeringens behov av beslutsunderlag för olika handlingsalternativ.
- Samarbetet och samordningen skall stärkas mellan myndigheterna inom den militära underrättelseverksamheten och andra myndigheter i syfte att utveckla förmågan att hantera en bredare hotbild och att stödja internationella insatser.

2.3.1 Underrättelseprocessen

Försvarsunderrättelseverksamhet definieras sammanfattningsvis som en process för att inhämta, bearbeta och delge information som skall utgöra underlag för bedömningar och beslut på olika nivåer bl.a. för ett framtida agerande. I en trängre militärt inriktad säkerhetspolitisk mening brukar underrättelseverksamhet beteckna den verksamhet som syftar till att kartlägga främmande makters militära och politiska förhållanden samt handlingsmöjligheter.

Underrättelseprocessen kan i grova drag delas in i fyra steg. Det första steget i underrättelseprocessen brukar anges som *planering och inriktning* av underrättelseverksamheten. En underrättelseplan görs upp av ledningen för underrättelsetjänsten som sedan uppdrar åt olika inhämtningsorgan att samla in behövlig information.

Inhämtningen är det andra steget i underrättelseprocessen. Den består i att öppen och hemlig information inhämtas från olika källor och med olika metoder. Den största informationsmängden finns i dag att hämta i olika öppna källor som är allmänt tillgängliga. Det kan då vara fråga om information som hämtas från press, television, facktidskrifter, officiella rapporter eller elektroniska databaser (t.ex. Internet) m.m. Detta kallas för OSINT (open source intelligence). Hemlig information hämtas i första hand in med tekniska hjälpmedel och då särskilt via signalspaning, s.k. SIGINT (signal intelligence), vilket är Försvarets radioanstalts huvuduppgift. Inhämtning sker även direkt via enskilda personer på såväl öppen som hemlig väg, HUMINT (human intelligence). Öppen inhämtning kan ske via t.ex. attachéer eller diplomater och hemlig inhämtning kan ske bl.a. i samarbete med andra länders underrättelsetjänster. En vanlig form av inhämtning är även den som sker vid kontakter med myndigheter och olika organisationer. Militära förband och enheter hämtar information genom bl.a. radarspaning samt fartygs- och flygspaning.

Nästa steg i underrättelseprocessen innebär att det sker en *bearbetning* av det inhämtade informationsmaterialet genom bl.a. översättning, redigering och dechiffrering samt *analys*, varigenom informationen värderas och förädlas till en fullständig underrättelseprodukt.

Det sista steget i underrättelseprocessen är *delgivning*, och innebär att det analyserade materialet presenteras för uppdragsgivaren eller annan som bedöms ha behov av att ta del av den färdigbearbetade underrättelsen.

2.4 Författningsreglering av försvarsunderrättelseverksamhet

Försvarsunderrättelseverksamhetens uppgifter och arbetsformer regleras i lagen (2000:130) om försvarsunderrättelseverksamhet. Lagen anger att försvarsunderrättelseverksamhet skall bedrivas för att kartlägga yttre militära hot mot landet och till stöd för svensk utrikes-, försvars- och säkerhetspolitik. I verksamheten ingår att medverka i svenskt deltagande i internationellt säkerhetssamarbete och att, enligt vad regeringen närmare bestämmer, medverka med underrättelser för att stärka samhället vid svåra påfrestningar på samhället i fred. Lagen anger även att regeringen skall bestämma försvarsunderrättelseverksamhetens inriktning. I anslutning till lagen har regeringen beslutat förordningen (2000:131) om försvarsunderrättelseverksamhet. Författningsregleringen är ett led i en strävan att så långt det är möjligt öppet redovisa verksamheten hos de myndigheter som bedriver försvarsunderrättelseverksamhet.

Den militära underrättelsetjänsten i Sverige sysslar med rikets yttre säkerhet och har inte sådana uppgifter som enligt regeringsformen fordrar lagform. Det har ändå ansetts viktigt i ett demokratiskt samhälle att en sådan betydelsefull och ofta uppmärksammad verksamhet som försvarsunderrättelseverksamheten är reglerad i lag samt att riksdagen lägger fast ramarna för denna underrättelseverksamhet och anger dess huvudsakliga uppgifter och arbetsformer.

Underrättelseverksamheten är av sådan art att det av naturliga skäl inte är möjligt att i lagform reglera den i detalj. Samtidigt framhålls i förarbetena att en lagreglering inte innebär någon förändring vad gäller regeringens konstitutionella möjligheter att styra försvarsunderrättelseverksamheten. Informella kontakter mellan regeringen eller företrädare för Regeringskansliet och tjänstemän hos myndigheterna är viktiga och nödvändiga inslag i regeringens relationer till myndigheterna.

För att ge nödvändigt utrymme för de informella kontakter som behövs på underrättelseområdet och för att förstärka samordningen av underrättelseverksamheten lämnade Underrättelsekommittén i sitt betänkande Underrättelsetjänsten – en översyn (SOU 1999:37) förslag om att inrätta en samordnande funktion i Regeringskansliet för kontinuerlig inriktning av försvarsunderrättelseverksamheten. Regeringen har som en följd härav låtit inrätta ett särskilt organ bestående av en beredningsgrupp på statssekreterarnivå och ett samordningssekretariat i Regerings-

kansliet (prop. 1999/2000:25 s. 12f.). Detta har skett genom etablerandet av en styrgrupp för säkerhetspolitiska underrättelsefrågor. I styrgruppen ingår en departementsöverskridande sammansättning av representanter på statssekreterarnivå samt överbefälhavaren och cheferna för den militära underrättelse- och säkerhetstjänsten, Försvarets radioanstalt och Säkerhetspolisen. Styrgruppen stöds av ett sekretariat inom Regeringskansliet, Samordningssekretariatet för säkerhetspolitiska underrättelsefrågor i Regeringskansliet (SUND), vilket är placerat hos Försvarsdepartementet. Sekretariatet har till uppgift att löpande följa underrättelseverksamheten, att bedöma underrättelseunderlaget samt att bidra till en sammanvägd syn på hot mot landets yttre säkerhet och intressen. Sekretariatet skall verka för att regelbundet samråd äger rum mellan underrättelsetjänsterna och Regeringskansliet och att en adekvat delgivning av material sker. Sekretariatet skall informera Försvarets underrättelsenämnd om sin verksamhet när det gäller frågor som rör försvarsunderrättelseverksamhet (se prop. 2001/02:10 s. 244).

2.4.1 Lagen om försvarsunderrättelseverksamhet

Lagen om försvarsunderrättelseverksamhet tar sikte på uppgifter och arbetsformer för de myndigheter, som regeringen enligt lagen skall utse för att bedriva sådan verksamhet. I lagen anges att försvarsunderrättelseverksamhet skall bedrivas för att kartlägga yttre militära hot mot landet och till stöd för svensk utrikes-, försvars- och säkerhetspolitik. Begreppet försvarsunderrättelseverksamhet tar inte enbart sikte på underrättelseverksamhet till stöd för det militära försvaret och svensk utrikes-, försvars- och säkerhetspolitik. Begreppet täcker även sådan verksamhet som har samband med internationellt säkerhetssamarbete eller som syftar till att stärka samhället vid svåra påfrestningar (se prop. 1999/2000:25 s. 7).

Verksamheten får inte avse uppgifter som enligt lag eller andra föreskrifter ligger inom ramen för polisens och andra myndigheters brottsbekämpande och brottsförebyggande arbete. Vidare anges att det i verksamheten ingår att medverka i svenskt deltagande i internationellt säkerhetssamarbete och att, enligt vad regeringen närmare bestämmer, medverka med underrättelser för att stärka samhället vid svåra påfrestningar i fredstid.

Det har i förarbetena till lagen betonats att förändringarna i omvärlden avsevärt har påverkat uppgifterna för den tidigare militärt inriktade underrättelsetjänsten. Det framhålls att nya säkerhetshot har efterträtt tidigare militära angreppshot mot landet och vårt närområde. Dessa hot har uppstått i form av migrationstryck, politisk och social instabilitet och påfrestningar på det ekologiska systemet. Härtill kommer risk för spridning av massförstörelsevapen, terrorism, etniska och kulturella konflikter m.m. Det har också i olika sammanhang framhållits att en helhetssyn skall prägla samhällets satsningar och åtgärder för att förebygga och hantera hot och risker i såväl fred som krig och att underrättelsefunktionen här har en viktig uppgift (jfr. bl.a. prop. 1995/96:12 s. 30f. och 45ff.). Ansvaret för åtgärder mot nya säkerhetshot, som inte bedöms utgöra någon direkt fara för landet, ligger på olika civila statliga och kommunala myndigheter. Enligt förarbetena till lagen bör emellertid den militära underrättelsetjänsten inom ramen för olika uppdrag kunna stödja dessa myndigheter med inhämtning och analys av information i särskilda fall (se SOU 1999:37 s. 239ff. och prop. 1999/2000:25 s. 6 och 14).

Verksamhetens inriktning och arbetsmetoder

Regeringen ansvarar enligt lagen om försvarsunderrättelseverksamhet för den närmare inriktningen av verksamheten som skall bedrivas av Försvarsmakten och de andra myndigheter som regeringen bestämmer. Uppgiften att bedriva underrättelseverksamhet skall fullgöras genom inhämtning, bearbetning och analys av information. Mot denna bakgrund skall det enligt lagen utarbetas hotbildsanalyser och underrättelsebedömningar i underrättelsefrågor som skall rapporteras till Regeringskansliet och andra berörda myndigheter (se prop. 1999/2000:25 s. 15f.).

I förarbetena till lagen läggs fast vilka övergripande arbetsmetoder som skall användas i försvarsunderrättelseverksamheten. Enligt regeringen består försvarsunderrättelseprocessen i stora drag av inhämtning, bearbetning och analys samt delgivning av information. Analyser av hotbilder och bedömningar i underrättelsefrågor skall rapporteras till Regeringskansliet och andra berörda myndigheter.

I lagen föreskrivs vidare att de myndigheter som skall bedriva försvarsunderrättelseverksamhet får, enligt regeringens närmare bestämmande, etablera och upprätthålla samarbete i underrättelse-

frågor med andra länder och internationella organisationer. I begreppet samarbete innefattas utbyte av underrättelseinformation. Sådant utbyte får dock endast ske under förutsättning att syftet är att tjäna statsledningen och det svenska totalförsvaret samt att lämnade uppgifter inte är till skada för svenska intressen. Frågan om underrättelsesamarbete är inom regeringen i första hand en uppgift för försvarsministern. Utrikesministern skall hållas underrättad.

Försvarsunderrättelseverksamhetens fyra grundprinciper

I förarbetena till lagen läggs fyra grundprinciper fast som skall gälla för försvarsunderrättelseverksamhet. Försvarsunderrättelseverksamheten skall enligt den första principen bedrivas i enlighet med *statsmakternas utrikes-, försvars- och säkerhetspolitiska intentioner.* Verksamheten får styras endast av Sveriges egna behov och prioriteringar. Härvid skall dock även hänsyn tas till den ökade vikt som statsmakterna fäster vid det internationella säkerhetssamarbetet i form av stöd till och deltagande i säkerhetsfrämjande samarbete och fredsfrämjande och humanitära insatser och de särskilda krav på underrättelseverksamheten som detta ställer.

Försvarsunderrättelseverksamhet får enligt den andra principen uteslutande avse underrättelser av betydelse för *rikets yttre säkerhet* och för det *internationella säkerhetssamarbetet* i form av svenskt stöd till och deltagande i säkerhetsfrämjande samarbete samt i fredsfrämjande och humanitära insatser. Den får inte avse uppgifter som ligger inom ramen för polisens och andra myndigheters brottsbekämpande och brottsförebyggande arbete.

Försvarsunderrättelseverksamhet skall enligt den tredje principen *tjäna endast vårt lands säkerhetspolitiska intressen* och får därmed inte bedrivas på uppdrag av någon annan stat och andra staters intressen får inte gå före Sveriges egna.

Försvarsunderrättelseverksamhetens *utbyte av information* med utländska underrättelse- och säkerhetstjänster får enligt princip fyra ske endast under förutsättning att syftet är att *tjäna statsledningen och det svenska totalförsvaret* samt att lämnade uppgifter *inte är till skada för svenska intressen*. I sammanhanget erinras om den begränsning i fråga om utlämnande av uppgifter som de svenska bestämmelserna om sekretess och personuppgifter kan innebära.

Myndigheter som skall bedriva försvarsunderrättelseverksamhet

I lagen anges att försvarsunderrättelseverksamhet skall bedrivas av Försvarsmakten och de andra myndigheter som regeringen bestämmer. I förordningen om försvarsunderrättelseverksamhet anges att verksamheten skall bedrivas förutom av Försvarsmakten även av Försvarets radioanstalt, Försvarets materielverk (FMV) och Totalförsvarets forskningsinstitut (FOI). De myndigheter som bedriver försvarsunderrättelseverksamhet får också samarbeta i underrättelsefrågor med andra länder och internationella organisationer. Sådant samarbete får dock endast ske om syftet är att tjäna den svenska statsledningen och det svenska totalförsvaret samt att lämnade uppgifter inte är till skada för svenska intressen.

Information och samverkan

I förordningen om försvarsunderrättelseverksamhet finns vidare ett antal bestämmelser om skyldigheten för de myndigheter som bedriver försvarsunderrättelseverksamhet att i olika avseenden lämna information i frågor som rör verksamheten eller att samverka i sådana frågor. Till Regeringskansliet (Försvarsdepartementet) skall anmälas frågor om samarbete i underrättelsefrågor med andra länder. Myndigheterna skall vidare samverka med SUND när det gäller försvarsunderrättelseverksamhet. Vidare skall Försvarets underrättelsenämnd informeras om bl.a. samarbetet med andra länder.

Försvarsunderrättelseverksamheten får inte avse uppgifter som ligger inom ramen för polisens och andra myndigheters brottsbekämpande och brottsförebyggande arbete. Denna bestämmelse syftar emellertid inte till att utgöra ett hinder mot att myndigheter som sysslar med försvarsunderrättelseverksamhet skall, enligt regeringens bestämmande, kunna lämna andra myndigheter biträde och syssla med uppdragsverksamhet för annan myndighets räkning.

Insyn

Försvarets underrättelsenämnd har till uppgift att följa underrättelsetjänsten inom Försvarsmakten och Försvarets radioanstalt samt de övriga myndigheter som bedriver försvarsunderrättelseverksamhet.

2.5 Militär säkerhetstjänst

Den militära säkerhetstjänstens uppgift är att upptäcka, identifiera och möta säkerhetshot som riktas mot Försvarsmakten och dess intressen såväl inom som utom landet. Säkerhetstjänsten är en del av Försvarsmaktens grundberedskap och skall fungera fullt ut i fred och vara anpassad efter krav och behov.

Den säkerhetshotande verksamhet som riktas mot Försvarsmakten brukar delas in i underrättelseverksamhet, kriminalitet, sabotage, subversion samt terrorism. Den säkerhetshotande verksamheten kan riktas mot hela eller delar av Försvarsmakten, viss funktion eller verksamhet, förband eller enskilda samt verksamhet inom Försvarsmaktens intresseområde, t.ex. försvarsindustri.

Underrättelseverksamhet riktad mot Försvarsmakten kan bedrivas av såväl främmande makt som olika organisationer, företag och kriminella personer. Främmande makts underrättelseverksamhet kan ske på svenskt territorium, utanför landet eller riktas mot Försvarsmakten i samband med internationell verksamhet eller uppträdande utomlands i andra sammanhang. Den *kriminalitet* som riktas mot Försvarsmakten utgörs främst av tillgreppsbrott, andra förmögenhetsbrott och skadegörelse. Med *sabotage* avses i detta sammanhang avsiktlig skadegörelse eller förstörelse av Försvarsmaktens materiel, anläggningar eller lokaler samt samhällsviktiga installationer för t.ex. kommunikation och försörjning. *Subversion* innebär att utan att tillgripa öppet eller direkt våld söka omstörta eller påverka statsskicket. Under subversion faller t.ex. infiltration. Med *terrorism* avses i regel organiserat våld, med politiskt eller religiöst syfte.

2.5.1 Den militära säkerhetstjänstens uppgifter

Enligt 4 § 2. förordningen (2000:555) med instruktion för Försvarsmakten åligger det Försvarsmakten att leda och bedriva militär säkerhetstjänst. Huvudansvaret för den militära säkerhetstjänsten ligger organisatoriskt på säkerhetsavdelningen inom den militära underrättelse- och säkerhetstjänsten (MUST) vid Försvarsmaktens högkvarter.

Den militära säkerhetstjänstens uppgift är att tillvarata säkerhetsintressen som berör Försvarsmakten, genom att upptäcka, förebygga och avvärja aktuella säkerhetshot. Häri ingår bl.a. att

biträda polisen i dess ansvar beträffande skyddet av rikets säkerhet. Försvarsmaktens säkerhetsintressen kan hänföras till personal, materiel, anläggningar, information samt planering och planer i vid bemärkelse.

Säkerhetstjänsten omfattar tre huvudområden: säkerhetsunderrättelsetjänst, säkerhetsskyddstjänst och signalskyddstjänst.

Säkerhetsunderrättelsetjänst

Säkerhetsunderrättelsetjänsten skall klarlägga den säkerhetshotande verksamheten som kan komma att riktas mot Försvarsmakten och dess intressen, såväl inom som utom landet. Säkerhetsunderrättelsetjänstens syfte är att utifrån aktuella säkerhetsunderrättelsebehov lämna underlag för beslut om t.ex. säkerhetsskyddsåtgärder, beredskap eller förbandsproduktion.

Inom säkerhetsunderrättelsetjänsten används samma arbetsform som inom underrättelsetjänsten. Säkerhetsunderrättelsetjänsten måste emellertid ibland genomföras med särskilda krav på säkerhetsskydd. I vissa fall är det oundgängligen nödvändigt att kunskap om vissa förhållanden är förbehållen en mycket liten krets av personer eller att t.ex. bearbetning av säkerhetsunderrättelser sker under särskilda förutsättningar avseende arbetsplats, datorstöd etc.

Inhämtning av säkerhetsunderrättelser sker genom utnyttjande av samma typ av källor som används av underrättelsetjänsten i övrigt. Härutöver inhämtas information genom t.ex. utfrågning i samband med fall av säkerhetshotande verksamhet och via uppgiftslämnare eller i samverkan med andra myndigheter.

Säkerhetsskyddstjänst

Säkerhetsskyddstjänstens uppgift är att ta fram åtgärder som syftar till att hindra eller försvåra säkerhetshotande verksamhet. Den arbetar med att förebygga att hemliga uppgifter som rör rikets säkerhet obehörigen röjs, ändras eller förstörs. Säkerhetsskyddstjänsten skyddar också materiel och anläggningar mot sabotage och stöld samt personal, anläggningar och materiel mot terrorism. Inom säkerhetsskyddstjänsten arbetar man med informationssäkerhet, infiltrationsskydd, tillträdesbegränsning, utbildning och kontroll av säkerhetsskyddet.

Informationssäkerhet skall förebygga att uppgifter som omfattas av sekretess och som rör rikets säkerhet obehörigen röjs, ändras eller förstörs. IT-säkerhet ingår som en viktig del i informationssäkerheten.

Infiltrationsskydd i form av säkerhetsprövning skall förebygga att personer som inte är pålitliga från säkerhetssynpunkt deltar i verksamhet som har betydelse för rikets säkerhet.

Tillträdesbegränsning skall hindra att obehöriga får tillträde till anläggningar, inrättningar, fordon, fartyg, luftfartyg samt andra föremål eller områden, där hemlig uppgift eller annat av betydelse för rikets säkerhet förvaras, eller där verksamhet av sådan betydelse förekommer.

Utbildning ingår som en del i grund- och vidareutbildning av militär personal. Dessutom sker specialutbildning för den personal som har särskilt ansvar för underrättelse- och säkerhetstjänst.

Säkerhetsskyddet skall enligt Försvarsmaktens föreskrifter främst bedrivas i linjeorganisationen och angår härvid all personal som är inblandad i den skyddsvärda verksamheten. Förbandschef eller annan chef är alltid ansvarig för säkerhetsskyddet inom sitt område eller sin verksamhet. Kontroll syftar till att konstatera om säkerhetsskyddsnivån är anpassad till aktuell hotbild och att reglerna för säkerhetsskyddet följs.

Signalskyddstjänst

Försvarsmakten skall leda och samordna signalskyddstjänsten inom hela totalförsvaret. Inom Försvarsmakten är det totalförsvarets signalskyddssamordning (TSA) som utför dessa uppgifter. TSA är organisatoriskt en sektion inom MUST:s avdelning för IT-säkerhet.

Signalskyddstjänsten syftar till att minska verkan av signalspaning, falsk signalering och störsändning mot totalförsvarets telekommunikations- och informationssystem. Den skall förhindra obehörig insyn i och påverkan av totalförsvarets telekommunikationer, samt användning av kryptografiska funktioner i informationssystemen. Signalkontroll avser också kontroll av röjande signaler (RÖS) samt att systemen används enligt gällande regler. Signalkontrollen har till syfte att dels ge en bild av vad främmande signalspaning kan ha uppfattat av befordrad information, dels att kontrollera att totalförsvarets signalskyddssystem (kryptofunktioner) används och fungerar på önskat sätt. Resultatet från en

signalkontroll utnyttjas i första hand för att förbättra rutinerna vid meddelandeväxling.

Signalkontroll kan genomföras med avseende på såväl ett radiobefordrat meddelande som ett meddelande som förmedlas via tråd. Kontrollen kan även avse annan informationsöverföring än tal. Signalkontroll kan avse såväl innehållet i ett signalmeddelande som att klarlägga om signalering över huvud taget förekommer eller att konstatera om en utrustning avger röjande signaler. Vidare skall signalkontrollen ge underlag för bedömning av vilka uppgifter som kan ha röjts för obehörig och som rör något förhållande som omfattas av sekretess.

Signalkontroll innebär att underlag inhämtas främst genom avlyssning av analog och digital signalering i telekommunikations- och informationssystem. De inhämtade underlagen granskas och bearbetas, varefter gjorda iakttagelser delges och rapporteras. Signalkontroll genomförs i totalförsvarets telekommunikations- och informationssystem stickprovsvis med hjälp av fasta eller rörliga kontrollorgan. Signalkontroll genomförs dels med avseende på verksamhet som kräver ett högt eller långvarigt skydd mot att sekretessbelagda uppgifter röjs, dels vid t.ex. större försvarsmaktsövningar och internationell verksamhet där svenska förband deltar.

Vid en signalkontroll kan det framkomma att en person – ofta en anställd i Försvarsmakten – i ett meddelande som inte är skyddat av krypteringsfunktioner röjer en uppgift som omfattas av sekretess. I några sådana fall har det lett till att rättsliga åtgärder har vidtagits mot den som röjt uppgiften. Det har även förekommit att Försvarsmaktens personal har gripit in i ett samtal och förhindrat att ytterligare sekretessbelagd information har röjts. Signalkontroll sker aldrig i form av hemlig avlyssning. Någon av parterna i t.ex. ett telefonsamtal är alltid medveten om att avlyssning kan förekomma.

Försvarsmakten har i Försvarets författningssamling (FFS 1999:11) meddelat särskilda föreskrifter om signalskyddstjänsten inom totalförsvaret.

2.6 Författningsreglering av säkerhetsskyddet inom Försvarsmakten

Den militära säkerhetstjänsten styrs av ett omfattande regelverk. Den grundläggande lagstiftningen utgörs av tryckfrihetsförordningen, där de intressen som får skyddas genom att allmänna

handlingar hålls hemliga anges. Så får t.ex. enligt 2 kap. 2 § tryckfrihetsförordningen ske med hänsyn till rikets säkerhet eller dess förhållande till annan stat eller mellanfolklig organisation. Begränsning av rätten att ta del av allmänna handlingar skall enligt tryckfrihetsförordningen anges noga i särskild lag, vilket sker i sekretesslagen (1980:100). Genom sekretesslagens bestämmelser om tystnadsplikt och förbud att lämna ut allmänna handlingar föreskrivs en skyldighet för myndigheten att hemlighålla vissa uppgifter. Vidare kan regeringen enligt vad som anges i sekretesslagen utfärda närmare föreskrifter om hur en sekretessbestämmelse skall tillämpas.

För den sekretess som gäller för att trygga rikets säkerhet har det ansetts nödvändigt med särskilda säkerhetsskyddsåtgärder. Detta regleras i säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordningen (1996:633). I säkerhetsskyddslagen finns bestämmelser som rör säkerhetsskydd och registerkontroll samt särskild personutredning. Med säkerhetsskydd avses olika åtgärder för att skydda totalförsvaret och rikets säkerhet i övrigt. Registerkontroll med särskild personutredning innebär ett inhämtande av upplysningar ur olika register beträffande den som innehar eller avses tillträda en sådan tjänst hos en myndighet som är av betydelse för totalförsvaret eller rikets säkerhet i övrigt. Enligt 44 § säkerhetsskyddsförordningen har Försvarsmakten bemyndigats att meddela föreskrifter om verkställigheten av säkerhetsskyddslagen för sina respektive tillsynsområden. Försvarsmakten har i enlighet härmed beslutat Försvarsmaktens föreskrifter (FFS 1999:10) om säkerhetsskydd. Dessa föreskrifter kompletteras slutligen med interna bestämmelser och särskilda handböcker.

2.6.1 Säkerhetsskyddslagen

I säkerhetsskyddslagen finns, som nämnts, bestämmelser som rör säkerhetsskydd och registerkontroll. Säkerhetsskyddslagen gäller vid verksamhet hos staten, kommunerna och landstingen. Lagen gäller också verksamhet hos aktiebolag, handelsbolag, föreningar och stiftelser över vilka staten, kommuner eller landsting utövar ett rättsligt bestämmande inflytande, och enskilda, om verksamheten är av betydelse för rikets säkerhet eller särskilt behöver skyddas mot terrorism.

I verksamhet där lagen gäller skall det finnas det säkerhetsskydd som behövs med hänsyn till verksamhetens art, omfattning och övriga omständigheter. Säkerhetsskyddet skall utformas med beaktande av enskildas rätt att enligt tryckfrihetsförordningen ta del av allmänna handlingar.

Vilken nivå skyddet skall ligga på kan enligt förarbetena (se prop. 1995/96:129) inte bestämmas allt för precist i lagen. Övervägandena i frågan om säkerhetsskyddets utformning i en verksamhet där man regelmässigt handlägger frågor av mycket känslig natur måste skilja sig från dem i en verksamhet där man mer tillfälligt kommer i kontakt med sådana frågor. För att ge utrymme åt olika hänsynstaganden anges endast att säkerhetsskyddet i det enskilda fallet skall ha den utformning som krävs med hänsyn till verksamhetens art, omfattning och övriga omständigheter. Mer detaljerade bestämmelser kan meddelas genom tillämpningsföreskrifter.

Med säkerhetsskydd avses olika åtgärder för att skydda rikets säkerhet. Med rikets säkerhet avses såväl den yttre säkerheten för det nationella oberoendet som den inre säkerheten för det demokratiska statsskicket. Skyddet för den yttre säkerheten tar i första hand sikte på totalförsvaret. Ett hot mot rikets yttre säkerhet kan dock förekomma även om det inte utgör ett hot mot totalförsvaret. Sammanfattningsvis avses med säkerhetsskydd skydd mot spionerі, sabotage och andra brott som kan hota rikets säkerhet, skydd i andra fall av uppgifter som omfattas av sekretess enligt sekretesslagen (1980:100) och som rör rikets säkerhet, och skydd mot brott som innebär användning av våld, hot eller tvång för politiska syften (terrorism), även om brotten inte hotar rikets säkerhet (se prop. 1995/96:129 s. 22ff.).

För att uppfylla syftet med säkerhetsskyddslagen skall de myndigheter m.fl. som omfattas av lagen vidta vissa säkerhetsskyddsåtgärder. Dessa åtgärder benämns i lagen informationssäkerhet, tillträdesbegränsning samt säkerhetsprövning.

Informationssäkerhet (7 § 1. och 9 §)

Med informationssäkerhet avses skydd mot att uppgifter som omfattas av sekretess och som rör rikets säkerhet obehörigen röjs, ändras eller förstörs vare sig det sker uppsåtligen eller av oaktsamhet. Vid utformningen av informationssäkerheten skall behovet av skydd vid automatisk informationsbehandling beaktas

särskilt. Härmed avses såväl att datasäkerheten är hög som att telefonförbindelser och andra kommunikationsvägar håller en tillräckligt hög nivå från säkerhetssynpunkt.

För en tillfredsställande informationssäkerhet bör enligt regeringen vidare krävas att handlingar med sekretessbelagda uppgifter förvaras på ett betryggande sätt och att man fortlöpande kontrollerar att handlingarna finns i behåll (se prop. 1995/96:129 s. 75).

Tillträdesbegränsning (7 § 2. och 10 §)

Tillträdesbegränsning innebär att obehöriga inte får tillträde till platser där de kan få tillgång till uppgifter som omfattas av sekretess och som rör rikets säkerhet eller där verksamhet som har betydelse för rikets säkerhet bedrivs. Konkret innebär bestämmelsen en skyldighet att överväga behovet av inre och yttre bevakning genom vaktpersonal eller andra hjälpmedel som TV-övervakning och larmanordningar.

Tillträdesbegränsningar skall enligt förarbetena till lagen utformas så att den enskildes rätt att röra sig fritt inte inskränks mer än nödvändigt. Allmänhetens rätt att övervara offentliga förhandlingar och värdet av den öppenhet som präglar svensk förvaltning bör också beaktas vid valet av åtgärder. I 5 § säkerhetsskyddslagen anges att säkerhetsskyddet skall utformas med beaktande av enskildas rätt att enligt tryckfrihetsförordningen ta del av allmänna handlingar. En noggrann avvägning måste ske så att eventuella begränsningar inte blir onödigt ingripande.

Säkerhetsprövning (7 § 3.)

Säkerhetsprövning avser kontroll av en person i syfte att förhindra att någon som inte är pålitlig från säkerhetssynpunkt kommer att delta i verksamhet som har betydelse för rikets säkerhet. Säkerhetsprövningen skall i vissa fall omfatta registerkontroll och särskild personutredning (se prop. 1995/96:129 s. 38ff.).

En säkerhetsprövning skall göras avseende alla som skall delta i verksamhet som har betydelse för rikets säkerhet eller för sysslor som är viktiga vid bevakandet av skyddet mot terrorism. Pålitlighetsprövningen skall inte bara innefatta en bedömning av om det kan finnas risk för att personen i fråga kan göra sig skyldig till spioneri eller dylikt. Prövningen skall också innehålla en bedöm-

ning av om det är lämpligt att personen anförtros sekretessbelagda uppgifter. Härvid skall beaktas bl.a. risken för att han eller hon blir utsatt för olika påtryckningar, att han eller hon genom slarv eller på annat oavsiktligt sätt röjer de sekretessbelagda uppgifterna. Säkerhetsprövningen är knuten till de krav som befattningen eller verksamheten ställer i det enskilda fallet och inte till person.

I de mer kvalificerade fallen innefattar säkerhetsprövningen en *registerkontroll*, dvs. en kontroll i polisens register. Syftet med registerkontrollen är att skaffa fram ett underlag för bedömningen av om en person bör anförtros uppgifter av säkerhetskänslig karaktär.

Med registerkontroll avses att uppgifter hämtas från ett register som omfattas av lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister eller polisdatalagen (1998:622). Med registerkontroll avses också att sådana personuppgifter hämtas som Rikspolisstyrelsen eller Säkerhetspolisen behandlar utan att det ingår i ett sådant register som avses i de nämnda lagarna.

Med utgångspunkt i vilka följder ett eventuellt röjande av sekretessbelagda uppgifter får för rikets säkerhet i det konkreta fallet delas olika anställningar in i tre säkerhetsklasser. En anställning eller annat sådant deltagande i verksamhet som skall bli föremål för registerkontroll placeras i säkerhetsklass, om den anställde eller den som deltar i verksamheten får del av uppgifter som omfattas av sekretess och är av betydelse för rikets säkerhet.

I *säkerhetsklass 1* är sådan verksamhet placerad där den anställde i stor omfattning får del av uppgifter som omfattas av sekretess och är av synnerlig betydelse för rikets säkerhet.

Säkerhetsklass 2 omfattar sådan verksamhet där den anställde i en omfattning som inte är obetydlig får del av uppgifter som omfattas av sekretess och är av synnerlig betydelse för rikets säkerhet.

I *säkerhetsklass 3* är sådan verksamhet placerad där den anställde i övrigt får del av uppgifter som omfattas av sekretess och som är av betydelse för rikets säkerhet, om ett röjande av uppgifterna kan antas medföra men för rikets säkerhet som inte endast är ringa.

Säkerhetsskyddet omfattar också ett skydd mot terrorism, oavsett om denna hotar rikets säkerhet eller inte. Registerkontroll skall därför även göras om det behövs för skyddet mot terrorism. Registerkontrollen till skydd mot terrorism är inte knuten till säkerhetsklasser. Registerkontroll i detta syfte får endast ske om det finns särskilda skäl. Föreskrifter om detta meddelas av regeringen.

Den som säkerhetsprövningen gäller skall ha gett sitt *samtycke* innan registerkontroll och särskild personutredning får göras. Syftet med denna bestämmelse är att den som avses bli kontrollerad skall ha möjlighet att återkalla sin ansökan om anställning, om han eller hon har anledning att befara att ofördelaktiga uppgifter om honom eller henne skulle komma fram vid registerkontrollen. Samtycket bör normalt lämnas skriftligen. Något uttryckligt krav på skriftlig form föreligger dock inte. Ett lämnat samtycke skall anses innefatta ett godkännande av förnyade registerkontroller så länge den kontrollerade avses ha samma anställning.

Särskild personutredning (18 §)

Om registerkontrollen avser en anställning eller annat deltagande i verksamhet som har placerats i säkerhetsklass 1 eller 2 skall en särskild personutredning göras. Detta gäller också när en framställan om registerkontroll har gjorts av en annan stat eller mellanfolklig organisation. Personutredningen skall omfatta en undersökning av den kontrollerades ekonomiska förhållanden och i övrigt ha den omfattning som behövs.

Säkerhetsskyddsavtal (8 §)

När staten avser att begära in anbud eller träffa avtal om upphandling där det förekommer uppgifter som med hänsyn till rikets säkerhet omfattas av sekretess, skall staten träffa ett skriftligt avtal, säkerhetsskyddsavtal, med anbudsgivaren eller leverantören om det säkerhetsskydd som behövs i det särskilda fallet. Detsamma gäller för kommuner och landsting.

Tillsyn och föreskrifter om verkställighet

Den som regeringen bestämmer skall kontrollera säkerhetsskyddet hos myndigheter och andra som lagen gäller för samt hos anbudsgivare och leverantörer som har träffat ett s.k. säkerhetsskyddsavtal. Därutöver skall staten, kommuner och landsting se till att det finns ett tillfredsställande säkerhetsskydd hos aktiebolag, handelsbolag, föreningar och stiftelser över vilka de utövar ett rättsligt bestämmande inflytande samt hos anbudsgivare och leverantörer med vilka de har träffat ett säkerhetsskyddsavtal.

Enligt 39 § första punkten säkerhetsskyddsförordningen (1996:633) skall Försvarsmakten kontrollera säkerhetsskyddet när det gäller Fortifikationsverket samt de myndigheter som hör till Försvarsdepartementet utom Kustbevakningen, Krisberedskapsmyndigheten, Statens räddningsverk och Styrelsen för psykologiskt försvar.

Regeringen eller den myndighet som regeringen utser meddelar de närmare föreskrifter som behövs för lagens tillämpning.

Enligt 44 § säkerhetsskyddsförordningen får Försvarsmakten meddela ytterligare föreskrifter om verkställigheten av säkerhetsskyddslagen inom myndighetens tillsynsområde.

Registernämnden

Registernämnden har inrättats för att som särskild myndighet handlägga frågor om utlämnande av uppgifter från polisens register. Enligt 1 § i förordningen (1996:730) med instruktion för registernämnden har nämnden till uppgift att i ärenden om registerkontroll enligt säkerhetsskyddslagen pröva frågor om utlämnande av

1. uppgifter från register som omfattas av lagen (1998:620) om belastningsregister,
2. uppgifter från register som omfattas av lagen (1998:621) om misstankeregister,
3. uppgifter från register som omfattas av polisdatalagen (1998:622), eller
4. övriga uppgifter som Rikspolisstyrelsen eller Säkerhetspolisen behandlar enligt polisdatalagen om de inte ingår i en förundersökning eller särskild undersökning i kriminalunderrättelseverksamhet.

Nämnden skall pröva frågor om utlämnande av uppgifter även i sådana fall som avses i 10 § förordningen (1998:149) om bevakningsföretag m.m.

Nämnden skall vidare granska Säkerhetspolisens behandling av personuppgifter enligt polisdatalagen (1998:622), särskilt med avseende på 5 § polisdatalagen, som avser behandling av känsliga personuppgifter.

Avsikten med införandet av Registernämnden är att stärka den parlamentariska och medborgerliga insynen i Säkerhetspolisens verksamhet. Detta ansågs vara av största betydelse när det gäller rättssäkerheten och skyddet för den personliga integriteten i ärenden om säkerhetskontroll.

3 Försvarets radioanstalts underrättelseverksamhet

Försvarets radioanstalt, som bildades år 1942, är en central civil förvaltningsmyndighet under Försvarsdepartementet. Försvarets radioanstalts huvuduppgift enligt de beslut och direktiv som statsmakterna givit myndigheten är att bedriva försvarsunderrättelseverksamhet i form av signalspaning. Härigenom skall myndigheten kartlägga yttre militära hot mot landet och bidra med underrättelser till stöd för svensk utrikes-, försvars- och säkerhetspolitik. Till huvuduppgiften hör också att genom signalspaningsverksamhet medverka i svenskt deltagande i internationellt säkerhetssamarbete och att bidra med underrättelser för att stärka samhället vid svåra påfrestningar i fred. Försvarets radioanstalt skall i övrigt bedriva signalspaning enligt den inriktning som regeringen, Försvarsmakten och övriga uppdragsgivare ger.

Försvarets radioanstalts verksamhet inriktas genom försvarsbeslut och de uppgifter som Försvarets radioanstalt har genom bestämmelserna i lagen (2000:130) om försvarsunderrättelseverksamhet och förordningen (2000:131) om sådan verksamhet. Mer i detalj inriktas verksamheten dels genom förordningen (1994:714) med instruktion för Försvarets radioanstalt och genom det årliga regleringsbrevet för myndigheten, dels genom den inriktningen som regeringen, Försvarsmakten och övriga uppdragsgivare anger genom olika uppdrag.

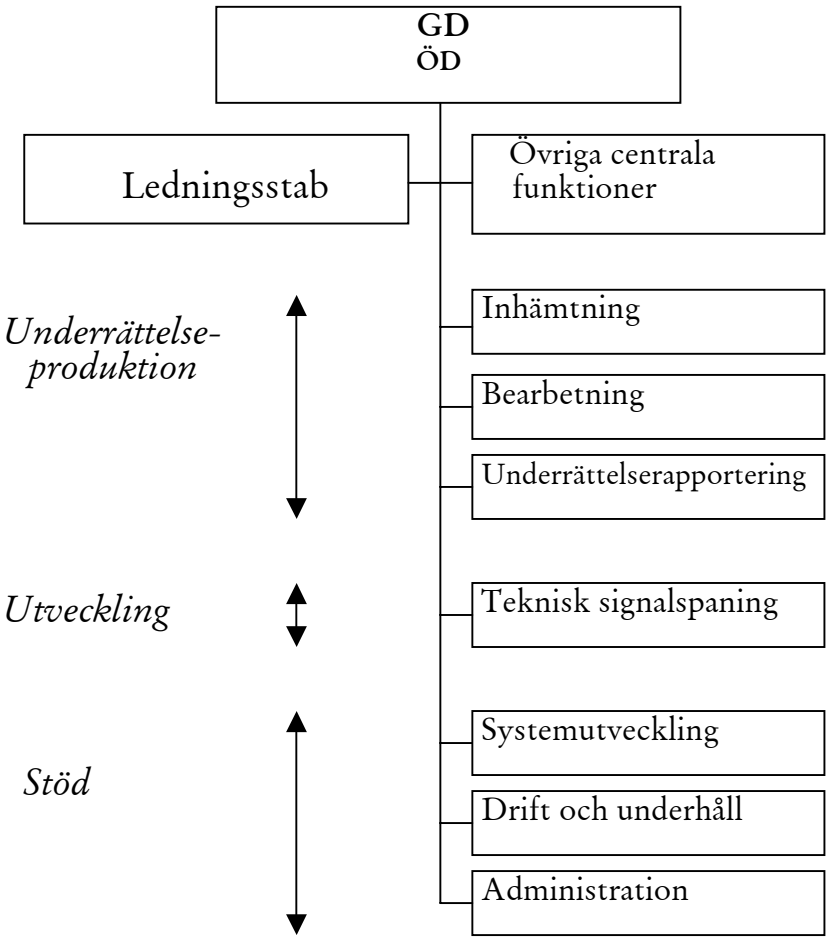
I Försvarets radioanstalts underrättelseverksamhet gäller för myndigheten vad som beskrivits i föregående kapitel om försvarsunderrättelseverksamhet. Försvarets radioanstalts huvuduppgift och verksamhet såsom försvarsunderrättelseorgan tar emellertid sikte på underrättelseverksamhet i en mer allmän säkerhetspolitisk mening. Myndigheten skall inte enbart ägna sig åt att klarlägga främmande makters rent militära och försvarspolitiska förhållanden eller militära handlingsmöjligheter. I underrättelsekommitténs betänkande Underrättelsetjänsten – en översyn (SOU 1999:37)

framhålls att Försvarets radioanstalt inte omfattas av den grundprincip för försvarsunderrättelseverksamhet som säger att sådan verksamhet uteslutande får avse underrättelser av betydelse för rikets yttre säkerhet. Försvarets radioanstalt bedriver inte enbart militär underrättelsetjänst utan har även andra uppgifter, bl.a. som ett regeringens utrikes- och säkerhetspolitiska civila inhämtningsorgan. Försvarets radioanstalt kan också ges särskilda uppdrag att med sin tekniska expertis lämna stöd för annan myndighetsverksamhet än sådan som rör yttre hot (SOU 1999:37 s. 219).

3.1 Försvarets radioanstalts organisation

Under hösten 1999 genomfördes en förändring av Försvarets radioanstalts organisation. Omorganisationen syftade bl.a. till en samordning av militär och icke militär signalspaning som tidigare bedrivits i olika avdelningar vilka i princip varit helt skilda från varandra. Vardera avdelningen bedrev separat inhämtning, bearbetning och analys samt rapportproduktion. Den nya organisationen skall bl.a. möjliggöra en bättre beredskap för att följa upp nya hot och risker inom ramen för en förändrad säkerhetspolitisk situation och ett vidgat säkerhetsbegrepp. Genom att skapa gemensamma avdelningar för militär och civil inhämtning, bearbetning samt underrättelserapportering har det även varit möjligt att göra vissa samordningsvinster.

Omorganisationen har medfört att det under generaldirektören finns en ledningsstab och sju avdelningar jämte vissa särskilda funktioner. Med undantag för vad som inryms under en särskild avdelning för teknisk signalspaning så har all inhämtning, bearbetning respektive analys och rapportering samlats under tre särskilda avdelningar. Avdelningen för teknisk signalspaning genomför egen inhämtning, bearbetning och rapportering. Vidare finns avdelningar för administration, drift och underhåll samt systemutveckling.



3.2 Försvarets radioanstalts uppgifter och verksamhet

Försvarets radioanstalts verksamhet regleras i första hand genom 1–3 §§ förordningen (1994:714) med instruktion för Försvarets radioanstalt. Här anges att Försvarets radioanstalt är en central förvaltningsmyndighet med uppgift att bedriva signalspaning enligt den inriktning som regeringen, Försvarsmakten och övriga uppdragsgivare anger. Det är uppdragsgivarna som på detta sätt styr verksamheten. Försvarets radioanstalt är således enligt instruktionen en uppdragstagande myndighet som skall utföra signalspaning i enlighet med vad olika uppdragsgivare anger såsom målsättning och syfte med spaningen.

Vid utövandet av sin verksamhet skall Försvarets radioanstalt enligt 2 § i instruktionen särskilt

- följa förändringen av signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet,
- fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten, och
- utföra matematiska bedömningar av kryptosystem för totalförsvaret.

Försvarets radioanstalt skall också, enligt 3 § i myndighetens instruktion, biträda andra myndigheter vid värdering, utveckling, anskaffning och drift av signalspaningssystem.

Verksamhetsmålen för Försvarets radioanstalts försvarsunderrättelseverksamhet läggs närmare fast i regeringens regleringsbrev för myndigheten. Av regleringsbrevet för budgetåret 2003 framgår att Försvarets radioanstalt genom sin rapportproduktion skall tillgodose regeringens, Försvarsmaktens och övriga uppdragsgivares behov av underrättelser för att skapa fullgoda underlag för planering, beslut och genomförande av verksamhet. Försvarets radioanstalts verksamhet skall bedrivas så att den snabbt kan anpassas till händelseutvecklingen i omvärlden och produktionen skall vara förankrad i och styrd av uppdragsgivarens behov.

Enligt regleringsbrevet skall Försvarets radioanstalt producera signalreferensbibliotek för i första hand Försvarsmaktens behov. Försvarets radioanstalt skall även stödja Försvarsmaktens förbandsproduktion och därvid utveckla och anskaffa signalspaningssystem samt utveckla metodik och fackutbilda personal. Försvarsmakten får ge Försvarets radioanstalt uppdrag om hur dessa uppgifter skall utföras. Försvarets radioanstalt skall också stödja Försvarsmakten vad avser uppgiften territoriell integritet.

Försvarets radioanstalt skall vidare stödja svenska förband i internationell tjänst vad gäller signalspaningsutrustning och metodik som behövs främst för att förvarna om omedelbara hot mot förbanden. Försvarets radioanstalt skall även förbereda underrättelsestöd till svenska förband anmälda till EU:s styrkeregister, ett register som upprättats inom ramen för EU:s krishantering.

Målet för verksamheten inom det civila försvaret är enligt regleringsbrevet att värna civilbefolkningen, trygga livsnödvändig försörjning och säkerställa de viktigaste samhällsfunktionerna samt bidra till Försvarsmaktens förmåga vid väpnat angrepp och krig i Sveriges omvärld. Härvid skall Försvarets radioanstalt även bidra

till fred och säkerhet i omvärlden och stärka samhällets förmåga att förebygga och hantera svåra påfrestningar på samhället i fred.

I en särskild bilaga till regleringsbrevet ges riktlinjer för försvarsunderrättelseverksamheten vid bl.a. Försvarets radioanstalt. Den mer detaljerade inriktningen innefattar i huvudsak en sammanfattning av vad regeringen i tidigare propositioner angivit om de uppgifter som faller på försvarsunderrättelseorganen och som framgår av föregående kapitel.

3.3 Signalspaning

Signalspaning sker genom att med mottagarsystem och andra elektroniska hjälpmedel registrera telesändningar och signaler för att hämta in information som kan användas i underrättelseverksamheten. Signalerna kan komma från kommunikation genom tal, telegrafi, data och fjärrskrift eller ha andra funktioner i samband med radar, navigering eller överföring av mätvärden.

Signalspaningen har av tradition haft till huvuduppgift att vara s.k. larmklocka, vilket innebär att varna för angreppsförberedelser eller omedelbart hot om angrepp mot Sverige. Att upprätthålla denna förmåga har varit en grundläggande uppgift för Försvarets radioanstalt. Myndigheten har under senare år även utvecklat spanings- och bearbetningsmetoder för att rapporteringen skall svara mot det nya säkerhetspolitiska läget och krav på långsiktighet.

Signalspaning riktar sig mot alla typer av eterburna telesändningar och främst mot sådana som är avsedda att överföra information i tal eller skrift. Den information som erhålles spänner över ett brett spektrum, från det utrikes- och försvarspolitiska området till detaljuppgifter om t.ex. enskilda militära förband eller vapensystem och deras kapacitet.

Signalspaning måste bedrivas under sträng sekretess. Denna betingas inte, som i andra underrättelsesammanhang, i första hand av behovet att skydda källorna/signalerna. Dessa kan vara tillgängliga även med en ganska enkel utrustning. Den höga sekretessen motiveras främst av behovet av att hemlighålla metoder och teknik som används, bl.a. för att bryta igenom signalskydd. Om dessa röjs försvåras eller omintetgörs fortsatt arbete.

Försvarets radioanstalts signalspaning innefattar såväl inhämtning som bearbetning och analys samt rapportering till

myndighetens olika uppdragsgivare. Inhämtningen sker genom avlyssning och registrering av utvalda signaler. Den sändande parten söker vanligen skydda innehållet i kommunikationen genom ett högt utvecklat signalskydd. Bearbetningen syftar till att forcera signalskyddet och ta fram informationen i klartext eller beskriva sändningarnas innehåll. Teknisk analys, trafikbearbetning och kryptoforcering är verktyg för detta. En fortsatt analys ger sedan de faktiska underrättelser, som är syftet med verksamheten.

Signalspaningen bedrivs som kommunikationsspaning (KOS) mot radiokommunikation och som teknisk signalspaning (TES) mot vissa sändningar av annan karaktär. Den utförs från stationer, som med hänsyn till radiovågornas utbredning är placerade på lämpliga platser. Spaning bedrivs även från flygburna stationer och från fartyget HMS Orion.

Kommunikationsspaning

Kommunikationsspaning (KOS) riktar sig mot radiokommunikation som bär ett verbalt kommunikationsinnehåll mellan en sändare och en mottagare, dvs. telefoni, telegrafi, fjärrskrift eller dataöverföring. Informationen kan överföras via t.ex. kommunikationssatellit eller radiolänk. KOS bedrivs av Försvarets radioanstalt inom alla våglängdsområden där kommunikationssändningar förekommer. Främst inom kortvågsområdet är räckvidden mycket god. Signaler kan ofta uppfångas från krisområden på andra kontinenter.

Kommunikationsspaningen kan delas in i inhämtning, trafikbearbetning och kryptoforcering. *Inhämtning* av långvariga sändningar kan ske på klassiskt sätt, genom att en radiooperatör vrider på sin radiomottagare tills han eller hon hör något som erfarenhetsmässigt är intressant. När det gäller kortvariga eller komprimerade sändningar krävs däremot automatiska spaningssystem som endera är bredbandiga eller snabbt skannar sig igenom stora frekvensområden. De uppfångade radiosignalerna lägesbestäms, vilket främst sker genom pejling. För god precision krävs flera avlyssningsplatser lämpligt placerade i förhållande till den pejlade sändaren.

Trafikbearbetningen syftar till att bringa ordning i det skenbara kaos som det inhämtade materialet erbjuder. Härigenom kan man konstatera vem som kommunicerar med vem och varför. De uppfångade radiosignalerna identifieras och trafikmönster fastställs.

Identifiering av radiosändningar kan ske på ett antal olika sätt. Anropssignaler, frekvensanvändning och trafikprocedur kan identifiera sambandscentralen, analys av signalernas modulation kan identifiera radiosändaren, analys av röst eller personlig stil kan identifiera sambandspersonalen och analys av själva meddelandena kan identifiera korrespondenten, dvs. användaren av radiostationen.

Kryptoforceringens yttersta mål är att i klartext kunna läsa den information som främmande stater och andra organisationer förmedlar i form av t.ex. olika rapporter och order m.m. För att skydda sig mot detta har krypteringstekniken utvecklats snabbt. På motsvarande sätt har även kryptoforceringen utvecklats och blivit allt mer datorstödd. Kunskap om kryptoforcering är också en nödvändig förutsättning för att kunna konstruera egna goda krypton. Det sista momentet i kommunikationsspaningskedjan är analys och delgivning av det bearbetade underlaget.

Teknisk signalspaning

Teknisk signalspaning riktar sig huvudsakligen mot signaler med andra syften än samband, främst målsökar-, radar- och navigeringssystem. Teknisk signalspaning följer framförallt främmande militära rörelser i vårt närområde och analyserar delar av den signalering som är associerad med dessa. Den används i huvudsak för att utvinna teknisk information och för att identifiera och lägesbestämma bl.a. flygplan och fartyg. Teknisk signalspaning syftar till att följa motståndarens rörelser och därigenom stödja den egna yt- och luftlägesbilden. Den har också till uppgift att analysera de strålande delarna av motståndarens vapensystem och därmed lämna underlag för att bedöma deras prestanda och kunna anpassa egna vapen, motmedel eller taktik.

Utvecklingen inom området för s.k. telekrigföring med elektroniska stridsmedel utgör ett allt större hot, eftersom sådana stridsmedel helt kan såväl förstöra vitala civila informations- och kommunikationssystem som oskadliggöra påkostade militära ledningss- och vapensystem. Utvecklingen ställer ökade krav på signalkunskap och på att Försvarets radioanstalt bl.a. kan förse Försvarsmakten med aktuella s.k. signalbibliotek, som kan utnyttjas i varnar- och motmedelssystem på bl.a. örlogsfartyg och i stridsflygplan (JAS).

3.4 Försvarets radioanstalts delgivning av underrättelser

Försvarets radioanstalt är enligt instruktionen en uppdragstagande myndighet som skall utföra signalspaning i enlighet med vad olika uppdragsgivare anger såsom målsättning och syfte med spaningen. Genom signalspaning utvinner myndigheten underrättelser som delges de olika uppdragsgivarna genom flera typer av rapporter. Försvarets radioanstalt deltar också i det internationella underrättelsesamarbetet som det åligger myndigheten att medverka i enligt lagen (2000:130) om försvarsunderrättelseverksamhet.

Försvarets radioanstalt delger olika underrättelser i enlighet med sin instruktion och respektive mottagares ansvarsområde. Mottagarna av Försvarets radioanstalts underrättelser är i första hand regeringen i form av Statsrådsberedningen samt Utrikes- och Försvarsdepartementen. Den underrättelseinformation som delges rör huvudsakligen internationella relationer, krishärdar och de internationella uppdrag i vilka svensk personal deltar. Därutöver delges viss information rörande terrorism, exportkontroll, protokollära ärenden och händelser i närheten av svenskt territorium. De nämnda departementens underlydande myndigheter får underrättelser som hör till respektive myndighets ansvarsområde. Så får t.ex. Inspektionen för strategiska produkter (ISP) information om bl.a. exportkontrollärenden. Försvarsmakten – främst den militära underrättelse- och säkerhetstjänsten (MUST) och Operativa insatsledningen (OPIL) – samt Totalförsvarets forskningsinstitut (FOI) och Försvarets materielverk (FMV) delges företrädesvis information rörande den militära situationen i Sveriges närområde. Myndigheterna erhåller också information om de internationella uppdrag i vilka svensk personal deltar samt om frågor rörande spridning av massförstörelsevapen, betydelsefulla vapen, vapenexportärenden och militär teknologisk utveckling. Övriga uppdragsgivare, exempelvis Säkerhetspolisen, kriminalpolisens underrättelsetjänst, Tullverket och Kustbevakningen delges information rörande bl.a. terrorism, främmande underrättelseverksamhet och organiserad brottslighet.

Försvarets radioanstalts rapportering skall anpassas till regeringens behov i enlighet med vad som anges av Regeringskansliets samordningssekretariat för säkerhetspolitiska underrättelsefrågor (SUND). Vidare skall Försvarsmakten genom s.k. inriktningsdokument ge mera generella uppdrag på årsbasis åt

Försvarets radioanstalt. Mellan Försvarets radioanstalt och några uppdragsgivande myndigheter finns avtal om vissa uppgifter som Försvarets radioanstalt skall ha. Sådana avtal föreligger mellan Försvarets radioanstalt och Försvarsmakten, Försvarets radioanstalt och Säkerhetspolisen (SÄPO) samt Försvarets radioanstalt och Försvarets materielverk (FMV). I övrigt har Försvarets radioanstalt såsom en uppdragstagande myndighet att utföra de uppdrag som under hand ges av regeringen, Försvarsmakten och andra myndigheter.

Rapporteringen av underrättelser från Försvarets radioanstalt kan t.ex. röra främmande stridskrafters rörelser, övningar och prov av vapen samt kränkningar av svenskt territorium. I underrättelseverksamheten ingår också rapportering av biografiska underrättelser. Den dagliga rapporteringen rör information av betydelse för bedömningar av internationell krishantering samt den allmänna utrikes- och försvarspolitiska utvecklingen. Regelbunden rapportering sker om bl.a. extremism, terrorism och proliferation (spridning av massförstörelsevapen). Försvarets radioanstalt rapporterar om förhållandena i vissa regioner som bedöms som kris- eller spänningsområden. En mer långsiktig och bearbetad redovisning sker på månads- eller årsbasis om bland annat underrättelser kopplade till främmande stridskrafters taktik, organisation, struktur och ledning.

4 Övergripande rättslig reglering av behandling av personuppgifter

Från och med den 24 oktober 1998 regleras den grundläggande ramen för behandling av personuppgifter i personuppgiftslagen (1998:204), som därigenom ersatte datalagen (1973:289). Personuppgiftslagen har sin utgångspunkt i Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (dataskyddsdirektivet). Detta kapitel innehåller en kortfattad genomgång av vissa internationella överenskommelser jämte dataskyddsdirektivet samt en redogörelse för personuppgiftslagens bestämmelser. Härutöver behandlas artikel 8 i den europeiska konventionen den 4 november 1950 om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) jämte artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Båda artiklarna behandlar skyddet av personuppgifter.

4.1 Dataskyddskonventionen

Internationella riktlinjer har meddelats för automatisk databehandling av personuppgifter. Bestämmelser av betydelse finns i bl.a. Europarådets konvention från 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter (dataskyddskonventionen). Konventionens innehåll kan ses som en precisering av skyddet vid användning av automatisk databehandling enligt artikel 8 i Europakonventionen. Dataskyddskonventionens syfte är att säkerställa den enskildes rätt till personlig integritet i samband med automatisk databehandling av personuppgifter och att förbättra förutsättningarna för ett fritt informationsflöde över gränserna.

Dataskyddskonventionen innehåller principer för dataskydd som de konventionsanslutna staterna måste uppfylla i sin nationella

lagstiftning. Personuppgifter som är föremål för automatisk databehandling skall hämtas in och behandlas på ett korrekt sätt för särskilt angivna ändamål. Uppgifterna måste vara relevanta för ändamålen och får inte senare användas på ett sätt som är oförenligt med dessa. Vidare måste uppgifterna vara riktiga och aktuella och uppgifterna får inte bevaras längre än vad som är nödvändigt för ändamålen. Vissa personuppgifter får behandlas endast om den nationella lagen ger ett ändamålsenligt skydd. Till sådana personuppgifter hör uppgifter om enskildas ras, politiska tillhörighet, religiösa tro eller övertygelse i övrigt, hälsa eller sexualliv eller uppgifter som hänför sig till misstanke om brott och dom för brott.

För att skydda personuppgifter mot oavsiktlig eller otillåten förstörelse m.m. föreskriver konventionen att lämpliga skyddsåtgärder skall vidtas. Vidare skall den registrerade ha möjligheter till insyn i register och till att få uppgifter rättade. I vissa fall får undantag göras från bestämmelserna om uppgifternas beskaffenhet och rätten till insyn. Sådana inskränkningar i den enskildes skydd förutsätter stöd i den nationella lagstiftningen och att inskränkningen är nödvändig i ett demokratiskt samhälle för vissa ändamål, t.ex. statens penningintressen och brottsbekämpning samt för att skydda enskildas fri- och rättigheter.

Dataskyddskonventionens roll som riktmärke för automatiserad behandling av personuppgifter övertas i princip av dataskyddsdirektivet i och med att detta införlivas i EU-ländernas nationella lagstiftningar, på de områden där direktivet är tillämpligt dvs. EU:s första pelare. Inom andra områden såsom t.ex. allmän säkerhet, försvar, statens säkerhet och statens verksamhet på straffrättens område är dataskyddskonventionen emellertid alltjämt av betydelse. Direktivet behandlas närmare i avsnitt 4.4.

Under år 2001 har Europarådets ministerkommitté antagit ett tilläggsprotokoll till dataskyddskonventionen. Tilläggsprotokollet har öppnats för undertecknande. Det innehåller bestämmelser om dataskyddsmyndigheter och överföring av personuppgifter mellan länder. Den svenska regeringen beslutade den 25 oktober 2001 att underteckna och ratificera tilläggsprotokollet vilket skedde den 8 november samma år.

4.2 Europarådets rekommendation om användning av personuppgifter inom polissektorn

I sammanhanget bör också Europarådets rekommendation (Recommendation No. R (87) 15) om användning av personuppgifter inom polissektorn beröras. Rekommendationen innehåller speciella dataskyddsregler för personuppgifter som förs av polismyndighet med hjälp av automatiserad behandling. Genom reglerna har man sökt finna en balans mellan å ena sidan den enskildes intresse av personlig integritet och å andra sidan samhällets intresse av att förhindra och bekämpa brott samt upprätthålla allmän ordning. Regleringen omfattar all insamling, lagring, användning och kommunikation av personuppgifter för polisändamål. Medlemsstaterna får utsträcka regleringen även till manuellt förda register. Det är emellertid inte tillåtet att flytta över personuppgifter från automatiserade register till manuella register för att därigenom undgå rekommendationens reglering. Med polisregister i rekommendationen avses alla former av strukturerade personuppgifter som förs av polismyndighet med syfte att förhindra och bekämpa brott samt upprätthålla allmän ordning. Polismyndighet skall anmäla sina register till dataskyddsmyndigheten. Endast sådana personuppgifter får samlas in som är nödvändiga för att förhindra en verklig fara eller bekämpa ett visst brott såvida inte den inhemska lagstiftningen godkänner att mer omfattande uppgifter samlas in. Om möjligt bör den enskilde informeras om att uppgifter samlats in om honom eller henne när det inte längre är till skada för polisverksamheten. Lagrade uppgifter skall så långt det är möjligt vara riktiga och begränsade till sådant som är nödvändigt för att polismyndigheten skall kunna fullgöra sina lagstadgade uppgifter. Personuppgifter i polisregister får endast användas för polisändamål och överföras från en polismyndighet till en annan om uppgifterna behövs av mottagaren för att förhindra eller bekämpa brott eller upprätthålla allmän ordning. För att den enskilde skall kunna utöva vissa rättigheter skall det finnas en offentlig uppgift om befintliga polisregister. Den enskilde skall nämligen kunna få polisregisterutdrag och kräva att felaktiga uppgifter rättas eller tas bort. En begäran att få registerutdrag kan i princip vägras endast i två fall, nämligen om det krävs för att skydda vittnen eller polisinformatörer eller om det är oundgängligen nödvändigt för att utföra en lagstadgad polisuppgift. Den enskilde skall även ha rätt att överklaga ett avslagsbeslut. Datakvaliteten skall fortlöpande kontrolleras i ett

polisregister. Särskilda krav ställs också på datasäkerheten, bl.a. skall det föras ett loggregister (uppgifterna om rekommendationen är hämtade från Claes Kring & Sten Wahlqvist: Datalagen med kommentarer, Stockholm 1989; s. 40f.).

4.3 Riktlinjer från OECD

Internationella riktlinjer ifråga om integritetsskydd och persondataflöde över gränserna har även utarbetats inom Organisationen för ekonomiskt samarbete och utveckling (OECD). Riktlinjerna är från 1980. Ett antal internationella organisationer och företag har antagit egna regler om dataskydd som bygger på OECD:s riktlinjer. Riktlinjerna motsvarar i princip de bestämmelser som återfinns i dataskyddskonventionen. Det bör tilläggas att år 1998 antogs OECD:s ministerdeklaration ”Protection of Privacy on Global Networks”, som innebar att man slog fast intentionen att i ett internationellt perspektiv harmonisera de regler som bör gälla för hantering av personuppgifter i globala nätverk, för att skydda den personliga integriteten.

4.4 Dataskyddsdirektivet

Syftet med dataskyddsdirektivet är att garantera en hög och i alla medlemsstater likvärdig skyddsnivå när det gäller enskilda personers fri- och rättigheter med avseende på behandling av personuppgifter.

Dataskyddsdirektivet är direkt bindande för medlemsstaterna i fråga om det resultat som skall uppnås. För att bli gällande rätt måste direktivet införlivas i medlemsstaternas nationella lagstiftning. Medlemsstaterna bestämmer själva på vilket sätt direktivet skall införlivas, men är därvid starkt bundna av direktivets innehåll. Medlemsstaterna kan inte föreskriva vare sig ett bättre eller sämre skydd för den personliga integriteten vid behandling av personuppgifter eller för det fria flödet av sådana uppgifter än vad som följer av dataskyddsdirektivet.

4.4.1 Tillämpningsområde

Dataskyddsdirektivet handlar om fysiska personers skydd. Skyddet för juridiska personer berörs inte av direktivet. Direktivet omfattar

inte bara helt eller delvis automatiserad behandling, utan också manuell behandling av personuppgifter som ingår eller kommer att ingå i ett register. Utanför tillämpningsområdet faller t.ex. ostrukturerade akter. Dataskyddsdirektivet omfattar inte behandling av personuppgifter för privat bruk.

Dataskyddsdirektivet gäller inte heller för sådan behandling av personuppgifter som utgör ett led i en verksamhet som faller utanför gemenskapsrätten, och inte under några omständigheter behandlingar som rör allmän säkerhet, försvar, statens säkerhet och statens verksamhet på straffrättens område (artikel 3.2 första strecksatsen). Som en följd härav omfattas således inte Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt Försvarets radioanstalts underrättelseverksamhet av direktivets bestämmelser. Den svenska personuppgiftslagen, genom vilken direktivet införlivas i svensk rätt, har däremot gjorts generellt tillämplig och omfattar även sådan verksamhet som faller utanför EG-rättens område, således även försvarsmyndigheternas underrättelseverksamhet och militär säkerhetstjänst. Enligt personuppgiftslagen gäller emellertid att avvikande bestämmelser i lag eller förordning har företräde framför personuppgiftslagen.

4.4.2 Bestämmelser om när personuppgifter får behandlas

Enligt dataskyddsdirektivet måste all behandling av personuppgifter vara laglig och korrekt. Uppgifterna måste vara riktiga och aktuella samt adekvata, relevanta och nödvändiga med hänsyn till de ändamål för vilka de behandlas. Ändamålen skall vara uttryckligt angivna vid tiden för insamling av uppgifterna. De ändamål för vilka uppgifterna senare behandlas får inte vara oförenliga med de ursprungliga ändamålen.

Personuppgifter får enligt direktivet behandlas bara i vissa fall. Här kan nämnas att uppgifter får behandlas i första hand efter att den registrerade otvetydigt har lämnat sitt samtycke, men också om det är nödvändigt för att fullgöra en rättslig förpliktelse som åvilar den registeransvarige eller för att utföra en arbetsuppgift som antingen är av allmänt intresse eller utgör ett led i myndighetsutövning. Personuppgifter får även behandlas om intresset av att den registeransvarige får behandla uppgifterna överväger den registrerades intresse av att de inte behandlas.

Vissa särskilda i direktivet angivna kategorier av uppgifter får som huvudregel inte behandlas utan uttryckligt samtycke av den

registrerade. Det gäller uppgifter som avslöjar den enskildes ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse eller medlemskap i fackförening samt uppgifter som rör hälsa och sexualliv. Medlemsländerna får emellertid under förutsättning av lämpliga skyddsåtgärder och av hänsyn till ett viktigt allmänt intresse besluta om undantag från förbudet.

4.4.3 Information och rättelse m.m.

Dataskyddsdirektivet föreskriver att den registeransvarige skall informera den registrerade om att personuppgifter är föremål för behandling och därvid redogöra för ändamålet med behandlingen. Har uppgifterna inte samlats in från den registrerade själv behöver den registeransvarige däremot inte lämna någon information, om det skulle visa sig vara omöjligt eller innebära en ansträngning som inte står i proportion till nyttan. Den registrerade har dock rätt att på begäran få information om de registrerade uppgifterna. Vidare har den registrerade rätt att få sådana uppgifter som inte har behandlats i enlighet med direktivet rättade, utplånade eller blockerade.

Direktivet innehåller även regler om säkerhet vid behandlingen. Genom lämpliga tekniska och organisatoriska åtgärder skall den registeransvarige skydda personuppgifter mot otillåten behandling samt mot förstöring, förlust, ändring eller otillåten spridning.

4.4.4 Tillsynsmyndighet

Enligt dataskyddsdirektivet skall varje medlemsstat tillse att det utses en eller flera myndigheter som har till uppgift att inom dess territorium övervaka tillämpningen av de bestämmelser som medlemsstaterna antar till följd av direktivet. Dessa myndigheter skall fullständigt oberoende utöva de uppgifter som åläggs dem. Datainspektionen har utsetts till sådan tillsynsmyndighet i Sverige.

Varje tillsynsmyndighet skall ha särskilda undersöknings-befogenheter. Härmed avses t.ex. befogenhet att få tillgång till uppgifter som blir föremål för behandling och att ingripa när de nationella bestämmelser som antagits till följd av direktivet har överträtts.

I dataskyddsdirektivet föreskrivs ett relativt omfattande anmälningsförfarande till tillsynsmyndigheten när det gäller helt

eller delvis automatiserad behandling av personuppgifter. För icke-automatiserade behandlingar får medlemsländerna föreskriva ett förenklat anmälningsförfarande. Undantag från anmälningsplikt eller tillämpning av ett förenklat anmälningsförfarande får också föreskrivas, dels om det med hänsyn till de behandlade uppgifterna inte är sannolikt att den registrerades fri- eller rättigheter kränks, dels om den registeransvarige har utsett uppgiftsskyddsombud (personuppgiftsombud).

4.4.5 Överföring av personuppgifter till tredje land

Direktivet syftar till ett fritt flöde av personuppgifter mellan medlemsländerna. Som huvudregel gäller att överföring av personuppgifter till ett land utanför EU eller Europeiska ekonomiska samarbetsområdet (EES), tredje land, får ske endast om det mottagande landets lagstiftning kan säkerställa en adekvat skyddsnivå. Vad som är en adekvat skyddsnivå får avgöras med hänsyn tagen till bl.a. de uppgifter som skall behandlas och ändamålet med behandlingen.

I vissa fall får personuppgifter föras över till länder vars lagstiftning i och för sig inte erbjuder en adekvat skyddsnivå. Det gäller bl.a. om den registrerade otvetydigt samtycker till att överföring sker eller om överföringen är nödvändig eller bindande enligt författning av skäl som rör viktiga allmänna intressen. Exempel på det sistnämnda är vissa överföringar vid internationellt utbyte av uppgifter mellan skattemyndigheter eller tullmyndigheter.

4.5 Europakonventionen

Den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna gäller som svensk lag här i landet. I artikel 8 stadgas att var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. En offentlig myndighet får inte inskränka åtnjutande av denna rättighet annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till statens säkerhet, den allmänna säkerheten, landets ekonomiska välstånd eller till förebyggande av oordning eller brott eller till skydd för hälsa eller moral eller för andra personers fri- och rättigheter.

Såvitt gäller laglighetskriteriet krävs, utöver att intrånget skall grundas på nationell lag, att den åberopade lagen uppfyller vissa minimikrav i fråga om kvalitet och tydlighet. En rättighetsinskränkande tolkning av lagen skall kunna förutses och lagen skall vara allmänt tillgänglig. Att ett ingripande skall vara nödvändigt innebär att det skall föreligga ett ”angeläget samhälleligt behov” av åtgärden i fråga. Åtgärden får dock inte gå längre än vad som är erforderligt med beaktande av proportionalitetsprincipen, dvs. den skall stå i rimlig relation till det intresse åtgärden är avsedd att tillgodose. Vid denna avvägning har staterna ett visst handlingsutrymme att inom rimliga gränser göra de avvägningar i bevis- och andra bedömningsfrågor, vilka läggs till grund för ett ingripande.

Primärt innebär artikel 8 att staten skall avhålla sig från ingrepp i den skyddade rättigheten, utom i de fall som omfattas av de i artikeln föreskrivna undantagen. Artikelns räckvidd är dock inte begränsad i detta avseende utan staten är också i viss mån skyldig att vidta positiva åtgärder för att skydda den enskildes privata sfär. Sådana positiva åtgärder kan utgöras av lagstiftningen men också av skydd mot övergrepp i särskilda situationer. Även utan att det förekommit något ingripande från myndighet eller offentlig tjänsteman kan staten således under vissa förutsättningar anses ha brutit mot artikel 8 genom att tolerera en föreliggande situation eller genom att inte skapa ett tillräckligt rättsligt skydd. Statens ansvar för en underlåtenhet kan då aktualiseras, trots att det övergrepp som visat att det rättsliga skyddet var otillräckligt utförts av en enskild person, för vars handlande staten inte i och för sig kan anses ansvarig. De krav som ställs på staten måste vara rimliga. Vad som i huvudsak kan förväntas är att staten utfärdar lagar och förordningar som ger ett tillfredsställande skydd åt privatliv, familjeliv, hem och korrespondens (se Hans Danelius, Mänskliga rättigheter i europeisk praxis – En kommentar till Europakonventionen om de mänskliga rättigheterna, uppl. 2:1, 2002, Norstedts Juridik, Stockholm, s. 261f).

4.6 Europeiska unionens stadga om de grundläggande rättigheterna

Den 7 december 2000 tillkännagavs Europeiska unionens stadga om de grundläggande rättigheterna av parlamentet, rådet och kommissionen. I stadgan bekräftas de rättigheter som har sin grund

i medlemsstaternas gemensamma författningstraditioner och internationella förpliktelser samt i Fördraget om Europeiska unionen och gemenskapsfördragen, såsom Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, gemenskapens och Europarådets sociala stadgor och rättspraxis vid Europeiska gemenskapernas domstol och Europeiska domstolen för de mänskliga rättigheterna. Stadgans syfte är att kodifiera de grundläggande fri- och rättigheterna som EU redan erkänner. För närvarande är stadgan inte mer än en politisk viljeförklaring avseende de redan existerande rättigheterna. Stadgan är således inte rättsligt bindande.

I stadgans artikel 8 föreskrivs att var och en har rätt till skydd av de personuppgifter som rör honom eller henne. Dessa uppgifter skall behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem. En oberoende myndighet skall kontrollera att reglerna efterlevs.

Stadgan riktar sig till EU:s egna organ och institutioner samt till medlemsstaterna endast när de tillämpar unionsrätten. Stadgan riktar sig alltså inte till medlemsstaterna när de stiftar nationella lagar inom områden där EU inte har givits lagstiftningskompetens.

Varje begränsning i utövningen av de rättigheter och friheter som erkänns i stadgan skall vara föreskrivna i lag och vara förenliga med proportionalitetsprincipen och det väsentliga innehållet i fri- och rättigheterna. De rättigheter som skyddas i stadgan skall ha samma innebörd och räckvidd som de som skyddas i Europakonventionen. Stadgans artiklar får inte tolkas som att de inskränker eller inkräktar på fri- och rättigheter enligt andra konventioner eller överenskommelser. Missbruk av rättigheter, såsom att t.ex. utnyttja en bestämmelse i stadgan för att åsidosätta en annan bestämmelse, är uttryckligen förbjudet i stadgan.

4.7 Personuppgiftslagen

Med anledning av att dataskyddsdirektivet skulle antas tillsatte regeringen 1995 en kommitté med uppgift att utreda på vilket sätt direktivet skulle införlivas i svensk rätt (Datalagskommittén). Uppdraget redovisades i betänkandet Integritet – Offentlighet – Informationsteknik (SOU1997:39). Personuppgiftslagen (1998:204) bygger i allt väsentligt på det förslag som lades fram i

betänkandet. Det bör anmärkas att regeringen den 1 mars 2002 tillsatte en utredning med uppgift att i vissa hänseenden se över personuppgiftslagen (Dir. 2002:31).

4.7.1 Allmänt om lagen och dess tillämpningsområde

Personuppgiftslagen reglerar själva hanteringen av personuppgifter och inte bara missbruk av sådana uppgifter. Det innebär att behandling av personuppgifter som inte sker med stöd av personuppgiftslagen är otillåten. Med behandling av personuppgifter avses varje åtgärd som vidtas med uppgifterna, t.ex. insamling, lagring, bearbetning, inhämtande, utlämnande, samkörning eller förstöring. Personuppgifter i lagens mening är all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.

Personuppgiftslagen tillämpas på all automatiserad behandling av personuppgifter. Dessutom är lagen tillämplig på manuell behandling av uppgifter som ingår, eller är avsedda att ingå, i en strukturerad samling av personuppgifter, vilka är tillgängliga för sökning eller sammanställning enligt särskilda kriterier. Lagen omfattar även sådan verksamhet som faller utanför gemenskapsrätten, t.ex. allmän säkerhet och försvaret. Sedan tidigare har Sverige haft ett system som utgår från en generell lag kompletterad med särregler i s.k. registerförfattningar för viktigare eller känsligare register på det offentliga området. Enligt 2 § personuppgiftslagen gäller särreglering i lag eller förordning framför bestämmelserna i personuppgiftslagen. Att det krävs en särskild författning för att avvika från det integritetsskydd som personuppgiftslagen ger ansåg regeringen vidare vara en garanti för att behovet av särregler övervägs noga i den ordning som gäller för författningsgivning. Målet har också varit att myndighetsregister med ett stort antal registrerade och ett särskilt känsligt innehåll skall regleras särskilt i lag (jfr. bet. 1990/91:KU11 s. 11 och 1997/98:KU18 s. 48 samt prop. 1990/91:60 s. 58 och prop. 1997/98:44 s. 40f.).

Uppgifter om juridiska personer som definitionsmässigt inte utgör personuppgifter omfattas inte av personuppgiftslagen. Inte heller behandling som en fysisk person utför i verksamhet av rent privat natur omfattas, även om behandlingen avser personuppgifter. Dessutom undantas all behandling av personuppgifter som skyddas av tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Vissa viktiga undantag från lagens bestämmelser görs också för sådan

personuppgiftsbehandling som sker uteslutande för journalistiska ändamål eller konstnärligt eller litterärt skapande.

Särreglering i lag eller förordning gäller som nämnts framför personuppgiftslagen. I lagen anges emellertid uttryckligen att den inte får inskränka myndigheternas skyldighet att lämna ut personuppgifter enligt 2 kap. tryckfrihetsförordningen och att den inte heller får hindra att en myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet.

4.7.2 Förutsättningar för behandling av personuppgifter

Grundläggande krav

Ansvarig för behandling av personuppgifter är den personuppgiftsansvarige, dvs. den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.

Personuppgifter skall alltid behandlas på ett korrekt och lagligt sätt samt i enlighet med god sed. De skall samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Efter insamlingen får uppgifterna inte behandlas för något ändamål som är oförenligt med det ändamål för vilket de samlades in. Det anses inte oförenligt med de ursprungliga ändamålen att behandla uppgifterna för historiska, statistiska eller vetenskapliga ändamål. De behandlade uppgifterna måste vara riktiga och relevanta och inte alltför omfattande i förhållande till de ändamål för vilka de behandlas.

Uppfyller personuppgifterna inte kraven skall den personuppgiftsansvarige vidta alla rimliga åtgärder för att utplåna, blockera eller rätta de felaktiga eller ofullständiga uppgifterna.

Personuppgifterna får enligt personuppgiftslagen inte sparas längre än nödvändigt med hänsyn till de ändamål för vilka uppgifterna behandlas. Uppgifter får emellertid inte avidentifieras eller på annat sätt förstöras (dvs. gallras) om det strider mot bl.a. tryckfrihetsförordningens bestämmelser om allmänna handlingar.

När behandling av personuppgifter är tillåten

Enligt personuppgiftslagen är det tillåtet att behandla personuppgifter efter den registrerades samtycke. Med samtycke avses

varje slag av frivillig, särskild och otvetydig viljeyttring genom vilken den registrerade, efter att ha fått information, godtar behandling av personuppgifter som rör honom eller henne. Lagen uppställer inget krav på att samtycke skall vara skriftligt eller på annat sätt formbundet.

Personuppgifter får – trots att samtycke från den registrerade saknas – behandlas om det är nödvändigt *för att* ett avtal med den registrerade skall kunna fullgöras, *för att* den personuppgiftsansvarige skall kunna fullgöra en rättslig skyldighet, *för att* vitala intressen för den registrerade skall kunna skyddas, *för att* en arbetsuppgift av allmänt intresse skall kunna utföras, *för att* den personuppgiftsansvarige eller någon annan till vilken personuppgifter har lämnats ut skall kunna utföra en arbetsuppgift i samband med myndighetsutövning *samt för att* tillgodose ett berättigat intresse hos den personuppgiftsansvarige, om det väger tyngre än den registrerades intresse av integritetsskydd.

Nödvändighetsrekvisitet har bl.a. tolkats så att personuppgifter får behandlas automatiserat även i de fall det är faktiskt möjligt med manuell behandling, om det innebär att förfarandet underlättas.

Känsliga personuppgifter

För vissa slag av uppgifter gäller enligt personuppgiftslagen särskilda restriktioner. Enligt huvudregeln får uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse samt medlemskap i fackförening inte behandlas. Likaså är det förbjudet att behandla sådana personuppgifter som rör hälsa eller sexualliv.

Förbudet mot att behandla känsliga personuppgifter är dock inte undantagslöst. Uppgifterna får behandlas efter den registrerades uttryckliga (dvs. klart manifesterade) samtycke eller när den registrerade har offentliggjort känsliga uppgifter på ett tydligt sätt.

Behandling av känsliga personuppgifter får utföras även när det är nödvändigt *för att* den personuppgiftsansvarige skall kunna fullgöra sina skyldigheter eller utöva sina rättigheter inom arbetsrätten, *för att* rättsliga anspråk skall kunna slås fast, göras gällande eller försvaras *samt för att* den registrerades eller någon annans vitala intressen skall kunna skyddas, om den registrerade är förhindrad att lämna samtycke. Förbudet mot att behandla känsliga personuppgifter gäller inte heller när behandlingen utförs inom

ramen för en ideell organisations berättigade verksamhet med ett politiskt, filosofiskt, religiöst eller fackligt syfte, om behandlingen avser uppgifter om bl.a. medlemmar. Slutligen undantas från förbudet viss behandling av uppgifter inom hälso- och sjukvården samt viss behandling för forsknings- och statistikändamål.

Regeringen eller den myndighet som regeringen bestämmer, dvs. Datainspektionen, får meddela föreskrifter om ytterligare undantag, om det behövs med hänsyn till ett viktigt allmänt intresse.

Uppgifter om brott och användning av personnummer

Vissa uppgifter som inte omfattas av definitionen av känsliga personuppgifter är ändå sådana att behandlingen av dem regleras särskilt i personuppgiftslagen.

Det är förbjudet för andra än myndigheter att behandla personuppgifter om lagöverträdelser, domar och säkerhetsåtgärder i brottmål. Regeringen eller Datainspektionen har dock möjlighet att föreskriva undantag från förbudet, om det är befogat att behandlingen utförs av annan än myndighet och behandlingen står under tillfredsställande kontroll av en myndighet.

Uppgifter om personnummer och samordningsnummer får behandlas bara när den registrerade samtycker till det eller när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

4.7.3 Information och rättelse m.m.

Personuppgiftslagen innehåller bestämmelser som avser att trygga den registrerades rätt att dels kontrollera om behandling av personuppgifter om honom eller henne pågår, dels att begära rättelse av personuppgifter som har behandlats felaktigt.

Information

Den personuppgiftsansvarige skall självmant lämna den registrerade information rörande behandling av personuppgifter, när uppgifter samlas in från den registrerade själv eller från en annan källa. I sistnämnda fall skall den registrerade som huvudregel informeras när uppgifterna noteras, men information behöver inte lämnas om det är omöjligt eller skulle innebära en oproportionerligt stor

arbetsinsats eller om det i lag eller annan författning finns särskilda bestämmelser om registreringen eller utlämnandet av personuppgifter.

Informationen skall omfatta uppgifter om vem den personuppgiftsansvarige är, ändamålet med behandlingen samt all övrig information som den registrerade behöver för att kunna ta tillvara sina rättigheter i samband med behandlingen. Endast sådana uppgifter som den registrerade inte redan känner till behöver lämnas.

Den personuppgiftsansvarige är vidare skyldig att, efter ansökan, en gång per kalenderår gratis informera om huruvida uppgifter som rör sökanden behandlas eller inte, ändamålet med behandlingen, vilka uppgifter som behandlas, varifrån dessa kommer och till vem de lämnas ut. Under förutsättning att uppgifterna inte har lämnats ut till tredje man behöver information dock inte lämnas beträffande personuppgifter som behandlas endast i löpande text som ännu inte har fått sin slutliga utformning, om behandlingen inte har pågått under längre tid än ett år, eller som utgör minnesanteckningar.

Bestämmelserna om informationsskyldighet gäller över huvud taget inte om sekretess eller tystnadsplikt för uppgifterna är föreskriven i förhållande till den registrerade.

Rättelse m.m.

Personuppgifter som är felaktiga eller ofullständiga eller som annars inte har behandlats i enlighet med personuppgiftslagen eller anknytande föreskrifter skall på begäran av den registrerade rättas, utplånas eller blockeras av den personuppgiftsansvarige.

4.7.4 Säkerhet vid behandlingen

Den personuppgiftsansvarige har enligt personuppgiftslagen ett stort ansvar för säkerheten vid behandling av personuppgifter. Bland annat får de personer som arbetar med personuppgifter behandla dessa endast efter den personuppgiftsansvariges instruktioner. För det allmännas verksamhet gäller att om det i annan lagstiftning finns bestämmelser om säkerheten vid behandling av personuppgifter, skall i stället de bestämmelserna tillämpas. Det gäller framför allt bestämmelser om tystnadsplikt och sekretess.

Den personuppgiftsansvarige har vidare ansvar för att tekniska och organisatoriska åtgärder vidtagits för att skydda de behandlade personuppgifterna. Åtgärderna skall åstadkomma en lämplig säkerhetsnivå med beaktande av de tekniska möjligheter som finns, kostnaden för att genomföra åtgärderna, riskerna med behandlingen och hur känsliga de behandlade uppgifterna är.

4.7.5 Överföring av personuppgifter till tredje land

Det är enligt personuppgiftslagen förbjudet att utan samtycke från den registrerade föra över personuppgifter till en stat utanför EU eller EES (tredje land) som inte har en adekvat nivå för skyddet av personuppgifter. Vid bedömningen av om ett land har en adekvat skyddsnivå skall hänsyn tas till samtliga omständigheter som har samband med överföringen. I lagen anges att särskild vikt skall läggas vid uppgifternas art, ändamålet med behandlingen, hur länge behandlingen skall pågå, ursprungslandet, det slutliga mottagarlandet och de regler som finns för behandlingen i det tredje landet.

Från överföringsförbudet görs vissa undantag, bl.a. om behandlingen är nödvändig *för att* fullgöra ett avtal som är i den registrerades intresse, *för att* på den registrerades begäran vidta åtgärder innan ett avtal träffas, *för att* kunna fastställa, göra gällande eller försvara rättsliga anspråk *eller för att* skydda vitala intressen för den registrerade.

Dessutom får regeringen i viss omfattning meddela föreskrifter om undantag från förbudet. Regeringen får meddela föreskrifter om generella undantag från förbudet att föra över personuppgifter till tredje land. Regeringen får också föreskriva undantag när det behövs med hänsyn till viktiga allmänna intressen eller om överföringen sker under sådana omständigheter att det finns tillräckliga garantier till skydd för de registrerades rättigheter. Dessutom får regeringen under vissa förutsättningar besluta om undantag från förbudet i enskilda fall.

4.7.6 Datainspektionens befogenheter som tillsynsmyndighet

Datainspektionens tillsyn

Enligt dataskyddsdirektivet skall en särskild tillsynsmyndighet utses. I Sverige har Datainspektionen tilldelats den uppgiften. Som

ett led i sin tillsynsverksamhet skall Datainspektionen ha tillgång till behandlade personuppgifter och dessutom tillträde till lokaler med anknytning till behandlingen. Datainspektionen kan också vid vite förbjuda fortsatt behandling samt ansöka hos länsrätt om att personuppgifter skall utplånas.

Anmälningsskyldighet och personuppgiftsombud

Helt eller delvis automatiserad behandling av personuppgifter omfattas av anmälningsskyldighet, vilket innebär att den personuppgiftsansvarige skall anmäla sådana behandlingar till Datainspektionen. Syftet med anmälningsskyldigheten är att göra behandlingens ändamål och dess viktigaste egenskaper kända. Datainspektionen skall föra register över anmälda behandlingar. I såväl personuppgiftslagen som personuppgiftsförordningen (1998:1191) och föreskrifter från Datainspektionen (DIFS 1998:2) föreskrivs emellertid om undantag från anmälningsskyldigheten i olika situationer.

Anmälan till Datainspektionen behöver t.ex. inte göras när ett personuppgiftsombud har utsetts av den personuppgiftsansvarige. Personuppgiftsombudet skall ha till uppgift att självständigt se till att den personuppgiftsansvarige behandlar personuppgifter på ett korrekt och lagligt sätt. Personuppgiftsombudet skall ha en förteckning över de behandlingar som den personuppgiftsansvarige utför och han eller hon skall även hjälpa registrerade personer att få rättelse vid misstanke om att personuppgifter är felaktiga eller ofullständiga. Anmälan till Datainspektionen behöver vidare inte ske när behandlingen av personuppgifter regleras genom särskilda föreskrifter i lag eller förordning.

4.7.7 Sanktioner

Om behandling av personuppgifter i strid med personuppgiftslagen orsakar skada för den registrerade har han eller hon rätt till ersättning från den personuppgiftsansvarige för skada och för den kränkning av den personliga integriteten som behandlingen kan ha medfört. Skadeståndsansvaret är i princip strikt, men kan jämkas om den personuppgiftsansvarige visar att felet i behandlingen inte berodde på honom eller henne.

Den som uppsåtligen eller av oaktsamhet gör sig skyldig till vissa förfaranden kan dessutom dömas till böter eller fängelse. Det gäller när osanna uppgifter lämnas i information till den registrerade eller i anmälan eller information till Datainspektionen. Vidare tillämpas straffbestämmelsen om någon i strid med lagen behandlar känsliga personuppgifter, för över uppgifter till tredje land eller låter bli att göra föreskriven anmälan om behandling till Datainspektionen. Straffbestämmelsen tillämpas inte i ringa fall.

5 Försvarsmaktens informationshantering i militär underrättelse- och säkerhetstjänst

Användningen av automatisk databehandling har sedan den senare delen av 1900-talet stadigt ökat inom all offentlig verksamhet och därmed även behandlingen av personuppgifter. Försvarsmakten och Försvarets radioanstalt utgör därvid inget undantag. Inom den militära underrättelse- och säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet behandlas en stor mängd information, såväl personuppgifter som andra uppgifter. För att myndigheternas verksamhet skall kunna bedrivas effektivt är det i detta sammanhang av avgörande betydelse att det finns ett rationellt datorstöd. Utifrån de särskilda krav som respektive verksamheter ställer, vad gäller bl.a. informationssäkerhet och sekretess, har det inom de båda myndigheterna utvecklats olika system för att på automatiserad väg behandla den omfattande mängd uppgifter som är nödvändiga för att uppnå syftet med verksamheterna.

Enligt direktiven har utredningen till uppgift att göra en översyn av regleringen av behandling av personuppgifter inom Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet. Utredningen skall härvid kartlägga behandlingen av personuppgifter och analysera behovet av särskilda bestämmelser. Detta och nästföljande kapitel innehåller en beskrivning av den behandling av personuppgifter som för tillfället förekommer inom Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet. Beskrivningen inleds med en redovisning av den särskilda författning, förordningen (2001:703) om viss behandling av personuppgifter inom Försvarsmakten och Försvarets radioanstalt, som i dag reglerar den aktuella behandlingen av personuppgifter. I övrigt behandlas frågor som rör hur uppgifter

samlas in och lagras samt i övrigt används i verksamheterna. Även säkerhet och behörighet att ta del av behandlade uppgifter tas upp.

Inom framför allt den militära säkerhetstjänsten har det fram till i dag behandlats personuppgifter i manuella register. Dessa är nu på väg att avvecklas och meningen är att även dessa uppgifter inom kort skall behandlas på automatiserad väg.

5.1 Rättslig reglering av behandling av personuppgifter i den militära underrättelse- och säkerhetstjänsten

Den behandling av personuppgifter som omfattas av utredningens uppdrag regleras i dag i förordningen (2001:703) om viss behandling av personuppgifter inom Försvarsmakten och Försvarets radioanstalt, som trädde i kraft den 1 oktober 2001.

I förordningen finns olika allmänna bestämmelser som gäller för all behandling av personuppgifter enligt författningen, således både i Försvarsmaktens och i Försvarets radioanstalts verksamhet. Här finns bestämmelser om tillämpningsområde, personuppgiftsansvar, behandling av känsliga personuppgifter, utlämnande av uppgifter till utländsk myndighet eller internationell organisation, rättelse och skadestånd samt gallring och överklagande. Därutöver finns särskilda bestämmelser som gäller enbart för Försvarsmaktens respektive Försvarets radioanstalts behandling av personuppgifter. Bestämmelserna reglerar vilka register och databaser som får föras i respektive myndighets verksamhet samt under vilka förutsättningar som personuppgifter får behandlas i verksamheten.

Tillämpningsområde (1–2 samt 7 och 13 §§)

Förordningen gäller utöver personuppgiftslagen (1998:204) i fråga om viss behandling hos myndigheterna som är helt eller delvis automatiserad. Detta innebär att det är personuppgiftslagens regler som bestämmer förutsättningarna för behandling av personuppgifter, i den mån det inte finns avvikande bestämmelser i den särskilda förordningen.

Förordningen gäller för Försvarsmakten när myndigheten fullgör uppgifter enligt lagen (2000:130) om försvarsunderrättelseverksamhet, förordningen (2000:131) om försvarsunderrättelseverksamhet och säkerhetsskyddslagen (1996:627). Enligt förordningen skall Försvarsmakten bedriva försvarsunderrättelse-

verksamhet och säkerhetsskyddsverksamhet. Någon definition av begreppen ges inte i förordningen, på annat sätt än att hänvisning görs till de nämnda författningarna.

Definitioner (2 §)

De begrepp som används i förordningen har samma betydelse som i personuppgiftslagen.

Personuppgiftsansvarig (3 §)

I förordningen anges att Försvarsmakten och Försvarets radioanstalt är personuppgiftsansvariga för den behandling av personuppgifter som myndigheterna har att utföra enligt nämnda författningar.

Behandling av känsliga personuppgifter (4 §)

Enligt personuppgiftslagen är det förbjudet att behandla personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening. Det är vidare förbjudet att behandla sådana personuppgifter som rör hälsa eller sexualliv. Det finns vissa undantag från förbudet, bl.a. om samtycke har lämnats. Övriga undantag från förbudet är inte tillämpliga på försvarsunderrättelseverksamhet och militär säkerhetstjänst. Det krävs därför särskilda bestämmelser i annan författning för att behandling av sådana uppgifter skall vara tillåten utan samtycke.

Enligt förordningen får känsliga personuppgifter såsom uppgifter om ras, politiska åsikter, religiös övertygelse, medlemskap i fackförening, hälsa eller sexualliv inte utgöra ensam grund för behandling. Behandlas uppgifter om en person på annan grund får uppgifterna dock kompletteras med sådana känsliga personuppgifter, om det är nödvändigt för syftet med behandlingen.

Utlämnande av uppgifter (5 §)

Uppgifter får lämnas ut till en utländsk myndighet eller en internationell organisation endast om utlämnandet tjänar den svenska

statsledningen eller det svenska totalförsvaret och inte är till skada för svenska intressen.

Rättelse och skadestånd (6 §)

I fråga om rättelse och skadestånd anges att bestämmelserna i personuppgiftslagen gäller.

Gallring (16 §)

Personuppgifter skall enligt personuppgiftslagen inte bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Personuppgifter får dock bevaras för historiska, statistiska eller vetenskapliga ändamål. Bestämmelserna i personuppgiftslagen hindrar inte att en myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet. Genom arkivlagen (1990:782) är myndigheterna som huvudregel ålagda att bevara allmänna handlingar.

Personuppgifter som behandlats enligt förordningen skall gallras senast tio år efter den senaste införda uppgiften om den registrerade. Om det finns särskilda skäl får dock uppgifterna stå kvar under längre tid. Riksarkivet får, efter samråd med Försvarsmakten eller Försvarets radioanstalt, meddela föreskrifter om att uppgifter som skall gallras får bevaras för historiska, statistiska eller vetenskapliga ändamål.

Överklagande (17 §)

Andra beslut än beslut om rättelse enligt 6 § i förordningen och om avslag på ansökan om information enligt 26 § personuppgiftslagen får inte överklagas.

Försvarsunderrättelseregister (7–9 §§)

Utöver de allmänna bestämmelserna gäller att Försvarsmakten skall föra försvarsunderrättelseregister och säkerhetsregister. Ett försvarsunderrättelseregister har till särskilt ändamål att underlätta tillgången till allmänna uppgifter med anknytning till försvarsunderrättelseverksamhet samt att ge underlag för säkerhetspolitiska

och militärstrategiska bedömningar, analys av pågående och bedömda framtida konflikter samt biografisk försvarsunderrättelsetjänst.

Försvarsunderrättelseregister får endast innehålla personuppgifter om det är nödvändigt för att Försvarsmakten skall kunna fullgöra sina uppgifter enligt lagen och förordningen om försvarsunderrättelseverksamhet. I övrigt får försvarsunderrättelseregister endast innehålla identifieringsuppgifter, uppgifter om de omständigheter och händelser som ger anledning att anta att den registrerade har betydelse för försvarsunderrättelseverksamheten, och upplysningar om varifrån den registrerade uppgiften kommer och om uppgiftslämnarens trovärdighet.

Säkerhetsregister (13–15 §§)

Försvarsmakten skall föra säkerhetsregister, i den omfattning som är nödvändigt, för att kunna bedriva säkerhetsskyddsverksamhet. Ändamålet med sådan behandling är att ge underlag för beslut eller bedömningar i frågor som syftar till att förhindra säkerhetshotande verksamhet som riktas mot Försvarsmakten, andra myndigheter eller någon annan som Försvarsmakten enligt säkerhetsskyddsförordningen (1996:633) har tillsyn över.

Ett säkerhetsregister får endast innehålla personuppgifter om personen kan misstänkas för att ha utövat eller komma att utöva verksamhet som innefattar hot mot rikets säkerhet eller terrorism, om uppgifter förekommer i samband med att en person har genomgått registerkontroll enligt säkerhetsskyddslagen, om det kan antas att personen bedriver annan säkerhetshotande verksamhet och det finns särskilda skäl till att registret skall innehålla uppgiften eller om personen har lämnat uppgifter om säkerhetshotande verksamhet.

I övrigt får ett säkerhetsregister endast innehålla identifieringsuppgifter, uppgifter om de omständigheter och händelser som ger anledning att anta att den registrerade har betydelse för myndighetens verksamhet att förhindra säkerhetshotande verksamhet, upplysningar om varifrån den registrerade uppgiften kommer och om uppgiftslämnarens trovärdighet, och hänvisning till de ärenden där uppgifter om den registrerade behandlas.

5.2 Behandling av personuppgifter i den militära underrättelse- och säkerhetstjänsten

I den militära underrättelse- och säkerhetstjänsten förekommer alla former av behandling av personuppgifter. Personuppgifter behandlas helt manuellt i särskilda register och i löpande text i olika pappersdokument. Behandling av personuppgifter sker också automatiserat i enskildas handläggares fristående persondatorer samt i elektroniska uppgiftssamlingar där personuppgifterna är gemensamt tillgängliga för flera personer i verksamheten. De manuella register som förs, i framför allt den militära säkerhetstjänsten, är på väg att datoriseras. För att kunna behandla personuppgifter på ett effektivt och ändamålsenligt sätt, anpassat till den stora informationsmängd som är nödvändig för verksamheten, har det inom den militära underrättelse- och säkerhetstjänsten utarbetats flera olika datorbaserade system.

Inhämtning av uppgifter

I den militära underrättelse- och säkerhetstjänsten hämtas uppgifter in med hjälp av flera olika metoder. Huvudsakligen samlas uppgifter in från olika former av öppna källor såsom tidskrifter och litteratur samt via Internet. Inom den militära underrättelse- och säkerhetstjänsten (MUST) finns en särskild sektion, Sektionen för öppna källor, som enbart arbetar med att söka information i sådana allmänt tillgängliga källor.

Försvarsattachéerna vid Sveriges olika ambassader är underställda chefen för MUST och även de har till uppgift att på öppen väg hämta in information om bl.a. militärpolitiska förhållanden och om den militärtekniska utvecklingen i värdlandet. Försvarsattachéerna rapporterar också om de säkerhetspolitiska förhållanden i värdlandet som kan få konsekvenser för Sverige. Den underrättelseinformation som attachéerna förmedlar hämtas i första hand in genom egna observationer vid möte med utländska kollegor och företrädare för värdlandet samt via öppna källor såsom radio, TV, tidningar och tidskrifter. Försvarsattachéerna rapporterar till Högkvarteret/MUST via ett särskilt datasystem som beskrivs nedan.

Inom ramen för Sveriges deltagande i internationella fredsbevarande och humanitära insatser hämtar svenska förbandsenheter in information, som kan vara av betydelse främst för underrättelse-

verksamheten och säkerhetsskyddet vid den enskilda operationen. Kommunikation av sådana uppgifter med Högkvarteret/MUST sker även den i ett särskilt datasystem som beskrivs närmare nedan.

Försvarsmakten bestämmer som uppdragsgivare till viss del inriktningen av Försvarets radioanstalts signalspaning. Den militära underrättelse- och säkerhetstjänsten är också en av de viktigaste mottagarna av de underrättelserapporter som Försvarets radioanstalt förmedlar.

Den militära underrättelse- och säkerhetstjänsten har vidare en dold verksamhet som utförs av Kontoret för särskild inhämtning (KSI). KSI arbetar uteslutande med insamling av underrättelser och använder sig härvid av särskilda metoder. Med särskilda metoder avses förfaringssätt som det inte ankommer på andra underrättelseorgan att använda. Det underrättelsematerial som KSI hämtar in överlämnas i form av rapporter till MUST för vidare bearbetning. KSI utför även inhämtningsuppdrag för andra underrättelsemyndigheter såsom Totalförsvarets forskningsinstitut (FOI) och Försvarets materielverk (FMV).

Till en liten del får MUST uppgifter även från enskilda, t.ex. officerare på utlandsbesök eller privatpersoner med utlandskontakter, som på eget initiativ vänder sig till myndigheten med information som kan vara av underrättelsekaraktär.

Information som på dessa sätt kommer in till den militära underrättelse- och säkerhetstjänsten kan hänföras till både försvarsunderrättelseverksamhet och säkerhetstjänst beroende på arten av den information som erhålls. När det gäller information som uteslutande rör säkerhetstjänst är det vanligast att uppgifterna kommer in i form av en anmälan eller en rapport om en faktisk säkerhetshändelse, t.ex. ett inbrott eller att en hemlig handling har förkommit. Säkerhetstjänsten har också ett samarbete med Säkerhetspolisen (SÄPO) som överlämnar information som är av intresse för Försvarsmakten.

De uppgifter som hämtas in i den militära underrättelse- och säkerhetstjänsten kan naturligtvis avse alla typer av uppgifter, såväl personuppgifter som andra uppgifter vilka inte alls kan hänföras till viss person, t.ex. uppgifter om främmande makts militära stridskrafter. När det gäller personuppgifter förekommer i försvarsunderrättelseverksamhet bl.a. uppgifter om personer som verkar inom andra staters försvars- och underrättelseväsenden och personer som förekommer i underrättelserapporter eller kan komma att få ett underrättelsevärde. I säkerhetstjänsten förekommer uppgifter om t.ex. personer vid andra staters under-

rättelseväsenden eller annan företrädare för främmande makt som bedöms kunna utgöra ett säkerhetshot, personer som varit föremål för registerkontroll enligt säkerhetsskyddslagen och personer som av annan anledning är av betydelse för säkerhetsfunktionen inom Försvarsmakten och dess tillsynsområde. Det är för ändamålet med den militära underrättelse- och säkerhetstjänsten betydelsefullt att myndigheten har möjlighet att på ett effektivt sätt behandla alla kända uppgifter om sådana personer.

5.3 System för automatiserad behandling av personuppgifter m.m.

Inom den militära underrättelse- och säkerhetstjänsten finns flera olika datoriserade system som används för automatiserad behandling av personuppgifter. Systemen är individuellt utformade och anpassade till de olika ändamål inom verksamheten som de skall tjäna. De är dessutom fysiskt skilda från varandra på så sätt att uppgifterna inom varje system är åtkomliga endast via vissa särskilda datorer. Bakgrunden härtill är de stränga säkerhetskrav som betingas av verksamhetens art och syfte. Endast den särskilda databas som innehåller uppgifter från öppna källor är tillgänglig från handläggarens ordinarie persondator. De olika systemen är dock utformande enligt samma grundläggande principer, och skiljer sig således främst åt när det gäller för vilket eller vilka ändamål uppgifter behandlas i systemet och vilka personer som har tillgång till dessa uppgifter.

Gemensamt för de olika systemen är att de i princip fungerar som ett datorsystem vanligen gör på en arbetsplats där flera handläggare har gemensam tillgång till vissa uppgifter. Varje enskild handläggares persondator är kopplad till en och samma server där den information som är gemensamt tillgänglig finns samlad. Vad som skiljer den militära underrättelse- och säkerhetstjänstens olika system från vad som vanligen gäller annars är de väldigt strikta säkerhetskrav som omgärdar varje system. Det är av grundläggande betydelse att endast den som är behörig att ta del av vissa uppgifter skall ha möjlighet att göra så. Härvid gäller självklart att utomstående inte skall kunna ta del av informationen, men även att varje handläggare inom verksamheten endast skall få ta del av de uppgifter som denne har behov av för att kunna utföra sina uppgifter och därmed har särskild behörighet till.

Som exempel på vilka säkerhetsrutiner som omgärdar den militära underrättelse- och säkerhetstjänstens olika system för behandling av personuppgifter kan nämnas det största och viktigaste systemet, som benämns Informationssystem för den militära underrättelse- och säkerhetstjänsten (IS UNDSÄK). Systemet är helt slutet på så sätt att det inte är kopplat till något externt informationssystem som t.ex. Internet eller liknande. Vid befordran av uppgifter inom systemet men till en enhet utanför Högkvarteret/MUST skickas informationen via Försvarsmaktens IP-nät, eller på publikt nät men i en kryptoteknisk struktur som är så avancerad att obehöriga inte kan tillägna sig uppgifterna. Tillgång till de uppgifter som finns i systemet kan endast erhållas via vissa särskilda datorer. Varje handläggare inom MUST eller annan behörig användare har en särskild dator kopplad till systemet, som kan användas först efter att handläggaren identifierat sig med hjälp av ett särskilt kort och tillhörande kod. Den särskilda datorn är vidare försedd med en löstagbar hårddisk som förvaras inlåst när systemet inte används. Nya uppgifter tillförs systemet genom analog eller digital inmatning. Analog inmatning kan ske via tangentbordet av varje enskild handläggare som har tillgång till systemet. Digital eller elektronisk inmatning av uppgifter sker via särskilda datorenheter, i första hand för att undvika att virus kommer in i systemet, och först efter beslut av ställföreträdande chefen för MUST.

5.3.1 Informationsdatabasen – Sektionen för öppna källor

Sektionen för öppna källor är organisatoriskt en enhet inom MUST:s lägesavdelning. Den övergripande uppgiften för sektionen för öppna källor är att genomföra en militärstrategisk omvärldsbevakning genom inhämtning av information via allmänt tillgängliga källor (öppna källor) och sammanställa, bearbeta samt delge sådan information. Inom sektionen arbetar man med att upptäcka, värdera och övervaka öppna elektroniska källor för att på ett systematiskt sätt kunna inhämta och lagra relevant öppen information.

Sektionen för öppna källor producerar och delger regelbundna sammanställningar över intressanta områden och tar varje dag fram en särskild dygnsrapport som sprids via e-post till Regeringskansliet och andra myndigheter. Sektionen svarar vidare på särskilda underrättelse- eller informationsfrågor, s.k. ad hoc-frågor,

från handläggare inom den militära underrättelse- och säkerhetstjänsten. Svar på dessa frågor lämnas efter inhämtning i öppna källor på en bränd cd-skiva direkt till berörd handläggare. Från öppna källor hämtas uppgifter in som kan vara av intresse för hela den militära underrättelse- och säkerhetstjänstens ansvarsområde. Det kan t.ex. röra sig om information om migration, proliferation, mellan- eller inomstatliga konflikter, elektronisk krigföring samt organiserad kriminalitet.

Inhämtningen av information från öppna källor sker genom sökning enligt särskilt angiven inriktning. Sökning sker i databaser på Internet och i viss mån i litteratur och tidskrifter m.m. Enheten köper även uppgifter från Faktiva som är en kommersiell nyhetsleverantör och i vars databas sökning sker enligt vissa generella sökord. Vilka sökord som används vid sökning i Faktivas databas och i övrigt på Internet bestäms inom Sektionen för öppna källor. De begrepp som används innehåller aldrig personuppgifter och innebär av sekretesskäl ofta en mycket vid sökning. Vanligtvis används ca 6–7 sökord och som exempel kan nämnas att sökning sker på ”säkerhetspolitik”. Informationen som finns hos Faktiva kommer från 4000 olika källor. Inhämtning från Faktiva sker åtta gånger per dag och Sektionen för öppna källor laddar ned ca 2 000 dokument per dygn. Informationen som hämtas in från Faktiva lagras direkt i den s.k. Informationsdatabasen, vilken sektionen har som särskilt ansvar att sköta.

Informationsdatabasen

I Informationsdatabasen lagras den information som samlats in från de olika öppna källor sektionen söker i. I denna databas är det för MUST:s handläggare möjligt att genom fritextsökning söka efter nödvändig information, till stöd för de analyser av förhållanden i omvärlden som myndigheten utför.

Det finns inga särskilda behörighetsregler för att ta del av uppgifterna i Informationsdatabasen. Alla handläggare inom MUST som har behov av att utnyttja databasen har också tillgång till all information som finns i databasen.

Uppgifterna i databasen är vidare tillgängliga för andra myndigheter genom direktåtkomst. De myndigheter som i dag har direktåtkomst till Informationsdatabasen är Försvarets materielverk, Försvarets radioanstalt och Regeringskansliet. Det är

sektionens avsikt att denna service i framtiden skall erbjudas även andra myndigheter.

Öppen information som lagras i Informationsdatabasen och är av betydelse för den militära underrättelse- och säkerhetstjänsten kan föras över till systemet IS UNDSÄK, som behandlas nedan, och hanteras där som hemlig. Av säkerhetsskäl överförs information från Informationsdatabasen till IS UNDSÄK via en speciell dator enligt en särskild rutin.

Uppgifterna som behandlas i Informationsdatabasen är av stor betydelse för den militära underrättelse- och säkerhetstjänsten och informationen sparas därför så länge som det är tekniskt möjligt. Särskilt när det gäller information om en viss källa som utnyttjas vid inhämtning är det viktigt att sådan information kan behandlas så länge källan existerar och används. Informationsdatabasen är i dag ca 10 år gammal och även om den innehåller en mycket stor mängd uppgifter har det hittills inte uppstått någon kapacitetsbrist. Av dessa skäl har myndigheten valt att i princip spara allt material. Den information som köpts in från Faktiva rensas emellertid automatiskt från systemet efter 90 dagar.

En mycket stor del av den information som lagras i informationsdatabasen kan heller inte omfattas av någon skyldighet för Försvarsmakten att gallra. Det gäller ovan nämnd information från Faktiva, men även sådan information som Sektionen för öppna källor köper via t.ex. prenumeration på militärvetenskapliga tidskrifter bl.a. från Janes information group. Sådan information omfattas av 2 kap. 11 § tredje punkten tryckfrihetsförordningen, den s.k. biblioteksregeln, och utgör därmed inte allmän handling hos myndigheten. Enligt bestämmelsen undantas från begreppet allmän handling bl.a. tryckt skrift, ljud eller bildupptagning eller annan handling som ingår i bibliotek. Med gallring avses att förstöra allmänna handlingar eller uppgifter i allmänna handlingar på så sätt att det medför någon form av informationsförlust. Gallring kan således bara komma i fråga när det gäller allmänna handlingar och får ske endast i enlighet med särskilda gallringsföreskrifter i lag eller förordning eller föreskrifter eller beslut av Riksarkivet.

5.3.2 Informationssystem för den militära underrättelse- och säkerhetstjänsten (IS UNDSÄK)

Systemet IS UNDSÄK är det största och viktigaste systemet för behandling av personuppgifter inom den militära underrättelse- och säkerhetstjänsten. Här behandlas merparten av den sekretessbelagda information som är nödvändig för försvarsunderrättelseverksamheten och den militära säkerhetstjänsten. Uppgifterna är tillgängliga för ett stort antal personer inom Försvarsmakten, inom olika enheter och på olika nivåer. Dessutom är uppgifterna tillgängliga för vissa andra myndigheter genom direktåtkomst. Som tidigare nämnts är uppgifterna i systemet endast tillgängliga via vissa särskilda datorenheter och för varje sådan enhet är endast en viss person behörig användare. Det finns i dag ca 800 enheter, eller klienter, till systemet IS UNDSÄK.

IS UNDSÄK utnyttjas för behandling av alla typer av uppgifter från personuppgifter till sådana uppgifter som helt saknar anknytning till en fysisk person, t.ex. uppgifter om främmande makts militära förband. I systemet behandlas dels öppen information, dels hemliga uppgifter innefattande kvalificerat hemliga uppgifter, dvs. uppgifter som är av synnerlig betydelse för rikets säkerhet.

Uppgifterna i IS UNDSÄK används som underlag för såväl försvarsunderrättelseverksamhet som militär säkerhetstjänst. I databasen finns en rad olika rutiner som är anpassade för att tillgodose de olika behov som kan finnas för försvarsunderrättelseverksamhet respektive säkerhetstjänst. En rutin är en löst avgränsad arbetsprocess som används för att få fram nödvändiga underrättelser. Som exempel på olika rutiner kan nämnas förbands, materiel-, anläggnings-, underrättelsebehovs-, organisations-, handlings-, person- och registerkontrollrutinen. Inom varje rutin behandlas de uppgifter som bedömts nödvändiga för respektive verksamhet.

Som exempel på vilken typ av uppgifter som hanteras i IS UNDSÄK kan nämnas några av de rutiner som är av särskild betydelse för den militära underrättelse- och säkerhetstjänsten när det gäller behandling av personuppgifter. Flertalet av de rutiner som används inom systemet innehåller information om t.ex. främmande länders stridskrafter, förband och materiel m.m. och innehåller därmed inga personuppgifter.

Under *Rutinen Person* finns biografiska underrättelser för försvarsunderrättelseverksamhet och militär säkerhetstjänst. Det rör sig då om personuppgifter gällande t.ex. personer på ledande

befattningar i andra stater såsom politiker, andra opinionsbildare och militärer. Uppgifterna är av betydelse för att kunna bedöma andra staters avsikter i säkerhetspolitiskt och militärt avseende, och det är därför angeläget för Försvarsmakten att kunna behandla alla kända uppgifter om sådana personer. Under samma rutin registrerar säkerhetstjänsten uppgifter och uppdaterar information om aktuella personer samt andra biografiska underrättelser och aktiviteter som är av intresse ur säkerhetshänseende. I säkerhetstjänsten är uppgifterna av betydelse för att t.ex. kunna avgöra vilket säkerhetshot företrädare för främmande makt utgör i Sverige eller från någon annan plats.

I *Rutinen Handling* behandlar säkerhetstjänsten uppgifter som avser faktiska säkerhetshändelser, t.ex. inbrott i ett förråd, eller händelser som bedöms tyda på säkerhetshotande verksamhet, t.ex. en observation av ett fordon i anslutning till ett skyddsvärt objekt. Sådana händelser rapporteras enligt gällande rutiner antingen muntligt eller skriftligt i en säkerhetsrapport, vilken efterhand återfinns i IS UNDSÄK. I säkerhetsrapporter kan det förekomma personuppgifter som t.ex. namn på ägare till fordon eller uppgiftslämnare.

MUST:s säkerhetsavdelning har tidigare fört ett manuellt register över personer som varit föremål för registerkontroll enligt säkerhetsskyddslagen och uppgifter som har samband därmed. Detta register har överförts till IS UNDSÄK under *Rutinen RK* (registerkontroll). I rutinen finns endast uppgifter om personal vid Försvarsmakten och personer med anknytning till säkerhetsskyddad upphandling med säkerhetsskyddsavtal (SUA). De uppgifter som förekommer är vilken säkerhetsklass en registerkontroll avser, när en framställan om registerkontroll har gjorts och vem som har beslutat om framställan.

Behörigheten att ta del av uppgifter i IS UNDSÄK är kopplad till vilken befattning den enskilde handläggaren har. Behörigheten är även avgörande för möjligheten att uppdatera och förändra uppgifter i systemet. För varje uppgift eller handling som görs tillgänglig i databasen bestäms särskilt vilken behörighet (befattning) som skall gälla för att få ta del av informationen, samt för att uppdatera eller ändra en uppgift. Vilken behörighetsnivå som skall gälla avgörs av den som gör uppgiften eller dokumentet tillgängligt i systemet. Det finns ett stort antal behörighetsnivåer. Behörigheten att ta del av en uppgift kan vara fri så att alla som har tillgång till systemet kan använda den. Tillgången kan också vara

begränsad så att endast någon enstaka befattningshavare har rätt att ta del av, uppdatera eller ändra vissa uppgifter.

IS UNDSÄK används i den militära underrättelse- och säkerhetstjänsten för att underlätta tillgången till såväl hemliga som öppna uppgifter med anknytning till försvarsunderrättelseverksamhet och militär säkerhetstjänst. Till systemet förs ständigt ny information som bearbetas och analyseras och som därefter utgör underlag för de rapporter och andra åtgärder som är syftet med verksamheten. IS UNDSÄK är även det viktigaste delgivningsinstrumentet när det gäller underrättelser som utarbetas av den militära underrättelse- och säkerhetstjänsten. Delgivning av underrättelser sker genom att uppgifterna görs tillgängliga för mottagarna inom systemet. Till de mottagare av underrättelserapporter och annan information från den militära underrättelse- och säkerhetstjänsten som inte har tillgång till IS UNDSÄK sker delgivning av underrättelser i första hand i pappersform.

Uppgifterna i IS UNDSÄK är vidare direkt tillgängliga för vissa myndigheter utanför Försvarsmakten. Regeringskansliet (Försvarsdepartementet), Försvarets materielverk, Försvarets radioanstalt, Tullverket och Krisberedskapsmyndigheten har alla tillgång till systemet genom direktåtkomst. Inom kort kan även Totalförsvarets forskningsinstitut komma att ha direktåtkomst till databasen.

All information som läggs in i IS UNDSÄK indexeras. Detta innebär att alla uppgifter som finns i de särskilda s.k. kommentar- och anteckningsfälten samt i bifogade filer i systemet går att söka på genom fritextsökning. Härigenom är det även möjligt att söka på känsliga personuppgifter. Den militära underrättelse- och säkerhetstjänsten har inget självständigt behov av att kunna använda känsliga personuppgifter som sökord. Det kan emellertid i vissa sammanhang vara viktigt att sådana uppgifter kan användas i kombination med andra uppgifter, t.ex. i verksamhet inom ett internationellt fredsbevarande- eller humanitärt projekt i avsikt att skydda en etnisk minoritet.

Uppgifterna i IS UNDSÄK kan vara av betydelse för den militära underrättelse- och säkerhetstjänsten under lång tid. För ett fullgott beslutsunderlag måste man kunna följa personer och företeelser under en mycket lång period. Samtidigt kan uppgifter som i dag inte har direkt betydelse för verksamheten i framtiden visa sig innehålla mycket värdefull information. Hittills har inte kapacitetstaket i systemet nåtts och därför har heller ingen gallring eller rensning av uppgifter skett. Det finns vidare ett problem med att gallra vissa personuppgifter eftersom detta kan innebära att

viktiga informationskomponenter i en handling, som i övrigt kan sparas under en längre tid, går förlorade. En viktig handling kan på så sätt bli värdelös.

5.3.3 MUST:s internationella sambands- och kryptosystem (MINSK)

MINSK är ett fristående kommunikationssystem för rapporter och meddelanden om särskilda underrättelsebehov från Sveriges försvarsattachéer. Systemet används inom den militära underrättelse- och säkerhetstjänsten för kommunikation med Sveriges försvarsattachéer. Som tidigare nämnts lyder försvarsattachéerna under chefen för MUST och har till uppgift att hämta in underrättelser via öppna källor inom det land där de är verksamma.

Systemet består av en server, som är placerad på Försvarsmaktens högkvarter, till vilken ett antal olika persondatorer, utan egen hårddisk är kopplade. En försvarsattaché som skriver en rapport på sin dator arbetar således direkt mot servern på Högkvarteret. De datorer som är kopplade till systemet finns dels hos MUST, dels hos respektive försvarsattaché.

5.3.4 Bearbetning Analys Internationella Operationer (BANIO)

BANIO är ett system för bearbetning och analys i samband med de internationella operationer som Försvarsmakten deltar i. Den tekniska uppbyggnaden av systemet motsvarar MINSK. Systemet används för kommunikation med den personal inom den svenska insatsen som sysslar med försvarsunderrättelseverksamhet, National Intelligence Cell (NIC).

5.3.5 Totalförsvarets signalskyddssamordning (TSA)

TSA utövar signalkontroll av radio- och trådbefordrad information eller annan informationsöverföring. Signalkontrollen syftar till att ge en bild av vad främmande signalspaning kan ha uppfattat av befordrad information samt att kontrollera att egna signalskyddssystem används och fungerar på önskat sätt.

Resultatet från en signalkontroll utnyttjas i första hand för att förbättra rutinerna och anpassa uttryckssätt eller formuleringar i radiotrafik, eller annan talöverföring som inte är krypterad, i syfte att sekretessbelagda förhållanden inte skall avslöjas. Detta kan vara aktuellt exempelvis beträffande radiotrafik mellan ett provflygplan och markledningen. Vid en signalkontroll kan det framkomma att en person – ofta en anställd i Försvarsmakten – i ett meddelande som inte är skyddat av krypteringsfunktioner röjer en uppgift som omfattas av sekretess. I några sådana fall har det lett till att rättsliga åtgärder har vidtagits mot den som röjt uppgiften. Det har även förekommit att Försvarsmaktens personal har gripit in i ett samtal och förhindrat att ytterligare sekretessbelagd information har röjts.

Signalkontroll sker aldrig i form av hemlig avlyssning. Någon av parterna i t.ex. ett telefonsamtal är alltid medveten om att avlyssning pågår.

Ett meddelande från en signalkontroll sparas oftast i ett särskilt datorsystem för vidare analys. Det system i vilket meddelandena hanteras är helt slutet och är endast tillgängligt för en liten grupp av personer hos TSA. Gruppen består för närvarande av fyra anställda. De meddelanden som sparas från ett kontrolltillfälle sorteras endast så att de kan hänföras till detta tillfälle, och samlas sålunda inte individrelaterat. I verksamheten förs inga särskilda personregister. Någon behandling av personnummer förekommer inte heller i verksamheten. För att kunna konstatera om en viss person förekommer i ett meddelande krävs att inspelningen lyssnas igenom. Meddelandena kan komma att sparas upp till 15 år. Normalt sparas dock ett meddelande endast 5 – 10 år.

5.3.6 Övriga system för automatiserad behandling av personuppgifter

Som beskrivits tidigare bedrivs militär underrättelse- och säkerhetstjänst inte bara centralt vid Högkvarterets enhet MUST, utan även ute på olika förband och enheter. I samband härmed kan det förekomma automatiserad behandling av personuppgifter utan att tillgång finns till de permanenta system som beskrivits ovan. Så sker t.ex. när en organisationsenhet, som även kan innefatta ett förband i utlandsstyrkan, behöver följa upp enskilda personers förehavanden. Behandling av uppgifter kan då ske för att enheten skall kunna fullgöra sina åligganden såväl när det gäller försvarsunderrättelseverksamhet som säkerhetstjänst.

En organisationsenhet kan ha behov av ett eget system med uppgifter som är gemensamt tillgängliga för behöriga personer inom underrättelsefunktionen. I ett sådant system behandlas bl.a. biografiska underrättelser i form av personuppgifter som är av betydelse för t.ex. en aktuell utlandsmission. Syftet med behandlingen är i sådant fall ofta att kunna bedöma staters och eventuellt andra organisationers avsikter i säkerhetspolitiskt och militärt avseende. Uppgifterna kan också komma att kommuniceras med företrädare för andra stater inom uppdraget som har behov av informationen. Säkerhetstjänstfunktionen vid ett förband i utlandsstyrkan kan t.ex. behöva registrera säkerhetshotande händelser inom förbandet.

Även i övrigt förekommer mer tillfällig automatiserad behandling av personuppgifter i ordbehandlingssystem i samband med att olika former av promemorior och andra dokument utarbetas.

Säkerhetsregistret

I säkerhetstjänsten finns ett särskilt system för manuell behandling av personuppgifter rörande händelser som bedöms eller ha konstaterats utgöra säkerhetshotande verksamhet riktad mot Försvarsmakten. Om händelsen kan relateras till viss person och det finns anledning att följa upp denne, registreras personen i ett särskilt kortregister. Detta system benämns *Säkerhetsavdelningens arbetsdiarium* och är ett register över personer med anknytning till säkerhetshotande verksamhet. Den som blir föremål för registrering i registret kan i många fall vara anställd i Försvarsmakten. I registret förekommer endast grundläggande uppgifter samt en anteckning om var ytterligare information om den registrerade finns att hämta. Bakomliggande information finns i promemorior, för närvarande i pappersform. Syftet med registreringen är att kunna bedöma vilket säkerhetshot företrädare för främmande makt eller annan person utgör i Sverige eller från någon annan plats.

Registret förs i dag helt manuellt med hjälp av särskilda registerkort. I detta register kan man endast söka på efternamn. Registret kommer under år 2003 att datoriseras under namnet *Säkerhetsregistret*, varigenom bl.a. sökmöjligheterna kommer att utökas och alla uppgifter om en registrerad kommer att samlas. Uppgifterna kommer då förmodligen att läggas in i IS UNDSÄK eller motsvarande enskilt system. Uppgifterna i registret är tillgängliga endast för en mycket begränsad krets av personer inom MUST.

6 Försvarets radioanstalts informationshantering i underrättelseverksamheten

Försvarets radioanstalt behandlar i sin underrättelseverksamhet en mycket stor mängd information som inhämtas genom signalspaning och från öppna källor. Härtill kommer att den information som hämtas in i signalspaningsverksamheten ofta är krypterad och avfattad på ett främmande språk. För att framställa de rapporter med underrättelser som svarar mot uppdragsgivarnas behov och som är avsikten med underrättelseverksamheten måste den stora informationsmängden bearbetas och analyseras. Med hänsyn härtill är det av grundläggande betydelse för att verksamheten skall kunna bedrivas effektivt att Försvarets radioanstalt kan behandla den inhämtade informationen på automatiserad väg med hjälp av datorer. I enlighet härmed sker all behandling av personuppgifter och annan information inom Försvarets radioanstalts underrättelseverksamhet i datorer.

Försvarets radioanstalt är, precis som Försvarsmakten, en av de myndigheter som skall bedriva försvarsunderrättelseverksamhet. Det grundläggande syftet med behandlingen av personuppgifter är således att kartlägga yttre militära hot mot landet och att utgöra stöd för svensk utrikes-, försvars- och säkerhetspolitik. Försvarets radioanstalts verksamhet som underrättelseorgan tar emellertid även sikte på underrättelseverksamhet i en mer allmän säkerhetspolitisk mening. Försvarets radioanstalt är regeringens civila utrikes- och säkerhetspolitiska inhämtningsorgan. Försvarets radioanstalt är vidare en uppdragstagande myndighet som kan ges särskilda uppdrag som t.ex. att med sin tekniska expertis lämna stöd för annan myndighetsverksamhet än sådan som rör yttre hot (jfr. kap. 3).

6.1 Rättslig reglering av behandling av personuppgifter i Försvarets radioanstalts underrättelseverksamhet

Den behandling av personuppgifter hos Försvarets radioanstalt som omfattas av utredningens uppdrag regleras i dag i förordningen (2001:703) om viss behandling av personuppgifter inom Försvarsmakten och Försvarets radioanstalt. Förordningen gäller utöver personuppgiftslagen i fråga om viss behandling av personuppgifter hos myndigheterna som är helt eller delvis automatiserad. Detta innebär att det är personuppgiftslagens regler som bestämmer förutsättningarna för behandlingen av personuppgifter i den mån det inte finns avvikande bestämmelser i den särskilda förordningen.

I förordningen finns olika allmänna bestämmelser som gäller för all behandling av personuppgifter enligt författningen, således både i Försvarsmaktens och i Försvarets radioanstalts verksamhet. Här finns bestämmelser om tillämpningsområde, personuppgiftsansvar, behandling av känsliga personuppgifter, utlämnande av uppgifter till tredje land, rättelse och skadestånd samt gallring och överklagande. Dessa bestämmelser beskrivs närmare i avsnitt 5.1.

Därutöver finns särskilda bestämmelser som gäller enbart för Försvarsmaktens respektive Försvarets radioanstalts behandling av personuppgifter. Bestämmelserna reglerar vilka register och databaser som får föras i respektive myndighets verksamhet samt under vilka förutsättningar som personuppgifter får behandlas i verksamheten.

Tillämpningsområde (1–2 och 10 §§)

Förordningen gäller utöver personuppgiftslagen i fråga om viss behandling hos myndigheterna som är helt eller delvis automatiserad. Detta innebär att det är personuppgiftslagens regler som bestämmer förutsättningarna för behandling av personuppgifter, i den mån det inte finns avvikande bestämmelser i den särskilda förordningen.

Förordningen gäller för Försvarets radioanstalt när myndigheten fullgör uppgifter enligt lagen (2000:130) om försvarsunderrättelseverksamhet och förordningen (2000:131) om försvarsunderrättelseverksamhet samt enligt 1–3 §§ förordningen (1994:714) med instruktion för Försvarets radioanstalt (se avsnitt 3.2).

Försvarets radioanstalts databaser (10–12 §§)

I förordningen anges, utöver de allmänna bestämmelserna, att Försvarets radioanstalt skall ha vissa särskilda databaser; källdatabas, styrdatabas, analysdatabas och underrättelsedatabas. Databaserna har enligt förordningen till ändamål att möjliggöra den bearbetning av information som behövs för att myndigheten skall kunna fullgöra sina uppgifter.

En källdatabas får endast innehålla obearbetat och automatiskt bearbetat material inhämtat genom signalspaning och från öppna källor. En styrdatabas får endast innehålla långsiktiga inhämtningsdirektiv eller kortsiktig spaningsinriktning. En analysdatabas får endast innehålla analysresultat samt bearbetnings- och rapportunderlag, och en underrättelsedatabas får endast innehålla färdiga rapporter.

Det anges särskilt att Försvarets radioanstalts databaser får innehålla personuppgifter endast om det är nödvändigt för att myndigheten skall kunna fullgöra sina uppgifter enligt ovan nämnda författningar.

6.2 Behandling av personuppgifter i Försvarets radioanstalts underrättelseverksamhet

Försvarets radioanstalt bedriver signalspaning. Signalspaning sker genom att man med mottagarsystem och andra elektroniska hjälpmedel registrerar telesändningar och signaler för att hämta in information som kan användas i underrättelseverksamheten. Signalerna kan komma från kommunikation genom tal, telegrafi, data och fjärrskrift eller ha andra funktioner i samband med radar, navigering eller överföring av mätvärden. Försvarets radioanstalt hämtar också in underrättelser från öppna källor, såsom t.ex. Internet. Den information som Försvarets radioanstalt härigenom erhåller kan omfatta allt från det utrikes- och försvarspolitiska området till detaljuppgifter om t.ex. enskilda militära förband eller vapensystem. I underrättelseverksamheten ingår också rapportering av underrättelser som till viss del innehåller personuppgifter. Det rör sig härvid om uppgifter om personer som är av intresse för Sverige ur utrikes-, försvars- eller säkerhetspolitiskt hänseende.

För att på ett rationellt sätt kunna hantera denna mycket omfattande och komplexa informationsmängd sker bearbetning och analys med hjälp datorer. All behandling av personuppgifter i

Försvarets radioanstalts underrättelseverksamhet sker datoriserat. Myndigheten för inga manuella register och behandling sker heller inte i fristående persondatorer.

6.3 System för automatiserad behandling av personuppgifter m.m.

De personuppgifter i Försvarets radioanstalts underrättelseverksamhet som hämtats in genom signalspaning och från öppna källor lagras i elektronisk form i olika uppgiftssamlingar (databaser). Uppgifterna är sedan gemensamt tillgängliga för en eller flera handläggare inom myndighetens underrättelseverksamhet. De olika uppgiftssamlingarna är inte fysiskt skilda från varandra på så sätt att de endast är tillgängliga via särskilda datorer. Avgörande för vilken databas en uppgift tillhör är i stället tillvägagångssättet för att ta del av informationen. Tillgång till den information som finns lagrad i de olika uppgiftssamlingarna erhålls via access som är speciell för varje enskild databas. Den underrättelseinformation och andra uppgifter som finns i den enskilda databasen kan handläggaren få tillgång till enligt de särskilda kriterier som gäller för respektive databas, med den begränsning som handläggarens behörighet medger. Tillgången till uppgifter i Försvarets radioanstalts olika databaser är reglerad genom ett särskilt behörighetssystem med ett flertal nivåer. Vilken åtkomst varje enskild handläggare har till uppgifter i de olika databaserna beror på vilken grupp denne tillhör i organisationen.

Försvarets radioanstalts system för behandling av personuppgifter i sin underrättelseverksamhet är helt anpassat till underrättelseprocessen. Här finns särskilda uppgiftssamlingar till stöd för alla väsentliga delar i underrättelseprocessen, såväl för inriktning och inhämtning som för bearbetning och analys samt delgivning. För inriktning av myndighetens underrättelseverksamhet används Urvalsdatabasen. Information som hämtas in lagras i Källdatabasen eller Databasen för öppna källor. Bearbetning och analys sker i Analysdatabasen och underrättelserapporterna som är färdiga för delgivning lagras i Rapportdatabasen. Försvarets radioanstalts underrättelseproduktion illustreras av *bilaga 2*.

6.3.1 Urvalsdatabasen – planering och inriktning

Urvalsdatabasen består av en samling uppgifter som används för planering och inriktning av underrättelseverksamheten. Försvarets radioanstalt bedriver som tidigare nämnts signalspaning och underrättelseverksamhet i övrigt enligt den inriktning som regeringen, Försvarsmakten och övriga uppdragsgivare anger. Underrättelseverksamheten styrs härvid främst genom riktlinjer och anvisningar från regeringen och de uppgifter som Försvarsmakten ger myndigheten. Därutöver deltar Försvarets radioanstalt i ett internationellt samarbete på försvarsunderrättelsetjänstens område.

Utöver de riktlinjer som Försvarets radioanstalt erhåller i form av t.ex. statsmakternas försvarsbeslut och regleringsbrev bidrar uppdragsgivarna och partners även med mer detaljerad information för planering och inriktning av myndighetens underrättelseverksamhet. Informationen som på så sätt kommer in till myndigheten består av meddelanden som tas emot av berörd personal vid Försvarets radioanstalts underrättelseavdelning. Denna information innehåller uppgifter som bedömts vara nödvändiga för pågående uppdrag och för framtida behov av underrättelseinhämtning. Underrättelseavdelningen sammanställer och överför sedan informationen till lämplig uppgiftssamling i Försvarets radioanstalts system av databaser, t.ex. Urvalsdatabasen.

I Urvalsdatabasen, som tidigare var benämnd tele- och adressregistret, behandlas främst sökord i form av olika personuppgifter, såsom t.ex. namn. Den information som lagras i Urvalsdatabasen används för inriktning på kort och på lång sikt av Försvarets radioanstalts underrättelseverksamhet. Uppgifterna i databasen används i underrättelseverksamheten vid sökning genom signalspaning och i öppna källor. Spaning sker även efter vissa tekniska parametrar, vilka även de återfinns i Urvalsdatabasen. Med parametrar avses såväl manuella som automatiska frekvenser, e-postadresser och telefonnummer.

Urvalsinformationen i urvalsdatabasen benämns som antingen långsiktiga inhämtningsdirektiv eller kortsiktig spaningsinriktning. Långsiktig inriktning är på årsbasis. Den kortsiktiga inriktningen utformas via en löpande dialog mellan Försvarets radioanstalt och dess uppdragsgivare, i första hand regeringen och Försvarsmakten. Försvarets radioanstalt har därutöver en särskild inriktning för varje vecka som är koncentrerad till ett särskilt problemområde.

6.3.2 Källdatabasen – inhämtning genom signalspaning

Källdatabasen är den primära databasen för lagring av den information som Försvarets radioanstalt hämtar in i sin underrättelseverksamhet. Ändamålet med databasen är att underlätta tillgången till och behandlingen av den information som myndigheten hämtar in genom signalspaning. Källdatabasen innehåller endast hemlig information i form av signalspaningsmaterial.

Inhämtning sker såväl utan urval som enligt särskilda sökkriterier. Ofta sker inget urval vid inhämtning genom signalspaning, varför databasen tillförs stora mängder obearbetad information. Källdatabasen är på så sätt ”en spegling” av förekommande signaler. Det inhämtade materialet kan vara såväl krypterat som avfattat på ett främmande språk. Försvarets radioanstalt vet således inte på detta stadium i underrättelseprocessen vilken information uppgifterna innehåller.

Försvarets radioanstalt genomför också signalspaning enligt de särskilt utvalda sökkriterier som återfinns i Urvalsdatabasen. Sökning sker då efter dels tekniska parametrar, dels särskilda sökord. Med tekniska parametrar avses t.ex. frekvenser. De särskilda sökorden är t.ex. e-postadresser och telefonnummer.

Källdatabasen är en mycket omfattande databas. Till denna förs ständigt nya uppgifter med den konsekvensen att äldre information i princip överlagras när kapacitetstaket nåtts. Lagringstiden varierar starkt. Merparten av data lagras mycket kort tid, men det finns också information som kan behöva lagras under lång tid.

Källdatabasen innehåller, om än till mindre del, personuppgifter som kan eftersökas. Sökorden som används kan då vara t.ex. namn på personer, adresser eller personnummer. I sakens natur ligger att även personuppgifter som rör politiska åsikter, etniskt ursprung och andra känsliga personuppgifter kan förekomma. Behandling av känsliga personuppgifter är en förutsättning för att Försvarets radioanstalt skall kunna utföra sitt uppdrag som leverantör av underrättelser. Sådan känslig information är inte intressant i sig men kan i kombination med andra uppgifter vara av största betydelse för rapporteringen.

6.3.3 Databasen för öppna källor – inhämtning

Till Försvarets radioanstalts uppgifter hör att ha en övergripande bevakning av vad som sker i omvärlden och det som kan påverka

Sverige i utrikes-, försvars- och säkerhetspolitiskt hänseende. Detta görs t.ex. genom prenumeration på utländska tidningar, sökning av information på Internet eller helt enkelt genom inhämtning av uppgifter från olika webbsidor. Internet är således en viktig källa för information och inhämtning sker numera helt automatiskt.

De uppgifter som samlats in från sådana öppna källor lagras regelmässigt en kort tid i Databasen för öppna källor. I databasen kan myndighetens handläggare i underrättelseverksamheten söka information genom användandet av särskilda sökord. Dessa sökord utgörs antingen av de urvalskriterier som finns i Urvalsdatabasen eller är handläggarens egna. Om uppgifterna bedöms kunna vara av intresse för underrättelseverksamheten förs uppgifterna över till Analysdatabasen för vidare bearbetning och analys.

Databasen för öppna källor innehåller personuppgifter, avseende framför allt utländska men även svenska medborgare, samt uppgifter med anknytning till vissa personer. Detta är i stor utsträckning samma uppgifter som återfinns i Urvalsdatabasen i form av sökord och andra urvalskriterier. Personuppgifterna används som sökord och fungerar således som ingång till andra uppgifter om personer som är intressanta i underrättelseverksamheten.

Varje dag inhämtas ett mycket stort antal personuppgifter från öppna källor. Det är emellertid endast en bråkdel av denna information som sparas för vidare bearbetning innan informationen, på grund av att kapacitetstaket i Databasen för öppna källor nåtts, överlagras av ny information och på så sätt försvinner. Det är vidare ytterst få av de uppgifter som lagras i databasen som är att betrakta som känsliga i personuppgiftslagens mening.

För Försvarets radioanstalt är det av stor betydelse med en databas enbart för information hänförlig till öppna källor. Under de senaste åren har en allt större mängd personinformation kommit att samlas in just från öppna källor. Denna form för insamling av underrättelseinformation beräknas också öka kraftigt i framtiden. Vidare är den information som samlas in via öppna källor inte hemlig innan den har överförts till Analysdatabasen för vidare bearbetning, till skillnad från signalspaningsmaterial som i princip är hemligt redan vid själva inhämtningen. Såväl med hänsyn till den stora informationsmängden som till sekretess är det således en fördel med en särskild databas för öppna källor.

6.3.4 Analysdatabasen – bearbetning och analys

I Analysdatabasen sker analys och annan bearbetning, såsom dekryptering och översättning, av den information som Försvarets radioanstalt hämtat in och lagrat i Källdatabasen samt Databasen för öppna källor. Bearbetning går ut på att göra materialet läsbart och hanterbart för analys. I Analysdatabasen mellanlagras också arbetsmaterialet, innan det färdigställs till underrättelserapporter och lagras i Rapportdatabasen. I Analysdatabasen görs bedömningen av om Försvarets radioanstalt skall arbeta vidare med materialet eller om det skall sållas bort.

I databasen behandlas både hemlig och öppen information. Med öppen information avses i princip uppgifter som tillförts verksamheten på annat sätt än genom signalspaning. Den öppna informationen samlas som tidigare nämnts i första hand in genom automatiska sökningar på Internet och lagras inledningsvis i Databasen för öppna källor. Den information som bedöms vara av intresse för underrättelseverksamheten överförs sedan från Databasen för öppna källor till Analysdatabasen där den blir hemlig, men där ursprunget blir tydligt spårbart.

Resultatet av arbetet i Analysdatabasen kan komma att levereras från Försvarets radioanstalt om slutprodukten är av godkänd kvalitet. Det sker i så fall i form av rapporter. Dessa rapporter lagras i Rapportdatabasen.

6.3.5 Rapportdatabasen – delgivning

Rapportdatabasen innehåller endast Försvarets radioanstalts underrättelserapporter. I rapporterna finns de underrättelser som myndighetens uppdragsgivare erhåller. Av varje rapport framgår det ämne rapporten behandlar och den uppdragsgivare som skall ha rapporten. I databasen kan rapporter eftersökas genom namn på uppdragsgivare, datum på rapporten eller det ämne rapporten behandlar. På så sätt liknar databasen ett register.

I de slutliga underrättelserapporterna har all ovidkommande information sållats bort. I rapporterna presenteras enbart allt det som bedöms vara väsentligt för Försvarets radioanstalts uppdragsgivare. Försvarets radioanstalt lämnar även ut uppgifter inom ramen för det internationella underrättelsesamarbete som myndigheten deltar i.

Försvarets radioanstalt levererar endast färdiga rapporter. Rapporterna kan delges myndighetens uppdragsgivare och andra behöriga mottagare via datorsamband. Fram tills i dag har emellertid av sekretesskäl huvuddelen av rapporterna delgivits i pappersform. Under år 2003 kommer rapportdatabasen att göras tillgänglig för vissa mottagare av rapporter via direktåtkomst med särskilda begränsningar. Härigenom kommer allt fler rapporter att överlämnas i elektronisk form.

VÅRA ÖVERVÄGANDEN